**Die Landesbeauftragte
für den Datenschutz und
für das Recht auf Akteneinsicht**

LAND BRANDENBURG

LDA

Schutz der
- *Persönlichkeitsrechte*
- *Informationsfreiheit*

Tätigkeitsbericht 2014/2015

- 18. Tätigkeitsbericht -

Tätigkeitsbericht

der Landesbeauftragten für den Datenschutz

und für das Recht auf Akteneinsicht

zum 31. Dezember 2015

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 8. April 2014 vorgelegten Tätigkeitsbericht 2012/2013 an und deckt den Zeitraum vom 1. Januar 2014 bis zum 31. Dezember 2015 ab.

Der Tätigkeitsbericht kann auch aus unserem Internetangebot unter

http://www.lda.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: E899 5780 7F65 F282 8CAC
C504 37F3 83FE 0844 834D

Druck: Brandenburgische Universitätsdruckerei und Verlagsgesellschaft
Potsdam mbH

Inhaltsverzeichnis

Teil C
Akteneinsicht und Informationszugang

Teil D
Die Dienststelle

Anlagen

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

Einleitung

„Jede Person hat das Recht
auf Schutz der sie betreffenden personenbezogenen Daten.“

Mit diesem Satz beginnt Artikel 8 der Charta der Grundrechte der Europäischen Union. Er ist das Versprechen und die Aufforderung, den Schutz der Persönlichkeitsrechte als gemeinsamen europäischen Grundwert zu gewährleisten. Die Verarbeitung personenbezogener Daten stellt einen Eingriff in die Privatsphäre dar und darf nur erfolgen, wenn die Betroffenen eingewilligt haben oder eine Rechtsgrundlage dafür besteht. Sie ist stets an einen festgelegten Zweck gebunden.

Nie zuvor waren personenbezogene Daten so sehr ein Wirtschaftsgut wie heute. Nie zuvor wurde das Grundrecht auf Datenschutz so sehr infrage gestellt. Big Data ist das große Zauberwort, das erfolgreiche wirtschaftliche und segensreiche wissenschaftliche Entwicklungen verspricht. Personenbezogene Daten, also die Daten jedes Einzelnen von uns, werden als das Öl oder das Gold der Zukunft bezeichnet.

Was aber bedeutet Big Data? Mit dem Begriff wird die Verarbeitung großer Datenmengen sowie ihre Auswertung nach unterschiedlichsten Gesichtspunkten bezeichnet. Je größer der hierzu genutzte Datenvorrat ist, desto zielgerichteter kann die Analyse erfolgen. Beispielsweise können auch Fragen der Wahrscheinlichkeit zukünftiger persönlicher Entwicklungen beantwortet werden. Das Interesse insbesondere der Werbewirtschaft, der Pharmaindustrie, der Versicherungen oder der Wissenschaft an solchen Analysen ist groß.

Mit dem Grundrecht auf den Schutz der eigenen personenbezogenen Daten und dem Ziel der Wirtschaft, eben diese Daten mittels Big-Data-Verfahren zu nutzen, stehen sich zwei völlig unterschiedliche Interessen gegenüber. Unsere Gesellschaft muss entscheiden, welche Bedeutung das Grundrecht auf Datenschutz bei der Entwicklung von Big Data haben soll. Bisher verlaufen die Diskussionen sehr einseitig. Datenschutz wird als Behinderung der wirtschaftlichen Entwicklung angesehen und nicht wenige Kritiker fordern, ihn hinter die wirtschaftlichen Interessen zurücktreten zu lassen. Doch damit machen sie es sich zu einfach. Ein Grundrecht kann nicht ohne Weiteres eingeschränkt werden. Vielmehr bedarf es in diesem Interessenkonflikt der Erkenntnis, dass auch bei jeder wirtschaftlichen Entwicklung Grundrechte zu wahren sind. Das Recht auf informationelle Selbstbestimmung sollte ein Ansporn dafür sein, bei der Entwicklung neuer Produkte von Anfang an datenschutzgerechte Lösungen und Privacy by Design zu verwirklichen. So können technische Innovationen mit Datenschutz sinnvoll verbunden werden.

Niemand fordert den Verzicht auf die Entwicklung innovativer Produkte. Die technischen Entwicklungen, die heute möglich sind, können die Gesellschaft in jeder Hinsicht verändern. Sie bieten Chancen und Risiken zugleich. Europa kann mithilfe seiner Grundrechte den Menschen bei technischen Entwicklungen in den Mittelpunkt stellen. Und hierzu gehört in einer Welt, in der personenbezogene Daten zu einem Rohstoff geworden sind, die Beachtung des Grundrechts auf den Schutz der eigenen Daten, die informationelle Selbstbestimmung. Das Grundrecht als einen Wert begreifbar zu machen, für den sich der Einsatz lohnt, ist eine meiner wichtigsten Aufgaben als Datenschutzbeauftragte.

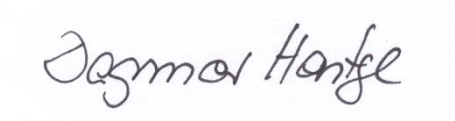
Der Europäische Gerichtshof hat in den vergangenen Jahren mit seinen Urteilen zu Artikel 8 der Charta der Grundrechte wiederholt sehr deutlich gezeigt, dass er die Grundrechte gegen Angriffe verteidigt. Beispiele hierfür sind die Entscheidung zur Vorratsdatenspeicherung, die Google-Entscheidung zum sog. Recht auf Vergessenwerden und die Schrems-Entscheidung zu Safe Harbor.

Auch für die Bürgerinnen und Bürger ist Datenschutz in ihrem Alltag ein ständiges Thema. Sie erleben täglich, dass ihre Persönlichkeitsrechte nicht immer den Schutz erhalten, der ihnen zusteht. Unwissen und Unachtsamkeit der verantwortlichen Stellen führen im Alltag zu zahlreichen Datenschutzverletzungen. Teilweise geschieht dies auch mit Vorsatz. Mein Tätigkeitsbericht für die Jahre 2014 und 2015 zeigt auf, welche Datenschutzthemen in Brandenburg von besonderer Bedeutung waren.

Ein Thema, das mir seit dem Beginn meiner Tätigkeit sehr am Herzen liegt, ist die Datensicherheit. Hier gilt der Satz: „Wir sind auf dem Weg, aber noch lange nicht angekommen.“ Auch in Brandenburg machen die Gefährdungen im Bereich der IT-Sicherheit weder vor öffentlichen noch vor privaten Stellen halt. Es geht deshalb bei meiner Arbeit nicht zuletzt darum, die Verantwortlichen dazu zu bewegen, das Thema ernst zu nehmen und ihren Einsatz für Verbesserungen trotz der damit verbundenen Kosten weiter zu intensivieren.

Liebe Leserinnen und Leser, ich wünsche Ihnen bei der Lektüre meines Tätigkeitsberichts für die Jahre 2014 und 2015 viele neue Erkenntnisse und eine interessante Lektüre.

Kleinmachnow, den 12. April 2016



Dagmar Hartge

Teil A

Brennpunkte

1 Die europäische Datenschutz-Grundverordnung auf der Zielgeraden

Die Beratungen zur EU-Datenschutz-Grundverordnung[1] sind mit den Trilogverhandlungen zwischen Europäischem Parlament, Rat der Europäischen Union und Europäischer Kommission Mitte 2015 in die entscheidende Phase eingetreten. Für die Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder war von Anfang an ein verbesserter, mindestens aber dem bisherigen Standard gleichwertiger Grundrechtsschutz von außerordentlicher Bedeutung. Sie richtete deshalb an die Trilogpartner nochmals den Appell, die Datenschutz-Grundverordnung in wesentlichen Punkten nachzubessern.[2]

Der Kompromisstext des Europäischen Parlaments zur Datenschutz-Grundverordnung griff viele der von der Datenschutzkonferenz zum Kommissionsvorschlag zuvor dargelegten Empfehlungen auf. Dagegen stellte der Ratsvorschlag sogar grundlegende Prinzipien des Datenschutzes infrage. Hierauf richtete sich die aktuelle Kritik der Konferenz.

Sie forderte die explizite Verankerung des Prinzips der Datenvermeidung und Datensparsamkeit in der Verordnung. In Anbetracht der Allgegenwärtigkeit der Datenverarbeitung und des Einsatzes von Big-Data-Technologien werden sehr große Mengen (auch personenbezogener) Daten erzeugt. Für eine möglichst grundrechtsschonende Datenverarbeitung haben sich sowohl Staat als auch Wirtschaft auf das notwendige Maß zu beschränken.

Des Weiteren wurde der Grundsatz der Zweckbindung, welcher in der Europäischen Grundrechtecharta als tragendes Prinzip des Datenschutzes verankert ist, nicht hinreichend berücksichtigt. Die Zweckbindung dient der Transparenz und Vorhersehbarkeit der Verarbeitung personenbezogener Daten und stärkt damit die Autonomie der Betroffenen. Insoweit war die vom Rat vorgeschlagene Regelung, mit der Zweckänderungen in einem sehr weiten Umfang zugelassen würden, abzulehnen.

---

1 siehe Tätigkeitsbericht 2012/2013, B 1

2 Entschließung „Datenschutz-Grundverordnung darf keine Mogelpackung werden“ vom 18./19. März 2015 (Anlage 1.3.2) und Stellungnahme „Datenschutzrechtliche Kernpunkte für die Trilogverhandlungen zur Datenschutz-Grundverordnung“ vom 14. August 2015 (http://www.lda.brandenburg.de)

Darüber hinaus verlangte die Konferenz, dass die Einwilligung des Betroffenen auch weiterhin seine Datenhoheit sichern muss. Das Recht auf informationelle Selbstbestimmung bedeutet, dass der Einzelne im Rahmen der Einwilligung grundsätzlich selbst über die Preisgabe und Verwendung seiner personenbezogenen Daten entscheiden kann. Eine Einwilligung ist aber nur dann ein wesentliches Element zur Gewährleistung der Datenhoheit, wenn sie durch eine ausdrückliche Willensbekundung erfolgt. Lediglich unmissverständliche Einwilligungserklärungen, wie der Rat sie vorgeschlagen hatte, würden es den global agierenden Diensteanbietern ermöglichen, durch pauschale Datenschutzbestimmungen und datenschutzunfreundliche Voreinstellungen weitreichende Datenverarbeitungsbefugnisse ohne ausdrückliche Einwilligung des Nutzers für sich zu reklamieren. Eine solche stillschweigende Erlaubnis der Datenverarbeitung hätte für Betroffene den Nachteil, ihr aktiv widersprechen zu müssen (Opt-out). Den Ratsvorschlag hat die Konferenz daher als unzureichend abgelehnt.

Damit einhergehend sprachen sich die unabhängigen Datenschutzbehörden des Bundes und der Länder auch für umfassende Informationsrechte der Betroffenen und gegen die vom Rat vorgesehenen Beschränkungen aus. Betroffene müssen in die Lage versetzt werden, Umfang und Risiko der Datenverarbeitung einzuschätzen. Die Ausübung ihrer Rechte und die hierfür von der verantwortlichen Stelle zu ergreifenden Maßnahmen müssen für sie unentgeltlich sein.

Zudem hat die Konferenz auch eine wirksame Begrenzung der Profilbildung gefordert, weil die vorgesehenen Regelungen hier zu kurz griffen. Sie wies daher erneut auf die Notwendigkeit einer strikten Regelung zur Profilbildung hin, mit der einer Zusammenführung und Auswertung personenbezogener Daten über eine Person enge Grenzen gesetzt werden.

Nach den Enthüllungen von Edward Snowden ist zudem ein besserer Schutz der personenbezogenen Daten von europäischen Bürgern gegenüber Behörden und Gerichten in Drittstaaten sowie mehr Transparenz und Kontrolle im Hinblick auf die nachrichtendienstliche Überwachung dringend geboten. Insoweit schloss sich die Konferenz dem Vorschlag des Parlaments an, wonach Urteile von Gerichten und Entscheidungen von Verwaltungsbehörden eines Drittstaates, die von einer Daten verarbeitenden Stelle die Weitergabe personenbezogener Daten verlangen, in der EU nur auf der Grundlage internationaler Übereinkommen zur Amts- und Rechtshilfe anerkannt und vollstreckt werden.

Die o. g. und weitere Kernforderungen der Konferenz wurden im Rahmen eines Meinungsaustausches mit den Trilogpartnern erörtert, an dem die Landesbeauftragte teilnahm. Erfreulicherweise sind einige Forderungen noch in den Text der Datenschutz-Grundverordnung eingeflossen, auf den sich die

Trilogpartner schließlich im Dezember 2015 geeinigt haben, wie die Verankerung des Prinzips der Datensparsamkeit, die Zweckbindung oder Regelungen zur Datenübermittlung an Behörden und Gerichte in Staaten außerhalb der EU. Andere Punkte, wie die ausdrückliche Einwilligung oder die wirksame Begrenzung der Profilbildung, sind jedoch leider nicht aufgenommen worden. Ein verbesserter, zumindest aber dem bisherigen Standard gleichwertiger Grundrechtsschutz wurde damit aus deutscher Sicht zwar nicht erreicht, die Einigung auf ein europaweit einheitliches Datenschutzniveau stellt jedoch eine beachtenswerte Errungenschaft dar. Die Datenschutz-Grundverordnung kann nun tatsächlich im Frühjahr 2016 in Kraft treten und nach einem Übergangszeitraum von zwei Jahren 2018 zur Anwendung kommen.

Gerade in Zeiten von Big Data und globaler Datenverarbeitung sind die Autonomie des Einzelnen, Datensparsamkeit, Zweckbindung und die Gewährleistung der Betroffenenrechte wichtige Elemente des Grundrechts auf informationelle Selbstbestimmung. Zumindest einige Forderungen der Datenschutzbehörden wurden in den Trilogverhandlungen berücksichtigt. Diese sind mittlerweile abgeschlossen. Nun ist die Umsetzung der europäischen Datenschutz-Grundverordnung durch alle Beteiligten vorzubereiten.

2 Gesundheit

2.1 E-Health-Gesetz – digitale Wende im Gesundheitswesen

Zu Beginn des Jahres 2015 wurde vom Bundesgesundheitsministerium der Entwurf eines Gesetzes für sichere digitale Kommunikation und Anwendungen im Gesundheitswesen (E-Health-Gesetz) vorgelegt. Der Deutsche Bundestag verabschiedete es zum Ende des Berichtszeitraums.[3] Das Gesetz sieht eine Fülle neuer Elemente im Gesundheitsbereich vor.

Insbesondere soll durch Fristvorgaben die zügige Einführung zusätzlicher Anwendungen auf der elektronischen Gesundheitskarte unterstützt werden.

Geplant ist, auf Wunsch der Patienten auch Notfalldaten auf der Gesundheitskarte zu speichern, auf die Ärzte ggf. auch ohne Mitwirken der Betroffenen zugreifen können. Zur Vermeidung von gefährlichen Wechselwirkungen zwischen Arzneimitteln erhalten insbesondere chronisch kranke Versicherte einen Anspruch auf einen Medikationsplan. Dieser soll zunächst in Papier-

3 Gesetz für sichere digitale Kommunikation und Anwendungen im Gesundheitswesen vom 21. Dezember 2015, BGBl. I S. 2408

form, von 2018 an auch über die elektronische Gesundheitskarte zur Verfügung stehen.

Bis Ende 2018 müssen die Voraussetzungen für eine umfassende digitale Patientenakte z. B. mit Arztbriefen, Notfalldaten und Medikationsplan geschaffen werden. Zeitgleich ist ein funktionierendes „Patientenfach“ einzurichten. Unabhängig von der Möglichkeit, in einer Arztpraxis Einsicht in die auf der Karte gespeicherten Daten nehmen zu können, sollen die Versicherten zukünftig in die Lage versetzt werden, sich mit der elektronischen Gesundheitskarte eigenständig über den Inhalt ihrer elektronischen Patientenakte zu informieren. Die Betroffenen können dort dann auch noch eigene Eintragungen vornehmen.

Die Zusammenarbeit zwischen Krankenhäusern und Arztpraxen soll entscheidend verbessert und beschleunigt werden. Deshalb ist eine finanzielle Unterstützung elektronischer Arztbriefe im Jahr 2017 vorgesehen. Durch die technische Vernetzung der an einer Behandlung Beteiligten soll darüber hinaus eine funktionierende Telematikinfrastruktur im Gesundheitswesen entstehen. Zur Förderung dieser Infrastruktur ist beispielsweise geplant, dass Behandelnde etwa Fachärzte bzw. besondere Spezialisten mithilfe der Telemedizin zu Röntgenaufnahmen befragen können.

Auch Online-Videosprechstunden können ab Juli 2017 von Kassenpatienten als ärztliche Leistung in Anspruch genommen werden. Weite Entfernungen zur Arztpraxis, die eigene urlaubsbedingte Abwesenheit, ein Umzug oder berufliche Anlässe sowie eine eingeschränkte Mobilität des Versicherten werden durch die Möglichkeit aufgefangen, zukünftig über einen PC oder Laptop mit Kamera und Mikrofon einen vorab vereinbarten Termin mit seinem Arzt auch von zu Hause oder aus der Ferne wahrzunehmen.

Durch ein sogenanntes Interoperabilitätsverzeichnis der Gesellschaft für Telematikanwendungen der Gesundheitskarte mbH (gematik), die schon für die Einführung der elektronischen Gesundheitskarte verantwortlich ist, soll die Kommunikation der im Gesundheitsbereich eingesetzten IT-Systeme weiter verbessert werden. Das Verzeichnis soll einheitliche technische und inhaltliche Standards vorgeben, um zu gewährleisten, dass die Zusammenarbeit technisch auch funktioniert.

Bereits zu dem umfangreichen Gesetzentwurf hatte die Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder im Frühjahr 2015 eine Entschließung verabschiedet. Drei Punkte waren dabei besonders wichtig:

- Entgegen der Gesetzeslage und entsprechenden Ankündigungen war eine Erprobung des Patientenzugriffs zunächst unterblieben. Die Umset-

zung des Zugriffsrechts der Betroffenen auf ihre Daten ist jedoch Voraussetzung für die Wahrnehmung ihrer Rechte insbesondere auf Auskunft und Löschung. Die Konferenz hat daher die Erprobung gefordert, um sicherzustellen, dass die Versicherten ihre gesetzlich zugestandenen Rechte auch wahrnehmen können.

- Bei der Erstellung des Interoperabilitätsverzeichnisses sind auch Datenschutzexperten beratend hinzuzuziehen, um zu gewährleisten, dass das hohe Schutzniveau von Gesundheitsdaten eingehalten wird.

- Angesichts des Umfangs der EDV-Ausstattung ihrer Praxen sowie des oft fehlenden praxisinternen Sachverstands sind Ärzte inzwischen regelmäßig auf externe IT-Dienstleister angewiesen. Bei der Vergabe von Aufträgen an diese Dienstleister besteht für die Ärzte als Berufsgeheimnisträger die Gefahr, gegen ihre Schweigepflicht zu verstoßen und sich nach § 203 Strafgesetzbuch strafbar zu machen, wenn sie nicht von allen Patienten die Einwilligung zur Datenverarbeitung durch den Auftragnehmer eingeholt haben. Die Konferenz hat erneut darauf hingewiesen, dass es hier einer rechtlichen Regelung bedarf: Die Offenbarung von Patientendaten an einen Dienstleister ist auf das unbedingt Erforderliche zu beschränken. Der Auftragnehmer muss nicht nur den Weisungen des Arztes unterworfen werden, sondern auch einer Verschwiegenheitspflicht, die der speziellen ärztlichen Schweigepflicht vergleichbar ist.

Die Forderungen der Datenschutzbehörden wurden in unterschiedlichem Maße berücksichtigt. So räumt das E-Health-Gesetz, wie bereits oben dargestellt, den Betroffenen ab dem Jahr 2018 nunmehr einen Anspruch auf ein digitales Patientenfach ein, über welches sie sich umfassend und ohne das Einschalten der Arztpraxen über ihre Behandlung informieren können. Zwar nennt das Gesetz weiterhin nicht ausdrücklich die Möglichkeit, Datenschutzexperten hinzuzuziehen, schließt jedoch auch nicht völlig aus, dass beispielsweise der Vertreter einer Landesdatenschutzbehörde als Experte berufen werden könnte. Keine Berücksichtigung fand die Forderung nach einer Regelung zur Schweigepflicht der von den Ärzten beauftragten IT-Dienstleister. Offen ist, ob dies durch das Bundesministerium der Justiz und für Verbraucherschutz im Rahmen einer Änderung des Strafgesetzbuchs aufgegriffen werden wird.

Gerade bei der Verarbeitung besonders sensitiver Daten im Gesundheitsbereich darf nicht nur das technisch Machbare im Mittelpunkt stehen. Stets sind auch die Persönlichkeitsrechte der Patienten zu wahren.

2.2 Fernwartung medizinischer Geräte

Zwei Krankenhäuser wandten sich an uns mit der Frage, ob sie mit einem bayerischen Unternehmen einen Vertrag über eine Fernwartung schließen können. Dem Auftragnehmer sollte darin das Recht eingeräumt werden, einen Subunternehmer außerhalb des Europäischen Wirtschaftsraumes in die Vertragserfüllung einzubeziehen.

Das Brandenburgische Datenschutzgesetz (BbgDSG) enthält in § 11 a spezielle Vorschriften zur Wartung von Datenverarbeitungssystemen. Diese sind bereits von Anfang an so zu gestalten, dass bei ihrer Wartung möglichst nicht auf personenbezogene Daten zugegriffen werden kann. Sofern dies nicht sichergestellt ist, hat der Auftraggeber durch technisch-organisatorische Maßnahmen zu gewährleisten, dass nur der Zugriff auf die für die Wartung unbedingt erforderlichen Daten möglich ist.

Wartungen durch externe Dienstleister bedürfen gem. § 11 Abs. 2 BbgDSG einer schriftlichen Vereinbarung. Kann ein Zugriff auf personenbezogene Daten nicht ausgeschlossen werden, so gilt: Der Auftrag ist unter Festlegung des Gegenstandes und des Umfanges der Wartung, der technischen und organisatorischen Maßnahmen und etwaiger Unterauftragsverhältnisse schriftlich zu erteilen. Der Auftraggeber hat vor Vertragsschluss zu prüfen, ob der Auftragnehmer tatsächlich Gewähr für die Einhaltung der technischen und organisatorischen Maßnahmen nach § 10 BbgDSG bietet. Die mit Wartungsarbeiten betrauten Personen sind zur Wahrung des Datengeheimnisses zu verpflichten.

Auftragnehmer gelten datenschutzrechtlich als Teil des Auftraggebers. Werden Daten an sie offenbart, handelt es sich um eine interne Datennutzung gem. § 3 Abs. 2 Nr. 7 BbgDSG, jedoch nicht um eine Übermittlung an einen Dritten. Dennoch ist nach unserer Ansicht für Patientendaten eine Offenbarungsbefugnis nach § 203 Strafgesetzbuch (StGB) erforderlich. Eine Wartungsfirma kann nach unserer Auffassung nicht als berufsmäßiger Gehilfe i. S. d. § 203 Abs. 3 Satz 2 StGB – quasi als medizinisches Hilfspersonal – angesehen werden, an den die Offenbarung von Geheimnissen der Patienten zulässig wäre. Wir vertreten gerade auch im Interesse der Auftragnehmer die Auffassung, dass das Strafgesetzbuch insoweit eng auszulegen ist. Der herrschenden Meinung schließen wir uns damit an. Auch die Regelungen zum Beschlagnahmeschutz gem. § 97 Strafprozessordnung zeigen, dass der Gesetzgeber Dienstleister nicht mit Gehilfen gleichsetzt, denn für beide gelten unterschiedliche Absätze dieser Vorschrift.

Auch wenn die Gesetzesbegründung zu § 11 a BbgDSG davon ausgeht, dass die für den Auftragnehmer des Wartungsvertrages tätigen Personen auch dem Berufsgeheimnis unterliegen, widerspricht dies den strafrechtlichen

Vorschriften und der herrschenden Meinung. Dementsprechend ist im Gesetzestext des § 11 a BbgDSG selbst nur die Verpflichtung auf die Wahrung des Datengeheimnisses gefordert. Dieses Schutzniveau genügt nicht, um der ärztlichen Schweigepflicht ausreichend Rechnung zu tragen.

Darüber hinaus dürfen Patientendaten gemäß § 28 Abs. 1 Nr. 1 Brandenburgisches Krankenhausentwicklungsgesetz nur zur Behandlung des Patienten genutzt werden. Aufgrund der Zweckbindung haben wir Bedenken, diese Regelung als Befugnis zur Datenweitergabe an den Auftragnehmer eines Wartungsvertrages anzusehen, da der Behandlungsbegriff so extrem weit ausgelegt würde.

Wir können daher nicht ausschließen, dass Ermittlungsbehörden und Strafgerichte zu dem Schluss kommen, dass eine Wartung mit Offenbarung personenbezogener Gesundheitsdaten ohne Einwilligung der Patienten den Tatbestand des § 203 StGB erfüllt. Eine Einwilligungslösung erscheint uns dabei jedoch nicht wirklich praktikabel. Insgesamt haben wir von einer Wartung mit Zugriff auf Patientendaten, die von nicht medizinischem, externem Personal wahrgenommen wird, daher abgeraten.

Über die Bedenken wegen der ärztlichen Schweigepflicht hinaus, ist die Beauftragung von Subunternehmen, die sich außerhalb des Europäischen Wirtschaftsraumes (EWR) befinden, wegen des eventuell niedrigeren Schutzniveaus nicht ideal. Um den Bedenken zu begegnen, sollte der Auftraggeber im Rahmen des Vertrags berücksichtigen, dass

- die Wartung mit Zugriff auf Patientendaten durch ein Unternehmen mit Sitz außerhalb des EWR nur erfolgen darf, wenn sie zwingend erforderlich bzw. alternativlos ist,

- die für den Schutz der in Frage stehenden Daten erforderlichen technischen und organisatorischen Maßnahmen getroffen sind und

- ein angemessenes Schutzniveau sichergestellt wird (beispielsweise durch den Abschluss eines EU-Standardvertrages).

Von einer Wartung medizinischer Geräte, bei welcher Patientendaten einem Auftragnehmer bzw. Subunternehmer, der nicht an die ärztliche Schweigepflicht gebunden ist, zur Kenntnis gelangen können, raten wir ab. Dies gilt umso mehr, wenn der Auftragnehmer seinen Sitz außerhalb des Europäischen Wirtschaftsraums hat.

2.3 Umfrage zum Datenschutz und zur Informationssicherheit in Krankenhäusern

Die moderne, rechnergestützte Gesundheitsversorgung in Brandenburg setzt auch die Erfüllung hoher Anforderungen an die Gewährleistung von Datenschutz und Informationssicherheit voraus. Eine im Berichtszeitraum bei den unserer Aufsicht unterliegenden Krankenhäusern durchgeführte Umfrage gibt nun Aufschluss darüber, in welchem Maße die datenschutzrechtlichen Regelungen der einschlägigen Gesetze (z. B. Brandenburgisches Krankenhausentwicklungsgesetz, Brandenburgisches Datenschutzgesetz) beachtet werden.

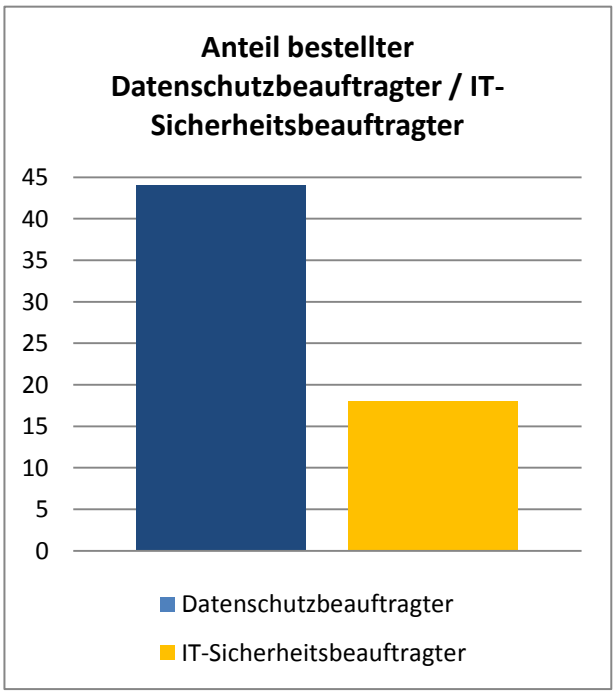
Im Juni 2015 starteten wir eine Umfrage zum Datenschutz und zur Informationssicherheit in Krankenhäusern. Dazu wurden alle 45 brandenburgischen Krankenhäuser angeschrieben, die sich nicht dem Datenschutzrecht einer Religionsgemeinschaft unterworfen haben (z. B. dem Datenschutzgesetz der Evangelischen Kirche in Deutschland) und deren Träger in Brandenburg registriert sind. Mit der Umfrage war der Wunsch nach einem allgemeinen und landesweiten Überblick zum Stand von Datenschutz und zur Informationssicherheit im Krankenhausbereich verbunden.

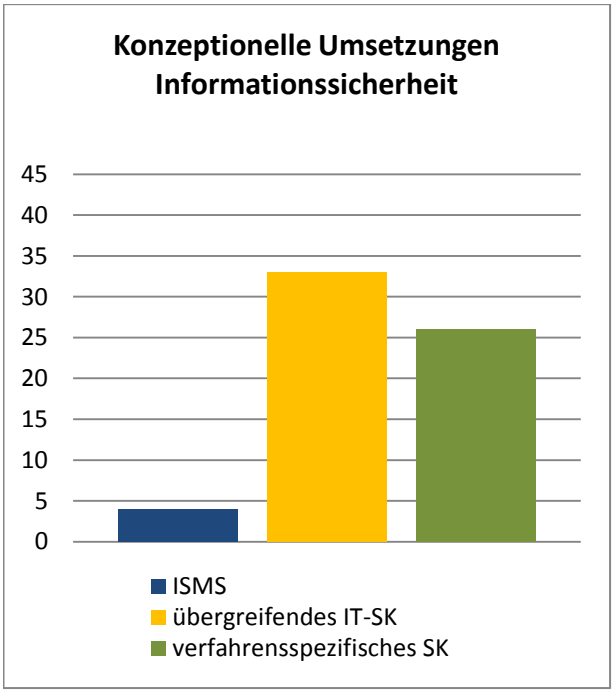
Der von uns entwickelte Fragebogen thematisierte in unterschiedlicher Detailtiefe datenschutzrechtliche und technisch-organisatorische Aspekte zu den verschiedensten Gebieten. Neben dem Schwerpunkt der technischen und organisatorischen Umsetzung von Informationssicherheit erbaten wir auch Angaben zu den genutzten informationstechnischen Systemen und Verfahren sowie zum Schutz von und zum Umgang mit Patientendaten. Im Folgenden fassen wir die wichtigsten Ergebnisse der Auswertung unserer Umfrage zusammen.

44 Krankenhäuser gaben an, dass sie einen Datenschutzbeauftragten bestellt haben, mehr als die Hälfte davon einen externen Beauftragten.

Hinsichtlich der Bestellung eines IT-Sicherheitsbeauftragten ergab die Umfrage, dass nur 40 % der Krankenhäuser diese Position, meist mit einem internen Beschäftigten, besetzt haben. Das Brandenburgische Datenschutzgesetz verlangt zwar nicht explizit diese Funktion, wir empfehlen aber dennoch, sie vorzusehen. Der IT-Sicherheitsbeauftragte sollte der zentrale Ansprechpartner für alle IT-Sicherheitsfragen sein. Er nimmt im Rahmen des Informationssicherheitsmanagements und im Auftrag der Unternehmensleitung eine koordinierende und steuernde Funktion ein. Dass mehr als die Hälfte der Krankenhäuser keinen IT-Sicherheitsbeauftragten bestellt haben, spiegelt sich auch in den Resultaten bei der Etablierung eines Informationssicherheitsmanagementsystems (ISMS) und der Erstellung von übergreifenden und verfahrensspezifischen Sicherheitskonzepten deutlich wider. Lediglich

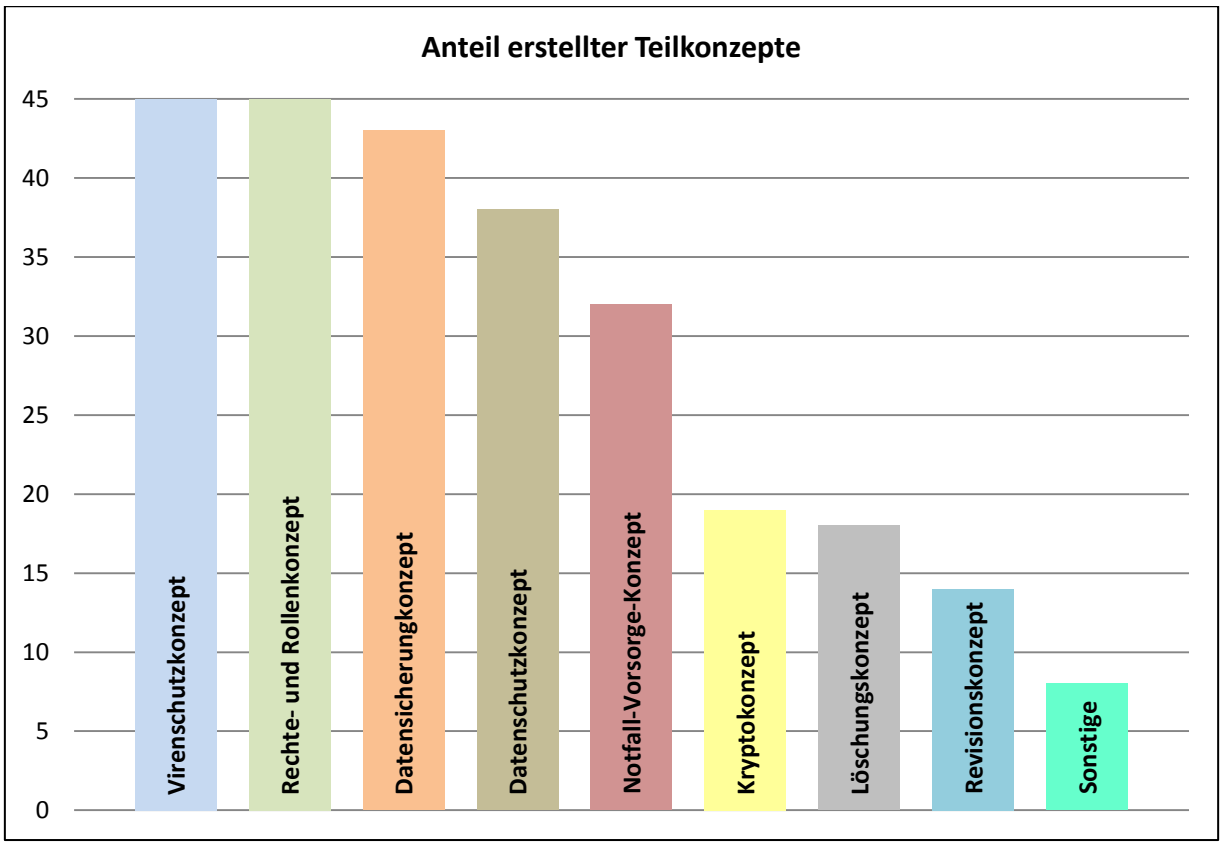
9 % der Krankenhäuser verfügen über ein ISMS, 73 % haben eine übergreifende IT-Sicherheitskonzeption erstellt und nur knapp über die Hälfte (58 %) können verfahrensspezifische Sicherheitskonzepte vorweisen, aus denen die technischen und organisatorischen Maßnahmen abgeleitet werden können, die eine Beherrschung der von Verfahren der IT-gestützten Patientenversorgung ausgehenden Risiken für die Rechte und Freiheiten der Betroffenen ermöglichen.[4]





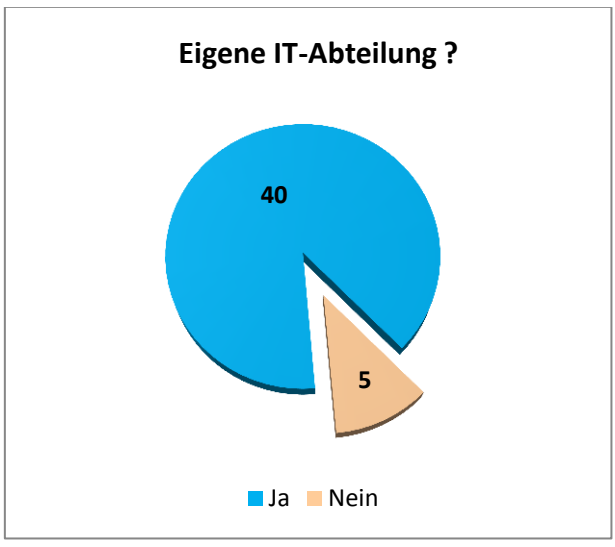
Der Anteil der Krankenhäuser, die angaben, Teilkonzepte zur Informationssicherheit entwickelt und umgesetzt zu haben, lag bei 100 % und gliedert sich wie folgt:

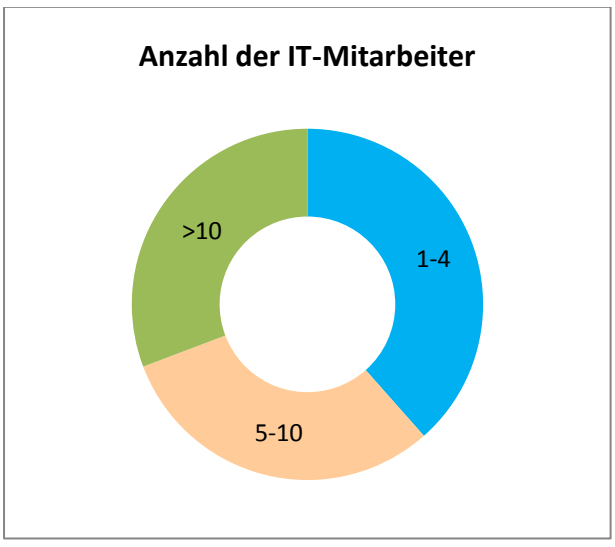
[4] In den Abbildungen wird jeweils die absolute Anzahl der Krankenhäuser pro Merkmal angezeigt.



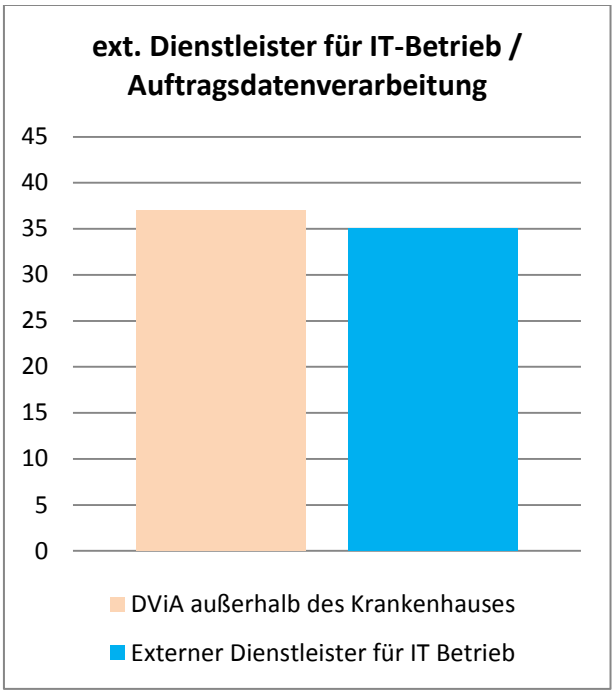
Offenbar messen alle bzw. fast alle Krankenhäuser dem Schutz vor Schadsoftware, der Vergabe von Berechtigungen im für die Aufgabenerfüllung erforderlichen Umfang sowie der Datensicherung eine wesentliche Bedeutung bei. Konzepte zum Einsatz kryptografischer Verfahren, zur Protokollierung und Löschung liegen dagegen nur in ca. 1/3 der Fälle vor.

Die IT-Administration sowie die Erstellung und Umsetzung der Konzeptionen wird meist von der eigenen IT-Abteilung wahrgenommen. Ihre personelle Ausstattung richtet sich in der Regel nach der Größe des Krankenhauses und der Komplexität und Anzahl der zu betreuenden Komponenten und Verfahren.

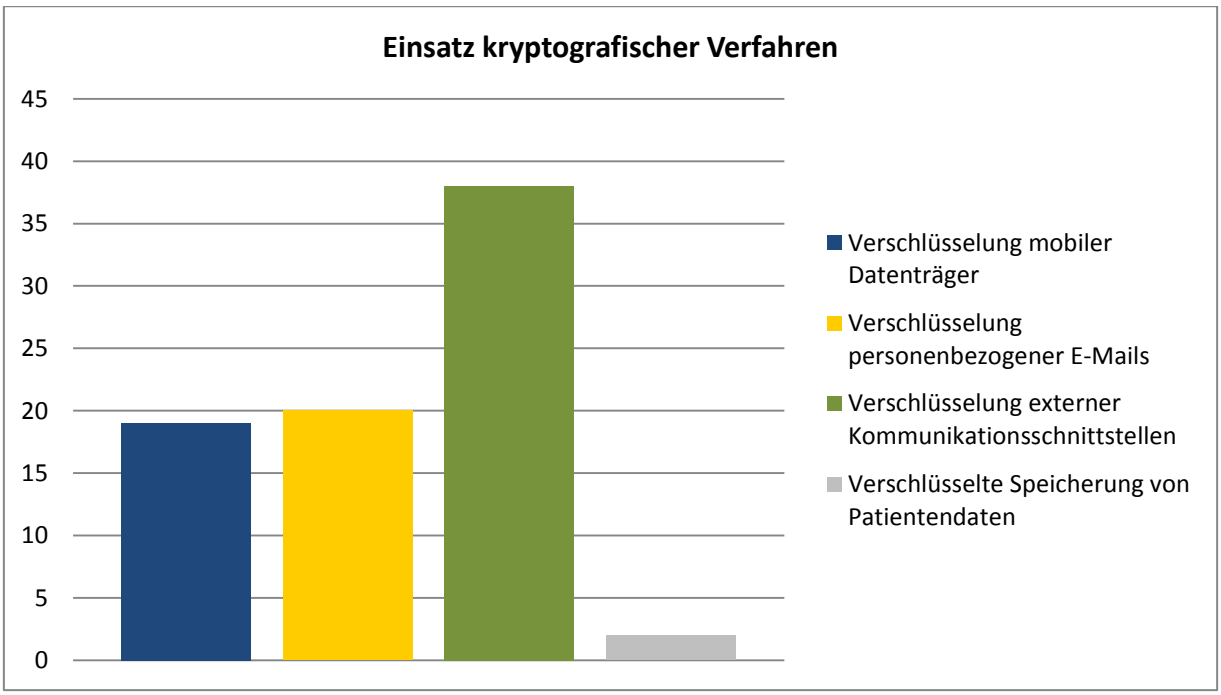




Für den Betrieb der IT-Infrastruktur werden von den meisten Befragten (35 Krankenhäuser) zusätzlich externe Dienstleister in Anspruch genommen. Eine Auftragsdatenverarbeitung personenbezogener Daten außerhalb des Krankenhauses gaben 37 Häuser an. Da das Krankenhausentwicklungsgesetz keine Regelungen zur Datenverarbeitung im Auftrag trifft, ist grundsätzlich § 11 Brandenburgisches Datenschutzgesetz (BbgDSG) anzuwenden. Werden Daten im Auftrag verarbeitet, die der ärztlichen Schweigepflicht (Patientendaten) unterliegen, sind die technischen und organisatorischen Maßnahmen zu treffen, die eine Wahrung des Geheimnisses auch gegenüber dem Auftragnehmer sicherstellen (§ 11 Abs. 2 Satz 3 BbgDSG).



Das wirksamste und oftmals einzige Mittel, um die Vertraulichkeit des Patientengeheimnisses zu wahren, liegt in der Verschlüsselung der Daten. Sie kann auch dazu eingesetzt werden, um organisatorische Rollentrennungen, die unbefugte Offenbarungen innerhalb des Krankenhauses unterbinden sollen, wirksam zu unterstützen. Die kryptografische Sicherung der Patientendaten sollte umfassend erfolgen. Dazu zählt u. a. neben der gesicherten Speicherung von Daten im Krankenhausinformationssystem, auch die Verschlüsselung der mobilen Datenträger und die kryptografische Sicherung aller externen Kommunikationsschnittstellen (inkl. E-Mail). Dass Patientendaten bei der Verarbeitung, insbesondere durch kryptografische Maßnahmen geschützt und nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können, scheint oftmals nicht ausreichend gewährleistet zu sein, insbesondere hinsichtlich der Speicherung von Patientendaten. Lediglich zwei Krankenhäuser gaben an, Patientendaten auch verschlüsselt zu speichern.



Mit der durchgeführten Umfrage konnten wir uns einen allgemeinen Überblick zur Umsetzung des Datenschutzes und der Informationssicherheit in den brandenburgischen Krankenhäusern verschaffen. Sie zeigt an mehreren Stellen Defizite auf, die einer datenschutzgerechten und sicheren Verarbeitung personenbezogener Gesundheitsdaten entgegenstehen.

Die Verarbeitung von Patientendaten in brandenburgischen Krankenhäusern erfolgt nicht immer unter vollständiger Beachtung der datenschutzrechtlichen Vorgaben. Insbesondere im technisch-organisatorischen Bereich zeigte unsere Umfrage Mängel, auf deren Beseitigung wir drängen werden.

3 Prüfungen des technischen und organisatorischen Datenschutzes in Landkreisen und kreisfreien Städten

Einer der Tätigkeitsschwerpunkte unserer Behörde im Jahr 2015 waren Prüfungen in den Verwaltungen von sieben Landkreisen und zwei kreisfreien Städten. Am Beispiel ausgewählter Sachgebiete und Verfahren, in denen personenbezogene Daten verarbeitet werden, wollten wir uns einen Überblick über den aktuellen Stand der Erfüllung technischer und organisatorischer Anforderungen des Datenschutzes und der Informationssicherheit in diesen Behörden verschaffen. Die Ergebnisse sind in der Regel nicht zufriedenstellend.

3.1 Prüfungen allgemeiner technischer und organisatorischer Aspekte

Das Brandenburgische Datenschutzgesetz (BbgDSG) enthält aus technischer und organisatorischer Sicht eine Reihe von Anforderungen, die öffentliche Stellen bei der Einführung und dem Betrieb von Verfahren zur automatisierten Verarbeitung personenbezogener Daten zu beachten haben. So muss die Daten verarbeitende Stelle für diese Verfahren (soweit sie nicht unter die Ausnahmen von § 8 Abs. 5 BbgDSG fallen) jeweils ein Verfahrensverzeichnis mit den Angaben aus § 8 Abs. 1 BbgDSG erstellen. Der erstmalige Einsatz oder wesentliche Änderungen eines Verfahrens erfordern gem. § 7 Abs. 3 BbgDSG die schriftliche Freigabe. Diese darf nach derselben Vorschrift nur erteilt werden, wenn in einem Sicherheitskonzept nachgewiesen wurde, dass die von dem Verfahren ausgehenden Risiken für die Rechte und Freiheiten Betroffener durch technische und organisatorische Sicherheitsmaßnahmen gem. § 10 BbgDSG beherrscht werden und für Verfahren, in denen besondere Risiken entstehen können, eine Vorabkontrolle durch den behördlichen Datenschutzbeauftragten gem. § 10 a BbgDSG erfolgt ist. Wird die Verarbeitung durch eine externe Stelle im Auftrag durchgeführt oder übernimmt eine solche Stelle die Wartung des Verfahrens, sind zusätzlich entsprechende Verträge schriftlich zu schließen (§§ 11 bzw. 11 a BbgDSG).

Wir haben uns von allen 9 für die Prüfung ausgewählten Verwaltungen im Vorfeld entsprechende Unterlagen zusenden lassen bzw. – wenn ihr Umfang zu groß war – die Einsichtnahme bei der späteren Vor-Ort-Kontrolle angekündigt. Dies betraf sowohl allgemeine verfahrensunabhängige Dokumente (wie z. B. Informationssicherheitsrichtlinien, allgemeine Dienstanweisungen und Dienstvereinbarungen mit Bezug zu Datenschutz und Informationssicherheit, allgemeine Sicherheitskonzepte) als auch verfahrensspezifische Unterlagen (wie z. B. Verfahrensverzeichnisse, verfahrensspezifische Sicherheits- und Berechtigungskonzepte, Vorgaben zur Protokollierung, Verträge zur Datenverarbeitung im Auftrag bzw. zur Wartung). Nach Auswertung der zugesandten Dokumente prüften wir jeweils vor Ort stichprobenartig die Umsetzung der allgemeinen und verfahrensspezifischen Festlegungen, wobei auch Einblick in die jeweiligen Verfahren genommen bzw. die genutzten IT-Infrastrukturkomponenten begutachtet wurden.

Grundsätzlich ist festzustellen, dass die organisatorischen Festlegungen für Datenschutz und Informationssicherheit in den geprüften Verwaltungen in der Regel eine gute Qualität hatten – wenn sie denn vorhanden und aktuell waren. Zum Teil lagen die Dokumente nur im Entwurf vor und mussten noch intern abgestimmt bzw. verabschiedet werden, zum Teil wurden sie seit vielen Jahren nicht mehr gepflegt und waren veraltet. So verwies beispielsweise die interne Dienstanweisung zum Datenschutz in einer Kreisverwaltung

auf rechtliche Regelungen, die bereits im Jahr 2007 aus dem Brandenburgischen Datenschutzgesetz gestrichen worden waren.

Interne organisatorische Regelungen zur Einbindung des behördlichen Datenschutzbeauftragten existierten oftmals lediglich auf dem Papier. Seine Beteiligung bei der Einführung oder Änderung von Verfahren zur Verarbeitung personenbezogener Daten erfolgte häufig zu spät oder gar nicht, seine Hinweise wurden von der Verwaltung nicht oder unzureichend beachtet, Zuarbeiten zu Angaben im Verfahrensverzeichnis durch die Fachbereiche nicht oder nicht rechtzeitig geleistet und die Ergebnisse von Vorabkontrollen zum Teil ignoriert.

Bezüglich der verfahrensunabhängigen Sicherheitsmaßnahmen und ihrer praktischen Umsetzung ergab sich das folgende Bild: Die meisten Verwaltungen realisierten zumindest teilweise und mit unterschiedlichen, selbst bestimmten Schwerpunkten sowie zeitlichen Abfolgen allgemeine technische Sicherheitsmaßnahmen und orientierten sich dabei z. B. an anerkannten Richtlinien, Empfehlungen oder sog. „Best Practices“ (wie IT-Grundschutz). Sie gingen aber in der Regel nicht strukturiert, systematisch und ganzheitlich vor. Dementsprechend konnte nur eine Behörde ein aktuelles, umfassendes IT-Sicherheitskonzept vorweisen. Dieses dokumentierte auch die bestehenden Mängel, enthielt allerdings keine Realisierungsplanung für noch nicht umgesetzte Maßnahmen. Eine andere Behörde hatte zwar im Rahmen eines Verwaltungsneubaus insbesondere infrastrukturelle Sicherheitsmaßnahmen berücksichtigt (z. B. für die Gebäude-, Raum- und Netzinfrastruktur), versäumte es jedoch, diesen Zustand und die Maßnahmen umfassend zu dokumentieren.

Bei einer weiteren Verwaltung zeigten sich im Rahmen der Kontrolle vor Ort erhebliche Defizite bei der Absicherung von Räumen der technischen Infrastruktur und der Umsetzung erforderlicher Sicherheitsmaßnahmen. Ein Serverraum war ohne Sichtschutzmaßnahmen und von außen leicht einsehbar. Aufgrund seiner Lage, der unter den Fenstern positionierten Müllcontainer und des fehlenden Einbruchsschutzes an den Fenstern war er darüber hinaus von außen leicht zugänglich. Die Verwaltung plante zwar eine Sanierung des Gebäudes, Empfehlungen des behördlichen Datenschutzbeauftragten und des IT-Sicherheitsbeauftragten zur technischen Absicherung der Räume für die technische Infrastruktur wurden dabei jedoch nicht berücksichtigt.

Weiterhin wurden hier – wie auch in anderen kontrollierten Behörden – konkrete Vorgaben aus den allgemeinen Dienstanweisungen zum Datenschutz und zur Informationssicherheit nur unzureichend umgesetzt. So war z. B. trotz Sicherheitsmaßnahmen zur Verhinderung der Nutzung von USB-Wechselmedien deren Verwendung während der Prüfung möglich. Somit kann weder zuverlässig kontrolliert werden, ob auf diesem Weg personenbe-

zogene Daten die Verwaltung verlassen, noch, ob Schadsoftware in das IT-System hineingelangt.

3.2 Prüfungen kommunaler Jobcenter

Im Berichtszeitraum haben wir damit begonnen, alle kommunalen Träger der Grundsicherung für Arbeitsuchende (Jobcenter) im Land Brandenburg hinsichtlich der Einhaltung der datenschutzrechtlichen Vorgaben zu prüfen. Gemäß § 78 a Zehntes Buch Sozialgesetzbuch (SGB X) haben Jobcenter als für die Datenverarbeitung verantwortliche Stellen die technischen und organisatorischen Maßnahmen einschließlich der Dienstanweisungen zu treffen, die erforderlich sind, um die Ausführungen der Vorschriften dieses Gesetzbuches, insbesondere die in der Anlage zu dieser Vorschrift genannten Anforderungen, zu gewährleisten.

Bezüglich der uns von den Jobcentern vorab übersandten Verfahrensverzeichnisse war festzustellen, dass diese nur in einem Fall vollständig und aktuell waren. Ein verfahrensspezifisches Sicherheitskonzept konnte nur eine Verwaltung vorlegen – allerdings befand sich dieses noch im Entwurfsstadium. Bei den anderen Behörden erfolgte der Verfahrensbetrieb ohne Sicherheitskonzept. Von besonderer Brisanz war ein Fall, in dem der behördliche Datenschutzbeauftragte im Rahmen seiner Vorabkontrolle der Verfahrenseinführung wegen des Fehlens der erforderlichen Sicherheitsdokumentation nicht zustimmen konnte und dies den Verantwortlichen auch schriftlich mitteilte. Eine Inbetriebnahme des Verfahrens erfolgte jedoch trotzdem.

Auffällig waren auch die im Verlauf der Prüfung festgestellten Mängel bei der Verwendung von Passwörtern im Fachverfahren. Ihre konfigurierte Mindestlänge variierte (je nach Behörde) zwischen fünf und acht Zeichen, die Gültigkeitsdauer zwischen sechs Wochen und einem Jahr. Darüber hinaus gehende Festlegungen, z. B. zur Komplexität von Passwörtern, wurden meist nicht getroffen. Da eine zuverlässige Authentifizierung der Nutzer die Basis vieler darauf aufbauender Sicherheitsmechanismen (z. B. der Zugriffskontrolle oder der Protokollierung) ist, forderten wir einheitlich für alle Jobcenter eine Verschärfung der programmseitig implementierten Passwortrichtlinie. Künftig ist vorzusehen, dass Passwörter mindestens acht Zeichen lang sind, mindestens zwei Sonderzeichen enthalten, nicht wiederverwendet werden können und mindestens alle 90 Tage gewechselt werden. Eine dreimalige Eingabe des falschen Passwortes muss zur Sperrung des Systemzugangs führen. Anforderungen zur Komplexität der Passwörter sind organisatorisch festzulegen, da eine Umsetzung im Fachverfahren zurzeit nicht möglich ist. Weil wir vereinzelt feststellten, dass Passwörter nicht geheim gehalten und schriftlich am Arbeitsplatz hinterlegt wurden, mahnten wir auch eine zusätzliche Sensibilisierung der Mitarbeiter an.

Durch den Einsatz von dem Stand der Technik entsprechenden Verschlüsselungsverfahren kann sichergestellt werden, dass Sozialdaten bei ihrer Verarbeitung und Nutzung, insbesondere bei der elektronischen Übertragung über Netze und nach der Speicherung auf Datenträgern, nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können. Der Gesetzgeber hat auf diese Maßnahme in der Anlage zu § 78 a SGB X besonders hingewiesen und ihre Umsetzung eingefordert. Dem steht unser Prüfergebnis gegenüber: Keine der kontrollierten Verwaltungen verfügte über eine kryptografisch gesicherte Datenbank, alle Sozialdaten des Fachverfahrens wurden im Klartext gespeichert. Auch eine Verschlüsselung der Datenübertragung wäre nach dem Schutzbedarf der Daten und dem Stand der Technik zwingend geboten gewesen, wurde jedoch nirgends eingesetzt. Wir haben die Jobcenter aufgefordert, als Teil des IT-Sicherheitskonzepts auch ein Kryptokonzept zu erarbeiten, aus dem die kryptografischen Sicherheitsmaßnahmen sowie die Umsetzungsplanung hervorgehen.

Weiter ergab unsere Prüfung vor Ort, dass grundsätzlich die Mitarbeiter eines Jobcenterstandorts lesenden und schreibenden Zugriff auf die Daten aller an diesem Standort verwalteten Leistungsempfänger hatten. Aus unserer Sicht wäre eine Einschränkung der möglichen Zugriffe datenschutzrechtlich geboten gewesen – sowohl bezüglich der innerbehördlichen Zuständigkeiten für Gruppen von Leistungsempfängern als auch bezüglich abgestufter Rechte zum Lesen, Schreiben, Ändern bzw. Löschen der Daten. Zugriffsmöglichkeiten sind auf das zur Aufgabenerfüllung notwendige Maß zu begrenzen. Ggf. muss dafür die programmtechnische Umsetzung vom Verfahrenshersteller eingefordert werden.

Zur Gewährleistung der Revisionsfähigkeit verfügt die in den Jobcentern genutzte Fachanwendung über verschiedene Varianten der Protokollierung (z. B. Fehlerprotokoll, Änderungsprotokoll, globales Änderungsprotokoll und Systemprotokoll). Um diese applikationsseitig vorgesehenen Möglichkeiten datenschutzkonform zu nutzen, ist entsprechend den Anforderungen und spezifischen Gegebenheiten im jeweiligen Jobcenter z. B. festzulegen, welche Ereignisse mit welchen Attributen wo protokolliert werden, wer Zugriff auf Protokolle hat, wie diese ausgewertet werden und wann ihre Löschung erfolgt. Keines der geprüften Jobcenter verfügte diesbezüglich jedoch über konzeptionelle Vorgaben. In der Regel wurden beispielsweise die monatlich automatisiert erstellten Fehlerprotokolle weder ausgewertet noch nach einem angemessenen Zeitraum gelöscht. Sie wurden ohne weitere Zugriffsbeschränkungen im Dateisystem vorgehalten. Wir haben die Verwaltungen zur Beseitigung dieser Mängel und Erstellung eines Revisionskonzepts aufgefordert.

Schließlich gab es auch in keinem der geprüften Jobcenter eine strukturierte und geregelte Verfahrensweise zur Löschung personenbezogener Sozialda-

ten. Insofern konnte auch keine Verwaltung sicherstellen, dass die Anforderungen von § 84 Abs. 2 SGB X umfassend umgesetzt werden. Danach sind Sozialdaten zu löschen, wenn ihre Kenntnis für die verantwortliche Stelle zur rechtmäßigen Erfüllung der in ihrer Zuständigkeit liegenden Aufgaben nicht mehr erforderlich ist und kein Grund zu der Annahme besteht, dass durch die Löschung schutzwürdige Interessen der Betroffenen beeinträchtigt werden.

3.3 Prüfungen der Personaldatenverarbeitung

Als weiteren Gegenstand unserer Kontrollen wählten wir Prozesse und Verfahren der Personaldatenverarbeitung, konkret die Arbeitszeiterfassung sowie die Gehalts- und Bezügezahlung. Auch hier baten wir die jeweiligen Verwaltungen im Vorfeld einer Vor-Ort-Prüfung um die Zusendung datenschutzrechtlich erforderlicher Unterlagen (z. B. Verfahrensverzeichnisse, Berechtigungskonzepte, Verträge mit externen Unternehmen zur Pflege des Verfahrens oder zur Datenverarbeitung im Auftrag) sowie verfahrensspezifischer und allgemeiner Dienstvereinbarungen oder Dienstanweisungen mit Bezug zu Datenschutz und Informationssicherheit. Bereits frühzeitig kündigten wir an, vor Ort jeweils auch in die verfahrensspezifischen sowie in allgemeine Sicherheitskonzepte Einblick zu nehmen und am Rechner exemplarisch die Umsetzung einiger Sicherheitsmaßnahmen zu überprüfen.

In einem Fall übersandte uns der verantwortliche Fachbereich einer Kreisverwaltung zwar ein Verfahrensverzeichnis für ein Verfahren zur Gehalts- und Bezügezahlung, allerdings war dieses Verfahren längst nicht mehr im Einsatz. Auch bei mehreren Kontakten zur Vorbereitung der Vor-Ort-Prüfung hielt es der Fachbereich nicht für nötig, uns über den Verfahrenswechsel zu unterrichten. Erst im direkten Gespräch mit den zuständigen Mitarbeitern wurde der Mangel deutlich und auf Entscheidungen des Fachbereichsleiters verwiesen, uns lediglich die veralteten Unterlagen ohne weitere Information zukommen zu lassen. Versäumt wurde trotz schriftlicher Aufforderung auch, uns den Wartungsvertrag zur Pflege der Software vorab zuzusenden. Wir haben unser Unverständnis über das Agieren des Fachbereichs deutlich gegenüber dem Landrat zum Ausdruck gebracht.

Für alle geprüften Verwaltungen war im Ergebnis der Auswertung der übersandten Unterlagen festzustellen, dass die Verfahrensverzeichnisse jeweils einer Überarbeitung bedurften. Zum Teil enthielten sie einige wesentliche Informationen gar nicht, zum Teil waren die hinterlegten Daten nicht konkret genug (z. B. bei den Rechtsgrundlagen der Datenverarbeitung) oder veraltet (z. B. bei den technischen oder organisatorischen Maßnahmen). Größere Unsicherheiten, die sich auch im persönlichen Gespräch mit den zuständigen Mitarbeitern der Personalabteilungen manifestierten, gab es in Bezug auf die Aufbewahrungsfristen und Löschpflichten für Personalaktendaten.

Besonders kritisch zu vermerken ist, dass in keinem der geprüften Fälle eine Vorabkontrolle des Verfahrens zur Gehalts- und Bezügezahlung durch den behördlichen Datenschutzbeauftragten stattfand, obwohl ihre Durchführung durch diesen in der Regel angemahnt wurde. Die Vorabkontrolle wäre erforderlich gewesen, da in dem Verfahren besonders sensitive personenbezogene Daten verarbeitet werden, wie z. B. Daten über krankheitsbedingte Abwesenheiten, Schwerbehinderungen und die Religionszugehörigkeit sowie Steuer- und Kontodaten. Darüber hinaus unterliegen die verarbeiteten Personalaktendaten einem besonderen Dienst- und Amtsgeheimnis.

In Bezug auf die verfahrensspezifischen Sicherheitskonzepte mussten wir feststellen, dass es ein solches nur in einer einzigen Verwaltung gab. Es war allerdings veraltet und hätte auch nach den dortigen verwaltungsinternen Vorgaben bereits aktualisiert werden müssen. Berechtigungskonzepte, die Grundlage für die Erteilung von Rechten zum Zugriff auf Funktionen bzw. auf Daten im Verfahren sind, lagen nur in Ansätzen vor. In der Regel hatten die Verwaltungen Rollen und Zugriffsrechte auf Programmbereiche lediglich mit Blick auf das bereits laufende Softwaresystem dokumentiert. Versäumt wurde jedoch, die jeweils erforderlichen, minimalen Rechte ausgehend von den den Mitarbeitern zugewiesenen Arbeitsaufgaben und vor der Konfiguration der Software zu bestimmen. In einem Fall mussten wir bei der anschließenden Prüfung am PC auch feststellen, dass der betreffende Mitarbeiter weitergehende Rechte im Verfahren hatte als erforderlich – er konnte Personalaktendaten ändern, obwohl für seine Aufgaben Leserechte ausgereicht hätten und dies auch im Berechtigungskonzept so vorgesehen war.

Nachbesserungsbedarf wurde auch bezüglich der vorgelegten Wartungsverträge ersichtlich. Diese sind datenschutzrechtlich dann erforderlich, wenn bei der Wartung nicht ausgeschlossen werden kann, dass auf personenbezogene Daten zugegriffen wird. In den geprüften Fällen unterzeichneten die Verwaltungen häufig lediglich einen Standardpflegevertrag, der ihnen vom Softwarehersteller vorgelegt wurde. Dieser erfüllte jedoch die datenschutzrechtlichen Anforderungen nicht in vollem Umfang. Insbesondere wurden die Mindestvertragsinhalte für Wartungsverträge, die in den Anlagen 3 und 4 der Verwaltungsvorschriften zum Brandenburgischen Datenschutzgesetz enthalten sind, nicht hinreichend beachtet.

Letztlich nutzten wir vor Ort jeweils auch einen typischen Arbeitsplatz-PC, prüften dort die Umsetzung von Sicherheitsmaßnahmen und verwendeten den Zugang eines Mitarbeiters, um exemplarisch einige Funktionen des jeweiligen Verfahrens zur Personaldatenverarbeitung einzusehen. Dabei fiel auf, dass in keiner der geprüften Verwaltungen die eigenen, internen Passwortregelungen in Bezug auf das Fachverfahren eingehalten wurden. Die entsprechenden Passwörter waren zu kurz, die Applikationssoftware erzwang auch keine längeren. Weiterhin wurde deutlich, dass in keiner der Verwaltun-

gen die sensitiven Personalaktendaten bei der Übertragung über das Netz oder bei der Speicherung verschlüsselt wurden. In einem Fall wurde z. B. ein Webportal angeboten, damit die Beschäftigten ihre eigenen Daten im Intranet einsehen und pflegen können. Die Mitarbeiterdaten selbst wurden genauso wie die Zugangsdaten zum Portal mittels unverschlüsselter http-Verbindung übertragen, wodurch die Vertraulichkeit der Datenverarbeitung gefährdet war.

In allen geprüften Verwaltungen haben wir eine Erstellung bzw. Überarbeitung der gesetzlich vorgesehenen Unterlagen (Verfahrensverzeichnis, Sicherheitskonzepte, Wartungsverträge) gefordert. Auch die Durchführung der Vorabkontrolle durch den behördlichen Datenschutzbeauftragten spätestens bei der nächsten wesentlichen Änderung des Verfahrens zur Gehalts- und Bezügezahlung mahnten wir an. Darüber hinaus verlangten wir, dem Schutzbedarf der Personaldaten angemessene und dem Stand der Technik entsprechende Sicherheitsmaßnahmen umzusetzen, insbesondere in den Bereichen Verschlüsselung, Zugriffsrechte und Verwendung von Passwörtern.

3.4 Prüfungen von Ratsinformationssystemen und Katasterverfahren

Aufgrund einer vermehrten Zahl von Beschwerden über unzulässige Veröffentlichungen personenbezogener Daten in Ratsinformationssystemen wurden auch diese Verfahren während der durchgeführten Kontrollen genauer geprüft. Ratsinformationssysteme, wie sie heute häufig von Kommunen betrieben werden, unterstützen nicht nur die Vorbereitung und Durchführung von Sitzungen der jeweiligen Parlamente (Kreistage, Stadtverordnetenversammlungen, Gemeindevertretungen). Sie können auch Transparenz in der politischen Arbeit schaffen sowie die Beteiligung bzw. die Information der Bürger gewährleisten.

Da in Ratsinformationssystemen in der Regel auch personenbezogene Daten verarbeitet werden, bedürfen sie einer datenschutzrechtlichen Prüfung. Dies bezieht sich zum einen auf die Bereitstellung von für die Öffentlichkeit zugänglichen Informationen. Zum anderen sind von der jeweiligen Verwaltung als Daten verarbeitender Stelle Maßnahmen umzusetzen, die sicherstellen, dass nur Berechtigte Zugriff auf nicht öffentliche Unterlagen mit ggf. sensitiven personenbezogenen Daten erhalten. In dieser Hinsicht stellten wir bei unseren Kontrollen keine Mängel fest. Die praktische Umsetzung und der Betrieb der Verfahren erfüllten in der Regel die datenschutzrechtlichen Anforderungen. Auch Regelungen für Zugriffsberechtigungen auf Sitzungsunterlagen sowie für eine zeitgerechte Löschung von Dokumenten wurden durch die Verwaltungen sachgerecht getroffen und implementiert. Geringen Nachbesserungsbedarf sahen wir vereinzelt bei den vorgelegten Verfahrensverzeichnissen.

Ein weiterer Schwerpunkt unserer Kontrollen in den Landkreisen und kreisfreien Städten bezog sich auf die Erteilung von Auskünften aus dem Liegenschaftskataster. Anlass waren auch hier Beschwerden von Bürgern über vermeintlich unberechtigte Auskünfte. Nach dem Gesetz über das amtliche Vermessungswesen im Land Brandenburg ist bei der Bereitstellung personenbezogener Geobasisinformationen aus dem Liegenschaftskataster das Vorliegen eines berechtigten Interesses, das gegenüber der Verwaltung darzulegen ist, oder die Zustimmung des Betroffenen erforderlich.

Im Rahmen unserer Prüfungen vor Ort wurde deutlich, dass sich die Verantwortlichen mit den rechtlichen Voraussetzungen zur Bereitstellung der personenbezogenen Geodaten auseinandergesetzt und entsprechende organisatorische Regelungen zum Nachweis und zur Prüfung des berechtigten Interesses der Auskunft Begehrenden getroffen hatten. Auch eine Dokumentation über erteilte Auskünfte wurde vorgenommen. Die Vorgehensweisen waren datenschutzrechtlich nicht zu beanstanden.

Unsere Kontrollen zur Einhaltung technischer und organisatorischer Anforderungen des Datenschutzes und der Informationssicherheit in den Verwaltungen ausgewählter Landkreise und kreisfreier Städte offenbarten zum Teil gravierende Mängel. Keine Verwaltung erfüllte alle Anforderungen, in manchen wurde erheblicher Nachholbedarf deutlich. Auffallend ist die Tatsache, dass häufig die umfangreichen Erfahrungen der jeweiligen behördlichen Datenschutzbeauftragten vor Ort nicht genutzt und ihre Empfehlungen oder Forderungen durch die Verwaltungsleitungen ignoriert wurden.

Teil B

Datenschutz

1 Europa und Internationales: Entwicklung des Datenschutzes

1.1 Neue EU-Datenschutz-Richtlinie im Bereich von Justiz und Inneres

Im Zuge der Neuordnung und Harmonisierung des europäischen Datenschutzrechts hat die Europäische Kommission nicht nur eine Datenschutz-Grundverordnung vorgeschlagen, sondern auch eine Überarbeitung spezifischer Datenschutzbestimmungen – wie des Rahmenbeschlusses 2008/977/JI – im Bereich der polizeilichen und justiziellen Zusammenarbeit angeregt. Zweck des bereits 2012 vorgelegten Entwurfs der Kommission für die sog. JI-Richtlinie[5] ist es, ein einheitliches Datenschutzniveau zu garantieren und den freien Datenverkehr und die Zusammenarbeit zwischen europäischen Polizei- und Justizbehörden zu erleichtern. Zum Ende des Berichtszeitraums wurde der Entwurf in den Trilogverhandlungen zwischen Europäischem Parlament, Rat der Europäischen Union und Europäischer Kommission abschließend beraten.

Im Gegensatz zur EU-Datenschutz-Grundverordnung bezweckt die Richtlinie für die Mitgliedstaaten nur eine Rechtsangleichung. Die dort festgelegten Regelungen sind hinsichtlich des zu erreichenden Ziels verbindlich, überlassen den Staaten im Rahmen ihrer innerstaatlichen Rechtsordnungen jedoch die Wahl der Form und der Mittel, um die Vorgaben im nationalen Recht umzusetzen. Gerade deshalb setzt sich die Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder dafür ein, ein möglichst hohes Datenschutzniveau in der Richtlinie festzuschreiben und wendet sich gegen zu allgemeine Formulierungen – wie sie häufig in der vom Rat vorgelegten Fassung für die JI-Richtlinie enthalten sind.

Da die spezielleren Vorschriften der JI-Richtlinie die Anwendung der Datenschutz-Grundverordnung in diesem Bereich verdrängen, kommt der Abgrenzung der Anwendungsbereiche eine wesentliche Bedeutung zu. Ablehnend

5 Vorschlag für eine Richtlinie des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Aufdeckung, Untersuchung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr vom 25. Januar 2012 (2012/0010 COD)

betrachtet die Konferenz Bestrebungen des Rates, den Anwendungsbereich der Richtlinie neben der Verhütung und Verfolgung von Straftaten und der Strafvollstreckung auch auf die allgemeine präventive Gefahrenabwehr – eine weitere klassische Aufgabe von Polizei- und anderen Behörden – und sogar auf die Ordnungsverwaltung (bei Bußgeldverfahren) auszudehnen. Dies würde bedeuten, dass im Gegensatz zum bisherigen Rechtsrahmen auch Behörden, die keine polizeilichen Aufgaben wahrnehmen, bei der Datenverarbeitung zu diesen Zwecken die JI-Richtlinie anwenden müssten und nicht die konkretere, unmittelbar geltende Datenschutz-Grundverordnung.

Die Datenschutzbehörden des Bundes und der Länder setzten sich dafür ein, dass präzisere Vorgaben für die Weiterverarbeitung von polizeilich erhobenen Daten festgelegt werden. Kerngedanke muss der Grundsatz der Zweckbindung sein, der als tragendes Prinzip des Datenschutzes in der europäischen Grundrechtecharta und im nationalen Recht verankert ist. Er besagt, dass der rechtmäßige Zweck einer Datenverarbeitung explizit definiert und erkennbar festgelegt werden muss, bevor diese geschieht. Eine Weiterverwendung erhobener Daten zu einem anderen Zweck ist nur in engen Grenzen möglich und bedarf einer eigenen Rechtsgrundlage. Dies dient dem Schutz der Betroffenen vor unbegrenzter Nutzung einmal vorhandener Daten.

Die Datenschutzkonferenz mahnte in ihrer Stellungnahme unter anderem an:

- Während die Kommission erstmals vorschlug, hinsichtlich der Datenverarbeitung von verschiedenen Personengruppen (z. B. Verdächtigen, Straftätern, Kontaktpersonen, Opfern und möglichen Zeugen) zu unterscheiden, wurde diese Regelung im Änderungsvorschlag des Rates wieder gestrichen. Aus datenschutzrechtlicher Sicht sind strengere Speichervoraussetzungen oder kürzere Speicherfristen für Personen, die keiner Straftat verdächtig sind, jedoch sinnvoll, weshalb die Konferenz diese Regelung im Richtlinienentwurf des Europäischen Parlaments unterstützte.

- Ebenso sprach sich die Konferenz für umfangreiche Informationspflichten gegenüber den von heimlichen Datenerhebungen betroffenen Personen aus, um diesen einen effektiven Rechtsschutz zu ermöglichen.

- Die festgelegten Betroffenenrechte auf Information, Auskunft, Berichtigung, Löschung und Einschränkung der Verarbeitung sollten zudem nicht durch nationalstaatliches Strafprozessrecht unterlaufen werden können, wenn es um Daten in Gerichtsbeschlüssen oder staatsanwaltliche Ermittlungsakten geht.

Schließlich stellte die Konferenz klar, dass nicht nur bei der Datenschutz-Grundverordnung sondern auch im Bereich der JI-Richtlinie eine Daten-

schutz-Folgeabschätzung äußerst wichtig ist. Gerade vor neuen Verarbeitungsvorgängen der Strafverfolgungsbehörden in großen Datenbanken, beim Einsatz von Vorhersagesoftware oder der Nutzung von Daten, die aufgrund ihrer Natur oder ihrer Zweckbestimmung erhöhte Risiken bergen, ist die Abwägung zwischen der Erforderlichkeit und Verhältnismäßigkeit der Speicherung einerseits und den erhöhten Risiken für das Persönlichkeitsrecht eines Betroffenen andererseits geboten.

Die Datenschutz-Richtlinie im Bereich von Justiz und Inneres wird den maßgeblichen Rahmen für die Datenverarbeitung der nationalen Ermittlungsbehörden und die länderübergreifende polizeiliche und justizielle Zusammenarbeit setzen. Die Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder hat sich dafür eingesetzt, dass die Richtlinie konkrete Grenzen für die Erfassung und Speicherung im Bereich der polizeilichen Datenverarbeitung setzt und den Mitgliedstaaten keinen zu weiten Gestaltungsspielraum für die nationale Umsetzung gibt.

1.2 Europäische Richtlinie zur Vorratsdatenspeicherung

Der Gerichtshof der Europäischen Union (EuGH) erklärte am 8. April 2014 die Richtlinie 2006/24/EG der Europäischen Union über die Vorratsdatenspeicherung von Telekommunikations-Verkehrsdaten aus dem Jahr 2006 rückwirkend für ungültig.[6]

Die Richtlinie hatte die Mitgliedstaaten verpflichtet, zu gewährleisten, dass Telekommunikationsdienstebetreiber bestimmte Datenkategorien bei Telefongesprächen und E-Mails wie Zeitpunkt, Dauer, Gesprächsteilnehmer, Sender/Empfänger – nicht aber Inhalte von Gesprächen – für Zwecke der Ermittlung und Verfolgung schwerer Straftaten speichern. Der Deutsche Bundestag hatte zur Umsetzung der Richtlinie das Gesetz zur Neuregelung der Telekommunikationsüberwachung und anderer verdeckter Ermittlungsmaßnahmen verabschiedet, das am 1. Januar 2008 in Kraft trat. Diese deutschen Regelungen zur Vorratsdatenspeicherung wurden allerdings durch das Bundesverfassungsgericht bereits im Jahr 2010 für überwiegend nichtig befunden.[7] Vier Jahre später kippte der Europäische Gerichtshof auch die europäische Rechtsgrundlage für die Vorratsdatenspeicherung.

Die Verpflichtung zur anlass- und verdachtslosen Speicherung der Telekommunikationsverkehrsdaten und die Zugriffsmöglichkeit der zuständigen nationalen Behörden auf diese stellt nach Auffassung des Europäischen Gerichtshofs einen besonders schwerwiegenden Eingriff in die durch die europäische

6 Urteil des Europäischen Gerichtshofs vom 8. April 2014, Rechtssachen C-293/12, C-594/12

7 Urteil des Bundesverfassungsgerichts vom 2. März 2010, 1 BvR 256/08, 1 BvR 263/08, 1 BvR 586/08

Grundrechtecharta gewährleisteten Rechte auf Achtung des Privatlebens und Schutz der personenbezogenen Daten dar. Die Zielsetzung der Richtlinie – die Bekämpfung schwerer Kriminalität – diene zwar dem Gemeinwohl und somit der öffentlichen Sicherheit. Der Unionsgesetzgeber habe bei der Richtlinie jedoch die Grenzen überschritten, die er zur Wahrung des Grundsatzes der Verhältnismäßigkeit hätte einhalten müssen.

Im Einzelnen begründete das Gericht seine Entscheidung damit, dass die Richtlinie eine Speicherpflicht für alle Verkehrsdaten sämtlicher Personen enthalte, die elektronische Kommunikationsmittel nutzen – ohne hinreichende Differenzierung des betroffenen Personenkreises, der geografischen oder zeitlichen Ausdehnung oder Ausnahmen z. B. für Personen, deren Kommunikation dem Berufsgeheimnis unterliegt. Auch die allgemein vorgeschriebene Dauer der Vorratsdatenspeicherung für einen Zeitraum von sechs Monaten lasse keine Unterscheidung von Datenkategorien nach ihrem Nutzen für das verfolgte Ziel zu. Hinsichtlich der Frage der Datensicherheit befand das Gericht, dass die Richtlinie keine ausreichende Gewähr dafür bietet, dass die Daten gegen Missbrauch geschützt sind. Weder sei ein spezieller Schutz aus technisch-organisatorischer Sicht vorgesehen, noch sei festgelegt, dass die Daten innerhalb des Unionsgebiets gespeichert werden müssten, um eine unabhängige Kontrolle auf Grundlage des Unionsrechts zu gewährleisten. Es fehle auch an einer Verpflichtung der Mitgliedstaaten, den Zugang der Behörden zu den Daten durch eine vorherige gerichtliche oder anderweitige Kontrollstelle zu prüfen und zu beschränken.

Die Entscheidung des Europäischen Gerichtshofs, die europäische Richtlinie zur Vorratsdatenspeicherung für ungültig zu erklären, ist aus datenschutzrechtlicher Sicht zu begrüßen, auch wenn das Gericht die Vorratsdatenspeicherung als solche nicht für unzulässig erklärte. Die Richtlinie enthielt jedoch keine klaren und präzisen Vorgaben für die Anwendung der Maßnahme und keine Mindestanforderungen, um eine Beschränkung des Rechts auf Achtung des Privatlebens auf das absolut Notwendige zu gewährleisten. Ob es einen neuen Anlauf zur Regulierung der Vorratsdatenspeicherung auf europäischer Ebene geben wird, ist derzeit nicht ersichtlich.

1.3 Die Entscheidung des Europäischen Gerichtshofs zum Recht auf Vergessenwerden

Mit der Entscheidung[8] in dem Verfahren Google gegen die spanische Datenschutzbehörde hat der Europäische Gerichtshof die Gelegenheit genutzt, gleich mehrere Grundsatzfragen des europäischen Datenschutzrechts zugunsten des Persönlichkeitsrechts der Betroffenen zu beantworten.

Der Betroffene war im Jahr 1998 mit der Entrichtung von Sozialversicherungsbeiträgen in Rückstand geraten, woraufhin eine Lokalzeitung, spanischem Recht folgend, eine Anzeige schaltete, durch die potenzielle Bieter für eine Zwangsversteigerung einer Immobilie des Betroffenen zur Meldung aufgerufen wurden. Die Lokalzeitung überführte die Anzeigen in ihr Onlinearchiv. Im Jahr 2010 wandte sich der Betroffene sowohl gegen die Internetveröffentlichung durch die Zeitung als auch gegen die Indexierung und Verbreitung durch die Suchmaschine Google. Die Beschwerde gegen die Zeitungsnotiz wurde von der Datenschutzaufsicht mit Hinweis auf die Rechtslage zum Zeitpunkt der Veröffentlichung zurückgewiesen, Google wurde dagegen zur Streichung der Seite aus dem Index verpflichtet. Die Audiencia Nacional, die über das von Google eingelegte Rechtsmittel zu entscheiden hatte, legte dem Europäischen Gerichtshof daraufhin bisher uneinheitlich beantwortete Fragen

- zur Verantwortlichkeit von Suchmaschinenbetreibern für die vorgehaltenen Inhalte,

- zum anwendbaren Recht für (teilweise) außerhalb der EU ansässige Unternehmen sowie

- zum Anspruch Betroffener gegenüber Suchmaschinenbetreibern auf Löschung ihrer personenbezogenen Daten aus persönlichkeitsrechtlichen Gründen auf Grundlage der EU-Datenschutzrichtlinie (Richtlinie 95/46/EG) – sog. Recht auf Vergessenwerden

zur Vorabentscheidung vor.

Der Gerichtshof stellte klar, dass Suchmaschinenbetreiber personenbezogene Daten im Sinne von Art. 2 b der Datenschutzrichtlinie verarbeiten und hierfür auch verantwortlich sind.

Er sah es als Anknüpfungspunkt für die Anwendbarkeit nationalen Datenschutzrechts als ausreichend an, dass die verantwortliche Stelle in dem betreffenden Mitgliedsstaat ein Büro für Anzeigenakquise unterhält, wie dies

8 Urteil des Europäischen Gerichtshofs vom 13. Mai 2014, Rechtssache C-131/12

bei Google Spain der Fall war. Hierbei handelt es sich bereits um eine Niederlassung im Sinne von Art. 4 Abs. 1 a der Richtlinie. Nur ein solches Begriffsverständnis erfülle den Zweck der Richtlinie, das Recht des einzelnen Unionsbürgers umfassend zu sichern. Mit dieser Weichenstellung machte der Gerichtshof auch den Weg frei zu einer weiterreichenden Anwendbarkeit deutschen Rechts auf Unternehmen außerhalb des Europäischen Wirtschaftsraums mit Niederlassungen in Deutschland.

Der Gerichtshof gelangte zur Feststellung einer von den Webseitenanbietern unabhängigen Pflicht des Suchmaschinenbetreibers, dafür zu sorgen, dass die eigenen Datenverarbeitungsmaßnahmen rechtmäßig erfolgen, woraus auch eine eigene Löschpflicht für rechtswidrig gespeicherte Daten folgen kann.

Schließlich hatte der Gerichtshof noch über die Voraussetzungen des Löschanspruchs in materieller Hinsicht zu entscheiden. Konkret ging es um die Frage, ob Suchmaschinenergebnisse zu erledigten Sachverhalten, die geeignet sind, dem Betroffenen Nachteile zu bereiten, gelöscht werden müssen, wenn sie etwa wegen Zeitablaufs nicht mehr aktuell sind. Dies ist ein Teilaspekt der datenschutzrechtlichen und gesellschaftlichen Diskussion, die in den letzten Jahren zum Schlagwort „Recht auf Vergessenwerden“ stattgefunden hat. Dabei geht es um die Abwägung zwischen der Informationsfreiheit von Internetnutzern und den wirtschaftlichen Interessen der verarbeitenden Stelle sowie dem Persönlichkeitsrecht der Betroffenen.

Der Gerichtshof bejahte die Möglichkeit eines Löschanspruchs nicht nur, sondern stellte die rechtliche Vermutung auf, dass sich im Normalfall die Persönlichkeitsrechte des Betroffenen sowohl gegen die wirtschaftlichen Interessen der Daten verarbeitenden Stelle als auch den Informationsanspruch der Öffentlichkeit durchsetzen sollten. Die Pflicht zur Löschung verortete er einfachrechtlich in Art. 6 Abs. 1 c bis e der Richtlinie, wonach vorgehaltene Daten nur in solchem Umfang und über einen solchen Zeitraum verarbeitet werden dürfen, wie es zur Erreichung des ursprünglichen Zwecks erforderlich ist, und die Daten sachlich richtig und aktuell sein müssen.

Die Landesbeauftragte hat Beschwerden über unzureichend berücksichtigte Löschanfragen bei Google an den für die Datenschutzaufsicht über dieses Unternehmen zuständigen Hamburgischen Beauftragten für Datenschutz und Informationsfreiheit weitergeleitet.

Die Landesbeauftragte begrüßt die Entscheidung des Europäischen Gerichtshofs ausdrücklich. Im Ergebnis des Urteils existiert damit in der Europäischen Union ein auf die Abwägung im Einzelfall gestütztes Recht auf Vergessenwerden.

1.4 Das EuGH-Urteil zu Safe Harbor schlägt hohe Wellen

Der Europäische Gerichtshof hat die Safe-Harbor-Entscheidung der Europäischen Kommission (2000/520/EG) für ungültig erklärt.[9] Auf Grundlage dieser Entscheidung konnten Unternehmen seit dem Jahr 2000 personenbezogene Daten in die USA übermitteln, wenn sich der Datenempfänger durch einfache Erklärung den Safe-Harbor-Regelungen unterwarf. Nach Ansicht der Kommission war allein durch die Erklärung das laut Datenschutzrichtlinie notwendige, angemessene Datenschutzniveau gewährleistet.

Spätestens nach Bekanntwerden der massenhaften Zugriffe durch US-Sicherheitsbehörden auf die in den Vereinigten Staaten von Amerika gespeicherten Daten gab es erhebliche datenschutzrechtliche Bedenken an diesem Vorgehen. Die Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder brachte schon frühzeitig ihre Besorgnis darüber zum Ausdruck, dass die NSA (National Security Agency) und andere ausländische Geheimdienste umfassend und anlasslos ohne Einhaltung der Grundsätze der Erforderlichkeit, Verhältnismäßigkeit und Zweckbindung auf personenbezogene Daten zugreifen, die von Unternehmen in Deutschland an Stellen in den USA übermittelt werden. Im März 2015 wies die Konferenz nochmals darauf hin, dass die Safe-Harbor-Entscheidung keinen ausreichenden Schutz für das Grundrecht auf Datenschutz bei der Übermittlung personenbezogener Daten in die USA entfaltet.[10]

Unmittelbar nach dem Urteil des Europäischen Gerichtshofs nahmen die Datenschutzbehörden des Bundes und der Länder sowie der Mitgliedstaaten der Europäischen Union intensive Abstimmungsgespräche auf. Schnell wurde klar, dass durch das Urteil zahlreiche Datentransfers in die USA einer neuen Rechtsgrundlage bedürfen. Nicht nur Datenübermittlungen, die bislang auf die Safe-Harbor-Entscheidung gestützt wurden, sind unzulässig. Auch andere Instrumente für Datenübermittlungen in Drittstaaten, wie Standardvertragsklauseln oder verbindliche Unternehmensregelungen (BCR), stehen aus Sicht der Datenschutzbehörden infrage. Selbst Einwilligungen kommen nur in Ausnahmefällen in Betracht.

Das Urteil machte zudem deutlich, dass in Drittstaaten nicht nur das betreffende Unternehmen selbst, sondern auch der Staat das für Datentransfers notwendige angemessene Datenschutzniveau zu gewährleisten habe, insbesondere gerichtlichen Rechtsschutz für Betroffene. Dies anhand der vom

---

9 Urteil des Europäischen Gerichtshofs vom 6. Oktober 2015, Rechtssache C-362/14

10 Entschließung „Safe Harbor bietet keinen ausreichenden Schutz für den Datentransfer in die USA“ vom 18./19. März 2015 (Anlage 1.3.8)

Gerichtshof vorgegebenen, strengen Kriterien zu prüfen, obliege der Kommission und den Datenschutzbehörden.

Zu den Konsequenzen des Urteils hat die Konferenz noch im Oktober 2015 ein Positionspapier mit ersten Schlussfolgerungen veröffentlicht.[11] Darin wurde u. a. angekündigt, ausschließlich auf Safe Harbor gestützte Datenübermittlungen in die USA zu untersagen, soweit Aufsichtsbehörden Kenntnis von diesen erlangen, und vorerst keine neuen Genehmigungen für entsprechende Datenübermittlungen auf Grundlage von BCR oder Datenexportverträgen zu erteilen. Die Europäische Kommission und die Bundesregierung wurden aufgefordert, in Verhandlungen mit den Vereinigten Staaten auf die Schaffung ausreichend weitreichender Garantien zum Schutz der Privatsphäre zu drängen, insbesondere durch gerichtlichen Rechtsschutz und Beschränkungen der Zugriffsmöglichkeiten amerikanischer Behörden. Unternehmen waren aufgerufen, umgehend ihre Verfahren zum Datentransfer datenschutzgerecht zu gestalten – obwohl auf viele Fragen in diesem Zusammenhang nicht alsbald zufriedenstellende Antworten zu erwarten waren.

Auch die Artikel-29-Gruppe, in der sich die Datenschutzaufsichtsbehörden aller Mitgliedstaaten der Europäischen Union abstimmen, hat ein entsprechendes Statement abgegeben.[12] Sie machte deutlich, dass die Datenschutzaufsichtsbehörden verpflichtet sind, alle notwendigen und angemessenen Maßnahmen zu ergreifen, wenn bis Ende Januar 2016 keine tragfähige Lösung gefunden wird bzw. diese nicht die vom Gericht gestellten Anforderungen erfüllt. In der Zwischenzeit würde sowohl entsprechenden Beschwerden nachgegangen als auch eingehend untersucht, wie sich das Safe-Harbor-Urteil auf die anderen Übermittlungsinstrumente auswirkt.

Das Europäische Parlament hat in einer Entschließung vom 23. Oktober 2015 ebenfalls Konsequenzen gefordert und beklagt, dass die Grundrechte der Bürger vor dem Hintergrund der Enthüllungen über elektronische Massenüberwachung durch Geheimdienste nach wie vor nicht hinreichend geschützt sind. Die Europäische Kommission wurde aufgefordert, umgehend die notwendigen Maßnahmen zu ergreifen, damit für alle in die USA übermittelten personenbezogenen Daten ein effektiver Schutz gilt, sowie über Alternativen zum Safe-Harbor-Grundsatz nachzudenken und bis Ende 2015 darüber zu berichten.

---

11 Positionspapier der Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder zu den Auswirkungen des EuGH-Urteils zum Safe-Harbor-Abkommen vom 6. Oktober 2015 (C-362/14) vom 26. Oktober 2015, siehe http://www.lda.brandenburg.de

12 Statement der Artikel-29-Datenschutzgruppe zur Umsetzung des Urteils des Europäischen Gerichtshofs vom 6. Oktober 2015 in der Rechtssache Maximilian Schrems vs. Datenschutzbeauftragter (C-362/14) vom 16. Oktober 2015, siehe http://www.lda.brandenburg.de

Die Europäische Kommission kündigte am 6. November 2015 an, die ohnehin laufenden Verhandlungen mit den USA im Lichte der EuGH-Entscheidung zügig voranzubringen und innerhalb von drei Monaten abzuschließen.

Das Urteil des Europäischen Gerichtshofs zu Safe Harbor stärkt nachhaltig das Grundrecht auf Datenschutz. Es stellt die bisher angewandten Instrumente zur Datenübermittlung in Drittstaaten auf einen Schlag infrage. Zu hoffen bleibt, dass zügig tragfähige Lösungen für transatlantische Datentransfers geschaffen werden.

2 Technisch-organisatorische Entwicklungen

2.1 Menschenrechte bei der elektronischen Kommunikation sichern

Unser letzter Tätigkeitsbericht[13] stand unter dem Eindruck der Enthüllungen von Edward Snowden zur anlasslosen und massenhaften Überwachung der weltweiten elektronischen Kommunikation durch Geheimdienste, insbesondere durch diejenigen der USA und Großbritanniens. Die Informationen waren damals erst wenige Monate alt. Im Verlauf des Berichtszeitraums wurden immer neue Einzelheiten über die Vorgehensweisen und die zum Ausspähen eingesetzten Verfahren bekannt. Welche technischen Möglichkeiten gibt es, um eine solche Überwachung zu verhindern oder zumindest zu erschweren?

Die Erhebung, Speicherung und Auswertung von Daten aus der elektronischen Kommunikation (z. B. bei der Nutzung von Telefonie-, Kurznachrichten-, Internet- oder E-Mail-Diensten) stellt einen Eingriff in verfassungsmäßig garantierte Grundrechte wie das Recht auf informationelle Selbstbestimmung oder das Recht auf Vertraulichkeit und Integrität informationstechnischer Systeme dar. Privat kommunizieren zu können, ohne dass Dritte Inhalte oder Umstände der Kommunikation erfahren, ermöglicht auch die Wahrnehmung anderer Grundrechte wie der Meinungs- und Versammlungsfreiheit.

Von dem anlasslosen und unbeschränkten Sammeln und Auswerten der Daten aus der elektronischen Kommunikation kann grundsätzlich jeder Einzelne betroffen sein. Aber auch Regierungen, Parlamente, Behörden und Unternehmen waren und sind nachweislich Ziele geheimdienstlicher Spähaktivitäten. Aus diesem Grund ist jeder Einzelne und jede Institution aufgefordert, das Kommunikationsverhalten zu überprüfen und ggf. Vorkehrungen zu treffen, das Überwachen der elektronischen Kommunikation zu verhindern

13 Tätigkeitsbericht 2012/2013, Einleitung

oder zumindest zu erschweren. Damit kann im Übrigen nicht nur der Tätigkeit von Geheimdiensten, sondern auch Aktivitäten von Internetkriminellen ein Riegel vorgeschoben werden.

Vor diesem Hintergrund hat die Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder im März 2014 einen Katalog von Anforderungen[14] vorgelegt, der sich an Anbieter elektronischer Kommunikationsdienste sowie an Behörden, Unternehmen und Bürger als Nutzer dieser Dienste richtet. Er enthält eine Reihe von technischen und organisatorischen Maßnahmen gegen die Überwachung der elektronischen Kommunikation.

Insbesondere wird darauf verwiesen, dass der Einsatz von Verschlüsselungsverfahren ein geeignetes Mittel ist, Daten sowohl bei ihrem Transport als auch bei ihrer Speicherung vor einer Kenntnisnahme durch Dritte zu schützen. Die den kryptografischen Algorithmen zu Grunde liegenden mathematischen Aussagen haben nach wie vor Gültigkeit – korrekt angewendete Kryptografie stellt eine erhebliche Hürde für Geheimdienste oder Kriminelle dar. Dies betrifft sowohl den Schutz der Inhalte der Kommunikation (d. h. der Inhalte einer E-Mail oder einer Internetkommunikation) als auch ihrer näheren Umstände (d. h. wer wann wie lange mit wem kommuniziert hat). Für beide Bereiche gibt es mit der Ende-zu-Ende- bzw. der Verbindungsverschlüsselung passende kryptografische Verfahren.

Allerdings ist auch festzustellen, dass Verschlüsselungsfunktionen häufig noch nicht in Hard- und Softwareprodukte integriert und ihre Bedienung zu schwierig ist. Auch eine breit angelegte, einfach von jedermann zu nutzende Infrastruktur – z. B. zur Überprüfung der Gültigkeit und Authentizität von Schlüsseln für kryptografische Verfahren – gibt es noch nicht. Die genannten Defizite wurden von Produktherstellern und Anbietern von Kommunikationsdiensten offenbar erkannt: Gerade in den letzten Monaten gab es verstärkt Meldungen, dass Sicherheitseigenschaften von Produkten oder Diensten explizit deklariert und als Wettbewerbsvorteil vermarktet werden. Auch wenn dies noch nichts über die Korrektheit der Implementierung aussagt, die erst im Rahmen einer Überprüfung und ggf. Zertifizierung durch unabhängige Stellen festgestellt wird, zeigt es doch die erhöhte Sensibilität gegenüber sicherheitstechnischen Fragestellungen. Dieser Prozess kann durch entsprechenden Druck und stete Nachfrage der Nutzer (also der Behörden, Unternehmen und Bürger) weiter verstärkt werden.

Weiterhin weist die Datenschutzkonferenz darauf hin, dass die Politik gefordert ist, die Rahmenbedingungen für einen breiten Einsatz von Verschlüsselungslösungen und für die Durchsetzung der erforderlichen Maßnahmen zu

[14] Entschließung „Gewährleistung der Menschenrechte bei der elektronischen Kommunikation“ vom 27. März 2014 (Anlage 1.7.5)

schaffen. Innovationen auf diesem Gebiet, insbesondere zur Integration kryptografischer Lösungen in Produkte sowie zur Vereinfachung ihrer Nutzung, sind zu fördern und die Begutachtung und Zertifizierung von entsprechenden Hard- und Softwareprodukten bzw. von Kommunikationsdiensten voranzutreiben.

Die Überwachung und das Ausspähen elektronischer Kommunikation können durch den Einsatz geeigneter Verfahren wirksam erschwert werden. Sichere kryptografische Lösungen hierfür sind seit Langem bekannt, werden allerdings weder routinemäßig genutzt noch überall dort eingesetzt, wo es erforderlich wäre. Alle Beteiligten an elektronischer Kommunikation einschließlich der Produkthersteller und der Diensteanbieter sind aufgefordert, geeignete und angemessene Maßnahmen zur Gewährleistung und Aufrechterhaltung der verfassungsmäßig garantierten Grundrechte umzusetzen.

2.2 Das Standard-Datenschutzmodell

Bei jeder automatisierten Verarbeitung personenbezogener Daten sind eine Reihe rechtlicher Anforderungen zu erfüllen, insbesondere bedarf sie einer tragfähigen Rechtsgrundlage. Darüber hinaus verlangen alle Datenschutzgesetze die Umsetzung geeigneter und dem Schutzbedarf der personenbezogenen Daten angemessener technischer und organisatorischer Maßnahmen, durch die die Risiken der Datenverarbeitung für Betroffene beherrscht werden können. Zur Überwindung der Lücke zwischen den rechtlichen Anforderungen einerseits und den technisch-organisatorischen Schutzmaßnahmen andererseits dient das Standard-Datenschutzmodell.

Bereits vor einigen Jahren setzte die Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder eine entsprechende Arbeitsgruppe ein. Diese entwarf unter Einbeziehung nationaler und internationaler Standards der IT-Sicherheit (wie z. B. IT-Grundschutz oder der ISO 2700x-Reihe) und deren Weiterentwicklung mit einem speziellen Fokus auf Aspekte des Datenschutzes einen neuen Ansatz, der

- aus den rechtlichen Datenschutzanforderungen sieben übergreifende Gewährleistungsziele ableitet,
- den Gewährleistungszielen einen Katalog an geeigneten konkreten Schutzmaßnahmen zur Seite stellt und
- Empfehlungen und Hinweise zur systematischen Anwendung des Ansatzes bei der Identifikation und Umsetzung von Schutzmaßnahmen in konkreten DV-Verfahren enthält.

Das Ergebnis, das Standard-Datenschutzmodell, wurde im Oktober 2015 von der Konferenz zustimmend zur Kenntnis genommen, zur Anwendung empfohlen und veröffentlicht.[15] Durch die Veröffentlichung soll auch eine breite Diskussion der Vorschläge unter nationalen und internationalen Fachleuten sowie mit Verantwortlichen bei Daten verarbeitenden Stellen angestoßen werden, die zu einer Weiterentwicklung und Verbesserung des Modells führen kann.

Zu den zentralen rechtlichen Anforderungen, die an jede automatisierte Verarbeitung personenbezogener Daten gestellt werden, gehören die Begrenzung der Verarbeitung auf das unbedingt erforderliche Maß, die strikte Zweckbindung der Datenverarbeitung, die Berücksichtigung der Rechte der Betroffenen (z. B. auf Auskunft, Berichtigung, Sperrung, Löschung), die Nachvollziehbarkeit und Prüfbarkeit der Datenverarbeitung sowie die IT-Sicherheit (im herkömmlichen Sinne) der Daten und IT-Systeme. Aus diesen Anforderungen lassen sich insgesamt sieben übergreifende Gewährleistungsziele ableiten: Neben die drei klassischen Ziele der IT-Sicherheit Vertraulichkeit, Integrität und Verfügbarkeit treten die drei datenschutzspezifischen Ziele Nichtverkettbarkeit, Transparenz und Intervenierbarkeit. Das Gewährleistungsziel Nichtverkettbarkeit bildet die datenschutzrechtliche Forderung der Zweckbindung ab: Personenbezogene Daten dürfen nicht für andere Zwecke als für diejenigen verarbeitet werden, die ihrer Erhebung zugrunde lagen. Eine Verkettung der Daten über Verfahrensgrenzen hinweg ist auszuschließen. Das Ziel der Transparenz sichert die Nachvollziehbarkeit und Prüfbarkeit von Verfahren, um ggf. Mängel erkennen und beheben zu können. Und letztlich garantiert das Gewährleistungsziel der Intervenierbarkeit die Einhaltung der Betroffenenrechte. Verantwortliche Daten verarbeitende Stellen sind verpflichtet, Maßnahmen umzusetzen, die z. B. das Berichtigen, Sperren und Löschen personenbezogener Daten ermöglichen.

Das siebte Gewährleistungsziel, die Datensparsamkeit, konkretisiert den datenschutzrechtlichen Grundsatz der Erforderlichkeit. Dieses Ziel ist grundlegend in dem Sinne, dass es den Umfang der Verarbeitung personenbezogener Daten sowohl bezüglich der Daten selbst als auch bezüglich der Zugriffe darauf minimiert. Alle anderen Gewährleistungsziele entfalten ihre Wirkung nur im Kontext dieses übergreifenden Ziels.

Im Standard-Datenschutzmodell werden den genannten sieben Gewährleistungszielen Schutzmaßnahmen zugeordnet, die die Umsetzung der Ziele ermöglichen. Darunter sind neben bereits aus der IT-Sicherheit bekannten Maßnahmen (wie Verschlüsselung von Daten oder Zugriffskontrolle) auch datenschutzspezifische Maßnahmen (wie zweckgebundene Pseudonyme für die Nichtverkettbarkeit oder spezifische Datenfelder zur Dokumentation von

[15] http://www.lda.brandenburg.de

Einwilligungen, Auskünften an oder Widersprüchen durch Betroffene). Soweit sie aus etablierten Katalogen der IT-Sicherheit (wie z. B. dem IT-Grundschutz) entnommen werden können, geschieht dies. Dort nicht enthaltene Maßnahmen für datenschutzspezifische Gewährleistungsziele entstammen der Beratungs- und Kontrollpraxis der Datenschutzbehörden. Der Schutzmaßnahmen-Referenzkatalog wird zurzeit vervollständigt und einzelne Maßnahmen werden detailliert beschrieben.

Dritter wesentlicher Bestandteil des Standard-Datenschutzmodells sind Hinweise und Empfehlungen zu seiner Anwendung. Auch hier werden Anleihen bei etablierten Methoden der IT-Sicherheit genommen (z. B. bei den Standards des Bundesamtes für Sicherheit in der Informationstechnik zur Vorgehensweise nach IT-Grundschutz), diese jedoch datenschutzspezifisch weiterentwickelt. Insbesondere sieht das Modell vor, bei der Bestimmung des Schutzbedarfs für Daten, IT-Systeme und Prozesse die Auswirkungen für Betroffene in den Mittelpunkt zu stellen. Es unterscheidet sich darin von klassischen Methoden der IT-Sicherheit, die den Schutzbedarf in der Regel aus Sicht der Daten verarbeitenden Stelle und der Risiken für die Organisation, also die Behörde oder das Unternehmen, identifizieren.

Die Hinweise und Empfehlungen zur Anwendung des Modells geben auch den Datenschutzbehörden eine wertvolle Hilfe: Einerseits können im Rahmen der Beratung frühzeitig datenschutzrechtliche Anforderungen auf technische und organisatorische Vorgaben zur Gestaltung des Verfahrens abgebildet werden. Dies leistet einen Beitrag zur Umsetzung des Grundprinzips „Privacy by Design“. Andererseits liegt mit dem Standard-Datenschutzmodell erstmalig auch ein einheitlicher Rahmen vor, der eine systematische, nachvollziehbare und vergleichbare Prüfung von Verfahren durch die Aufsichtsbehörden aus rechtlicher und technisch-organisatorischer Sicht ermöglicht.

Das Standard-Datenschutzmodell stellt einen neuen Ansatz zur Berücksichtigung der rechtlichen Anforderungen des Datenschutzes bei der Einführung und dem Betrieb von Verfahren zur Verarbeitung personenbezogener Daten dar. In unserer Beratungs- und Prüftätigkeit werden wir es in ausgewählten Projekten anwenden. Die Fachöffentlichkeit und alle Interessierten sind aufgerufen, an der Weiterentwicklung des Modells mitzuwirken.

2.3 Orientierungshilfe zur Entwicklung von Apps

Applikationen für mobile Endgeräte (Apps) können erhebliche Datenschutzrisiken auf das Smartphone oder Tablet bringen. Viele Apps weisen Sicherheitsmängel auf oder verstoßen gegen Datenschutzregeln. Die Datenschutzbehörden haben eine Orientierungshilfe herausgegeben, um die datenschutzgerechte App-Entwicklung zu unterstützen.

In den letzten Jahren haben sich Smartphones und Tablets stark verbreitet. Dadurch hat auch die Nutzung von Apps – also kleiner Programme, die auf den mobilen Geräten laufen – deutlich zugenommen. Leider sind jedoch bei Untersuchungen auch immer wieder Datenschutzverstöße und Sicherheitsmängel aufgefallen.[16] Um diesem Umstand zu begegnen, hat die Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder eine Orientierungshilfe[17] herausgegeben, die sich an Entwickler und Anbieter von Apps richtet. Sie befasst sich ausführlich mit den datenschutzrechtlichen und technischen Notwendigkeiten bei der Entwicklung und dem Vertrieb von Apps.

Im ersten Teil der Orientierungshilfe wird zunächst auf die Anwendbarkeit deutschen Datenschutzrechts und die jeweiligen Verantwortlichkeiten von App-Entwicklern, App-Anbietern und Betreiber von App-Stores eingegangen. Zudem wird dargelegt, dass der sachliche Anwendungsbereich des Datenschutzrechts schon aufgrund der gegebenen Bestimmbarkeit von Personen durch Daten wie die IP-Adresse, eindeutige Geräte- und Kartenkennungen, Standortdaten etc. eröffnet ist. Die Rechtsgrundlagen, die Erlaubnistatbestände und die geltenden Datenschutzgrundsätze werden ausführlich erläutert. Besonderes beachtenswert sind hierbei sowohl die Hinweise zu Bestands- und Nutzungsdaten, zu pseudonymisierten Nutzungsprofilen und zur Nutzereinwilligung als auch zu den Grundsätzen der Datensparsamkeit, der anonymen und pseudonymen Nutzung, der Zweckbindung und der Erforderlichkeit.

Wesentlicher Bestandteil von Apps muss auch eine transparente Information der Nutzer über die Erhebung und Verwendung personenbezogener Daten sein. Wie eine Datenschutzerklärung vom Inhalt und der Form her an Apps angepasst zu gestalten ist, wird daher ebenfalls in der Orientierungshilfe erläutert.

Im zweiten Teil wird ausführlich auf die Aspekte des technischen Datenschutzes eingegangen. Es werden Ausführungen für eine sichere Authentifizierung, die Behandlung von Anmeldedaten und eindeutigen Kennungen getroffen und detaillierte Informationen zur sicheren Datenübertragung gegeben. Darüber hinaus werden die lokale Datenspeicherung, die Protokollierung, der Zugriff auf Standortdaten und die Einbindung von Webseiten und Server-Diensten besprochen.

App-Entwickler und App-Anbieter sollten die Orientierungshilfe gründlich studieren und die Hinweise beachten. Dies dient im Übrigen nicht nur dem

16 Tätigkeitsbericht 2012/2013, A 2

17 http://www.lda.brandenburg.de

Datenschutz ihrer Kunden, sondern vermeidet auch aufsichtsrechtliche Maßnahmen wie Anordnungen oder Bußgelder.

Auch Apps müssen datenschutzrechtlichen Anforderungen entsprechen. Anbieter und Entwickler, die Apps auf dem deutschen Markt vertreiben wollen, sind aufgefordert, sich an die Vorgaben der Orientierungshilfe zur App-Entwicklung zu halten.

2.4 Cloud Computing – was gibt's Neues?

Die Datenschutzbehörden beschäftigen sich schon seit geraumer Zeit mit der Technologie des Cloud Computing, die zunehmend Bestandteil von Datenverarbeitungsprozessen der Privatwirtschaft sowie der öffentlichen Verwaltung ist. Insbesondere soll die Möglichkeit, flexibel, schnell und bedarfsgerecht für die Datenverarbeitung benötigte Ressourcen von einem Cloud-Anbieter beziehen zu können, zu einer Kostenreduktion führen. Allerdings dürfen dabei Aspekte des Datenschutzes und der Informationssicherheit nicht außer Acht gelassen werden.[18]

Die von der Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder im Jahr 2011 gemeinsam erarbeitete Orientierungshilfe Cloud Computing wurde im Berichtszeitraum weiterentwickelt und in der Version 2.0 veröffentlicht.[19] Hierbei fanden auch die zahlreichen Kommentare aus Wirtschaft und Verwaltung Berücksichtigung.

Das Dokument enthält im Wesentlichen Erläuterungen der datenschutzrechtlichen sowie der technischen und organisatorischen Aspekte des Cloud Computing. So werden aus rechtlicher Sicht detailliert die Verantwortlichkeit des Cloud-Anwenders, die Kontrolle der Cloud-Anbieter, die Gefahr der unrechtmäßigen Kenntniserlangung von Daten, die Verarbeitung verschlüsselter Daten, die Betroffenenrechte und der grenzüberschreitende Datenverkehr dargestellt. Auf Basis der anschließenden, genaueren Betrachtung der typischen Schutzziele des Datenschutzes und der Informationssicherheit sowie der klassischen und cloudspezifischen Risiken werden technische und organisatorische Maßnahmen abgeleitet, deren Umsetzung geboten ist. Diese Maßnahmen werden im Kontext der verschiedenen Betriebsmodelle (IaaS, PaaS, SaaS) erläutert.

Empfehlungen der Orientierungshilfe zur datenschutzkonformen Nutzung von Cloud-Angeboten fanden auch Einzug in dem Pilotprojekt „Datenschutz-Zertifizierung für Cloud-Dienste", welches im Auftrag des Bundesministeriums für Wirtschaft und Energie vom Kompetenzzentrum Trusted Cloud in Koope-

18 Tätigkeitsbericht 2010/2011, A 3.1

19 http://www.lda.brandenburg.de

ration mit Projektpartnern des Technologieprogramms Trusted Cloud durchgeführt wurde. Auch hier beteiligte sich unsere Dienststelle. Das Projekt mündete u. a. in einem Trusted Cloud-Datenschutzprofil für Cloud-Dienste, einem Prüfstandard für die Datenschutz-Zertifizierung von Cloud-Diensten.

Die Orientierungshilfe Cloud Computing und die Ergebnisse des Projekts Trusted Cloud liefern sowohl Cloud-Anbietern als auch Cloud-Nutzern wertvolle Hinweise und Empfehlungen für die datenschutzkonforme Planung und Umsetzung der Nutzung von Cloud-Diensten.

2.5 Cloud-unterstützte Betriebssysteme

Immer mehr moderne Betriebssysteme sehen eine dauerhafte Anbindung an internetbasierte Cloud-Dienste der Hersteller vor. Diese gewinnen damit zugleich die physische Hoheit über die privaten Daten der Nutzer. Standardeinstellungen sind fast immer so ausgelegt, dass eine automatisierte Datenübertragung in die Cloud stattfindet.

Ein Betriebssystem ist eine Sammlung von Software, die dazu dient, die physischen Elemente des Computers (Hauptplatine, Arbeitsspeicher, Festplatte, Grafikeinheit etc.) zu betreiben und mit den Anwendungen wie Schreib- und Mailprogrammen, Browser und Spielen zu verbinden. In der klassischen Form laufen Betriebssysteme lokal auf PCs und Servern und können ihre Aufgaben auch ohne Anschluss an das Internet vollständig ausführen.

Mit der Verbreitung von Mobilgeräten wie Smartphones und Tablets wurden neue Betriebssysteme entwickelt, die den speziellen Anforderungen dieser Gerätegeneration gerecht werden mussten. Dabei traten zwei Probleme in den Vordergrund: mangelnder Speicherplatz und hoher Aufwand für die Synchronisierung der Daten zwischen den kleinen Begleitern und den Heim-PCs. Um diese Probleme zu lösen, entwickelten die Hersteller der beiden dominierenden Mobilbetriebssysteme Apple und Google die Idee, den Nutzern die Datenspeicherung auf ihren Servern im Internet zu ermöglichen und die dazugehörigen Dienste im Betriebssystem darauf auszulegen, immer mit diesen Servern Kontakt zu halten. Zugleich sollten diese Dienste auch auf den jeweiligen Heim-PCs integriert werden. Ziel war es, sämtliche Nutzerdaten, auch die sich ständig ändernden wie Browserverläufe und Spielstände, den Anwendern sofort in aktueller Form zur Verfügung zu stellen und zwar unabhängig von dem Gerät, auf dem sie gerade arbeiten. Dazu ist es aber erforderlich, dass die Geräte einer Person ständig mit dem Internet verbunden sind und sämtliche persönlichen Daten auf den Servern in den Rechenzentren der Betriebssystemhersteller gespeichert und verarbeitet werden. Diese Server basieren auf der Cloud-Technologie, die sich unter anderem

dadurch auszeichnet, dass Daten abhängig vom gerade vorhandenen Ressourcenbedarf automatisiert verschoben werden und damit der physische Speicherort zu einem bestimmten Zeitpunkt innerhalb der Cloud unbestimmt ist.[20]

Neben den Annehmlichkeiten, die sich für Kunden ergeben, wenn sie ihre Daten der Apple- oder Google-Cloud anvertrauen, entstehen jedoch auch neue Risiken für ihre Privatsphäre, denn die Hersteller räumen sich oftmals ein weitgehendes Recht zur Auswertung der bei ihnen gespeicherten Daten ein, häufig mit der Begründung, die „Nutzererfahrung verbessern“ zu wollen. In der Regel gehört dazu jedoch auch, die Konzerneinnahmen durch den Verkauf personalisierter Werbung zu erhöhen. Insofern haben Hersteller handfeste Vorteile davon, wenn Kunden ihre Cloud-Systeme verwenden. Neben einer offensiven Werbung dafür versuchen sie häufig auch, den Kunden durch entsprechende Standardeinstellungen dazu zu bewegen, die Cloud zu verwenden. Meist wird es Nutzern zwar durchaus ermöglicht, die Geräte auch ohne ständige Cloud-Verbindung zu benutzen, diese Möglichkeit wird aber oft verschleiert, sodass Kunden, die keine tiefere Kenntnis der Einstellungsmöglichkeiten haben, ohne ihr aktives Wissen und Wollen in der Cloud landen können.

Nach den genuinen Mobilsystemen iOS und Android ist nun auch das neue Microsoft-Betriebssystem Windows 10 entsprechend der aktuellen Maxime des Konzerns „Mobile first, cloud first“ so konzipiert worden, dass es primär cloudunterstützt arbeitet. Die enge Verknüpfung mit den Online-Diensten führt dazu, dass Desktop-Einstellungen, Browserverläufe, Positionsverläufe u. v. m. automatisch auf den Microsoft-Servern landen. Ebenso benötigt die Suchassistentin Cortana weitreichende Befugnisse zur Übertragung persönlicher Daten. Es ist zwar durchaus möglich, vieles davon abzuschalten und alle Daten nur lokal zu verarbeiten, aber dazu müssen zunächst viele, im System weit verstreute Standardeinstellungen aktiv verändert werden. Im Übrigen wurde noch von keiner unabhängigen Stelle überprüft, inwieweit dadurch Datenübertragungen tatsächlich eingeschränkt werden.

Die Standardeinstellungen cloudunterstützter Betriebssysteme hat auch die Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder in einer Entschließung[21] deutlich kritisiert und die Hersteller aufgefordert, ihre Systeme mit datenschutzfreundlichen Grundeinstellungen auszuliefern. Darüber hinaus müssen die Hersteller auch vollständig darüber informieren, welche Daten zu welchen Zwecken übertragen werden.

---

20 Tätigkeitsbericht 2010/2011, A 3.1

21 Entschließung „Cloud-unterstützte Betriebssysteme bergen Datenschutzrisiken“ vom 30. September 2015 (Anlage 1.1.2)

Wir empfehlen den Nutzern der neuen Betriebssysteme, sich schon im Vorfeld über Funktionen und Einstellmöglichkeiten zu informieren. Insbesondere sind Unternehmen und Behörden gehalten, keinesfalls personenbezogene Daten durch den unbedachten Einsatz der Systeme ins Internet zu übertragen, sondern ihre datenschutzrechtliche Verantwortlichkeit ernst zu nehmen.

Cloud-unterstützte Betriebssysteme bringen neue Datenschutzrisiken mit sich. Die Hersteller sind aufgefordert, die Standardeinstellungen der Systeme datenschutzfreundlich zu gestalten. Nutzer sollten die Möglichkeiten zur Abschaltung der Datenübertragung in die Cloud kennenlernen und bewusst entscheiden, ob und wenn ja, welche Daten sie übertragen wollen.

2.6 Windows XP – Auch nach Ende des Support noch im Einsatz

Das Unternehmen Microsoft hat am 8. April 2014 den offiziellen Support für das Betriebssystem Windows XP eingestellt. Dieser Termin war seit vielen Jahren bekannt. Umso erstaunter waren wir, als wir erfuhren, dass auch noch über ein Jahr später diese Software bei verschiedenen öffentlichen Stellen zur Verarbeitung von z. T. sensitiven personenbezogenen Daten genutzt wurde.

Hersteller von Betriebssystemen und Anwendungssoftware bieten für ihre Produkte regelmäßig Aktualisierungen (sog. Updates oder Patches) an, die bestehende Fehler beseitigen und Sicherheitslücken schließen sollen. Betreibern von DV-Systemen ist dringend zu empfehlen, diese (nach entsprechenden Tests) zeitnah einzuspielen, um potenziellen Angreifern eine möglichst kleine Fläche zu bieten und die Sicherheit der Systeme zu gewährleisten.

Nach dem Ende des sog. Extended Supports für das Betriebssystem Windows XP am 8. April 2014 werden durch den Hersteller Microsoft keine Sicherheitsaktualisierungen mehr veröffentlicht. Neu entdeckte Fehler oder Sicherheitslücken werden somit nicht mehr geschlossen. Eine sichere Weiternutzung von PCs mit diesem Betriebssystem ist insbesondere dann kaum realisierbar, wenn es sich um vernetzte Systeme mit einem Internetzugang handelt – der Regelfall in Unternehmen und Behörden. Selbst wenn nur ein einziger von vielen Rechnern mit dem veralteten Betriebssystem läuft, kann einem Angreifer diese Schwachstelle genügen, um dort Schadsoftware zu platzieren und in der Folge das gesamte Netz zu gefährden. Grundsätzlich kann jede Kommunikationsschnittstelle eines Rechners – neben der Anbindung an ein Weitverkehrsnetz sind das z. B. USB-Schnittstellen oder Laufwerke für externe Datenträger – so zu einer Gefährdung für die Verarbeitung personenbezogener Daten werden. Auch der übliche Einsatz von Firewalls und Antivirenprogrammen zum Schutz der IT-Systeme kann den Wechsel auf

ein aktuelles und dem Support des Herstellers unterliegendes Betriebssystem nicht vollständig ersetzen.

Mit der Deutschen Rentenversicherung Berlin-Brandenburg, der Steuerverwaltung sowie der Polizei des Landes wurden uns drei Stellen im öffentlichen Bereich bekannt, in denen noch im Mai 2015 überdurchschnittlich viele Rechner unter Windows XP zur Verarbeitung von z. T. sensitiven personenbezogenen Daten genutzt wurden. Wir haben diese Stellen auf die o. g. Gefahren hingewiesen und sie aufgefordert, unverzüglich auf eine aktuelle Betriebssystemversion umzusteigen. Die Deutsche Rentenversicherung Berlin-Brandenburg hat daraufhin den Zeitplan für die Umstellung des Betriebssystems Windows XP auf Windows 7 überprüft und modifiziert. Damit sollten insbesondere die großen Abteilungen Rente und Versicherung sowie Rehabilitation und Gesundheitsförderung bis Ende Oktober 2015, und damit früher als geplant, umgestellt werden. Diese Abteilungen decken die nach den Sozialgesetzbüchern vorgegebenen Aufgaben eines Rentenversicherungsträgers weitgehend ab. Bis Ende des Jahres 2015 sollte die Migration auf Windows 7 abgeschlossen sein – wir werden dies selbstverständlich kontrollieren.

Aufgrund unserer Nachfrage im Mai 2015 zeigte sich, dass auch in der Finanzverwaltung noch ca. 1800 PCs mit Windows XP genutzt wurden. Die Umstellung auf Windows 7 war zwar bereits begonnen, hatte sich nach Angaben des Ministeriums der Finanzen jedoch wegen anderer vordringlicher Arbeiten verzögert. Sie sollte bis zum Ende des dritten Quartals 2015 abgeschlossen sein. Obwohl auf den PCs hoch schutzbedürftige Steuerdaten verarbeitet wurden, war eine weitere Nutzung von Windows XP bis zu diesem Zeitpunkt datenschutzrechtlich noch akzeptabel, da die Finanzverwaltung zusätzliche Sicherheitsmaßnahmen vorgesehen hatte. So erfolgte die Verarbeitung der Steuerdaten auf den PCs in einer vollständig gekapselten Umgebung, aus der ein Hinein- oder Herauskopieren von Daten nicht möglich ist. Der Internetzugang der PCs wurde ausschließlich über einen besonders abgesicherten Terminalserver realisiert.

Bei der Polizei Brandenburg wurden im Mai 2015 noch ca. 1300 PCs mit Windows XP betrieben. Die Standard-Arbeitsplatzcomputer der Polizei sind im sicheren Polizeinetz des Landes eingebunden und besitzen keinen direkten Zugang zum Internet. Eine Gefährdung kann daher mit großer Wahrscheinlichkeit ausgeschlossen werden. Bis Ende Mai 2015 erfolgte eine deutliche Reduzierung auf ca. 400 PCs. Die restlichen Geräte müssen auf der Basis von Einzelfallentscheidungen weiter mit Windows XP betrieben werden, da u. a. Fachanwendungen existieren, bei denen herstellerseitig die Umstellung auf Windows 7 oder eine höhere Version noch nicht erfolgt ist.

Der Einsatz von Betriebssystemen, deren Support eingestellt wurde, kann ein hohes Risiko für die Vertraulichkeit, Integrität und Verfügbarkeit der damit verarbeiteten personenbezogenen Daten darstellen. Verantwortliche Stellen sollten daher frühzeitig eine Strategie zur Migration auf aktuelle Versionen der von ihnen verwendeten Software erarbeiten und konsequent umsetzen.

2.7 GeoBusiness Code of Conduct – eine freiwillige Selbstverpflichtung der Geoinformationswirtschaft

Bei der Verarbeitung und Nutzung von Geodaten durch Unternehmen können auch datenschutzrechtliche Probleme auftreten. Insbesondere besteht Unsicherheit bzgl. der Frage, wann diese Daten personenbeziehbar sind und wie Unternehmen mit staatlich bereitgestellten, personenbezogenen Geodaten umzugehen haben. Ein neuer Code of Conduct (Verhaltensregeln) soll hier Abhilfe schaffen.

Geodaten sind in der heutigen digitalen Welt für eine Vielzahl von Unternehmen von großem Wert. Häufig sind sie selbst Bestandteil von Produkten und Dienstleistungen oder dienen dazu, diese besser zu vermarkten. Oftmals möchten die Unternehmen dabei auch auf Geodaten zurückgreifen, die von öffentlichen Stellen (z. B. im Rahmen der Umsetzung der INSPIRE-Richtlinie der Europäischen Union) bereitgestellt werden. Wenn diese Daten einen Personenbezug aufweisen, sind sowohl bei ihrer Übermittlung an Unternehmen als auch bei ihrer anschließenden Verarbeitung und Nutzung datenschutzrechtliche Aspekte zu beachten.

Die Kommission für Geoinformationswirtschaft des Bundesministeriums für Wirtschaft und Energie (GIW-Kommission), in der die Spitzenverbände der deutschen Wirtschaft vertreten sind, und der Verein Selbstregulierung Informationswirtschaft e. V. haben im Berichtszeitraum Verhaltensregeln für die Verarbeitung und Nutzung von Geodaten erstellt und in einem GeoBusiness Code of Conduct „GeoBusiness und Datenschutz“ zusammengefasst.[22] Die Arbeiten wurden durch die Unterarbeitsgruppe Geodaten der Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder inhaltlich begleitet. Unsere Dienststelle wirkte hierbei mit. Mittlerweile wurden die Verhaltensregeln gem. § 38 a Abs. 2 Bundesdatenschutzgesetz (BDSG) durch den zuständigen Berliner Beauftragten für Datenschutz und Informationsfreiheit anerkannt.

Der Code of Conduct enthält u. a. eine Beschreibung von Fällen, in denen die Verarbeitung und Nutzung von Geodaten, die Unternehmen von der öffentlichen Hand erhalten haben, grundsätzlich datenschutzrechtlich zulässig ist.

[22] https://www.geodatenschutz.org

Hierbei werden insbesondere Kriterien benannt, nach denen in der Regel davon auszugehen ist, dass die Verarbeitung der personenbezogenen Geodaten schutzwürdige Interessen der Betroffenen nicht beeinträchtigt (z. B. bei Unterschreiten eines Kartenmaßstabs, Überschreiten einer Bildauflösung oder Aggregation der Daten von mindestens vier Haushalten). Öffentliche Stellen können diese Kriterien ergänzend zu konkreten Rechtsvorschriften heranziehen, um zu entscheiden, ob eine Übermittlung von Geodaten an Unternehmen zulässig ist.

Weiterhin ermöglicht der Code of Conduct Unternehmen der Geoinformationswirtschaft, sich der freiwilligen Selbstkontrolle bzgl. der datenschutzkonformen Verarbeitung und Nutzung von Geodaten zu unterwerfen. Mit dem Beitritt zu den Verhaltensregeln verpflichten sich die Unternehmen, ihre Geschäftsprozesse beim Umgang mit personenbezogenen Geodaten akkreditieren zu lassen. Falls kein Personenbezug vorliegt oder schutzwürdige Interessen der Betroffenen nicht beeinträchtigt werden, können die Unternehmen Geschäftsprozesse zum Umgang mit Geodaten freiwillig akkreditieren lassen. Im Rahmen der Akkreditierung muss das Unternehmen insbesondere das Vorliegen eines auf Schutzziele[23] ausgerichteten Datenschutzmanagementsystems bestätigen. Hierzu gehören u. a. die Bestellung eines betrieblichen Datenschutzbeauftragten, die Umsetzung geeigneter technisch-organisatorischer Maßnahmen gem. § 9 BDSG und das Vorhandensein eines internen Beschwerdemanagements. Die Akkreditierungsstelle bei der GIW-Kommission prüft diese Angaben auf Plausibilität und Vereinbarkeit mit den Verhaltensregeln.

Mit dem GeoBusiness Code of Conduct werden Rahmenbedingungen für eine einheitliche und datenschutzkonforme Verarbeitung und Nutzung von Geodaten in Deutschland geschaffen. Unternehmen, die diesen Verhaltensregeln beitreten und ihre Geschäftsprozesse akkreditieren lassen, verpflichten sich freiwillig zum Einsatz eines Datenschutzmanagementsystems sowie technisch-organisatorischer Maßnahmen und tragen damit zur Erhöhung des Datenschutzniveaus bei der Verarbeitung von Geodaten bei.

[23] siehe B 2.2

2.8 IT-Sicherheitsgesetz

Weite Bereiche des gesellschaftlichen Lebens sind heute vom korrekten Funktionieren der dort verwendeten Informationstechnik abhängig. Ausfälle oder Störungen z. B. durch Angriffe auf Hard- und Software, auf Kommunikationsverbindungen oder auf die verarbeiteten Daten können zum Teil gravierende negative Auswirkungen für Bürger, Wirtschaft und Behörden haben. Dies gilt in besonderem Maße für so genannte kritische Infrastrukturen. Ein neues Gesetz soll hier Vorsorge treffen.

Das IT-Sicherheitsgesetz[24] ist Mitte 2015 in Kraft getreten. Es hat das Ziel, eine signifikante Verbesserung der IT-Sicherheit in Deutschland zu erreichen, indem einerseits Vorgaben für die Implementierung von IT-Sicherheitsmaßnahmen getroffen und andererseits Meldepflichten bei IT-Sicherheitsvorfällen eingeführt werden. Betroffen sind hiervon Betreiber kritischer Infrastrukturen. Dazu zählen Einrichtungen, Anlagen oder Anlagenteile in den Sektoren Energie, Informationstechnik, Telekommunikation, Transport und Verkehr, Gesundheit, Wasser, Ernährung sowie Finanz- und Versicherungswesen, die von hoher Bedeutung für das Funktionieren des Gemeinwesens sind, weil durch ihren Ausfall oder ihre Beeinträchtigung erhebliche Versorgungsengpässe oder Gefährdungen für die öffentliche Sicherheit eintreten würden. Die gesetzliche Definition des Begriffs der kritischen Infrastrukturen soll durch eine noch zu erlassende Rechtsverordnung präzisiert werden.

Betreiber kritischer Infrastrukturen sind verpflichtet, spätestens zwei Jahre nach Inkrafttreten der genannten Verordnung angemessene technische und organisatorische Maßnahmen zur Gewährleistung der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit ihrer maßgeblichen informationstechnischen Systeme zu treffen. Dies kann auf der Basis branchenspezifischer Standards erfolgen, die durch das Bundesamt für Sicherheit in der Informationstechnik (BSI) zu prüfen sind. Die Einhaltung der Anforderungen ist regelmäßig alle zwei Jahre z. B. durch Audits oder Zertifizierungen nachzuweisen. Werden hierbei Sicherheitsmängel aufgedeckt, kann das BSI deren Beseitigung verlangen.

Darüber hinaus legt das Gesetz fest, dass Betreiber kritischer Infrastrukturen erhebliche Störungen der Sicherheit ihrer informationstechnischen Systeme, die zu einem Ausfall oder einer Beeinträchtigung der Funktionsfähigkeit der Infrastrukturen führen können oder geführt haben, über eine Kontaktstelle unverzüglich an das BSI zu melden haben. Das BSI sammelt diese und andere, allgemeine Meldungen z. B. über Sicherheitslücken oder Schadpro-

[24] Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme vom 17. Juli 2015, BGBl. I S. 1324

gramme, wertet sie aus und führt sie mit Informationen zur Abwehr von Gefahren für die Informationstechnik zusammen. Es gibt seine Erkenntnisse an die Betreiber kritischer Infrastrukturen sowie an die zuständigen Aufsichtsbehörden des Bundes und der Länder weiter.

Die Regelungen des IT-Sicherheitsgesetzes sind insoweit zu begrüßen, als dass für Betreiber kritischer Infrastrukturen eine Vereinheitlichung branchenweiter und hoher IT-Sicherheitsstandards ermöglicht wird und die Umsetzung von Sicherheitsmaßnahmen regelmäßig verbindlich nachzuweisen ist. Auch die Sammlung und Auswertung von Informationen über Sicherheitsvorfälle und Abwehrmaßnahmen sowie die Bereitstellung der Analyse zur Erhöhung des Niveaus der IT-Sicherheit kritischer Infrastrukturen sind positiv zu bewerten. Wünschenswert wäre allerdings gewesen, die Einbeziehung der Datenschutzbehörden explizit im Gesetz zu regeln, da sowohl bei der Datenverarbeitung in kritischen Infrastrukturen als auch bei Meldungen über Störungen der IT-Sicherheit personenbezogene Daten betroffen sein können. Insofern hätten die Datenschutzbehörden ihre Erfahrungen, z. B. bei der Festlegung von hohen Informationssicherheitsstandards oder bei der datenschutzgerechten Gestaltung der Meldeverfahren bei Störungen, einbringen können.

Betreiber kritischer Infrastrukturen sind aufgefordert, ihr Informationssicherheitsmanagement und die realisierten IT-Sicherheitsmaßnahmen gemäß den Anforderungen des IT-Sicherheitsgesetzes zu überprüfen und die ggf. erforderlichen Aktivitäten zeitnah zu beginnen. Soweit auch die Verarbeitung personenbezogener Daten betroffen ist, sind wir gern bereit, sie zu beraten.

3 Arbeit und Soziales

3.1 Datenschutzrechtliche Prüfungen von Jobcentern

Im Berichtszeitraum kontrollierten wir mehrere Jobcenter, die von Landkreisen in eigener Verantwortung betrieben werden,[25] auf die Einhaltung datenschutzrechtlicher Bestimmungen im Umgang mit personenbezogenen Daten der Leistungsempfänger. Schwerpunkte dieser angekündigten, anlassunabhängigen Kontrollen waren technisch-organisatorische Maßnahmen zur Gewährleistung von Datenschutz und Informationssicherheit,[26] die Gebäude- und Rauminfrastruktur, die Stellung des behördlichen Datenschutzbeauftragten im Jobcenter und die Aktenführung.

[25] zur Zuständigkeit für die Datenschutzkontrolle siehe Tätigkeitsbericht 2010/2011, A 4.1

[26] siehe A 3.2

3.1.1 Gebäude- und Rauminfrastruktur

Gemäß § 78 a Zehntes Buch Sozialgesetzbuch (SGB X) haben Jobcenter, als für die Datenverarbeitung verantwortliche Stellen, die technischen und organisatorischen Maßnahmen zu treffen, die erforderlich sind, um den Sozialdatenschutz für ihre Kunden zu gewährleisten. Die Wahrung des Sozialgeheimnisses gem. § 35 Abs. 1 Erstes Buch Sozialgesetzbuch (SGB I) umfasst die Verpflichtung, auch innerhalb des Jobcenters sicherzustellen, dass die Sozialdaten nur Befugten zugänglich sind. Entsprechend ist die Gebäude- und Rauminfrastruktur zu gestalten.

Die Eingangsbereiche der geprüften Jobcenter, in denen der Erstkontakt mit den Bürgern bei Antragstellung stattfindet, entsprachen – bis auf einen Fall, in dem noch Schallschutzmaßnahmen erfolgen müssen – den datenschutzrechtlichen Anforderungen. Die Jobcenter hatten Diskretionszonen in ausreichendem Abstand vom Tresen ausgewiesen. Auch konnten die Bürger ungestört Anträge ausfüllen. Teilweise wird für die Erstantragstellung sogar ein individueller Termin vereinbart. Die Erstberatung findet sodann in einem abgetrennten Bereich der Eingangszone statt. Durch die direkte Übergabe von Anträgen ist zugleich sichergestellt, dass die Bürger nach Hinweis der Mitarbeiter Schwärzungen auf den Kopien einzureichender Unterlagen vornehmen können.

PC-Bildschirme sind so einzurichten, dass Dritte diese nicht einsehen können. Aus diesem Grund wurden in einem Jobcenter Sichtschutzfolien auf die Monitore aufgebracht.

In jedem Fall haben die Mitarbeiter dafür Sorge zu tragen, dass dem Kunden keine personenbezogenen Daten anderer Leistungsempfänger zur Kenntnis gelangen können. Demgemäß sind die Akten entsprechend zu lagern und Telefonate über Angelegenheiten von Kunden nicht in Anwesenheit Dritter zu führen.

Die gleichzeitige Beratung mehrerer Kunden in Doppelbüros ist unzulässig und kann nur durch eine Einzelterminvergabe vermieden werden. Dies wird in den Jobcentern in der Regel so umgesetzt. Alternativ sind Doppelbüros durch bauliche Maßnahmen wie Schall- und Sichtschutzwände so zu gestalten, dass das Sozialgeheimnis gewahrt bleibt. Zudem empfehlen wir, ein separates Beratungszimmer vorzuhalten, damit die Möglichkeit eines Einzelgesprächs gegeben ist. Hierüber ist der Bürger vor dem Gespräch zu informieren. Dies gilt insbesondere, wenn Mitarbeiter, die sich nicht gegenseitig vertreten, gemeinsam ein Büro nutzen, da auch hier eine Datenübermittlung an unzuständige Dritte erfolgen könnte.

Darüber hinaus sind die Akten vor einem Zugriff Dritter, hierzu zählen auch Reinigungskräfte und Mitarbeiter des Wachschutzes, zu schützen und verschlossen aufzubewahren. Nicht alle Jobcenter erfüllten diese Anforderung. So mussten wir bei der Besichtigung von mehreren Büros feststellen, dass Aktenschränke wegen defekter Schlösser nicht abgeschlossen werden konnten, Aktenstapel auf dem Boden lagen oder in offenen Kisten aufbewahrt wurden, weil Archive überfüllt waren oder der Transport an einen anderen Standort auf sich warten ließ.

Im Eingangsbereich einer Kreisverwaltung fanden wir überfüllte und zur Abholung bereitgehaltene Papiercontainer vor. Auf unseren Hinweis hin trug die Behörde dafür Sorge, dass die zur Vernichtung vorgesehenen personenbezogenen Unterlagen künftig nicht mehr problemlos von jedermann entnommen werden können. Das unbefugte Entwenden von Unterlagen muss auch bei den von den Jobcentern verwendeten Briefkästen verhindert werden. Teilweise waren hier die Einwurföffnungen so groß, dass sich Unterlagen einfach herausnehmen ließen.

In einem Jobcenter erfolgt die Vernichtung von Papierdokumenten zentral in einem Kellerraum. Dort werden die Unterlagen in zahlreichen offenen Behältnissen gesammelt und von einer verantwortlichen Person mit einem Aktenvernichter in unregelmäßigen Abständen vernichtet. Der Raum war zwar verschlossen, allerdings verhinderten lediglich ein paar lose zusammengeschraubte Holzbretter und ein handelsübliches Vorhängeschloss das unbefugte Betreten des Raumes. Dies war eine völlig ungenügende Zutrittssicherung.

Zudem erfüllte der eingesetzte Aktenvernichter nicht die Anforderungen der Sicherheitsstufe, die für die Vernichtung sensitiver Daten anzusetzen ist. Sozialdaten sind hoch schutzbedürftige Daten und entsprechend der DIN 66399 „Büro- und Datentechnik – Vernichtung von Datenträgern“ der Schutzklasse 2 zuzuordnen. Bereits in unserem letzten Tätigkeitsbericht[27] hatten wir empfohlen, zur Erfüllung der gesetzlichen Anforderungen des Löschens diese nach der Sicherheitsstufe 4 – besser nach Stufe 5 – zu vernichten.

Die Einhaltung des Datenschutzes verlangt auch die Beachtung räumlicher und infrastruktureller Mindeststandards. Vertraulichkeit von Gesprächen ist genauso zu gewährleisten wie die Sicherung des Zugangs zu Briefkästen und Aktenvernichtungsanlagen.

[27] Tätigkeitsbericht 2012/2013, B 2.4

3.1.2 Behördliche Datenschutzbeauftragte der Jobcenter

Daten verarbeitende Stellen haben einen behördlichen Datenschutzbeauftragten zu bestellen. Dies gilt nach § 81 SGB X i. V. m. § 7 a Brandenburgisches Datenschutzgesetz (BbgDSG) auch für die Jobcenter. In den von uns geprüften Jobcentern wird die Funktion durch den behördlichen Datenschutzbeauftragten des jeweiligen Landkreises ausgeübt. Gemäß § 7 a BbgDSG hat dieser ein direktes Vorspracherecht bei der Behördenleitung, unterliegt in Ausübung seiner Funktion keinen Weisungen und darf wegen der Erfüllung seiner Aufgaben nicht benachteiligt werden. Wie sich der Verwaltungsvorschrift des Ministeriums des Innern zur Durchführung des Brandenburgischen Datenschutzgesetzes entnehmen lässt, „ist zu gewährleisten, dass der behördliche Datenschutzbeauftragte mit den notwendigen Ressourcen ausgestattet ist. Dies betrifft sowohl die materielle Ausstattung als auch den für diese Tätigkeit zur Verfügung stehenden Zeitanteil. Es muss gewährleistet sein, dass der behördliche Datenschutzbeauftragte seinen Verpflichtungen im ausreichenden Umfang nachkommen kann."

Während der Prüfungen konnten wir uns davon überzeugen, dass die behördlichen Datenschutzbeauftragten über eigene Büros und eine eigene funktionsbezogene E-Mail-Adresse verfügen. Somit sind Gespräche unter vier Augen sowie eine direkte und vertrauliche Kontaktaufnahme möglich.

Allerdings mangelte es in einigen Fällen deutlich an genügenden zeitlichen Ressourcen sowie an der Einbindung in und Information über datenschutzrelevante Vorgänge und Verfahren durch die verantwortlichen Stellen. Ohne diese Informationen können die behördlichen Datenschutzbeauftragten ihrer Pflicht zur Beratung der Dienststellen nicht in ausreichendem Maße nachkommen.

Wie wir leider auch feststellen mussten, sind die behördlichen Datenschutzbeauftragten in den überwiegenden Fällen nicht ausschließlich im Bereich des Datenschutzes tätig, vielmehr sind sie zugleich für verschiedenste andere Arbeitsbereiche (z. B. Arbeitsschutz, Katastrophenschutz, Sachbearbeitung in einer Fachabteilung) zuständig. Für die Bearbeitung datenschutzrechtlicher Fragen in den Jobcentern bleibt deshalb sehr wenig Zeit. Dies gilt umso mehr, da die behördlichen Datenschutzbeauftragten jeweils für die gesamte Kreisverwaltung bestellt sind. Sie sind Ansprechpartner sowohl für alle Mitarbeiter als auch für Bürger.

Zudem verfügen die Landkreise meist über diverse Außenstellen (allein die Jobcenter haben in der Regel mehrere Standorte) und nachgeordnete Einrichtungen. Für all diese Stellen müssen die behördlichen Datenschutzbeauftragten den gesetzlichen Anforderungen entsprechend tätig werden und sind folglich mit einer Fülle unterschiedlicher fachlicher Anforderungen konfron-

tiert. Hierzu zählen etwa die Pflege der Verfahrensverzeichnisse für die gesamte Landkreisverwaltung, die Prüfung bestehender und neuer Verfahren auf ihre datenschutzrechtliche Zulässigkeit, die Schulung sämtlicher Mitarbeiter im Datenschutzrecht und ihre Beratung und Unterstützung in Angelegenheiten des Personaldatenschutzes.

Ausgehend von einer Vollzeitstelle mit einer Arbeitszeit von 40 Stunden in der Woche dürfte der den behördlichen Datenschutzbeauftragten der Landkreise zur Verfügung gestellte Zeitanteil von teilweise nur 30 % oder weniger für ein derart umfangreiches Aufgabenspektrum nicht ausreichen. Es stellt sich die Frage, ob die nach dem Brandenburgischen Datenschutzgesetz vorgesehene Bestellung eines behördlichen Datenschutzbeauftragten in solchen Fällen überhaupt ordnungsgemäß erfolgt ist. Der Blick auf die Rechtslage für die als gemeinsame Einrichtungen von Bund und Ländern geführten Jobcenter lässt vielmehr darauf schließen, dass die Bestellung unwirksam ist. Schließlich hat der Gesetzgeber bestimmt, dass die gemeinsamen Jobcenter einen Mitarbeiter als behördlichen Datenschutzbeauftragten zu benennen haben, und zwar ausschließlich für das jeweilige Jobcenter. Nur so kann es seine komplexen, datenschutzrechtlichen Aufgaben bewältigen.

Die Landkreise sind aufgefordert, dafür Sorge zu tragen, dass die im Gesetz verankerte Pflicht der datenschutzrechtlichen Beratung, Prüfung, Kontrolle durch den behördlichen Datenschutzbeauftragten tatsächlich umgesetzt wird. Wir empfehlen dringend, den Arbeitszeitanteil für die datenschutzrechtlichen Aufgabenstellungen bei den Datenschutzbeauftragten zu erhöhen und sie zudem im erforderlichen Umfang (z. B. durch Vertretungsregelungen) zu unterstützen.

3.1.3 Aktenführung

Eine korrekte Aktenführung gibt sowohl den Betroffenen als auch der Behörde die Möglichkeit, sich einen umfassenden Überblick über die Entscheidungsgrundlagen zu verschaffen. Insbesondere bei Ermessensentscheidungen wird erkennbar, welche Sachverhalte in die Entscheidungsfindung eingeflossen sind.

Grundsätzlich dürfen die Leistungsträger gem. § 67 a Abs. 1 Satz 1 SGB X Sozialdaten nur dann erheben, wenn ihre Kenntnis für die Erfüllung einer ihnen im Gesetz zugewiesenen Aufgabe erforderlich ist, um den Anspruch auf die Leistung dem Grunde und der Höhe nach feststellen zu können. Eine darüber hinausgehende Datenerhebung ist unzulässig.

Wir prüften in jedem Jobcenter mehrere, nach dem Zufallsprinzip ausgewählte Leistungsakten und Akten aus dem Bereich der Vermittlung. Die Aktenfüh-

rung genügte nicht in allen Punkten den datenschutzrechtlichen Anforderungen.

3.1.3.1 Vorlage von Unterlagen

Nach dem Sozialgesetzbuch sind alle, die Sozialleistungen beantragen, zur Mitwirkung verpflichtet. Klare gesetzliche Vorgaben, ob und in welchem Umfang der Leistungsträger in diesem Zusammenhang beispielsweise die Vorlage von vollständigen Mietverträgen und Scheidungsurteilen verlangen darf, und welche Angaben geschwärzt werden dürfen, enthalten diese Vorschriften jedoch nicht. Die Entscheidung, welche Unterlagen jeweils vorzulegen sind, richtet sich nach den konkreten Bedingungen des Einzelfalls. Die Anfertigung von Kopien ist in der Regel nicht erforderlich, der Betroffene kommt seiner Nachweispflicht auch durch bloße Vorlage der Unterlagen nach. Häufig reicht es aus, dass Mitarbeiter Einzelangaben vermerken. Insbesondere Informationen über die Gesundheit sind ggf. in einem gesonderten, verschlossenen Umschlag zu den Akten zu nehmen. Im Einzelnen stellt sich dies wie folgt dar:

- Kontoauszüge

In den kontrollierten Jobcentern hat sich der Umgang mit den angeforderten Kontoauszügen im Vergleich zu den letzten Berichtszeiträumen verbessert. Größtenteils wurden lediglich die leistungsrelevanten Informationen im jeweiligen Vorgang mittels eines Vermerks gespeichert. Dies war erfreulich.

- Sparbücher

Die Anfertigung von Kopien von Sparbüchern ist aus unserer Sicht nicht notwendig. Ein Vermerk über das bestehende Guthaben bzw. die Zinserträge ist – ähnlich wie bei den Kontoauszügen – ausreichend und im Rahmen der Vermögensprüfung zu notieren. In der Regel fertigten die Jobcenter jedoch Kopien der letzten Seite des Sparbuchs an.

- Lebensversicherungen, Sparbriefe

Bei der Feststellung von Vermögen sind Sparbriefe und andere Wertpapiere ebenso relevant, wie abgeschlossene Kapitallebensversicherungen. Auf eine vollständige Kopie aller Unterlagen ist jedoch mangels Erforderlichkeit zu verzichten. Es genügt, sich vom Betroffenen eine Bescheinigung über den Rückkaufswert, also einen Nachweis über eine mögliche Verwertbarkeit, vorlegen zu lassen.

- Personalausweis

Vereinzelt wurden Kopien von Personalausweisen in den Akten gespeichert. Die Anfertigung und Speicherung von Personalausweiskopien ist für Zwecke der Jobcenter jedoch unzulässig. Zwar müssen bei Anträgen auf Arbeitslosengeld II die dazu erforderlichen Unterlagen vorgelegt werden, um die Anspruchsvoraussetzungen feststellen zu können, was auch die Überprüfung der Identität und der aktuellen Wohnanschrift einschließt. Eine Kopie des Personalausweises zu der Akte zu nehmen, ist jedoch nicht erforderlich. Vielmehr genügt ein auf dem Antragsformular anzubringender Vermerk, dass der aktuelle Personalausweis oder ein anderes Ausweisdokument vorgelegen hat.

- Schwerbehindertenausweis, Krankenversicherungskarte und Sozialversicherungsausweis

Für eine erfolgreiche Vermittlung und die berufliche Integration ist es bedeutsam, gesundheitliche Einschränkungen zu kennen. Dennoch ist eine Kopie des Schwerbehindertenausweises nicht in der Akte zu speichern. Diese enthält – nicht zuletzt mit dem darauf befindlichen Foto – mehr Informationen, als für die Leistungsgewährung notwendig. Auch hier genügt ein Vermerk über die Vorlage und die vergebenen Merkzeichen. Dies gilt auch für die Krankenversicherungskarte und den Sozialversicherungsausweis. Der Nachweis über die Krankenversicherung kann mit der Krankenversicherungskarte bzw. der neuen elektronischen Gesundheitskarte oder aber auch mit anderen Unterlagen, wie z. B. einer Bescheinigung der Krankenkasse, erbracht werden. Es genügt ein Abgleich mit den im Antrag gemachten Angaben.

- Arbeitsverträge, Ausbildungsverträge

Die Anforderung des gesamten Arbeits- oder Ausbildungsvertrages ist nur zulässig, wenn dem Jobcenter ohne dessen Kenntnis eine rechtmäßige Erbringung von Leistungen nicht möglich wäre. In der Regel liegen dem Jobcenter aber alle für die Entscheidung über die weitere Leistungsgewährung erforderlichen Informationen mit der Veränderungsmitteilung und der noch vorzulegenden Einkommensbescheinigung vor.

- Prüfungszeugnis

Grundsätzlich halten wir die Einsichtnahme in Zeugnisse für ein wichtiges Instrument der erfolgreichen Integrationsarbeit mit den betroffenen Leistungsempfängern. Die Begleitung des Integrationsprozesses sollte auf einer möglichst detaillierten Kenntnis des individuellen Beratungsfalles beruhen. Durch die Einsichtnahme in Zeugnisse können Fehlentwicklungen im schulischen oder beruflichen Werdegang erkannt und entsprechende Maßnahmen

ergriffen werden. Allerdings erschließt sich nicht die Notwendigkeit der Speicherung des vollständigen Prüfungszeugnisses in der Akte des Arbeitsvermittlers bzw. Fallmanagers, wenn die Prüfung und damit die Ausbildung nicht bestanden wurden. Hier würde gegebenenfalls ein kurzer Vermerk genügen.

- Mietverträge

In geprüften Akten befanden sich auch vollständige Mietverträge nebst Betriebskostenabrechnung. Um die aktuelle Miete nachzuweisen, genügt es, wenn der Betroffene beispielsweise das letzte Mieterhöhungsschreiben oder die Betriebskostenabrechnung vorlegt. Die Anfertigung von Kopien des vollständigen Vertrages ist im Regelfall nicht erforderlich. Der Antragsteller trägt selbst in der Regel die erforderlichen Angaben zur Miete in den Antragsvordrucken ein. Nach unserer Auffassung hat der Mitarbeiter die Angaben anhand des vorzulegenden Mietvertrages zu kontrollieren und das Ergebnis seiner Kontrolle in einem Aktenvermerk oder auf dem Antragsvordruck festzuhalten.

- Geburtsurkunden der Kinder

In den Vorgängen wurden – zum Teil mehrfach – die Geburtsurkunden der Kinder abgespeichert. Aus unserer Sicht ist die Speicherung dieser Dokumente in der Akte nicht notwendig. Allenfalls könnte bei der Aufnahme Neugeborener in die Bedarfsgemeinschaft eine Geburtsbescheinigung zu den Akten genommen werden.

- Schulbescheinigungen

Aus welchem Grund Schulbescheinigungen für die Leistungsgewährung in jedem Fall zwingend erforderlich sind, ist unklar. Angesichts der bestehenden Schulpflicht ist in der Regel davon auszugehen, dass ein Kind die Schule besucht. Eine Schulbescheinigung ist also nur in Ausnahmefällen erforderlich: wenn beispielsweise das Kind das 15. Lebensjahr vollendet hat, muss das Jobcenter über den schulischen oder beruflichen Werdegang des 15-jährigen Leistungsempfängers informiert sein, um ggf. rechtzeitig beratend und unterstützend tätig werden zu können. Die Vorlage von Schulbescheinigungen ist dann erforderlich und aus datenschutzrechtlicher Sicht unbedenklich.

3.1.3.2 Gesundheitsangaben

Ein Anspruch auf Arbeitslosengeld II besteht nur, wenn der Betroffene erwerbsfähig ist, also nicht wegen Krankheit oder Behinderung auf absehbare Zeit außerstande ist, unter den üblichen Bedingungen des allgemeinen Arbeitsmarktes mindestens drei Stunden täglich erwerbstätig zu sein (§ 8

Abs. 1 SGB II). Bestehen Zweifel an der Erwerbsfähigkeit oder daran, ob ein bestimmtes Arbeitsangebot oder eine Maßnahme wahrgenommen werden kann, ist der Amtsarzt einzuschalten. Dieser nimmt die notwendige Untersuchung bzw. Bewertung der eingereichten Dokumente vor. Der Leistungssachbearbeiter erhält lediglich das Ergebnis der ärztlichen Feststellungen zur Kenntnis. Zusätzliche Angaben, wie die vom Arzt verordneten Therapien oder Diagnosen sind für den Sachbearbeiter nicht erforderlich.

- Arztbriefe, Atteste, Krankenhausentlassungsberichte

Angaben über die Gesundheit zählen gem. § 67 Abs. 12 SGB X zu den besonderen Arten personenbezogener Daten. Sie sind besonders vertraulich zu behandeln. Aus diesem Grund sollten derartige Daten, wie z. B. Arztbriefe, Atteste, Krankenhausentlassungsberichte und ähnliche Unterlagen mit medizinischen Daten nicht in die Leistungsakte aufgenommen werden. Falls dies ausnahmsweise doch erforderlich ist, sind sie in einem verschlossenen Umschlag in der Akte aufzubewahren.

In dieser Hinsicht haben wir bei der Aktenprüfung gravierende Mängel festgestellt. Nur teilweise wurden Arztbriefe über stationäre Aufenthalte der Betroffenen in einem verschlossenen Umschlag aufbewahrt. So ließ sich einem Vorgang beispielsweise entnehmen, dass sich der Betroffene stationär in einer Entzugssuchtklinik aufhielt. Noch problematischer erscheint die unverschlossene Aufbewahrung von Unterlagen im Zusammenhang mit der Durchführung einer Psychotherapie. So fanden wir beispielsweise eine zwischen einer Betroffenen und ihrem behandelnden Arzt abgeschlossene Anti-Suizidvereinbarung.

In einem Fall gab der Leistungsempfänger selbst bekannt, an welcher Erkrankung er leidet, um die Zustimmung zum Umzug in eine andere Wohnung zu erreichen. Auch wenn die Betroffenen Gesundheitsdaten preisgeben, sollten derartige Informationen verschlossen aufbewahrt, soweit wie möglich geschwärzt, ggf. an den Amtsarzt weitergeleitet oder an die Betroffenen zurückgereicht werden. Stets ist zu klären, ob die Information im Detail überhaupt leistungsrelevant ist.

- Mutterpass

In einem Vorgang speicherte das Jobcenter die Kopie des Mutterpasses. Dieser Ablichtung waren sowohl der voraussichtliche Entbindungstermin als auch die bei der Vorsorgeuntersuchung erhobenen Befunde zu entnehmen. Gleichzeitig waren die Blutgruppe der Betroffenen und die Ergebnisse der Laboruntersuchungen erkennbar. Dies sind Informationen, die für die Feststellung der Leistung dem Grunde und der Höhe nach nicht relevant sind. Im Allgemeinen sollte ein Vermerk über den voraussichtlichen Entbindungster-

min ausreichend sein. Wird dies als nicht ausreichend angesehen, so ist der Schwangeren entweder die Möglichkeit einzuräumen, ein ärztliches Attest vorzulegen, oder die weiteren Gesundheitsdaten müssen auf der Kopie geschwärzt werden.

- Arbeitsunfähigkeitsbescheinigungen

Die Arbeitsunfähigkeitsbescheinigungen sind nicht zur Leistungsakte zu nehmen. Lediglich in Fällen von Zweifeln an der Arbeitsunfähigkeit dürfen sie in einem verschlossenen Umschlag im Vorgang abgelegt werden.

- Mehrbedarf für kostenaufwendige Ernährung

Nach § 21 Abs. 5 SGB II besteht kein pauschaler Anspruch auf einen krankheitsbedingten Mehrbedarf. Vielmehr setzt ein Anspruch nach dieser Vorschrift voraus, dass der Betroffene konkret einer kostenaufwendigen Ernährung aus medizinischen Gründen bedarf und sich hieraus auch ein konkreter Mehrbedarf ergibt. Zur Angemessenheit des Mehrbedarfs können die hierzu vom Deutschen Verein für öffentliche und private Fürsorge e. V. entwickelten und an typisierbaren Fallgestaltungen ausgerichteten Empfehlungen herangezogen werden. In der Regel bescheinigt der behandelnde Arzt im Ankreuzverfahren, auf welche Erkrankungsgruppe sich der Mehrbedarf gründet. Diese Verfahrensweise ist datenschutzgerecht. Die Jobcenter, die noch nicht so verfahren, haben wir zur Änderung aufgefordert.

3.1.3.3 Eingliederungsvereinbarung

In einer Eingliederungsvereinbarung zwischen dem Jobcenter und dem Leistungsempfänger werden unter anderem konkrete Eingliederungsbemühungen des Leistungsempfängers festgelegt sowie die Nachweise, die für deren Erfüllung beizubringen sind. Eine Verletzung dieser Pflichten aus der Eingliederungsvereinbarung kann vom Jobcenter sanktioniert werden. Darauf wird der Leistungsempfänger ausdrücklich hingewiesen. Aus datenschutzrechtlicher Sicht unzulässig ist es, in der Eingliederungsvereinbarung die Angabe von personenbezogenen Daten, die außerhalb der Eingliederungsvereinbarung nur freiwillig erhoben werden dürfen, zu verlangen. So darf beispielsweise die Freiwilligkeit der Angabe der privaten Telefonnummer nicht durch gegenteilige Regelungen in der Eingliederungsvereinbarung unterlaufen werden. Bei dem Abschluss der Eingliederungsvereinbarung sind die Vorschriften nach § 37 Satz 3 SGB I zu beachten.

3.1.3.4 Kontaktaufnahme mit Dritten und Datenübermittlung an unzuständige Dritte

Auch für die Datenübermittlung gilt der Grundsatz, dass sie nur zulässig ist, wenn eine gesetzliche Befugnis vorliegt oder der Betroffene in die Übermittlung eingewilligt hat. Im Bereich des Sozialleistungsrechts ergeben sich diese Befugnisse entweder aus den §§ 67 d ff. SGB X oder aus den bereichsspezifischen Datenverarbeitungs- und Datenschutzregelungen der einzelnen Sozialleistungsbereiche. Daneben ist gem. § 67 d i. V. m. § 67 b Abs. 1 SGB X eine Datenübermittlung auch dann zulässig, wenn sie auf eine wirksame Einwilligungserklärung des Betroffenen gestützt wird. Für die Zulässigkeit der Übermittlung im Einzelfall trägt die übermittelnde Stelle die Verantwortung. Sie muss also prüfen, ob die Übermittlung tatsächlich von einer einschlägigen gesetzlichen Befugnis oder einer wirksamen Einwilligung gedeckt ist.

In einigen der von uns geprüften Fälle bestanden ernsthafte Zweifel an der Zulässigkeit der Datenübermittlung. So kontaktierte etwa ein Jobcenter die zuständige Bank, um die Möglichkeit einer Kündigung des Bausparvertrages für das Kind der Leistungsempfänger zu besprechen. In einem weiteren Fall beantragte ein Leistungsempfänger die Übernahme der Kosten für einige Haushaltsgegenstände und reichte dafür Kostenvoranschläge von verschiedenen Herstellern ein. Hier nahm das Jobcenter Kontakt mit dem Anbieter auf. Damit wurde der Sozialleistungsbezug der Betroffenen sowohl der Bank als auch dem Hersteller bekannt. Eine Rechtsgrundlage für eine derartige Datenübermittlung war nicht ersichtlich.

3.1.3.5 Dokumentation von Hausbesuchen

Die meisten Jobcenter haben Dienstanweisungen für die Durchführung von Hausbesuchen herausgegeben. Datenschutzrechtlich waren diese nicht zu beanstanden. Lediglich in einzelnen Punkten waren die Vorschriften zu ergänzen. Dies betraf etwa die Frage, wann die erhobenen Daten vom Außendienst zu löschen sind. Nach § 84 Abs. 2 Satz 2 SGB X sind Sozialdaten zu löschen, wenn ihre Kenntnis für die verantwortliche Stelle zur rechtmäßigen Erfüllung der in ihrer Zuständigkeit liegenden Aufgaben nicht mehr erforderlich ist und kein Grund zu der Annahme besteht, dass durch die Löschung schutzwürdige Interessen des Betroffenen beeinträchtigt werden. Das bedeutet, dass die Daten nach Abschluss der Ermittlungstätigkeiten durch den Außendienst und der Übermittlung der Ergebnisse an den Auftraggeber zu löschen sind. Lediglich für bereits feststehende Nachermittlungen besteht eine weitere Speicherbefugnis. Die in den Dienstanweisungen festgelegten Verfahrensweisen und Anforderungen zur Dokumentation wurden in den geprüften Fällen eingehalten.

Auch die Aktenführung im Sozialleistungsbereich muss sich nach dem Grundsatz der Datensparsamkeit richten. Häufig reicht es aus, zu vermerken, dass Unterlagen vorlagen, statt sie in Kopie zur Akte zu nehmen. Gesundheitsdaten müssen auf ein Mindestmaß reduziert und in verschlossenen Umschlägen aufbewahrt werden. Auch ist darauf zu achten, dass Angaben immer zuerst bei dem Betroffenen selbst zu erfragen sind, bevor Dritte einbezogen werden.

3.2 Ergänzende Angaben zum Wohngeldantrag

Das Wohngeld ist ein staatlicher Zuschuss zu den Wohnkosten. Die Höhe des Wohngelds ist von verschiedenen Faktoren abhängig, z. B. dem Einkommen, der Anzahl der Familienmitglieder in der Wohnung und der Miete. Welche Daten darf die Verwaltung erheben, um entsprechende Ansprüche zu prüfen?

Wer Wohngeld beantragt, hat im Rahmen des Wohngeldgesetzes und der §§ 60 bis 65 Erstes Buch Sozialgesetzbuch Mitwirkungspflichten, die darauf zielen, der zuständigen Wohngeldstelle alle Tatsachen anzugeben, die für die zu gewährende Leistung erheblich sind. Die Datenerhebung erfolgt mittels eines Vordrucks „Antrag auf Wohngeld (Mietzuschuss).“ Darin haben die Antragsteller u. a. ihre und die Einkünfte der zu ihrem Haushalt gehörenden Personen detailliert anzugeben und durch entsprechende Nachweise zu belegen. Was zu den Einnahmen gehört, ist in den Hinweisen zum Ausfüllen des Vordrucks beispielhaft beschrieben.

Ein Betroffener informierte die Landesbeauftragte über die Verwendung eines weiteren Fragebogens „Ergänzende Angaben zum Wohngeldantrag; Erklärung über persönliche und sachliche Verhältnisse gem. Ziffer 15.01 WoGVwV zum § 15 Abs. 1 des Wohngeldgesetzes“ durch eine Stadtverwaltung. Mit diesem wurde abgefragt, welche Beträge die Antragsteller und die zum Haushalt gehörenden Personen durchschnittlich im Monat für die Bestreitung des Lebensunterhaltes u. a. für Kosmetika, Körperpflege, Kleidung und Hobbys aufwenden. Die Antragsteller sollten mit ihrer Unterschrift versichern, dass ihre Angaben der Wahrheit entsprechen und dass sie darüber informiert wurden, dass falsche oder unvollständige Angaben zur Rücknahme des Wohngeldbescheides und zur Rückforderung des bereits gezahlten Wohngeldes führen können. Auch der Hinweis auf die Möglichkeit eines Verfahrens wegen Betruges nach § 263 Strafgesetzbuch fehlte nicht in dem Vordruck. Der Fragebogen sollte im Einzelfall dazu dienen, bei einem deutlichen Missverhältnis zwischen Einnahmen und Ausgaben durch Angabe weiterer Tatsachen, Erläuterungen und ggf. Nachweise die Glaubhaftigkeit der Angaben im Wohngeldantrag besser einschätzen zu können.

Im Wohngeldgesetz ist jedoch konkret geregelt, welche Daten zur Entscheidung über einen Wohngeldantrag erhoben werden dürfen. Der Nachweis täglicher oder monatlicher Ausgaben gehört keinesfalls dazu. Die Formulierungen des Vordruckes und das gewählte Verfahren suggerierten zudem eine Verpflichtung der Antragsteller, diese Angaben zu machen, die eben nicht im Rahmen der gesetzlichen Mitwirkungspflichten erforderlich sind.

Die beschriebene Datenerhebung ist unzulässig, es sei denn, sie erfolgt mit freiwilliger und ausdrücklicher Zustimmung (Einwilligung) des Betroffenen gem. § 67 b Zehntes Buch Sozialgesetzbuch.

Eine Einwilligung kommt zwar in den Bereichen in Betracht, die keiner Regelung durch Rechtsvorschriften unterliegen. Im vorliegenden Fall ist eine Regelung im Wohngeldgesetz vorhanden, welche Daten zur Entscheidung über einen Wohngeldantrag erhoben werden dürfen. Angesichts der Kopplung von Pflichtangaben zur Leistungsbewilligung mit weiteren Angaben, kann der Eindruck entstehen, dass die Leistung nur bei Beantwortung der Fragen erfolgt. Von einer wirklichen Freiwilligkeit ist unter diesen Umständen nicht auszugehen. Eine Datenerhebung aufgrund einer freiwillig erteilten Einwilligung scheidet daher aus.

Im Ergebnis unserer Prüfung hat das zuständige Ministerium alle Wohngeldbehörden angeschrieben und für die Zukunft die weitere Verwendung solcher zusätzlichen Fragebögen im Rahmen der Plausibilitätsprüfung untersagt.

Im Wohngeldgesetz ist konkret geregelt, welche Daten zur Entscheidung über einen Wohngeldantrag erhoben werden dürfen. Eine darüber hinausgehende Erhebung und Verarbeitung von Daten wie z. B. über tägliche oder monatliche Ausgaben für persönliche Zwecke sieht das Gesetz nicht vor.

4 Banken- und Inkassowesen

4.1 Wann darf ein Zahlungsverzug einer Auskunftei gemeldet werden?

Ein Telekommunikationsunternehmen hatte ein Inkassobüro mit der Beitreibung ausstehender Forderungen beauftragt. Mehrfach meldete dieses der Schufa daraufhin vermeintlich zahlungsunwillige Kunden, obwohl diese zuvor die Rechtmäßigkeit der Forderung bestritten hatten. Mängel bei der Vertragserfüllung und daraus resultierende Reklamationen hatten die Kunden veranlasst, die Zahlungen zu verweigern. In einem Fall hatte sogar ein Betrüger die Identität des Kunden, der schließlich die Rechnung für den unter falschem Namen abgeschlossenen Mobilfunkvertrag erhielt, missbraucht. Die Schufa erteilte aufgrund der Meldungen negative Bonitätsauskünfte über die betroffenen Kunden. Dies hatte beispielsweise zur Folge, dass deren Kreditkarten gesperrt oder ihnen Abschlüsse von Verträgen verweigert wurden.

Die Kunden hatten die Rechtmäßigkeit der Forderungen zum Zeitpunkt der Übergabe an das Inkassobüro bereits bestritten. In seinem Schreiben informierte das Inkassobüro die Kunden über seine Beauftragung und forderte sie zur Zahlung auf. Es unterrichtete die Kunden außerdem pauschal darüber, dass eine Meldung an die Schufa erfolgt, „sofern der Betroffene die Forderung nicht bestritten hat und die gesetzlichen Voraussetzungen gegeben sind“. Diese Mitteilung ließ nicht nur die Tatsache außer Acht, dass die Kunden bereits gegenüber dem Telekommunikationsunternehmen widersprochen hatten, sondern war auch ansonsten zu allgemein. Zwar besteht nach § 28 a Abs. 1 Nr. 5 Bundesdatenschutzgesetz die Möglichkeit der Meldung an eine Auskunftei, wenn ein Vertragsverhältnis wegen Zahlungsrückständen fristlos gekündigt werden kann und die verantwortliche Stelle den Betroffenen über die bevorstehende Übermittlung unterrichtet hat. Die Information muss dabei aber mindestens folgende Angaben enthalten:

- Hinweis auf die Entscheidung und Absicht zur Übermittlung,
- Bezeichnung der Daten, die übermittelt werden sollen,
- Benennung des konkreten Empfängers der übermittelten Informationen (Auskunftei),
- Darlegung, auf welche konkrete Forderung sich die Übermittlung bezieht,
- beabsichtigter Zeitpunkt der Übermittlung.

Die o. g. Mindestangaben gewährleisten die erforderliche Transparenz und informieren den Kunden über das Auslaufen der Handlungsoption zum Begleichen der Forderung. Ein bloßer Hinweis auf die Allgemeinen Geschäftsbedingungen, auf denen der Vertrag mit dem Telekommunikationsunternehmen basiert sowie der Verweis auf einen möglichen Schufa-Eintrag, genügen nicht.

So fehlten in den Inkassoschreiben die Bezeichnung der zu übermittelnden Daten sowie der genauen Forderung und ein konkretes Datum für die drohende Übermittlung an die Schufa.

In dem beschriebenen Betrugsfall hatte der Kunde bestritten, überhaupt einen Vertrag mit dem Telekommunikationsunternehmen abgeschlossen zu haben. Diese wichtige Information hatte das Inkassounternehmen jedoch verspätet erhalten. Zu diesem Zeitpunkt konnte der Sachverhalt aus organisatorischen Gründen vor der Meldung an die Schufa nicht mehr berücksichtigt werden. Erst im Ergebnis einer Überprüfung der Beschwerde des Kunden hat der externe betriebliche Datenschutzbeauftragte des Telekommunikationsunternehmens den Betrug aufgedeckt. Das Inkassobüro hat in diesem und auch in den übrigen Fällen umgehend veranlasst, dass die Einträge bei der Schufa gelöscht werden.

Die Landesbeauftragte hat das Inkassobüro aufgefordert, die Formulierungen in dem ersten Schreiben zur Zahlungsaufforderung in datenschutzgerechter Weise zu konkretisieren. Die Eingaben an uns haben durch das schnelle und kompetente Eingreifen der betrieblichen Datenschutzbeauftragten des Inkassounternehmens auch dazu geführt, eine neue Schnittstelle zwischen dem Telekommunikationsunternehmen und dem Inkassobüro zu schaffen, um Forderungen besonders zu kennzeichnen. Zukünftig sollen nur noch titulierte Forderungen bei der Schufa eingemeldet werden.

Wird ein Vertragsverhältnis wegen Zahlungsrückständen fristlos gekündigt, ist eine Meldung des Sachverhalts an eine Auskunftei nur zulässig, wenn der Kunde zuvor hinreichend konkret und aussagekräftig hierüber informiert wurde.

4.2 Kontostandanzeige bei Geldautomaten

Kunden einer Sparkasse störten sich daran, dass bei der Geldabhebung am Automaten der aktuelle Kontostand für kurze Zeit auf dem Bildschirm erscheint. Er war gegebenenfalls auch für andere Anwesende lesbar. Die Kunden vermissten eine Wahlmöglichkeit, über die Kontostandanzeige während des Auszahlvorganges frei entscheiden zu können.

Die Sparkasse vertritt die Auffassung, dass die Anzeige ihrer Geldausgabeautomaten hinreichend vor dem Einblick Dritter geschützt sei. Da die Monitore schräg in die Wand eingelassen sind, werde die Einsehbarkeit aus der zweiten Reihe erheblich erschwert. Die durch die Schrägung entstehenden seitlichen Begrenzungen der Monitore, die Laibung und Einfassung in der Wand als bauliche Maßnahmen böten einen ausreichenden Sichtschutz. Schließlich stelle der Kunde, der weiß, dass der Kontostand angezeigt werde, selbst einen ausreichenden Sichtschutz nach hinten dar. Er könne darüber hinaus den Kontostand ausreichend vor Blicken schützen, indem er seine Hand auf die Stelle des Monitors legt, an der der Kontostand erscheint. Dies sei ihm auch zuzumuten, da er aufgrund des Erfordernisses, seine PIN verdeckt einzugeben, ohnehin sensibilisiert sei. Die Sparkasse betrachtet die Anzeige des Kontostandes als Serviceleistung und möchte an ihr festhalten.

Nach unserer Auffassung ist die Möglichkeit, den Monitor abzudecken, unvollkommen. Es sind viele Situationen denkbar, in denen der Kunde aufgrund der Position des Geldausgabeautomaten diesen nicht so abdecken kann, dass Unbefugte keine Einsicht nehmen können. Wir haben deshalb gegenüber der Sparkasse gefordert, das Auswahlmenü um eine Funktion für die Anzeige des Kontostandes nach der Geldabhebung zu erweitern. Alternativ könnte generell die Anzeigefunktion abgeschaltet werden.

Eine solche zentrale Abschaltung lehnt die Sparkasse mit dem Argument ab, dass ihre Kunden diese Serviceleistung großflächig angenommen hätten und nur in Brandenburg Probleme aufgetreten seien. Sie weist ferner die von uns vorgeschlagenen Maßnahmen (z. B. Sichtschutzblenden, Schutzfolien) zurück, da sie meint, mit den o. g. Vorkehrungen den Anforderungen des § 9 Bundesdatenschutzgesetz ausreichend gerecht zu werden.

Zur Lösung des Problems mit den bestehenden Geldautomaten befinden wir uns mit der Sparkasse noch im Gespräch. Wir haben außerdem vorgeschlagen, bei der Planung neuer Automaten zu überlegen, Monitore zukünftig datenschutzgerechter zu positionieren. Darauf ist die Sparkasse bisher jedoch nicht eingegangen.

Der Kontostand sollte beim Geldauszahlen am Automaten nur angezeigt werden, wenn der Kunde eine entsprechende Auswahl getroffen hat. Im Übrigen sind die Sparkassen verpflichtet, durch einen ausreichenden Sichtschutz sicherzustellen, dass Unbeteiligte die Anzeige nicht einsehen können.

5 Beschäftigtendatenschutz

5.1 Betriebliches Eingliederungsmanagement – Teilnahme einer Vertrauensperson aus dem privaten Umfeld?

Eine Dienststelle des Landes Brandenburg war sich unsicher, ob sie dem Wunsch des Betroffenen Rechnung tragen darf, eine Vertrauensperson aus seinem privaten Umfeld für die Durchführung des Betrieblichen Eingliederungsmanagements hinzuzuziehen.

Arbeitgeber (ebenso Dienstherren) sind nach § 84 Abs. 2 Neuntes Buch Sozialgesetzbuch zur Durchführung des Betrieblichen Eingliederungsmanagements (BEM) verpflichtet, sobald ein Arbeitnehmer (oder Beamter) innerhalb eines Jahres länger als sechs Wochen ununterbrochen oder wiederholt arbeitsunfähig ist. Bei der Durchführung dieses Verfahrens hat der Arbeitgeber bzw. der mit der Durchführung des Verfahrens betraute BEM-Beauftragte ein Höchstmaß an Vertraulichkeit bei der Verarbeitung personenbezogener Daten des Betroffenen zu gewährleisten.

Die an uns gerichtete Anfrage zielte nicht, wie sonst üblich, auf den Schutz personenbezogener Daten des BEM-Betroffenen ab. Vielmehr hatte der Arbeitgeber Sorge, dass einer hinzugezogenen Vertrauensperson dienstliche Belange (auch Daten anderer Kollegen) bekannt werden könnten.

Ein Betroffener hat immer das Recht, im Rahmen der Durchführung des BEM-Verfahrens eine Vertrauensperson zu benennen. Im angefragten Fall schlug die Dienststelle hierfür ein Mitglied des Personalrats, den Betriebsarzt, einen Vertreter der Arbeitssicherheit, die Gleichstellungsbeauftragte, einen Vertreter der Krankenkasse oder der Rentenversicherung vor. Der Betroffene lehnte den vorgenannten Personenkreis ab und wünschte die Hinzuziehung einer ihm bekannten Privatperson, die in keinem Verhältnis zum Arbeitgeber stand und auch sonst keiner Verschwiegenheitspflicht unterlag. Der Arbeitgeber hatte in Anbetracht dieses Vorschlags und unter Berücksichtigung der im BEM-Gespräch zu erörternden möglichen Eingliederungsmaßnahmen, die dienstliche Belange (auch die anderer Kollegen) berühren könnten, Sorge, mit der Einbeziehung der gewünschten Privatperson gegen den Datenschutz zu verstoßen.

Wir haben den Arbeitgeber dahingehend beraten, dem Wunsch des Betroffenen Rechnung zu tragen. Dem lagen folgende Überlegungen zugrunde:

- Es ist einem BEM-Betroffenen immer erlaubt, eine Person seines Vertrauens hinzuzuziehen. Dies kann ein Kollege oder eine Person aus dem privaten Umfeld sein.

- Ein Datenschutzproblem besteht deshalb nicht, weil bei einem Gespräch in Gegenwart einer Person des Vertrauens immer die gleichen datenschutzrechtlichen Maßstäbe zugrunde zu legen sind, wie für ein Gespräch mit dem Betroffenen allein.

- Der mit der Durchführung des Verfahrens betraute BEM-Beauftragte darf im Gespräch zu keiner Zeit Personalaktendaten oder gar BEM-Daten eines Kollegen offenbaren.

- Das BEM-Gespräch behandelt einzig und allein den Fall des Betroffenen. Der Betroffene entscheidet, was er selbst offenbaren möchte und setzt damit den BEM-Beauftragten und die Person des Vertrauens freiwillig über seine Situation in Kenntnis.

- Soweit Eingliederungsmaßnahmen als Konsequenz des BEM-Gesprächs abzuleiten sind und diese unmittelbar oder mittelbar andere Kollegen betreffen (etwa Änderungen der Arbeitsorganisation), sollten diese nicht bereits im BEM-Gespräch personenbezogen besprochen werden.

Arbeitnehmer dürfen als Vertrauensperson auch solche aus ihrem privaten Umfeld hinzuziehen. Der Arbeitgeber bzw. BEM-Beauftragte muss allerdings dieselben datenschutzrechtlichen Maßstäbe zugrunde legen wie für ein Gespräch mit dem Betroffenen allein.

5.2 Betriebliches Eingliederungsmanagement – unerlaubte Datenübermittlung

Ein Bediensteter einer Fachhochschule beschwerte sich darüber, dass personenbezogene Daten aus seinem Verfahren zum Betrieblichen Eingliederungsmanagement (BEM-Verfahren) nach § 84 Abs. 2 Neuntes Buch Sozialgesetzbuch unerlaubt an nicht am Verfahren beteiligte Dritte übermittelt wurden.

Der Arbeitgeber hatte einem Langzeiterkrankten ein BEM-Verfahren angeboten, welches dieser im Vertrauen auf die Einhaltung der auch in der Dienstvereinbarung geregelten datenschutzrechtlichen Vorgaben annahm. In einem Gespräch informierte der Betroffene die Leiterin des BEM-Teams u. a. über sein zurzeit ruhendes Mobbingverfahren, welches nicht im Rahmen des BEM-Verfahrens geführt wurde. Er willigte ein, dass die BEM-Teamleiterin die Dienststellenleitung kontaktiert, um das Mobbingverfahren wieder aufzunehmen. Er übersandte ihr per E-Mail seine Aufzeichnungen und Unterlagen, die das Mobbing belegen würden (Mobbingtagebuch), zur Kenntnis und Bearbeitung. Daraufhin sah sich die Empfängerin der Unterlagen veranlasst, diese,

ohne die weitere Einwilligung des Betroffenen einzuholen, sofort an die Leiterin der Personalabteilung weiterzuleiten. Letztere wiederum stellte die Unterlagen sodann der Dienststellenleitung zur Verfügung. Die BEM-Team-Leiterin glaubte, mit der Übermittlung in seinem Sinne gehandelt zu haben, der Petent jedoch fühlte sich in seinem Recht auf informationelle Selbstbestimmung verletzt.

Die Landesbeauftragte hat nach Prüfung der Sach- und Rechtslage festgestellt, dass die Datenübermittlung aus dem BEM-Verfahren des Betroffenen wegen des Verstoßes gegen § 29 Abs. 1 Brandenburgisches Datenschutzgesetz (BbgDSG) rechtswidrig war. Diesen Verstoß hat sie auf der Grundlage von § 25 Abs. 1 BbgDSG beanstandet.

Nach § 4 Abs. 1 BbgDSG dürfen personenbezogene Daten nur mit freiwilliger und ausdrücklicher Zustimmung (Einwilligung) des Betroffenen oder aufgrund einer Rechtsvorschrift verarbeitet werden. Die Übermittlung der personenbezogenen Daten des Petenten im Mobbingtagebuch konnte weder auf eine Einwilligung gestützt werden, noch erlaubte eine Rechtsvorschrift die Datenverarbeitung.

Eine ausdrückliche Einwilligung zur Weiterleitung des Mobbingtagebuchs an die Dienststelle zu Zwecken der Prüfung der Wiederaufnahme des Mobbingverfahrens lag seitens des Betroffenen nicht vor. Es war lediglich schriftlich dokumentiert, dass eine Kontaktaufnahme der BEM-Team-Leiterin mit der Dienststellenleitung erfolgen sollte mit dem Ziel, dass das Mobbingverfahren wieder aufgenommen wird. Diese Willenserklärung ist eindeutig und impliziert nicht, dass Dokumente, die das BEM-Team im BEM-Verfahren vom Betroffenen erhält, ohne dessen ausdrückliches Einverständnis an nicht am Verfahren Beteiligte übermittelt werden dürfen.

Auch aus der E-Mail, die der Petent zusammen mit seinen Mobbingunterlagen an die BEM-Team-Leiterin sandte, war keine Einwilligung für eine Weiterleitung des Tagebuchs ersichtlich. Er schrieb: „… anbei … zur Kenntnis für Ihre Bearbeitung.“ Eine Datenverarbeitung darf die BEM-Team-Leiterin aber nur für das BEM-Verfahren vornehmen, etwa um festzustellen, dass sie die Aufnahme des Mobbingverfahrens für (dringend) geboten hält. Nur dieses Ergebnis hätte sie letztlich der Dienststellenleitung gegenüber kommunizieren dürfen.

Die Datenübermittlung entbehrte auch einer entsprechenden Erlaubnisnorm. Da der Petent das Mobbingtagebuch in das BEM-Verfahren eingebracht hatte, handelte es sich um Personaldaten, für deren Übermittlung in Ermangelung einer entsprechenden Vorschrift im Landesbeamtengesetz (im Gegensatz zu Personalaktendaten) § 29 Abs. 1 BbgDSG Anwendung findet. Danach dürfen Personaldaten u. a. dann übermittelt werden, wenn eine

Dienstvereinbarung dies erlaubt. Die Fachhochschule hatte mit dem Personalrat eine Dienstvereinbarung zum Betrieblichen Eingliederungsmanagement abgeschlossen. Diese regelt neben der Verschwiegenheitspflicht der Mitglieder des BEM-Teams explizit den vertraulichen Umgang mit erlangten Informationen. Übermittlungsbefugnisse an Nichtverfahrensbeteiligte stützen sich nach der Dienstvereinbarung ausschließlich auf die vorherige Zustimmung des Betroffenen.

Die Beanstandung wurde anerkannt und die Dienstvereinbarung deutlicher gefasst, um Missverständnissen vorzubeugen.

Die mit einem BEM-Verfahren Beauftragten müssen vor einer Datenübermittlung aus dem Verfahren genauestens prüfen, ob die Betroffenen der jeweiligen Übermittlung zugestimmt haben oder ob eine Rechtsgrundlage diese erlaubt. Mutmaßliche Einwilligungen sind hier absolut fehl am Platz.

5.3 Akteneinsicht von Gemeindevertretern in Disziplinarvorgänge

Begehrt ein Gemeindevertreter Akteneinsicht in den Disziplinarvorgang des Hauptverwaltungsbeamten, muss die Disziplinarbehörde als Akten führende Stelle sorgfältig prüfen, ob sie tatsächlich Einsicht gewähren darf.

Die Gemeindevertretung ist Dienstvorgesetzte und oberste Dienstbehörde eines Hauptverwaltungsbeamten. Leitet allerdings die Rechtsaufsichtsbehörde gegen den Hauptverwaltungsbeamten ein Disziplinarverfahren ein, muss der Dienstvorgesetzte, also die Gemeindevertretung, über die Einleitung des Disziplinarverfahrens, die Erhebung einer Disziplinarklage sowie Einstellungs- und Disziplinarverfügungen informiert werden. Diese Mitteilungspflicht besteht bereits kraft Gesetzes nach § 89 Abs. 2 Landesdisziplinargesetz (LDG). Nach dieser Vorschrift muss die Disziplinarbehörde der Gemeindevertretung auf deren Antrag auch Auskünfte zum Verfahrensstand erteilen, wenn dies ohne Gefährdung der Sachverhaltsaufklärung möglich ist.

Die Gemeindevertretung erhält damit bereits wesentliche Informationen über das Disziplinarverfahren des Hauptverwaltungsbeamten. Dennoch kann es vorkommen, dass den Gemeindevertretern die Mitteilungen nicht genügen. Für diesen Fall sieht § 30 Abs. 2 LDG weitere Rechte der Dienstvorgesetzten auf Akteneinsicht in die Disziplinarunterlagen vor. Wünscht ein Gemeindevertreter Einsicht in den Disziplinarvorgang, muss er einen Beschluss der Gemeindevertretung, die als Dienstvorgesetzte des Hauptverwaltungsbeamten nur als Organ handeln kann und als solches die Akteneinsicht beantragen muss, herbeiführen. Dieser Beschluss muss auch die Namen der jeweiligen

Gemeindevertreter enthalten, die Akteneinsicht für die Gemeindevertretung wahrnehmen. Aus dem Beschluss der Gemeindevertretung muss zudem hervorgehen, weshalb eine Akteneinsicht aus besonderen dienstlichen Gründen erforderlich ist.

Dem einzelnen Gemeindevertreter darf ohne Beschluss der Gemeindevertretung keine Akteneinsicht in Disziplinarvorgänge gewährt werden. Die Notwendigkeit für die Akteneinsicht muss substantiiert begründet werden.

5.4 Entgeltabrechnungen und Arbeitgeberbescheinigungen online

Eine Beschäftigte informierte uns, dass ihr Arbeitgeber die monatlichen Entgeltabrechnungen nur noch in elektronischer Form über ein Online-Mitarbeiterportal zum Abrufen und Ausdrucken bereitstellt. Gleiches sollte für Bescheinigungen zur Vorlage beim Finanzamt und der Sozialversicherung gelten. Da am Arbeitsplatz unserer Petentin jedoch kein Drucker verfügbar war, verwies der Arbeitgeber sie darauf, Drucker am Arbeitsplatz der Vorgesetzten bzw. an öffentlich zugänglichen PCs im Foyer des Unternehmens zu nutzen.

Arbeitgeber sind gem. § 108 Abs. 1 Gewerbeordnung verpflichtet, Arbeitnehmern bei Zahlung des Arbeitsentgelts eine Abrechnung in Textform zu erteilen. Ob hierfür die Papierform mit postalischer Übermittlung oder die elektronische Form per Online-Abruf oder per E-Mail-Versand genutzt wird, kann der Arbeitgeber selbst festlegen. Er ist bei der elektronischen Variante allerdings verpflichtet, die Anforderungen des Bundes- bzw. Landesdatenschutzgesetzes insbesondere zur Wahrung der Vertraulichkeit und Integrität der Daten einzuhalten. Durch die Umsetzung technischer und organisatorischer Maßnahmen ist zu gewährleisten, dass die personenbezogenen Daten der Entgeltabrechnung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können. Gleiches gilt für andere Bescheinigungen, die der Arbeitgeber Arbeitnehmern z. B. zur Vorlage bei Finanz- oder Sozialbehörden ausstellt.

Im konkreten Fall hatte das Unternehmen bereits eine Reihe von Maßnahmen realisiert, die den Zugriff Unbefugter auf Entgeltabrechnungen und andere Dokumente, die über das Mitarbeiterportal bereitgestellt werden, verhindern sollten: die Datenübertragung wurde verschlüsselt, der Abruf erst durch Eingabe eines starken Passworts möglich und der Benutzer nach einer gewissen Zeit der Inaktivität beim Portal automatisch abgemeldet. Der Vorschlag, den Ausdruck der Abrechnungen oder Bescheinigungen unbeaufsichtigt und auf einem räumlich vom Arbeitsplatz entfernten Drucker (z. B. bei Vorgesetzten) durchzuführen, war jedoch untauglich, da so nicht ausge-

schlossen werden konnte, dass Dritte sensitive personenbezogene Daten der Beschäftigten zur Kenntnis nehmen. Dies ließe sich z. B. durch eine sogenannte Follow-Me-Funktion am Drucker verhindern, bei der der eigentliche Druck erst dann erfolgt, wenn der Beschäftigte am Gerät steht und dort eine personengebundene PIN oder Chipkarte zum Start des Druckvorgangs eingibt.

Auch die Nutzung von PCs und Druckern in öffentlich zugänglichen Bereichen des Unternehmens verbietet sich für die genannten Zwecke, da diese missbräuchlich verwendet werden können, wenn nicht entsprechende Vorkehrungen getroffen werden. Die Möglichkeiten für Angreifer reichen von der Einschleusung von Schadsoftware oder -hardware (z. B. Keylogger zur Protokollierung von Tastatureingaben) bis hin zur Anbringung von Miniaturkameras im Raum, die Bildschirminhalte fotografieren. Stattdessen wäre die Bereitstellung von Selbstbedienungsterminals, die in nicht öffentlich zugänglichen Bereichen des Unternehmens aufgestellt werden und unter administrativer Kontrolle der IT-Abteilung stehen, eine Alternative.

Da das Unternehmen bereits in ausgewählten Abteilungen Drucker mit Follow-Me-Funktion einsetzte, sagte es zu, die Beschäftigten auf die Nutzung dieser Geräte zum Druck der Entgeltabrechnungen oder Arbeitgeberbescheinigungen zu verweisen. Parallel sollte geprüft werden, bei Ersatzbeschaffungen von Druckern und Multifunktionsgeräten diese Funktion verbindlich vorzuschreiben. Weiterhin zog das Unternehmen auch die Installation von Selbstbedienungsterminals in nicht öffentlich zugänglichen Bereichen in Erwägung.

Bei der Überprüfung der Verschlüsselungslösung für die elektronische Übertragung der Beschäftigtendaten aus dem Mitarbeiterportal stellten wir fest, dass das verwendete Zertifikat, mit dem sich der Server des Unternehmens gegenüber einem Client-PC ausweist, Schwächen aufwies. Diese führten zu einer Warnung, die in ähnlicher Form auch bei Angriffen auf die Verschlüsselung auftreten würde und Unsicherheiten bei den Beschäftigten hätte hervorrufen können: Sie mussten die Kenntnisnahme der Warnung explizit bestätigen, um weiter zum Abruf der Entgeltabrechnungen oder der Arbeitgeberbescheinigungen zu gelangen. Das Unternehmen sagte eine Änderung der Serverkonfiguration zu.

Ergänzend forderten wir, dass der Fingerabdruck zur Prüfung der Korrektheit des Zertifikats auf mehreren verschiedenen Informationskanälen an die Beschäftigten weiterzugeben ist. So kann verhindert werden, dass Dritte durch Manipulieren der elektronischen Kommunikation sowohl das Zertifikat selbst als auch dessen Fingerabdruck verändern und verschlüsselte Inhalte anschließend im Klartext zur Kenntnis nehmen können. Das Unternehmen sagte zu, diese Forderung zu erfüllen.

Entgeltabrechnungen und Arbeitgeberbescheinigungen z. B. zur Vorlage bei Finanz- oder Sozialbehörden enthalten sensitive Daten von Beschäftigten. Stellt der Arbeitgeber die Dokumente nur in elektronischer Form zur Verfügung, muss er durch geeignete und angemessene technische und organisatorische Maßnahmen ausschließen, dass die Daten Dritten zur Kenntnis gelangen.

6 Finanzen

Amtshilfeersuchen von Finanzämtern an Jobcenter

Regelmäßig erfragte ein Finanzamt bei einem Jobcenter, ob Steuerpflichtige von dort Überbrückungsgeld, Arbeitslosengeld oder sonstige Leistungen beziehen. Falls dem so war, sollte das Jobcenter zusätzlich die Höhe der Leistung sowie die Stammnummer des Empfängers angeben.

Das Finanzamt stützte sich auf die Amtshilfevorschriften der §§ 111 ff. Abgabenordnung i. V. m. der gesetzlichen Mitteilungspflicht des § 71 Abs. 1 Nr. 3 Zehntes Buch Sozialgesetzbuch. Danach ist das Jobcenter verpflichtet, die Angaben zu übermitteln, sofern die Auskunft zur Sicherung des Steueraufkommens benötigt wird und die Datenerhebung beim Jobcenter erforderlich ist, d. h. kein bei gleicher Eignung milderes Instrument zur Sachverhaltsermittlung zur Verfügung steht. Als solches ist vor allem die Erhebung unmittelbar beim Betroffenen selbst zu betrachten (Ersterhebungsgrundsatz). Erst wenn eine Aufklärung des Sachverhalts auf diese Weise nicht möglich ist, kann sich das Finanzamt mit einem Amtshilfeersuchen an das Jobcenter wenden. Das Finanzamt muss also nicht nur in jedem Einzelfall die Erforderlichkeit des Ersuchens prüfen, sondern stets auch die Frage klären, ob die Datenerhebung beim Betroffenen nicht zum Erfolg geführt hat oder ausnahmsweise nicht angezeigt war.

Die Landesbeauftragte hat zunächst die Auffassung vertreten, dass das Finanzamt dem Jobcenter im Falle eines Auskunftsersuchens stets das Ergebnis dieser Prüfung, also die tragenden Gründe für das Ersuchen, mitteilen muss. Dazu gehört unter anderem die Beschreibung der bisher durchgeführten Ermittlungsmaßnahmen sowie eine Darlegung der Art und Höhe der in Rede stehenden Steuerrückstände.

Das gleichzeitig von uns um eine Stellungnahme gebetene Ministerium der Finanzen vertrat hingegen die Auffassung, dass es genüge, wenn das Jobcenter im Rahmen eines Amtshilfeersuchens lediglich in die Lage versetzt

wird, die eigene Verpflichtung zur Datenübermittlung nachvollziehen zu können. Es forderte das Finanzamt auf, regelmäßig ergänzend darauf hinzuweisen, dass eine Datenerhebung beim Steuerpflichtigen nicht erfolgreich oder ggf. nicht angezeigt war. Eine detaillierte Begründung in dem oben beschriebenen Sinne hielt das Ministerium jedoch für überflüssig, erklärte aber, die Mitarbeiter der Finanzverwaltung dahingehend zu sensibilisieren, Amtshilfeersuchen nicht lediglich aus Gründen der „Bequemlichkeit“ unreflektiert sowie zur Arbeitsvereinfachung durchzuführen oder weil die Daten bei der ersuchten Behörde schneller zu ermitteln sind.

Vor diesem Hintergrund und angesichts des Gebots der Datensparsamkeit hielten wir im Ergebnis die Beschränkung auf einen Hinweis im Amtshilfeersuchen, aus dem die Erfolglosigkeit der versuchten Datenerhebung beim Steuerpflichtigen hervorgeht, für ausreichend.

Ein Jobcenter muss sich darauf verlassen können, dass es zur Übermittlung von Daten der Leistungsempfänger erst dann in Anspruch genommen wird, wenn die Finanzämter mit der Erhebung beim Betroffenen keinen Erfolg hatten. Auf das Scheitern einer solchen Ersterhebung müssen die Finanzämter beim Amtshilfeersuchen nachvollziehbar hinweisen und dies vor allem aktenkundig festhalten.

7 Gesundheit

7.1 Krebsregister – Daten für Forschung und Behandlung

Im Berichtszeitraum hatte sich die Landesbeauftragte mit datenschutzrechtlichen Fragen zu zwei unterschiedlichen Krebsregistern zu befassen, und zwar mit dem bereits bestehenden epidemiologischen Gemeinsamen Krebsregister Berlins und der neuen Länder sowie mit dem im Aufbau befindlichen klinischen Krebsregister der Länder Berlin und Brandenburg.

7.1.1 Meldedaten für das Gemeinsame Krebsregister der neuen Länder

Das Gemeinsame Krebsregister der Länder Berlin, Brandenburg, Mecklenburg-Vorpommern, Sachsen-Anhalt und der Freistaaten Sachsen und Thüringen basiert auf einem Staatsvertrag der beteiligten Länder aus dem Jahre 1999. Im Anschluss an einen bundesweiten Aufbau von epidemiologischen Krebsregistern wurde damit die Fortführung des Nationalen Krebsregisters der DDR auf eine landesgesetzliche Grundlage gestellt. Zweck des Gemeinsamen Krebsregisters ist die Verbesserung der Datengrundlage für die Krebsepidemiologie. Es soll vornehmlich anonymisierte Daten für die Wis-

senschaft liefern, das Auftreten und die Trendentwicklung aller Formen von Krebserkrankungen beobachten und statistische Daten für die Gesundheitsplanung und Ursachenforschung bereitstellen. Das Register nimmt die Meldungen der Ärzte und Zahnärzte über Krebserkrankungen entgegen. Außerdem haben alle Gesundheitsämter die Pflicht, dem epidemiologischen Krebsregister die Kopien aller Leichenschauscheine bzw. die entsprechenden Daten elektronisch zu übermitteln. Das Gemeinsame Krebsregister hat seinen Sitz in Berlin und wird als nachgeordnete Einrichtung (nichtrechtsfähige Anstalt des öffentlichen Rechts) bei der Senatsverwaltung für Gesundheit und Soziales Berlin geführt.

Mitte März 2015 informierte uns der Berliner Beauftragte für Datenschutz und Informationsfreiheit, der für die datenschutzrechtliche Kontrolle des Gemeinsamen Krebsregisters verantwortlich ist, über einen Referentenentwurf zur Änderung des Staatsvertrags. Dieser sah vor, dass im Rahmen des Abgleichs der dem Register bereits vorliegenden Identitätsdaten mit dem Melderegister eine halbjährliche Übermittlung von Meldedaten jeweils für das gesamte zurückliegende Kalenderjahr erfolgen sollte. Eine solche Regelung hätte bedeutet, dass die Daten stets mehrfach hätten übermittelt werden müssen. Dies haben wir kritisiert. Auch das Ministerium des Innern und für Kommunales forderte eine überschneidungsfreie Lieferung von Meldedaten.

Die von uns bemängelte Mehrfachübermittlung von Meldedaten an das Gemeinsame Krebsregister unterbleibt nunmehr. Allerdings mussten wir eine Verlängerung der maximalen Frist zur Aufbewahrung dieser Daten beim Register auf 12 Monate akzeptieren. Grund hierfür ist ein für uns nachvollziehbarer, großer Zeitaufwand für den Abgleich der Daten.

Es ist zudem mit Übergangsschwierigkeiten aufgrund umfangreicher Umstrukturierungen zu rechnen: So ist vorgesehen, die Meldungen über Krebserkrankungen künftig über das neu einzurichtende klinische Krebsregister für Berlin und Brandenburg zu beziehen. Außerdem sind die für die Lieferung der Meldedaten zuständigen zentralen Stellen der Länder anzubinden. Wegen dieser neuen Übermittlungswege müssen auch im Gemeinsamen Krebsregister erst die entsprechenden technisch-organisatorischen Maßnahmen etabliert werden. Auch hier sind Übergangsschwierigkeiten abzusehen. Daher haben die Datenschutzbehörden für eine längere Übergangszeit notgedrungen Löschfristen von maximal zwei Jahren akzeptiert.

7.1.2 Errichtung eines klinischen Krebsregisters für Berlin und Brandenburg

Im Frühjahr des Jahres 2013 wurde im Fünften Buch Sozialgesetzbuch (SGB V) auf Grundlage des Krebsfrüherkennungs- und -registergesetzes ein neuer § 65 c eingefügt. Diese Vorschrift enthält die Verpflichtung für die

Länder, klinische Krebsregister einzuführen. Zweck dieser Register ist es, die Qualität der onkologischen Versorgung, also der konkreten Krebsbehandlung, zu verbessern. Hierzu werden Informationen über Krankheitsfälle und Therapien detailliert und über einen längeren Zeitraum gesammelt, verglichen und systematisch ausgewertet. Die Resultate sollen Eingang in aktuelle und zukünftige Behandlungen von Erkrankten finden und deren individuelle Betreuung optimieren. Berlin und Brandenburg wollen hierzu durch einen Staatsvertrag die notwendigen rechtlichen Grundlagen für ein länderübergreifendes klinisches Krebsregister schaffen. Es soll seinen Sitz in Brandenburg erhalten. Der Entwurf dieser Vereinbarung wird derzeit unter unserer Beteiligung erarbeitet; zugleich wird die Vorbereitung der Errichtung des Registers begleitet.

Das Register sollte nach unserer Vorstellung in streng voneinander getrennte Bereiche zur personenbezogenen Erfassung der Patienten- und Behandlungsdaten (Versorgungsbereich) bzw. zur Auswertung der Daten und Rückmeldung der Ergebnisse sowie zum Datenaustausch mit anderen Stellen (Auswertungsbereich) aufgeteilt werden. Die Auswertung hat sich mit pseudonymisierten Angaben zu den Patienten zu begnügen und außerdem diejenigen Aufgaben nach § 65 c SGB V zu erfüllen, für die personenbezogene Daten nicht erforderlich sind.

Es ist vorgesehen, Meldungen über Krebserkrankungen künftig nur noch über das klinische Krebsregister für Berlin und Brandenburg und nicht mehr, wie bisher, direkt an das zu Forschungszwecken eingerichtete Gemeinsame Krebsregister zu richten. Das schon bisher in Brandenburg bestehende Widerspruchsrecht der Patienten gegen diese Meldung ist im Rahmen der Umstellung aus unserer Sicht beizubehalten. Auch gegen die Meldung an das klinische Krebsregister soll ein Widerspruchsrecht für die Betroffenen bestehen. Um dieses Recht sicherzustellen, aber auch, um dem Register eine Größenvorstellung davon zu geben, wie viele Fälle aus diesem Grund nicht gemeldet werden, wird beim klinischen Krebsregister künftig eine Liste der Widersprechenden geführt werden.

Außerdem setzen wir uns für das Auskunftsrecht der Betroffenen ein: Die Auskunft sollen Patienten nunmehr – anders als beim Gemeinsamen Krebsregister – auch unabhängig von einer Vermittlung durch Mediziner erhalten können.

7.2 Akteneinsicht in medizinische Unterlagen contra Urheberrecht

Ein naher Angehöriger eines im Krankenhaus verstorbenen Patienten erbat von dieser Einrichtung unter anderem den Verlegungsbrief der zuvor behandelnden Klinik in Kopie. Während in die übrige Akte Einsicht gewährt wurde, wurde die Herausgabe der Kopie des Verlegungsbriefes der anderen Klinik mit dem Argument verweigert, dass dem Urheberrechte der anderen Stelle entgegenstünden.

Nach unserer Auffassung steht dem Angehörigen ein Akteneinsichtsrecht auch in das Schreiben der anderen Klinik zu.

Das Urhebergesetz schützt persönliche geistige Schöpfungen (Werke) der Literatur, Wissenschaft und Kunst. Die letzten drei Begriffe sind zwar weit auszulegen, dennoch kann die Krankenbehandlung nicht unter den Wissenschaftsbegriff gefasst werden. Dem Ersteller des Verlegungsbriefes ging es darum, im Interesse des Patienten der anderen Klinik wesentliche Gesundheitsdaten für die Anschlussbehandlung zur Verfügung zu stellen. Würde ein Arzt sein Schreiben an einen weiterbehandelnden Kollegen urheberrechtlich schützen wollen, so würde er damit ggf. in Datenschutzrechte des Patienten eingreifen, der ein Recht auf Auskunft darüber hat, welche Informationen der Empfänger über ihn speichert (§ 34 Abs. 1 Nr. 1 Bundesdatenschutzgesetz). Auch wird das Schriftstück ja gerade erstellt, weil ein Interesse an einer Nutzung der Angaben durch weitere Behandler oder Einrichtungen besteht. Würde der Urheberrechtsschutz greifen, dürfte die empfangende Klinik selbst die Angaben in dem Verlegungsbrief ggf. gar nicht verwenden.

Nach § 630 g Bürgerliches Gesetzbuch (BGB) hat der Patient grundsätzlich das Recht, die ihn betreffende Patientenakte einzusehen. Zu dieser gehört auch der darin aufgenommene Verlegungsbrief. Die Vorschrift unterscheidet nicht nach selbst- oder fremderstellten Unterlagen in der Patientenakte, sondern spricht diese Dokumente als Ganzes an.

Im Falle des Todes des Patienten stehen seine Rechte zur Wahrnehmung vermögensrechtlicher Interessen (z. B. Klärung von Schadensersatzansprüchen) seinen Erben zu (§ 630 g Abs. 3 Satz 1 i. V. m. § 1922 Abs. 1 BGB). Die nächsten Angehörigen dürfen dann nach § 630 g Abs. 3 Satz 2 BGB sogar eigene immaterielle Interessen geltend machen. Lediglich der entgegenstehende Wille des Patienten kann die Rechte der Erben bzw. Angehörigen ausschließen. Ein solcher war hier nicht erkennbar.

Das Urheberrecht steht einer Akteneinsichtnahme in Dokumente einer Patientenakte, die von anderen Behandlern stammen, nicht entgegen.

7.3 Die App „AOK mobil vital“ – Gesundheitsdaten auf dem Smartphone

Mit der App „AOK mobil vital“ bietet die AOK Nordost ihren Versicherten eine Fitness-App an, mit der sportliche Aktivitäten und die gesunde Lebensweise der Teilnehmer gefördert werden sollen. Dazu werden auch persönliche Daten u. a. in Gesundheitsprofilen gespeichert und ausgewertet.

Mit der App werden über einen längeren Zeitraum verschiedenste Aktivitäten automatisiert aufgezeichnet oder manuell eingetragen und zu einer relativen Messgröße („health score“), die den Gesundheitszustand und das Fitnessniveau des Teilnehmers darstellt, ausgewertet. In die Berechnungen fließen auch verschiedene andere Daten der Lebensführung wie Ernährung, Rauchen, Alkoholkonsum, Stresssituationen und Schlafphasen ein. Die App verarbeitet damit auch sensitive, hoch schutzbedürftige personenbezogene Gesundheitsdaten.

Da immer mehr Krankenkassen großes Interesse am Einsatz derartiger Anwendungen zeigen, wollten wir am konkreten Beispiel die Vereinbarkeit dieser App mit dem geltenden Datenschutzrecht prüfen. Wir haben daraufhin die AOK Nordost aufgefordert, uns die Rechtmäßigkeit sowie die technische Umsetzung des Verfahrens darzulegen. Im Ergebnis können wir feststellen, dass mit „AOK mobil vital“ keine personenbezogene Daten zur Auswertung oder Speicherung an die AOK Nordost fließen. Diese werden bei der Züricher Firma dacadoo ag, welche auch die App bereitstellt, in der Schweiz verarbeitet. Über eine Kooperationsvereinbarung zwischen der Krankenkasse und dem Unternehmen erhält die AOK Nordost lediglich regelmäßig statistische Auswertungen wie z. B. die Anzahl der angemeldeten Versicherten, die Gruppierung nach Altersklassen, die Bereiche der erzielten health-score-Werte und einen durchschnittlichen Gesundheitsindex.

Die Teilnahme des Versicherten ist freiwillig und erfolgt durch Abgabe einer schriftlichen Teilnahme- und Einwilligungserklärung (mit AOK-Logo) gegenüber der Firma dacadoo. Da die personenbezogenen Daten in der Schweiz verarbeitet werden, kommt nicht das deutsche Datenschutzrecht zur Anwendung, sondern das Schweizer Recht. Der Eidgenössische Datenschutz- und Öffentlichkeitsbeauftragte hat das Konzept von dacadoo geprüft. Wer die App nutzen möchte, sollte in jedem Fall die Allgemeinen Geschäftsbedingungen und die Datenschutzbestimmungen des Anbieters genau lesen. Sie sind mit der AOK Nordost abgestimmt und hinsichtlich z. B. der Gewährleistung von Vertraulichkeit im Zuge der Kooperationsvereinbarung verbindlich und dauerhaft festgelegt worden.

Obwohl im konkreten Fall keine datenschutzrechtlichen Bedenken gegen das Projekt der AOK Nordost bestehen, sollte jeder Versicherte im Vorfeld intensiv prüfen, ob er seine eigenen gesundheitsrelevanten Daten an Dritte weitergeben möchte.

Mit der App „AOK mobil vital“ verarbeitet die AOK Nordost keine personenbezogenen Gesundheitsdaten der teilnehmenden Nutzer. Sie erhält lediglich statistische Auswertungen und zusammengefasste Aussagen über deren Gesundheitszustand und des Fitnessniveau.

7.4 Auskunft Feuerwehrtauglichkeit – Rolle des Betriebsarztes

Durch eine Anfrage aus einer Kommune wurden wir darauf aufmerksam, dass die Durchbrechung der ärztlichen Schweigepflicht für den Betriebsarzt bei Tauglichkeitsprüfungen für hauptamtlich tätige Feuerwehrleute im laufenden Beschäftigungsverhältnis nicht gesetzlich geregelt ist.

In einem bundesweit vorgegebenen Formular der Deutschen Gesetzlichen Unfallversicherung kann der Betriebsarzt ankreuzen, ob dauernde, befristete oder keine gesundheitlichen Bedenken bestehen bzw. ob eine Tauglichkeit unter bestimmten Voraussetzungen bejaht wird. Für die beiden letzten Fälle ist ein Bemerkungsfeld vorgesehen. Darin hatte der Betriebsarzt im vorliegenden Fall das konkrete Problem notiert und eine Kopie an die Personalstelle gesandt.

Eine Einwilligungslösung bezüglich solcher Offenbarungen von Gesundheitsdaten durch die Betroffenen selbst oder den Betriebsarzt erscheint uns problematisch. Die Auskunftspflichten der Feuerwehrleute gegenüber dem Arbeitgeber stellen die Freiwilligkeit der Einverständniserklärung infrage. Eine Regelung in einem Gesetz halten wir für angemessen, da der Einsatz gesundheitlich nicht voll tauglicher Feuerwehrleute deren und anderer Leben und Gesundheit gefährden könnte.

Wir baten das Ministerium des Innern und für Kommunales sowie das Ministerium für Arbeit, Soziales, Gesundheit, Frauen und Familie um Stellungnahmen zu der Problematik. Letzteres sprach sich für eine Regelung im Landesrecht, z. B. im Brandenburgischen Brand- und Katastrophenschutzgesetz, aus. Ersteres geht davon aus, dass die Unfallverhütungsvorschriften „Feuerwehren“, die derzeit überarbeitet werden, die Problematik zukünftig regeln werden. Unfallverhütungsvorschriften dürfen durch die Unfallversicherungsträger aufgrund von § 15 Siebtes Buch Sozialgesetzbuch erlassen werden.

Wir unterstützen den Lösungsweg des Ministeriums für Arbeit, Soziales, Gesundheit, Frauen und Familie. Eine Rechtsgrundlage aus dem Siebten Buch Sozialgesetzbuch scheint uns bei arbeitsrechtlichen Tauglichkeitsprüfungen nicht in Betracht zu kommen.

Für die Mitteilung des Ergebnisses von Tauglichkeitsprüfungen bei Feuerwehrleuten im laufenden Beschäftigungsverhältnis an den Arbeitgeber bzw. Dienstherrn sollten landesrechtliche Regelungen geschaffen werden.

7.5 Kooperation bei der Verarbeitung notfallmedizinischer Daten

Zu Beginn des Jahres 2013 traten zwei Landkreise und eine kreisfreie Stadt, welche für alle drei Beteiligten eine Regionalleitstelle für den Brandschutz, Rettungsdienst und Katastrophenschutz betreibt, mit der Bitte an uns heran, ihre gemeinsame Ausschreibung von Tablet-PCs als Dokumentationsinstrumente zur elektronischen Erfassung relevanter notfallmedizinischer Daten zu begleiten.

Zunächst bestanden Überlegungen, die integrierte Leitstelle für alle Datenspeicherungen in diesem Zusammenhang zuständig zu machen und für die drei Kooperationspartner einen gemeinsamen Server zu nutzen. Ab dem Jahr 2016 sollen die Tablet-PCs in den Rettungswagen zum Einsatz kommen.

Die integrierten Leitstellen haben nach § 19 Abs. 3 Brandenburgisches Rettungsdienstgesetz die Befugnis, Einsatzanforderungen entgegenzunehmen und Einsatz- und Beförderungsaufträge weiterzugeben sowie bei Notrufen personenbezogene Daten im erforderlichen Umfang zu verarbeiten. Eine Verarbeitung der vom Notarzt dokumentierten Daten durch sie erscheint daher nach dem Gesetz allenfalls in geringem Umfang bzw. Ausnahmefällen erforderlich. Die Abrechnung des Rettungseinsatzes ist Sache des Trägers des Rettungsdienstes, die medizinische Versorgung der Patienten verantworten im Wesentlichen die Rettungswachen bzw. Notärzte. Den integrierten Leitstellen für all diese Datenspeicherungen insgesamt die Zuständigkeit zu übertragen, begegnete daher auch im Hinblick auf die Wahrung der ärztlichen Schweigepflicht Bedenken.

Für die von uns aus Rechtsgründen empfohlenen Datenverarbeitungen im Auftrag wiesen wir im Hinblick auf Patientendaten darauf hin, dass es – bei personenbezogener Verarbeitung – einer Befugnis zur Durchbrechung der ärztlichen Schweigepflicht bedarf. Deshalb war insoweit vorrangig eine Verwendung von anonymisierten oder verschlüsselten Daten durch einen Dienstleister anzustreben. Außerdem forderten wir, den Zugriff der Administratoren

auf die gespeicherten medizinischen Daten technisch auszuschließen sowie die Speicherung der Daten verschiedener Stellen voneinander abzuschotten. Dem wurde Rechnung getragen.

Weiter war uns wichtig, dass dann, wenn Daten mit hohem Schutzbedarf (z. B. medizinische Daten) auf dem mobilen Endgerät gespeichert werden, diese mit sicheren kryptographischen Verfahren zu verschlüsseln sind. Auch die zwischen den Mobilgeräten und dem Einsatzleitsystem übertragenen personenbezogenen Daten sind gleichermaßen zu schützen. Der in der Regel innerhalb eines IT-Sicherheitskonzeptes dokumentierte Nachweis, dass die Gefahren, die von dem Verfahren für die Rechte und Freiheiten der Betroffenen ausgehen, beherrscht werden, wurde bisher noch nicht vollständig erbracht.

Die Möglichkeit der Zusammenarbeit von Kommunen in einer gemeinsamen Rettungsleitstelle bedeutet nicht zwingend, dass datenschutzrechtliche Verantwortlichkeiten aufgegeben werden: Die patientenbezogenen Daten der an der Kooperation im Rettungsdienst Beteiligten müssen getrennt verarbeitet und aufgrund des hohen Schutzbedarfs der Daten verschlüsselt gespeichert und übertragen werden.

8 Informationstechnik in der Landesverwaltung

8.1 Strategie weiter unklar

Schon in unseren beiden letzten Tätigkeitsberichten[28] kritisierten wir die fehlende Weiterentwicklung der IT-Strategie der Landesverwaltung. Wir hatten exemplarisch verschiedene Bereiche benannt, für die Entscheidungen ausstehen und darauf hingewiesen, dass Versäumnisse sich auch negativ auf die Gewährleistung von Datenschutz und Informationssicherheit auswirken können. Gleiches gilt für die längst überfällige Fortschreibung der E-Government-Strategie des Landes. Was hat sich im Berichtszeitraum in dieser Hinsicht getan?

Die obige Leerstelle im Text ist kein Versehen. Aktivitäten zur inhaltlichen Abstimmung oder gar Ergebnisse bei der Weiterentwicklung der IT- oder der E-Government-Strategie in der Landesverwaltung sind uns im Berichtszeitraum leider nicht bekannt geworden, auch wenn das Ministerium des Innern und für Kommunales auf eine Kleine Anfrage im Landtag antwortet, dass es diese Strategien derzeit neu entwickelt.[29] Unsere Kritik halten wir deshalb auch nach nunmehr sechs Jahren aufrecht.

[28] Tätigkeitsbericht 2012/2013, B 7.1 sowie Tätigkeitsbericht 2010/2011, A 10.1

[29] Landtags-Drucksache 6/2009 vom 13. Juli 2015

8.2 Informationssicherheitsmanagement in der Landesverwaltung

Seit 2008 gibt es in der Landesverwaltung mit dem Informationssicherheitsmanagementteam ein Gremium, das der ressortübergreifenden Koordinierung und Verbesserung des Informationssicherheitsmanagements in den Landesbehörden dient. Es besteht aus den IT-Sicherheitsbeauftragten der Ressorts und dem IT-Sicherheitsmanager des Landes. Der Brandenburgische IT-Dienstleister und unsere Behörde wirken beratend mit.

Die Einführung, Aufrechterhaltung und stetige Verbesserung von Prozessen zur Gewährleistung der Informationssicherheit ist für jede Behörde und jedes Unternehmen von grundlegender Bedeutung. Informationen sind mit geeigneten und dem Schutzbedarf angemessenen Maßnahmen davor zu schützen, dass sie z. B. durch Unbefugte zur Kenntnis genommen, verändert oder gelöscht werden. Sicherheitsvorfälle können Auswirkungen auf Geschäftsabläufe in Unternehmen oder die Aufgabenerfüllung von Behörden haben und ggf. auch mit erheblichen Kosten oder Ansehensverlusten verbunden sein. Die Gewährleistung der Informationssicherheit ist immer als Prozess zu sehen, da Sicherheitsmaßnahmen regelmäßig an geänderte Bedrohungslagen und die Weiterentwicklung des Standes der Technik anzupassen sind.

Gerade in großen, verteilten Organisationen mit dezentralen Entscheidungsstrukturen (wie der öffentlichen Verwaltung eines Landes) kommt der übergreifenden Koordinierung des Informationssicherheitsmanagements besonderes Gewicht zu. Es bedarf einer ganzheitlichen Betrachtungsweise, der Abstimmung von Zielen und Maßnahmen, der Planung von Ressourcen, der abgestimmten Erfolgskontrolle sowie der Einbeziehung aller Mitarbeiter, um einen einheitlichen und ausreichend hohen Schutz gegen mögliche Angriffe für die Gesamtorganisation zu etablieren und aufrecht zu erhalten. Denn letztlich kann bereits eine kleine Sicherheitslücke ausreichen, um die Datenverarbeitung insgesamt nachhaltig zu beeinträchtigen.

Vor diesem Hintergrund hat das Informationssicherheitsmanagementteam der Landesverwaltung seine Tätigkeit im Berichtszeitraum planmäßig fortgesetzt.[30] Ergebnisse sind z. B. die Fortschreibung der Informationssicherheitsleitlinie für die Landesverwaltung, um sie an die Regelungen der „Leitlinie für die Informationssicherheit in der öffentlichen Verwaltung“ des IT-Planungsrates anzupassen, sowie Zuarbeiten für die IT-Standards des Landes mit verbindlichen Vorgaben für die Ministerien und ihre nachgeordneten Bereiche in Bezug auf die Informationssicherheit.

[30] Tätigkeitsbericht 2012/2013, B 7.2

Darüber hinaus wurden unter Einbeziehung unserer Vorschläge weitere landesweite Sicherheitsrichtlinien inhaltlich erarbeitet und abgestimmt sowie die Umsetzung bereits verabschiedeter Richtlinien geplant. Hier sind insbesondere die Richtlinie zur Mandantentrennung und Virtualisierung bei Verfahren, die der Brandenburgische IT-Dienstleister im Auftrag betreibt, die Richtlinie für die Fernwartung von Arbeitsplatz-PCs in den Ressorts durch den Dienstleister und die Richtlinie zum Einsatz dienstlicher mobiler Endgeräte[31] zu nennen. Regelmäßiger Tagesordnungspunkt der Beratungen ist auch die Berichterstattung über die Tätigkeit des CERT Brandenburg (Computer Emergency Response Team), das Sicherheitsvorfälle analysiert, präventive und reaktive Maßnahmen empfiehlt, einen Warn- und Informationsdienst betreibt und in engem Austausch mit den CERTs des Bundes und der anderen Länder agiert.

Bei der Arbeit des Informationssicherheitsmanagementteams der Landesverwaltung spielt der Brandenburgische IT-Dienstleister (ZIT-BB) stets eine herausragende Rolle. Er gibt wesentliche inhaltliche Impulse, erarbeitet Vorschläge für technische Lösungen und plant bzw. koordiniert die Umsetzung von abgestimmten Sicherheitsmaßnahmen. Dies ist auch deshalb nicht verwunderlich, da der ZIT-BB als Auftragnehmer eine Vielzahl von Verfahren auf seiner technischen Infrastruktur betreibt, allgemeine IT-Dienste für die gesamte Landesverwaltung erbringt (wie z. B. das Landesverwaltungsnetz, Spam- und Virenfilter, Firewalls) und eine große Zahl von Benutzerarbeitsplätzen in den Ministerien und ihren nachgeordneten Bereichen technisch betreut.

Festzustellen ist allerdings auch, dass die konzeptionellen Arbeiten des ZIT-BB im Bereich der Informationssicherheit nur auf wenige Schultern verteilt sind. Das zuständige Dezernat ist neben dem bereits Genannten weiterhin u. a. für das CERT Brandenburg, für die Beratung von Kunden des ZIT-BB bei der Erstellung sowie Fortschreibung von Sicherheitskonzepten sowie für die zentrale Plattform zur elektronischen Pflege dieser Konzepte in der Landesverwaltung verantwortlich. Darüber hinaus koordiniert es das interne Informationssicherheitsmanagement im ZIT-BB selbst. Die starke Auslastung der Mitarbeiter führte im Berichtszeitraum mitunter zur Verzögerung von Zuarbeiten, Abstimmungsrunden oder Umsetzungsplanungen, da andere Aktivitäten Priorität hatten. Die personelle Stärkung dieses Dezernats würde nicht nur der Bedeutung des Informationssicherheitsmanagements im ZIT-BB und in der Landesverwaltung insgesamt besser gerecht werden. Sie könnte auch zu einer Intensivierung und Beschleunigung der konzeptionellen Arbeiten führen.

[31] siehe B 8.4

Die Koordinierung von Prozessen des Informationssicherheitsmanagements ist für die Landesverwaltung von großer Bedeutung. Nur auf diese Weise kann ein einheitlicher und hoher Standard beim Schutz der Datenverarbeitung gegen mögliche Angriffe – gerade in Bezug auf die Verarbeitung personenbezogener Daten – erreicht werden. Vor dem Hintergrund der rasant zunehmenden Gefährdungen, der Abhängigkeit der Landesverwaltung von einer sicheren und ordnungsgemäßen Datenverarbeitung sowie der Komplexität und Kompliziertheit der vom ZIT-BB zu betreuenden Verfahren regen wir an, das für Informationssicherheit zuständige Dezernat des Dienstleisters personell zu stärken.

8.3 Unverschlüsselte E-Mails mit sensitiven Daten im Landesverwaltungsnetz

Ein Mitarbeiter einer öffentlichen Stelle, die an das Landesverwaltungsnetz angebunden ist, informierte uns, dass er wiederholt E-Mails mit zum Teil sensitiven personenbezogenen Daten von verschiedenen Landesbehörden erhielt. Es stellte sich heraus, dass es sich dabei um fehlerhaft adressierte Nachrichten handelte.

Die Übertragung von sensitiven personenbezogenen Daten in Weitverkehrsnetzen (z. B. Landesverwaltungsnetz) ist mit erheblichen Risiken verbunden. Es müssen technische und organisatorische Maßnahmen realisiert werden, die den Schutz dieser Daten sicherstellen. Kryptographische Verfahren (z. B. symmetrische und asymmetrische Verschlüsselung, digitale Signatur) sind besonders geeignet, um Verletzungen des Datenschutzes beim Transport schutzwürdiger elektronisch gespeicherter Daten zu verhindern. Mit ihrer Hilfe lassen sich Manipulationen und Übertragungsfehler nachweisen und die unberechtigte Kenntnisnahme verhindern. Derartige Verfahren sind heute Stand der Technik und können mit vertretbarem Aufwand eingesetzt werden. Werden E-Mails mit sensitiven personenbezogenen Daten im Landesverwaltungsnetz übertragen, dann ist von den jeweiligen Daten verarbeitenden Stellen sicherzustellen, dass die Daten mit einer Ende-zu-Ende-Verschlüsselung gesichert werden. Ist dies nicht möglich, so sind die Mitarbeiter darauf hinzuweisen, dass in diesen Fällen eine elektronische Kommunikation nicht erfolgen darf. In einer Dienstanweisung zum Umgang mit E-Mails sollte genau festgelegt werden, welche personenbezogenen Daten mit welchem Schutzbedarf wie übertragen werden dürfen.

Die fehlerhafte Adressierung der E-Mails lag im konkreten Fall einerseits an einer mangelhaften Konfiguration des zentralen Outlook-Adressbuchs, welche vom Brandenburgischen IT-Dienstleister umgehend behoben wurde, und andererseits an der Unachtsamkeit der Nutzer, die vor dem Absenden einer E-Mail keine Kontrolle der Empfängeradressen durchführten. Gerade bei

einem größeren Adressatenkreis sollten die Empfänger sorgfältig überprüft werden.

Sensitive personenbezogene Daten dürfen im Landesverwaltungsnetz nur Ende-zu-Ende verschlüsselt übertragen werden. Dabei sind kryptographische Verfahren nach dem Stand der Technik einzusetzen. Vor dem Versenden einer E-Mail ist die Empfängerliste auf Korrektheit zu überprüfen, um eine Fehladressierung zu verhindern.

8.4 Mobile Endgeräte in der Landesverwaltung

Die Nutzung mobiler Endgeräte wird auch in der Landesverwaltung immer wichtiger. Der Brandenburgische IT-Dienstleister (ZIT-BB) unterstützt daher eine Reihe von Modellen unter zentraler Administration. Zudem wurde eine zu den Sicherheitsrichtlinien der Landesverwaltung gehörende Richtlinie zum Umgang mit mobilen Endgeräten verabschiedet.

Der ZIT-BB hat aufgrund von Kundenanforderungen seine Aktivitäten zur Einführung und zum Betrieb mobiler Endgeräte ausgeweitet und unterstützt nun auch iPhones, iPads, Android-Smartphones und neue Blackberry-Geräte. Wir haben den ZIT-BB bei seinen Arbeiten datenschutzrechtlich beraten und dabei insbesondere folgende Aspekte betrachtet:

- Beurteilung des Schutzbedarfes der verarbeiteten personenbezogenen Daten,
- Erstellung eines aus einer Risikoanalyse entwickelten Sicherheitskonzeptes,
- Trennung eines geschäftlichen (geschützten) und privaten (ungeschützten) Bereichs auf Smartphones und Tablets,
- zentrale Administration der Geräte durch den ZIT-BB,
- Erarbeitung einer Richtlinie zum Einsatz der mobilen Endgeräte.

Grundsätzlich gilt für Informationssicherheitskonzepte, dass sie einen ganzheitlichen Blick auf Verfahren, Prozesse und Infrastruktur werfen müssen, in die die zu betrachtenden Komponenten eingebunden sind. Allerdings kann man bei der Einführung und dem Betrieb mobiler Endgeräte auch technische Einzelmaßnahmen identifizieren, deren Erfüllung für einen sicheren Betrieb unabdingbar ist. Dazu gehören die Implementierung einer Authentifizierung durch sichere Passwörter, die zügige Gerätesperrung bei Untätigkeit (sog. Security Timeout), die sichere Geräteverschlüsselung und eine verschlüssel-

te Verbindung zum Landesverwaltungsnetz. Auch die Erkennung von unberechtigten Ausweitungen von Zugriffsrechten auf den Mobilbetriebssystemen (Root-, Jailbreak-Erkennung) und eine Fernlöschung bei Verlust des Gerätes sind wichtige Maßnahmen, die umgesetzt werden müssen.

Eine besondere Schwierigkeit ergab sich bei der Umsetzung der Sicherheitsmaßnahmen insbesondere bei der Akzeptanz komplexer Passwörter in Verbindung mit kurzen Zeitspannen bis zur Sperrung des geschützten Bereichs auf dem Endgerät. Wie sich herausstellte, erkennen manche Geräte das Telefonieren nicht als Nutzung des Smartphones, sodass nach einem längeren Telefonat der geschäftliche Bereich schon wieder gesperrt ist und mit dem komplexen Passwort erneut entsperrt werden muss. Auf einer virtuellen Tastatur ist dies jedoch recht unbequem, sodass viele Nutzer eine Fristverlängerung für den ungesperrten Zustand des Gerätes forderten. Letztlich haben wir einer Sperrfrist von einer Viertelstunde zugestimmt, um einen Kompromiss zwischen Sicherheitsanforderungen und Nutzerakzeptanz zu finden. Eine aus Sicherheitssicht wünschenswerte Verkürzung dieser Frist würde Änderungen an der Betriebssystemsoftware durch den Hersteller voraussetzen: Die Zeitspanne bis zur Sperrung des geschützten Bereichs sollte erst nach Beendigung des Telefonats beginnen.

Die Abstimmung einer einheitlichen Richtlinie zur Nutzung mobiler Endgeräte zwischen den Ressorts und dem ZIT-BB war ebenfalls aufwendig. Es zeigte sich, dass die verantwortlichen Stellen, also die Behörden der Landesverwaltung, zum Teil sehr unterschiedliche Wünsche und Vorstellungen bezüglich der Nutzung mobiler Endgeräte hatten. Leider liefen diese allerdings oft den Sicherheitsanforderungen zuwider, sodass sich die Erstellung einer vollständigen und datenschutzrechtlich akzeptablen Richtlinie, die zugleich von allen Beteiligten mitgetragen wurde, als ein langwieriger Prozess erwies. Schwierig waren z. B. immer wieder auftauchende Wünsche nach der Einbindung privater Endgeräte zur dienstlichen Nutzung oder der Aufweichung der Passwortregelungen. Auch bei der Nutzung freier bzw. heimischer Funknetze (WLAN) für die Verarbeitung dienstlicher Daten trat ein Dissens zutage. Letztlich gelang eine Einigung, die Anforderungen der Informationssicherheit hinreichend berücksichtigt.

Die Einbindung mobiler Endgeräte zur Verarbeitung dienstlicher Daten erfordert eine stetige Weiterentwicklung der IT-Strategie und des Sicherheitskonzeptes des Landes. Hierbei müssen alle Akteure zusammenwirken und gegebenenfalls auch auf eigene Wünsche zugunsten von Informationssicherheit und Datenschutz verzichten.

8.5 Elektronische Identifizierung mittels Personalausweis – Aufbau einer eID-Infrastruktur für die Landesverwaltung

Der neue Personalausweis ermöglicht die elektronische Identifizierung und Authentisierung des Inhabers gegenüber Unternehmen und Verwaltung. Auch die Landesverwaltung Brandenburg ist bestrebt, diese sog. Online-Ausweisfunktion (oder eID-Funktion) bei der Erbringung von Verwaltungsdienstleistungen zu berücksichtigen. Im Berichtszeitraum startete ein entsprechendes Pilotprojekt. Weiterhin wurde ein Konzept zur Bereitstellung einer zentralen eID-Infrastruktur des Landes für die Nutzung der Online-Ausweisfunktion erarbeitet.

Das Landesamt für Soziales und Versorgung betreibt das Fachverfahren „Schwerbehindertenausweis-Online“, das Betroffenen ermöglicht, einen Schwerbehindertenausweis auf elektronischem Wege zu beantragen. Aufgrund der gesetzlich vorgeschriebenen Schriftform des Antrags konnte dieser bislang zwar online ausgefüllt werden, musste aber anschließend ausgedruckt, unterschrieben und auf dem Postweg beim Amt eingereicht werden. Zur Vereinfachung und für ein medienbruchfreies Antragsverfahren wurde nun geprüft, die eID-Funktion des neuen Personalausweises für das Verfahren zu nutzen. Gem. § 36 a Erstes Buch Sozialgesetzbuch kann nämlich die Schriftform eines Antrags durch die Abgabe einer Erklärung in einem von der Behörde über öffentlich zugängliche Netze bereitgestellten elektronischen Formular ersetzt werden, wenn gleichzeitig ein sicherer Identitätsnachweis (z. B. mit dem neuen Personalausweis) erfolgt.

Damit ein Unternehmen oder eine öffentliche Stelle die eID-Funktion nutzen und personenbezogene Daten des Inhabers aus dem Personalausweis auslesen kann, wird gem. § 21 Personalausweisgesetz ein sog. Berechtigungszertifikat benötigt. Dieses ist bei der Vergabestelle für Berechtigungszertifikate beim Bundesverwaltungsamt zu beantragen. Mit dem Antrag sind insbesondere die Kategorien der aus dem Personalausweis benötigten Daten, der konkrete Verwendungszweck sowie die Erforderlichkeit der Daten für diesen Zweck darzulegen. Weiterhin ist die Gewährleistung von Datenschutz und Datensicherheit schriftlich zu bestätigen und ggf. nachzuweisen. Das Berechtigungszertifikat ist damit stets gebunden an die beantragende Stelle, den Datenkatalog, den konkreten Verwendungszweck und das genutzte Verfahren.

Im Rahmen der Anwendung „Schwerbehindertenausweis-Online“ hat das Landesamt die erforderlichen Arbeiten für die Nutzung des neuen Personalausweises zur Identifizierung und Authentisierung der Antragsteller durchgeführt. Dabei wurden insbesondere die Schnittstellen zur Integration der eID-

Funktion implementiert und das Sicherheitskonzept entsprechend fortgeschrieben.

Parallel zum Pilotprojekt erarbeitete das Ministerium des Innern und für Kommunales ein allgemeines Konzept zur Nutzung der Online-Ausweisfunktion im Land Brandenburg und zur zentralen Bereitstellung einer eID-Infrastruktur. Danach war geplant, für die Landesverwaltung nur ein einziges Berechtigungszertifikat zu beschaffen. Der IT-Leitstelle im Ministerium sollte per Organisationsverfügung die Aufgabe des zentralen Identitätsmanagements für die gesamte Landesverwaltung übertragen werden. In dieser Funktion sollte sie als verantwortliche Daten verarbeitende Stelle die Personalausweisdaten von Bürgern in E-Government-Verfahren auslesen und an andere Stellen als Betreiber der jeweiligen Fachverfahren übermitteln.

Wir haben dem Ministerium bereits frühzeitig signalisiert, dass wir eine Organisationsverfügung nicht als tragfähige Rechtsgrundlage für die Erhebung und Übermittlung personenbezogener Daten ansehen. Vielmehr bedarf es hierzu nach unserer Auffassung einer gesetzlichen Regelung bzw. der informierten Einwilligung der Betroffenen im Einzelfall. Außerdem meldeten wir Zweifel an, ob den Anforderungen des Personalausweisgesetzes zur Erteilung von Berechtigungszertifikaten durch die Angabe eines sehr allgemeinen Verwendungszwecks der Ausweisdaten Rechnung getragen werden kann.

Neben den organisatorischen Überlegungen enthielt das vom Ministerium entwickelte Dokument auch eine technische Konzeption zum Aufbau und zum Betrieb einer zentralen eID-Infrastruktur für die Landesverwaltung. Diese war datenschutzrechtlich nicht zu beanstanden. Die Infrastruktur sollte vorrangig durch den Brandenburgischen IT-Dienstleister im Rahmen einer Datenverarbeitung im Auftrag gem. § 11 Brandenburgisches Datenschutzgesetz betrieben werden. Für den eigentlichen technischen Identifizierungsprozess (eID Service) sollten ein Unterauftragnehmer einbezogen werden. Allerdings stockte die Umsetzung der Pläne, sodass letztlich auch das von Landesamt verfolgte Pilotprojekt bis zum Ende des Berichtszeitraums den Produktivbetrieb nicht aufnehmen konnte.

Grundsätzlich ist der Einsatz der eID-Funktion oder anderer Varianten zur Ersetzung der Schriftform in E-Government-Diensten des Landes zu begrüßen. Allerdings bedarf die Zentralisierung von Aufgaben, insbesondere der Erhebung und Übermittlung von Personalausweisdaten, einer tragfähigen und klaren datenschutzrechtlichen Grundlage. Diese ist im Land noch zu schaffen.

9 Jugend und Familie

9.1 Der Kita-Planer – ein Anmeldesystem für Kitaplätze

Vermehrt bemühen sich kommunale Verwaltungen, die Anmeldungen für die Vergabe von Kitaplätzen über webbasierte Systeme zu optimieren. Sowohl von einer Stadtverwaltung als auch von betroffenen Eltern wurden wir um eine datenschutzrechtliche Bewertung gebeten.

Im konkreten Fall hatte eine Stadt mit einem Projekt zur zentralen Vergabe von Kitaplätzen sowohl der städtischen als auch der freien Träger begonnen. Für die Verarbeitung personenbezogener Daten bei einer zentralen Vermittlung von Kitaplätzen sahen wir allerdings keine gesetzliche Grundlage, sodass die Datenverarbeitung, insbesondere die Übermittlung, nur über eine Einwilligung der Sorgeberechtigten erfolgen konnte. Bei den für die zentrale Kitaplanung zu erhebenden Daten handelte es sich um Sozialdaten, die nach den Vorschriften der Sozialgesetzbücher zu verarbeiten sind. Eine Einwilligung war demnach nach den Vorgaben des § 67 b Abs. 2 Zehntes Buch Sozialgesetzbuch (SGB X) einzuholen.

Die Stadt beabsichtigte weiter, nach der zentralen Vermittlung der Kinder an die Tageseinrichtungen diesen die erhobenen Grunddaten zu übermitteln. Dies sollte durch die Vergabe von Zugriffsrechten im Anmelde- und Informationssystem erfolgen. Jede Tageseinrichtung hätte danach ihren eigenen Datenbestand und wäre damit Daten verarbeitende Stelle. Die Sorgeberechtigten mussten somit zur Datenverarbeitung mittels Vermittlungssoftware und zur Datenübermittlung (Stadt – Kita) jeweils separat einwilligen.

Ursprünglich hatte die Stadt den Plan, den technischen Betrieb des Verfahrens an den Hersteller der verwendeten Software zu übertragen. Dieser beabsichtigten Verarbeitung von Sozialdaten im Auftrag durch eine nicht öffentliche Stelle standen jedoch die strengen Vorgaben von § 80 Abs. 5 SGB X entgegen. Daraufhin entschied sich die Stadt, das Anmelde- und Informationssystem selbst zu betreiben. Sie agiert damit auch als Auftragnehmer für die sich beteiligenden Kitas und muss mit diesen eine Vereinbarung zur Verarbeitung von Sozialdaten im Auftrag gem. § 80 Abs. 2 SGB X abschließen.

Weiterhin machte die Stadt von der Möglichkeit des Server Housing Gebrauch, indem sie eigene Hardware in einem fremden Rechenzentrum unterstellte und sich mit einer Netzanbindung sowie weiteren Infrastrukturdiensten versorgen ließ. Hierbei handelt es sich nicht um eine Auftragsdatenverarbeitung. Voraussetzung ist allerdings, dass die Stadt den Betrieb des Verfahrens und die Administration des Servers mit eigenem Personal komplett übernimmt. Der Betreiber des Rechenzentrums darf keinen Zugriff auf die perso-

nenbezogenen Daten, die auf der untergebrachten Hardware liegen, erhalten. Dies gilt auch für das Erstellen und Aufbewahren von Sicherungskopien der Daten. Beides muss im Verantwortungsbereich der öffentlichen Stelle erfolgen. Die Stadt sagte dies zu.

Die Verarbeitung personenbezogener Daten bei einer zentralen Vermittlung von Kitaplätzen kann nur über eine Einwilligung der Sorgeberechtigten erfolgen. Die Beauftragung von nicht öffentlichen Stellen zum Betreiben der Plattform ist meist nicht mit den Vorschriften zum Sozialdatenschutz nach § 80 Abs. 5 SGB X vereinbar.

9.2 Jugendhilfe – Sozialdatenschutz und Strafverfolgung

Das Verhältnis von Sozialdatenschutz und Strafverfolgung ist ein immer wiederkehrendes Thema der Jugendhilfe, weil Jugendämter vermeintlich Strafprozesse verhindern. Aus diesem Grund hat die Landesbeauftragte zu einem Gespräch mit Vertretern der Generalstaatsanwaltschaft und der Staatsanwaltschaften sowie den Jugendamtsleitern eingeladen. Dieses diente der Erörterung der jeweiligen rechtlichen Regelungen, dem Erfahrungsaustausch und der Beratung über das zukünftige Vorgehen.

Damit Daten zwischen Jugendämtern und Strafverfolgungsbehörden ausgetauscht werden dürfen, bedarf es auf beiden Seiten einer entsprechenden Befugnis: einerseits zur Übermittlung und andererseits zur Erhebung dieser Daten („Zwei-Türen-Modell“). Die Jugendämter unterliegen dem Sozialgeheimnis und dürfen Sozialdaten nur mit Einwilligung des Betroffenen oder auf der Grundlage einer Übermittlungsbefugnis aus dem Sozialgesetzbuch an Polizei und Staatsanwaltschaft weitergeben (§ 35 Erstes Buch Sozialgesetzbuch – SGB I). Auch die Aussage eines Jugendamtsmitarbeiters als Zeuge im Ermittlungs- oder Strafverfahren setzt eine sozialrechtliche Übermittlungsbefugnis voraus. Insoweit finden die strafprozessualen Befugnisse der Ermittlungsbehörden aus der Strafprozessordnung (StPO) ihre Grenzen im Sozialdatenschutz.

Ohne entsprechende Einwilligung bzw. Rechtsgrundlage ist eine Datenübermittlung unzulässig. In diesem Fall besteht gemäß § 35 Abs. 3 SGB I auch keine Auskunftspflicht, Zeugnispflicht oder Pflicht zur Vorlegung oder Auslieferung von Sozialdaten, Schriftstücken und Dateien, auch nicht im Strafverfahren (sozialrechtliches Zeugnisverweigerungsrecht). Die Daten bzw. die Unterlagen sind sozusagen beschlagnahmefest. Die unbefugte Übermittlung von Sozialdaten stellt zudem eine Ordnungswidrigkeit nach § 85 Zehntes Buch Sozialgesetzbuch (SGB X) dar; möglicherweise ist auch eine Strafvorschrift verletzt (z. B. § 203 Strafgesetzbuch – StGB). Darüber hinaus kommen z. B. dienst- bzw. arbeitsrechtliche Folgen oder auch Schadensersatzansprü-

che nach § 82 SGB X in Betracht. Auch eine Aussagegenehmigung durch den Dienstherrn gem. § 54 StPO hilft hier letztlich nicht weiter, da sich diese nur auf öffentliche Geheimhaltungsinteressen beziehen kann, nicht jedoch auf amtlich bekannt gewordene Privatgeheimnisse.

Eine Übermittlungsbefugnis seitens des Jugendamtes besteht nur in wenigen Fällen:

So regelt § 68 SGB X die Übermittlung zur Erfüllung von Aufgaben der Polizeibehörden, der Staatsanwaltschaften und Gerichte, allerdings nur bezüglich spezifisch aufgelisteter Daten, wie Name, Vorname, Geburtsdatum, Geburtsort, Anschrift und Arbeitgeber des Betroffenen. Und auch diese Daten dürfen nur übermittelt werden, wenn kein Grund zur Annahme besteht, dass dadurch schutzwürdige Interessen des Betroffenen beeinträchtigt werden. Dies wird z. B. jedoch entsprechend einer Entscheidung des Bundesverwaltungsgerichts[32] grundsätzlich angenommen, wenn jemand dem Jugendamt Hinweise, z. B. bezüglich einer möglichen Kindeswohlgefährdung, gibt, sodass in diesem Fall eine Übermittlung auch, z. B. nur des Namens des Informanten, ohne dessen Einwilligung zu unterbleiben hat.[33]

Nach § 69 Abs. 1 Nr. 1 SGB X ist eine Übermittlung von Sozialdaten zur Erfüllung einer gesetzlichen Aufgabe des Jugendamtes zulässig. Allerdings ist die Strafverfolgung nicht Aufgabe des Jugendamtes; sie obliegt allein den Strafverfolgungsbehörden.

Eine Übermittlung käme nach § 69 Abs. 1 Nr. 2 SGB X in Betracht, wenn sie erforderlich ist zur Durchführung eines Straf- bzw. gerichtlichen Verfahrens. Dieses müsste jedoch mit der Erfüllung einer Aufgabe des Jugendamtes in einem sachlichen Zusammenhang stehen. Berührungspunkte allein oder ein örtlicher oder zeitlicher Zusammenhang mit der Tätigkeit des Jugendamtes reichen hierfür nicht.

Aber auch für den Fall, dass eine der dargestellten Übermittlungsbefugnisse greift, ergeben sich aufseiten des Jugendamtes aus dem Achten Buch Sozialgesetzbuch (SGB VIII) weitere Beschränkungen:

Beispielsweise ist die Datenübermittlung gemäß § 64 Abs. 2 SGB VIII nur zulässig, soweit dadurch der Erfolg einer zu gewährenden Leistung nicht infrage gestellt wird.

Auch unterliegen Sozialdaten, die einem Jugendamtsmitarbeiter zum Zwecke persönlicher und erzieherischer Hilfe anvertraut worden sind, einem besonde-

[32] Urteil des Bundesverwaltungsgerichts vom 4. September 2003, Az.: 5 C 48.02

[33] Tätigkeitsbericht 2010/2011, A 11.3

ren Vertrauensschutz. Eine Übermittlung kommt nur unter den engen Voraussetzungen des § 65 Abs. 1 SGB VIII in Betracht, also z. B. für familiengerichtliche Maßnahmen bei einer Kindeswohlgefährdung. Ausschlaggebend ist, ob aufgrund der persönlichen Betreuung und Beratung ein zu schützendes Vertrauensverhältnis besteht und die Daten dem Jugendamtsmitarbeiter in diesem Kontext bzw. in Erwartung einer besonderen Vertraulichkeit persönlich anvertraut wurden.

Im Hinblick auf diese Ausnahmeregelung zum Schutz des für die Aufgabenerfüllung im Einzelfall notwendigen besonderen Vertrauensverhältnisses zwischen einem Jugendamtsmitarbeiter und dem betroffenen Kind bzw. Jugendlichen ist nicht nachvollziehbar, dass in der Rechtsprechung § 65 Abs. 1 SGB VIII meist auch auf den Namen eines Hinweisgebers angewendet wird. Folgt man dieser Auffassung, wäre eine entsprechende Datenübermittlung so gut wie immer ausgeschlossen, und zwar auch bei einer richterlichen Anordnung nach § 73 SGB X. Sie käme auch nicht in Betracht, wenn das Jugendamt im Rahmen seiner Aufgabenerfüllung großes Interesse an einer Datenübermittlung hat oder in den Fällen, in denen Anhaltspunkte dafür vorliegen, dass der Informant leichtfertig falsche Informationen gegeben oder rufschädigend gehandelt hat. Im Ergebnis halten wir es unter Berücksichtigung und Abwägung der allseitigen Interessen für ausreichend, dass der Name eines Informanten nur dem einfachen Sozialdatenschutz und den dargelegten Grenzen einer Übermittlung unterliegt. Der besondere Vertrauensschutz sollte besonderen Konstellationen vorbehalten sein, z. B. bezüglich derjenigen, die die persönliche und erzieherische Hilfe für sich in Anspruch nehmen und als Ausgleich für die notwendige Offenheit darauf angewiesen sind.

Auch bei einer richterlichen Anordnung ist zu prüfen, in welchem Umfang eine Datenübermittlung erforderlich ist und ob sich Einschränkungen hinsichtlich der Übermittlungsbefugnis (z. B. aus § 65 SGB VIII) ergeben: So kann eine Datenübermittlung nur auf § 73 Abs. 1 SGB X gestützt werden bei dem Verdacht eines Verbrechens (mindestens ein Jahr Freiheitsstrafe droht) oder einer sonstigen Straftat von erheblicher Bedeutung; eine Interessenabwägung wie in § 68 SGB X ist hier nicht erforderlich. Viele Straftatbestände, wie z. B. die Körperverletzung, der sexuelle Missbrauch von Kindern oder die Misshandlung von Schutzbefohlenen, erfüllen dieses Kriterium jedoch meist nicht. Bei Zweifeln hinsichtlich einer richterlichen Anordnung bzw. eines gerichtlichen Beschlusses bleibt dem Jugendamt letztlich nur die Möglichkeit, dagegen Beschwerde einzulegen und die Aussetzung der sofortigen Vollziehung zu beantragen (§§ 304, 307 StPO).

Jugendämter unterliegen dem Sozialgeheimnis und dürfen Sozialdaten nur mit Einwilligung des Betroffenen oder auf der Grundlage einer Übermittlungsbefugnis aus dem Sozialgesetzbuch an Polizei und Staatsanwaltschaft weitergeben. Übermittlungen – auch des Namens eines Hinweisgebers – sind nur in wenigen Fällen zulässig. Die unbefugte Datenübermittlung stellt eine Ordnungswidrigkeit dar; sie kann zudem sowohl strafrechtliche als auch dienst- bzw. arbeitsrechtliche Folgen sowie Schadensersatzansprüche nach sich ziehen.

9.3 Kita-Antrag – Offenbarung des Arbeitgebers einer Gemeindevertreterin

Eine Gemeindevertreterin hatte im Rahmen der Kommunalwahlen – entsprechend der rechtlichen Vorgaben – als Beruf bzw. Tätigkeit „Bundesbeamtin, Diplomverwaltungswirtin“ angegeben. Der Bürgermeister brachte über einen Antrag der Gemeindevertreterin auf einen Kita-Platz deren konkreten Arbeitgeber in Erfahrung und teilte diese Erkenntnis der Vorsitzenden der Gemeindevertretung und dem Landrat mit. Darüber beschwerte sie sich bei uns.

Nach unserer Auffassung stellt sowohl die Übermittlung der Daten aus dem Antrag auf einen Kita-Platz an den Bürgermeister als auch deren Nutzung und Übermittlung an die Vorsitzende der Gemeindevertretung und den Landrat einen Verstoß gegen § 61 Abs. 1 Achtes Buch Sozialgesetzbuch i. V. m. § 67 b Abs. 1 Zehntes Buch Sozialgesetzbuch (SGB X) dar.

Bezüglich der Übermittlung der Daten durch die für die Bearbeitung der Kita-Anträge zuständige Stelle der Gemeindeverwaltung an den Bürgermeister wurde vorgetragen, diese sei zur Prüfung der Angaben der Gemeindevertreterin auf Grundlage der Hauptsatzung erfolgt. Zudem sei es um die Prüfung eines Verstoßes gegen die Kita-Gebührensatzung, hier bzgl. der Angaben zum Arbeitgeber, gegangen.

Die betreffenden Angaben unterliegen jedoch dem Sozialdatenschutz (Sozialgeheimnis). Die Verarbeitung dieser Daten setzt eine Rechtsgrundlage im Sozialgesetzbuch voraus; andere z. B. kommunalrechtliche Befugnisse kommen daneben nicht in Betracht. Eine entsprechende Rechtsgrundlage gab es vorliegend nicht. Zum einen lag der Antrag der Gemeindevertreterin auf einen Kita-Platz bereits einige Jahre zurück; die Daten wären daher sogar teilweise schon zu löschen gewesen. Zum anderen gab es ersichtlich keine Zweifel am Rechtsanspruch (Erwerbstätigkeit der Gemeindevertreterin) und individuellen Bedarf (Betreuungsumfang) für die Kinderbetreuung sowie an den Angaben zum Elterneinkommen, sodass auch insoweit keine Datenübermittlung angezeigt war.

Hinsichtlich der Speicherung bzw. Nutzung der Daten seitens des Bürgermeisters und der anschließenden Übermittlung an die Vorsitzende der Gemeindevertretung und den Landrat ergibt sich kein anderes Bild: Eine Befugnis aus dem Sozialgesetzbuch ist auch für dieses Vorgehen nicht ersichtlich. Letztlich bleibt festzuhalten, dass unbefugt übermittelte Sozialdaten überhaupt nicht verarbeitet oder genutzt werden dürfen, sondern gemäß § 84 Abs. 2 SGB X umgehend zu löschen sind.

Die vorläufige datenschutzrechtliche Bewertung wurde den betreffenden Personen dargelegt. Da die Betroffene auch Strafanzeige erstattete, ruhte die weitere Prüfung – auch bezüglich der Einleitung eines Bußgeldverfahrens – zunächst jedoch im Hinblick auf das von der Staatsanwaltschaft eingeleitete Ermittlungsverfahren. Sie ist in diesen Fällen gemäß § 40 Ordnungswidrigkeitengesetz für die Verfolgung der Tat auch unter dem Gesichtspunkt einer Ordnungswidrigkeit zuständig. Das strafrechtliche Ermittlungsverfahren wurde zwischenzeitlich eingestellt und das hiesige Prüfverfahren wieder aufgenommen. Ein abschließendes Ergebnis liegt noch nicht vor.

Eine vom ursprünglichen Zweck abweichende Verarbeitung oder Nutzung von sensitiven Sozialdaten erfordert die Einwilligung der Betroffenen oder eine spezielle Rechtsgrundlage im Sozialgesetzbuch; kommunalrechtliche Befugnisse (z. B. Satzungen) genügen nicht.

10 Justiz

Vorratsdatenspeicherung in Deutschland wieder eingeführt

Der Gesetzgeber hat mit einem neuen Artikelgesetz zur Einführung einer Speicherpflicht und einer Höchstspeicherfrist für Verkehrsdaten[34] u. a. die Regelungen im Telekommunikationsgesetz (TKG) ersetzt, die das Bundesverfassungsgericht im Jahr 2010 wegen Verstoßes gegen das Fernmeldegeheimnis (Artikel 10 Grundgesetz) für nichtig erklärt hatte.[35] Trotz anhaltender Kritik der Datenschutzbehörden und der Forderung, den erst Ende Mai 2015 vorgelegten Gesetzentwurf ausführlich und unter umfassender Öffentlichkeitsbeteiligung zu erörtern, wurde das Gesetz im Eiltempo verabschiedet. Damit wurde die Vorratsdatenspeicherung von Telekommunikationsverkehrsdaten für Zwecke der Strafverfolgung und der Gefahrenabwehr wieder eingeführt.

Gegenstand der Neuregelung im Telekommunikationsgesetz ist die anlasslose und unterschiedslose Speicherung von Daten von Telekommunikationsteilnehmern unabhängig von einem konkreten Verdacht gegen die jeweilige Person. Die Neufassung der §§ 113 a und 113 b TKG verpflichtet Erbringer von öffentlich zugänglichen Telekommunikationsdiensten, Verkehrsdaten mit Ausnahme von Standortdaten, für die eine Speicherfrist von vier Wochen gilt, für zehn Wochen zu speichern. Zu diesen Daten gehören bei Telefondiensten die Rufnummern der beteiligten Anschlüsse, Zeitpunkt und Dauer der Verbindung und Angaben von genutzten Diensten, beim Mobilfunk auch die internationalen Kennungen der mobilen Teilnehmer der anrufenden bzw. angerufenen Anschlüsse (Seriennummer der SIM-Karte) und des Endgerätes (sog. IMEI, IMSI), der Standort des Mobiltelefons (Funkzelle) und bei der Internetnutzung (Surfen, Internettelefonie etc.) die Internetprotokoll-Adressen der Nutzer, Datum, Uhrzeit von Beginn und Ende der Nutzung sowie eine zugewiesene Benutzerkennung. Entsprechendes gilt bei der Nutzung von Kurz-, Multimedia- oder ähnlichen Nachrichten. Ausgenommen von der Speicherpflicht sind Anbieter, die ihren Kunden nur eine kurzzeitige Nutzung von Telekommunikationsdiensten (Telefon oder W-LAN) ermöglichen, also zum Beispiel Betreiber von Internet-Cafés, Hotels und Restaurants. Auch Inhalte der Kommunikation, Daten über aufgerufene Internetseiten und Daten von Diensten der elektronischen Post dürfen aufgrund dieser Vorschrift nicht gespeichert werden.

---

34 Gesetz zur Einführung einer Speicherpflicht und einer Höchstspeicherfrist für Verkehrsdaten vom 10. Dezember 2015, BGBl. I S. 2218

35 Urteil des Bundesverfassungsgerichts vom 2. März 2010, 1 BvR 256/08, 1 BvR 263/08, 1 BvR 586/08

Die gespeicherten Daten dürfen die Diensteanbieter gemäß § 113 c TKG für Auskünfte an Strafverfolgungsbehörden zur Verfolgung besonders schwerer Straftaten verwenden oder auch an Behörden zur Abwehr einer konkreten Gefahr für hohe Rechtsgüter (z. B. Leib, Leben) übermitteln.

Zugleich wurde mit diesem Gesetz als Folgeänderung der Zugriff der Strafverfolgungsbehörden auf Verkehrsdaten gemäß § 100 g der Strafprozessordnung neu gefasst und eine ausdrücklich benannte Rechtsgrundlage für die Erhebung aller in einer Funkzelle anfallenden Verkehrsdaten (sog. Funkzellenabfrage) geschaffen. Mit der Begründung, den strafrechtlichen Schutz von Informationssystemen zu verbessern und den Handel mit illegal erlangten Daten einzudämmen, schuf das Gesetz darüber hinaus einen neuen Straftatbestand. Nach § 202 d Strafgesetzbuch kann der Handel mit oder die Überlassung von rechtswidrig erlangten Daten in Schädigungs- oder Bereicherungsabsicht künftig als Datenhehlerei mit einem Strafrahmen bis zu drei Jahren Freiheitsstrafe oder Geldstrafe geahndet werden.

Wir haben grundsätzliche Zweifel an der Eignung und Erforderlichkeit der Vorratsdatenspeicherung für Zwecke der effektiven Gefahrenabwehr und Strafverfolgung. Sowohl die Bundesregierung als Initiatorin des Gesetzgebungsvorhabens als auch Strafverfolgungsbehörden sind den Nachweis schuldig geblieben, dass die Vorratsdatenspeicherung den Erfolg strafrechtlicher Ermittlungen verbessern wird. Auch Gutachten des Max-Planck-Instituts und des Wissenschaftlichen Dienstes des Deutschen Bundestages aus dem Jahr 2011 haben die Wirksamkeit der Maßnahme infrage gestellt. In der Gesetzesbegründung wurde lediglich darauf hingewiesen, dass die Speicherdauer der für geschäftliche Zwecke der Anbieter ohnehin vorgehaltenen Verkehrsdaten bei einzelnen Unternehmen bisher unterschiedlich sei und dies im Einzelfall dazu führen könnte, dass strafrechtliche Ermittlungen ohne Erfolg bleiben. Ein konkret dokumentierter Nutzen einer flächendeckenden Vorratsdatenspeicherung in Form messbarer Aufklärungsquoten konnte in der Praxis dagegen nicht belegt werden.

Aber auch eine von den Sicherheitsbehörden rein theoretisch angenommene Effektivitätssteigerung bei der Kriminalitätsbekämpfung begründet nicht notwendig eine neue Befugnis für weitreichende Verkehrsdatenspeicherungen. Nach den Prüferfahrungen der Bundesbeauftragten für den Datenschutz und die Informationsfreiheit, deren Aufsicht die Telekommunikationsbranche unterliegt, werden Verkehrsdaten bei Telefonverbindungen und SMS von den Diensteanbietern vielfach zwischen drei und sechs Monaten für betriebliche Zwecke vorgehalten. Auf diese kann bereits nach geltendem Recht zugegriffen werden.

Darüber hinaus ist es höchst fraglich, ob die oben erwähnten Ausnahmen von der Speicherpflicht nicht gerade Kriminellen, deren Kommunikationsverhalten

für die Sicherheitsbehörden erklärtermaßen zur Aufklärung schwerer Straftaten relevant ist, Umgehungsmöglichkeiten schaffen und somit „speicherfreie“ Kommunikationswege bieten.

Sowohl das Bundesverfassungsgericht[36] als auch der Europäische Gerichtshof[37] haben die vorsorgliche und anlasslose Vorratsdatenspeicherung aller Verkehrsdaten wegen ihrer hohen Eingriffsintensität als schwerwiegenden Grundrechtseingriff bewertet. Auch ohne Kenntnis eines Gesprächsinhalts können aus Verkehrsdaten sehr genaue Schlüsse auf das Privatleben einer Person gezogen werden. Kommunikationspartner und soziale Beziehungen lassen sich feststellen. Standortdaten geben sogar Ort und Zeit des Aufenthalts einer Person preis – Daten, aus denen Bewegungs-, Tätigkeits- und Kontaktprofile abgeleitet werden können. Nach Auffassung des Bundesverfassungsgerichts darf deshalb keine gesetzliche Entwicklung eingeleitet werden, die darauf abzielt, alle zur Strafverfolgung oder Gefahrenabwehr nützlichen Telekommunikationsverkehrsdaten möglichst flächendeckend zu speichern. Die höchstrichterliche Rechtsprechung hat deshalb besondere Anforderungen an die Zulässigkeit dieser Maßnahme gestellt, die aus unserer Sicht mit dem vorliegenden Gesetz nicht vollständig umgesetzt wurden.

Zentrale Voraussetzung für eine verfassungsrechtlich unbedenkliche anlasslose Speicherung der genannten Daten ist, dass diese eine Ausnahme bleibt.[38] Das Bundesverfassungsgericht hat deutlich gemacht, dass für die Beurteilung, ob die Datenerfassung der Bürger bereits diese Ausnahmeschwelle überschritten hat, auch berücksichtigt werden muss, dass die Verkehrsdatenspeicherung nicht im Zusammenspiel mit anderen, bereits vorhandenen Dateien zur Rekonstruierbarkeit praktisch aller Aktivitäten der Bürger führt. Insbesondere im Hinblick auf die Speicherung von Internetprotokoll-Adressen (IP-Adressen), die bei praktisch sämtlichen Telekommunikationsformen künftig zehn Wochen lang gespeichert werden, dürfte eine problematische Zahl von gespeicherten und auswertefähigen Daten erreicht sein. In zahlreichen Gesetzen wurden in den vergangenen Jahren Rechtsgrundlagen für die Verarbeitung von IP-Adressen durch Sicherheitsbehörden festgeschrieben. Auch nach dem Brandenburgischen Polizeigesetz dürfen diese genutzt werden. Der Datenvorrat wird sich zudem auch dadurch erheblich erhöhen, dass die bisher vom Bundesgerichtshof für zulässig gehaltene Speicherfrist von dynamischen IP-Adressen von einer Woche[39] mit der Neu-

---

36 Urteil des Bundesverfassungsgerichts vom 2. März 2010, 1 BvR 256/08, 1 BvR 263/08, 1 BvR 586/08

37 Urteil des Europäischen Gerichtshofs vom 8. April 2014, Rechtssachen C-293/12, C-594/12; siehe B 1.2

38 Urteil des Bundesverfassungsgerichts vom 2. März 2010, 1 BvR 256/08, 1 BvR 263/08, 1 BvR 586/08, Absatz Nr. 218

39 Urteil des Bundesgerichtshofs vom 3. Juli 2014, III ZR 391/13

regelung auf das Zehnfache verlängert wird. Problematisch ist auch, dass die gegenwärtig vorangetriebene Umstellung der Telekommunikationsbranche auf IP-basierte Telefonanschlüsse (Internet-Telefonie) künftig zu einer massiven Erhöhung von vorgehaltenen IP-Adressen führen wird.

Auch der Europäische Gerichtshof stellte in seiner Entscheidung über die Ungültigkeit der Europäischen Richtlinie zur Vorratsdatenspeicherung klar, dass sich verhältnismäßige Ausnahmen vom Schutz des Rechts auf Privatleben nach der europäischen Grundrechtecharta auf das absolut Notwendige beschränken müssen. Dies sei jedoch schon dann nicht mehr gewährleistet, wenn die Daten unabhängig davon gespeichert werden, in welchem Zusammenhang die betroffenen Personen zu einer schweren Straftat stehen. Es sei u. a. erforderlich, den Kreis der Betroffenen auf diejenigen Personen zu beschränken, die in irgendeiner Weise in eine schwere Straftat verwickelt sein könnten, oder deren Daten aus anderen Gründen zur Verhütung, Feststellung oder Verfolgung schwerer Straftaten beitragen könnten.[40] Diese Vorgaben sind neben denen des Grundgesetzes zu beachten. Aus unserer Sicht wird eine zehnwöchige Speicherpflicht für einen erheblichen Teil der anfallenden Verkehrsdaten diesen Anforderungen auch dann nicht gerecht, wenn relativ strenge Abrufregelungen für die Sicherheits- und Strafverfolgungsbehörden gesetzlich festgelegt werden.

Ein weiterer Kritikpunkt an dem Gesetz ist, dass die Beschränkungen des Europäischen Gerichtshofes, für die berufliche Kommunikation von Berufsgeheimnisträgern (z. B. Anwälten oder Ärzten) nur unzureichend umgesetzt wurde. Während das Gericht gefordert hatte, dass deren Verkehrsdaten erst gar nicht gespeichert werden dürfen, sieht das Gesetz eine flächendeckende Speicherung vor und schränkt in § 100g Abs. 4 Strafprozessordnung lediglich den behördlichen Zugriff und die Nutzung der Daten auf Verwertungsebene ein.

Aus datenschutzrechtlicher Sicht immerhin zu begrüßen ist die Festlegung, dass eine verpflichtende Speicherung der Daten im Inland vorgeschrieben ist, womit eine Anforderung des europäischen Gerichtshofes erfüllt wurde.

[40] Urteil des Europäischen Gerichtshofs vom 8. April 2014, Rechtssachen C-293/12, C-594/12; Absatz Nr. 59

Durch das Gesetz zur Einführung einer Speicherpflicht und einer Höchstspeicherfrist für Verkehrsdaten wurde die Vorratsdatenspeicherung neu aufgelegt. Die Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder hatte bereits gegenüber dem Gesetzentwurf erhebliche verfassungsrechtliche Bedenken geäußert, weil die Regelungen grundrechtlichen Anforderungen nicht genügen.[41] Leider wurde die Chance versäumt, höchstrichterliche Forderungen zum Schutz des Rechts auf Privatleben gemäß der europäischen Grundrechtecharta und des Grundrechts der informationellen Selbstbestimmung auf gesetzlicher Ebene zufriedenstellend umzusetzen.

11 Inneres und Kommunales

11.1 Personenbezug von Geodaten – wann sagen Grundstücksdaten etwas über Menschen aus?

In wenigen Bereichen ist die Frage, ob einzelne Daten personenbezogen sind, so umstritten und so schwierig zu beantworten wie im Fall von Geodaten. Die Landesbeauftragte hatte im Berichtszeitraum die Grenzen des Personenbezugs in Abgrenzung zu reinen Sachdaten sowie zur Anonymität zu beurteilen.

Uns erreichte eine Beschwerde von Gemeindevertretern über die Veröffentlichung der Kartenanlage zu einer Beschlussvorlage auf der Internetseite der Gemeinde. Sie zeigte einen Ausschnitt des Gemeindegebiets als Flurkarte, d. h. mit den Grundstücksgrenzen. Für jedes zu Wohnzwecken genutzte Grundstück war die Anzahl der dort gemeldeten Personen durch die entsprechende Anzahl Kästchen vermerkt. Namen enthielt die Karte nicht. Die Gemeinde ging davon aus, dass es sich um anonyme Daten handelt.

Demgegenüber befand die Landesbeauftragte, dass zumindest in einigen Fällen ein Personenbezug vorlag und das Datenschutzrecht daher anwendbar war. Gemäß § 3 Abs. 1 Brandenburgisches Datenschutzgesetz (BbgDSG) sind personenbezogene Daten Einzelangaben über persönliche und sachliche Verhältnisse einer bestimmten oder bestimmbaren Person – die Bestimmbarkeit über Zusatzwissen reicht aus. Es wäre möglich gewesen, etwa durch Blick auf das Klingelschild einen Personenbezug herzustellen. Fraglich war nur, ob es sich um Einzelangaben über persönliche oder sachliche Verhältnisse handelte.

[41] Entschließung „Gegen den Gesetzentwurf zur Vorratsspeicherung von Telekommunikationsverkehrsdaten bestehen erhebliche verfassungsrechtliche Bedenken“ vom 9. Juni 2015, siehe Anlagen 1.2

Bei Geodaten ist zwischen rein raumbezogenen Sachdaten (zum Beispiel der Höhe eines Grundstücks über Normalnull) und solchen Daten zu unterscheiden, die zwar auch mit einem Grundstück verbunden sind, aber gleichzeitig einzelnen, bestimmbaren Personen zugeordnet werden können. Soweit im konkreten Fall der Personenbezug herstellbar war, konnte der Karte als informationeller Mehrwert zumindest entnommen werden, dass die bestimmbare Person gegebenenfalls allein lebte. Hierbei handelte es sich um eine individuelle Entscheidung Einzelner über ihre Lebensweise, also eine Information über persönliche Verhältnisse im Sinne des Datenschutzrechts. Da diese Information nicht allgemein zugänglich ist, war die Veröffentlichungsbefugnis nicht gegeben. Deren Verbreitung konnte zudem, wie dies auch von den Gemeindevertretern beklagt worden war, potenziellen Einbrechern dabei helfen, die Abwesenheit des Hausbewohners auszunutzen.

Die Landesbeauftragte bat die Gemeinde um Aufklärung über die Rechtsgrundlagen der Veröffentlichung der Karte. Da diese aber nach eigener Prüfung von der Anonymität der Daten ausgegangen war, hatte sie keine Betrachtungen mehr zu möglichen Rechtsgrundlagen angestellt. Jedoch hatte sie die Karte bereits anlässlich unserer Bitte um Auskunft unaufgefordert in den nicht frei zugänglichen Bereich der Webseite verschoben, sodass nur solche öffentlichen Stellen auf sie zugreifen konnten, die die Daten zur Erfüllung ihrer Aufgaben benötigten. Ein weiteres Vorgehen war nicht mehr erforderlich.

Auch Daten zu Grundstücken können unter Umständen eine besondere Beziehung zu einem einzigen, zumindest durch Zusatzwissen bestimmbaren Betroffenen (z. B. Eigentümer, Mieter) in der Weise besitzen, dass sie Aussagekraft über dessen Individualität gewinnen. Besteht ein solcher Personenbezug, bedarf es für die Übermittlung an Dritte durch Einstellung ins Internet einer Rechtsgrundlage.

11.2 SKEiBB – Einsatzleitsystem in den Regionalleitstellen

Die Regionalleitstellen des Landes Brandenburg für den Brandschutz, den Rettungsdienst und den Katastrophenschutz führten im Berichtszeitraum ein einheitliches Standardisiertes Kommunales Einsatzleitsystem Brandenburg (SKEiBB) ein, um im Fall der Überlastung oder des Ausfalls einer Regionalleitstelle eine Unterstützung oder Vertretung durch eine andere Leitstelle zu ermöglichen. Dabei wurden jedoch wesentliche datenschutzrechtliche Anforderungen nicht beachtet.

Jede der fünf Regionalleitstellen des Landes ist in Bezug auf das Einsatzleitsystem eine eigene Daten verarbeitende Stelle. Im System werden die beim täglichen Betrieb der Leitstellen anfallenden Einsatzdaten zu Brand- und

Katastrophenfällen sowie zu besonderen Hilfeleistungen in Not- und Unglücksfällen verarbeitet. Dies umfasst immer auch personenbezogene Daten. Die Regionalleitstellen hatten deshalb unsere Behörde frühzeitig in das Projekt eingebunden und um Beratung gebeten. Sie sagten zu, die datenschutzrechtlichen Anforderungen bei der Verfahrensentwicklung und -einführung zu beachten.[42]

Nach einer längeren Phase ohne direkten Kontakt fragten wir im Berichtszeitraum nach dem aktuellen Projektstand. Daraufhin wurden wir darüber informiert, dass die Leitstellen das Einsatzleitsystem zwischenzeitlich jeweils eingeführt hatten. Obwohl in dem Verfahren ausschließlich Echtdaten verarbeitet wurden und das zuvor für diese Zwecke genutzte System bereits abgeschaltet war, wurde der Status uns gegenüber als „Testbetrieb“ bzw. als „erweiterter Pilotbetrieb“ deklariert. Dieser Einschätzung konnten wir jedoch nicht zustimmen. De facto handelte es sich im konkreten Fall um einen Produktivbetrieb. Außerdem würde die Verwendung personenbezogener Echtdaten für Testzwecke im Widerspruch zu § 13 Abs. 3 Brandenburgisches Datenschutzgesetz (BbgDSG) stehen.

Da das Einsatzleitsystem von den Regionalleitstellen im Produktivbetrieb genutzt wurde, hätten diese zuvor eine datenschutzrechtliche Freigabe gem. § 7 Abs. 3 BbgDSG erteilen müssen. Eine solche gab es jedoch nicht. Entsprechend der gesetzlichen Anforderungen hätten hierfür auch ein verfahrensspezifisches Sicherheitskonzept sowie – da im Verfahren sensitive personenbezogene Daten verarbeitet werden – ein positives Ergebnis der Vorabkontrolle durch den jeweils zuständigen behördlichen Datenschutzbeauftragten vorliegen müssen. Auch diese Voraussetzungen wurden in keiner der beteiligten Regionalleitstellen erfüllt.

Wir haben die Leitstellen aufgefordert, für das Verfahren des Einsatzleitsystems umgehend einen rechtskonformen Zustand herzustellen und die bislang noch nicht erfüllten Anforderungen des Brandenburgischen Datenschutzgesetzes umzusetzen. Dies wurde uns zugesagt. Die Landesbeauftragte wird die datenschutzrechtliche Kontrolle und Beratung des Projekts fortführen.

Wenn eine Daten verarbeitende Stelle den Produktivbetrieb eines Verfahrens zur Verarbeitung personenbezogener Daten fälschlicherweise als Test- oder Pilotbetrieb deklariert, kann sie sich damit nicht von der Erfüllung der gesetzlichen Anforderungen befreien. Insbesondere sind bei der Verwendung personenbezogener Echtdaten die erforderlichen technischen und organisatorischen Maßnahmen zur Beherrschung der mit dem Verfahren verbundenen Risiken umzusetzen und ggf. eine Vorabkontrolle durch den Datenschutzbeauftragten durchzuführen.

[42] Tätigkeitsbericht 2012/2013, B 8.3

11.3 Zutrittskontrollen in Gemeinschaftsunterkünften für Flüchtlinge

Brandenburg bewältigt die Aufnahme zahlreicher Flüchtlinge und schafft es, quer durch Gesellschaft und Politik die Neuankömmlinge im Land willkommen zu heißen. Besucher in Gemeinschaftsunterkünften stellen sich hingegen oft die Frage, ob sie in den Häusern willkommen sind – dort stehen sie meist zunächst Wachschutzmitarbeitern gegenüber, die zahlreiche Daten notieren, Ausweise kontrollieren und einen Besucher abweisen, wenn er sich nicht ausweisen kann oder will. Infolgedessen stellt sich die Frage: Darf der Wachschutz das?

11.3.1 Datenschutzrechtlich zulässige Kontrollmaßnahmen

Die Errichtung und Erhaltung von Einrichtungen zur vorläufigen Unterbringung von Flüchtlingen ist gem. §§ 1 Abs. 1, 4 Abs. 2 Landesaufnahmegesetz (LAufnG) eine Pflichtaufgabe der Landkreise und kreisfreien Städte. Auch der Neuentwurf[43] des Gesetzes ändert an dieser Aufgabenzuweisung nichts. Ziele des Landesaufnahmegesetzes sind eine menschenwürdige Unterbringung und die Integration der Flüchtlinge.

Im Dialog mit einigen Landkreisen, auf deren Unterkünfte sich die Nachfragen bezogen, erfuhren wir von den täglichen Herausforderungen, die diese bei dem Betrieb der Gemeinschaftsunterkünfte zu bewältigen haben. Als großes Problem wurden mehrfach die sog. Verdichtungen geschildert, also das Herabsetzen der Mindeststandards zum Zweck der Unterbringung einer größeren Personenanzahl. Aufgrund der sehr eingeschränkten Privatsphäre werden Besucher eines Mitbewohners häufig als störend empfunden.

Hinzu kommt, dass untergebrachte Personen nicht immer in ihrer jeweiligen Unterkunft bleiben, sondern aus verschiedenen Gründen diese verlassen und in anderen Unterkünften schlafen. So komme es vor, dass „Besucher“ die Unterkünfte betreten, um dort für längere Zeit bei Verwandten, Freunden oder Bekannten unterzukommen. Daneben werden einige Unterkünfte in Brandenburg häufig durch noch nicht untergebrachte Flüchtlinge aus einem benachbarten Bundesland aufgesucht. Die zusätzlichen Schlafgäste erhöhen dann das Konfliktpotenzial unter den eng beieinander lebenden Bewohnern. Eine Besucherdokumentation soll dazu dienen, am Ende der Besuchszeit festzustellen, ob sich noch fremde Personen im Gebäude befinden.

Zudem werden die Unterkünfte auch von Personen betreten, deren Motivation im Interesse der Bewohner zweifelhaft ist: z. B. Glaubensbekehrer, Dro-

[43] Entwurf der Landesregierung für ein Landesaufnahmegesetz, Landtags-Drucksache 6/3080 vom 30. November 2015

gendealer und Personen, die ihre Neugierde ohne Rücksicht auf die Bewohner befriedigen möchten. Eine lückenlose Zutrittskontrolle mit der Erhebung von Personendaten soll nach Vorstellung der Betreiber die Konfliktneigung von Besuchern bereits beim Betreten vermindern.

Auch die Zahl der Angriffe auf Unterkünfte, Flüchtlinge und Helfer ist sehr stark gestiegen. Es besteht daher sowohl ein hoher Schutzbedarf für die untergebrachten Flüchtlinge als auch ein anerkennenswertes Interesse von Helfern, ihre Daten nicht in größerem Maß preiszugeben als unbedingt erforderlich.

Nach unserer Einschätzung können Betreiber eingriffsintensive Maßnahmen einer Zugangskontrolle (Identitätsnachweis, Zutrittsverweigerung) im Regelfall nicht auf das allgemeine Hausrecht stützen. Als Rechtsgrundlage für datenschutzrechtlich relevante Zutrittskontrollen kann aber § 12 Abs. 1 Brandenburgisches Datenschutzgesetz (BbgDSG) i. V. m. den §§ 1 Abs. 1, 4 Abs. 2 LAufnG herangezogen werden. § 12 Abs. 1 BbgDSG erlaubt eine Datenerhebung zur Erfüllung einer gesetzlich zugewiesenen Aufgabe, wenn die Datenerhebung hierfür erforderlich ist. Die Aufgabe einer menschenwürdigen Unterbringung der Flüchtlinge umfasst auch die Sicherung der Einrichtungen sowie den Schutz der untergebrachten Personen gegen Übergriffe und die Gewährleistung eines Mindestmaßes an Privatsphäre gegenüber unerwünschten Besuchern oder Besuchern anderer Bewohner. Die Landkreise und kreisfreien Städte dürfen daher bei Zutrittskontrollen Daten erheben, wenn und soweit dies für die vorläufige Unterbringung im genannten Sinn erforderlich ist. Anders als nach unserer früher geäußerten Ansicht,[44] halten wir einen Abgleich der erhobenen Besucherdaten mit Ausweispapieren in diesen rechtlichen Grenzen ebenfalls für zulässig.

Auf dieser Grundlage sind aufgrund der bestehenden Gefahrenlage folgende Maßnahmen erforderlich und damit zulässig:

- Zutrittskontrollen, bei denen der Vor- und der Nachname des Besuchers und der Zweck des Besuchs (etwa Name des besuchten Bewohners) erfasst wird – etwa in Besucherscheinen,

- ein Abgleich der erhobenen Daten mit einem Ausweispapier,

- eine kurzfristige Speicherung der Daten auch über den Besuch hinaus für einen angemessenen kurzen Zeitraum von etwa einem Tag, wenn zugleich organisatorisch sichergestellt wird, dass die Daten bei Fehlen besonderer Vorkommnisse tatsächlich am Folgetag vernichtet werden.

[44] Tätigkeitsbericht 2002, 4.3.2.1

Des Weiteren empfehlen wir, die Besucher über den weiteren Umgang mit ihren Daten in geeigneter Form zu informieren.

Zu beachten ist, dass die erforderlichen Maßnahmen von den jeweils bestehenden Umständen abhängen. In Hinblick auf unsere obigen Vorgaben bedeutet dies insbesondere, dass die Landkreise und kreisfreien Städte gefordert sind, ihre Kontrollmaßnahmen wieder abzubauen, wenn es hierfür keinen Anlass mehr gibt. Bei der Verringerung der Zahl der unterzubringenden Personen sollte der ebenfalls bestehenden Integrationsaufgabe wieder mehr Bedeutung zugemessen werden. Sollte dann ein Bewohner einen Besucher legitimieren, der keinen Ausweis vorlegen oder seinen Namen nicht nennen möchte, kann regelmäßig kein Anlass bestehen, dem Besucher den Zutritt zu verwehren. Bei einer erheblichen Reduzierung der Gefahr von Übergriffen von außen sollte auf eine Speicherung von Daten über die Besuchszeit hinaus verzichtet werden.

11.3.2 Beauftragung von Wachschutzunternehmen für Zutrittskontrollen

Der Betrieb von Gemeinschaftsunterkünften erfolgt entweder durch den Landkreis bzw. die kreisfreie Stadt selbst oder gemäß § 4 Abs. 3 Landesaufnahmegesetz (LAufnG) durch eine beauftragte nicht öffentliche Stelle. Die Sicherung der Gemeinschaftsunterkünfte wird regelmäßig durch ein beauftragtes Wachschutzunternehmen durchgeführt. Die Landkreise und kreisfreien Städte schließen selbstständig die Verträge mit den Betreibern bzw. den Sicherheitsdiensten. Bei der Ausgestaltung der Verträge konnten wir in den überprüften Fällen große Unsicherheiten feststellen.

Wachschutzunternehmen dürfen nur als sog. Verwaltungshelfer, also als unselbstständige Hilfsorgane in die Sicherung von Gemeinschaftsunterkünften eingeschaltet werden. Eine andere Gestaltung (Funktionsübertragung, Beleihung) kommt mangels gesetzlicher Grundlage nicht in Betracht. Soweit ein beauftragtes Wachschutzunternehmen personenbezogene Daten erhebt, ist zu beachten, dass der Landkreis bzw. die kreisfreie Stadt rechtlich für die Datenerhebung und den weiteren Umgang mit den Daten nach § 11 Brandenburgisches Datenschutzgesetz (BbgDSG) verantwortlich bleibt. Der Kreis bzw. die Stadt ist daher verpflichtet, mit dem Dritten einen Vertrag über eine Auftragsdatenverarbeitung zu schließen. Dieser Vertrag muss sicherstellen, dass der Auftragnehmer die Bestimmungen des Brandenburgischen Datenschutzgesetzes befolgt und jederzeit vom Auftraggeber veranlasste Kontrollen ermöglicht. Der Auftrag ist schriftlich zu erteilen und muss auch Festlegungen zum Gegenstand und zum Umfang der Datenverarbeitung und zu den technischen und organisatorischen Maßnahmen enthalten. Es muss zudem ein strenges Weisungsrecht des Landkreises bzw. der kreisfreien Stadt gewährleistet sein. In Hinblick auf eine Datenerhebung bei Zutrittskon-

trollen ist dieses Weisungsrecht besonders wichtig, damit zügig und flexibel auf geänderte Situationen mit einer angemessenen Anpassung der Kontrollmaßnahmen reagiert werden kann. Besteht kein Vertrag nach den Maßstäben des § 11 BbgDSG, ist die Datenerhebung durch das Wachschutzunternehmen unzulässig.

Im Rahmen des Neuentwurfs des Landesaufnahmegesetzes durch die Landesregierung wirkte die Landesbeauftragte auf eine Klarstellung der Rechtslage hin. In § 19 Abs. 3 Satz 4 des Entwurfs wurde ein Hinweis auf § 11 BbgDSG aufgenommen und in der Gesetzesbegründung erläutert, dass eine Aufgabenübertragung nur im Wege der Verwaltungshilfe erfolgen kann und daher zwingend § 11 BbgDSG zu beachten ist.

In Unterkünften der vorläufigen Unterbringung von Flüchtlingen können angesichts der aktuellen Gefahrenlage als zulässig erachtet werden: Zutrittskontrollen mit der Erfassung u. a. des Namens des Besuchers, ein Abgleich der Daten mit Ausweisdokumenten und eine Speicherung der Daten bis zum Folgetag. Bei einer Veränderung der Gefährdungssituation sind die Maßnahmen auf das jeweils erforderliche Maß anzupassen.

Private Wachschutzunternehmen können als Verwaltungshelfer in die Sicherung von Unterkünften eingeschaltet und mit der Erhebung von Daten beauftragt werden. Bei der Auftragserteilung müssen sich die Landkreise und kreisfreien Städte u. a. ein Weisungsrecht vorbehalten. Wird kein Vertrag nach den Maßstäben des § 11 BbgDSG geschlossen, ist jede Datenverarbeitung durch das Wachschutzunternehmen unzulässig.

11.4 Liveübertragung von Kreistagssitzungen

Seit der Einführung einer speziellen Rechtsgrundlage in der Kommunalverfassung des Landes Brandenburg für Übertragungen sowie Bild- und Tonaufzeichnungen der Sitzungen von Vertretungskörperschaften beschäftigt die Frage ihrer Umsetzung die kommunale Praxis.

Ein Landkreis fragte uns nach den rechtlichen Voraussetzungen für die Echtzeit-Übertragung von Sitzungen des Kreistags ins Internet und deren Speicherung sowie das Bereithalten zum Download auf der Internetseite des Landkreises.

Das Vorhaben stützt sich auf § 36 Abs. 3 Kommunalverfassung des Landes Brandenburg (BbgKVerf), nach dem die Anfertigung von Bild- und Tonaufzeichnungen in der Geschäftsordnung geregelt werden können. Fehlt eine solche satzungsmäßige Regelung, bedarf es zur Zulässigkeit eines einstimmigen Beschlusses der Vertretungskörperschaft.

Wir hatten uns bereits in einem früheren Tätigkeitsbericht[45] mit dieser Problematik beschäftigt. Durch die Anfrage des Landkreises erhielten wir die Gelegenheit, die damals erfolgten Ausführungen zu präzisieren. Kernaussage unserer Antwort war, dass weiterhin der Grundsatz der Saalöffentlichkeit, nicht aber der Internetöffentlichkeit gilt. Im Einzelnen folgt hieraus:

- Die Gebietskörperschaft als verantwortliche Stelle hat für diejenigen Rechtsverstöße einzustehen, die durch eine unzulässige Übertragung oder Aufzeichnung der Sitzungen entstehen. Für die Inhalte sind die jeweiligen Redner verantwortlich.

- Grundsätzlich zulässig sind Aufnahmen nur in öffentlicher Sitzung. Möglich ist auch, in der Geschäftsordnung des Vertretungsorgans festzulegen, dass durch Beschluss in weiteren Fällen eine Aufzeichnung oder Übertragung unterbunden werden kann.

- Da die Geschäftsordnung nur Mitglieder des Vertretungsorgans binden kann, taugt sie grundsätzlich nicht als Rechtsgrundlage für die Anfertigung von Aufnahmen sonstiger Personen. Dies bedeutet, dass alle gezeigten Personen, die nicht Mitglieder des Vertretungsorgans sind (z. B. Mitarbeiter der Gemeinde, Bürger in Fragestunden), in die Aufzeichnung einwilligen müssen. Die Einwilligung ist höchstpersönlich abzugeben, d. h. dass etwa ein Dezernatsleiter nicht wirksam für seine Mitarbeiter einwilligen kann.

- Die von der Gebietskörperschaft selbst bewirkte Anfertigung von Bildaufnahmen nach § 36 Abs. 3 Satz 2 BbgKVerf ist von der Zulassung der Aufzeichnung durch Medien (Satz 1) sowie von Tonaufzeichnungen zur Unterstützung des Protokolls (§ 42 Abs. 2 Satz 2 BbgKVerf) rechtlich strikt zu trennen. Letztere Vorhaben besitzen vollkommen andere Voraussetzungen und Rechtsfolgen.

Schließlich wiesen wir darauf hin, dass der Gesetzgeber eine Gleichbehandlung von Liveübertragung und längerfristige Speicherung angestrebt hat. Abweichungen ergeben sich für rechtmäßig aufgezeichnetes Material insoweit nicht.

Die Kommunalverfassung des Landes Brandenburg enthält zwar eine weitgehende Befugnis zur Anfertigung von Bild- und Tonaufzeichnungen. Bei der konkreten Ausgestaltung sind jedoch datenschutzrechtliche Einschränkungen zu beachten.

[45] Tätigkeitsbericht 2010/2011, A 13.4

11.5 Einwohnerfragestunde – nicht immer ein Datenschutzproblem

Einwohnerfragestunden geben als wichtiger Teil von Gemeindevertretungssitzungen immer wieder Anlass für datenschutzrechtliche Anfragen. Dabei ist jedoch nicht immer klar, ob personenbezogene Daten überhaupt eine Rolle spielen.

Eine Bürgerin hatte die Gemeinde um detaillierte Auskunft über Kosten eines Bauvorhabens gebeten. Die Maßnahme betraf ein im Gemeindeeigentum stehendes Denkmal. Sie beantragte die Beantwortung im Rahmen der nächsten Einwohnerfragestunde.

Das Auskunftsbegehren war insbesondere nach der gemeindlichen Einwohnerbeteiligungssatzung zu beurteilen. Danach musste die Stadt Fragen zu den Beratungsgegenständen in der öffentlichen Sitzung beantworten.

Letztlich war eine datenschutzrechtliche Prüfung im vorliegenden Fall nicht erforderlich, da die Beantwortung keine Übermittlung personenbezogener Daten erforderte und der Anwendungsbereich des Brandenburgischen Datenschutzgesetzes daher nicht eröffnet war. Es wurde nur die Herausgabe von Geschäftsdaten angefordert, die keine Zuordnung zu Einzelpersonen erlaubten. Die Frage, ob sonstige schutzbedürftige Daten (etwa Betriebs- und Geschäftsgeheimnisse) vorlagen, über die im Rahmen der Einwohnerbeteiligungssatzung keine Auskunft zu erteilen wäre, konnte mangels Zuständigkeit von uns nicht beantwortet werden.

Unabhängig vom vorliegenden Fall gehören Beratungsgegenstände, die sich notwendig mit Einzelpersonen beschäftigen (z. B. Personalangelegenheiten) regelmäßig in die nicht öffentliche Sitzung. Die Weitergabe personenbezogener Daten im Rahmen von Bürgeranfragen ist grundsätzlich ausgeschlossen. Interessierte Bürger können zwar die Akteneinsichtsrechte nach dem Akteneinsichts- und Informationszugangsgesetz bzw. dem Umweltinformationsgesetz geltend machen oder eine Übermittlung nach § 16 Brandenburgisches Datenschutzgesetz beantragen. Allerdings sehen auch diese Rechtsgrundlagen Vorschriften zum Schutz personenbezogener Daten vor.

Die Einwohnerfragestunde ist üblicherweise auf Gegenstände der öffentlichen Sitzung beschränkt. In dieser werden regelmäßig Sachverhalte ohne Personenbezug behandelt, sodass sich datenschutzrechtliche Fragen erst gar nicht stellen.

11.6 Einsicht in Unterschriftenlisten für ein Bürgerbegehren durch Gemeindevertreter

Regelmäßig erreichen uns Anfragen im Zusammenhang mit Anträgen von Gemeindevertretern auf Akteneinsicht gemäß § 29 Abs. 1 der Kommunalverfassung des Landes Brandenburg (BbgKVerf). In einem speziellen Fall war zu entscheiden, ob Gemeindevertreter das Recht haben, Unterschriftenlisten zu einem Bürgerbegehren einzusehen.

Eine Gemeinde hatte Unterschriftenlisten zu einem Bürgerbegehren entgegengenommen. Nachdem diese ausgezählt worden waren, stellte der Wahlleiter das Erreichen des kommunalrechtlich erforderlichen Quorums fest, das die Befassung der Gemeindevertretung mit dem Begehren notwendig machte. Die Gemeindevertretung beschloss jedoch mehrheitlich, dass das Bürgerbegehren einen unzulässigen Gegenstand betraf und daher unabhängig von der Unterschriftenzahl unzulässig sei. Daraufhin begehrten einzelne Gemeindevertreter Einsicht in die Unterschriftenlisten mit der Begründung, die Rechtmäßigkeit der Auszählung nach gültigen und ungültigen Stimmen sowie den Umgang mit den Listen überprüfen zu wollen. Der Wahlleiter bat uns um Rat, wie mit diesem Antrag umzugehen sei.

Gemäß § 29 Abs. 1 Kommunalverfassung des Landes Brandenburg (BbgKVerf) kann jeder Gemeindevertreter im Rahmen seiner Aufgabenerfüllung vom Hauptverwaltungsbeamten Auskunft und Akteneinsicht verlangen. Zur Kontrolle der Verwaltung besteht der Auskunfts- und Akteneinsichtsanspruch in allen Angelegenheiten, in denen die Gemeinde zuständig ist. Die Akteneinsicht bedarf eines Antrags unter Darlegung des konkreten Anlasses. Es muss also schlüssig sein, warum die Kenntnis der begehrten Informationen erforderlich ist.

Die Landesbeauftragte hatte empfohlen, den Antrag zurückzuweisen. Die Begründung war hinsichtlich keines der beiden zulässigen Zwecke der Akteneinsicht schlüssig. Nach § 29 Abs. 1 Satz 1 BbgKVerf ist ein Recht auf Akteneinsicht nur im Rahmen der Aufgabenerfüllung des Gemeindevertreters gegeben. Dies war hier zu verneinen, da nach der Ungültigerklärung des Bürgerbegehrens die Gemeindevertreter keinerlei Aufgaben mehr hinsichtlich der Unterschriftenlisten wahrzunehmen hatten.

Nach Satz 2 dieser Vorschrift kommt eine Akteneinsicht auch zur Kontrolle der Verwaltung infrage. In diesem Fall muss sich aus der Begründung des Antrags ergeben, dass die Akteneinsicht zur Kontrolle der Verwaltung überhaupt geeignet ist. Konkret sollte der Umgang mit den Listen nachgeprüft werden. Es war jedoch nicht dargetan oder ersichtlich, inwieweit die Unterschriftenlisten selbst Anzeichen dieses Umgangs zeigten. Insoweit hätte Akteneinsicht nur in den restlichen, nicht personenbezogenen Verwaltungs-

vorgang gewährt werden können. Auch hinsichtlich des Wunsches nach Überprüfung der Auszählung kamen wir zu dem Ergebnis, dass es in dem konkreten Antragsschreiben an der ausreichenden Darlegung des konkreten Anlasses für die Einsichtnahme fehlte. So war etwa nicht dargelegt, ob das Erreichen des Quorums angezweifelt werde oder nur die Feststellung der Stimmanzahl als solche nachgeprüft werden sollte. Geringe Fehler in der Auszählung hätten das Ergebnis nicht beeinflusst. Zudem handelte es sich um einen abgeschlossenen Vorgang.

Auch bei ordnungsgemäßer Begründung des Antrags wäre eine Einsicht in die Unterschriftslisten wahrscheinlich abzulehnen gewesen. Gem. § 29 Abs. 1 Satz 4 BbgKVerf sind Auskunft und Akteneinsicht zu verweigern, wenn und soweit schutzwürdige Belange Betroffener oder Dritter entgegenstehen. Es darf vermutet werden, dass die Interessen der Betroffenen an der Geheimhaltung ihrer Unterschrift zu diesem Zeitpunkt überwogen hätten. Schließlich stellen die personenbezogenen Daten Meinungsäußerungen in einer die Gemeinde seinerzeit spaltenden Frage dar. Diese hätten unter Umständen nachteilige Auswirkungen für die Betroffenen haben können.

Akteneinsichts- und Auskunftsbegehren von Gemeindevertretern müssen schlüssig und unter Bezugnahme auf den konkreten Anlass begründet werden. Die Akteneinsicht findet ihre Grenze in den überwiegenden schutzwürdigen Belangen Betroffener.

11.7 Gelbe Säcke – Einwohner unter Überwachung ihrer Verwaltung?

Die Träger des Dualen Systems sind für die Ausgabe gelber Säcke zur Wertstoffentsorgung verantwortlich. Durch Verträge wird die Ausgabe oft auf andere Stellen übertragen – auch auf Gemeinden. Dabei kommt es oft zu Engpässen und dem Wunsch nach Rationierung – und im Zuge dessen auch zu der Idee, Listen darüber zu führen, wer bereits wie viele gelbe Säcke abgeholt hat. Konflikte mit dem Recht auf Datenschutz sind vorprogrammiert.

Einer Bürgerin, die im Rathaus ihrer Stadt gelbe Säcke zur Wertstoffentsorgung abholen wollte, wurden diese nur gegen Angabe ihres Namens und Wohnorts ausgehändigt. Die Verwaltung registrierte ihren Namen sodann in einer elektronisch geführten Liste.

Auf Nachfrage teilte die Stadt mit, sie erhalte vom Entsorgungsträger nur eine gewisse Anzahl von Säcken pro Jahr zur Ausgabe. Die Rationierung und damit zusammenhängende Datenerhebung und -nutzung geschehe, um zu verhindern, dass Betroffene mehr als ein bestimmtes Kontingent an gelben

Säcken pro Jahr mitnähmen, was eine verbreitete Praxis darstelle. Teilweise kämen zu diesem Zweck sogar Betroffene aus angrenzenden Regionen, für die andere Entsorgungsträger zuständig sind. Die Folge sei gewesen, dass bereits im Herbst des Vorjahres keine Säcke mehr hätten ausgegeben werden können.

Bei der Datenerhebung und dem Abgleich des Namens der Betroffenen mit den Listen handelt es sich um eine Verarbeitung personenbezogener Daten, die einer Rechtsgrundlage bedarf. Eine spezialgesetzliche Befugnis zur Datenerhebung bei der Ausgabe von gelben Säcken besteht nicht. Nach § 12 Abs. 1 Brandenburgisches Datenschutzgesetz (BbgDSG) ist eine Erhebung personenbezogener Daten darüber hinaus nur zulässig, wenn die öffentliche Stelle mit ihr eine Aufgabe erfüllt, die ihr durch Gesetz zugewiesen ist.

Den Rechtsvorschriften ist keine Befugnis zur Rationierung von gelben Säcken durch Gemeinden zu entnehmen. Nach § 6 Verpackungsverordnung trifft die Pflicht zur Rücknahme von Verkaufsverpackungen ausschließlich die Hersteller. Dieser kommen sie durch Anschluss an das Duale System nach. Dessen privatrechtliche Träger können im Rahmen ihrer Privatautonomie in zivilrechtlichen Verträgen und Unterverträgen die Ausführung einzelner Maßnahmen – auch die Ausgabe gelber Säcke – auf Dritte übertragen. Hieraus ergibt sich jedoch keine gesetzliche Aufgabenzuweisung an die Gemeinden im Sinne von § 12 BbgDSG.

Die Hersteller bzw. die von ihnen beauftragten Träger des Dualen Systems müssen dafür sorgen, dass Säcke in bedarfsdeckender Anzahl bereitgestellt werden. Eine Befugnis zur Rationierung lässt sich den anwendbaren Vorschriften nicht entnehmen. Daher war die Erhebung der Daten Betroffener durch die Stadt unzulässig.

Da die Stadt selbst keine Rechtsgrundlage für die Verarbeitung der Abholerdaten sah, stellte sie die Erhebung von Daten unaufgefordert ein.

Öffentliche Stellen müssen vor der Erhebung personenbezogener Daten – wenn sie nicht durch spezielle Normen erlaubt ist – prüfen, ob die Maßnahme zur Erfüllung einer durch Gesetz zugewiesenen Aufgabe erforderlich ist. Vertragliche Vereinbarungen allein berechtigen hierzu regelmäßig nicht.

11.8 Fundsache Smartphone – Zwischen Eigentums- und Datenschutzrecht

Auch Fundsachen unterliegen dem Datenschutzrecht, wenn darauf personenbezogene Daten gespeichert sind. Dies trifft z. B. für mobile Endgeräte wie Smartphones, Tablets oder Notebooks zu. Der Umgang hiermit kann kommunale Fundbüros vor datenschutzrechtliche Herausforderungen stellen.

Smartphones und andere mobile Endgeräte sind heute unsere alltäglichen Begleiter. Bei Verlust eines Gerätes entsteht nicht nur ein finanzieller Schaden, auch die darauf gespeicherten personenbezogenen Daten können u. U. von unberechtigten Dritten missbraucht werden. Deshalb sollte einerseits der Nutzer bzw. der Hersteller eines mobilen Endgerätes Sicherheitsmechanismen umsetzen bzw. vorsehen, die das Gerät und die darauf gespeicherten Daten vor unbefugtem Zugriff schützen. Wenn mobile Endgeräte als Fundsache in kommunalen Fundbüros abgegeben werden, liegt es andererseits in deren Verantwortung als Daten verarbeitende Stelle, dass die darauf gespeicherten personenbezogenen Daten vor einer Weitergabe gelöscht oder die Geräte fachgerecht entsorgt werden.

Grundsätzlich gehen Fundsachen, die nach §§ 965 ff. Bürgerliches Gesetzbuch (BGB) durch den Finder bei der zuständigen Stelle angezeigt und dort entsprechend verwahrt worden sind, gem. § 973 BGB nach sechs Monaten in des Eigentum des Finders über – er erwirbt somit das Recht auf Eigentum an der Sache. Ist die Fundsache ein Datenverarbeitungsgerät wie ein Smartphone, Tablet oder Notebook und enthält dieses personenbezogene Daten, ist aus datenschutzrechtlicher Sicht jedoch nicht nur das Recht auf Eigentum an der dinglichen Sache selbst, sondern auch das Recht auf informationelle Selbstbestimmung des Betroffenen, auf den sich diese Daten beziehen, zu beachten.

Mit Abgabe der Fundsache und somit auch der auf dem mobilen Endgerät gespeicherten Daten geht die Verantwortung für die Verarbeitung der personenbezogenen Daten auf die Gemeinde über, die das Fundbüro betreibt. Diese darf personenbezogene Daten nur an Dritte übermitteln, soweit hierfür gem. § 16 Brandenburgisches Datenschutzgesetz eine Rechtsgrundlage vorliegt. Die Voraussetzungen dieser Vorschrift liegen bei der Übermittlung an den Finder nicht vor.

Die Fundbüros sind daher verpflichtet, dafür Sorge zu tragen, dass vor einer Weitergabe die auf mobilen Endgeräten gespeicherten personenbezogenen Daten vollständig gelöscht werden und eine Wiederherstellbarkeit ausgeschlossen ist. Sollte dies nicht möglich sein, ist aus datenschutzrechtlicher Sicht die Herausgabe der Fundsache zu verweigern und diese der Verschrot-

tung zuzuführen. Aus Sicht des Finders ist das natürlich unbefriedigend, schützt aber die Rechte desjenigen, der das mobile Endgerät verloren hat bzw. derjenigen, deren Daten auf dem Gerät gespeichert sind. Der Finder, der ggf. die Herausgabe des Geräts erwartet, ist im Sinne der Transparenz über die Entsorgung zu unterrichten.

Auch für Fundsachen gelten die Anforderungen des Datenschutzrechts, wenn auf ihnen personenbezogene Daten gespeichert sind. Fundbüros müssen vor der Herausgabe mobiler Endgeräte an den Finder oder vor der Versteigerung auf einer Fundsachenauktion für die vollständige Löschung aller auf den Geräten gespeicherten personenbezogenen Daten sorgen.

12 Polizei und Verfassungsschutz

12.1 Bestandsdatenerhebung – Notwendige Änderung des Brandenburgischen Polizeigesetzes

Das zehnte Gesetz zur Änderung des Brandenburgischen Polizeigesetzes[46] diente der notwendig gewordenen Anpassung des Gesetzes an die durch das Bundesverfassungsgericht zwei Jahre zuvor aufgestellten Vorgaben zu Bestandsdatenerhebungen und weiteren Datenabrufen der Polizei. Die bisher für diese Maßnahmen herangezogenen Rechtsgrundlagen des Telekommunikationsgesetzes (TKG) hatte das Gericht für sich genommen als nicht ausreichend eingestuft.

Im Januar 2012 legte das Bundesverfassungsgericht in einem Beschluss[47] die maßgeblichen Vorschriften des Telekommunikationsgesetzes (§§ 111 bis 113 TKG), die Telekommunikationsanbieter verpflichten, Bestandsdaten zu speichern und Sicherheitsbehörden darüber Auskunft zu erteilen, verbindlich aus. Bestandsdaten sind Daten, die zur Begründung, Änderung oder Beendigung eines Vertrags über Telekommunikationsdienste von den Anbietern gespeichert werden. Zu ihnen gehören Name, Adresse, Bankverbindungsdaten und Telefonnummer von Teilnehmern, Passwörter, PIN und auch Rechnungsinformationen. Ferner umfasst der auskunftspflichtige Datenbestand auch Name und Anschrift des Inhabers sowie Kennungen eines elektronischen Postfachs, Mobilfunkanschlüsse und Endgerätenummern.

Das Gericht führte aus, dass § 113 Abs. 1 Satz 1 TKG als Öffnungsklausel zu verstehen ist, die jedoch für sich genommen nicht schon die Voraussetzungen für den Datenabruf schafft. Verfassungsrechtlich ist es geboten, dass die

[46] Gesetz vom 28. April 2014, GVBl. I Nr. 20

[47] Beschluss des Bundesverfassungsgerichts vom 24. Januar 2012, 1 BvR 1299/05

Berechtigung für das sog. manuelle Auskunftsverfahren aufseiten der abrufenden Behörden durch eine normenklare spezifische – ggf. landesrechtliche – Erhebungsbefugnis ergänzt und gesetzlich konkretisiert wird.

Eine spezifische Rechtsgrundlage ist auch für die Zuordnung von temporär zugewiesenen sog. dynamischen Internetprotokoll-Adressen (IP-Adressen) erforderlich, für die nicht mehr § 113 TKG herangezogen werden konnte. Zudem hatte das Gericht festgestellt, dass die Erhebung von Zugangssicherungscodes (z. B. Passwörter, PIN oder PUK), die den Zugang zu Endgeräten sichern, nur insoweit für zulässig erachtet werden kann, als auch die Voraussetzungen für deren tatsächliche Nutzung vorliegen.

Die brandenburgischen Sicherheitsbehörden hatten bisher Auskunftsersuchen allein auf diese unzureichende Rechtsnorm und die polizeirechtliche Generalklausel für Datenerhebungen gestützt. Entsprechende Neuregelungen, die dem Schutz des Rechts auf informationelle Selbstbestimmung und im Falle der Zuordnung dynamischer IP-Adressen dem auf Art. 10 Grundgesetz beruhenden Schutz der näheren Umstände von Telekommunikationsverkehr dienen, wurden mit der o. g. Änderung in das Brandenburgische Polizeigesetz (BbgPolG) eingefügt. Aus datenschutzrechtlicher Sicht ist die Gesetzesanpassung gelungen.

§ 33 c Abs. 1 Satz 1 BbgPolG erlaubt der Polizei nunmehr, einen Telekommunikationsanbieter zur Auskunft über die o. g. Bestandsdaten zu verpflichten, wenn die Voraussetzungen einer Gefahr für Leib, Leben oder Freiheit einer Person oder für den Bestand oder die Sicherheit des Bundes oder des Landes vorliegen. Der Zugriff auf Zugangssicherungscodes wird durch die Befugnis in Satz 2 dieser Vorschrift ermöglicht, sofern „die gesetzlichen Voraussetzungen für die konkret beabsichtigte Nutzung der Daten im Zeitpunkt des Ersuchens vorliegen“. Damit wurde das Gesetz an die verfassungsrechtlichen Vorgaben für den Datenabruf angepasst. Die Auskunft bezüglich dynamischer IP-Adressen ist bei Vorliegen eng umgrenzter Voraussetzungen nunmehr normenklar in § 33 c Abs. 2 BbgPolG geregelt. Positiv ist auch hervorzuheben, dass ein durchgehender Richtervorbehalt gem. § 33 c Abs. 3 BbgPolG und die Regelungen zur Benachrichtigung der Betroffenen spätestens sechs Monate nach Beendigung der Maßnahme für einen erhöhten Schutz bzw. nachträgliche Rechtsschutzmöglichkeiten der Betroffenen sorgen.

Unserer Empfehlung, bei Auskünften über Zugangssicherungen, die einen höheren Schutzbedarf als die übrigen Bestandsdaten haben, nicht die abstrakte formulierte Voraussetzung des Bundesverfassungsgerichts zu übernehmen, sondern die konkreten Maßnahmen und jeweiligen Voraussetzungen abschließend zu benennen, für die diese Daten verwendet werden dürfen, wurde leider nicht entsprochen.

Unerwartet enthielt der Gesetzentwurf auch eine Regelung über den Zugriff der Sicherheitsbehörden auf Bestands- und Nutzungsdaten, die aufgrund §§ 14 und 15 Telemediengesetz bei Telemediendiensteanbietern gespeichert sind. Unter die Telemediendienste fallen z. B. Kommunikations- und Informationsdienste im Internet, Onlineangebote von Waren und Dienstleistungen, Internetsuchmaschinen, Chatrooms und Foren. Zu den gespeicherten Daten gehören zum einen solche, die für die Begründung und Nutzung von Vertragsverhältnissen bei Nutzung der Dienste erforderlich sind, zum anderen Merkmale zur Identifikation des Nutzers (z. B. dynamische IP-Adressen, E-Mail-Adressen und Kennungen), Dauer und Umfang der Nutzung sowie Angaben über die in Anspruch genommenen Telemedien.

Nach der Gesetzesbegründung sollte damit vergleichbar den Verkehrsdaten bei Telekommunikationsanbietern eine bestehende Lücke im Hinblick auf Datenabrufe bei Telemediendiensten geschlossen werden. Insbesondere seien bei Androhung von Suiziden oder Straftaten in Chatrooms wirksame Ermittlungen nur möglich, wenn Informationen zu den handelnden Personen abgerufen werden könnten. Zu diesem Zweck wurde in dem neu geschaffenen § 33 c BbgPolG auch die Auskunft über Bestandsdaten nach dem Telemediengesetz aufgenommen und die bereits bestehende Befugnis für verdeckte Verkehrsdatenerhebungen bei Telekommunikationsdiensten gem. § 33 b BbgPolG um die Nutzungsdatenauskunft bei Telemediendiensteanbietern ergänzt.

Die explizite Ermächtigung zu Abrufen von Bestands- und Nutzungsdaten auch nach Telemediengesetz trägt grundsätzlich zur Normenklarheit bei. Allerdings sind Nutzungsdaten über in Anspruch genommene Telemedien nach unserer Auffassung nicht mit entsprechenden Angaben zu Telekommunikationsdiensten vergleichbar, da sie aussagekräftiger sein können. Die Angabe, welchen Mediendienst ein Nutzer angeklickt hat, kann bereits eine Vielzahl von Informationen – auch besonders sensitiver Art – etwa bei Internetportalen zu Gesundheitsthemen, religiösen oder politischen Gruppierungen preisgeben und damit auch Rückschlüsse auf Inhalte der Kommunikation zulassen. Angesichts der besonders strengen Voraussetzungen, unter denen eine Auskunft zu diesen Daten gemäß § 33 b Abs. 6 BbgPolG zur Abwehr einer Gefahr weniger hoher Rechtsgüter und unter Richtervorbehalt möglich ist, bestehen jedoch aus unserer Sicht enge Erhebungsbeschränkungen, die dem besonderen Informationsgehalt dieser Daten noch hinreichend Rechnung tragen.

Das Zehnte Gesetz zur Änderung des Brandenburgischen Polizeigesetzes fügte die erforderlichen spezialgesetzlichen Erhebungsbefugnisse für Bestandsdatenauskünfte nach Telekommunikations- und Telemediengesetz, den Zugriff auf Zugangssicherungscodes und dynamische IP-Adressen in das Polizeigesetz ein. Die Umsetzung der vom Bundesverfassungsgericht zuvor geforderten normenklaren Regelungen ist aus datenschutzrechtlicher Sicht zu begrüßen.

12.2 Kontrolle der polizeilichen Kennzeichenerfassung in Brandenburg

Die im Jahr 2006 neu eingeführte Befugnis zur anlassbezogenen, automatischen Kennzeichenerfassung – § 36a Brandenburgisches Polizeigesetz – wäre nach bisheriger Rechtslage am 31. Dezember 2015 außer Kraft getreten. Da sich die Kennzeichenfahndung aus Sicht der Polizei bewährt hat, sollte sie nach dem Willen der Landesregierung dauerhaft in das Polizeigesetz übernommen werden. Diese inzwischen umgesetzte Planung[48] haben wir im September 2015 zum Anlass genommen, das in Brandenburg eingesetzte Kennzeichenerfassungssystem KESY datenschutzrechtlich zu prüfen.

Die technische Durchführung der automatischen Kennzeichenerfassung in Brandenburg erfolgt mithilfe von stationären oder mobilen Kameras. Derzeit sind jedoch ausschließlich stationäre Geräte im Einsatz. Diese können im Fahndungs- oder Aufzeichnungsmodus betrieben werden. Im Fahndungsmodus lesen sie die Kennzeichen aller passierenden Fahrzeuge aus und gleichen sie mit dem Inhalt einer zuvor mit Kennzeichendaten befüllten Fahndungsdatei ab. Bei einer Übereinstimmung (Trefferfall) erfolgt ein Signal bei der zuständigen Polizeidienststelle. Nur diese Trefferdaten werden gespeichert. Im sog. Aufzeichnungsmodus hingegen werden alle erfassten Kennzeichen gespeichert.

§ 36 a BbgPolG erlaubt die heimliche Datenerhebung unter engen Eingriffsvoraussetzungen zu drei Zwecken: wenn sie zur Abwehr einer gegenwärtigen Gefahr für Leib oder Leben erforderlich ist, zur Abwehr einer Gefahr i. V. m. einer Identitätsfeststellung und wenn eine Person oder ein Fahrzeug polizeilich ausgeschrieben wurde und Tatsachen die Annahme unmittelbar bevorstehender, für die Ausschreibung relevanter Straftaten rechtfertigen. Rechtlich problematisch ist, dass durch die Kennzeichenfahndung ein legales Verhalten (das Befahren einer Straße) einer unbestimmten Vielzahl von Personen einer polizeilichen Wahrnehmung unterzogen wird. Auch wenn die

[48] Elftes Gesetz zur Änderung des Brandenburgischen Polizeigesetzes vom 17. Dezember 2015, GVBl I Nr. 40

Erfassung eines Kennzeichens nach der Rechtsprechung des Bundesverfassungsgerichts nur bei einem Trefferfall einen Eingriff in das informationelle Selbstbestimmungsrecht darstellt, hat das Gericht dennoch festgelegt, dass die Kennzeichenerfassung nicht den Eindruck einer flächendeckenden Kontrolle vermitteln darf, weil dies zu Einschüchterungseffekten und Beeinträchtigungen in der Ausübung von Grundrechten führt.[49]

Die noch im Jahr 2011 überwiegende Anzahl von Einsätzen der Kennzeichenerfassung zum Zweck, gestohlene Kraftfahrzeuge aufzufinden, ließ sich aus unserer Sicht nicht auf präventive, polizeigesetzliche Rechtsgrundlagen stützen, sondern stellte eine Strafverfolgungsmaßnahme dar, für die ausschließlich strafprozessuale Ermächtigungsnormen herangezogen werden können. Aus den Jahresberichten des Innenministeriums an den entsprechenden Ausschuss des Landtages über bestimmte Maßnahmen der Datenerhebung – u. a. auch gemäß § 36 a BbgPolG – lässt sich in den letzten Jahren ein Wandel erkennen: Anlass für die präventive Nutzung der Kennzeichenfahndung war in den Jahren 2012 – 2014 zu weit über 90 % die Suche nach einer vermissten oder suizidgefährdeten Person. Bei diesen Einsätzen sind hohe Schutzgüter (körperliche Unversehrtheit, Leben) betroffen und der präventive Zweck steht außer Frage. Auch wenn die Erfolgsquoten dieser Einsätze gering sein mögen, stufen wir diese unter Abwägung der betroffenen Rechte und der insgesamt geringen Anzahl von Nutzungen – im Jahr 2014 unter 130 Fälle – als verhältnismäßig ein und halten den Einsatz des Fahndungssystems für angemessen. Entsprechend hat sich die Landesbeauftragte in einer Stellungnahme zum Gesetzentwurf gegenüber dem Ausschuss für Inneres und Kommunales im November 2015 geäußert.

Große Sorge bereitet uns hingegen die Nutzung der Kennzeichenfahndung für repressive Zwecke, d. h. die hohe Anzahl von Eilfahndungen nach Kraftfahrzeugen, die gestützt auf die Rechtsgrundlage § 100 Abs. 1 Satz 1 Nr. 2 Strafprozessordnung in der Regel auf polizeilichen Anordnungen sowohl von Polizeidienststellen in Brandenburg als auch aus anderen Ländern beruhen. Sie liegt monatlich im hohen dreistelligen Bereich. Hinzu kommen längerfristige Fahndungen aufgrund richterlicher Beschlüsse. Nach dem vorgelegten Zahlenmaterial ist deshalb davon auszugehen, dass die Kameras ständig Kennzeichen aufzeichnen und daher bestimmte Straßenabschnitte entgegen der Entscheidung des Bundesverfassungsgerichts flächendeckend erfasst werden.

Schon vor der Prüfung wurden wir darüber in Kenntnis gesetzt, dass das Kennzeichenerfassungsverfahren ohne die nach dem Brandenburgischen Datenschutzgesetz (BbgDSG) erforderliche Verfahrensdokumentation betrieben wird. Nach § 7 Abs. 3 BbgDSG ist vor der Freigabe eines erstmalig

[49] Urteil des Bundesverfassungsgerichts vom 11. März 2008, 1 BvR 2074/05, 1 BvR 1254/07

eingesetzten automatisierten Verfahrens zur Verarbeitung personenbezogener Daten eine Risikoanalyse und ein Sicherheitskonzept zu entwickeln, das technisch-organisatorische Maßnahmen zum Schutz der Betroffenenrechte enthält. Darüber hinaus ist ein Verfahrensverzeichnis zu erstellen, in dem wesentliche Informationen über das Verfahren (wie z. B. Rechtsgrundlagen, Zweckbestimmung, Datenkategorien, betroffene Personengruppen) dokumentiert werden müssen. Bei der Projektentwicklung von KESY im Jahr 2008 wurden diese Vorgaben nicht beachtet. Dieser Zustand hält bis heute an. Wir haben diesen Mangel gerügt und die Zusage erhalten, dass die Verfahrensdokumentation umgehend nachgearbeitet wird. Eine abschließende Prüfung und Bewertung der technisch-organisatorischen Ausgestaltung des Systems steht daher noch aus.

Das automatische Kennzeichenerfassungssystem der Polizei in Brandenburg, KESY, wird präventiv seit 2006 eingesetzt. Die Rechtsgrundlage, § 36 a Brandenburgisches Polizeigesetz, war zunächst mit Befristungen in das Gesetz eingefügt worden, die zu Beginn des Jahres 2016 entfallen. Die Kontrolle der polizeilichen Anwendungspraxis zur Gefahrenabwehr durch die Landesbeauftragte ist noch nicht abgeschlossen, hat aus rechtlicher Sicht bisher jedoch keine Hinweise auf Datenschutzverletzungen ergeben. Eine vollständige Bewertung ist erst möglich, wenn die gesetzlich vorgeschriebene, aber bisher nicht erstellte Verfahrensdokumentation zur Verfügung steht.

12.3 Prüfung der Telekommunikationsüberwachungsanlage

Im Berichtszeitraum führten wir eine Kontrolle der Telekommunikationsüberwachungsanlage (TKÜ-Anlage) bei der Polizei Brandenburg durch. Die Kontrolle ergab Mängel bei der Umsetzung technisch-organisatorischer Maßnahmen.

Die TKÜ-Anlage wird gemeinsam mit dem Land Berlin betrieben. Eines der Ziele ist, im Bedarfsfall – insbesondere beim Ausfall von Systemkomponenten eines Partners – gegenseitige Hilfeleistungen bereitzustellen. Hierzu wurde die technische Infrastruktur redundant sowohl in Berlin als auch in Brandenburg aufgebaut und die Standorte über eine direkte, verschlüsselte Datenleitung verbunden. Auch die Datenhaltung erfolgt redundant in Berlin und Brandenburg.

Bei der Polizei Brandenburg werden mithilfe der TKÜ-Anlage sowohl Maßnahmen im Rahmen der Strafverfolgung als auch im Rahmen der Gefahrenabwehr durchgeführt. Das Ministerium des Innern und für Kommunales informierte uns zu Beginn des Jahres 2015, dass die neue TKÜ-Anlage gem. § 48 Abs. 5 Brandenburgisches Polizeigesetz i. V. m. Nr. 5 der Dateienrichtlinie-Polizei in Betrieb genommen wurde.

Unsere Kontrolle beschränkte sich auf den in Brandenburg installierten Teil der TKÜ-Anlage. Dabei stellten wir insbesondere fest, dass das gem. § 7 Abs. 3 Brandenburgisches Datenschutzgesetz (BbgDSG) erforderliche Sicherheitskonzept sowie die Umsetzung wichtiger technischer und organisatorischer Sicherheitsmaßnahmen gem. § 10 Abs. 1 und 2 BbgDSG nicht den gesetzlichen Anforderungen entsprachen.

Das uns vom Polizeipräsidium u. a. vorgelegte IT-Rahmensicherheitskonzept der Polizei befand sich noch im Entwurfsstadium und hatte einen Stand von 2010. Wir haben gefordert, es schnellstmöglich zu aktualisieren und umzusetzen. Auch das verfahrensspezifische IT-Sicherheitskonzept zur TKÜ-Anlage war noch nicht vollständig fertiggestellt. Die Analyse der Dokumente ergab jedoch gute Ansätze bei der Etablierung eines umfassenden IT-Sicherheitsprozesses. Die Verantwortlichen folgten den Empfehlungen des Bundesamtes für Sicherheit in der Informationstechnik (BSI) sowohl bzgl. der Methoden als auch der Maßnahmen nach den IT-Grundschutzkatalogen. Dieser Weg sollte konsequent fortgesetzt werden.

Die Daten der TKÜ-Maßnahmen beider Länder werden in einer zentralen Datenbank redundant gespeichert. Diese gemeinsame Speicherung halten wir derzeit für unzulässig. Die Datenverarbeitung soll gem. § 7 Abs. 1 Satz 3 BbgDSG so organisiert sein, dass insbesondere bei der Übermittlung, der Kenntnisnahme im Rahmen der Aufgabenerfüllung und der Einsichtnahme die Trennung der Daten nach den jeweils verfolgten Zwecken und nach unterschiedlichen Betroffenen möglich ist. Wegen der hohen Sensitivität der verarbeiteten Daten halten wir eine strikte Trennung für erforderlich. Wir haben das Polizeipräsidium aufgefordert, die datenschutzgerechte Trennung der Datenbestände schnellstmöglich umzusetzen. Die Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder hat hierzu in der Orientierungshilfe „Mandantenfähigkeit“ technische und organisatorische Anforderungen an die Trennung von automatisierten Verfahren bei der Benutzung einer gemeinsamen IT-Infrastruktur beschrieben.[50]

In der zentralen Datenbank werden sensitive personenbezogene Daten unverschlüsselt gespeichert. Dies haben wir kritisiert. Es ist nicht auszuschließen, dass diese Daten durch Administratoren und Wartungspersonal unberechtigt eingesehen werden. Kryptographische Verfahren (z. B. symmetrische und asymmetrische Verschlüsselung, digitale Signatur) sind besonders geeignet, um Verletzungen des Datenschutzes bei der Verarbeitung von personenbezogenen Daten abzuwenden. Mit ihrer Hilfe lassen sich Manipulationen und Übertragungsfehler nachweisen und die unberechtigte Kenntnisnahme verhindern. Derartige Verfahren sind heute Stand der Technik und können mit vertretbarem Aufwand eingesetzt werden.

[50] http://www.lda.brandenburg.de

Aufgrund der Komplexität des gesamten Systems spielt die Ausbildung der Administratoren eine entscheidende Rolle für die Gewährleistung von Informationssicherheit. Zum Zeitpunkt der Kontrolle hatten die Administratoren noch nicht alle Seminare besucht, die für einen ordnungsgemäßen Betrieb des TKÜ-Systems erforderlich gewesen wären. Wir haben gefordert, die noch offenen Fortbildungsveranstaltungen schnellstmöglich zu absolvieren.

Das Polizeipräsidium ist aufgefordert, die Erstellung des IT-Sicherheitskonzeptes unter Berücksichtigung der BSI-Standards 100-2 und 100-3 zügig abzuschließen und den daraus resultierenden Maßnahmenkatalog konsequent und zeitnah umzusetzen. Die in der gemeinsamen TKÜ-Infrastruktur verarbeiteten Daten der Länder Berlin und Brandenburg sind datenschutzgerecht zu trennen und verschlüsselt auf den Servern zu speichern.

12.4 Gemeinsames Kompetenz- und Dienstleistungszentrum für Telekommunikationsüberwachung

Im Rahmen der Sicherheitskooperation der Freistaaten Sachsen und Thüringen, der Länder Sachsen-Anhalt und Brandenburg sowie des im Juli 2015 beigetretenen Landes Berlin wird derzeit die Einrichtung eines länderübergreifenden Gemeinsamen Kompetenz- und Dienstleistungszentrums auf dem Gebiet der Telekommunikationsüberwachung (GKDZ) geplant. Das Zentrum soll als technischer Dienstleister im Auftrag der Strafverfolgungsbehörden der beteiligten Länder tätig werden.

Im Februar 2015 wurde die Öffentlichkeit durch einen Medienbericht darauf aufmerksam, dass die Staatsregierung in Sachsen zur Realisierung des gemeinsamen Projektes 4,2 Millionen Euro im Haushaltsentwurf vorgesehen hatte. In Beantwortung einer daraufhin gestellten parlamentarischen Anfrage bestätigte die brandenburgische Landesregierung lediglich „Erwägungen der für die öffentliche Sicherheit und Ordnung zuständigen Abteilungsleiter der Innenresorts der Länder… zur Errichtung eines GDKZ“.[51] Im Übrigen berief sie sich jedoch darauf, dass bisher intern erarbeitete Dokumente zu dem Projekt noch im Entwurfsstatus seien und eine abschließende rechtliche Würdigung ablauforganisatorischer Einzelfragen sowie die Festlegung des konkreten Aufgabenspektrums noch ausstehe.

Obwohl seit 2010 eine gemeinsame Arbeitsgruppe Telekommunikationsüberwachung bestand, um länderübergreifende Kooperationsmöglichkeiten auszuloten, wurde die Landesdatenschutzbeauftragte offiziell erst Ende

[51] Antwort der Landesregierung auf die Kleine Anfrage 283, Landtags-Drucksache 6/889 vom 18. März 2015

Februar 2015 von dem zuständigen Ministerium des Innern und für Kommunales des Landes Brandenburg über das geplante Projekt informiert.

Im April 2015 nahmen wir zusammen mit Kollegen der anderen Länder an einem Informationstreffen zu dem Kooperationsvorhaben beim federführenden sächsischen Staatsministerium des Innern teil. Dieses bot Gelegenheit zu einem ersten Austausch zwischen Vertretern der beteiligten Innenresorts und der Datenschutzbehörden. Dabei wurde bestätigt, dass das GKDZ als technischer Dienstleister IT-Systeme zur Verarbeitung von polizeilicher Telekommunikationsüberwachung zentralisiert zur Verfügung stellen und technisches Know- how bündeln soll. Die hoheitliche Aufgabe der Telekommunikationsüberwachung soll bei den Polizeien der jeweiligen Länder verbleiben, sodass keine neuen Eingriffsbefugnisse geschaffen werden. Aufgrund des technologischen Fortschritts der Telekommunikation seien erhebliche Investitionen erforderlich, um technische Systeme vorzuhalten, die eine Überwachung zur Bekämpfung schwerster Straftaten ermöglichen. Deshalb sei eine länderübergreifende Kooperation sinnvoll.

Diese Haltung ist aus Sicht der Sicherheitsbehörden nachvollziehbar. Die Verarbeitung großer Mengen an sensitiven, dem Fernmeldegeheimnis unterliegenden Daten in einer zentralen Institution birgt jedoch ein erhebliches Gefährdungspotenzial für das informationelle Selbstbestimmungsrecht. Es muss gewährleistet sein, dass die Daten einer strengen Zweckbindung unterliegen und die Datensicherheit nicht beeinträchtigt ist. Insbesondere ist darauf zu achten, dass der zur Errichtung des Zentrums erforderliche Staatsvertrag die Aufgaben des Zentrums, Art und Umfang der Datenspeicherung, die Trennung der länderspezifischen Datenbestände, Regelungen zur Datenverarbeitung im Auftrag sowie die Kontrollbefugnisse der Datenschutzbehörden klar festlegt.

Brandenburg ist eines von fünf Ländern, die ein gemeinsames Kompetenz- und Dienstleistungszentrum auf dem Gebiet der Telekommunikationsüberwachung planen. Dieses Zentrum soll als technischer Dienstleister in Form einer Anstalt öffentlichen Rechts errichtet werden. Zwischenzeitlich wurden wir vom Ministerium des Inneren und für Kommunales in den Abstimmungsprozess eingebunden. Dies ist aus unserer Sicht auch notwendig, um rechtzeitig datenschutzrechtliche und technisch-organisatorische Forderungen in das länderübergreifende Projekt einbringen zu können.

12.5 Die Polizei Brandenburg auf Facebook

Das Kommunikations- und Informationsverhalten hat sich im Onlinezeitalter grundlegend verändert. Immer mehr Personen nutzen regelmäßig das Internet, um Informationen zu beruflichen wie privaten Zwecken zu erhalten und zu verbreiten. Insbesondere unter 30-Jährige sind stark in sozialen Netzwerken vertreten und über herkömmliche Medien kaum mehr erreichbar. Wie viele staatliche Institutionen sieht auch die Polizei in Brandenburg eine Herausforderung in der Nutzung sozialer Netzwerke und digitaler Kommunikation mit den Bürgern. Zu diesem Zweck hat sie neben ihrem bereits bestehenden offiziellen Internetauftritt, der Internetwache, im Juli 2015 auch bei Facebook eine eigene sog. Fanpage freigeschaltet.

Im Februar 2015 wurde uns die Konzeption des Polizeipräsidiums zur Nutzung sozialer Medien vorgestellt. Da Facebook das mit Abstand am meisten genutzte Netzwerk in Deutschland ist, möchte auch die Polizei diese Plattform nutzen. Die Webseiten sollen für zielgruppengerechte Informationen zu polizeilichen Themen, Präventionsempfehlungen, Öffentlichkeitsarbeit, Hinweise auf Veranstaltungen, zur Werbung und Nachwuchsgewinnung, aber auch Prävention und Kriminalitätsbekämpfung eingesetzt werden. In dem Konzept wurde auch die Öffentlichkeitsfahndung mithilfe von sozialen Netzwerken thematisiert.

Wir sehen den Einsatz sozialer Netzwerke durch Behörden grundsätzlich kritisch. Bei der Nutzung jedes Internetdienstes entstehen Informationen darüber, wer diesen Dienst in Anspruch genommen hat. Nach dem Telemediengesetz (TMG) dürfen diese Daten in personenbeziehbarer Form bis auf wenige Ausnahmen nur für die Erbringung des Dienstes selbst, nicht jedoch für weitere Zwecke genutzt werden. Soziale Netzwerke werten personen- und ortsbezogene Nutzerdaten aber in der Regel in erheblichem Umfang aus und erstellen für sich und Dritte Analysen. Dies kann auch nicht angemeldete Nutzer betreffen.

Bei dem sozialen Netzwerk Facebook bereitgestellte Inhalte und Nutzungsdaten werden in den USA bzw. dem außereuropäischen Raum gespeichert. Dort finden deutsche Datenschutzstandards keine Anwendung und eine Kontrolle durch deutsche Aufsichtsbehörden ist nicht gewährleistet. Zudem gibt es immer wieder Schwierigkeiten bei der Löschung von Daten. Einmal eingestellte Inhalte können in der Regel nicht mehr verlässlich zurückgenommen werden, weil entsprechende Löschersuchen nicht durchsetzbar sind oder die Seiteninhalte bereits anderweitig verbreitet wurden. Die geltenden telemedienrechtlichen Anforderungen können daher von Fanpage-Anbietern nicht eingehalten werden, denn sie haben keine Einflussmöglichkeiten darauf, was der Betreiber Facebook mit den erhobenen Nutzerdaten macht.

Gerade öffentliche Stellen sollten hier eine Vorbildfunktion wahrnehmen und Nutzer mit ihrem Angebot nicht auf Webseiten locken, die Grundrechtseingriffe ermöglichen.

Wir hinterfragen daher die Erforderlichkeit von Fanpages bei öffentlichen Stellen und erwarten, dass diese den unabdingbaren Bedarf für ihre Zwecke darlegen. Sie müssen außerdem sicherstellen, dass Inhalte auf sozialen Netzwerken ein Zusatzangebot bleiben und Bürger nicht faktisch dazu gezwungen werden, Facebook zu nutzen, wenn sie bestimmte Informationen haben wollen. Darüber hinaus dürfen Facebook-Funktionen nicht für Kernbereiche der Verwaltung oder gar zur Durchführung von hoheitlichen Maßnahmen genutzt werden. Wir empfehlen dringend, die Kommunikation mit den Nutzern – soweit es über das bei Facebook vorgegebene Liken, Teilen und Kommentieren hinausgeht – auf Kanäle außerhalb des sozialen Netzwerks zu verlegen, damit möglichst wenig Nutzungsdaten generiert werden.

Wir haben diese und weitere Anforderungen zu technischen Schutzvorkehrungen mit Fachkräften der Polizei diskutiert. Sie hatten sich zuvor in einer internen Arbeitsgruppe mit den Chancen und Risiken der Nutzung sozialer Netzwerke befasst und die konzeptionelle Umsetzung der Fanpage vorbereitet. Dabei zeigte sich, dass sich die Polizei intensiv mit der Thematik beschäftigt hatte und sich der datenschutzrechtlichen Risiken bewusst ist. Sie hat nicht vor, polizeiliche Kernaufgaben mit Facebook zu erledigen, sieht jedoch die Notwendigkeit, sich als staatliche Behörde bürgernah, modern und zukunftsweisend zu präsentieren. Dazu gehöre auch, die Zielgruppe der unter 30-Jährigen anzusprechen, die ohne polizeiliche Facebookpräsenz nur bedingt erreichbar sei. Zudem lassen sich Informationen in kürzester Zeit mit einem breiten Publikum teilen. Diese Funktion kann für Maßnahmen der Beweissicherung aber auch zur Suche nach Personen genutzt werden. Auch hätten bisherige Erfahrungen gezeigt, dass die Bevölkerung gern häufiger mit Behörden in Kontakt treten möchte. Die Polizei verspricht sich daher über das Netzwerk eine intensivere Interaktion mit der Bevölkerung, was sich vertrauensbildend auswirken soll. Um unerwünschten Reaktionen der Nutzer wie überhöhte Moralisierungen, diffamierende Äußerungen, Hassreden und Stigmatisierungen zu begegnen, wird die Webseite 24 Stunden von entsprechend geschultem Personal beobachtet. Zudem gibt es einen Hinweis auf der Fanpage, dass personenbezogene Daten nicht über Facebook verbreitet werden sollen. Für Aufgaben der Strafverfolgung findet die Kommunikation zwischen Polizei und Nutzern nicht über die Plattform statt. Damit sind zumindest einige unserer Forderungen erfüllt.

Dass die Polizeipräsenz bei Facebook die Möglichkeiten der externen Öffentlichkeitsarbeit und Kommunikation mit der Bevölkerung erweitert und in diesem Sinne nützlich ist, ist unbestritten. Zweifel bleiben hinsichtlich der Frage, ob die Fanpage neben der polizeieigenen Internetpräsenz für die polizeiliche

Aufgabenerfüllung erforderlich ist. Wir haben gegenüber der Polizei deutlich gemacht, dass sich die Kommunikation in Netzwerken vielfach einer wirksamen Kontrolle entzieht. Gerade bei Themen der inneren Sicherheit besteht die Gefahr, dass es zu Radikalisierungen, Stigmatisierungen von Personen durch Nutzer oder gar Verabredungen gewalttätiger Gruppen kommt. Ob das vorgesehene Beobachtungspersonal ausreicht, um kritische Entwicklungen zu vermeiden, bleibt abzuwarten. Sinnvoll wäre es, für konkrete Szenarien passende Reaktionsmaßnahmen zu entwickeln. Auch die datenschutzrechtliche Verantwortung von Fanpage-Betreibern für die von Facebook verarbeiteten Nutzerdaten ist bisher nicht höchstrichterlich geklärt.

Was den Spezialfall Öffentlichkeitsfahndungen angeht, haben wir unsere Position bereits mehrfach eindeutig klargestellt[52]. Hier stehen besonders schutzwürdige Interessen von Beschuldigten auf dem Spiel. Die für Ermittlungsbehörden bestehende Richtlinie für die Inanspruchnahme von Publikationsorganen bei Öffentlichkeitsfahndungen sieht bisher vor, keine privaten Internetanbieter dafür einzubinden. Aus unserer Sicht widerspricht eine direkt auf einer Facebook Fanpage eingestellte oder verlinkte Fahndung datenschutzrechtlichen Vorgaben. Auch in diesem Punkt ist die brandenburgische Polizei unseren Empfehlungen nachgekommen und verzichtet bis zur Fortschreibung des Konzeptes auf Öffentlichkeitsfahndungen in sozialen Netzwerken.

Die Vorzüge der Nutzung einer weltweiten Kommunikationsplattform wie Facebook, die mit Millionen von Nutzern für eine schnelle, flächendeckende Verbreitung von Informationen sorgt, dürfen nicht den Blick für die Risiken verstellen, die das Veröffentlichen von Daten auf der Plattform mit sich bringt. Diese können nicht sicher gelöscht werden. Nutzerrechte werden im Rahmen der Registrierung und Auswertung des Verhaltens durch Facebook beeinträchtigt. Schließlich ist eine datenschutzrechtliche Kontrolle durch deutsche Aufsichtsbehörden nicht gewährleistet.

12.6 Prüfung der Datenverarbeitung des Verfassungsschutzes in der Antiterrordatei und der Rechtsextremismus-Datei

Im Berichtszeitraum hat die Landesbeauftragte eine anlassunabhängige, gesetzlich geforderte Kontrolle der brandenburgischen Verfassungsschutzbehörde durchgeführt. Gegenstand der Überprüfung war die Datenverarbeitung in der Antiterrordatei sowie der Rechtsextremismus-Datei, die beide zentral beim Bundeskriminalamt für alle Länder und den Bund geführt werden.

52 Tätigkeitsbericht 2012/2013, B 12.1

Das Bundesverfassungsgericht hatte bereits in seinem Urteil zum Antiterrordateigesetz[53] betont, dass die Transparenz der Datenverarbeitung und der individuelle Rechtsschutz durch das Gesetz nur sehr eingeschränkt möglich sind und der Gewährleistung einer effektiven Kontrolle umso größere Bedeutung zukommt. Seine Vorgabe, mindestens alle zwei Jahre datenschutzrechtliche Kontrollen durchzuführen, wird durch § 10 Abs. 2 Antiterrordateigesetz bzw. § 11 Abs. 2 Rechtsextremismus-Datei-Gesetz umgesetzt.

Um die Kontrolle durchzuführen, hat die Landesbeauftragte beim Bundeskriminalamt unter anderem die Protokolldaten angefordert, die Aufschluss über die im Jahr 2014 erfolgten Datenverarbeitungen durch die auf die Dateien jeweils zugriffsberechtigten Mitarbeiter der brandenburgischen Verfassungsschutzbehörde geben. Den zur Verfügung gestellten, umfänglichen Protokolldaten konnten wir zwar entnehmen, welche Daten bzw. Datensätze angesehen, neu angelegt, gelöscht oder geändert und welche Suchanfragen im betreffenden Zeitraum durchgeführt wurden. Allerdings war es nicht möglich, den Grund für die Erhebung bzw. Speicherung jeweils nachzuvollziehen. Im Anschluss an die Auswertung der Protokolle haben wir daher für ausgewählte Einzelfälle eine ergänzende Vor-Ort-Kontrolle bei der brandenburgischen Verfassungsschutzbehörde durchgeführt. Nur unter zusätzlicher Heranziehung der dort vorhandenen Informationen konnte eine datenschutzrechtliche Bewertung der Zugriffe erfolgen. Im Ergebnis waren keine Auffälligkeiten ersichtlich. Die Erforderlichkeit der geprüften Datenerhebungen bzw. -speicherungen konnte anhand der weiteren, bei der Verfassungsschutzbehörde vorhandenen Dokumente nachvollzogen werden. Insgesamt haben wir den Eindruck gewonnen, dass insbesondere die Antiterrordatei nur sehr restriktiv genutzt wird.

Neben der begrenzten Aussagekraft der Protokolldateien allein hat die Prüfung weitere Fragen hinsichtlich der Durchführbarkeit und Effizienz entsprechender Kontrollen seitens der Datenschutzaufsichtsbehörden aufgeworfen.

Neben der Heranziehung weiterer lokaler Dokumente ist meist auch ein Zugriff auf andere Dateien, z. B. das nachrichtendienstliche Informationssystem NADIS, erforderlich. Zudem ist jede teilnehmende Behörde gesetzlich dazu verpflichtet, bei Bekanntwerden entsprechender Informationen die Daten in die Antiterrordatei bzw. Rechtsextremismus-Datei einzuspeisen. Personen sind daher oftmals mehrfach gespeichert. Letztlich ist bei einer Suchanfrage in der Trefferliste nicht vermerkt, ob die darin aufgelisteten Einträge auch tatsächlich angesehen wurden; hierfür ist ein Abgleich mit der Liste der angesehenen Einträge notwendig.

53 Urteil des Bundesverfassungsgerichts vom 24. April 2013, 1 BvR 1215/07

Die Datenschutzbehörden des Bundes und der Länder befinden sich in einem Erfahrungsaustausch zur Kontrolle der Antiterror- bzw. Rechtsextremismus-Datei. Zum Ende des Berichtszeitraums fand in diesem Kontext ein Informationsbesuch beim Bundeskriminalamt statt.

Die Kontrolle der Datenverarbeitung des brandenburgischen Verfassungsschutzes in der Antiterror- bzw. Rechtsextremismus-Datei ergab keine datenschutzrechtlichen Mängel. Die aufwendige Prüfung hat jedoch Fragen hinsichtlich der Durchführbarkeit und Effizienz solcher Kontrollen offengelegt.

13 Schule

13.1 Schüler am Pranger – Aushang mit Verhaltensverstößen in einer Schule

In einer Schule wurden die gegen Schüler verhängten Ordnungsmaßnahmen in einem Schaukasten bekannt gemacht. Sowohl die Namen als auch die Art (z. B. schriftlicher Verweis, zeitweiser Ausschluss vom Unterricht) und der Grund (z. B. Betrug, Diebstahl, unentschuldigtes Fernbleiben vom Unterricht) für die Verhängung der Ordnungsmaßnahme wurden dort angegeben. Eltern beschwerten sich bei uns.

Bei einer Kontrolle vor Ort gab der Schulleiter an, dass er die Aushänge veranlasst hatte, sie sich dort seit einer Woche befanden und dies eine übliche Verfahrensweise sei. Sogar die Schulordnung sah eine Veröffentlichung der Ordnungsmaßnahmen per Aushang in der Schule als Erziehungsmaßnahme vor.

Bei den in der Bekanntmachung aufgeführten Angaben handelt es sich um personenbezogene Daten der betroffenen Schüler. Der Aushang der Informationen mit der Möglichkeit zur Kenntnisnahme durch Dritte stellt eine Verarbeitung personenbezogener Daten in der Form des Übermittelns dar.

Die Verarbeitung personenbezogener Daten ist nur zulässig, wenn der Betroffene (oder sein gesetzlicher Vertreter) eingewilligt hat oder eine Rechtsvorschrift die Datenverarbeitung erlaubt. Im Hinblick auf das Verbot entwürdigender Maßnahmen in § 63 Abs. 1 Brandenburgisches Schulgesetz (BbgSchulG) wäre eine Einwilligung unter solchen Umständen wohl nicht zulässig. Auch eine Rechtsgrundlage, die eine Übermittlung der fraglichen Daten rechtfertigen würde, existiert nicht.

Schulen dürfen nach § 65 Abs. 2 BbgSchulG personenbezogene Daten von Schülern verarbeiten, soweit dies zur rechtmäßigen Erfüllung des schulischen

Bildungs- und Erziehungsauftrages notwendig ist. Gemäß § 64 BbgSchulG ist die Verhängung von Ordnungsmaßnahmen gegen Schüler bei schwerwiegenden Verstößen gegen Rechts- bzw. Verwaltungsvorschriften oder die Schulordnung zulässig. Ordnungsmaßnahmen müssen angemessen sein und den Grundsätzen der Verhältnismäßigkeit genügen. Ziel einer Ordnungsmaßnahme ist es, den Schülern ihr Fehlverhalten deutlich vor Augen zu führen und sie dadurch zukünftig zu einem normgerechten Verhalten zu veranlassen. Die Ordnungsmaßnahme hat vorrangig erzieherischen Charakter und keine Straffunktion.

Durch die öffentliche und namentliche Bekanntmachung der verhängten Ordnungsmaßnahmen wurde im konkreten Fall der betreffende Schüler bloßgestellt und diffamiert (Prangerwirkung). Die Veröffentlichung war nicht zur rechtmäßigen Erfüllung der Aufgaben der Schule gemäß § 65 Abs. 2 BbgSchulG erforderlich.

Hinzu kam, dass in den hier getroffenen Bekanntmachungen die Gründe für die verhängte Maßnahme genannt wurden. Dabei wurden Begriffe wie Betrug, Urkundenfälschung, versuchte Sachbeschädigung und Diebstahl benutzt, d. h. Straftatbestände aus dem Strafgesetzbuch. Die Feststellung der Erfüllung strafrechtlicher Tatbestände ist nicht Aufgabe von Schulleitungen, sondern Aufgabe der Gerichte. Allein schon die Verwendung der o. g. Begriffe ist geeignet, die Person, in deren Zusammenhang sie verwendet werden, in der Öffentlichkeit als Straftäter erscheinen zu lassen und sie damit langfristig zu stigmatisieren. Die damit verbundene Rufschädigung für den Betroffenen ist regelmäßig ein sehr schwerwiegender Eingriff in die Persönlichkeitsrechte der jeweiligen Person, der eine entwürdigende Maßnahme i. S. v. § 63 Abs. 1 BbgSchulG darstellt, und damit verboten ist.

Auch die Schulordnung als untergesetzliche Rechtsvorschrift darf vom Brandenburgischen Schulgesetz nicht zum Nachteil der Betroffenen abweichen und eine Veröffentlichung der Ordnungsmaßnahmen vorsehen. Derartige Festlegungen sind rechtswidrig. Im konkreten Fall verstoßen sie auch gegen die Verwaltungsvorschriften über die Organisation der Schulen in inneren und äußeren Schulangelegenheiten (VV-Schulbetrieb), in denen das Ministerium für Bildung, Jugend und Sport unter „18 – Informations- und Anschlagtafeln“ die folgende Regelung trifft:

„Informationen über gesundheitliche Beeinträchtigungen oder das Fehlverhalten einzelner Schülerinnen und Schüler sind nicht auszuhängen. Die Informationen erfolgen unter Beachtung der datenschutzrechtlichen Bestimmungen.“

Die vom Schulleiter vorgeschlagene Lösung, zukünftig nicht die vollen Namen der betroffenen Schüler im Aushang zu nennen, sondern stattdessen nur die Initialen zu verwenden, ist ebenfalls nicht datenschutzgerecht. Der

Schulöffentlichkeit wäre damit noch immer klar, um welche konkrete Person es sich handelt.

Auch wenn die Aushänge bei unserem Kontrollbesuch entfernt wurden, haben wir das rechtswidrige Verhalten des Schulleiters beanstandet. Das Bildungsministerium sowie das Landesamt für Schule und Lehrerbildung wurden über unsere Beanstandung informiert.

Die Bekanntmachung der Namen von Schülern, der Ordnungsmaßnahmen und der Gründe hierfür stellte eine rechtswidrige Übermittlung personenbezogener Daten an Dritte dar. Besonders schwerwiegend an diesem Verstoß gegen datenschutzrechtliche Vorschriften war die Tatsache, dass es sich bei den übermittelten personenbezogenen Daten um Informationen mit einem sehr hohen diskreditierenden Potenzial handelte.

13.2 Aushang von alten Zeugnissen zum Schuljubiläum

Jubiläen sollen begangen werden. Um an Zurückliegendes zu erinnern, bietet sich eine kleine Ausstellung an. Wenn aber eine Schule anlässlich ihres 60-jährigen Bestehens Dokumente zeigt, in denen sich personenbezogene Daten ehemaliger Schüler befinden und deren Aufbewahrungsfristen abgelaufen sind, entstehen Probleme mit dem Datenschutzrecht. Hierzu erreichte uns eine Beschwerde.

Anlässlich eines Schuljubiläums hatte eine Grundschule das Zeugnis des Petenten aus der 7. Klasse, einschließlich der darin enthaltenen persönlichen Beurteilung, der Öffentlichkeit zugänglich gemacht. Es stammte aus den 1980er Jahren. Besucher der Ausstellung hatten den Petenten mehrfach auf sein Zeugnis angesprochen.

Gemäß § 12 Datenschutzverordnung Schulwesen dürfen Zeugnisse, wenn es sich nicht um Abschluss- oder Abgangszeugnisse handelt, fünf Jahre aufbewahrt werden. Danach sind sie dem zuständigen Archiv anzubieten oder zu vernichten. Dass die Schule hier das Zeugnis noch immer aufbewahrte, war von keiner Rechtsgrundlage gedeckt und stellte somit eine rechtswidrige Datenspeicherung dar.

Bei den Angaben in einem Zeugnis handelt es sich um personenbezogene Daten des Schülers. Diese dürfen Dritten nur zugänglich gemacht werden, wenn der Betroffene, oder bei Minderjährigen dessen Eltern, dem zugestimmt haben. Nach unseren Erkenntnissen lag eine solche Einwilligung in vorliegendem Fall nicht vor. Hinzu kommt, dass Zeugnisinhalte für den Betroffenen durchaus diskreditierende Angaben enthalten können. Da die Schule keinerlei Übermittlungsbefugnisse für die Veröffentlichung der Noten und der Beurteilung des Petenten an Dritte hatte, erfolgte die Präsentation in der Jubilä-

umsausstellung unter Verstoß gegen geltendes Recht und stellte eine schwerwiegende Verletzung des Persönlichkeitsrechtes dar.

Die Schule wurde über ihr rechtswidriges Verhalten aufgeklärt und sicherte zu, ihren Aktenbestand dementsprechend zu überprüfen.

Die Aufbewahrung von personenbezogenen Daten über gesetzlich normierte Aufbewahrungsfristen hinaus ist eine rechtswidrige Datenverarbeitung. Gleiches gilt, wenn personenbezogene Daten Dritten zur Kenntnis gegeben werden, ohne dass eine gesetzliche Ermächtigung oder die Einwilligung des Betroffenen vorliegt.

13.3 Einsatz von Apps auf privaten IT-Systemen von Lehrkräften

Lehrkräfte haben in der Regel keinen Büroarbeitsplatz in der Schule und sind deshalb darauf angewiesen, einen Teil ihrer Arbeit zu Hause zu erledigen. Für die automatisierte Verarbeitung personenbezogener Daten besteht hierbei häufig der Wunsch, die eigenen, privaten IT-Systeme zu nutzen – wegen der technischen Entwicklung zunehmend auch mobile Endgeräte wie Notebooks, Tablets und Smartphones. Fraglich ist, unter welchen rechtlichen und technisch-organisatorischen Rahmenbedingungen eine solche Datenverarbeitung zulässig ist, gerade auch vor dem Hintergrund der erheblichen Risiken, die durch den Einsatz von Apps auf mobilen Endgeräten entstehen können.[54]

Der Unterarbeitskreis Datenschutz und Schule der Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder wollte sich zu diesem Thema einen Überblick über die vorhandenen Rechtsvorschriften in den einzelnen Bundesländern verschaffen. Im Ergebnis ist festzustellen, dass zwar in vielen Ländern Regelungen für die Verarbeitung personenbezogener Daten durch Lehrkräfte auf eigenen, privaten IT-Systemen und außerhalb der Schule existieren (mit unterschiedlichen Anforderungen), jedoch der Einsatz von Apps auf privaten mobilen Endgeräten nirgendwo explizit betrachtet wird.

Auch im Land Brandenburg ist zur Beantwortung der Frage auf allgemeine Regelungen zurückzugreifen – konkret auf die Datenschutzverordnung Schulwesen (DSV). Gem. § 5 DSV kann der Schulleiter Lehrkräften oder dem sonstigen pädagogischen Personal die Verarbeitung von personenbezogenen Daten auf privaten IT-Systemen und außerhalb der Schule dann gestatten, wenn eine Reihe von Voraussetzungen erfüllt sind. Insbesondere dürfen die in Rede stehenden Daten nicht jenen Datenkategorien angehören, deren Verarbeitung gem. Anlage 1 DSV außerhalb der Schule untersagt ist (z. B.

54 siehe B 2.3 und Tätigkeitsbericht 2012/2013, A 2

Gesundheitsdaten der Schüler oder Angaben zu ihrer Teilnahme an sonderpädagogischer Förderung). Die Genehmigung darf durch den Schulleiter nur dann erteilt werden, wenn u. a. ein Sicherheitskonzept gem. § 7 Abs. 3 Brandenburgisches Datenschutzgesetz (BbgDSG) existiert, das auch die besonderen Risiken der Datenverarbeitung außerhalb der Schule und auf privaten Geräten berücksichtigt, und die Umsetzung technischer und organisatorischer Maßnahmen nach dem Sicherheitskonzept sowie gem. § 10 Abs. 1 und 2 BbgDSG nachgewiesen und durch den Schulleiter bestätigt wurde.

Für die Beantragung und Genehmigung der Datenverarbeitung außerhalb der Schule und auf privaten IT-Systemen ist ein in Anlage 7 DSV vorgegebenes Formular zu verwenden. In diesem sind u. a. der Zweck der Verarbeitung, die eingesetzten Programme, die betroffenen Personengruppen (Klasse, Jahrgangsstufe, Lerngruppe) und die Kategorien der zu verarbeitenden Dateien zu beschreiben. Außerdem muss die jeweilige Lehrkraft dort ihr Einverständnis erklären, sich der datenschutzrechtlichen Kontrolle durch unsere Behörde zu unterwerfen.

Die vorgenannten Regelungen der DSV gelten selbstverständlich auch, wenn private mobile Geräte genutzt werden. Allerdings entstehen hierbei im Vergleich zum Einsatz stationärer IT-Systeme besondere Risiken für die Vertraulichkeit, die Integrität und die Verfügbarkeit der verarbeiteten Schülerdaten, etwa bei einem Verlust des Gerätes. Gleiches gilt auch bei der Verwendung von Apps: Diese können erhebliche Sicherheitsmängel aufweisen, aus datenschutzrechtlicher Sicht bedenklich oder gar unzulässig sein. Letzteres ist z. B. dann anzunehmen, wenn eine ungeregelte Weitergabe von Schülerdaten an einen Dienstleister, wie etwa im Rahmen des Cloud Computing üblich, erfolgt. Wegen der möglichen Risiken sind die technischen und organisatorischen Gegenmaßnahmen in diesen Nutzungsszenarien besonders sorgfältig zu planen und umzusetzen. Das Sicherheitskonzept für die Verarbeitung der personenbezogenen Daten der Schüler ist unter Berücksichtigung der privaten mobilen Geräte und der Nutzung der jeweiligen Apps fortzuschreiben.

Auch für den Einsatz von Apps auf privaten mobilen Geräten der Lehrkräfte gelten die Regelungen der Datenschutzverordnung Schulwesen. Eine Genehmigung dieses Einsatzes verlangt aufgrund der zusätzlichen Risiken, vorab besondere technische und organisatorische Maßnahmen zur Gewährleistung des Datenschutzes und der Informationssicherheit zu planen und umzusetzen.

13.4 Projekte „Verbraucherbildung an Schulen“ und „Überarbeitung der Rahmenlehrpläne“

Der sichere und bewusste Umgang mit Neuen Medien, orientiert an geltenden sozialen und rechtlichen Normen, ist eine Basiskompetenz in unserer Gesellschaft. Deren Vermittlung an Kinder und Jugendliche, ist Teil des Bildungs- und Erziehungsauftrages. Zwei Projekte im Land Brandenburg wollen dem Rechnung tragen.

Ende 2009 hat das damalige Ministerium für Umwelt, Gesundheit und Verbraucherschutz den Arbeitskreis „Verbraucherbildung“, damals bestehend aus Vertretern dieses Ministeriums, des Ministeriums für Bildung, Jugend und Sport, der Verbraucherzentrale Brandenburg, des Landesinstituts für Schule und Medien Berlin-Brandenburg (LISUM), des Ministeriums für Arbeit, Soziales, Familie und Frauen und der Universität Potsdam gebildet. Seit 2013 ist auch die Landesbeauftragte hier Mitglied.

Der Arbeitskreis geht davon aus, dass unzureichende Kenntnisse und Erfahrungen junger Verbraucher bei Alltagskompetenzen zu wirtschaftlich und gesundheitlich nachteiligen Marktentscheidungen sowie zu einem (moralisch-ethischen) Werteverlust führen können. Durch die frühzeitige Entwicklung bewussten Verbraucherverhaltens kann bei Kindern und Jugendlichen eine Einflussnahme auf gesellschaftliche Entwicklungen im Sinn von Nachhaltigkeitsstrategien erzielt werden. Deshalb setzt sich der Arbeitskreis das Ziel, die Vermittlung notwendiger Alltagskompetenzen an Kinder und Jugendliche über den Schulunterricht abzustimmen und zu organisieren.

Der Aspekt der Medienkompetenz und des Datenschutzes ist wesentlicher Bestandteil der Verbraucherkompetenz. Ergebnis der Arbeit des Arbeitskreises war das Projekt „Verbraucherbildung an Schulen“. Märkische Schulen konnten sich mit dem Ziel bewerben, das Profil „Verbraucherkompetenzschule“ zu erhalten. Dabei unterstützten Träger des Arbeitskreises diese Schulen durch Informations- und Weiterbildungsangebote. In einer Auftaktveranstaltung im November 2014, an der wir teilnahmen, konnten vier Schulen für das Pilotvorhaben gewonnen werden.

Auch an einem zweiten Projekt waren wir beteiligt. Unter Federführung des LISUM haben die Länder Berlin und Brandenburg gemeinsame Rahmenlehrpläne erarbeitet. Bestandteil ist dabei auch ein Basiscurriculum Medienbildung. In gemeinsamen Beratungen mit dem LISUM konnten wir explizite Anforderungen zur altersgemäßen und medienbezogenen, fachübergreifenden Vermittlung von Grundlagen des Urheber- und Persönlichkeitsrechts, des Datenschutzes und des Jugendmedienschutzes aufnehmen. Darüber hinaus haben wir dem LISUM angeboten, fachbezogene Schulungen zur Umsetzung des Curriculums durchzuführen.

Die neugestalteten Lehrpläne werden voraussichtlich im Schuljahr 2017/2018 in den brandenburgischen und Berliner Schulen wirksam werden.

Medienbildung bei Kindern und Jugendlichen ist eine der Hauptbildungsaufgaben in unserer sich technisch rasant weiterentwickelnden Lebenswirklichkeit. In brandenburgischen Schulen wird der Datenschutz in diesem Rahmen künftig stärkere Berücksichtigung finden.

14 Wissenschaft und Forschung

14.1 Mentoren – Beratung nur auf gleicher Augenhöhe

Um den Studienerfolg junger Menschen zu verbessern, werden den Studenten an brandenburgischen Hochschulen Mentoren zugeordnet. Deren Aufgabe besteht darin, bei der Studiengestaltung, der zeitlichen Planung, bzw. der inhaltlichen Ausrichtung beratend zu unterstützen. Ein Hochschullehrer trat an uns heran, um zu klären, ob er zur Ausübung seiner Mentorenfunktion vom Hochschulprüfungsamt die Notenliste für von ihm zu betreuende Studenten erhalten dürfe.

Er begründete die Notwendigkeit damit, dass sich ein Beratungsbedarf aus einer kritischen Notensituation ergäbe und dass regelmäßig davon auszugehen sei, dass insbesondere jüngere Studenten den Bedarf zur rechtzeitigen Beratung nicht selbst erkennen.

Diese Auffassung vermochten wir nicht zu teilen. Zum einen fehlt es an der rechtlichen Grundlage, um die Noten aus dem Prüfungsamt herauszugeben, zum anderen entspricht das Bild von den Studenten hier offensichtlich nicht dem von einem erwachsenen, an die Wissenschaft heranzuführenden jungen Menschen.

Das Mentoring können nach § 20 Brandenburgischen Hochschulgesetz Hochschullehrer, akademische Mitarbeiter sowie geeignete wissenschaftliche oder künstlerische Hilfskräfte oder Tutoren übernehmen. Alle gelten als Fachpersonen, die Studenten auf dem Weg der akademischen Ausbildung weiterhelfen können.

Bei den infrage stehenden Angaben zum Noten- und Prüfungsverlauf handelt es sich um sensitive personenbezogene Daten der betroffenen Studenten. Um sie weitergeben zu können, bedarf es einer ausreichenden rechtlichen Grundlage, die sich nicht aus den Vorschriften des Hochschulrechts ableiten lässt.

Darüber hinaus basiert das Modell des Mentorings auf einem Vertrauensverhältnis. Die Preisgabe von personenbezogenen Daten beruht dabei auf dem Prinzip der freiwilligen Einwilligung. Das Mentoring ist nicht mit einer verpflichtenden Studienberatung zu vergleichen, in deren Rahmen bindende Auflagen erteilt werden können. Aus diesem Grunde ist auch nicht von einem unbeabsichtigten Fehlen einer Befugnis zur Weitergabe von Prüfungsdaten auszugehen. Benötigen Mentoren Angaben zum Leistungsstand der von ihnen betreuten Studenten, müssen sie diese selbst danach fragen.

Ein wirksames Mentoring setzt eine Vertrauensbasis voraus. Ein einseitiger Informationsvorsprung aufseiten der Mentoren führt möglicherweise zur Ablehnung von an sich sinnvollen Betreuungsangeboten. Studenten müssen ihrem Gegenüber auf gleicher Augenhöhe begegnen können.

14.2 Ist eine Belohnung für die Teilnahme an wissenschaftlichen Umfragen zulässig?

Initiatoren von Umfragen zu Forschungszwecken begehren oft personenbezogene Daten und locken Betroffene zum Teil mit Belohnungen, damit Auskünfte erteilt werden. Fraglich ist, ob damit trotz Freiwilligkeit der Teilnahme unerlaubt Zwang ausgeübt wird.

Häufig werden Schreiben, mit welchen um die Teilnahme an einer Studie gebeten wird, nicht beantwortet und wandern unbeachtet in den Papierkorb. Um auf eine größere Rückläuferquote zu erreichen, stellen einige Initiatoren von Umfragen eine Belohnung für die Beteiligung in Aussicht.

Die Preisgabe der eigenen personenbezogenen Daten erfolgt entweder freiwillig oder aufgrund einer gesetzlichen Verpflichtung. Nur ausnahmsweise, etwa wenn ein förmlicher Heranziehungsbescheid zur Beantwortung von Fragen zur Erhebung von Daten für eine amtliche Statistik vorliegt, besteht eine gesetzliche Pflicht zur Beantwortung eines Fragebogens.[55] Im Übrigen ist die Teilnahme an Meinungsumfragen, Markterhebungen oder eben Forschungsvorhaben selbstverständlich freiwillig. Die Datenerhebung ist dann nur auf der Basis einer Einwilligung möglich. Von einer Freiwilligkeit ist auch dann auszugehen, wenn für die Preisgabe der eigenen Daten eine Gegenleistung versprochen wird. Es steht im Belieben des Betroffenen, so zu handeln und ist als eine Möglichkeit der Ausübung des Grundrechts auf informationelle Selbstbestimmung zu begreifen.

Die Grenze ist jedoch dort erreicht, wo die Gestaltung des Fragebogens oder die Art und Weise des Herantretens an die Befragten suggeriert, dass eine Pflicht zur Teilnahme besteht. Vielmehr muss deutlich auf die Freiwilligkeit

[55] siehe B 19

hingewiesen werden. Auch ist es nicht zulässig, auf diesem Weg Auskünfte über Dritte in Erfahrung zu bringen. Die Befragten dürfen nur Angaben über ihre eigenen Verhältnisse machen. Zudem muss deutlich zu erkennen sein, wer zu welchem Zweck Daten erheben möchte.

Auch wenn es eine Belohnung für die Preisgabe der eigenen Information gibt, steht die Beantwortung von Fragen im Belieben der Teilnehmer an einer wissenschaftlichen Umfrage. Jeder muss selbst entscheiden, welchen Wert er dem Schutz der eigenen Daten zumisst.

15 Telekommunikation und Medien

15.1 Einsatz von Google Analytics durch Krankenhäuser

Webseiten von Krankenhäusern oder Rehakliniken werden überdurchschnittlich häufig von Personen angesehen, die aufgrund eigener gesundheitlicher Beeinträchtigungen Informationen über Krankheiten und Behandlungsmöglichkeiten suchen. Die Verarbeitung personenbezogener Daten im Rahmen von Reichweitenanalysen durch Betreiber solcher Webseiten muss daher im besonderen Maße den Anforderungen des Datenschutzes genügen.

Google Analytics wird auf sehr vielen Webseiten zur Reichweitenmessung eingesetzt, beinhaltet allerdings datenschutzrechtlich problematische Verarbeitungsprozesse, da in der Standardeinstellung personenbezogene Daten wie IP-Adressen der Webseitenbesucher an das Unternehmen Google in die USA übermittelt und in die Auswertung einbezogen werden. Es besteht für Webseitenbetreiber allerdings die Möglichkeit, Google Analytics so zu verwenden, dass lediglich anonymisierte Daten in die Messung einfließen und zudem Nutzern das Recht eingeräumt wird, einer Erfassung ihrer Daten durch das Setzen von Browsereinstellungen zu widersprechen. Wenn eine Webseite das Reichweitenmesswerkzeug auf diese Weise einsetzt, wird den Regeln des Datenschutzes, wie sie im Telemediengesetz festgelegt sind, Genüge getan. Darüber hinaus handelt es sich bei der Anonymisierung der IP-Adressen durch Google um eine Auftragsdatenverarbeitung, sodass die verantwortlichen Stellen einen entsprechenden Vertrag mit diesem Unternehmen abschließen müssen.[56] Aufgrund dessen Geschäftspraktiken steht diese Möglichkeit jedoch nur den nicht öffentlichen Stellen zur Verfügung.

Im Berichtszeitraum haben wir die Webseiten von Krankenhäusern und Rehabilitationskliniken mit Sitz im Land Brandenburg auf den rechtskonfor-

[56] Tätigkeitsbericht 2010/2011, A 3.2

men Einsatz von Google Analytics geprüft. Insgesamt testeten wir 57 Internetangebote. Davon hatten 19 Seiten, betrieben von 13 Kliniken bzw. Klinikgesellschaften, Google Analytics im Einsatz. Sechs der verantwortlichen Stellen hatten die technischen Vorgaben zur IP-Anonymisierung, zur korrekten Datenschutzerklärung und zur Widerspruchslösung richtig umgesetzt. Bei einer Klinik war zwar die IP-Anonymisierung realisiert worden, jedoch fehlten Hinweise zur Möglichkeit des Widerspruchs in der Datenschutzerklärung. Sechs weitere Stellen wiederum mussten wir auffordern, die IP-Anonymisierung vorzusehen und die Datenschutzerklärungen nachzubessern. Zudem verlangten wir von allen verantwortlichen Stellen, uns den Vertrag zur Auftragsdatenverarbeitung mit Google zu übersenden.

Im Ergebnis konnten wir festhalten, dass gegebenenfalls erforderliche Nachbesserungen vorgenommen bzw. die Verträge zur Auftragsdatenverarbeitung geschlossen wurden, sodass schließlich die Reichweitenmessung mittels Google Analytics datenschutzgerecht erfolgte.

Bemerkenswert war allerdings, dass nach unserer Kontaktaufnahme sieben der 13 Stellen Google Analytics sofort abgeschaltet haben. Dies wurde häufig damit begründet, dass die verantwortliche Stelle dieses Werkzeug gar nicht benötigen würde. Teilweise wussten die Stellen noch nicht einmal, dass sie Google Analytics einsetzen, weil dieses Tool beispielsweise standardmäßig von beauftragten Webentwicklern – ggf. auch ohne Rücksprache – aktiviert worden oder weil es in Vergessenheit geraten war. Dies zeigt, wie notwendig eine kontinuierliche Aufklärung zum Thema Datenschutz und Reichweitenmessung im Internet nach wie vor ist.

Die Kontrolle der Webseiten von Krankenhäusern und Rehakliniken hat im Ergebnis eine Verbesserung des Datenschutzes durch Abschaltung der Reichweitenmessung oder durch Umsetzung datenschutzgerechter Einstellungen erbracht.

15.2 Zulässigkeit einer Personensuchmaschine

Soll die Weiterverwendung von Daten, die ohne Zugangsbeschränkung im Internet verfügbar sind, zu neuen Zwecken erfolgen, ist dies oft umstritten. Grundsätzlich können allgemein zugängliche Daten unter vereinfachten Bedingungen verarbeitet werden. Die Verknüpfung solcher Daten erlaubt jedoch oft Einblicke in die Verhältnisse von Betroffenen, die sich aus den einzelnen Daten nicht gewinnen ließen. Der Betrieb eines entsprechenden Dienstes bedarf daher besonderer Sensibilität hinsichtlich der Zulässigkeit der Speicherung und der Sicherstellung der Rechte Betroffener. Die Landesbeauftragte befindet sich in der datenschutzrechtlichen Bewertung eines kommerziellen Anbieters von Personenprofilen aus verknüpften, überwiegend allgemein zugänglichen Daten.

Im Berichtszeitraum erreichte uns eine große Anzahl von Beschwerden aus dem gesamten Bundesgebiet zu einer von einem märkischen Unternehmen betriebenen Personensuchmaschine. Diese erstellt durch automatisierte Zusammenführung von Daten aus verschiedenen Online-Quellen nach Namen geordnete Profile von Betroffenen. Auf der Webseite werden auch Insolvenzdaten aus dem vom Land Nordrhein-Westfalen zentral nach der Insolvenzbekanntmachungsverordnung betriebenen Portal[57] gegen Entgelt zum Download bereitgehalten.

Die Frage der Zulässigkeit einer solchen Personensuchmaschine ist durch die Landesbeauftragte zunächst grundsätzlich begutachtet worden. Soweit ausschließlich allgemein zugängliche Daten verarbeitet werden, ist dies gemäß § 29 Abs. 1 S. 1 Nr. 2 Bundesdatenschutzgesetz (BDSG) in der Regel zulässig, es sei denn, dass die schutzwürdigen Interessen des Betroffenen offensichtlich überwiegen. Insofern war ein großer Teil der Beschwerden erfolglos.

Zweifel an der allgemeinen Zugänglichkeit können jedoch im Einzelfall bestehen, wenn personenbezogene Daten zu Profilen verknüpft werden und damit Einblicke in die sachlichen und persönlichen Verhältnisse möglich sind, die sich aus den isolierten Einzeldaten nicht ergeben. Gleiches kann auch auftreten, wenn Internetnutzer unbewusst Daten der Weiterverwendung zu neuen Zwecken öffnen bzw. diese Weitergabe durch die Plattformen erfolgt, ohne dass Betroffene hierauf Einfluss nehmen können.

Die Landesbeauftragte hatte in Einzelfällen Löschansprüche von Betroffenen wegen Zeitablaufs oder wegen ihrer überwiegenden schutzwürdigen Interessen zu prüfen. Für bestimmte Fallgruppen (z. B. nachweisbare Gefahr für Leib und Leben) herrscht Einvernehmen mit dem Betreiber, dass eine Lö-

[57] https://www.insolvenzbekanntmachungen.de

schung regelmäßig auch vor Ablauf gesetzlicher Fristen (§ 35 Abs. 2 S. 2 Nr. 4 BDSG) vorzunehmen ist. Vor dem Hintergrund der einschneidenden Folgen für die Betroffenen wirkt die Landesbeauftragte kontinuierlich gegenüber dem Betreiber der Personensuchmaschine auf die gewissenhafte Prüfung von Löschungsverlangen hin.

Die Landesbeauftragte wies den Betreiber wiederholt auf seine datenschutzrechtliche Verantwortlichkeit hin. Auch wenn einzelne Prozesse vollständig automatisch ablaufen und ihre konkreten Ergebnisse nicht vorhersehbar sind, bleibt die Stelle, die solche Maßnahmen in Gang setzt, datenschutzrechtlich verantwortlich. Der Geschäftsbetrieb muss schließlich so eingerichtet sein, dass der Betreiber seinen datenschutzrechtlichen Pflichten jederzeit nachkommen kann. Er muss Benachrichtigungs- und Auskunftspflichten einhalten und gewährleisten, dass im Einzelfall bestehende Löschansprüche durchgesetzt werden können.

Eine Gefahr für die Persönlichkeitsrechte Betroffener kann auch dann gegeben sein, wenn die Einzeldaten im Internet frei verfügbar sind. Wer eine Webseite betreibt, in der Einzeldaten automatisiert zu Profilen zusammengefasst werden, muss sich seiner datenschutzrechtlichen Verantwortung bewusst sein.

15.3 Grenzen des Datenschutzes I: Verlinkung bei Facebook

Ein Nutzer des sozialen Netzwerks Facebook beschwerte sich darüber, dass sein Name durch die Verlinkung seines Profils auf den Seiten eines „Freundes“ angezeigt wird. Er fühlte sich in seinen Persönlichkeitsrechten verletzt.

Bei Facebook besteht die Möglichkeit, durch Erwähnung des Namens eines „Freundes“ dessen Profil auf der eigenen Profilseite zu verlinken und es dadurch auffindbar zu machen. Eine generelle vorherige Zustimmung des Erwähnten ist nicht vorgesehen. Die einzigen Möglichkeiten, die Verlinkung zu verhindern, bestehen darin, den die Verknüpfung vornehmenden Nutzer entweder um Unterlassung zu bitten oder ihn zu blockieren. Hiergegen richtete sich die Beschwerde des Betroffenen, die Facebook selbst mit Hinweis auf die eigenen Nutzungsbedingungen zurückgewiesen hatte.

Die Landesbeauftragte ist örtlich für Beschwerden gegen Facebook nicht zuständig. Sie werden daher grundsätzlich an den Hamburgischen Beauftragten für Datenschutz und Informationsfreiheit abgegeben. Im vorliegenden Fall war schon nicht ganz eindeutig, inwieweit das Datenschutzrecht überhaupt anwendbar ist. Gemäß § 1 Abs. 2 Nr. 3 des Bundesdatenschutzgesetzes (BDSG) gilt das Datenschutzrecht nämlich nicht, wenn die Datenverarbeitung

ausschließlich für persönliche oder familiäre Tätigkeiten erfolgt. Vorliegend geschah die Verlinkung durch eine Privatperson zu persönlichen Zwecken; Facebook stellte hierzu lediglich die technischen Möglichkeiten zur Verfügung. Dennoch baten wir die Hamburger Kollegen um Prüfung. Diese verneinten schließlich einen Datenschutzverstoß auch in der Sache, da ein Interesse Dritter – des Facebook-Nutzers, der die Verknüpfung zur Seite des Petenten herstellte – an der Nutzung der Daten zur Markierung (§ 28 Abs. 1 S. 1 Nr. 2 BDSG) bestehe. Dem stehen die Interessen des Betroffenen regelmäßig nicht entgegen. Die Nutzer eines sozialen Netzwerks, die sich freiwillig daran beteiligen und die „Spielregeln“ akzeptiert haben, müssen es hinnehmen, dass ihre Daten im rechtlich zulässigen Rahmen von anderen Mitgliedern des sozialen Netzwerks genutzt werden. Jeder muss selbst entscheiden, ob dieser Preis es ihm wert ist, Teil des Netzwerks zu werden. Die Mitgliedschaft ist insofern nicht umsonst, sondern kostet die persönlichen Daten der Betroffenen.

Wer an einem sozialen Netzwerk teilnimmt, muss es hinnehmen, dass Andere seine Daten in einem rechtlich zulässigen Rahmen nutzen. Wer dies nicht möchte, muss seine Mitgliedschaft überdenken.

15.4 Grenzen des Datenschutzes II: Was gilt nach dem Tode?

Im Berichtszeitraum hatte sich die Landesbeauftragte mit der Anfrage einer Gemeinde hinsichtlich eines Weblogs (Blog) zu beschäftigen, welcher teilweise sehr persönliche Lebenssachverhalte einer inzwischen verstorbenen Mitarbeiterin der Verwaltung verbreitete.

Das im Volkszählungsurteil des Bundesverfassungsgerichts postulierte Recht auf informationelle Selbstbestimmung ist Teil des allgemeinen Persönlichkeitsrechts. Geschützt wird die Befugnis des Einzelnen, grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen. Es ist – wie die meisten Grundrechte – als Abwehrrecht gegen den Staat konstruiert, richtet aber auch im Wege der sog. mittelbaren Drittwirkung eine objektive Wertordnung auf, sodass es, insbesondere bei Interessenabwägungen, auch in Rechtsbeziehungen zwischen Privaten zu berücksichtigen und geeignet ist, entgegenstehenden Rechten Grenzen zu setzen.

Da jedoch schon der Bezeichnung nach die Selbstbestimmung den Wesensgehalt des genannten Grundrechts ausmacht, sind Sachverhalte, bei denen der Grundrechtsinhaber verstorben ist, nach ganz allgemeiner Ansicht nicht unter dem Aspekt der informationellen Selbstbestimmung zu beurteilen. Dies hat die grundsätzliche Unanwendbarkeit der Datenschutzgesetze auf derartige Sachverhalte zur Folge. Auf Verstorbene sind nur noch einzelne Normen

mit datenschutzrechtlichem Charakter anwendbar, deren postmortale Geltung besonders angeordnet ist (so z. B. die Bestattungsdatenschutzverordnung oder die ärztliche Schweigepflicht gemäß § 203 Strafgesetzbuch). Eine solche spezielle Vorschrift bestand vorliegend nicht. Daher war die Zuständigkeit der Landesbeauftragten nicht gegeben.

Wir haben die anfragende Gemeinde darauf hingewiesen, dass vorliegend nur sog. postmortale Persönlichkeitsrechte als verletzt in Betracht kommen, die Gemeinde jedoch nicht Inhaberin dieser Ansprüche ist und diese daher nicht, etwa in Form eines zivilrechtlichen Unterlassungsanspruchs, geltend machen kann. Zur Geltendmachung sind vielmehr ausschließlich Angehörige der Verstorbenen befugt.

Das Recht auf informationelle Selbstbestimmung benötigt einen handlungsfähigen Grundrechtsträger. Daher sind insbesondere die Datenschutzgesetze von Bund und Ländern auf Verstorbene unanwendbar. In der Konsequenz ist eine Zuständigkeit der Landesbeauftragten in solchen Fällen nicht gegeben.

15.5 Orientierungshilfe zu Smart-TV-Diensten

Die Möglichkeit, sich mit dem Internet zu verbinden und darüber Dienste zu nutzen und Angebote zu beziehen, ist nun auch zum Standard in aktuellen Fernsehgeräten geworden. Allerdings wird dadurch die bisherige Anonymität des Fernsehens gefährdet. Die Datenschutzbehörden haben in einer Orientierungshilfe die aufgeworfenen datenschutzrechtlichen Fragestellungen erörtert und Anforderungen abgeleitet.

Fernsehgeräte erhielten in den letzten Jahren immer mehr Funktionen und Schnittstellen, sodass man mit aktuellen Geräten weit mehr machen kann als nur fernzusehen. Man kann auf ihnen z. B. Fotos und Videos von angeschlossenen USB-Geräten anzeigen, Musik abspielen und sich mit dem Internet verbinden. Insbesondere Letzteres lässt einen erheblich erweiterten Funktionsumfang zu, z. B. durch die Nutzung von Mediatheken der Sendeanstalten oder von Apps der Endgerätehersteller. Dadurch wird der Fernseher, der bisher lediglich ein Empfänger war, zu einem interaktiven Gerät, das einen Rückkanal zum Internet aufbaut und darüber mit Fernsehsendern, Herstellern und anderen Dritten kommuniziert. Datenschutzrechtlich problematisch daran ist jedoch, dass durch diesen Rückkanal die mit herkömmlichen Geräten beim Fernsehen gewahrte Anonymität nicht mehr gesichert ist, da über die gesendeten IP-Adressen und ggf. Cookies eine Zuordnung zu einer konkreten Person bzw. einem Haushalt möglich wird. Außerdem gerät das Fernsehen damit grundsätzlich in den Rechtsbereich des Telemediengesetzes und dessen datenschutzrechtliche Bestimmungen. Fernsehsender, die Angebote über das Internet bereitstellen, aber auch die Hersteller, die z. B.

App-Angebote unterbreiten, müssen daher die Nutzer spätestens zu Beginn des Nutzungsvorgangs umfassend über die Datenerhebung und -verwendung informieren. Personenbeziehbare Daten von Nutzern dürfen nur verwendet werden, sofern dies zur Erbringung der Dienste oder zu Abrechnungszwecken erforderlich ist. Profilbildung darf ausschließlich pseudonym und unter Einräumung und technisch effektiver Umsetzung eines Widerspruchsrechts für Nutzer erfolgen. Insbesondere ist auch beim Smart-TV zu gewährleisten, dass anonymes Fernsehen weiter möglich bleibt.

Um Gerätehersteller, Fernsehsender und andere Anbieter im Zusammenhang mit Smart-TV bei der Umsetzung der Datenschutzanforderungen zu unterstützen, haben die unabhängigen Datenschutzbehörden des Bundes und der Länder eine Orientierungshilfe[58] erstellt, die ausführlich die datenschutzrechtlichen Rahmenbedingungen, die erforderlichen technischen und organisatorischen Maßnahmen und die konkreten Anforderungen an Anbieter von Smart-TV-Diensten erläutert. Besonderes Augenmerk wird in der Orientierungshilfe auf die Bereitstellung und Nutzung des HbbTV-Standards gelegt. Mit Hilfe dieses Standards können Sendeanstalten Zusatzangebote über das Internet bereitstellen und mittels Einblendung eines sog. Red Button im unteren Bildschirmbereich signalisieren, dass Nutzer durch Drücken des roten Knopfes auf der TV-Fernbedienung Zugang zu diesen Angeboten haben. Problematisch hieran ist, dass bereits bei Einschalten eines Fernsehprogramms über eine mit dem Rundfunksignal versandte Internetadresse (URL) sofort ohne weitere Nutzeraktivität eine Internetverbindung zu dem Server des HbbTV-Anbieters initiiert und dabei zumindest die IP-Adresse des jeweiligen Nutzeranschlusses übertragen wird. Allerdings hat zu diesem frühen Zeitpunkt der Nutzer noch gar keine Einwilligungserklärung dafür abgeben können. Diese ist aber erforderlich, da in der Regel die Anwahl eines Fernsehsenders auf dem TV-Gerät nur bedeutet, dass das Fernsehprogramm dieses Senders empfangen, nicht aber, dass eine sofortige Internetverbindung mit dem Server der Sendeanstalt hergestellt werden soll. Wie in der Orientierungshilfe ausgeführt wird, ist es daher erforderlich, dass Sendeanstalten ihre Datenverarbeitungsprozesse so umgestalten, dass erst bei Drücken des Red Button eine Internetverbindung hergestellt wird und der Nutzer dann leichten Zugang zu allgemein verständlichen Informationen über die Verarbeitung seiner Nutzungsdaten und sein Widerspruchsrecht gegen die Erstellung pseudonymer Nutzungsprofile erhält.

Weitere wichtige Inhalte der Orientierungshilfe sind Datenschutzhinweise bezüglich Software-Updates, Analyse des Nutzerverhaltens, Umgang mit Gerätekennungen, Kameras und Mikrofonen und Verwaltung von Cookies. Wir empfehlen allen Geräteherstellern, Sendeanstalten, App-Anbietern, Portalbetreibern und sonstigen verantwortlichen Stellen im Umfeld von

[58] http://www.lda.brandenburg.de

Smart-TV, die Orientierungshilfe genau zu studieren und die Anforderungen und Hinweise für die in der jeweiligen eigenen Verantwortung stehende Hard- und Software umzusetzen.

Alle Akteure im Bereich Smart-TV müssen sich über die Risiken für das informationelle Selbstbestimmungsrecht und ihre jeweilige datenschutzrechtliche Verantwortlichkeit bewusst sein. Insbesondere die Sendeanstalten müssen Wege zur rechtzeitigen Nutzerinformation und -einwilligung finden. Die Orientierungshilfe Smart-TV unterstützt hierbei mit Erläuterungen und Hilfestellungen.

16 Bauen, Wohnen und Verkehr

16.1 Kontrolle eines Wohnungsunternehmens offenbarte Mängel

Das Bundesdatenschutzgesetz erfordert zum Nachweis bestimmter Aktivitäten die Schriftform. So ist z. B. die Bestellung des betrieblichen Datenschutzbeauftragten schriftlich vorzunehmen. Auch Verträge über eine Datenverarbeitung im Auftrag sind schriftlich zu schließen, wobei das Gesetz Mindestvertragsinhalte vorgibt. Eine im Berichtszeitraum durchgeführte Kontrolle eines märkischen Wohnungsunternehmens zeigte in diesen Punkten Mängel.

Schwerpunkt der Prüfung in dem Wohnungsunternehmen waren die Erhebung, Verarbeitung und Nutzung von personenbezogenen Daten zum Zwecke der Begründung, Durchführung und Beendigung von Mietverhältnissen. Routinemäßig wurden daneben auch formale Aspekte der Einhaltung des Bundesdatenschutzgesetzes (BDSG) geprüft, wie etwa die Bestellung des betrieblichen Datenschutzbeauftragten sowie die Gestaltung von Verträgen zur Datenverarbeitung im Auftrag.

Unternehmen müssen gem. § 4 f Abs. 1 BDSG einen Beauftragten für den Datenschutz bestellen, wenn sie personenbezogene Daten automatisiert verarbeiten und hiermit in der Regel mindestens 10 Personen beschäftigt sind. Das Gleiche gilt, wenn personenbezogene Daten auf andere Weise (z. B. manuell) erhoben, verarbeitet oder genutzt werden und damit in der Regel mindestens 20 Personen beschäftigt sind. Die Bestellung des betrieblichen Datenschutzbeauftragten muss schriftlich erfolgen.

Im konkreten Fall hatte das Wohnungsunternehmen zunächst die gesetzlichen Anforderungen zur Bestellung eines betrieblichen Datenschutzbeauf-

tragten erfüllt. Es versäumte allerdings, nachdem der bisherige Inhaber von dieser Funktion entbunden wurde, schriftlich einen Nachfolger zu bestellen. Insgesamt war die Position über einen Zeitraum von 13 Monaten vakant.

Verantwortliche Stellen, die selbst oder im Auftrag personenbezogene Daten verarbeiten, haben hierbei die datenschutzrechtlichen Anforderungen zu erfüllen. Dies gilt auch für die letzte Phase der Datenverarbeitung, das Löschen von Daten bzw. das Vernichten von Informationsträgern (wie Festplatten, Magnetbändern, Disketten, Filmmaterial oder Papier). Gem. § 35 BDSG sind personenbezogene Daten, wenn sie für eigene Zwecke verarbeitet werden, zu löschen, sobald ihre Kenntnis für die Erfüllung des Zwecks der Speicherung nicht mehr erforderlich ist. Wird mit der Datenlöschung bzw. Vernichtung von Informationsträgern ein Dienstleister beauftragt, sind die gesetzlichen Anforderungen zur Datenverarbeitung im Auftrag gem. § 11 BDSG zu beachten.

Das kontrollierte Wohnungsunternehmen hatte persönliche Daten von Mietbewerbern zunächst in sog. Interessentenbögen auf Papier erhoben, die Bögen dann eingescannt und die Daten elektronisch gespeichert. Sämtliche Papierunterlagen (außer Mietverträge) wurden anschließend bis zur Entsorgung in verschlossenen Behältnissen zwischengelagert. Mit der Entsorgung selbst wurde eine darauf spezialisierte Firma beauftragt. Allerdings versäumte es das Wohnungsunternehmen, hierfür einen Vertrag zur Verarbeitung von Daten im Auftrag abzuschließen, der den Anforderungen von § 11 BDSG in vollem Umfang entspricht.

Zwar verpflichtete sich die Entsorgungsfirma als Auftragnehmerin in ihren Allgemeinen Geschäftsbedingungen, die Dienstleistung im Einklang mit den gesetzlichen Datenschutzbestimmungen zu erbringen und die für die Auftragsdatenverarbeitung gesetzlich bestimmten Voraussetzungen für Auftragnehmer, insbesondere § 11 Abs. 3 bis 5 BDSG, zu erfüllen. Dies ersetzte aber nicht einen Vertrag über die Datenverarbeitung im Auftrag, da wesentliche Auftragsbestandteile, die gem. § 11 Abs. 2 BDSG schriftlich festzulegen sind, so nicht fixiert wurden. Das betraf beispielsweise Angaben zur Art der Daten und zum Kreis der Betroffenen, um eine geeignete Sicherheitsstufe für die Vernichtung der Papierunterlagen zu bestimmen. Gleichfalls fehlte es an konkreten Ausführungen zur Übernahme der Datenträger, zum sicheren Transport und zum eigentlichen Vorgang der Vernichtung bei der Entsorgungsfirma. Weiterhin wurden keine Angaben zu internen Kontrollen beim Auftragnehmer bzw. widersprüchliche Aussagen zur Einbeziehung von Unterauftragnehmern getroffen.

Wegen der fehlenden schriftlichen Bestellung eines betrieblichen Datenschutzbeauftragten sowie wegen der Mängel bei der schriftlichen Erteilung des Auftrages an die Entsorgungsfirma zur Vernichtung von Papierunterlagen

wurde gegen die Verantwortlichen des Wohnungsunternehmens ein Ordnungswidrigkeitenverfahren eingeleitet.[59]

Durch die gesetzlich vorgeschriebene Verwendung der Schriftform werden die Nachweisbarkeit und die Verbindlichkeit bestimmter Handlungen datenschutzrechtlich verantwortlicher Stellen gewährleistet. Im Falle einer Datenverarbeitung im Auftrag schafft sie Rechtssicherheit zwischen Auftraggeber und Auftragnehmer. Das Fehlen der gesetzlich vorgeschriebenen Schriftform ist eine Ordnungswidrigkeit, die mit einer Geldbuße geahndet werden kann.

16.2 Leistungsbetrug – Übermittlung von Sozialdaten durch Wohngeldstelle an Ermittlungsbehörden

Immer wieder wenden sich Sozialleistungsträger mit der Frage an uns, ob sie personenbezogene Daten von Leistungsempfängern beim Verdacht auf Leistungsmissbrauch an die Polizei oder Staatsanwaltschaft weitergeben dürfen.

In einem konkreten Fall teilte uns eine Wohngeldbehörde mit, dass gegen einen Empfänger von Wohngeld der Verdacht des Leistungsbetruges bestehe. Die Behörde beabsichtigte, Strafanzeige zu erstatten. Dies wäre mit der Offenbarung von Sozialdaten des Betroffenen verbunden gewesen. Die Frage nach der Zulässigkeit dieser Datenübermittlung haben wir wie folgt beantwortet.

Das vom Bundesverfassungsgericht aus dem allgemeinen Persönlichkeitsrecht abgeleitete Recht auf informationelle Selbstbestimmung im Bereich der Sozialverwaltung findet seinen Niederschlag im Schutz des Sozialgeheimnisses gem. § 35 Erstes Buch Sozialgesetzbuch. Eine Durchbrechung dieser Geheimhaltungspflicht ist nur unter bestimmten Voraussetzungen erlaubt. Das Erheben, das Verarbeiten – hierzu gehört auch die Bekanntgabe an Dritte – und das Nutzen der Sozialdaten ist nur dann zulässig, wenn eine Rechtsvorschrift dies bestimmt oder der Betroffene eingewilligt hat.

In den seltensten Fällen wird der Betroffene in die Datenübermittlung zum Zwecke der Strafverfolgung gegen seine Person einwilligen. Dies ist gem. § 67 b Abs. 1 Zehntes Buch Sozialgesetzbuch (SGB X) aber auch nicht notwendig, wenn die Behörde die Weitergabe auf eine Rechtsnorm nach §§ 68 bis 77 SGB X oder auf eine andere Rechtsvorschrift im Sozialgesetzbuch stützen kann.

Eine solche Datenübermittlung ist hier nach § 69 Abs. 1 Nr. 1, 2. Alternative SGB X erlaubt. Diese Norm setzt voraus, dass die Übermittlung der in Rede

[59] siehe B 20.1

stehenden Sozialdaten für die Erfüllung einer gesetzlichen Aufgabe der übermittelnden Stelle erforderlich ist, sie ihre Aufgaben also ohne die Information nicht erfüllen kann. Das Wohngeld ist eine einkommensabhängige, steuerfinanzierte Sozialleistung. Insofern gehört es zu den Aufgaben der Wohngeldbehörde, diese Mittel entsprechend den gesetzlichen Bestimmungen zu vergeben. In diesem Zusammenhang ist der Sozialleistungsträger auch verpflichtet, Schäden für die Solidargemeinschaft abzuwenden.

Eine Übermittlung von Sozialdaten an die Polizei oder Staatsanwaltschaft aufgrund eines Verdachtes auf Leistungsbetrug ist für die Erfüllung der gesetzlichen Aufgaben des Sozialleistungsträgers, der selbst von der Straftat betroffen ist, nach dem Sozialgesetzbuch erforderlich und somit zulässig.

16.3 Einsicht in Schallschutzgutachten am neuen Flughafen

Die Flughafen Berlin Brandenburg GmbH (FBB) ist als Betreiberin verantwortlich für den Schallschutz in den voraussichtlich vom Fluglärm des künftigen Flughafens Berlin Brandenburg Willy Brandt besonders betroffenen Häusern bzw. Wohnungen. Sie ließ vor Ort Schallschutzgutachten erstellen, die als Grundlage für die Festlegung der zu treffenden Schallschutzmaßnahmen dienten. Zugang zu den Messdaten und weiteren Angaben aus dem Gutachten gewährte die Betreiberin den betroffenen Eigentümern zum Teil aber erst, nachdem deren Ansprüche bereits ermittelt worden waren. Dann allerdings wurden sämtliche Informationen offengelegt.

Im Ergebnis der Messungen vor Ort erstellten Ingenieurbüros im Auftrag der FBB schalltechnische Objektbeurteilungen, die sowohl Bestandteile der Grundstücke und Gebäude erfassten als auch die Ergebnisse schalltechnischer Messungen enthielten. Mittels eines Leistungsverzeichnisses wurden auf dieser Grundlage die Kosten für die erforderlichen Schallschutzmaßnahmen ermittelt. Allerdings sieht der Planfeststellungsbeschluss für den neuen Großflughafen vor, dass die Flughafen Berlin Brandenburg GmbH die Kosten für bauliche Maßnahmen zur Verbesserung des Schallschutzes (also zum Beispiel der Einbau von Schallschutzfenstern) nur bis zu einer Höhe von 30 % des schallschutzbezogenen Verkehrswertes des Objektes erstattet. Liegen die Kosten darüber, erhält der Eigentümer eine Entschädigungszahlung in Höhe eben jener 30 % zur freien Verfügung. Soweit nicht auszuschließen ist, dass diese Grenze überschritten wird, erfolgt eine schallschutzbezogene Verkehrswertermittlung. Die Eigentümer haben die Wahl, ob sie ein eigenes Verkehrswertgutachten in Auftrag geben oder ein von der Flughafengesellschaft beauftragtes Unternehmen akzeptieren.

Die Betreiberin stellte den betroffenen Eigentümern bis zum Ergebnis der Wertermittlung keine Daten aus dem vorangegangenen Schallschutzgutachten zur Verfügung. Sie argumentierte, die Ermittlung solle unbeeinflusst erfolgen können. Die Erfüllung des Auskunftsanspruchs zu einem früheren Zeitpunkt stelle eine erhebliche Gefährdung ihres Geschäftszwecks – nämlich die objektive und unabhängige Feststellung des Verkehrswertes der voraussichtlich vom Fluglärm betroffenen Grundstücke – dar. Außerdem bedürfe es einer Konzentration des Verfahrens, das nicht durch auskunftsbedingte Zwischenschritte verzögert werden solle. Gleichzeitig sagte die Gesellschaft eine vollständige Auskunft nach Vorliegen des Verkehrswertgutachtens zu.

Als juristische Person des Privatrechts unterliegt die Flughafen Berlin Brandenburg GmbH den Vorschriften des Bundesdatenschutzgesetzes. Dessen § 34 gibt Betroffenen ein umfassendes Recht auf Auskunft zu den über ihre Person gespeicherten Daten. Als personenbezogene Daten im Sinne dieses Gesetzes gelten auch Angaben zu den sachlichen Verhältnissen einer natürlichen Person. Die hier in Rede stehenden Messergebnisse und Angaben zum Wohneigentum der Betroffenen fallen somit unter diese Begriffsbestimmung. Allerdings ermöglicht § 34 Abs. 7 i. V. m. § 33 Abs. 2 Nr. 7 b BDSG unter bestimmten Umständen, die Auskunft zu verweigern, etwa wenn ansonsten die Geschäftszwecke des Unternehmens erheblich gefährdet würden.

Die Flughafengesellschaft verweigerte die Auskunft nicht dauerhaft, sondern nur bis zum Abschluss der Verkehrswertermittlung. Ein Verstoß gegen die Auskunftspflicht nach § 34 BDSG ist aber lediglich dann anzunehmen, wenn eine Verzögerung der Auskunft die Qualität einer dauerhaften Verweigerung darstellen würde. Dies war hier nicht der Fall; eine Schlechterstellung der Betroffenen erfolgte durch diese Vorgehensweise nicht. Die Eigentümer konnten ohnehin erst nach Vorliegen aller Unterlagen, zu denen auch das Verkehrswertgutachten zählt, in weitere Verhandlungen mit der Flughafenbetreiberin eintreten oder mit rechtlichen Schritten gegen die Entscheidung vorgehen. Ebenfalls ist zu berücksichtigen, dass die Festlegung der Art und Höhe der Ansprüche auch der Umsetzung des öffentlich-rechtlichen Planfeststellungsbeschlusses dient. Die Auskunft wird darüber hinaus nicht willkürlich verweigert. Vielmehr ermöglicht die Bündelung der Auskunft über die Messdaten mit den im Zusammenhang mit dem Verkehrswert daraus folgenden Festlegungen der Ansprüche überhaupt erst eine konkrete inhaltliche Aussage.

Ein Auskunftsersuchen nach § 34 BDSG wird auch dann erfüllt, wenn ihm zu einem späteren Zeitpunkt vollständig entsprochen wird. Die Verzögerung darf weder willkürlich sein, noch ausschließlich der Arbeitserleichterung dienen oder die Rechtsstellung des Auskunftsersuchenden verschlechtern.

16.4 Sorglose Übermittlung von Daten an MPU-Gutachter

Die Landesbeauftragte wurde von einem Betroffenen gebeten, den Inhalt seiner Fahrerlaubnisakte sowie deren Übermittlung an verschiedene medizinisch-psychologische Begutachtungsstellen aus datenschutzrechtlicher Sicht zu prüfen. Aus seiner Sicht habe die Akte zum Zeitpunkt der Übermittlungen Dokumente und Angaben zu seiner Person enthalten, die schon hätten gelöscht sein müssten.

Nach dem Straßenverkehrsgesetz (StVG) dürfen die Fahrerlaubnisbehörden der amtlich anerkannten medizinisch-psychologischen Begutachtungsstelle die Daten übermitteln, die diese zur Erfüllung ihrer Aufgaben benötigen. Die weitere Ausgestaltung des Verfahrens ist in der Fahrerlaubnis-Verordnung (FeV) geregelt. § 11 Abs. 6 FeV bestimmt, dass die Fahrerlaubnisbehörde der untersuchenden Stelle mitteilt, welche Fragen im Hinblick auf die Eignung des Betroffenen zum Führen von Kraftfahrzeugen zu klären sind und übersendet ihr die vollständigen Unterlagen, soweit sie unter Beachtung der gesetzlichen Verwertungsverbote verwendet werden dürfen.

Gemäß § 28 StVG führt das Kraftfahrt-Bundesamt ein Fahreignungsregister. Es speichert dort Daten, die erforderlich sind, u. a. um die Eignung und Befähigung von Personen zum Führen von Kraftfahrzeugen zu beurteilen. Hierzu gehören auch Angaben zu rechtskräftigen Entscheidungen wegen bestimmter Ordnungswidrigkeiten. Diese Angaben dürfen an Stellen für Verwaltungsmaßnahmen nach diesem Gesetz übermittelt werden, z. B. Fahrerlaubnisbehörden. Nach § 29 Abs. 1 StVG werden Eintragungen von Verkehrsverstößen aus dem Fahreignungsregister nach dem Ablauf der hier bestimmten Fristen getilgt. Ist dort eine Eintragung gelöscht, so dürfen die Tat und die Entscheidung dem Betroffenen nicht mehr vorgehalten und nicht zu seinem Nachteil verwertet werden (§ 29 Abs. 7 Satz 1 StVG).

Insofern sind alle Informationen auch aus der Fahrerlaubnisakte zu entfernen, die einen Rückschluss auf die bereits getilgten Eintragungen zulassen. Hierfür genügt es nicht, lediglich die vom Kraftfahrt-Bundesamt übersandten Eintragungen sukzessive zu vernichten. Im vorliegenden Fall übersandte die Führerscheinstelle die komplette Akte des Betroffenen an die Gutachter. Sie enthielt auch einen Widerspruchsbescheid zu einem vorangegangenen Verfahren. In dessen Anlage waren bereits getilgte Ordnungswidrigkeiten aufgeführt. Auch diese Informationen hätten vernichtet werden müssen, gelangten auf diese Weise jedoch den Gutachtern zur Kenntnis. Ob sie tatsächlich zum Nachteil des Betroffenen genutzt wurden und in die Erstellung des Gutachtens eingeflossen sind, konnte zumindest nicht ausgeschlossen werden.

Nach § 2 Abs. 14 StVG dürfen die Fahrerlaubnisbehörden nur die erforderlichen Daten an die Gutachter übermitteln. § 11 Abs. 6 Satz 4 FeV konkreti-

siert diese Vorschrift insoweit, als danach die vollständigen Unterlagen nur, soweit sie unter Beachtung der gesetzlichen Verwertungsverbote verwendet werden dürfen, gemeint sind.

Ist eine Eintragung im Fahreignungsregister gelöscht, dürfen die Tat und die Entscheidung dem Betroffenen im Rahmen der Eignungsprüfung nicht mehr vorgehalten und nicht zu seinem Nachteil verwertet werden. Insofern sind alle Informationen aus der Fahrerlaubnisakte zu entfernen, die einen Rückschluss auf die bereits getilgten Eintragungen zulassen.

17 Videoüberwachung

17.1 Intransparente Videoüberwachung eines Vereinsgeländes

Ein Vereinsvorstand wollte das Vereinsgelände gegen Einbrüche schützen und bat die Landesbeauftragte um Mithilfe bei der gesetzeskonformen Installation einer Videoüberwachung. Nach einer Beratung durch uns wurde die Videoüberwachung in Betrieb genommen. Einige Monate später teilte uns ein Vereinsmitglied erstaunliche Umstände mit.

In dem Beratungsgespräch legte uns der Vereinsvorstand seine Planungen dar. Es sollten mehrere Einzelbereiche auf dem umzäunten Vereinsgelände erfasst werden, das lediglich von Vereinsmitgliedern betreten würde. Die Videoüberwachung sollte in einem transparenten Verfahren und in Abstimmung mit den Vereinsmitgliedern eingeführt werden (vorherige Information, schriftliches Einverständnis der Mitglieder, Ausweisen der Kameras durch Hinweisschilder).

Neun Monate nach Inbetriebnahme der Kameras wurde uns in einer Beschwerde mitgeteilt, dass die Vereinsmitglieder der Videoüberwachung weder mündlich noch schriftlich zugestimmt hatten. Mangels detaillierter Information und Hinweisschildern war auch nicht bekannt, was und wie genau mit den Kameras aufgezeichnet wurde. Zudem erfasste eine der Kameras einen außerhalb des umzäunten Geländes verlaufenden öffentlichen Weg. Gegenüber den Vereinsmitgliedern hatte sich der Vorstand pauschal darauf berufen, die Überwachungsmaßnahmen seien mit der Landesbeauftragten abgestimmt. Konfrontiert mit der Beschwerde vertrat der Vorstand die Auffassung, für die Zulässigkeit der Videoüberwachung sei nicht die Einwilligung eines jeden Vereinsmitglieds erforderlich. Er berief sich auf einen Beschluss des Vereinsvorstands, der den Betrieb der Kameras erwähnte.

Der Vorstand konnte sich indes zur Rechtfertigung der Videoüberwachung weder auf die Abstimmung mit der Landesbeauftragten noch auf den Vorstandsbeschluss stützen. Die datenschutzrechtliche Zulässigkeit einer Videoüberwachung durch nicht-öffentliche Stellen richtet sich allein nach den gesetzlichen Vorschriften des Bundesdatenschutzgesetzes (BDSG). Eine behördliche Genehmigung ist danach nicht vorgesehen. Aufgrund der uns nachträglich bekannt gewordenen Umstände war eine andere rechtliche Bewertung zu treffen als vorab im Beratungsgespräch. Im Einzelnen waren dabei folgende rechtliche Erwägungen zu beachten:

Wenn eine nicht öffentliche Stelle, wie ein Verein, durch eine Videoüberwachung personenbezogene Daten erhebt, verarbeitet oder nutzt, ist dies gemäß § 4 Abs. 1 BDSG nur zulässig, soweit das Bundesdatenschutzgesetz oder eine andere Rechtsvorschrift es erlaubt oder die Betroffenen eingewilligt haben.

Entgegen der vorab bei der Beratung besprochenen Planung hatte der Vereinsvorstand keine schriftlichen Einwilligungen aller Vereinsmitglieder eingeholt. Eine Einwilligung kann nur höchstpersönlich abgegeben werden. Ein Beschluss des Vorstands ist daher kein ausreichender Ersatz. Zudem wären für die Videoüberwachung des Weges außerhalb des umzäunten Vereinsgeländes Einwilligungen der Vereinsmitglieder nicht ausreichend gewesen. Dieser Weg wurde von der Öffentlichkeit genutzt, sodass von der Videoüberwachung außer den Vereinsmitgliedern auch andere Personen betroffen waren.

Als gesetzliche Grundlage für die Videoüberwachung auf dem umzäunten Vereinsgelände käme § 28 Abs. 1 Nr. 3 BDSG in Betracht. Nach dieser Vorschrift muss die Videoüberwachung zur Wahrung berechtigter Interessen für konkret festgelegte Zwecke erforderlich sein und es dürfen keine Anhaltspunkte bestehen, dass schutzwürdige Interessen der Betroffenen überwiegen. Jede einzelne Videoüberwachungsmaßnahme ist in Hinblick auf den jeweiligen Zweck, die konkreten Umstände und die Interessen der jeweils betroffenen Personen zu bewerten.

Die Zulässigkeit einer Videoüberwachung des öffentlich genutzten Weges hätte sich nur aus § 6 b BDSG ergeben können. Nach dieser Vorschrift ist eine Videoüberwachung öffentlich zugänglicher Räume zulässig, wenn sie zur Wahrnehmung des Hausrechts (Abs. 1 Nr. 2) oder zur Wahrnehmung berechtigter Interessen für konkret festgelegte Zwecke (Abs. 1 Nr. 3) erforderlich ist und keine Anhaltspunkte bestehen, dass schutzwürdige Interessen der Betroffenen überwiegen.

Für eine datenschutzrechtliche Beratung ist die Landesbeauftragte auf richtige und vollständige Angaben des Anfragenden angewiesen. Eine gesetzlich nicht zulässige Videoüberwachung kann durch eine Rücksprache mit unserer Dienststelle nicht „geheilt“ werden. Die Zulässigkeit richtet sich allein nach den gesetzlichen Vorschriften des Bundesdatenschutzgesetzes.

17.2 Der Bäcker hört mit

Ein Kunde einer Bäckerei informierte uns über eine Videoüberwachung im Verkaufsladen. Auf Nachfrage sei ihm bestätigt worden, dass die Kamera auch den Ton aufzeichnen könne.

Wir gingen der Datenschutzbeschwerde unverzüglich nach und führten eine unangekündigte Vor-Ort-Kontrolle durch. Bereits beim Betreten des Bäckerladens bemerkten wir eine Videokamera an der gegenüberliegenden Wand, die augenscheinlich den gesamten Raum erfasste.

Nachdem wir uns gegenüber dem Geschäftsinhaber ausgewiesen hatten, nannten wir ihm den Grund der unangekündigten datenschutzrechtlichen Prüfung und belehrten ihn über seine Auskunftspflicht gemäß § 38 Abs. 3 Bundesdatenschutzgesetz (BDSG). Eine Verweigerung der Auskunft ist nur bei solchen Fragen zulässig, deren Beantwortung ihn selbst oder einen seiner in § 383 Abs. 1 Nr. 1 bis 3 Zivilprozessordnung (ZPO) bezeichneten Angehörigen der Gefahr strafrechtlicher Verfolgung oder eines Verfahrens nach dem Gesetz über Ordnungswidrigkeiten aussetzen würde. In diesem Fall muss er sich ausdrücklich auf dieses spezielle Auskunftsverweigerungsrecht berufen. Die Belehrung war hier von besonderer Bedeutung, da möglicherweise eine Straftat hätte vorliegen können: Wenn der Ladeninhaber mit der Kamera tatsächlich auch den Ton unbefugt aufgezeichnet hätte, läge eine Verletzung der Vertraulichkeit des Wortes vor. Diese kann gemäß § 201 Strafgesetzbuch mit Freiheits- oder Geldstrafe geahndet werden.

Der Geschäftsinhaber zeigte bereitwillig die Aufnahmetechnik der Videoanlage, die sich über dem Verkaufsladen in seiner Wohnung befand. Es war sofort festzustellen, dass die Anlage allem Anschein nach nicht in Betrieb war, da sich der Netzstecker nicht in der Steckdose befand. Speichermedien waren nicht vorhanden. Somit wäre eine Ton- und Bildaufzeichnung auch nicht möglich gewesen, falls Strom angelegen hätte. Der Inhaber der Bäckerei erklärte, dass er die Anlage nur einmal kurz zu Testzwecken eingeschaltet hatte. Ansonsten sei sie bisher nicht in Betrieb gewesen. Die Gründe für die Anschaffung des Videoüberwachungssystems seien vermuteter Diebstahl an der Kasse sowie Einbrüche in der Nachbarschaft. Er wollte sich vor der Inbetriebnahme der Anlage noch über die rechtliche Zulässigkeit informieren.

Um festzustellen, ob die Videoüberwachungsanlage tatsächlich über eine funktionstüchtige Kamera mit Audiofunktion verfügte, wurde das System eingeschaltet. Auf dem Monitor war der gesamte Verkaufsraum zu erkennen. Sowohl Verkäuferin als auch Käufer waren deutlich sichtbar. Ebenso waren Stimmen der Angestellten und Kunden zu vernehmen.

Wir teilten dem Kamerabetreiber mit, dass eine Tonaufzeichnung strafrechtliche Konsequenzen nach sich ziehen könnte. Zusätzlich informierten wir ihn grundsätzlich über die Beobachtung öffentlich zugänglicher Räume mit optisch-elektronischen Einrichtungen, die in § 6 b BDSG geregelt ist. Da er die Kamera nicht nur angeschafft hatte, um sich vor möglichen Einbrüchen zu schützen, sondern offensichtlich auch, um seine Angestellten zu überwachen, wiesen wir ergänzend auf Folgendes hin: Gemäß § 32 Abs. 1 Satz 2 BDSG dürfen personenbezogene Daten eines Beschäftigten zur Aufdeckung von Straftaten nur dann erhoben, verarbeitet oder genutzt werden, wenn zu dokumentierende tatsächliche Anhaltspunkte den Verdacht begründen, dass der Betroffene im Beschäftigungsverhältnis eine Straftat begangen hat, die Erhebung, Verarbeitung oder Nutzung zur Aufdeckung erforderlich ist und das schutzwürdige Interesse des Beschäftigten an dem Ausschluss der Erhebung, Verarbeitung oder Nutzung nicht überwiegt, insbesondere Art und Ausmaß im Hinblick auf den Anlass nicht unverhältnismäßig sind. Da in diesem Fall keine dokumentierten tatsächlichen Anhaltspunkte dahingehend vorlagen, dass die Mitarbeiter unerlaubt Geld aus der Kasse entwendet hatten, war davon auszugehen, dass eine Videoüberwachung auch ohne Tonaufzeichnung datenschutzrechtlich nicht zulässig gewesen wäre.

Der Geschäftsinhaber sicherte daraufhin zu, die Videoüberwachungsanlage wieder zu deinstallieren, was er später anhand von Bildmaterial bewies. Die Kameraanlage wurde vollständig abgebaut.

Wer unbefugt das nicht öffentlich gesprochene Wort eines anderen auf einen Tonträger aufnimmt, muss mit strafrechtlichen Konsequenzen rechnen. Dies gilt auch, wenn die Tonaufzeichnung im Rahmen einer Videoüberwachung erfolgt.

17.3 Videoüberwachung in Schwimm- und Erholungsbädern

Durch die Beschwerde eines Badbesuchers wurden wir auf die Videoüberwachung in einem Erholungsbad aufmerksam: der Betreiber überwachte mit Videokameras nahezu das gesamte Badgebäude inklusive der Sammelumkleidebereiche, der Solebecken sowie der Ein- und Ausgänge. Wir nahmen dies zum Anlass für eine beschwerdeunabhängige Prüfung eines weiteren Schwimmbades. Auch dort fanden wir eine Videoüberwachung mit datenschutzrechtlichen Mängeln vor.

Auffällig war bei beiden Prüfungen eine Unkenntnis der rechtlichen Grundlagen bzw. eine fehlende Sensibilität für die Rechte der von der Videoüberwachung Betroffenen. Nach § 6 b Abs. 1 Bundesdatenschutzgesetz (BDSG) muss die Überwachung zur Wahrnehmung berechtigter Interessen für konkret festgelegte Zwecke bzw. für die Wahrnehmung des Hausrechts der verantwortlichen Stelle erforderlich sein und es dürfen keine Anhaltspunkte bestehen, dass schutzwürdige Interessen der Betroffenen überwiegen. Zwecke für eine Videoüberwachung hatten die beiden Betreiber wegen der besonderen Gefahren- und Interessenlage in Schwimm- und Erholungsbädern schnell zur Hand. In dem einen Fall waren es vor allem die Badeaufsicht, die Verhinderung bzw. Dokumentierung von Spindaufbrüchen und ergänzend die Wahrnehmung des Hausrechts. Im anderen Fall stand für die Überwachung im Innenbereich die Badeaufsicht im Vordergrund. Daneben sollte der Kassenbereich geschützt werden. Im Außenbereich gaben erhebliche Vandalismusschäden Anlass zu einer Videoüberwachung des Gebäudes. In der gesetzlich geforderten Interessenabwägung sind demgegenüber typischerweise das Interesse der Badbesucher an der Wahrung der Intimsphäre, also nicht nackt oder leicht bekleidet beobachtet oder aufgezeichnet zu werden, und die Interessen ebenfalls erfasster Beschäftigter des Bades zu berücksichtigen.

17.3.1 Unsere Prüfung aus Anlass der Beschwerde

In dem Erholungsbad, auf das sich die Beschwerde bezog, ergab sich bei genauerem Hinsehen für viele Kameras, dass die jeweilige Videoüberwachung nicht erforderlich im Sinne des Bundesdatenschutzgesetzes war. Erforderlich ist eine Videoüberwachung nur, wenn sie geeignet ist, den Zweck zu erreichen und es keine anderen geeigneten und zumutbaren Alternativen gibt, die weniger in Rechte Betroffener eingreifen – sogenannte mildere Mittel. In Schwimmbadbereichen ohne besondere Gefahrenquellen, die der reinen Erholung dienen (z. B. Solebecken, Liege- und Ruhebereiche) ist die fehlende Erforderlichkeit besonders offensichtlich. Doch selbst in Bereichen, in denen der Betreiber eine Badeaufsicht mit besonderer Aufmerksamkeit durchzuführen hat (Schwimmbecken, Rutschen), ist eine Videoüberwachung nicht ohne Weiteres erforderlich, insbesondere wenn die Schwimmhalle sehr übersichtlich ist und keine verborgenen oder schwer einsehbaren Ecken hat. Eine besondere Gefahr muss sich aus objektiven Anhaltspunkten ergeben. Eine regelmäßige Kontrolle des Beckenbereichs kann und muss der Badbetreiber durch Kontrollgänge als milderes und meist sogar besser geeignetes Mittel sicherstellen. Nur sie gewährleistet die Möglichkeit des sofortigen Eingriffs im Notfall. Lediglich in Ausnahmefällen hat eine Videoüberwachung einen zusätzlichen Nutzen.

Auch der Videoüberwachung in den Spind- und Umkleidebereichen standen rechtliche Bedenken entgegen. Im konkreten Bad waren sämtliche Sam-

melumkleideräume zum Zweck der Verhinderung bzw. Dokumentation von Spindaufbrüchen mit Kameras ausgestattet. Für die Badegäste waren Einzelkabinen nicht in ausreichender Zahl und als leicht aufzufindendes Alternativangebot vorhanden. Zwar erfassten die Kameras nicht alle Bereiche der Sammelumkleideräume, doch war nicht – etwa durch eine Markierung oder durch Hinweisschilder – erkennbar, welchen Bereich die Videoüberwachung erfasst. Regelmäßig überwiegt das Interesse der Badegäste an unbeobachteten Bereichen zum Entkleiden und Umziehen gegenüber dem Interesse des Badbetreibers, potenzielle Aufbrüche der Spinde durch eine möglichst flächendeckende Videoüberwachung abzuschrecken.

Eine weitere – nicht nur bädertypische – Problematik ergab sich bei der Videoüberwachung von Ein- und Ausgängen, deren überwiegender Zweck die bildliche Erfassung aller Besucher für die Aufklärung von Verstößen und Straftaten in anderen Bereichen des Bades war. Eine solche verdachtslose Videoüberwachung mit großer Streubreite weist eine äußerst hohe Eingriffsintensität auf, da zahlreiche Personen erfasst werden, die in keiner Beziehung zu einem konkreten Fehlverhalten stehen.[60] Eine Videoüberwachung ist daher regelmäßig auf die konkret gefährdeten Orte zu beschränken. Die Gefährdung des Ortes muss sich objektiv begründen lassen. Eine verdachtslose Videoüberwachung ungefährdeter Orte lässt sich nicht rechtfertigen. Eine besondere Gefährdung konnte uns der Badbetreiber jedoch nicht darlegen.

Daneben hatte er auch zahlreiche Verfahrensvorschriften des Bundesdatenschutzgesetzes nicht beachtet. So ist bei umfangreichen Videoüberwachungsmaßnahmen ein betrieblicher Datenschutzbeauftragter zu bestellen, der vor Inbetriebnahme der Kameras eine datenschutzrechtliche Vorabkontrolle durchführt – vgl. §§ 4 f Abs. 1 Satz 1 und 6, 4 d Abs. 5 Satz 1 BDSG – und im weiteren Verlauf auf eine regelmäßige Evaluierung der Rechtmäßigkeitsvoraussetzungen hinwirkt. Zudem ist eine Verfahrensübersicht mit detaillierten Angaben u. a. zu den Zwecken, den zugriffsberechtigten Personen und den technischen und organisatorischen Maßnahmen zu erstellen – vgl. §§ 4 g Abs. 2, 4 e Satz 1 BDSG. Im geprüften Erholungsbad wurden die Voraussetzungen nicht erfüllt, insbesondere mangelte es an einer ausreichenden schriftlichen Fixierung. Im Laufe des langjährigen Betriebs der Kameras gab es in der Geschäftsführung und unter den Mitarbeitern zahlreiche Wechsel. Zum Zeitpunkt unserer Überprüfung konnte der Badbetreiber daher selbst nur schwer darstellen, wozu die Videoüberwachung im Einzelnen dienen sollte.

Die Landesbeauftragte setzte aufgrund des oben angedeuteten Umfangs und der Intensität der unzulässigen Videoüberwachungsmaßnahmen sowie der

[60] Beschluss des Bundesverfassungsgerichts vom 23. Februar 2007, 1 BvR 2386/06

erst nach Jahren erfolgten Bestellung einer Datenschutzbeauftragten gegen den Badbetreiber ein Bußgeld fest.[61]

Zum Zeitpunkt der Erstellung dieses Berichts befanden wir uns im Dialog mit dem Schwimmbadbetreiber über eine zukünftige Ausgestaltung einer zulässigen Videoüberwachung des Bades.

17.3.2 Anlasslose Prüfung eines weiteren Schwimmbades

Auch in diesem Bad stellten wir im Verlauf der Prüfung datenschutzrechtliche Mängel bei der Durchführung der Videoüberwachung fest – erfreulicherweise in deutlich geringerem Umfang. Der Badbetreiber hatte einen Datenschutzbeauftragten bestellt und sich in einer Verfahrensübersicht mit den Zwecken und den Rechtsgrundlagen auseinandergesetzt.

Eine über das zulässige Maß hinausgehende Videoüberwachung fand sich dennoch im Innenbereich des Gebäudes, wo zwei Kameras nicht im Sinne des § 6 b Abs. 1 BDSG erforderlich waren. In der übersichtlichen Schwimmhalle hatte die Videoüberwachung durch zwei von drei Kameras neben der regulären Badeaufsicht durch das Schwimmpersonal keinen zusätzlichen Nutzen. Zudem fand neben dem Live-Monitoring durch den Schwimmmeister ein Monitoring durch den Badleiter statt. Diese zusätzliche Beobachtung war für den Zweck der Badeaufsicht wegen der Zufälligkeit der Wahrnehmung der Bilder nicht geeignet.

Die Kamera im Kassenbereich sollte primär dem Schutz der Kassenmitarbeiter und des Bargeldbestands dienen. Hierfür war das Live-Monitoring durch Badleiter und Schwimmmeister bereits gar nicht bzw. jedenfalls nur sehr gering geeignet. Zudem waren mildere Mittel bereits vorhanden oder jedenfalls denkbar (Notfallknopf, Tresor). Der Badbetreiber setzte daher insbesondere auf einen Abschreckungseffekt der gut sichtbaren Videokamera und auf eine Erhöhung des Sicherheitsgefühls seiner Mitarbeiter. Als weiteren Zweck führte er organisatorische Gründe an: Schwimmmeister und Badleiter sollten sich durch einen schnellen Blick auf den Monitor einen Eindruck über die zu erwartende Auslastung verschaffen können. Unsere Bedenken eines Überwachungsdrucks für die Kassenmitarbeiter griff der Badbetreiber auf und sagte eine Ausblendung des Arbeitsbereichs und Abstellung der Bildübertragung an den Badleiter zu. Ob eine Überwachung des übrigen Foyerbereichs mit den genannten Gründen in Betracht kommt, wird noch geprüft.

Daneben empfahlen wir, die Videoüberwachung des Außenbereichs streng an der Erforderlichkeit zu orientieren. Der Betreiber sagte uns zu, die Erfas-

[61] siehe B 20.1

sungsbereiche der Kameras entsprechend zu beschränken und die Kameras (teilweise) nur zeitlich begrenzt zu betreiben.

Eine Videoüberwachung von Schwimm- und Erholungsbädern ist nur unter strengen Voraussetzungen zulässig. Dies gilt umso mehr, wenn Personen erfasst werden, die sich im überwachten Bereich zum Zwecke der Erholung aufhalten, die nur leicht oder gar nicht bekleidet sind oder die selbst nicht Anlass der Überwachung sind und dieser nicht ausweichen können. Gesetzliche Verfahrensanforderungen – wie die Bestellung eines Datenschutzbeauftragten, die Vorabkontrolle, das Erstellen einer Verfahrensübersicht – sollen im Vorhinein und nach Inbetriebnahme laufend sicherstellen, dass eine Videoüberwachung nur im gesetzlichen Rahmen erfolgt.

17.4 Orientierungshilfen zur Videoüberwachung

Die Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder hat im Berichtszeitraum eine Orientierungshilfe für die Videoüberwachung durch nicht-öffentliche Stellen und ein Zusatzpapier für die Videoüberwachung in Schwimmbädern herausgegeben. Hintergrund war das gemeinsame Anliegen der Aufsichtsbehörden, Unternehmen und Privatpersonen, die an einer Videoüberwachung interessiert sind, bereits frühzeitig Informationen zu den Rechten und Pflichten zur Hand zu geben.

17.4.1 Orientierungshilfe „Videoüberwachung durch nicht-öffentliche Stellen“

Nach der Grundregel des § 4 Abs. 1 Bundesdatenschutzgesetz (BDSG) gilt für nicht-öffentliche Stellen, also Unternehmen, Privatpersonen, Vereine usw. Folgendes: Eine Videoüberwachung, durch die eine andere Person in identifizierbarer Weise erfasst wird, ist unzulässig, wenn sie nicht auf einen Erlaubnistatbestand gestützt werden kann. Zulässig ist eine Videoüberwachung, wenn alle Betroffenen in ausreichender Form eingewilligt haben oder einer der gesetzlichen Erlaubnistatbestände des Bundesdatenschutzgesetzes (z. B. §§ 6 b Abs. 1 bzw. § 28 Abs. 1 Nr. 3 BDSG) erfüllt ist.[62]

Die Orientierungshilfe „Videoüberwachung durch nicht-öffentliche Stellen“[63] aus dem Jahr 2014 erläutert die wichtigsten Aspekte im Zusammenhang mit einer Videoüberwachung öffentlich zugänglicher Räume und mit den Pflichten vor, während und nach Einsatz von Videoüberwachungskameras und -anlagen. Für besondere Fallkonstellationen sind weitergehende Hinweise enthalten – etwa zu den Themen Webcams, Videoüberwachung in der

[62] siehe B 17.1 und 17.3

[63] http://www.lda.brandenburg.de

Gastronomie, Videoüberwachung von Beschäftigten, Videoüberwachung durch Nachbarn oder Vermieter.

Um eine Videoüberwachung handelt es sich bei jeder Beobachtung mit „optisch-elektronischen Einrichtungen“ – auch bei dem Einsatz von Webcams, Wildkameras, digitalen Fotoapparaten oder Mobiltelefonen mit integrierter Kamera kann also eine Videoüberwachung gegeben sein, die datenschutzrechtlich zu beurteilen ist. Bereits vor der Installation einer Videoüberwachung sind die verfolgten Ziele zu konkretisieren. Des Weiteren sollte sich die verantwortliche Stelle mit verschiedenen Fragestellungen beschäftigen – etwa, ob mit einer Videoüberwachung das verfolgte Ziel überhaupt erreicht werden kann, ob das Ziel auf eine andere Weise erreicht werden könnte, die in das Persönlichkeitsrecht anderer Personen weniger eingreift und, falls dies verneint wird, an welchen Orten und zu welchen Zeiten eine Überwachung unbedingt notwendig erscheint. Selbst wenn eine Videoüberwachung zur Wahrung des Hausrechts oder zur Wahrnehmung eines berechtigten Interesses erforderlich ist, darf sie nur in Betrieb genommen werden, wenn schutzwürdige Interessen der Betroffenen nicht überwiegen. Bei der Abwägung sind die Gesamtumstände des Einzelfalls maßgeblich.

Schon vor Beginn der Videoüberwachung hat die verantwortliche Stelle zahlreiche Pflichten zu erfüllen: Es sind technische und organisatorische Maßnahmen zur Gewährleistung des Datenschutzes zu treffen. In einer Verfahrensübersicht sind bestimmte Angaben zusammenzustellen, die der betriebliche Datenschutzbeauftragte – mit Ausnahme von Angaben zur Datensicherheit – jedermann auf Antrag verfügbar machen muss. Bei einer umfangreichen Videoüberwachung ist eine Vorabkontrolle durch den betrieblichen Datenschutzbeauftragten durchzuführen und zu dokumentieren.

Die verantwortliche Stelle muss zudem durch Erfüllung ihrer Hinweispflicht nach § 6 b Abs. 2 BDSG die Betroffenen in die Lage versetzen, bereits vor Betreten des überwachten Bereichs den Umstand der Überwachung erkennen zu können.

17.4.2 Videoüberwachung in Schwimmbädern – Zusatz zur Orientierungshilfe „Videoüberwachung durch nicht-öffentliche Stellen“

Im August 2015 wurde die allgemeine Orientierungshilfe um einen Zusatz zur Videoüberwachung in Schwimmbädern[64] ergänzt. Sowohl die Orientierungshilfe als auch der Zusatz richten sich an nicht-öffentliche Stellen, die Schwimmbäder betreiben.

64 http://www.lda.brandenburg.de

Im Zusatzpapier wird auf die besondere Interessenlage in Schwimmbädern eingegangen und auf regelmäßig in diesem Zusammenhang auftauchende Themen hingewiesen.[65] Der Schwimmbadbetreiber verfolgt mit einer Videoüberwachung typischerweise folgende Zwecke: die Verhinderung des Aufbruchs von Spinden und der unsachgemäßen Benutzung von Rutschen, die Sicherung von Kassenautomaten, die Zutrittskontrolle zu besonderen Bereichen, die Unterstützung der Badeaufsicht, den Ausschluss von Haftungsrisiken oder die Beweissicherung bei Einbrüchen. Alle genannten Ziele sind unter Berücksichtigung der Umstände des Einzelfalls sorgfältig an den gesetzlichen Anforderungen zu prüfen. Häufig ist eine Videoüberwachung nicht geeignet oder es gibt andere, mildere Mittel zur Zielerreichung, sodass eine Erforderlichkeit nicht gegeben ist. Im Rahmen der Interessenabwägung sind die besonders schutzwürdigen Interessen der Badegäste an einer unbeobachteten Freizeitgestaltung und der Wahrung ihrer Intimsphäre zu berücksichtigen. Das Zusatzpapier zur Videoüberwachung in Schwimmbädern gibt erste Anhaltspunkte für die rechtliche Beurteilung regelmäßig auftauchender Probleme.

Die Orientierungshilfe und das Zusatzpapier sollen nicht-öffentlichen Stellen und betroffenen Personen als eine erste Orientierung für die Bewertung der Zulässigkeit und des korrekten Einsatzes einer Videoüberwachung dienen. Die rechtlichen Hürden für eine Videoüberwachung sind, anders als vielfach angenommen, sehr hoch. Es ist stets eine sorgfältige Einzelfallprüfung vorzunehmen. Bei einer Videoüberwachung von Schwimmbädern sind die Interessen betroffener Schwimmbadgäste als besonders schutzwürdig anzusehen. Zudem sind vor und bei Durchführung einer Videoüberwachung zahlreiche technische, organisatorische und andere verfahrensbezogene Maßnahmen gesetzlich verpflichtend vorgeschrieben.

[65] siehe auch B 17.3

18 Wirtschaft

18.1 Werbung frei Haus – einmal eingewilligt, immer eingewilligt?

Im Jahr 2004 hatte ein Verein eine einmalige Veranstaltung organisiert und hierzu mit den Teilnehmern einen Vertrag abgeschlossen. Zehn Jahre später versandte er gänzlich unerwartet erneut Post an die Veranstaltungsteilnehmer – diesmal mit Werbung für die Mitgliedschaft in einer Krankenkasse. Weil einige von ihnen zum Zeitpunkt des Vertragsabschlusses explizit der Nutzung ihrer Daten für Werbezwecke widersprochen hatten, erhielten wir mehrere Beschwerden über das Agieren des Vereins.

Als nicht öffentliche Stelle unterliegt der Verein den Bestimmungen des Bundesdatenschutzgesetzes (BDSG). Personenbezogene Daten, die er für eigene Zwecke verarbeitet, hat er nach § 35 Abs. 2 Nr. 3 BDSG zu löschen, sobald ihre Kenntnis für die Erfüllung des Zwecks der Speicherung nicht mehr erforderlich ist. Da die Vertragsbeziehungen zwischen Teilnehmern und Verein bereits mit der Durchführung der Veranstaltung geendet hatten, war dies bereits im Jahr 2004 der Fall.

An die Stelle einer Löschung tritt nach § 35 Abs. 3 Nr. 1 BDSG eine Sperrung, soweit einer Löschung gesetzliche, satzungsmäßige oder vertragliche Aufbewahrungsfristen entgegenstehen. Solche Fristen können sich beispielsweise aus der Vereinssatzung oder dem Steuerrecht ergeben. Weil im vorliegenden Fall zur Ausrichtung der Veranstaltung durch den Verein ein Teilnahmebetrag erhoben worden war, hätten die personenbezogenen Daten ggf. aus steuerrechtlichen Gründen zwar für zehn Jahre aufbewahrt werden können, dann jedoch mit einem Sperrvermerk versehen werden müssen.

Selbst wenn die Daten noch rechtmäßig gespeichert gewesen wären, entbehrte ihre erneute Nutzung für Werbezwecke in jedem Fall einer entsprechenden Rechtsgrundlage. Insbesondere galt dies aufgrund der Vorschriften in § 28 Abs. 4 BDSG für diejenigen Veranstaltungsteilnehmer, die der Verwendung ihrer Daten zu Zwecken der Werbung widersprochen hatten. Aber auch bei Teilnehmern, die in die Nutzung ihrer Daten zu Werbezwecken eingewilligt hatten, war der Versand der Werbung für die Krankenkasse durch den Verein nicht rechtmäßig. Zwar ist die Verarbeitung oder Nutzung personenbezogener Daten für Zwecke des Adresshandels oder der Werbung gem. § 28 Abs. 3 BDSG zulässig, soweit der Betroffene einwilligt. Eine einmal erteilte Einwilligung gilt jedoch nicht unbegrenzt. Wird von ihr über einen

längeren Zeitraum kein Gebrauch gemacht, verliert sie ihre Gültigkeit und kommt nicht mehr als Grundlage für die Zusendung von Werbepost infrage.[66]

Die Nutzung der Adressdaten durch den Verein war somit unzulässig. Die Landesbeauftragte hat im Ergebnis ein Ordnungswidrigkeitenverfahren eingeleitet.

Widersprüche gegen die Verwendung personenbezogener Daten zu Werbezwecken sind strikt zu beachten. Aber auch eine in diesem Zusammenhang erteilte Einwilligung hat keine zeitlich unbegrenzte Gültigkeit. Wird hiervon lange Zeit kein Gebrauch gemacht, erlischt sie.

18.2 Kunden haben ein Recht auf Auskunft über ihre Daten

Immer wieder beschweren sich Kunden darüber, dass ihnen Unternehmen nur unzureichend oder keine Auskunft über die zu ihrer Person gespeicherten Daten erteilen. Auch die Empfänger persönlich adressierter Werbepost erhalten auf entsprechende Anfragen oft keine zufriedenstellende Antwort.

Die Rechtslage ist denkbar einfach: Nach § 34 Bundesdatenschutzgesetz (BDSG) hat die verantwortliche Stelle – in der Regel geht es um ein Unternehmen – dem Betroffenen unter anderem Auskunft darüber zu erteilen, welche zu seiner Person gespeicherten Daten dort vorliegen, woher sie stammen, an wen sie weitergegeben werden und welchem Zweck sie dienen. Diese Auskunft ist eine unabdingbare Voraussetzung für die Geltendmachung weiterer Datenschutzrechte. Ohne zu wissen, welche Daten vorhanden sind, kann ein Betroffener nicht beurteilen, ob sie richtig oder falsch sind. Das wiederum ist erforderlich, um möglicherweise Ansprüche auf Korrektur, Sperrung, Löschung oder Schadenersatz einzufordern.

Den Auskunftsanspruch können Kunden, aber beispielsweise auch Empfänger persönlich adressierter Werbepost geltend machen. Gerade in der letztgenannten Konstellation möchten Betroffene häufig wissen, wie Werbetreibende überhaupt an ihre Anschriften gelangt sind.

Vielen an uns gerichteten Beschwerden ist zu entnehmen, dass die Unternehmen sich gar nicht erst der Mühe unterziehen, zu antworten. Selbst wenn sich die Landesbeauftragte als Aufsichtsbehörde einschaltet, bedarf es oft einer förmlichen Zustellung, um überhaupt eine Reaktion zu erhalten. Dabei ist der Aufwand für die Erteilung einer Auskunft an Betroffene zumeist sehr gering. Wer eine solche Auskunft nach § 34 BDSG nicht, nicht richtig, nicht vollständig oder nicht rechtzeitig erteilt, erfüllt dadurch nach § 43 Abs. 1

66 Urteil des Landgerichts München I vom 8. April 2010, 17 HK O 138/10

Nr. 8 a BDSG den Tatbestand einer Ordnungswidrigkeit. Diese kann nach § 43 Abs. 3 BDSG mit einer Geldbuße bis zu 50.000 Euro geahndet werden.

In anderen Fällen haben Unternehmen ihre Verweigerung, die Auskunft zu erteilen, auf vertragliche Geheimhaltungspflichten gestützt. Die Vereinbarung zwischen einem werbenden Unternehmen und einem Adresshändler, den Betroffenen gegenüber die Herkunft ihrer Daten geheimzuhalten, ist unzulässig. Schließlich steht dem Betroffenen ein gesetzlicher Anspruch zu, der durch einen einfachen Vertrag zulasten Dritter nicht ausgeschlossen werden kann.

Auch begründen einige Unternehmen ihre Ablehnung von Auskunftsersuchen mit Geschäftsgeheimnissen. Zwar erlaubt § 34 Abs. 7 BDSG unter Bezugnahme auf § 33 Abs. 2 Satz 2 Nr. 7 b BDSG, eine Auskunft zu verweigern, wenn dadurch die Geschäftszwecke der verantwortlichen Stelle erheblich gefährdet würden. Die Argumentation mit dieser Vorschrift verkennt jedoch in den meisten Fällen, dass sie Unternehmen keineswegs vor bloßen Unannehmlichkeiten schützen soll. Sie kommt vielmehr nur dann zum Tragen, wenn von einer erheblichen Gefährdung der Geschäftszwecke auszugehen ist. Die Auskunft über Kundendaten bzw. über die mit ihnen abgewickelten Geschäfte erfüllt diese Anforderung nicht. Das Interesse der Betroffenen an einer umfassenden Information über ihre dem jeweiligen Unternehmen vorliegenden Daten überwiegt regelmäßig auch das teilweise angeführte Interesse von Unternehmen, beispielsweise ihre Werbestrategie geheim halten zu wollen. Dies gilt umso mehr, weil die Kundendaten selbst schließlich noch gar keine Werbestrategie darstellen.

Betroffene haben nach § 34 Bundesdatenschutzgesetz gegenüber Unternehmen ein weitgehendes Recht auf Auskunft über dort gespeicherte Daten mit Bezug zu ihrer Person. Der Anspruch umfasst auch die Information darüber, woher diese Daten stammen, an wen sie weitergegeben werden und welchem Zweck sie dienen. Ausnahmen sind restriktiv anzuwenden.

19 Statistik

Beschwerden gegen die Heranziehung für statistische Erhebungen

Bürger, die durch eine gesetzlich angeordnete Auskunftspflicht bei statistischen Erhebungen ihr Grundrecht auf informationelle Selbstbestimmung als verletzt ansehen, wenden sich häufig an uns, um die Rechtmäßigkeit der Erhebungen prüfen zu lassen.

Das Bundesverfassungsgericht hat in seinem „Volkszählungsurteil“ ausgeführt, dass das Grundrecht auf informationelle Selbstbestimmung nicht schrankenlos gewährleistet ist. Einschränkungen dieses Rechts müssen im überwiegenden Allgemeininteresse hingenommen werden. Zwingende Voraussetzung für eine derartige Einschränkung ist jedoch das Vorliegen einer normenklaren gesetzlichen Rechtsgrundlage.

Es ist grundsätzlich davon auszugehen, dass statistikrechtliche Auskunftspflichten in gesetzlich angeordneten amtlichen Statistiken den verfassungsrechtlichen Vorgaben genügen. Im Hinblick auf Stichprobenbefragungen hat das Bundesverfassungsgericht ausdrücklich darauf hingewiesen, dass bereits eine Verweigerung der Angaben durch wenige Befragte das Ergebnis der gesamten Repräsentativumfrage infrage stellen könnte. In § 23 Bundesstatistikgesetz (BStatG) und auch in § 25 Brandenburgisches Statistikgesetz (BbgStatG) ist aus diesem Grund geregelt, dass Auskunftspflichtige, die eine Auskunft nicht, nicht richtig, nicht vollständig oder nicht rechtzeitig erteilen, ordnungswidrig handeln und mit einer Geldbuße von bis zu fünftausend Euro belegt werden können. Alle Daten, zu denen eine Auskunftspflicht besteht, müssen per Gesetz klar definiert sein. Wenn bei einer gesetzlich vorgeschriebenen statistischen Erhebung zusätzlich Daten auf freiwilliger Basis abgefragt werden, müssen die entsprechenden Fragen selbstverständlich nicht beantwortet werden.

Untrennbar verbunden mit der statistikrechtlichen Auskunftspflicht für Betroffene ist die Pflicht zur Geheimhaltung für Stellen, die eine Statistik durchführen (siehe § 16 BStatG bzw. § 18 BbgStatG). Danach müssen diese Stellen, bzw. die dort beschäftigten Personen, Einzelangaben über persönliche oder sachliche Verhältnisse, die im Rahmen einer Statistik von Auskunftspflichtigen erhoben wurden, geheim halten. Dies erfordert insbesondere die Umsetzung entsprechender technischer und organisatorischer Sicherheitsvorkehrungen.

Veröffentlichungen von statistischen Ergebnissen sind nur zulässig, wenn ein Rückschluss auf einzelne Betroffene ausgeschlossen werden kann.

Auskunftspflichtige Personen, die per Heranziehungsbescheid zur Mitwirkung an einer Statistik verpflichtet werden, können sich dieser nach geltendem Recht nicht entziehen. Im überwiegenden Allgemeininteresse muss diese Einschränkung des Rechts auf informationelle Selbstbestimmung hingenommen werden.

20 Tätigkeit der Sanktionsstelle

20.1 Überblick zu den Ordnungswidrigkeitenverfahren

Im Berichtszeitraum hat die Landesbeauftragte 24 Ordnungswidrigkeitenverfahren wegen verschiedener Verstöße sowohl gegen das Brandenburgische als auch das Bundesdatenschutzgesetz abgeschlossen.

Von den 24 Verfahren haben wir in 10 Fällen ein Bußgeld verhängt und in einem Fall eine Verwarnung ausgesprochen. Die Summe der verhängten Bußgelder betrug 31.350 Euro. Darüber hinaus hat die Landesbeauftragte von ihrem Recht Gebrauch gemacht, in einer Sache Strafantrag zu stellen. Die übrigen 12 Verfahren waren einzustellen, weil einzelne Tatbestandsvoraussetzungen, wie beispielsweise das subjektive Merkmal der vorsätzlichen Begehungsweise bei § 38 Brandenburgisches Datenschutzgesetz (BbgDSG), nicht erfüllt wurden. Ein fahrlässiges Handeln kann nach dieser Vorschrift – im Gegensatz zum Bundesdatenschutzgesetz (BDSG) – nicht geahndet werden.

Die Verfahren, die mit der Festsetzung von Bußgeldern bzw. einer Verwarnung abgeschlossen wurden, betrafen unter anderem die unzulässige Verarbeitung von Adressdaten der Teilnehmer an einer Veranstaltung durch den ehemaligen Vertragspartner für Werbezwecke, nachdem das Vertragsverhältnis bereits seit über 10 Jahren beendet war,[67] die fehlende bzw. nicht schriftliche Bestellung eines betrieblichen Datenschutzbeauftragten sowie Mängeln beim Abschluss eines Vertrages zur Datenverarbeitung im Auftrag durch ein Wohnungsunternehmen.[68]

Zudem war die Verhängung von Sanktionen in mehreren Fällen der unzulässigen Videoüberwachung geboten. In einem Verfahren filmten die Verantwortlichen den öffentlichen Gehweg vor ihrem Friseursalon, wodurch Passanten und Kunden von der Kamera erfasst wurden. Ursprünglich geschah dies unter Wahrnehmung ihrer berechtigten Interessen, weil konkrete Straftaten gegen den Anlagenbetreiber begangen worden waren. Allerdings gab es seit zweieinhalb Jahren keine Vorfälle mehr, sodass nunmehr die Interessen der betroffenen Passanten und Kunden überwogen. Ohnehin wäre eine Videobeobachtung während der Öffnungszeiten nicht erforderlich gewesen, da stets Personal anwesend war und mögliche Vorfälle hätte beobachten, melden oder gar verhindern können.

---

67 siehe B 18.1

68 siehe B 16.1

In einem weiteren Fall erfolgte durch die Betreiber eines Schwimmbades eine flächendeckende Videoüberwachung über mehrere Jahre hinweg.[69] Besucher, Mitarbeiter und Kunden wurden sowohl im Innen- als auch im Außenbereich der Freizeiteinrichtung gefilmt. Die Bildaufnahmen wurden sieben Tage gespeichert und teilweise zum Zwecke der Strafverfolgung ausgewertet. Der Einsatz der Kameras war meist ungeeignet und damit zur Wahrnehmung des Hausrechts nicht erforderlich. Darüber hinaus mussten die Interessen der Kamerabetreiber (z. B. an der Verfolgung von Straftaten) hinter den Interessen der Betroffenen (selbst darüber zu bestimmen, wer wann, welche Videoaufnahmen von ihnen in ihrer Freizeit in besonders sensiblen Bereichen fertigt) zurücktreten.

Bereits im letzten Tätigkeitsbericht[70] informierten wir darüber, dass Daten verarbeitende Stellen gemäß § 38 Abs. 3 Satz 1 BDSG dazu verpflichtet sind, der Landesdatenschutzbeauftragten, die für die Erfüllung ihrer gesetzlichen Aufgaben erforderlichen Auskünfte zu erteilen. Ein Verstoß hiergegen kann mit der Festsetzung eines Bußgeldes gemäß § 43 Abs. 1 Nr. 10 BDSG geahndet werden. Dieses Mittel anzuwenden, sahen wir uns im Berichtszeitraum erneut gezwungen.

Gleichfalls mussten wir ein Bußgeld gemäß § 130 Abs. 1 Satz 1 Ordnungswidrigkeitengesetz gegen die Inhaberin eines Inkassodienstes erlassen. Diese hatte es versäumt, in ausreichendem Maße für die Einhaltung der datenschutzrechtlichen Vorschriften in dem Gewerbebetrieb zu sorgen. Deshalb war es möglich, dass eine Mitarbeiterin Briefe verschickte, bei denen im Sichtfenster des Briefumschlages nicht nur der Vor- und Zuname vermerkt war, sondern auch der Geburtsname, das Geburtsdatum und das frühere Betätigungsfeld des Adressaten. Dadurch war die Möglichkeit einer ungehinderten Kenntnisnahme der Daten durch unzuständige Dritte – wie z. B. Postzusteller gegeben. Die Angaben waren auch nicht für eine korrekte Zustellung erforderlich. Durch eine zumindest stichprobenweise Überwachung der für den Inkassodienst tätig werdenden Personen sowie der eingesetzten Datenverarbeitungsprogramme hätte die unzulässige Datenverarbeitung verhindert oder wenigstens wesentlich erschwert werden können.

In den Fällen, in denen ein Bußgeld wegen eines Datenschutzverstoßes nach § 38 BbgDSG erlassen worden war, handelte es sich um Mitarbeiter der öffentlichen Verwaltung, die zum einen ohne dienstlichen Anlass personenbezogene Daten aus den ihnen nur für dienstliche Zwecke zur Verfügung stehenden Datenbanken abgerufen bzw. aus Akten entnommen hatten, um diese für rein private Zwecke zu verwenden. Zum anderen wurde die Anfrage einer Bürgerin ohne deren Einwilligung und ohne, dass es eine dienstliche

[69] siehe B 17.3

[70] Tätigkeitsbericht 2012/2013, B 18.4

Notwendigkeit gab, an Dritte weitergegeben. Selbst nachdem sich die Bürgerin hierüber beschwerte, wurde auch diese Eingabe weitergeleitet. Eine Rechtsnorm, die diese Datenübermittlung erlaubt hätte, gab es nicht.

Neben ihrer beratenden und kontrollierenden Tätigkeit stellt die repressive Verfolgung und Ahndung von Ordnungswidrigkeiten für die Landesbeauftragte eine weitere Möglichkeit dar, die Einhaltung datenschutzrechtlicher Vorschriften durchzusetzen. Vor allem in gravierenden Fällen sollen durch die Festsetzung einer Geldbuße eine ernste Pflichtenmahnung ausgesprochen und die Betroffenen zur Einhaltung datenschutzrechtlicher Normen angehalten werden.

20.2 Private Kontaktaufnahme über Kundentelefonnummer

Eine Kundin gab ihrer Bank ihre private Telefonnummer bekannt, damit das Kreditinstitut sie in dringenden geschäftlichen Angelegenheiten schnell erreichen kann. Umso erstaunter war sie dann, als sie eines Abends sehr persönliche Nachrichten von einem Bankmitarbeiter über einen Kurznachrichtendienst erhielt. Wie sich herausstellte, hatte er die Telefonnummer aus den Unterlagen der Kundin entnommen, weil er an ihr Gefallen gefunden hatte und sich aus diesem privaten Grund verabreden wollte.

Ordnungswidrig handelt gemäß § 43 Abs. 2 Nr. 3 Bundesdatenschutzgesetz (BDSG), wer vorsätzlich unbefugt personenbezogene Daten, die nicht allgemein zugänglich sind, sich aus automatisierten Verarbeitungen oder nicht automatisierten Dateien verschafft. Ein Verstoß kann nach § 43 Abs. 3 BDSG als Ordnungswidrigkeit verfolgt und mit einer Geldbuße von bis zu 300.000 Euro geahndet werden.

Bei der privaten Telefonnummer der Kundin, die keinem allgemeinen, für jedermann zugänglichen Verzeichnis (z. B. Telefonbuch) entnommen werden konnte, handelte es sich um personenbezogene Daten im Sinne des § 3 Abs. 1 BDSG. Grundsätzlich dürfen solche Daten nur erhoben, verarbeitet oder genutzt werden, wenn der Betroffene darin eingewilligt hat oder eine Rechtsnorm dies erlaubt. Für die Verwendung der in Rede stehenden Daten durch den Bankmitarbeiter zu rein privaten Zwecken lag weder eine Einwilligung der Kundin vor, noch konnte es hierfür eine gesetzliche Ermächtigung geben.

In dem sich der Bankmitarbeiter die Nummer der Kundin aus den Unterlagen bzw. dem EDV-System der Bank heraussuchte und für sich speicherte, um die Kundin dann privat kontaktieren zu können, verschaffte er sich die Daten in unzulässiger Weise. „Sich-Verschaffen“ bedeutet in diesem Zusammen-

hang das Zur-Kenntnis-Nehmen oder Herstellen eines Zustandes, der es dem Täter erlaubt, die Daten später zur Kenntnis zu nehmen, sie zu nutzen oder sonst über sie zu verfügen, ohne dass die verantwortliche Stelle ihn daran noch hindern kann.

Dies war hier der Fall. Die Bank hatte keine Möglichkeit mehr, die Verwendung der Mobilfunknummer durch den Mitarbeiter zu unterbinden. Dieser konnte ungehindert darüber verfügen, was er dann auch tat, indem er privat Kontakt zur Kundin aufnahm. Dieses Verhalten haben wir mit einem Bußgeld geahndet.

Beschäftigte von Unternehmen dürfen die Daten ihrer Kunden nicht ohne deren Einwilligung für private Zwecke verwenden.

Teil C

Akteneinsicht und Informationszugang

1 Entwicklung der Informationsfreiheit

1.1 Europa

Bereits im Juli 2013 trat die Novellierung der Richtlinie über die Weiterverwendung von Informationen des öffentlichen Sektors (PSI-Richtlinie 2013/37/EU) in Kraft. Durch die Änderungen besteht nunmehr ein grundsätzliches Recht auf Weiterverwendung von Informationen, die auf der Grundlage von Informationsfreiheitsgesetzen zugänglich sind. Die Mitgliedstaaten werden verpflichtet, diese Informationen – idealerweise aus eigener Veranlassung und medienbruchfrei in einem Internetportal – zur Verfügung zu stellen. Nach Durchführung einer öffentlichen Konsultation, die zum Ziel hatte, konkrete Möglichkeiten der Erschließung von Informationen des öffentlichen Sektors für die Weiterverwendung aufzuzeigen, veröffentlichte die Europäische Kommission entsprechende Leitlinien für empfohlene Standardlizenzen, Datensätze und Gebühren.[71] Die Leitlinien sollen dazu beitragen, bestehende Hindernisse in den Mitgliedsstaaten bei der Freigabe von Verwaltungsinformationen nach den Open-Data-Grundsätzen abzubauen. In dem Papier erläutert die Kommission unter anderem Einzelheiten zu den empfohlenen Lizenzbedingungen sowie zum Umgang mit personenbezogenen Daten. Sie empfiehlt, fünf besonders nachgefragten, thematischen Datenkategorien den Vorrang bei der Bereitstellung für die Weiterverwendung einzuräumen: Geodaten, Informationen über Erdbeobachtung und Umwelt, Verkehrsdaten, Statistiken und Unternehmensregister. Außerdem erläutern die Leitlinien das Grenzkostenprinzip als Beschränkung der Erhebung von Kosten für die Weiterverwendung. Öffentliche Stellen dürfen danach – von Ausnahmen abgesehen – keine höheren Gebühren erheben als die aus der Reproduktion, Bereitstellung und Verbreitung entstehenden Grenzkosten.

Getragen werden die Leitlinien – ebenso wie die vorangegangene Novellierung der Weiterverwendungsrichtlinie – von der Überzeugung, dass von der öffentlichen Hand erzeugte Daten als Rohmaterial für innovative, wertschöpfende Dienste und Produkte verwendet werden können, die zur Belebung der Wirtschaft durch neue Arbeitsplätze und Investitionsförderung in datenintensiven Sektoren beitragen. Sie spielen, so die Kommission, auch eine Rolle,

[71] Leitlinien für empfohlene Standardlizenzen, Datensätze und Gebühren für die Weiterverwendung von Dokumenten, Amtsblatt der Europäischen Union, Teil II vom 24. Juli 2014 (2014/C 240/01)

wenn es darum geht, die Rechenschaftspflicht und Transparenz im staatlichen Handeln zu stärken. Sowohl die Leitlinien als auch die novellierte Weiterverwendungsrichtlinie sind somit Ausdruck des Open-Data-Gedankens, wie er bereits im Jahr 2013 von den Staats- und Regierungschefs der G8 anerkannt und in ihrer Charta für offene Daten bekräftigt wurde.

1.2 Bund

Der Gerichtshof der Europäischen Union hat in zwei Urteilen[72] entschieden, wann ein Ministerium eine informationspflichtige Stelle im Sinne der Umweltinformationsrichtlinie und somit zur Herausgabe von Informationen verpflichtet ist. Entgegen dem Wortlaut des bisherigen Umweltinformationsgesetzes sind Ministerien, die an einem Gesetzgebungsverfahren beteiligt sind, nur während dessen Dauer zur Herausgabe entsprechender Informationen nicht verpflichtet. Sind Ministerien hingegen an einem Verfahren zum Erlass von Rechtsverordnungen beteiligt, besteht die Informationspflicht grundsätzlich auch während der Dauer dieses Verfahrens. In den Fällen, die den Urteilen zugrunde lagen, richtete sich das Informationsbegehren gegen das Bundesministerium für Umwelt, Naturschutz und Reaktorsicherheit sowie gegen das Bundesministerium für Wirtschaft und Technologie. Der Bundesgesetzgeber hat durch eine entsprechende Änderung des Umweltinformationsgesetzes des Bundes diese Maßgaben umgesetzt. Das geänderte Umweltinformationsgesetz wurde am 27. Oktober 2014 in einer Neufassung bekanntgemacht.[73]

Auch die Änderung des Informationsweiterverwendungsgesetzes geht auf eine europarechtliche Vorgabe zurück. Die novellierte Weiterverwendungsrichtlinie[74] räumte den Mitgliedstaaten eine Frist zur Umsetzung bis zum 18. Juli 2015 ein. Der Bundesgesetzgeber hat mit dem Änderungsgesetz klargestellt, dass Informationen des öffentlichen Sektors künftig für die private und wirtschaftliche Nutzung weiterverwendet werden dürfen. Bisherige Weiterverwendungsverbote oder Genehmigungsvorbehalte sind entfallen. Darüber hinaus wurde der Anwendungsbereich auf Informationen von staatlichen Bibliotheken, Museen und Archiven ausgeweitet und die Grundsätze für die Bemessung von Entgelten für die Weiterverwendung präzisiert. Das Gesetz regelt, dass Metadaten jener Informationen, die über öffentlich zugängliche Netze in maschinenlesbaren Formaten bereitgestellt wurden, auf einem nationalen Datenportal zur Verfügung gestellt werden sollen. Die Zielrichtung des Richtlinien- und Gesetzgebers – nämlich die Förderung von Open Data –

---

72 Urteile vom 14. Februar 2012 (Rechtssache C-204/09) und vom 18. Juli 2013 (Rechtssache C-515/11)

73 Umweltinformationsgesetz in der Fassung der Bekanntmachung vom 27. Oktober 2014, BGBl. I S. 1643

74 siehe C 1.1

wird dadurch deutlich erkennbar. Auch die geänderten und am 17. Juli 2015 in Kraft getretenen Regelungen[75] enthalten kein Zugangsrecht; das richtet sich weiterhin nach den Informationsfreiheitsgesetzen.

Die G8-Staaten hatten sich auf fünf wesentliche Elemente zur Umsetzung von Open Data verständigt, vor allem auf das Kernprinzip, Daten der öffentlichen Verwaltung standardmäßig offen bereitzustellen.[76] Deutschland hat sich im Rahmen der G8-Open-Data-Charta im Juni 2013 zu Open Data bekannt und verpflichtet, einen Aktionsplan zur Umsetzung der Charta vorzulegen. Das Bundeskabinett hat diesen am 17. September 2014 beschlossen. Der Aktionsplan enthält verschiedene Verpflichtungen, um das genannte Ziel bis zum Ende des Jahres 2015 zu erreichen. Eine zentrale Rolle spielt das Bund-Länder-Portal „GovData – Das Datenportal für Deutschland“ als nationales Datenportal im Sinne des Informationsweiterverwendungsgesetzes. Nachdem GovData im Jahr 2013 als Betaversion freigeschaltet wurde, ist die Erprobungsphase inzwischen abgeschlossen. Am 1. Januar 2015 ging GovData in den Regelbetrieb; zudem übernahm die Freie und Hansestadt Hamburg vom Bund die Verantwortung für den Betrieb der Plattform; strategische Entscheidungen obliegen nach wie vor dem IT-Planungsrat.[77] Das Datenportal bietet über einen Katalog mit Metadaten einen einheitlichen, zentralen Zugang zu Verwaltungsdaten aus Bund, Ländern und Kommunen. Ziel ist es, diese Daten an einer Stelle auffindbar und so einfacher nutzbar zu machen.

Besondere öffentliche Aufmerksamkeit haben im Berichtszeitraum Entscheidungen des Bundesverwaltungsgerichts zum Informationsanspruch gegenüber dem Deutschen Bundestag gefunden. In zwei gleich gelagerten Fällen ging es um Informationen über den Sachleistungskonsum durch Abgeordnete für den Erwerb von iPods, Montblanc-Füllern und Digitalkameras.[78] Das Bundesverwaltungsgericht hat zwar unter Verweis auf den Ausschlussgrund des Informationsfreiheitsgesetzes zum Schutz mandatsbezogener Informationen einen Anspruch auf Namensnennung der einzelnen Abgeordneten verneint. Gleichzeitig hat das Gericht den Deutschen Bundestag aber verpflichtet, Auskunft zu bestimmten Fragen nach der Verwendung der Sachmittelpauschale zu erteilen, soweit sich diese Angaben auf die Gesamtheit der Mandatare beziehen.

---

75 Erstes Gesetz zur Änderung des Informationsweiterverwendungsgesetzes vom 8. Juli 2015, BGBl. I S. 1162

76 G8 Open Data Charta, beschlossen auf dem G8 Gipfel Staats- und Regierungschefs am Lough Erne (Vereinigtes Königreich von Großbritannien und Nordirland), veröffentlicht am 18. Juni 2013 durch die britische Präsidentschaft, siehe https://www.gov.uk/government/collections/g8-communique-and-documents

77 Unterrichtung durch die Bundesregierung: Digitale Verwaltung 2020, Regierungsprogramm 18. Legislaturperiode, Bundestags-Drucksache 18/3074 neu vom 30. Oktober 2014

78 Urteile des Bundesverwaltungsgerichts vom 27. November 2014, 7 C 19.12, 7 C 20.12

Ebenfalls mit dem Zugang zu Informationen des Parlaments hatte sich das Bundesverwaltungsgericht in zwei weiteren Fällen zu befassen.[79] Konkret strittig war die Herausgabe von Ausarbeitungen und Dokumentationen sowie einer vom Sprachendienst erstellten Übersetzung, die für den früheren Bundestagsabgeordneten Karl-Theodor zu Guttenberg angefertigt und von diesem für seine Dissertation verwendet worden waren. In einem zweiten Fall interessierte sich ein Antragsteller für ein Gutachten, das die Suche nach außerirdischem Leben, die Beobachtung unidentifizierter Flugobjekte und extraterrestrischer Lebensformen zum Gegenstand hatte. Das Bundesverwaltungsgericht hat entschieden, dass der Deutsche Bundestag eine informationspflichtige Stelle ist, soweit es um Gutachten der Wissenschaftlichen Dienste geht. Bei der Erstellung von Gutachten handele es sich um der Mandatsausübung vorgelagerte Verwaltungsaufgaben. Die Tatsache, dass Abgeordnete diese Unterlagen für ihre parlamentarische Tätigkeit nutzen, stehe dem nicht entgegen. Zudem enthält das Urteil ausführliche Darlegungen zum Urheberrecht. Es sei davon auszugehen, dass ein Beamter, der in Erfüllung seiner Dienstpflichten ein Werk geschaffen hat, seinem Dienstherrn stillschweigend sämtliche Nutzungsrechte einräumt, die dieser zur Erfüllung seiner Aufgabe benötigt. Dazu gehöre auch die Gewährung von Informationszugangsansprüchen. Öffentliche Stellen können damit Informationsbegehren kein Urheberrecht an von ihnen erstellten Gutachten entgegenhalten.

1.3 Länder

In die Diskussion um die Informationsfreiheit in jenen fünf Ländern, deren Gesetzgeber bislang kein Informationsfreiheitsgesetz verabschiedet haben, ist im Berichtszeitraum Bewegung gekommen. Kurz vor Ende des Berichtszeitraums ist das Landesinformationsfreiheitsgesetz Baden-Württemberg in Kraft getreten. Vorangegangen war eine langwierige Diskussion über die Einzelheiten der Umsetzung des von den Koalitionsfraktionen des Landtags bereits im Jahr 2011 vereinbarten Gesetzgebungsvorhabens. Im Rahmen der Anhörung zu dem Regierungsentwurf hatte die Konferenz der Informationsfreiheitsbeauftragten in Deutschland Stellung genommen.[80]

Eher schleppend geht die Vorbereitung eines Gesetzentwurfs in Niedersachsen voran. Zwar haben die Regierungsfraktionen bereits in ihrem Koalitionsvertrag vereinbart, eine umfassende Open-Data-Strategie mit einem modernen Informationsfreiheits- und Transparenzgesetz vorzulegen. Dieses soll staatliche Stellen verpflichten, alle relevanten Informationen digital in einem Transparenzregister zu veröffentlichen. Bis zum Redaktionsschluss dieses Tätigkeitsberichts wurde die Ankündigung aus dem Jahr 2013 jedoch nicht

[79] Urteile des Bundesverwaltungsgerichts vom 25. Juni 2015, 7 C 1.14, 7 C 2.14

[80] zur Bewertung des Entwurfs siehe D 5

umgesetzt; ein Referentenentwurf befand sich noch in der Ressortabstimmung.

Gleich zwei konkrete Entwürfe lagen dem Bayerischen Landtag vor. Eine Oppositionsfraktion hatte einen Entwurf für ein Bayerisches Transparenzgesetz in die Debatte eingebracht, dessen nahezu identischer Vorgänger bereits vor einigen Jahren gescheitert war. Gleichzeitig stellte die Landesregierung einen Entwurf zur Ergänzung des Bayerischen Datenschutzgesetzes vor. Dieser sieht ein Auskunftsrecht vor, verlangt vom Antragsteller aber die Darlegung eines berechtigten, nicht auf eine entgeltliche Weiterverwendung gerichteten Interesses. Während der Landtag den Entwurf für ein Transparenzgesetz ablehnte, traten die Änderungen des Bayerischen Datenschutzgesetzes im Dezember 2015 in Kraft.

Die hessischen Regierungsfraktionen haben in ihrem Koalitionsvertrag lediglich vereinbart, die Erfahrungen anderer Länder und des Bundes mit den jeweiligen Informationsfreiheitsgesetzen auszuwerten und zur Grundlage einer eigenen Regelung zu machen. Dabei soll bewertet werden, ob in der Praxis über die bestehenden Informationsrechte hinaus eine weitere Transparenz erreicht wird. Ein Entwurf der Landesregierung für ein Informationsfreiheitsgesetz dürfte nach diesen Vorgaben nicht so schnell zu erwarten sein. Stattdessen hat eine Oppositionsfraktion den Entwurf für ein Hessisches Transparenzgesetz in die parlamentarische Debatte eingebracht.

Die sächsischen Regierungsfraktionen beabsichtigen, in einem Informationsfreiheitsgesetz das Recht der Bürger klarzustellen, gegen angemessene Gebühren grundsätzlich Zugang zu behördlichen Informationen und Dokumenten zu bekommen. Ein konkreter Gesetzentwurf liegt bislang jedoch noch nicht vor.

In der Freien und Hansestadt Hamburg sieht das deutschlandweit erste Transparenzgesetz den Aufbau eines Transparenzregisters vor. Dieses hat im Oktober 2014 nach zwei Jahren der behördenübergreifenden Vorbereitung seinen Betrieb aufgenommen und wurde mit dem parallel entstandenen, landeseigenen Open-Data-Portal zusammengeführt. Das so entstandene Transparenzportal stellt – wie vom Hamburgischen Transparenzgesetz gefordert – alle veröffentlichungspflichtigen Daten und Dokumente zur Verfügung. Staatliche Gutachten, Senatsentscheidungen, Informationen über Subventionsempfänger, ein Baumkataster und eine Vielzahl von Verträgen der Hansestadt mit privaten Unternehmen sind auf diese Weise zugänglich. Die Zugriffszahlen belegen das enorme Interesse der Öffentlichkeit an diesem Portal. Hintergrund sind vermutlich die detaillierten Veröffentlichungspflichten des Gesetzes, die bewirken, dass die öffentlichen Stellen auch wirklich für die Bürger interessante Informationen einstellen müssen. So wird

gewährleistet, dass es sich nicht um eine verlängerte Öffentlichkeitsarbeit der Senatsverwaltung handelt.

Das Bremer Informationsfreiheitsgesetz wurde im Frühjahr 2015 ebenfalls erweitert. Es sieht nunmehr – ganz im Sinne eines Transparenzgesetzes – die verpflichtende Veröffentlichung von Informationen vor und enthält einen individuellen, d. h. notfalls auch gerichtlich einklagbaren Anspruch darauf. Das bisherige Informationsregister firmiert seit der Gesetzesänderung unter der Bezeichnung Transparenzportal Bremen.

Im Ergebnis eines umfangreichen Prozesses zur Beteiligung der Öffentlichkeit hat inzwischen auch Rheinland-Pfalz das bisherige Informationsfreiheitsgesetz zu einem Transparenzgesetz weiterentwickelt. Mit dem Gesetz wird die Verwaltung zur aktiven Veröffentlichung verpflichtet. Kern des Vorhabens ist die Schaffung einer digitalen Transparenzplattform. Außerdem führt das im November 2015 verabschiedete Landestransparenzgesetz das bisherige Landesinformationsfreiheitsgesetz und das Landesumweltinformationsgesetz zusammen. Rheinland-Pfalz ist damit das erste Flächenland, das über ein Transparenzgesetz verfügt. Die bisher auch für die Kommunen geltende – vor allem im Umweltinformationsrecht verankerte – Veröffentlichungspflicht wird dadurch jedoch nicht erweitert.

Vorhaben, ein bestehendes Informationsfreiheitsgesetz in ein umfassenderes Transparenzgesetz umzuwandeln, bestehen auch in anderen Bundesländern. So legten sich beispielsweise die Thüringer Regierungsfraktionen in ihrem Koalitionsvertrag darauf fest, das Informationsfreiheitsgesetz zu einem echten Transparenzgesetz nach dem Vorbild Hamburgs fortzuentwickeln. Die aktive Veröffentlichung von Informationen soll ausgebaut, die Bereichsausnahmen sowie die Versagensgründe sollen auf das verfassungsrechtlich zwingend gebotene Maß reduziert und Kontrollrechte des Informationsfreiheitsbeauftragten erweitert werden. Unabhängig hiervon wird die Verpflichtung aus dem Informationsfreiheitsgesetz, ein Informationsregister aufzubauen, in Thüringen umgesetzt. Allerdings steht den Behörden ein weitgehender Beurteilungsspielraum im Hinblick auf die dort einzupflegenden Informationen zu.

In Nordrhein-Westfalen ist verabredet worden, das Informationsfreiheitsgesetz zu einem Transparenzgesetz weiterzuentwickeln; bislang ist lediglich eine Open-Data-Strategie entstanden. Sie sieht zwar ausdrücklich das Bekenntnis zu wichtigen Open-Data-Prinzipien vor, enthält jedoch keinerlei Verpflichtung zur Veröffentlichung von Informationen. Vielmehr wird das Vorhaben als freiwillige Leistung betrachtet, welches eine Gesetzesänderung nicht erforderlich mache. Der Entwurf einer Oppositionsfraktion für ein Gesetz zur Verwirklichung von Transparenz und Informationsfreiheit im Land Nordrhein-Westfalen wurde bereits im Frühjahr 2014 abgelehnt.

Nachdem in Schleswig-Holstein das Informationsfreiheitsgesetz und das Umweltinformationsgesetz bereits im Jahr 2012 zu einem einheitlichen Informationszugangsgesetz zusammengeführt wurden, hat nunmehr 2014 auch die Landesverfassung eine wesentliche Ergänzung erfahren: Sie verpflichtet die Behörden des Landes, die Gemeinden und Gemeindeverbände, amtliche Informationen zur Verfügung zu stellen, soweit nicht entgegenstehende öffentliche oder schutzwürdige private Interessen überwiegen. Neben Brandenburg, das einen entsprechenden Passus bereits in seiner ursprünglichen Verfassung aus dem Jahr 1992 verankert hatte, ist Schleswig-Holstein nunmehr das zweite Land, das die Informationsfreiheit in den Verfassungsrang erhoben hat.

Im Berliner Informationsfreiheitsgesetz wurde im Berichtszeitraum vor dem Hintergrund der novellierten, bundesweiten Vorschriften zur Informationsweiterverwendung das bußgeldbewährte Verbot gestrichen, das die Veröffentlichung, Speicherung oder Sammlung von durch Akteneinsichten oder Aktenauskünfte erhaltenen Informationen zu gewerblichen Zwecken für unzulässig erklärte.

Verschiedene Landesgesetze zur Informationsfreiheit enthalten die Verpflichtung zur Evaluierung der Regelungen nach Ablauf einer bestimmten Frist. Dies ist auch in Sachsen-Anhalt der Fall. Das dortige Informationszugangsgesetz ist im Jahr 2008 in Kraft getreten und sah vor, dass die Auswirkungen des Gesetzes nach einem Erfahrungszeitraum von fünf Jahren seitens der Landesregierung unter Mitwirkung der kommunalen Spitzenverbände und gegebenenfalls weiterer Sachverständiger überprüft werden. Zur Unterstützung des Reformprozesses stellte der Landesbeauftragte für die Informationsfreiheit Sachsen-Anhalt Empfehlungen für die Weiterentwicklung des Informationsfreiheitsrechts vor. Unter anderem fordert er die Weiterentwicklung des Informationszugangsgesetzes zu einem modernen Transparenzgesetz, die Einführung eines Transparenzregisters und die Zusammenlegung des allgemeinen Informationsfreiheits- mit dem Umweltinformationsgesetz. Die Enquetekommission „Öffentliche Verwaltung konsequent voranbringen – bürgernah und zukunftsfähig gestalten“ des Landtags von Sachsen-Anhalt hat im September 2015 nach dreijähriger Tätigkeit ihren Abschlussbericht vorgelegt, der diese Empfehlungen weitgehend aufgreift. Eine Entscheidung der Landesregierung steht noch aus.

1.4 Brandenburg

Ebenso wie auf Bundesebene hat die Rechtsprechung des Gerichtshofs der Europäischen Union[81] zu einer Änderung des Brandenburgischen Umweltinformationsgesetzes geführt. Das Zweite Gesetz zur Änderung des Umweltin-

81 siehe C 1.1

formationsgesetzes des Landes Brandenburg trat am 7. Juli 2015 in Kraft.[82] Während vor der Änderung die obersten Landesbehörden nicht zu den informationspflichtigen Stellen gehörten, soweit sie im Rahmen der Gesetzgebung oder beim Erlass von Rechtsverordnungen tätig wurden, beschränkt sich diese Ausnahme in der aktuellen Fassung des Gesetzes nur noch auf ihre Tätigkeit im Rahmen der laufenden Gesetzgebung. Die Einschätzung des Gesetzgebers, dass diese Änderungen erforderlich waren, teilte die Landesbeauftragte. Die Gelegenheit der parlamentarischen Beratung zum Umweltinformationsrecht hat sie genutzt, um gegenüber dem Ausschuss für Ländliche Entwicklung, Umwelt und Landwirtschaft auf ein wesentliches Praxisproblem in diesem Zusammenhang hinzuweisen:[83]

Das Umweltinformationsgesetz des Landes Brandenburg ist, soweit sich ein Antrag auf Zugang zu Informationen über die Umwelt richtet, vorrangig vor dem Akteneinsichts- und Informationszugangsgesetz anzuwenden. Was unter den Begriff der Umweltinformation fällt, definiert das Umweltinformationsrecht in sehr weitgehender Weise. Dazu gehören bereits Maßnahmen oder Tätigkeiten, die sich auf die Umwelt auswirken oder wahrscheinlich auswirken oder den Umweltschutz bezwecken. Gemeint sind also mehr als nur Messdaten oder Umweltberichte. Vielmehr fällt ein großer Teil der Verwaltungsaufgaben auf den Gebieten der Planung, des Verkehrs und des Bauwesens darunter. Auf die entsprechenden Akten ist ausschließlich das speziellere Umweltinformationsgesetz des Landes Brandenburg anwendbar; es verdrängt das allgemeinere Akteneinsichts- und Informationszugangsgesetz. Auf den ersten Blick mag es als irrelevant erscheinen, welche Rechtsgrundlage für den Informationszugang zum Tragen kommt, ein zweiter Blick offenbart jedoch wesentliche Unterschiede in den Rechtsfolgen:

- Während das Umweltinformationsgesetz auch auf juristische Personen des Privatrechts anwendbar ist, soweit diese öffentliche Aufgaben im Zusammenhang mit der Umwelt wahrnehmen und dabei der Kontrolle öffentlicher Stellen unterliegen, kommt das Akteneinsichts- und Informationszugangsgesetz nur gegenüber den öffentlichen Stellen im engeren Sinne zum Tragen.

- Das Umweltinformationsgesetz gilt grundsätzlich auch während eines laufenden Verfahrens. Die Anwendbarkeit des Akteneinsichts- und Informationszugangsgesetzes hingegen ist bis zu einer bestands- oder rechtskräftigen Entscheidung nicht gegeben.

---

82 Zweites Gesetz zur Änderung des Umweltinformationsgesetzes des Landes Brandenburg vom 1. Juli 2015, GVBl I Nr. 19

83 Anlage 3 zum Protokoll der 5. Sitzung des Ausschusses für Ländliche Entwicklung, Umwelt und Landwirtschaft vom 22. April 2015, Landtags-Drucksache P-ALUL 6/5 vom 9. Juni 2015

- Eine Akteneinsicht vor Ort ist nach den Regelungen des Umweltinformationsrechts stets kostenfrei zu gewähren; das Akteneinsichts- und Informationszugangsgesetz sieht hierfür jedoch relativ hohe Gebühren vor.

- Sämtliche Ausnahmetatbestände des Umweltinformationsrechts unterliegen einer Abwägung mit dem öffentlichen Interesse am Informationszugang. Dies ermöglicht eine einzelfallgerechte Entscheidung, während das Akteneinsichts- und Informationszugangsgesetz zahlreiche Ablehnungstatbestände enthält, die eine Verweigerung der Informationsherausgabe zwingend vorsehen.

- Nach dem Umweltinformationsrecht sind bestimmte Informationen von den Behörden aktiv zu veröffentlichen; das Akteneinsichts- und Informationszugangsgesetz setzt hingegen in jedem Fall ein Antragsverfahren voraus.

Diese Beispiele lassen erkennen, dass die Anwendung des Umweltinformationsgesetzes des Landes Brandenburg für die Antragsteller häufig zu günstigeren Ergebnissen mit einem weiterreichenden Informationszugang führt. In der Praxis mangelt es jedoch nach unserer Erfahrung häufig an der Kenntnis dieser Rechtslage. Insbesondere sind der – nicht zuletzt aus der Rechtsprechung entwickelte – Umfang des Begriffs der Umweltinformation sowie die damit einhergehende Verdrängung des Akteneinsichts- und Informationszugangsgesetzes nicht hinreichend bekannt.

Aber auch informationspflichtige Stellen, die sich der Rechtslage bewusst sind, sind mit den Schwierigkeiten ihrer Umsetzung konfrontiert. Die genaue Abgrenzung der Umweltinformationen von allgemeinen Informationen und somit die Trennlinie zwischen beiden Gesetzen ist in der Praxis schwierig. Häufig stellt sich auch die Frage, wie zu verfahren ist, wenn sowohl spezielle Umweltinformationen als auch allgemeine Informationen in ein und derselben Akte vorhanden sind. Der Umgang mit solchen Unsicherheiten erfordert nicht selten eine zeitintensive Prüfung, die den Informationszugang verzögert.

Sowohl für Antragsteller als auch für informationspflichtige Stellen besteht erheblicher Beratungs- und Unterstützungsbedarf. Die gesetzliche Kompetenz der Landesbeauftragten für den Datenschutz und für das Recht auf Akteneinsicht erstreckt sich ausschließlich auf die Wahrung der Rechte nach dem Akteneinsichts- und Informationszugangsgesetz. Die gegenwärtige Rechtslage bedeutet daher, dass die Landesbeauftragte in zahlreichen Fällen nur feststellen kann, dass nicht das Akteneinsichts- und Informationszugangsgesetz, sondern ausschließlich das Umweltinformationsgesetz des Landes Brandenburg als Anspruchsgrundlage für einen Informationszugang zum Tragen kommt. Eine weitergehende Unterstützung von Antragstellern

oder Beratung von Verwaltungen steht ihr dann ebenso wenig zu wie die Vermittlung oder Kontrolle in Streitfällen. Auch gibt es keine andere Institution, die auf dem Gebiet des Umweltinformationsrechts eine vergleichbare Ombudsfunktion innehat.

Antragsteller stehen somit vor folgendem Dilemma: Mit dem spezielleren Umweltinformationsgesetz des Landes Brandenburg steht ihnen zwar ein weitgehender Informationszugang zu. Verweigert die informationspflichtige Stelle diesen, bleibt ihnen lediglich der Rechtsweg, um ihre Ansprüche durchzusetzen. Der Landesbeauftragten fehlt für eine Unterstützung die gesetzliche Kompetenz. Anders sieht es beim Akteneinsichts- und Informationszugangsgesetz aus: Hier können Antragsteller mit ihrer Unterstützung rechnen, haben dafür aber einen wesentlich weniger umfangreichen Anspruch auf Informationszugang. Vor allem weisen gerade jene Verwaltungsaufgaben, die von hohem Interesse für die Bürger (z. B. Planen, Verkehr, Bauen) sind, häufig einen Umweltbezug auf und sind dem Akteneinsichts- und Informationszugangsgesetz deshalb zum großen Teil entzogen.

Auf diese Probleme hatte die Landesbeauftragte bereits im Rahmen der zurückliegenden Novellierung des Akteneinsichts- und Informationszugangsgesetzes im Jahr 2013 aufmerksam gemacht. Ihr Vorschlag, die beiden Rechtsgrundlagen zu einem einheitlichen Informationszugangsgesetz zusammenzuführen, fand damals leider keine Berücksichtigung. Auch die Forderung der Konferenz der Informationsfreiheitsbeauftragten in Deutschland nach einer effektiven Kontrollzuständigkeit vom 28. November 2013 fand im Land keine Resonanz. Gegenüber dem Ausschuss für Ländliche Entwicklung, Umwelt und Landwirtschaft regte die Landesbeauftragte erneut eine weitergehende Befassung mit dem Informationszugangsrecht in Brandenburg an. Aufgegriffen wurde diese Anregung bislang nicht.

Im letzten Tätigkeitsbericht hatten wir darüber informiert, dass sich der Gesetzgeber nicht dazu entschließen konnte, die im September 2013 erfolgte Novellierung des Akteneinsichts- und Informationszugangsgesetzes zu nutzen, um Open Data dort gesetzlich zu verankern. Der Landtag verabschiedete lediglich einen Beschluss, mit dem die Landesregierung gebeten wurde, die Beteiligung des Landes Brandenburg an der Bund-Länder-Plattform GovData zu forcieren, Vorbereitungen für die Veröffentlichung von Daten des Landes im bestehenden Landesportal (www.brandenburg.de) zu treffen und den Aspekt Open Data bei der Weiterentwicklung der E-Government-Strategie des Landes zu berücksichtigen.

In seinem Bericht an den Ausschuss für Inneres des Landtags Brandenburg zur Umsetzung dieser Entschließung vom 5. Mai 2014[84] wies das Ministerium des Innern auf die Vorbereitung einer Verwaltungsvereinbarung zu GovData hin. Das Land Brandenburg hat am 1. Dezember 2014 diese Vereinbarung des Bundes und der Länder zum gemeinsamen Betrieb von „GovData – Das Datenportal für Deutschland“ (Verwaltungsvereinbarung GovData) unterzeichnet, die kurz darauf in Kraft trat.[85] In der Vereinbarung heißt es unter anderem: „Die Vereinbarungspartner beteiligen sich an der bedarfsorientierten Weiterentwicklung von GovData, achten auf eine koordinierte Bereitstellung von Metadaten, wirken bei übergreifenden Aufgaben mit und fördern in ihrem Bereich die Bekanntheit und Nutzung von GovData.“ Sie stellen außerdem die Finanzierung von GovData sicher. Vereinbarungspartner sind neben der Bundesrepublik Deutschland die Länder Baden-Württemberg, Berlin, Nordrhein-Westfalen, Rheinland-Pfalz, der Freistaat Sachsen und die Freie und Hansestadt Hamburg, die gleichzeitig Sitz der Koordinierungs- und Geschäftsstelle ist.

Ansonsten beschrieb das Ministerium des Innern in seinem Bericht an den Landtag im Wesentlichen, welche Maßnahmen zu ergreifen sind, um die Veröffentlichung von Daten des Landes im bestehenden Landesportal zu ermöglichen. Der Bericht regte an, für die flächendeckende Einführung von Open Government Data in der Landesverwaltung Brandenburg gesetzliche Rahmenregelungen in Erwägung zu ziehen und dabei auch das Verhältnis zum antragsbezogenen Informationszugang nach dem Akteneinsichts- und Informationszugangsgesetz zu berücksichtigen. Für erforderlich hielt das Ministerium weiterhin eine grundsätzliche gesetzgeberische Wertentscheidung zur Frage der unentgeltlichen Datenbereitstellung sowie zur Etatisierung im Landeshaushalt.

In seinen Ausführungen zur Weiterentwicklung der Open-Data-Strategie des Landes wies der Bericht auf die Erforderlichkeit der Berücksichtigung der Ebenen des Bundes und der Europäischen Union hin. Nicht zuletzt legte das Ministerium auch hier in seinen rechtssystematischen Erwägungen einen gesetzgeberischen Handlungsbedarf nahe. Im Vergleich zu der noch in der Stellungnahme der Landesregierung zum letzten Tätigkeitsbericht der Landesbeauftragten[86] dargestellten Auffassung, nach der Open Data und der Informationszugang nach dem Akteneinsichts- und Informationszugangsge-

---

84 Anlage 18 zum Protokoll der 53. Sitzung des Ausschusses für Inneres vom 22. Mai 2014, Landtags-Drucksache P-AI 5/53/2 vom 16. Juni 2014

85 Bekanntmachung der Vereinbarung des Bundes und der Länder zum gemeinsamen Betrieb von „GovData – Das Datenportal für Deutschland“ vom 16. März 2015, Amtsblatt für Brandenburg, Nr. 14 vom 15. April 2015, S. 331

86 Stellungnahme der Landesregierung zum Tätigkeitsbericht für die Jahre 2012 und 2013 der Landesbeauftragten für den Datenschutz und für das Recht auf Akteneinsicht, Landtagsdrucksache Nr. 5/9426 vom 15. August 2014

setz unterschiedliche Materien beträfen und Regelungen zu Open Data in diesem Gesetz nicht sachgerecht seien, stellt diese Ergebnisoffenheit immerhin eine Weiterentwicklung dar.

Abgesehen von der begrüßenswerten Beteiligung des Landes an dem Portal GovData spielte die Landesregierung die Sache kurz vor dem Auslaufen der 5. Legislaturperiode mit der Geltendmachung einer verbindlichen politischen Entscheidung jedoch wieder an das Parlament zurück. Im Februar 2015 teilte das Ministerium des Innern und für Kommunales der Landesbeauftragten auf Nachfrage mit, dass es beabsichtige, Informationen sukzessive und auf Basis der zur Verfügung stehenden Mittel auf dem GovData-Portal bereitzustellen. Das Ministerium prüfe sowohl Maßnahmen zur Akzeptanzerhöhung in den Ressorts der Landesregierung als auch die Erforderlichkeit von Rechtsvorschriften für Open Government Data. Ein Ergebnis dieser Prüfung lag der Landesbeauftragten bis zum Redaktionsschluss dieses Tätigkeitsberichts nicht vor.

Die Landesbeauftragte hält an ihrer Auffassung fest, dass es einer Modernisierung des Informationszugangsrechts in Brandenburg bedarf. Sie fordert die Zusammenführung des Umweltinformationsgesetzes mit dem Akteneinsichts- und Informationszugangsgesetz sowie die Schaffung einer – neben dem antragsgebundenen Informationsanspruch – zweiten Säule durch konkrete Veröffentlichungspflichten im Sinne von Open Data.

Auf dem Gebiet der Rechtsprechung zum Akteneinsichts- und Informationszugangsgesetz sind zwei Entscheidungen hervorzuheben: Das Oberverwaltungsgericht Berlin-Brandenburg wies eine Beschwerde gegen die Ablehnung einer einstweiligen Anordnung zur Offenlegung von Unterlagen zurück, die der ehemalige Ministerpräsident in seiner Funktion als Aufsichtsratsmitglied der Flughafen Berlin-Brandenburg GmbH erhalten hatte.[87] Es bestätigte damit die Auffassung des Verwaltungsgerichts Potsdam. Es gebe keine Koppelung beider Funktionen; als Aufsichtsratsmitglied habe der Ministerpräsident nicht zu den auskunftsverpflichteten Stellen gehört. Außerdem handele es sich nicht um Akten im Sinne des Akteneinsichts- und Informationszugangsgesetzes. Das Oberverwaltungsgericht verwies auf die spezialgesetzlichen Verschwiegenheitspflichten aus dem Aktiengesetz, die vom Jedermanns-Anspruch des Akteneinsichts- und Informationszugangsgesetzes unberührt blieben und auch bei privaten Unternehmen in öffentlicher Hand keine Einschränkung erführen. Zudem spreche viel dafür, dass Betriebs- und Geschäftsgeheimnisse betroffen seien, deren Offenbarung sich im Wettbewerb mit anderen Flughafenbetreibern nachteilig auswirken könne.

87 Urteil des Oberverwaltungsgerichts Berlin-Brandenburg vom 1. April 2014, 12 S 77.13

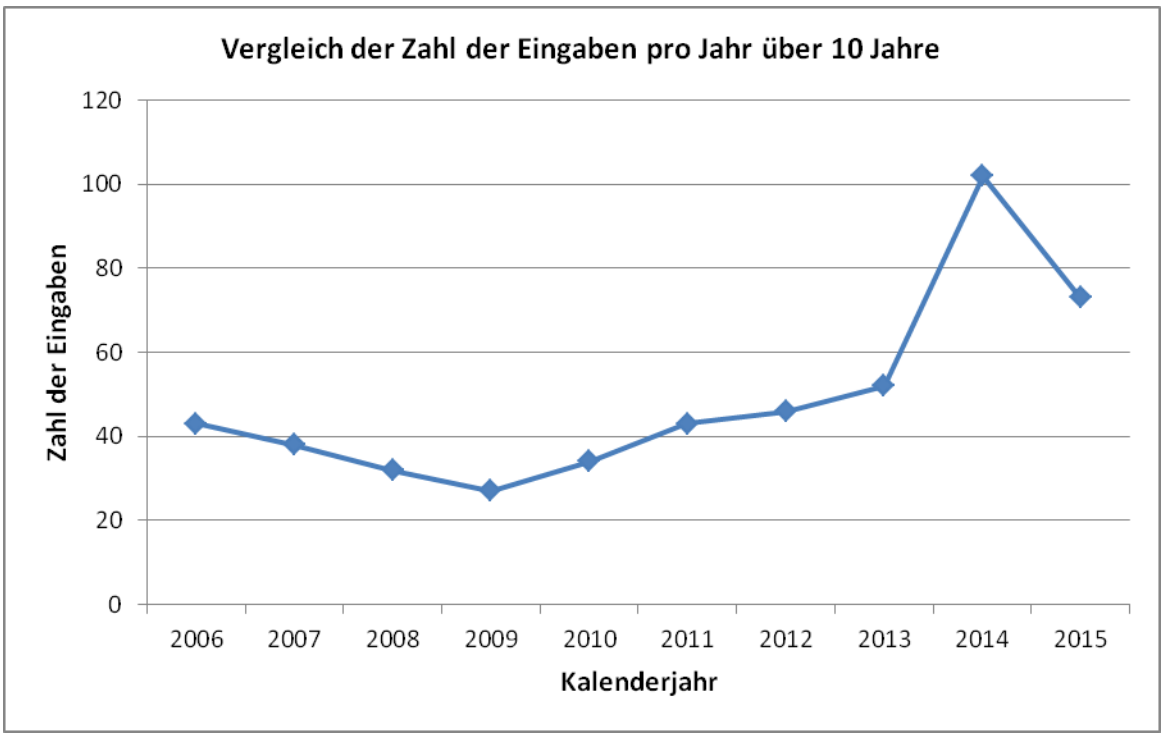
In einer weiteren Entscheidung urteilte das Oberverwaltungsgericht Berlin-Brandenburg, dass dem Zugang zu einem speziellen Gutachten zur Waldwertermittlung sowie zur Ermittlung eines möglichen Planungsgewinns der Schutz des Betriebs- und Geschäftsgeheimnisses entgegenstehe.[88] Das allein mit Blick auf die Vertragsverhandlungen erstellte Gutachten sei in dem in Rede stehenden Fall maßgeblich für die Kaufpreisbildung und die Vertragsgestaltung gewesen. Es sei hinreichend plausibel und nachvollziehbar, dass das Gutachten zumindest mittelbar Rückschlüsse auf wettbewerbsrelevante Entwicklungsstrategien, Kalkulationen und Renditeerwartungen des Vertragspartners zulässt. Auch solche mittelbaren Rückschlüsse auf Betriebs- und Geschäftsgeheimnisse werden von dem gesetzlichen Ausschlussgrund erfasst.

2 Eingaben bei der Landesbeauftragten

Die Landesbeauftragte für den Datenschutz und für das Recht auf Akteneinsicht hat nach § 11 Akteneinsichts- und Informationszugangsgesetz (AIG) die Aufgabe, das Grundrecht auf Akteneinsicht und Informationszugang zu wahren. Sie berät sowohl Bürger als auch öffentliche Stellen bei der Nutzung und Umsetzung des Akteneinsichts- und Informationszugangsgesetzes. Nach § 11 Abs. 1 AIG hat jeder das Recht, die Landesbeauftragte anzurufen, wenn er der Auffassung ist, in seinem Recht auf Informationszugang verletzt zu sein. Die folgenden Ausführungen beschränken sich auf die formalen Eingaben, also auf Beschwerden, die im Rahmen des oben genannten Anrufungsrechts – in der Regel schriftlich – an die Landesbeauftragte herangetragen wurden. Nur in diesen Fällen verfügt sie über ausreichende Informationen, die den Erfordernissen einer statistischen Auswertung genügen. Anfragen, die sie und ihre Mitarbeiter täglich mehrfach beantworten, werden statistisch nicht erfasst.

An der Zahl der Eingaben bei der Landesbeauftragten lässt sich eine stetige Entwicklung der Praxis des Informationszugangsrechts in Brandenburg erkennen, zumindest in quantitativer Hinsicht: In den fünf Jahren zwischen 2009 und 2013 hat sich die Zahl der Beschwerden insgesamt nahezu verdoppelt. Für eine weitere Verdoppelung bedurfte es dann nur noch eines einzigen Kalenderjahres, nämlich 2014. Von diesem hohen Niveau aus (in absoluten Zahlen handelte es sich um 102 Beschwerdeverfahren) hat sich die Zahl im Jahr 2015 hingegen um circa ein Viertel reduziert. Verglichen mit dem Jahr vor dem Berichtszeitraum (2013: 52; 2015: 74 Beschwerdeverfahren) handelt es sich aber immer noch um eine Steigerung in Höhe von über 40 vom Hundert.

88 Urteil des Oberverwaltungsgerichts Berlin-Brandenburg vom 6. März 2014, 12 B 19.12



Der massive Anstieg der Beschwerden im Jahr 2014 ging mit einer verstärkten Nutzung der Internetplattform www.fragdenstaat.de einher. Allerdings bewegte sich die Zahl der Petenten, die auf diese Weise an uns herantraten, im niedrigen einstelligen Bereich. Diese hohe Aktivität einzelner Antragsteller war im Jahr 2015 nicht mehr zu verzeichnen. Zwar reichten immerhin noch 29 vom Hundert ihre Beschwerden über die Plattform ein, ein nennenswerter Anteil einzelner Personen hieran war jedoch nicht gegeben. Wertet man den hohen Wert des Vorjahres in dieser Weise als Ausreißer, lässt sich seit dem Jahr 2009 ein kontinuierlicher Anstieg der Beschwerden feststellen. Die Nutzung der genannten Plattform scheint sich im Übrigen etabliert zu haben (2013: 10 %, 2014: 68 %, 2015: 27 % der Eingaben).

Lohnt es sich überhaupt, die Landesbeauftragte bei Schwierigkeiten mit der Wahrnehmung des Informationszugangsrechts anzurufen? Die Antwort auf diese Frage ist schwer in Zahlen zu fassen. Im Jahr 2015 war der Anteil der offenen Fälle mit über 60 % der Gesamtzahl ungewöhnlich hoch. Die Gründe hierfür sind vielfältig: Der Abschluss aufwendigerer oder spät im Jahr gestellter Beschwerden ist erst im Folgejahr möglich und entzieht sich dadurch der Auswertung. Teilweise erledigen sich die Anliegen der Beschwerdeführer auch aus der Sache heraus, d. h. ohne dass eine Entscheidung zum Informationszugang noch erforderlich wäre. In anderen Fällen belässt die Landesbeauftragte es bei einer informationszugangsrechtlichen Beratung der informationspflichtigen Stellen, weil sie Gründe hat, von einer künftig rechtmäßigen Bearbeitung auszugehen. Eine Kenntnis über das abschließende Ergebnis liegt ihr in solchen Fällen nicht vor. Im Jahr 2015 wurde der Informationszugang in genau der Hälfte der Beschwerden, deren Ergebnis vorliegt, nach unserem Tätigwerden gewährt. Dies entspricht dem Vorjahreswert. In der

Mehrzahl der übrigen Fälle stellten wir fest, dass beispielsweise Ausnahmetatbestände des Akteneinsichts- und Informationszugangsgesetzes der Einsichtnahme entgegenstanden und Anträge daher zu Recht abzulehnen waren.

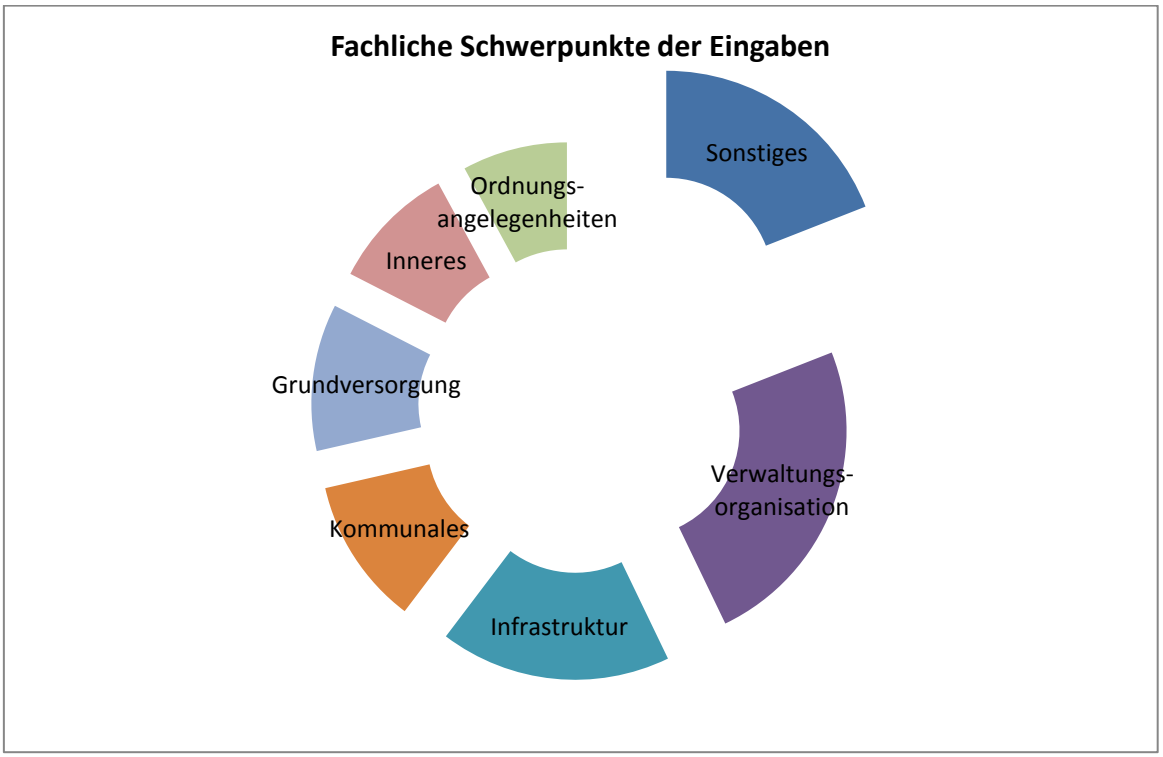
Hauptproblem im Jahr 2015 war erneut die Überschreitung der Bearbeitungsfrist, d. h. in einer Vielzahl der Fälle musste die Landesbeauftragte zunächst darauf hinweisen, dass ein Antrag in der Regel spätestens nach einem Monat bearbeitet sein muss. Die ebenfalls häufig auftretenden Unsicherheiten zum Anwendungsbereich betrafen erstens die Nichtanwendbarkeit des Gesetzes auf privatrechtlich organisierte Unternehmen der öffentlichen Hand, zweitens die seit der Novellierung im Jahr 2013 erweiterte Anwendbarkeit des Akteneinsichts- und Informationszugangsgesetzes auf die mittelbare Staatsverwaltung (Körperschaften des öffentlichen Rechts) und drittens den Ausschluss des Anspruchs auf Akteneinsicht während des laufenden Verfahrens. Nur mit knappem Abstand folgten Schwierigkeiten bei der Abgrenzung von Anspruchsgrundlagen. Diese bezogen sich nach wie vor im Wesentlichen auf die Überschneidungen zum Umweltinformationsrecht. Dass sich die statistische Relevanz des Verhältnisses zwischen dem allgemeinen Akteneinsichtsrecht und dem spezielleren, vorrangigen Umweltinformationsrecht im Vergleich zu früheren Jahren verringert hat, liegt keineswegs daran, dass dieses Problem in der Praxis der Informationsfreiheit in Brandenburg an Bedeutung verloren hätte. Der Effekt ist vielmehr darauf zurückzuführen, dass die Landesbeauftragte seit der parlamentarischen Entscheidung aus dem Jahr 2013, beide Rechtsgrundlagen nicht zusammenzuführen, dazu übergegangen ist, bereits im Vorfeld der Einreichung von Eingaben darauf hinzuweisen, dass ihr auf dem Gebiet des Umweltinformationsrechts keine Kompetenzen zustehen. Beschwerden, die in der Sache möglicherweise berechtigt sind, kann sie angesichts der Rechtslage ohnehin nicht nachgehen.

Häufig waren Fragen zur Bescheidung von Anträgen auf Akteneinsicht zu klären. Dabei ging es – insbesondere im Hinblick auf Anfragen, die über die Plattform www.fragdenstaat.de gestellt wurden – um das Schriftformerfordernis im Falle einer (teilweisen) Ablehnung oder Kostenerhebung. Nicht selten waren Ablehnungsbegründungen formal bzw. inhaltlich mangelhaft oder nicht nachzuvollziehen.

Im Hinblick auf die materiellen Ausnahmen vom Akteneinsichtsrecht standen der Umgang mit personenbezogenen Daten sowie mit solchen öffentlichen Geheimhaltungsinteressen, die eine zwingende Ablehnung des Zugangsbegehrens nach sich ziehen, bzw. mit spezialgesetzlichen Geheimhaltungspflichten im Vordergrund. Die Art und Weise des Informationszugangs schien trotz der eindeutigen Klarstellung des Gesetzgebers, dass in der Regel ein Wahlrecht zwischen Einsichtnahme, der Herausgabe von Kopien oder einem Zugang in elektronischer Form besteht, noch immer für Unsicherheiten zu

sorgen. Soweit Unternehmensdaten von Einsichtsanträgen betroffen waren, musste häufig das in solchen Fällen obligatorische Anhörungsverfahren erörtert werden. Auch die Erhebung von Kosten, die Verpflichtung des Antragstellers zur hinreichenden Bestimmung des Antrags sowie der Umgang mit Aussonderungen (Schwärzungen) stellten sich als Herausforderungen für Verwaltungen und Antragsteller heraus.

In welchen Fachbereichen das Einsichtsinteresse der Antragsteller am größten ist, lässt sich statistisch nur schwer kategorisieren. Insbesondere bereitet die Zuordnung der Anträge zu einzelnen Themen Schwierigkeiten. Im Ergebnis zeigte sich, dass Beschwerden über die Verweigerung von Informationen zur Verwaltungsorganisation öffentlicher Stellen im zweiten Berichtsjahr erstmals den ersten Rang einnahmen. Dieser Trend zeichnete sich bereits im Vorjahr ab. Beispielsweise ging es dabei um Angaben zum Haushalt, zum Personalbestand, zur Geschäftsverteilung oder auch zu verwaltungsinternen Vorschriften. Interessant ist diese Entwicklung vor allem deshalb, weil es sich hier in der Regel um einen Bereich handelt, der nur eine geringe unmittelbare Außenwirkung entfaltet und lange Zeit als „intern“, d. h. im Verständnis vieler Verwaltungen als uninteressant für die Öffentlichkeit galt. Die mittlerweile achtzehnjährige Praxis der Informationsfreiheit in Brandenburg zeigt, dass das Akteneinsichts- und Informationszugangsgesetz den Begriff „intern“ aus gutem Grunde nicht kennt und es dem Antragsteller überlässt, für welche Informationen er sich interessiert.



Der zweitwichtigste Aspekt, für den sich Antragsteller interessierten, betraf infrastrukturelle Aufgaben der öffentlichen Stellen, also vor allem Planen,

Bauen, Wohnen und Verkehr. Lange Zeit war dies die unumstrittene Nummer eins unter den Beschwerden. Hier und im Umweltbereich waren auch die Überschneidungen mit dem Umweltinformationsrecht am bedeutendsten. Den kommunalen Aufgaben wurden in der Statistik solche Anträge zugeordnet, die im weitesten Sinne mit kommunalrechtlichen Fragestellungen zusammenhingen, insbesondere in Bezug auf die kommunalen Vertretungskörperschaften. Fachaufgaben, die von den Kommunen erledigt werden, sind davon nicht umfasst. Unter Grundversorgung sind im Wesentlichen Aufgaben zu verstehen, die mit der Wasserver- und Abwasserentsorgung zusammenhängen und meist von Zweckverbänden wahrgenommen werden. Aktuelle Probleme der Beitragserhebungen im Land Brandenburg dürften hier im Fokus gestanden haben. Zum Bereich des Innern gehören beispielsweise Aufgaben der Polizei und des Vermessungswesens. Ordnungsangelegenheiten umfassen Genehmigungen für Veranstaltungen oder Ähnliches.

3 Kein laufendes Steuerverfahren durch (geplante) Insolvenzanfechtungen

Eine Reihe von Insolvenzverwaltern begehrte nach Eröffnung der Insolvenzverfahren bei den zuständigen Finanzämtern Einsicht in Kontoauszüge der Insolvenzschuldner. Die Besteuerungsverfahren, deren Bestandteil diese Kontoauszüge sind, waren zum Zeitpunkt der Insolvenzanfechtungen längst abgeschlossen. Die Finanzbehörden machten – dessen ungeachtet – unisono geltend, das Besteuerungsverfahren laufe bis zum Abschluss des Insolvenzverfahrens weiter. Das Akteneinsichts- und Informationszugangsgesetz sei deshalb nicht anwendbar.

Hintergrund der Anträge der Insolvenzverwalter auf Zugang zu den bei den Finanzämtern vorhandenen Jahreskontoauszügen der Insolvenzschuldner waren fehlende konkrete Kenntnisse über Zeitpunkt und Höhe der einzelnen Steuerzahlungen oder auch eine Unklarheit über die Vollständigkeit der bei Insolvenzschuldnern vorgefundenen Informationen. Die Insolvenzverwalter beabsichtigten, die steuerlichen und wirtschaftlichen Verhältnisse der Insolvenzschuldner aufzuarbeiten, um daraus Anfechtungsansprüche im Rahmen des Insolvenzverfahrens abzuleiten bzw. diese Ansprüche beziffern zu können.

Nach § 2 Abs. 4 Akteneinsichts- und Informationszugangsgesetz (AIG) wird Akteneinsicht in laufenden Verfahren bis zu einer bestands- oder rechtskräftigen oder in sonstiger Weise beendenden Entscheidung nur nach Maßgabe des jeweils anzuwendenden Verfahrensrechtes gewährt. Ein solcher Ausschluss vom Anwendungsbereich des Gesetzes besteht in den übrigen Informationsfreiheitsgesetzen nicht. Das in anderen Ländern durch die verwal-

tungsgerichtliche Rechtsprechung längst eindeutig bejahte Einsichtsrecht der Insolvenzverwalter sei, so argumentierten die brandenburgischen Finanzbehörden, aufgrund dieser Besonderheit des Landesrechts jedoch nicht übertragbar. Steuerforderungen würden durch die Insolvenzanfechtungen vielmehr wieder aufleben, sodass die Besteuerungsverfahren bis zum Abschluss der Insolvenzverfahren weiterliefen und die Anträge abzulehnen gewesen seien.

Diese landesspezifische Ausnahme hat der Gesetzgeber aufgenommen, weil Brandenburg als Vorreiter des ersten Akteneinsichts- und Informationszugangsgesetzes im Jahr 1998, die damals noch bestehende Bundeseinheitlichkeit des Verwaltungsverfahrensrechts nicht gefährden wollte. Obwohl diese Einheitlichkeit dann schon längst nicht mehr bestand, verschärfte der Gesetzgeber den Wortlaut der Ausnahme im Rahmen der Novellierung, die im Oktober 2013 in Kraft trat. Interessanterweise zeigt sich aber an der Berufung der Finanzbehörden auf den nur in Brandenburg bestehenden Schutz laufender Verfahren, dass es gerade das Land Brandenburg ist, das hier – verglichen mit den Informationsfreiheitsgesetzen anderer Länder – ausschert.

Mehrere Insolvenzverwalter beschwerten sich bereits im vorigen Berichtszeitraum bei der Landesbeauftragten über die beschriebene Verweigerung der Akteneinsicht durch die Finanzämter. In ihren Stellungnahmen verwiesen diese teilweise auf das Ministerium der Finanzen, mit dem die Landesbeauftragte die weitere Angelegenheit erörterte. Dies geschah auch mit dem Ziel, eine landesweite Klärung der diesen Fällen zu Grunde liegenden Rechtsfragen zu erreichen. Die Landesbeauftragte vertrat dabei die Auffassung, dass das ursprüngliche Besteuerungsverfahren weder durch die begehrte Akteneinsicht noch durch die Erhebung von Ansprüchen auflebt. Sie legte vielmehr dar, dass dies frühestens mit der erfolgreich durchgeführten Anfechtung der Fall sein könne. Der Ausschluss der Einsichtnahme in die Kontoauszüge vom Anwendungsbereich des Akteneinsichts- und Informationszugangsgesetzes komme somit gar nicht zum Tragen. Auch handele es sich bei zivilrechtlichen Insolvenzverfahren keineswegs um Verfahren im Sinne dieser Vorschrift. Das Ministerium der Finanzen hielt jedoch an seiner Auffassung fest, dass das Insolvenzverfahren untrennbar mit dem Besteuerungsverfahren verknüpft sei und deshalb insgesamt ein noch nicht abgeschlossenes Verfahren vorliegt. Die Insolvenzverwalter legten zwischenzeitlich Klage ein.

Im Ergebnis haben die Verwaltungsgerichte die Auffassung der Landesbeauftragten bestätigt und ein weitgehendes Einsichtsrecht der Insolvenzverwalter bejaht.[89] Gegen zwei dieser Entscheidungen hatten die beklagten Finanzäm-

[89] Urteile des Verwaltungsgerichts Potsdam vom 26. Juli 2013, 9 K 1767/12 sowie vom 24. April 2014, 9 K 312/13 und des Verwaltungsgerichts Cottbus vom 25. März 2015, 1 K 898/12

ter beim Oberverwaltungsgericht Berlin-Brandenburg die Zulassung der Berufung beantragt. Dieses ließ die Berufung insoweit zu, als es offen erschien, ob das Steuergeheimnis dem Informationszugang entgegensteht. Das Gericht stellte aber fest, dass die streitbefangenen Steuervorgänge den Klägern als Insolvenzverwaltern gegenüber keiner Geheimhaltungspflicht unterliegen und das Steuergeheimnis durch die begehrte Akteneinsicht nicht berührt wird. Im Übrigen lehnte es die Anträge ab. Insbesondere bestätigte das Oberverwaltungsgericht die Auffassung der Vorinstanz, dass ein Besteuerungsverfahren durch Steuerforderungen im Rahmen eines Insolvenzverfahrens nicht auflebt, mithin die Ausnahme laufender Verfahren vom Anwendungsbereich des Akteneinsichts- und Informationszugangsgesetzes nicht zum Tragen kommt sowie überwiegende öffentliche oder private Geheimhaltungsinteressen dem Informationszugang nicht entgegenstehen.[90] Die erstinstanzliche Verpflichtung, den Insolvenzverwaltern die Jahreskontoauszüge herauszugeben, hat somit Bestand.

Die Herausgabe der Jahreskontoauszüge von Insolvenzschuldnern an deren Insolvenzverwalter verstößt weder gegen das Steuergeheimnis noch bewirkt es ein Wiederaufleben abgeschlossener Besteuerungsverfahren. Die Ausnahme zum Schutz laufender Verfahren kann den Antragstellern somit nicht entgegengehalten werden. Die Kontoauszüge sind herauszugeben.

4 Informationszugang bei berufsständischen Kammern

Seit seiner Novellierung fallen auch berufsständische Kammern unter den Anwendungsbereich des Akteneinsichts- und Informationszugangsgesetzes. Einige von ihnen tun sich mit der Gewährung von Informationsansprüchen aber noch schwer.

Ein antragstellender Verein bat in ähnlich lautenden Begehren verschiedene Kammern des Landes Brandenburg um die Herausgabe von Informationen. Dabei ging es vor allem um bestimmte Daten aus dem Jahresabschluss, wie zum Beispiel die Einnahmen und Ausgaben einzelner Haushaltsjahre, das Eigenkapital bzw. Kammervermögen sowie Daten zu den Rücklagen. Außerdem interessierte sich der Verein für Angaben zu Vergütungen der Geschäftsführung, also für deren Jahresbruttogehalt sowie für etwaige zusätzliche Leistungen. Nachdem die meisten Kammern auf diese Anträge entweder nicht reagiert oder den Informationszugang pauschal und ohne Bezugnahme auf konkrete gesetzliche Ablehnungstatbestände verweigert hatten, trat die

[90] Beschlüsse des Oberverwaltungsgerichts Berlin-Brandenburg, vom 4. August 2014, 12 N 36.14 und 7. Oktober 2014, 12 N 83.13. Beide Beschlüsse beziehen sich auf die o. g. Urteile des Verwaltungsgerichts Potsdam.

Landesbeauftragte an diese Stellen heran und wies auf die Rechtslage hin. Außerdem machte sie auf eine Entschließung der Konferenz der Informationsfreiheitsbeauftragten in Deutschland aufmerksam. Diese forderten die berufsständischen Kammern auf, ihren Transparenzverpflichtungen nachzukommen.[91]

Mit In-Kraft-Treten der Novellierung des Akteneinsichts- und Informationszugangsgesetzes im Oktober 2013 wurde dessen Anwendungsbereich auf die mittelbare Staatsverwaltung ausgeweitet. Gegenüber Kammern, die als Körperschaften des öffentlichen Rechts des Landes verfasst sind, besteht somit grundsätzlich ein voraussetzungsloses Recht auf Akteneinsicht. Die Ablehnung eines Antrags ist nur zulässig, soweit die Ausnahmetatbestände des Gesetzes – insbesondere zum Schutz überwiegender öffentlicher und privater Interessen – erfüllt sind. Ein Antrag auf Informationszugang ist zudem innerhalb eines Monats zu bescheiden, eine Ablehnung schriftlich zu begründen. Im Hinblick auf die Haushaltsdaten ist nicht zu erkennen, dass eine Schutzvorschrift des Akteneinsichts- und Informationszugangsgesetzes deren Herausgabe entgegensteht. Da es eine spezielle Verpflichtung zur Offenlegung der Gehaltsangaben der Geschäftsführung nicht gibt, diese aber als personenbezogene Daten nur unter Vorbehalt der Zustimmung des Betroffenen offenbart werden dürfen, besteht für diesen Teil der Anfrage ein Zugangsrecht nur, soweit das Einverständnis erteilt wurde.

Die Reaktionen auf die Hinweise der Landesbeauftragten waren recht unterschiedlich: Eine Kammer gab sämtliche Informationen heraus. Dies umfasste auch die Angaben zum Verdienst der Geschäftsführung. Da die Geschäftsführerin persönlich antwortete, war klar, dass ihr erforderliches Einverständnis mit der Offenlegung dieser personenbezogenen Daten vorlag. Eine andere Kammer legte die erfragten Haushaltsangaben offen, eine weitere beantwortete auch die darauf gerichteten Fragen nur unvollständig.

In einem weiteren Fall stützte die Kammer ihre Ablehnung des Informationszugangs pauschal auf eine nicht näher begründete Verschwiegenheitspflicht. Nachdem wir auf die Rechtslage hingewiesen hatten, änderte sie ihre Taktik und machte geltend, dem Anwendungsbereich des Akteneinsichts- und Informationszugangsgesetzes gar nicht zu unterfallen. Ihr Kernargument lautete, sie sei zwar eine Körperschaft des öffentlichen Rechts, jedoch nicht, wie das Gesetz es fordert, des Landes Brandenburg, sondern lediglich im Land Brandenburg. Diese Entscheidung habe der Vorstand – trotz einer gegensätzlichen Auffassung der zuständigen Rechtsaufsichtsbehörde – einstimmig getroffen. Auf Nachfrage konnte uns die Kammer nicht mitteilen, welches Recht denn sonst für sie gelten würde.

---

[91] Entschließung der Konferenz der Informationsfreiheitsbeauftragten „Auch Kammern sind zur Transparenz verpflichtet!“ vom 30. Juni 2015, siehe D 5 sowie Anlage 3.2.2

Die Verwendungsabsichten des antragstellenden Vereins zog eine andere Kammer in Betracht. Da dieser beabsichtige, auf Basis der beantragten Daten einen Vergleich verschiedener Kammern anzustellen, sei es erforderlich, zwischen Daten aus pflichtigen und freiwilligen Mitgliedschaften zu unterscheiden. Diese Angaben lägen aber nur zusammengefasst vor und müssten erst noch getrennt werden, teilte die Kammer in einem Zwischenbescheid mit. Dadurch werde der Gebührenrahmen der Akteneinsichts- und Informationszugangsgebührenordnung in Höhe von 1000 Euro vollständig ausgeschöpft. Der Antragsteller könne vor diesem Hintergrund sein Begehren selbstverständlich zurückziehen. Nicht unerwähnt soll auch die Ablehnungsbegründung einer weiteren Kammer bleiben, die in einem Zwischenbescheid mitteilte, dass ein per einfacher E-Mail gestellter Antrag nicht rechtswirksam unterzeichnet sei und zudem die Assistentin der Geschäftsführung des Antrag stellenden Vereins zur Antragstellung gar nicht aktiv legitimiert sei. In einem anderen Fall erging sich eine Kammer in einer ausführlichen Argumentation gegenüber der Landesbeauftragten, weshalb sie dem Informationsbegehren nicht nachkommen könne. Unserer Aufforderung, einen der Rechtslage entsprechenden Bescheid zu erstellen und die Landesbeauftragte über dessen Inhalt in Kenntnis zu setzen, kam sie jedoch auch ein halbes Jahr nach Antragstellung nicht nach. Die Stellungnahme einer Kammer steht indes noch aus.

Die Begründungen der einzelnen Kammern zeugen zwar von einer erstaunlich vielfältigen Interpretation des Informationszugangsrechts, vermochten die Landesbeauftragte aber dennoch nicht zu überzeugen. Eine Verschwiegenheitspflicht, die der Informationspflicht des Gesetzes entgegensteht, ergibt sich hier weder aus Spezialnormen noch aus allgemeinen Erwägungen. Wie der Antragsteller die erfragten Daten verwenden will, darf nach den Grundsätzen des AIG grundsätzlich gar nicht berücksichtigt werden. Außerdem unterscheidet das Gesetz in den Regelungen zu seiner Anwendbarkeit nicht zwischen der Art der Mitgliedschaften. Eine darauf basierende Kostenankündigung in Höhe von 1000 Euro ist nicht nachvollziehbar und stellt eine unzulässige Abschreckung dar. Selbstverständlich kann ein Antrag auf Informationszugang auch per einfacher E-Mail gestellt werden. Das Akteneinsichts- und Informationszugangsgesetz wurde vor mehreren Jahren eigens geändert, um die Hürden der Antragstellung gerade nicht so hoch zu setzen, dass es einer qualifizierten Signatur bedarf. In Bezug auf ein Jedermannsrecht, wie das Akteneinsichts- und Informationszugangsgesetz es darstellt, auf eine fehlende Antragsbefugnis zu verweisen, erscheint ebenfalls eher von dem Bestreben getragen zu sein, formale Hürden zu schaffen. In Bezug auf die materiellen Ablehnungsgründe führte keine der Kammern einen gesetzlichen Ausnahmetatbestand des Akteneinsichts- und Informationszugangsgesetzes an. Die Nichteinhaltung der einmonatigen Regelbearbeitungsfrist stellte sich in fast allen Fällen als Problem dar.

Die Landesbeauftragte hat die oben beschriebene, auf die angebliche Nichtanwendbarkeit des Akteneinsichtsanspruchs gestützte Verweigerung einer Kammer, den Antrag auch nur zu bearbeiten, als Verstoß gegen das Akteneinsichts- und Informationszugangsgesetz schließlich beanstandet. Eine weitere, förmliche Beanstandung hat die Landesbeauftragte gegenüber jener Kammer ausgesprochen, die abschreckend hohe Gebühren veranschlagte und trotz mehrfacher Aufforderung nicht einmal ihrer Pflicht nachkam, die Landesbeauftragte bei der Erfüllung ihrer Aufgaben zu unterstützen. In den übrigen Fällen liegen noch keine abschließenden Ergebnisse vor.Die Landesbeauftragte steht mit den betroffenen Kammern im Kontakt, um eine Klärung der angesprochenen Rechtsfragen herbeizuführen bzw. eine rechtmäßige Entscheidung zu erreichen.

Der Anwendungsbereich des Akteneinsichts- und Informationszugangsgesetzes erstreckt sich auch auf Kammern, die als Körperschaften des öffentlichen Rechts des Landes verfasst sind. Ausnahmen – beispielsweise zum Schutz personenbezogener Daten – ergeben sich ausschließlich aus dem Gesetz.

5 Baumgutachten – vom Leben und Sterben der Straßenbäume

Für die Einsicht in Baumgutachten interessieren sich viele: Naturschützer, die Bäume erhalten wollen und Anwohner, die herabfallende Äste oder gar umstürzende Bäume befürchten oder beklagen. Müssen Baumgutachten ohne Weiteres zugänglich gemacht werden?

Im Rahmen der Verkehrssicherungspflicht sind Eigentümer dafür verantwortlich, Vorkehrungen zu treffen, dass von ihrem Eigentum keine Gefahr ausgeht. Geschieht dies nicht, drohen im Falle einer Schädigung Dritter Schadensersatzansprüche. Um mögliche Gefahren (z. B. Astbruch oder gar umstürzende Bäume) rechtzeitig zu erkennen, müssen die Eigentümer wissen, welche Bäume möglicherweise krank oder bereits morsch sind. Da sich insbesondere Straßenbäume, aber auch Parks und Grünanlagen auf öffentlichen Grundstücken befinden, haben die Städte und Gemeinden hier eine besondere Verantwortung. Um die Gefahren einzuschätzen, führen sie regelmäßig Baumkontrollen durch und geben bei Bedarf Baumgutachten in Auftrag. Im Ergebnis der Untersuchung wird der Zustand der Bäume bewertet und eine Prognose für die weitere Entwicklung abgegeben. Meist resultieren daraus Vorschläge zur Sanierung angegriffener Bäume oder es ergeht die Empfehlung, kranke Bäume zu fällen.

Immer wieder werden solche Gefahreneinschätzungen aber angezweifelt, und zwar sowohl von Naturschützern, die ein Interesse daran haben, Bäume zu erhalten als auch von besorgten Anwohnern, die möglicherweise bereits einen Schaden erlitten haben und die Vernachlässigung der Verkehrssicherungspflicht beklagen. Stets geht es dann darum, Einsicht in die vorliegenden Baumgutachten zu nehmen, um sich selbst ein Bild der Lage zu verschaffen.

In verschiedenen Fällen wurde die Landesbeauftragte angerufen, weil Städte oder Gemeinden sich geweigert hatten, den Zugang zu den Ergebnissen der Baumkontrollen („Baumschauen“) bzw. den Baumgutachten zu gewähren oder dies nur unvollständig taten:

Eine Stadtverwaltung, gegen die der Antragsteller auf zivilrechtlichem Wege Schadensersatzansprüche geltend machte, argumentierte, das Begehren des Klägers stelle einen unzulässigen Ausforschungsversuch dar. Diese Argumentation stützte sie zunächst ohne weitere Erläuterung auf § 8 Abs. 1 Nr. 3 Umweltinformationsgesetz. Danach ist der Antrag abzulehnen, soweit das Bekanntgeben der Informationen nachteilige Auswirkungen auf die Durchführung eines laufenden Gerichtsverfahrens hätte, es sei denn, das öffentliche Interesse an der Bekanntgabe überwiegt. In einem weiteren Schreiben an den Antragsteller stützte sich die Stadtverwaltung auf § 4 Abs. 1 Nr. 5 Akteneinsichts- und Informationszugangsgesetz (AIG). Danach ist ein Antrag abzulehnen, wenn durch die Gewährung von Akteneinsicht Inhalte von Akten offenbart würden, die eine Behörde zur Durchführung eines Gerichtsverfahrens erstellt hat oder die ihr aufgrund des Verfahrens zugehen. Beide Ausnahmetatbestände umfassen nach unserer Auffassung aber ausschließlich Unterlagen, die unmittelbar mit dem Gerichtsverfahren zusammenhängen, nicht jedoch solche, die lediglich Gegenstand der Auseinandersetzung sind. Das in Rede stehende Baumgutachten wurde nicht für das Gerichtsverfahren gefertigt, sondern weit vor dem strittigen Schadensfall und um den Zustand der Bäume zu bewerten. Eine Beeinträchtigung des zivilrechtlichen Gerichtsverfahrens ist somit in keiner Weise zu befürchten gewesen. Außerdem ist darauf hinzuweisen, dass dem Informationsfreiheitsrecht ein Ausforschungsverbot fremd ist. Die Sonderstellung, Grundrechtsbindung und Transparenzverpflichtung öffentlicher Stellen bestehen auch und gerade zum Zweck der Erleichterung der Geltendmachung von Ersatzansprüchen. Zivilprozessuale Beweisgrundsätze werden in das Informationsfreiheitsrecht auch nicht etwa im Wege einer Sperrwirkung übertragen, zumal die Gemeinde auch in ihrer Rolle als verklagte Partei vor einem Zivilgericht öffentlich-rechtlichen Grundsätzen unterliegt und für sich nicht in Anspruch nehmen kann, wie ein normaler Bürger behandelt zu werden.

Nachdem wir an die Stadtverwaltung herangetreten waren, konnten wir zumindest insoweit Einigkeit erzielen, als dass der Informationszugangsanspruch sich nach dem Umweltinformationsrecht bemisst. Bei den Ergebnis-

sen von Baumkontrollen oder bei Baumgutachten handelt es sich eindeutig um Umweltinformationen nach § 2 Abs. 3 Umweltinformationsgesetz. Nach § 1 AIG ist diese Regelung somit vorrangig anzuwenden. Auch wenn der Inhalt beider Vorschriften in diesem Fall weitgehend identisch ist, fehlen der Landesbeauftragten auf dem Gebiet des Umweltinformationsrechts die gesetzlichen Kompetenzen. Die Stadtverwaltung, die uns mitteilte, sich nur der Kommunalaufsicht gegenüber zur Rechenschaft verpflichtet zu fühlen und unsere informationszugangsrechtlichen Hinweise als Meinungsaustausch aufzufassen, konnte sich somit vollständig aus der Affäre ziehen. Nach Abschluss des laufenden Gerichtsverfahrens, teilte sie mit, werde dem Petenten selbstverständlich die gewünschte Einsicht gewährt – wohl wissend, dass die Informationen dann wertlos sein würden. Die Landesbeauftragte konnte dem Antragsteller mangels weiterer Kontrollkompetenzen nur empfehlen, den Rechtsweg zu beschreiten.

In einem anderen Fall beantragte eine Bürgerinitiative, die sich für den Erhalt von Straßenbäumen einsetzte, die Herausgabe der Kopie eines Baumgutachtens. Die Gemeinde gewährte die Einsichtnahme ausdrücklich auf der Grundlage des Akteneinsichts- und Informationszugangsgesetzes sowie des Umweltinformationsgesetzes. Allerdings verweigerte sie die Vervielfältigung des Gutachtens unter Verweis darauf, dass der Verfasser – der im Übrigen als Sachverständiger durch das zuständige Landesamt öffentlich bestellt und vereidigt war – seine Zustimmung hierzu auf Nachfrage verweigert habe. Ein Antrag auf Akteneinsicht ist abzulehnen, soweit der Einsicht Urheberrechte entgegenstehen. Diese Regelung findet sich in annähernd gleicher Formulierung sowohl im Akteneinsichts- und Informationszugangs- als auch im Umweltinformationsgesetz. Letzteres sieht eine Abwägung der Rechte des Urhebers mit dem öffentlichen Interesse vor.

Aus Sicht der Landesbeauftragten konnte die Herausgabe einer Kopie des Baumgutachtens nicht unter Verweis auf das Urheberrecht verweigert werden.[92] Sie wies die Gemeinde darauf hin und stellte ebenso wie in dem oben geschilderten Fall klar, dass vorrangig das Umweltinformationsrecht zum Tragen kommt. Die Gemeinde hielt nach nochmaliger Prüfung der Angelegenheit jedoch an ihrer entgegengesetzten Rechtsauffassung zum Urheberrechtsschutz fest. Auch hier blieb der Landesbeauftragten nichts anderes übrig, als der Bürgerinitiative mitzuteilen, dass ihr für eine weitere Unterstützung die gesetzlichen Kompetenzen fehlen.

[92] Zur Urheberrechtsproblematik in Bezug auf Gutachten siehe auch Tätigkeitsbericht 2012/2013, Punkt C 4.

Baumgutachten, die von öffentlichen Stellen in Auftrag gegeben werden und beispielsweise Straßen- oder Parkbäume betreffen, können ohne Weiteres eingesehen oder kopiert werden. In der Regel handelt es sich dabei um Umweltinformationen.

6 Durch Akteneinsicht zur besseren Examensnote?

Ein großes Medienecho erzielte der Antrag eines Schülers aus Münster (Westfalen), der sich auf ganz spezielle Weise auf die Abiturprüfung vorbereiten wollte. Er beantragte die Einsicht in die zentral gestellten Aufgaben – vor der Prüfung. War das wirklich eine gute Idee?

Der Schüler hatte mit seinem Antrag keinen Erfolg. Das zuständige Schulministerium machte eine Klausel geltend, die der Akteneinsicht entgegensteht, soweit der Erfolg einer bevorstehenden behördlichen Maßnahme erheblich beeinträchtigt würde. Ob die Antragstellung wirklich so clever war, wie einige Medien den Eindruck erweckt haben, mag also dahinstehen. Völlig überraschend war das Ergebnis schließlich nicht. Eine öffentliche Aufmerksamkeit für die Informationsfreiheit ist aus der Angelegenheit aber auf jeden Fall entstanden.

Die Landesbeauftragte hatte im Berichtszeitraum eine Frage zu beantworten, die auf den ersten Blick Ähnlichkeit mit diesem Fall aufwies. Ein Antragsteller interessierte sich unter anderem für die Aufgaben der Prüfungen am Ende der Jahrgangsstufe 10 aus zurückliegenden Schuljahren. Sein Begehren richtete er an das Landesinstitut für Schule und Medien Berlin-Brandenburg. Anders als in dem beschriebenen Fall aus Nordrhein-Westfalen ging es also nicht um bevorstehende Prüfungen, sondern um solche aus der Vergangenheit. Eine Gefährdung des Erfolgs behördlicher Maßnahmen, die auch nach dem brandenburgischen Akteneinsichts- und Informationszugangsgesetz der Einsicht entgegengehalten werden kann, erschien somit zumindest unwahrscheinlich. Zu klären war aber zunächst, ob das Landesinstitut in diesem Fall überhaupt als informationspflichtige Stelle anzusehen ist.

Die beteiligten Länder Berlin und Brandenburg haben sich per Staatsvertrag darauf geeinigt, dass für das Landesinstitut für Schule und Medien brandenburgisches Landesrecht – also auch das Akteneinsichts- und Informationszugangsgesetz – anzuwenden ist. Die Entwicklung von Unterricht und zentralen Prüfungen gehört nach diesem Staatsvertrag zu den Aufgaben des Landesinstituts. Es handelt sich somit um eine Prüfungseinrichtung im Sinne des Akteneinsichts- und Informationszugangsgesetzes. Gegenüber diesen Einrichtungen gilt das Gesetz jedoch unter anderem nur, soweit sie nicht im

Bereich von Unterricht und Prüfung tätig werden. Genau dies ist hier jedoch der Fall. Die Formulierung des Gesetzes stellt ausschließlich auf die Prüfungstätigkeit ab und verlangt keine künftige Ausrichtung derselben.

Das Akteneinsichts- und Informationszugangsgesetz war daher auf das Landesinstitut für Schule und Medien Berlin-Brandenburg im Hinblick auf die Prüfungsaufgaben zurückliegender Jahrgänge nicht anwendbar. Somit musste die Frage, ob hier überhaupt eine Gefährdung bevorstehender behördlicher Maßnahmen eintreten kann, nicht mehr geklärt werden.

Prüfungseinrichtungen sind vom Anwendungsbereich des Akteneinsichts- und Informationszugangsgesetzes auch dann ausgenommen, wenn die Herausgabe zurückliegender Prüfungsaufgaben beantragt wird.

7 Offenlegung von Verträgen nur nach Anhörung des Unternehmens?

Ein Antragsteller interessierte sich für den Vertrag über die Errichtung einer Brücke. Die Stadtverwaltung lehnte die Offenlegung der Vereinbarung mit der Begründung ab, der Vertragspartner – ein öffentlich kontrolliertes Eisenbahninfrastrukturunternehmen – habe seine Zustimmung zur Herausgabe verweigert.

Darüber hinaus war die Behörde der Auffassung, der Anwendungsbereich des Akteneinsichts- und Informationszugangsgesetzes sei gar nicht eröffnet, da es sich um einen auf zivilrechtlicher Grundlage abgeschlossenen Vertrag handelt. Der Antragsteller hat gegen den ablehnenden Bescheid Widerspruch eingelegt und die Landesbeauftragte um Unterstützung gebeten.

Das Akteneinsichts- und Informationszugangsgesetz unterscheidet nicht zwischen öffentlich-rechtlichen und zivilrechtlichen Handlungsformen. Für Informationen einer öffentlichen Stelle, die dem Anwendungsbereich des Gesetzes unterfällt – wie beispielsweise eine Stadtverwaltung – finden dessen Vorschriften also auch dann Anwendung, wenn Aufgaben in privatrechtlicher Form erfüllt werden. Die Stadtverwaltung haben wir darauf hingewiesen. Außerdem stellten wir klar, dass die fehlende Zustimmung des betroffenen Unternehmens allein eine Ablehnung des Informationszugangsantrags nicht rechtfertigt. Vielmehr hat sich die Rechtslage seit der Novellierung des Akteneinsichts- und Informationszugangsgesetzes im Oktober 2013 in dieser Hinsicht nicht unwesentlich geändert. Während das bis dahin geltende Gesetz die Herausgabe unternehmensbezogener Daten im Wesentlichen vom

Willen des Unternehmens abhängig machte, sieht die geltende Fassung ein zweistufiges Verfahren vor:

Handelt es sich bei den beantragten Angaben um Unternehmensdaten, die nicht bereits allgemein bekannt sind, ist das betroffene Unternehmen in einem ersten Schritt anzuhören. Dies soll es der aktenführenden Stelle ermöglichen, festzustellen, ob es sich um schutzwürdige Betriebs- und Geschäftsgeheimnisse handelt. Signalisiert das Unternehmen in diesem Zusammenhang, mit einer Herausgabe einverstanden zu sein, kann die Offenlegung ohne Weiteres erfolgen. Ist das Gegenteil der Fall, sollte es darlegen, aus welchen Gründen aus seiner Sicht Betriebs- und Geschäftsgeheimnisse vorliegen bzw. auf welche Aktenteile dies zutrifft. Entscheidend für die Antwort des Unternehmens ist in solchen Fällen bereits die Fragestellung. So sollte die Verwaltung in ihrer Formulierung deutlich machen, dass es nicht um eine Zustimmung geht, sondern eben um eine Anhörung, die sie ihrer letztendlich eigenen Entscheidung zugrunde legen wird.

In einem zweiten Schritt stellt die Behörde auf der Grundlage der Stellungnahme des Unternehmens fest, ob es sich bei den Angaben um Betriebs- und Geschäftsgeheimnisse handelt. Ist dies der Fall, muss sie den Antrag ablehnen – es sei denn, das betroffene Unternehmen stimmt zu. Erkennt sie den Schutzbedarf nicht, sind die Angaben offenzulegen. Eine solche positive Entscheidung ist ein Verwaltungsakt, der für den Antragsteller zwar eine Begünstigung, für das zuvor angehörte Unternehmen aber eine Belastung darstellt. Um sich gegen einen möglicherweise befürchteten Eingriff in seine Rechte zu wehren, kann es der Entscheidung widersprechen. In aller Regel hemmt dies die Offenlegung der strittigen Informationen.

Gleichzeitig ist die Vorschrift des Akteneinsichts- und Informationszugangsgesetzes zur Aussonderung der schutzbedürftigen und Offenlegung der übrigen Informationen zu beachten. Dies stellt eine sinnvolle Möglichkeit dar, zunächst den unstrittigen Teil herauszugeben, um die Auswirkung von Verzögerungen möglichst minimal zu halten. Gerade im Hinblick auf die oft umfassenden Gegenstände von Verträgen ist davon auszugehen, das im Ergebnis – wenn überhaupt – ohnehin nur ein geringer Teil als Betriebs- und Geschäftsgeheimnis einzustufen sein wird.

In dem geschilderten Fall stellte sich im Rahmen der Bearbeitung des Widerspruchs sogar heraus, dass es sich gar nicht, wie seitens der Verwaltung ursprünglich mitgeteilt, um einen privatrechtlichen, sondern um einen öffentlich-rechtlichen Vertrag handelte. Dessen Inhalte basierten weitgehend auf gesetzlich festgeschriebenen Erfordernissen, die gar kein Betriebs- und Geschäftsgeheimnis darstellen können. Auch war die Stellungnahme des angehörten Unternehmens wesentlich offener formuliert als zunächst ange-

nommen. Im Ergebnis gewährte die Stadtverwaltung die Einsicht in den vollständigen Vertrag.

Bevor Unternehmensdaten, die nicht allgemein bekannt sind, offengelegt werden dürfen, ist das betroffene Unternehmen anzuhören. Seine Stellungnahme ist Grundlage einer eigenständigen Entscheidung der Behörde, ob es sich um ein Betriebs- und Geschäftsgeheimnisse handelt. Nur wenn dies der Fall ist, darf der Informationszugang verweigert werden.

Teil D

Die Dienststelle

1 Die Dienststelle

1.1 Unabhängigkeit der Landesbeauftragten

In seiner Sitzung im Juli 2015 hat der Landtag Brandenburg das Fünfte Gesetz zur Änderung des Brandenburgischen Datenschutzgesetzes[93] beschlossen. Die Änderungen waren infolge des noch immer nicht abgeschlossenen Vertragsverletzungsverfahrens gegen die Bundesrepublik Deutschland notwendig geworden. Die Europäische Kommission hatte bereits im Jahr 2006 gerügt, dass die deutschen Datenschutzbeauftragten nicht völlig unabhängig im Sinne von Artikel 28 Abs. 1 der Richtlinie 95/46/EG (Datenschutzrichtlinie) seien und die Vertragsverletzung vor dem Europäischen Gerichtshof geltend gemacht. Brandenburg hatte zwar aufgrund des Urteils[94] das Brandenburgische Datenschutzgesetz geändert, doch waren diese Änderungen nach Auffassung der Europäischen Kommission nicht ausreichend. Neben einigen anderen Bundesländern wurde Brandenburg aufgefordert, nachzubessern. Ein wesentlicher Kritikpunkt der Kommission war die Regelung in § 22 Abs. 4 Satz 3 Brandenburgisches Datenschutzgesetz, die den Landesbeauftragten der Dienstaufsicht des Präsidenten des Landtags unterstellt hatte. Eine Dienstaufsicht ohne jede Einschränkung steht jedoch nach Auffassung der Europäischen Kommission im Widerspruch zu der vom Europäischen Gerichtshof für die Datenschutzbehörden geforderten völligen Unabhängigkeit. Die brandenburgische Regelung wurde deshalb durch die Gesetzesänderung dahingehend eingeschränkt, dass der Landesbeauftragte der Dienstaufsicht nur unterliegt, soweit diese die Unabhängigkeit des Amtes nicht berührt. Darüber hinaus wurde dem Landesbeauftragten die Ausübung der Aufgaben einer obersten Dienstbehörde für die bei ihm tätigen Beamten nach dem Landesdisziplinargesetz übertragen. Bisher oblagen dem Präsidenten des Landtages die Disziplinarbefugnisse. Durch die Neuregelungen wird der Unabhängigkeit des Landesbeauftragten nun besser Rechnung getragen.

Bedauerlicherweise wurde die Gelegenheit der Änderung des Brandenburgischen Datenschutzgesetzes nicht dazu genutzt, die Dienststelle der Landesbeauftragten als oberste Landesbehörde auszugestalten. Erst bei einer solchen Änderung wäre die völlige Unabhängigkeit gegeben. Es ist davon aus-

93 Fünftes Gesetz zur Änderung des Brandenburgischen Datenschutzgesetzes vom 27. Juli 2015, GVBl. I, Nr. 22

94 Urteil des Europäischen Gerichtshofs vom 9. März 2010, Rechtssache C-518/07

zugehen, dass nach dem Inkrafttreten der europäischen Datenschutz-Grundverordnung diese Frage erneut zur Entscheidung ansteht.

1.2 Organisation, Personal und Standort

Wie auch in den Jahren zuvor stieg die Zahl der Beratungsersuchen und Beschwerden im Berichtszeitraum weiter kontinuierlich an. Während sich kommunale Verwaltungen in noch höherem Maße als bisher mit der Bitte um Beratung an mich wandten, war auf dem Gebiet von Telekommunikation und Telemedien eine erhebliche Steigerung der Zahl der Eingaben durch die Nutzer zu verzeichnen. Für den Doppelhaushalt 2015/2016 hatte ich deshalb eine zusätzliche Stelle für den juristischen Bereich beantragt, die der Landtag Brandenburg auch bewilligte. So konnte zum 1. Juli 2015 ein Volljurist im Bereich Recht eingestellt werden.

Darüber hinaus war es in den vergangenen zwei Jahren wieder möglich, einen zusätzlichen Mitarbeiter befristet im Bereich Recht zu beschäftigen. So konnten wir die gestiegene Zahl der zu bearbeitenden Eingaben und den Beratungsbedarf besser bewältigen.

Zum Zeitpunkt der Verabschiedung des Doppelhaushalts 2015/2016 war das Ende des Gesetzgebungsverfahrens für einen europäischen Datenschutzrechtsrahmen noch nicht absehbar. Inzwischen ist klar, dass die europäische Datenschutz-Grundverordnung im Jahr 2016 in Kraft treten und im Jahr 2018 anzuwenden sein wird.[95] Für die Vorbereitung der Umsetzung sowie die Wahrnehmung der in der Grundverordnung für die Datenschutzbehörden geregelten zahlreichen neuen Aufgaben wird eine bessere Personalausstattung der Landesbeauftragten notwendig werden. Nur wenn die Datenschutzbehörden über ausreichend Personal verfügen, werden sie in der Lage sein, die Regelungen des neuen Rechtsrahmens angemessen umzusetzen. Dazu gehören auch eine enge Zusammenarbeit mit allen Datenschutzbehörden in der Europäischen Union und eine neue Form der Justiziabilität der datenschutzrechtlichen Entscheidungen der Landesbeauftragten. Die Umsetzung des europäischen Datenschutzrechtsrahmens stellt für alle Beteiligten eine große Herausforderung dar.

In das jahrelange Bemühen um die Verlagerung des Sitzes meiner Dienststelle in die Landeshauptstadt Potsdam ist Bewegung gekommen. Das insoweit zuständige Ministerium der Finanzen hat ein geeignetes Objekt am Standort Heinrich-Mann-Allee in Aussicht gestellt, dessen Nutzung jedoch erst nach Ende des nächsten Berichtszeitraums möglich sein soll. Ich bin guten Mutes, dass wir dann nach mehr als 25 Jahren in Kleinmachnow doch

[95] siehe A 1

noch in die Landeshauptstadt umziehen können und für Bürger endlich besser erreichbar sein werden.

1.3 Anbindung der Dienststelle an die E-Mail-Infrastruktur des Landes

Der Brandenburgische IT-Dienstleister (ZIT-BB) kündigte im Berichtszeitraum die mit unserer Dienststelle bestehende Servicevereinbarung über die Nutzung von Kommunikationsdiensten im Kommunikationsverbund des Landes. In dieser Servicevereinbarung wurde u. a. auch die Anbindung unseres GroupWise-E-Mail-Servers an den zentralen GroupWise-Server des ZIT-BB vertraglich geregelt. Hintergrund der Kündigung war die Entscheidung des RIO-Ausschusses über die IT-Standards des Landes, zukünftig in der Landesverwaltung nur noch Microsoft Exchange als sog. Groupware-Lösung einzusetzen. Der ZIT-BB unterbreitete uns das Angebot, zukünftig unsere E-Mail-Postfächer zentral beim ZIT-BB verwalten zu lassen und auf das Groupware-Produkt Microsoft Exchange umzusteigen. Dieses Angebot nahmen wir jedoch nicht an, weil damit u. a. auch die interne Kommunikation der Dienststelle über das Landesverwaltungsnetz zum ZIT-BB übertragen worden wäre. Auch die gem. § 7 Abs. 1 Brandenburgisches Datenschutzgesetz geforderte Trennung der Daten nach jeweils verfolgten Zwecken und nach unterschiedlichen Betroffenengruppen (hier die Behörden) wurde auf dem zentralen Kommunikationsserver beim Dienstleister nur ungenügend berücksichtigt. Dies hatten wir im Rahmen einer Prüfung festgestellt und den ZIT-BB aufgefordert, eine datenschutzgerechte Trennung der Daten zu realisieren.[96]

Letztendlich entschieden wir uns, den eigenen GroupWise-Server der Dienststelle weiter zu betreiben. Es wurde zusätzlich ein Internet-Gateway installiert und an die zentrale Kommunikationsinfrastruktur des ZIT-BB angebunden. Die Synchronisation unseres zentralen Adressbuchs mit dem Metaverzeichnis des ZIT-BB erfolgt über LDAP. Bei der Neustrukturierung unseres Kommunikationssystems hat uns der ZIT-BB tatkräftig unterstützt.

1.4 Neuer PGP-Schlüssel der Dienststelle

Die Übertragung von personenbezogenen Daten in Weitverkehrsnetzen (z. B. Internet) ist mit erheblichen Risiken verbunden. Mithilfe von kryptographischen Verfahren kann die Vertraulichkeit, Integrität und Authentizität der übertragenen Daten sichergestellt werden. Die Verfahren müssen sich nach dem jeweiligen Stand der Technik richten. Schon seit vielen Jahren können Bürger verschlüsselt per E-Mail mit unserer Dienststelle kommunizieren.

96 Tätigkeitsbericht 2012/2013, B 7.4

Wir setzen derzeit das Verschlüsselungspaket GNU Privacy Guard for Windows[97] (GPG4Win) in der Version 2.2.6 ein. Die Erstellung von GPG4Win wurde vom Bundesamt für Sicherheit in der Informationstechnik (BSI) beauftragt. GPG4Win unterstützt die aktuellen Verschlüsselungsverfahren und Schlüssellängen und ist Freie Software. Da der Quellcode des Programmsystems öffentlich verfügbar ist, verwenden wir nur selbst übersetzte Versionen von GPG4Win. Die Quelltexte werden stichprobenartig auf Sicherheitslücken hin untersucht.

Beim Einsatz kryptographischer Verfahren sind die Schlüssellängen und Algorithmen in regelmäßigen Abständen zu überprüfen und ggf. anzupassen. Das Bundesamt für Sicherheit in der Informationstechnik beschreibt in der Technischen Richtlinie „Kryptographische Verfahren: Empfehlungen und Schlüssellängen“[98] (BSI TR-02102) die entsprechenden Anforderungen. Da auch unser Verschlüsselungsschlüssel nicht mehr den Vorgaben des Bundesamtes entsprach, haben wir im Juli 2015 einen neuen Schlüssel generiert. Der Schlüssel steht in unserem Internetangebot[99] zum Abruf bereit.

2 Zusammenarbeit mit dem Landtag

Die enge und vertrauensvolle Zusammenarbeit mit dem Landtag setzte sich auch in diesem Berichtszeitraum fort.

Die Ausschüsse des Landtags baten mich in den vergangenen zwei Jahren regelmäßig um Berichte zu datenschutzrechtlichen Themen. Ich wurde zu zahlreichen Anhörungen eingeladen, um Stellungnahmen zu Gesetzentwürfen abzugeben. Im Ausschuss für Inneres und Kommunales habe ich mich zu mehreren Änderungen des Brandenburgischen Polizeigesetzes geäußert. Im Europaausschuss berichtete ich mehrmals über die beiden europäischen Gesetzgebungsverfahren zur Datenschutz-Grundverordnung und zur Datenschutzrichtlinie für Justiz und Inneres. Dem Finanz- und Haushaltsausschuss erläuterte ich eine Prüfung, die meine Dienststelle im Bereich der Finanzverwaltung durchgeführt hatte. Er befasste sich ausführlich damit. Im Ausschuss für Ländliche Entwicklung, Umwelt und Landwirtschaft habe ich anlässlich einer Gesetzesänderung des Umweltinformationsgesetzes das Thema der Rechtszersplitterung im Bereich des Informationsfreiheitsrechts zwischen dem Akteneinsichts- und Informationszugangsgesetz und dem Umweltinformationsgesetz angesprochen. Ich habe mich noch einmal eindringlich dafür eingesetzt, den Informationszugang in einem einheitlichen Gesetz zu regeln.

97 http://www.gpg4win.org

98 https://www.bsi.bund.de

99 http://www.lda.brandenburg.de

Eine Befassung des Landtages mit meinem Tätigkeitsbericht 2013/2014 entfiel leider. Durch die Landtagswahl im September 2014 hätte die Drucksache meines Tätigkeitsberichts in der neuen Legislaturperiode neu eingebracht werden müssen. Dies ist nicht erfolgt, sodass eine Beratung der Themen weder im Ausschuss für Inneres und Kommunales noch im Plenum stattfand.

Der im Mai 2015 vom Parlament verabschiedete Doppelhaushalt für die Jahre 2015 und 2016 hat einer Beschlussvorlage des zuständigen Ausschusses Rechnung getragen und für meine Dienststelle eine zusätzliche Stelle für den juristischen Bereich bewilligt.

3 Zusammenarbeit mit behördlichen Datenschutzbeauftragten

Auch in den Jahren 2014 und 2015 haben wir die behördlichen Datenschutzbeauftragten der Landkreise, kreisfreien Städte und größeren kreisangehörigen Gemeinden zu einer jeweils ganztägigen Beratung in unsere Dienststelle eingeladen. Die Treffen dienen dem Austausch der Beteiligten zu den Aufgabenfeldern der behördlichen Datenschutzbeauftragten sowie zur Umsetzung ihrer Empfehlungen in den jeweiligen Behörden. In der Regel werden dabei Themen aus der täglichen Praxis der behördlichen Datenschutzbeauftragten und von grundsätzlichem Interesse angesprochen. Durch eine rechtzeitige Erörterung von aktuellen Problemen können bei der Planung und dem Betrieb von Verfahren zur Verarbeitung von personenbezogenen Daten eventuell notwendige Maßnahmen oder Korrekturen schon vor der Einführung ergriffen werden. Thematische Schwerpunkte der letzten beiden Jahre waren u. a. die datenschutzgerechte Einrichtung von Pflegestützpunkten, die Auswirkungen des IT-Sicherheitsgesetzes auf die Kommunalverwaltung, der Umgang mit Katasterdaten, die Nutzung von E-Mail, De-Mail, ePost sowie das Anbieten von WLAN-Zugängen zum Internet in kommunalen Gebäuden und auf öffentlichen Plätzen.

Im Berichtszeitraum fand auch die zweite Beratung der behördlichen Datenschutzbeauftragten der optierenden Landkreise im Bereich der Grundsicherung für Arbeitsuchende statt. Im Mittelpunkt der Beratung standen aktuelle datenschutzrechtliche Themen und Schwerpunkte in den Jobcentern.

In den Beratungen und im Rahmen der Zusammenarbeit mit den behördlichen Datenschutzbeauftragten wird immer wieder die Bedeutung der Bereitstellung eines angemessenen Zeitanteils, der den behördlichen Datenschutzbeauftragten zur Bewältigung ihrer Aufgaben zur Verfügung steht, deutlich. Behördliche Datenschutzbeauftragte müssen von der Behördenleitung und allen Mitarbeitern unterstützt werden. Wie die Verwaltungsvorschrift zur

Durchführung des Brandenburgischen Datenschutzgesetzes ausführt, betrifft dies sowohl die materielle Ausstattung als auch den für diese Tätigkeit zur Verfügung stehenden Zeitanteil. Es muss gewährleistet sein, dass behördliche Datenschutzbeauftragte ihren Verpflichtungen im ausreichenden Umfang nachkommen können. Der entsprechende Zeitanteil ist auch regelmäßig Bestandteil unserer datenschutzrechtlichen Prüfungen.

4 Zusammenarbeit mit anderen Datenschutzbehörden

4.1 Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder

Zweimal im Jahr treffen sich die unabhängigen Datenschutzbehörden des Bundes und der Länder im Rahmen ihrer Konferenz, um aktuelle Fragen zu diskutieren und gemeinsame Positionen, z. B. in Form von Entschließungen und Orientierungshilfen, zu verabschieden. Der Vorsitz der Konferenz wechselt jährlich.

Im Jahr 2014 oblag der Vorsitz dem Hamburgischen Beauftragten für Datenschutz und Informationsfreiheit, Prof. Dr. Johannes Caspar. Auf ihrer Frühjahrskonferenz im März befassten sich die unabhängigen Datenschutzbehörden erneut mit der Reform des Datenschutzrechts durch die europäische Datenschutz-Grundverordnung. Sie verabschiedeten eine Entschließung zur Struktur der künftigen Datenschutzaufsicht in Europa, die sich mit der aktuellen Diskussion der Zusammenarbeit der Datenschutzbehörden in Europa befasste. Weitere Entschließungen wurden zur Öffentlichkeitsfahndung in sozialen Netzwerken gefasst, für die die Konferenz strenge Regeln eingefordert hat, zur Gewährleistung der Menschenrechte in der elektronischen Kommunikation als Folge der Snowden-Enthüllungen und der sich darin gezeigten Schwachstellen in der elektronischen Kommunikation, zur biometrischen Gesichtserkennung durch Internetdienste und zur Erforderlichkeit eines Beschäftigtendatenschutzgesetzes. Zwischen ihren Konferenzen verabschiedete die Datenschutzkonferenz im April eine Entschließung zum Ende der Vorratsdatenspeicherung. Anlass hierfür war das Urteil des Europäischen Gerichtshofs, der die Richtlinie zur Vorratsdatenspeicherung von Telekommunikations-Verkehrsdaten für ungültig erklärt hatte.

Auf ihrer zweiten Tagung im Oktober 2014 in Hamburg verabschiedete die Konferenz weitere fünf Entschließungen. Anlässlich der Diskussionen über die Befugnisse der Nachrichtendienste nach den Snowden-Enthüllungen forderte die Konferenz erneut eine effektive Kontrolle der Nachrichtendienste. Die sog. Google-Entscheidung des Europäischen Gerichtshofs war Anlass für eine Entschließung zum Recht auf Sperrung von Suchergebnissen bei Anbie-

tern von Suchmaschinen. Aus Anlass eines Entwurfs zur Änderung des Bundesdatenschutzgesetzes zwecks Herstellung der völligen Unabhängigkeit des Bundesbeauftragten verabschiedete die Konferenz die Entschließung „Unabhängige und effektive Datenschutzkontrolle für Grundrechtsschutz unabdingbar“. Die letzte Entschließung widmete sich dem Thema Marktmacht und informationelle Selbstbestimmung.

Im zweiten Berichtsjahr tagte die Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder unter dem Vorsitz des Hessischen Datenschutzbeauftragten, Prof. Dr. Michael Ronellenfitsch. Auf ihrer Frühjahrskonferenz in Wiesbaden verabschiedete sie acht Entschließungen. Die Entschließung „Datenschutz nach ‚Charlie Hebdo‘: Rechtsstaat und Grundrechte beweisen sich gerade in Zeiten terroristischer Bedrohung!“ stand im Zeichen der brutalen Terroranschläge, die Paris kurz zuvor erlebt hatte. Gerade in Zeiten des Terrors werden schnell Diskussionen über mögliche Freiheitseinschränkungen – insbesondere auf Kosten des Datenschutzes – geführt. Da der Rat der Europäischen Union im Frühjahr 2015 seine Beratungen über den Entwurf einer Datenschutz-Grundverordnung noch immer nicht beendet hatte, war die Reform des Datenschutzrechts erneut Grund für die Verabschiedung einer Entschließung zu diesem Thema. Die aus dem Rat bekanntgewordenen Positionen zur Einwilligung, Zweckbindung der Daten und zur Datensparsamkeit hatten eine Verschlechterung des Datenschutzes befürchten lassen. Die Konferenz positionierte sich mit ihrer Entschließung „Datenschutzgrundverordnung darf keine Mogelpackung werden“ dagegen. Mit einer Entschließung zur Safe-Harbor-Entscheidung der Europäischen Kommission wiesen die Datenschutzbehörden ein weiteres Mal darauf hin, dass diese keinen ausreichenden Schutz für Datenübermittlungen in die USA bietet. Mittlerweile hat der Europäische Gerichtshof in seinem Urteil vom 6. Oktober 2015 (Rechtssache C-362/14) die Safe-Harbor-Entscheidung für ungültig erklärt. Weitere Entschließungen der Konferenz befassten sich mit dem IT-Sicherheitsgesetz, dem E-Health-Gesetz und dem Mindestlohngesetz, dem Thema Verschlüsselung sowie mit Big Data zur Gefahrenabwehr und Strafverfolgung.

Auch im Jahr 2015 verabschiedete die Konferenz eine Entschließung zwischen ihren beiden Treffen im Frühjahr und Herbst. Anlass hierzu war das Gesetzgebungsverfahren zur Vorratsdatenspeicherung von Telekommunikationsverkehrsdaten. Die Bundesregierung hatte einen entsprechenden Gesetzentwurf in den Bundestag eingebracht. Mit ihrer Entschließung äußerte die Datenschutzkonferenz nochmals ihre erheblichen verfassungsrechtlichen Bedenken gegen diesen Entwurf. Mittlerweile hat der Bundestag dieses Gesetz mit Zustimmung des Bundesrates verabschiedet.

Die zweite Datenschutzkonferenz des Jahres 2015 fand im Herbst in Darmstadt statt. Trotz der bereits erfolgten Verabschiedung des Gesetzes zur

Verbesserung der Zusammenarbeit im Bereich des Verfassungsschutzes wies die Konferenz der unabhängigen Datenschutzbehörden mit ihrer Entschließung „Verfassungsschutzreform bedroht die Grundrechte“ noch einmal auf besonders kritische Punkte des Gesetzes hin. Dies betraf insbesondere die Zentralisierung von Aufgaben und Daten beim Bundesamt für Verfassungsschutz und die Erweiterung des Ausmaßes des Datenaustausches mit anderen Sicherheitsbehörden. Die Konferenz forderte erneut eine maßvolle und verfassungskonforme Ausgestaltung des Rechts der Nachrichtendienste. Die zweite Entschließung hatte die cloud-unterstützten Betriebssysteme und deren Risiken zum Inhalt. Die Konferenz forderte die Nutzer solcher Dienste auf, sich bereits vor einem Kauf über die Funktionsweisen zu informieren und alle Möglichkeiten für datenschutzfreundliche Einstellungen zu nutzen. Die verantwortlichen Stellen wurden ebenfalls aufgefordert, vor einem Einsatz dieser Betriebssysteme zu prüfen, ob sie dabei ihren datenschutzrechtlichen Pflichten nachkommen können oder im Zweifel darauf zu verzichten.

Die Entschließungen der Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder sind als Anlage zu diesem Tätigkeitsbericht veröffentlicht.

4.2 Zusammenarbeit mit weiteren Stellen

Wie in den Jahren zuvor fanden auch im Berichtszeitraum wieder regelmäßig Kooperationsgespräche mit meinem Berliner Kollegen, Dr. Alexander Dix, statt. Die Zusammenarbeit der Länder Berlin und Brandenburg, die nicht zuletzt in vielen Staatsverträgen geregelt ist, schlägt sich auch im Bereich des Datenschutzes nieder. Zahlreiche Themen beschäftigen beide Bundesländer gleichermaßen, so beispielsweise das gemeinsame Krebsregister oder die Kooperation beider Länder bei der Telekommunikationsüberwachung. In diesen Bereichen ist der intensive Austausch zwischen den Datenschutzbeauftragten der beiden Länder nicht nur sinnvoll, sondern geradezu zwingend.

Auch mit dem Ministerium des Innern und für Kommunales fand erneut ein Kooperationstreffen statt. Die nunmehr beschlossene europäische Datenschutz-Grundverordnung muss sowohl vom Bund wie auch von den Ländern innerhalb einer Zweijahresfrist umgesetzt werden. Das bedeutet auch für Brandenburg, dass datenschutzrechtliche Regelungen auf ihre Vereinbarkeit mit dem neuen Rechtsrahmen überprüft werden müssen.

Auch die beiden großen Kirchen haben mich wieder zu ihren jährlichen Konferenzen eingeladen. Im Mai 2014 war ich in Berlin zu Gast bei der Tagung der Datenschutzbeauftragten aus den Gliedkirchen der Evangelischen Kirche in Deutschland und berichtete von meiner Arbeit. Gleiches tat ich im September 2014 bei der Datenschutzkonferenz der römisch-katholischen Kirche, die ebenfalls in Berlin stattfand. Gerade in den Bereichen Gesundheit und Sozia-

les, aber auch bei Fragen des technisch-organisatorischen Datenschutzes wird sehr gut sichtbar, dass wir uns mit sehr ähnlichen Problemstellungen befassen.

5 Zusammenarbeit mit Informationsfreiheitsbeauftragten

Die Konferenz der Informationsfreiheitsbeauftragten in Deutschland befasst sich mit aktuellen Fragen des Informationszugangs. Ihr gehören die Beauftragten aus dem Bund sowie aus jenen Ländern an, in denen es ein Informationsfreiheitsgesetz gibt. Im Berichtszeitraum trat die Konferenz dreimal zusammen.

Im Jahr 2014 führte der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit, Prof. Dr. Johannes Caspar, den Vorsitz. Angesichts der Tatsache, dass sich auskunftspflichtige Stellen zur Ablehnung von Anfragen auf das Urheberrecht oder andere Rechte des „geistigen Eigentums“ berufen, forderte die Konferenz, das Urheberrecht nicht dafür einzusetzen, staatliche Informationen zurückzuhalten. In einer weiteren Entschließung stellte sie fest, dass die Anwendung der Informationsfreiheitsgesetze nicht von der Rechtsform abhängen darf, in der öffentliche Aufgaben erledigt werden. Eine Flucht vor der Informationsfreiheit in das Privatrecht ist mit einem modernen Staatsverständnis nicht zu vereinbaren. Außerdem forderten die Beauftragten, vorhandene Regierungsprogramme zu Open Data zügig in die Tat umzusetzen und weitere E- und Open-Government-Strategien zu entwickeln, damit Open Data in Deutschland zum Standard werden kann. Die Veröffentlichung amtlicher Informationen ist in ausschließlich von den öffentlichen Stellen selbst gesteuerten Veröffentlichungsmedien vorzunehmen. Dadurch sollen die voraussetzungslosen, für alle Menschen bestehenden Zugangsmöglichkeiten gewährleistet bleiben. Bestehende Open-Data-Ansätze unterstützte die Konferenz, betonte aber in diesem Zusammenhang das Erfordernis weitgehender gesetzlicher Veröffentlichungspflichten. Mit Blick auf eine umfassende und effektive Kontrolle der Umsetzung von Informationsfreiheitsrechten wiesen die Beauftragten auf ihre zumeist eingeschränkte Kontroll- und Beratungskompetenz hin und empfahlen, wo dies noch nicht geschehen ist, ihre Kompetenzen auf das Umwelt- und das Verbraucherinformationsrecht zu erweitern. Gleichzeitig mahnten sie, für eine ausreichende Ausstattung der Dienststellen Sorge zu tragen. Für den Umgang mit technischen Ermittlungsmethoden forderte die Konferenz mehr Transparenz ein, um das Vertrauen in den Rechtsstaat zu stärken.

Den Konferenzvorsitz der Informationsfreiheitsbeauftragten in Deutschland übernahm im Folgejahr der Landesbeauftragte für Datenschutz und Informationsfreiheit Mecklenburg-Vorpommern, Reinhard Dankert. Im Zusammen-

hang mit dem geplanten Freihandelsabkommen (Transatlantic Trade and Investment Partnership, TTIP) zwischen der EU und den Vereinigten Staaten von Amerika forderten die Beauftragten, der Öffentlichkeit neben zusammenfassenden und erläuternden Informationen vermehrt Originaldokumente zur Verfügung zu stellen, um es den Bürgern zu ermöglichen, sich eine eigene Meinung von den Inhalten und dem Ablauf der Verhandlungen zu bilden. Außerdem verlangten sie, dass für Streitigkeiten zwischen den Handelspartnern öffentlich tagende hoheitliche Gerichte geschaffen werden. Nur dadurch kann die notwendige Transparenz gewährleistet werden. In ihrer Entschließung „Auch Kammern sind zur Transparenz verpflichtet!“ befassten sich die Informationsfreiheitsbeauftragten mit der in der Praxis häufigen Weigerung berufsständischer Kammern, den Transparenzanforderungen der jeweiligen Informationszugangsgesetze nachzukommen. Die Konferenz wies darauf hin, dass Informationen, die im Rahmen der Tätigkeit dieser Körperschaften öffentlichen Rechts anfallen, den Informationszugangsgesetzen von Bund und Ländern unterfallen. Mit ihrer Entschließung „Informationsfreiheit 2.0 – endlich gleiches Recht in Bund und Ländern!“ forderte die Konferenz die Gesetzgeber in Bund und Ländern auf, die Einheitlichkeit der Lebensbedingungen auch im Bereich der Verwaltungstransparenz herzustellen. Dies betrifft jene Länder, die noch kein Informationsfreiheitsrecht kennen, aber auch solche, in denen – wie beispielsweise in Brandenburg – Novellierungen durchaus auch zu Rückschritten geführt haben. Moderne Regelungen über den Informationszugang gründen, so die Empfehlung der Beauftragten, auf vier wesentlichen Pfeilern: Der herkömmliche Zugang wird durch eine Verpflichtung zur aktiven Veröffentlichung ergänzt, Ausnahmen vom Informationszugangsanspruch werden auf ein unbedingt erforderliches Maß beschränkt, die Informationsfreiheits- bzw. Transparenzgesetze sind auch auf Unternehmen der öffentlichen Hand anwendbar und schließen das Umweltinformationsrecht mit ein.

In einer ausführlichen gemeinsamen Stellungnahme zum Entwurf eines Gesetzes zur Einführung der Informationsfreiheit in Baden-Württemberg begrüßten die Informationsfreiheitsbeauftragten zwar ausdrücklich das Vorhaben der Landesregierung, nunmehr endlich auch ein Landesinformationsfreiheitsgesetz zu schaffen. Gleichzeitig kritisierten sie, dass sich der Gesetzentwurf noch zu stark an den Regelungen des Informationsfreiheitsgesetzes des Bundes anlehnt, obwohl dessen Evaluierung bereits festgestellt hat, dass das Bundesrecht in vielen Punkten optimierungsbedürftig ist. Auch die Chance zur Weiterentwicklung des Informationsfreiheitsrechts zu einem modernen Transparenzgesetz und die Zusammenlegung des allgemeinen Informationsfreiheits- mit dem Umweltinformationsgesetz hat die baden-württembergische Landesregierung verstreichen lassen.

Die Entschließungen der Konferenz der Informationsfreiheitsbeauftragten in Deutschland sind als Anlage zu diesem Tätigkeitsbericht veröffentlicht.

6 Öffentlichkeitsarbeit

6.1 Veranstaltungen der Landesbeauftragten

Auf Initiative des Europarats wird in jedem Jahr am 28. Januar der Europäische Datenschutztag begangen. Anlass für diesen Jahrestag ist die Unterzeichnung der Europäischen Datenschutzkonvention durch die damaligen Mitgliedstaaten des Europarats am 28. Januar 1981. Die unabhängigen Datenschutzbeauftragten des Bundes und der Länder richten zu diesem Datum stets eine zentrale Veranstaltung aus.

Der achte Europäische Datenschutztag fand am 28. Januar 2014 im Abgeordnetenhaus von Berlin statt und befasste sich mit der Frage der rechtlichen Grenzen der Tätigkeit von Nachrichtendiensten vor dem Hintergrund der Ausspähaffären internationaler Geheimdienste. Im Jahr 2015 stand während des neunten Europäischen Datenschutztages, der ebenfalls in den Räumen des Berliner Landesparlaments ausgerichtet wurde, der Umgang mit dem unterschiedlichen Datenschutzniveau zwischen der Europäischen Union und den Vereinigten Staaten von Amerika auf der Tagesordnung. Beide Themen sollten sowohl die Arbeit der Datenschutzbeauftragten als auch die öffentliche Diskussion während des weiteren Verlaufs des Berichtszeitraums noch beschäftigen.

Die Landesbeauftragte und ihre Mitarbeiter standen am 5. und 6. Juli 2014 an ihrem Informationsstand auf dem Brandenburg-Tag in Spremberg/Grodk Rede und Antwort. Die Gespräche waren unter anderem geprägt durch die 2014 bereits seit einem Jahr andauernden Diskussionen zu den Snowden-Enthüllungen sowie weiteren Spionage- und Abhöraffären. Aber auch Maßnahmen zum Schutz vor unbefugtem Zugriff auf Daten im Internet oder der Datenschutz bei Hartz IV, insbesondere im Umgang mit der Verpflichtung von Leistungsempfängern, Kontoauszüge vorzulegen, waren Gegenstand zahlreicher Fragen. Die Landesbeauftragte bot an, die Sicherheit von Passwörtern überprüfen zu lassen und beriet im Hinblick auf die Generierung eines sicheren Passwortes. Außerdem zeigte sie anhand einer Präsentation die Möglichkeiten der Nachverfolgbarkeit durch RFID und klärte über dessen Risiken auf. In einem Preisrätsel drehte sich alles um den Datenschutz in sozialen Netzwerken.

Am 26. September 2015 luden der Landtag und die Landesregierung anlässlich des 25. Jahrestags der Neugründung des Landes Brandenburg zu einem großen Bürgerfest nach Potsdam ein, an dem auch wir uns mit einem Informationsstand beteiligten. Wir berieten die Gäste wiederum über Möglichkeiten zum Schutz ihrer Daten im Internet. Unser Preisrätsel hatte zum Zweck, die Verbraucher für Fragen der Sicherheit bei der Verwendung von Apps auf dem Smartphone zu sensibilisieren.

Bereits zum neunten Mal hat die Landesbeauftragte am 8. Juni 2015 ein Internationales Symposium zur Informationsfreiheit durchgeführt. Diese Veranstaltung findet stets in ungeraden Jahren statt; im Jahr 2015 trug sie den fragenden Titel „Informationsfreiheit und die Wirtschaft – zwei Welten?“ Die Wirtschaft spielt in der Informationsfreiheit auf den ersten Blick vor allem dann eine Rolle, wenn es um die Geheimhaltung von Betriebs- und Geschäftsgeheimnissen geht. Tatsächlich sind die Schnittstellen aber vielfältiger: Wird der Staat selbst wirtschaftlich aktiv, sieht er sich gestiegenen Transparenzanforderungen gegenüber. Gleiches gilt für den Einfluss wirtschaftlicher Interessen auf die Entscheidungsfindung in Politik und Verwaltung. Informationsfreiheit wird zudem als wichtiges Instrument zur Verhinderung von Korruption angesehen. Private Unternehmen öffnen sich zunehmend – teils freiwillig, teils verpflichten Gesetze sie hierzu. Es stellt sich die Frage, ob die Wirtschaft nicht auch selbst davon profitiert, wenn sie das Prinzip der Informationsfreiheit gegen sich gelten lässt. Auf dem Internationalen Symposium boten Experten aus Europa und Deutschland Einblicke in ihre Erfahrungen. Die Konferenz war bis auf den letzten Platz ausgebucht; neben internationalen und nationalen Gästen nahmen zahlreiche Vertreter aus der brandenburgischen Kommunal- und Landesverwaltung, aber auch aus Gerichten und dem Parlament an der Tagung teil. Sie wurde von der Deutschen Gesellschaft für Recht und Informatik e. V. mitveranstaltet.

6.2 Neue Publikationen der Landesbeauftragten

Im Berichtszeitraum traten zahlreiche gesetzliche Änderungen in Kraft, die es erforderlich machten, auch einige Publikationen der Landesbeauftragten zu überarbeiten. In einer neuen Auflage hat sie die Broschüren mit den Texten zum Umweltinformationsrecht sowie zum Informationsfreiheitsgesetz des Bundes herausgegeben. Die Broschüren zum Brandenburgischen Datenschutzgesetz sowie zum Akteneinsichts- und Informationszugangsgesetz wurden, um die hohe Nachfrage befriedigen zu können, in unveränderter Form nachgedruckt. Das Akteneinsichts- und Informationszugangsgesetz liegt inzwischen auch in englischsprachiger Übersetzung vor und kann aus unserem Internetangebot heruntergeladen werden.

Nach der Novellierung des Akteneinsichts- und Informationszugangsgesetzes im Jahr 2013 fanden die ersten Praxiserfahrungen Eingang in die überarbeiteten Anwendungshinweise zu diesem Gesetz. Die Landesbeauftragte gibt diese bereits in der 5. Auflage heraus und hat die Broschüre flächendeckend unter anderem allen Gemeinden, Ämtern, Städten und Landkreisen zur Verfügung gestellt.

Der Ratgeber zu Hartz IV wurde im Berichtszeitraum erneut aktualisiert. Er bietet Leistungsempfängern eine Unterstützung in Datenschutzfragen, die sich im Rahmen des Antragsverfahrens stellen. Außerdem hat die Landesbe-

auftragte eine Dokumentation ihres Internationalen Symposiums „Informationsfreiheit und die Wirtschaft – zwei Welten?“ vom 8. Juni 2015 veröffentlicht. Die Tagungsbeiträge sind als neunter Band in der Reihe „Potsdamer Materialien zu Akteneinsicht und Informationszugang“ erschienen.

Schließlich hat die Landesbeauftragte das umfangreiche und stets nachgefragte Datenscheckheft bereits im Jahr 2014 auf den neuesten Stand gebracht. Diese Broschüre enthält neben Erläuterungen zu den Datenschutzrechten in zahlreichen Lebenszusammenhängen Musterbriefe, mit denen die individuellen Auskunftsrechte gegenüber Behörden und Unternehmen ohne großen Aufwand geltend gemacht werden können. Dabei geht es unter anderem um Meldeangelegenheiten, Kraftfahrzeuge und Führerschein, Polizei und Strafverfolgung, um das Sozial- und Gesundheitswesen, das Schuldnerverzeichnis, Telekommunikation, Medien und Rundfunk, um Auskunfteien, das Finanzwesen, um Versicherung, Adresshandel und Werbung. Aufgrund aktueller Änderungen in einigen dieser Rechtsgebiete steht die nächste Überarbeitung des Datenscheckhefts bereits an.

Die Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder, deren Mitglied die brandenburgische Landesbeauftragte ist, hat im Berichtszeitraum verschiedene Orientierungshilfen herausgegeben:

Vor der Vermietung von Wohnraum erheben Vermieter bei den Mietinteressenten zum Teil sehr umfangreiche persönliche Angaben, auf deren Basis sie ihre Entscheidung über den Vertragsabschluss treffen. An der Beantwortung solcher Selbstauskünfte muss der Vermieter jedoch ein berechtigtes Interesse haben und es dürfen nur solche Daten erhoben werden, die zur Durchführung des Mietvertrags erforderlich sind. Die Aufsichtsbehörden für den Datenschutz im nicht öffentlichen Bereich haben hierzu eine Orientierungshilfe „Einholung von Selbstauskünften bei Mietinteressenten“ erstellt, die die wichtigsten Grundsätze aufzeigt.

Die Orientierungshilfe „Videoüberwachung durch nicht-öffentliche Stellen“ soll darüber informieren, unter welchen Voraussetzungen eine Videoüberwachung zulässig ist und welche gesetzlichen Vorgaben dabei einzuhalten sind. Ein Zusatz zu dieser Orientierungshilfe befasst sich mit der Videoüberwachung in Schwimmbädern – ein Thema, das viele Badegäste und -anstalten auch in Brandenburg beschäftigt. Die Orientierungshilfe „Videoüberwachung in öffentlichen Verkehrsmitteln“ soll eine datenschutzrechtliche Orientierung für den zulässigen Einsatz von Videoüberwachungseinrichtungen in öffentlichen Verkehrsmitteln geben. Frühere Empfehlungen der Aufsichtsbehörden haben diese unter Berücksichtigung zwischenzeitlicher Erfahrungen aus der Anwendungspraxis sowie der Entwicklungen auf dem Gebiet der Videoüberwachungstechnik fortgeschrieben. Zudem wurde der Anwendungsbereich der ursprünglich nur für den öffentlichen Personennahverkehr geltenden Orientie-

rungshilfe auf den länderübergreifenden schienengebundenen Regionalverkehr erweitert.

Die Orientierungshilfe Krankenhausinformationssysteme erschien im Berichtszeitraum in der zweiten Fassung. Sie konkretisiert die Anforderungen, die sich aus den Regelungen des Datenschutzrechts für den Krankenhausbetrieb und den Einsatz von Informationssystemen ergeben und beschreibt Maßnahmen zu deren technischer Umsetzung. Sie wurde unter Mitarbeit von Datenschutzbeauftragten der Evangelischen Kirche in Deutschland und der katholischen Kirche erstellt; auch Hersteller von Krankenhausinformationssystemen, Betreiber, Anwendervereinigungen und Datenschutzbeauftragte von Krankenhäusern wurden dabei einbezogen.

Die Orientierungshilfe zu den Datenschutzanforderungen an App-Entwickler und App-Anbieter richtet sich an Entwickler und Anbieter mobiler Applikationen (Apps). Sie zeigt datenschutzrechtliche und technische Anforderungen auf und macht diese anhand vieler Beispiele verständlich.

In zweiter Fassung liegt inzwischen auch die Orientierungshilfe Cloud-Computing vor, die den datenschutzgerechten Einsatz von Cloud-Computing fördern soll. Adressaten dieser Handlungsempfehlung sind Entscheidungsträger, betriebliche und behördliche Datenschutzbeauftragte sowie IT-Verantwortliche.

In den Anwendungshinweisen zur Erhebung, Verarbeitung und Nutzung von personenbezogenen Daten für werbliche Zwecke werden die Rahmenbedingungen für zulässige Werbung dargestellt. Unternehmen, Vereine oder Gewerbetreibende, aber auch Verbraucher finden darin eine Zusammenstellung der wichtigsten Rechte und Pflichten.

Die Orientierungshilfe zu den Datenschutzanforderungen an Smart-TV-Dienste richtet sich insbesondere an Gerätehersteller, Portalbetreiber, App-Anbieter, Anbieter von Empfehlungsdiensten und Anbieter von HbbTV-Angeboten. Sie gibt einen Überblick über die datenschutzrechtliche Bewertung durch die Aufsichtsbehörden.

Anlagen

1 Entschließungen der Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder – Datenschutzkontrolle öffentlicher Stellen

1.1 90. Konferenz vom 30. September bis 1. Oktober 2015 in Darmstadt

1.1.1 Verfassungsschutzreform bedroht die Grundrechte

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

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

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

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

1.1.2 Cloud-unterstützte Betriebssysteme bergen Datenschutzrisiken

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

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

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

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

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

1.2 Entschließung zwischen der 89. und 90. Konferenz

Entschließung vom 9. Juni 2015: Gegen den Gesetzentwurf zur Vorratsspeicherung von Telekommunikationsverkehrsdaten bestehen erhebliche verfassungsrechtliche Bedenken

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

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

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

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

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

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

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

1.3 89. Konferenz vom 18. bis 19. März 2015 in Wiesbaden

1.3.1 Datenschutz nach „Charlie Hebdo“: Rechtsstaat und Grundrechte beweisen sich gerade in Zeiten terroristischer Bedrohung!

Terrorismus und internationale Kriminalität erfordern effektive Abwehrmaßnahmen auch in freiheitlichen Verfassungsstaaten. Für etwaige Defizite kann der Datenschutz nicht verantwortlich gemacht werden. Eine Zielrichtung terroristischer Angriffe ist es, Furcht und Hass in der Gesellschaft zu verbreiten und demokratische Freiheitsrechte zu beseitigen. Die Verteidigung und Bewahrung der verfassungsmäßigen Freiheitsrechte sind zentrale Grundbedingungen zur Abwehr der vom Terrorismus ausgehenden Gefahren.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder bekräftigt ihren nach den Terror-Anschlägen vom 11. September 2001 formulierten Appell, dass alle neu erwogenen Maßnahmen sich daran messen lassen müssen, ob sie für eine wirkungsvolle Bekämpfung des Terrorismus wirklich zielführend und erforderlich sind und ob sie den Verfassungsgrundsatz der Verhältnismäßigkeit einhalten. Weder die Vorratsdatenspeicherung noch die pauschale Übermittlung von Flugpassagierdaten erfüllen diese Voraussetzungen. Einseitiges Streben nach einer umfassenden Sicherheit darf nicht den bisherigen gesellschaftlichen Konsens über die wertsetzende Bedeutung bürgerlicher Freiheits- und Persönlichkeitsrechte überlagern. Es darf in unserem Land zu keiner Verschiebung zugunsten staatlicher Überwachung und zu Lasten freier und unbeobachteter Aktion, Bewegung und Kommunikation der Bürgerinnen und Bürger kommen. Der Datenschutz ist nicht ein Hindernis für Abwehrmaßnahmen, sondern selbst ein identitätsstiftendes Merkmal des Verfassungsstaates oder – mit den Worten des Bundesverfassungsgerichts – „elementare Funktionsbedingung eines auf Handlungs- und Mitwirkungsfähigkeit seiner Bürger begründeten freiheitlich demokratischen Gemeinwesens“. Ließe man jeden Eingriff in die informationelle Selbstbestimmung zu, hätten die Terroristen eines ihrer Ziele erreicht.

1.3.2 Datenschutzgrundverordnung darf keine Mogelpackung werden!

Der Rat der Europäischen Innen- und Justizminister hat sich am 12. und 13. März 2015 erneut mit der Reform des Europäischen Datenschutzrechts befasst und dabei über drei weitere Kapitel der geplanten Datenschutz-Grundverordnung (DSGVO) grundsätzlich geeinigt. Hierzu gehören u. a. die zentralen Vorschriften über die Datenschutzgrundsätze und die Zulässigkeit der Verarbeitung personenbezogener Daten.

Die Datenschutzbeauftragten des Bundes und der Länder warnen eindringlich vor einer Aushöhlung des Datenschutzes in Europa durch eine Abkehr von den tragenden grundrechtlich vorgegebenen Datenschutzgrundsätzen. Die vom Rat nunmehr vorgeschlagene Fassung des Kapitels II der DSGVO hebelt zentrale Datenschutzgrundsätze aus:

- Der Rat verabschiedet sich mit seiner Einigung vom Grundsatz der Datensparsamkeit. Damit wird ein tragender Grundsatz des Rechts auf informationelle Selbstbestimmung aufgegeben, der die Datenverarbeitung auf das unbedingt notwendige Maß reduziert und einen Anreiz für datenschutzfreundliche Technologien darstellt.

- Nach den Vorstellungen des Rates sollen einerseits personenbezogene Daten ohne jede weitere Rechtsgrundlage zu anderen Zwecken als dem ursprünglichen Erhebungszweck verarbeitet werden dürfen, wenn der neue Zweck mit dem ursprünglichen Zweck noch vereinbar ist. Zweckänderungen sollen andererseits schon dann erlaubt sein, wenn der Datenverarbeiter hieran ein überwiegendes berechtigtes Interesse hat. Durch das Zusammenspiel dieser beiden Möglichkeiten und die ausdrücklich gewünschte Privilegierung der Datenverarbeitung zu Direktmarketingzwecken werden Zweckänderungen in einem derart weiten Umfang zulässig, dass das für den Datenschutz elementare Prinzip der Zweckbindung preisgegeben wird. Dies würde die Entscheidungsfreiheit und die Transparenz für den Einzelnen in problematischer Weise einschränken.

- Ferner wird in den Vorschlägen des Rates das Instrument der Einwilligung entwertet. In der Vergangenheit hat sich gezeigt, dass das bloße Unterlassen des Erhebens von Widersprüchen gegenüber der Datenverarbeitung (opt-out) eben nicht mit einer expliziten Willensbekundung (opt-in) gleichzusetzen ist. Der Vorschlag des Rates, „ausdrücklich“ zu streichen und durch den minder klaren Begriff „eindeutig“ zu ersetzen, ermöglicht es gerade den global agierenden Diensteanbietern, durch Verwendung pauschaler Datenschutzbestimmungen weitreichende Datenverarbeitungsbefugnisse ohne eine ausdrückliche Einwilligung des Nutzers für sich zu reklamieren. Mit diesem Vorschlag wird das informationelle Selbstbestimmungsrecht der Nutzer wesentlich geschwächt.

- Schließlich will der Rat die Verarbeitung personenbezogener Daten zu Forschungszwecken derart weitgehend privilegieren, dass ein angemessener Ausgleich mit dem Recht auf informationelle Selbstbestimmung der Betroffenen kaum noch möglich ist.

Mit diesen Vorschlägen fällt der Rat nicht nur hinter die Entwürfe der Europäischen Kommission und des Europäischen Parlaments zurück. Er ebnet dadurch den Weg zu einer Verschlechterung des derzeitigen Datenschutzniveaus, obwohl die Verbesserung des Datenschutzes eines der erklärten politischen Ziele der Reform ist.

Die Datenschutzbeauftragten des Bundes und der Länder appellieren daher an Bund und Länder, den Rat, das Europäische Parlament und die Europäische Kommission, sich in den im zweiten Halbjahr 2015 anstehenden Trilogverhandlungen für eine Verbesserung des Datenschutzniveaus einzusetzen und eine Aushöhlung zentraler Datenschutzgrundsätze zu verhindern.

1.3.3 Verschlüsselung ohne Einschränkungen ermöglichen

Zur Stärkung des Brief-, Post- und Fernmeldegeheimnisses und des Grundrechts auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme sowie im Interesse der ungestörten Kommunikation in Wirtschaft und Verwaltung sind neben entsprechenden gesetzlichen Regelungen und deren Umsetzung wirksame technische Vorkehrungen erforderlich, um elektronisch übermittelte und gespeicherte Daten vor Zugriffen Unberechtigter zu schützen. Schutzbedürftig sind neben der Kommunikation von Privatpersonen auch die geschäftliche Kommunikation von Wirtschaftsunternehmen, die Kommunikation von Berufsgruppen, die besonderen Verschwiegenheitspflichten unterliegen (z. B. Ärzte, Anwälte, Psychologen, Steuerberater), und die Kommunikation mit und innerhalb der öffentlichen Verwaltung.

Mit modernen kryptographischen Verfahren zur Verschlüsselung von Daten stehen datenschutzfreundliche Technologien zur Verfügung, die prinzipiell von jedermann genutzt werden können. Einer umfassenden und leicht nutzbaren Verschlüsselung stehen jedoch noch technische und organisatorische Hürden entgegen. Dies führt dazu, dass diese Schutzmaßnahmen bisher viel zu selten genutzt werden. Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder fordert daher,

- eine einfach bedienbare Verschlüsselungs-Infrastruktur und insbesondere eine sichere Ende-zu-Ende-Verschlüsselung ohne Eingriffsmöglichkeiten Dritter bereitzustellen,

- die Entwicklung sicherer, transparenter und einfach bedienbarer kryptographischer Verfahren ohne Hintertüren auf allen, insbesondere auch mobilen Plattformen zu fördern,

- die Wirtschaft bei der Wahrung der Vertraulichkeit und Integrität ihrer geschäftlichen Kommunikation zu unterstützen und

- kryptographische Technologien in E-Government-Verfahren standardmäßig zu implementieren

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder fordert einen aktiven Einsatz der Politik bei der Gestaltung des Grundrechts auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme.

Die Bundesregierung hat in ihren eigenen Zielstellungen aus der Digitalen Agenda 2014-2017 deutlich gemacht, wie wichtig eine zuverlässige und sichere Verschlüsselung ist.[1] Die Pläne der De-Mail-Anbieter für eine Ende-zu-Ende-Verschlüsselung ab April 2015 sind zwar ein erster Schritt in die richtige Richtung. Dennoch wird im Zusammenhang mit der Bekämpfung des internationalen Terrorismus in letzter Zeit erneut über eine Schwächung von Verschlüsselungstechnologien diskutiert.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder lehnt Forderungen ab, den Einsatz kryptographischer Verfahren durch staatliche Regulierungen zu unterbinden oder zumindest einzuschränken. Solche Regulierungen könnten leicht umgangen werden, wären kaum kontrollierbar, würden Grundrechte einschränken, den Schutz von Berufs- und Geschäftsgeheimnissen gefährden und Schwachstellen schaffen, die auch von Kriminellen ausgenutzt werden können. Im Ergebnis wäre dann der erhoffte Nutzen bei der Bekämpfung des internationalen Terrorismus äußerst fraglich.

1.3.4 IT-Sicherheitsgesetz nicht ohne Datenschutz!

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder sieht Informationssicherheit als eine Grundvoraussetzung an, um die Grundrechte auf informationelle Selbstbestimmung sowie auf Gewährleistung der Integrität und Vertraulichkeit informationstechnischer Systeme und das Telekommunikationsgeheimnis zu wahren.

Der von der Bundesregierung eingebrachte Gesetzentwurf für ein IT-Sicherheitsgesetz (BT-Drs. 18/4096 v. 25.02.2015) soll dazu beitragen, die Sicherheit informationstechnischer Systeme bei kritischen Infrastrukturen zu verbessern. Der Ausbau des Bundesamtes für die Sicherheit in der Informationstechnik (BSI) zu einer nationalen Zentrale für Informationssicherheit, die Festlegung von Sicherheitsstandards, die Pflicht zur Sicherheitsvorsorge in Unternehmen sowie die Melde- und Benachrichtigungspflichten bei sicherheitsrelevanten Vorfällen sollen dabei wichtige Bausteine einer nationalen Strategie für mehr Informationssicherheit sein.

---

[1] Zitat: „Wir unterstützen mehr und bessere Verschlüsselung. Wir wollen Verschlüsselungsstandort Nr. 1 in der Welt werden. Dazu soll die Verschlüsselung von privater Kommunikation in der Breite zum Standard werden."

Datenschutz und Informationssicherheit haben weitreichende Schnittmengen, nehmen in einzelnen Bereichen jedoch unterschiedliche Gewichtungen vor. Bei einer Gesamtabwägung darf es nicht zu einer Unterordnung oder gar Missachtung der grundrechtlich verankerten Bestimmungen des Datenschutzrechts kommen. Auch um das Vertrauen der Bevölkerung in die Gesetzgebung zur IT-Sicherheit zu stärken, muss ein beiden Seiten gerecht werdender Abwägungs- und Abstimmungsprozess deutlich zum Ausdruck kommen. Dies gilt sowohl bei der Festlegung von Sicherheitsstandards, als auch bei der Beurteilung von Einzelfällen.

Wenn Maßnahmen zur Erhöhung der Informationssicherheit ergriffen werden, geht damit in vielen Fällen auch eine Verarbeitung personenbezogener Daten einher. Die damit verbundenen Eingriffe in das Recht auf informationelle Selbstbestimmung sowie in das Telekommunikationsgeheimnis müssen gesetzlich auf das unabdingbar Erforderliche beschränkt werden. Es muss im Gesetz klar geregelt sein, welche personenbezogenen Daten im Rahmen der IT-Sicherheitsmaßnahmen von wem für welche Zwecke erhoben, verarbeitet und gespeichert werden dürfen. Diesen Anforderungen genügt der vorliegende Entwurf nicht. So fehlen Regelungen, die verpflichteten Unternehmen Klarheit über die Notwendigkeit und Zulässigkeit bestimmter Angriffspräventions- und -erkennungssysteme geben. Regeln zur Zweckbindung erhobener Daten sind nur für das BSI vorgesehen. Vorgaben zur Datensparsamkeit etwa durch Anonymisierung, Pseudonymisierung, frühzeitiges Löschen und Abschotten sind bei den vorgesehenen Maßnahmen zur Verbesserung der Informationssicherheit bisher nicht geplant.

Die Informationssicherheit darf nicht allein den Behörden im Direktionsbereich des Bundesministeriums des Innern überlassen bleiben, die bei einer Abwägung zwischen Informationssicherheit einerseits und klassischer Gefahrenabwehr und Strafverfolgung andererseits Interessenkonflikten ausgesetzt sein könnten. Die Beteiligung unabhängiger Datenschutzbehörden ist daher gefordert.

Neben der Zuständigkeit des BSI für die Informationssicherheit muss im Gesetzentwurf auch die Zuständigkeit der Datenschutzaufsichtsbehörden für Fragen der Geeignetheit und Angemessenheit der vom Datenschutzrecht geforderten technisch-organisatorischen Maßnahmen mit in den Blick genommen werden. Insofern sind die Datenschutzaufsichtsbehörden auch an der Festlegung von Informationssicherheitsstandards beteiligt und müssen daher in die Meldewege eingebunden und bei der Beratung der Beteiligten im Sinne des o.g. Abwägungsprozesses zwischen Informationssicherheits- und Datenschutzmaßnahmen beteiligt werden. Zudem kann mit der Pflicht zur Meldung erheblicher IT-Sicherheitsvorfälle an das BSI eine datenschutzrechtliche Meldeplicht von Datenpannen verbunden sein, woraus auch eine rechtliche Einbindung der Datenschutzaufsichtsbehörden in die Meldewege resul-

tiert. Dies setzt unabhängige und leistungsfähige Datenschutzaufsichtsbehörden und deren entsprechende Ausstattung voraus.

Die Bestrebungen nach mehr IT-Sicherheit dürfen sich nicht allein auf die Verabschiedung eines IT-Sicherheitsgesetzes beschränken. Das Grundrecht auf Gewährleistung der Integrität und Vertraulichkeit informationstechnischer Systeme enthält einen objektiven Auftrag an den Staat, für vertrauenswürdige und sichere IT-Infrastrukturen zu sorgen. Dabei kommt der Weiterentwicklung und Implementierung von Verfahren eine zentrale Funktion zu, die gleichzeitig eine starke Verschlüsselung und eine effektive Erkennung von Sicherheitsvorfällen ermöglichen.

1.3.5 Mindestlohngesetz und Datenschutz

Die Umsetzung des Mindestlohngesetzes wirft eine Reihe von datenschutzrechtlichen Problemen auf, die einer Klärung bedürfen.

Unter anderem haftet ein Unternehmen dafür, wenn ein Subunternehmer – und ggf. auch dessen Subunternehmer – den Beschäftigten nicht den Mindestlohn zahlt; außerdem kann ein hohes Bußgeld verhängt werden, wenn der Auftraggeber weiß oder fahrlässig nicht weiß, dass Auftragnehmer den Mindestlohn nicht zahlen. Da das Mindestlohngesetz nicht bestimmt, wie die Überprüfung durch den Auftraggeber konkret zu erfolgen hat, sichern sich – wie Industrie- und Handelskammern berichten – zahlreiche Unternehmen vertraglich durch umfangreiche Vorlagepflichten und Einsichtsrechte in Bezug auf personenbezogene Beschäftigtendaten beim Subunternehmer (z. B. Lohnlisten, Verdienstbescheinigungen usw.) ab. Dies ist in Anbetracht der schutzwürdigen Interessen der Beschäftigten weder datenschutzrechtlich gerechtfertigt noch im Hinblick auf die soziale Zielrichtung des Mindestlohngesetzes erforderlich.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder appelliert an den Bundesgesetzgeber, bei der in Aussicht genommenen Überprüfung des Mindestlohngesetzes stärker auf die Belange des Datenschutzes zu achten. Auch im Interesse einer unbürokratischen Lösung sollte der Gesetzgeber klarstellen, dass eine schriftliche Erklärung des Auftragnehmers ausreicht, um die Voraussetzungen des Mindestlohngesetzes einzuhalten. Dies kann eventuell durch Vertragsstrafenregelungen, Übernahme des Haftungsrisikos durch Bankbürgschaften sowie vertragliche Zustimmungsvorbehalte für den Fall der Beauftragung weiterer Subunternehmer durch den Auftragnehmer abgesichert werden. Aus Datenschutzsicht sind allenfalls stichprobenartige Kontrollen von geschwärzten Verdienstbescheinigungen hinnehmbar. Bei einer Novellierung des Gesetzes, sollte der Gesetzgeber darüber hinaus klarstellen, dass Zugriffe des Auftraggebers auf personenbezogene Beschäftigtendaten des Auftragnehmers unzulässig sind.

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

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

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

1. Der Gesetzentwurf hat zum Ziel, die elektronische Gesundheitskarte einschließlich der Telematikinfrastruktur als zentrale Kommunikationsplattform im Gesundheitsbereich zu etablieren. So soll der Einsatz freiwilliger Anwendungen, in denen Patientendaten verarbeitet werden, forciert werden. Es muss allerdings bei dem Grundsatz bleiben, dass die Betroffenen über die Speicherung von Diagnosen und anderen medizinischen Daten auf der Gesundheitskarte selbst entscheiden können. Zur Wahrung der Transparenz ist das den Betroffenen eingeräumte Zugriffsrecht auf ihre Daten von besonderer Bedeutung. Ihnen wird damit auch die Wahrnehmung ihrer Rechte, insbesondere auf Auskunft und Löschung, ermöglicht. Entgegen der Gesetzeslage und entsprechender Ankündigungen ist eine Erprobung des Patientenzugriffs bislang unterblieben. Es ist daher sicherzustellen, dass die Versicherten ihre gesetzlich zugestandenen Rechte auch wahrnehmen können. Für den Fall, dass die notwendigen Funktionalitäten nicht zeitgerecht zur Verfügung stehen, sollte der Gesetzgeber angemessene Sanktionen festlegen.

2. Nach dem Gesetzentwurf richtet die Gesellschaft für Telematik zukünftig ein öffentlich über das Internet verfügbares Interoperabilitätsverzeichnis „für technische und semantische Standards, Profile und Leitfäden für informationstechnische Systeme im Gesundheitswesen“ ein. Sie wird dabei von Experten insbesondere aus dem IT-Bereich beraten. Zur Sicherung des hohen Schutzniveaus von Gesundheitsdaten sind auch Datenschutzexperten hinzuzuziehen.

3. Der Bundesgesetzgeber muss klare Rahmenbedingungen für die Einschaltung externer Dienstleister durch Berufsgeheimnisträger schaffen und den Vertraulichkeitsschutz bei den Dienstleistern sicherstellen. Die Einschaltung von externen Dienstleistern ist für Berufsgeheimnisträger oft ohne Alternative, wenn sie – wie auch vom Gesetzgeber beispiels-

weise mit dem eHealth-Gesetz gewünscht – moderne Informationstechnik nutzen wollen. Jedoch ist damit regelmäßig die Gefahr eines Verstoßes gegen die Schweigepflicht verbunden.

Vor diesem Hintergrund muss der Gesetzgeber Rechtssicherheit schaffen, unter welchen Voraussetzungen Berufsgeheimnisträger externe Dienstleister einschalten dürfen. Die notwendige rechtliche Regelung muss (z. B. in § 203 StGB) gewährleisten, dass die Kenntnisnahme von Berufsgeheimnissen auf das unbedingt Erforderliche beschränkt wird, die Dienstleister einer Schweigepflicht unterworfen und die Patientendaten auch bei ihnen durch ein Beschlagnahmeverbot abgesichert werden. Zudem muss durch Weisungsrechte der Berufsgeheimnisträger deren Verantwortlichkeit für die Berufsgeheimnisse gewahrt bleiben. Über technische und organisatorische Maßnahmen und über das Herstellen von Transparenz ist das für sensible Daten erforderliche Schutzniveau herzustellen.

1.3.7 Big Data zur Gefahrenabwehr und Strafverfolgung: Risiken und Nebenwirkungen beachten

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

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

Besonders kritisch ist es, wenn Analysesysteme vermeintlich harmlose, allgemein zugängliche Daten aus dem Internet auswerten, etwa aus Foren oder sozialen Netzwerken. Diese können zudem mit polizeilichen Speicherungen verknüpft und einer konkreten Person zugeordnet werden. Es besteht das Risiko, dass die Systeme die Daten aus einem ganz anderen Zusammenhang verwenden, denen kein gefährdendes oder strafbares Verhalten zu Grunde liegt. Dann können Bürgerinnen und Bürger nicht mehr sicher sein,

welche ihrer Handlungen von der Polizei registriert und nach welchen Kriterien bewertet werden – zumal diese stets nur auf statistischen Erfahrungswerten beruhen, die im Einzelfall nicht zutreffen müssen. Sind die Kriterien und die Funktionsweise der Auswertealgorithmen nicht bekannt, ist es den Betroffenen unmöglich, das Ergebnis mit eigenen Angaben zu widerlegen.

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

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

1.3.8 Safe Harbor bietet keinen ausreichenden Schutz für den Datentransfer in die USA

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder weist darauf hin, dass die Safe Harbor-Entscheidung der Europäischen Kommission aus dem Jahr 2000 keinen ausreichenden Schutz für das Grundrecht auf Datenschutz bei der Übermittlung personenbezogener Daten in die USA entfaltet.

Im Jahr 2010 haben die deutschen Datenschutzaufsichtsbehörden im nichtöffentlichen Bereich bereits ausgeführt, dass die Erklärung über eine Selbst-Zertifizierung, wie sie die Safe Harbor-Grundsätze vorsehen, für Datenübermittlungen in die USA nicht ausreicht. Sie wiesen darauf hin, dass sich übermittelnde Unternehmen von den Datenempfängern nachweisen lassen müssen, dass die Safe Harbor-Grundsätze auch eingehalten werden. Mit den Enthüllungen von Edward Snowden wurde offengelegt, dass US-Sicherheitsbehörden systematisch und massenhaft auf in die USA übermittelte personenbezogene Daten zugreifen, und damit die Safe Harbor-Grundsätze mit großer Wahrscheinlichkeit gravierend verletzt werden.

Die Konferenz weist darauf hin, dass bei Übermittlungen in einen Staat, in dem europäisches Datenschutzrecht nicht direkt anwendbar ist, zumindest folgende Garantien für den Datenschutz gegeben sein müssen: Die Zweckbindung der Daten ist grundsätzlich sicherzustellen. Staatliche Zugriffsmöglichkeiten müssen auf ein angemessenes und grundrechtskonformes Maß begrenzt bleiben. Den Betroffenen ist ein effektiver Anspruch auf Auskunft und auf Berichtigung bzw. Löschung falscher bzw. unzulässig gespeicherter Daten zu gewähren. Bei Verstößen bedarf es eines effektiven Rechtsschutzes. Formelle und sprachliche Barrieren dürfen nicht dazu führen, dass die Betroffenen ihre Rechte nicht wahrnehmen können.

1.4 Entschließungen zwischen der 88. und 89. Konferenz

1.4.1 Entschließung vom 14. November 2014: Keine PKW-Maut auf Kosten des Datenschutzes!

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder (DSK) fordert die Bundesregierung auf, bei der geplanten Einführung einer allgemeinen Maut auf Bundesautobahnen und einzelnen Bundesfernstraßen auf eine automatisierte Erhebung, Verarbeitung und Nutzung von Fahrzeugkennzeichen aller Verkehrsteilnehmer über elektronische Kontrollpunkte zu verzichten. Für Abrechnungs- und Kontrollzwecke besteht hierfür kein Erfordernis, denn es stehen – beispielsweise durch Einführung einer physischen Vignette nach dem Vorbild anderer Staaten – mildere und gleichermaßen effektive Mittel zur Kontrolle der Entrichtung der Maut zur Verfügung, ohne täglich an hunderten Kontrollpunkten hunderttausende Kfz-Kennzeichen zu erfassen und zu speichern. Für die Kontrolle in Deutschland zugelassener Pkw ist die (optisch-)elektronische Überwachung schon deswegen nicht erforderlich, weil die Abrechnung über die Zulassungs- und Kfz-Steuerdaten erfolgen soll. Allein die Möglichkeit, sich die Infrastrukturabgabe für gänzlich ungenutzte Pkw erstatten zu lassen, rechtfertigt nicht die vorgesehene elektronische Erfassung und sogar dauerhafte – bis zu 13 Monaten währende – Speicherung von Bewegungsdaten in Deutschland zugelassener Pkw.

Die DSK lehnt die im Entwurf eines Infrastrukturabgabengesetzes geplante Einrichtung eines Zentralen Infrastrukturregisters beim Kraftfahrtbundesamt und einer Datei sämtlicher mautpflichtiger Autobahnnutzungen von Personenkraftwagen beim Bundesamt für Güterverkehr ab. Ebenso weist sie auf die Gefahren der Einbeziehung privater Betreiber in die Erhebung der Infrastrukturabgabe einerseits und eines privaten Dritten in die Überwachung der Infrastrukturabgabe andererseits im Hinblick auf die umfangreichen geplanten Befugnisse der Betreiber bzw. des Dritten zur Datenerhebung und –verarbeitung hin. Die DSK mahnt die Bundesregierung eindringlich zur Einhaltung der verfassungsrechtlich gebotenen Prinzipien der Datenvermeidung und Datensparsamkeit.

1.4.2 Entschließung vom 14. November 2014: Anforderungen an den Schutz der Datenübermittlungen zwischen medizinischen Leistungserbringern und klinischen Krebsregistern

Zur Verbesserung der Versorgung von Krebspatienten bauen die Bundesländer derzeit auf bundesgesetzlicher Grundlage ein flächendeckendes Netz von klinischen Krebsregistern auf. Diese Register erhalten hierzu vielfältige Daten über alle krebskranken Personen von allen niedergelassenen Ärzten und Krankenhäusern, die sie behandeln. Andererseits sollen die Register den behandelnden Ärzten die empfangenen Patientendaten zum Abruf zur Verfügung stellen. Die hierbei übermittelten Daten sind hoch sensibel und können mannigfaltig missbraucht werden. Dem müssen die Maßnahmen zu ihrem Schutz entsprechen.

Mit dieser Entschließung legt die Konferenz einen Katalog von Anforderungen vor und ruft die Bundesländer auf, für deren Erfüllung bei der Ausgestaltung der Kommunikation zwischen medizinischen Leistungserbringern und den klinischen Krebsregistern Sorge zu tragen.

Anlage zur Entschließung „Anforderungen an den Schutz der Datenübermittlungen zwischen medizinischen Leistungserbringern und klinischen Krebsregistern“

Die Anlage kann auch aus unserem Internetangebot unter http://www.lda.brandenburg.de abgerufen werden.

1.4.3 Entschließung vom 16. Dezember 2014: Schluss mit den datenschutzrechtlichen Missständen beim Umgang mit Krankengeldbeziehern!

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

Zudem werden nach den Prüferfahrungen der Datenschutzbeauftragten des Bundes und einiger Länder Versicherte beim „Krankengeldfallmanagement“ von ihrer Krankenkasse oftmals unter Druck gesetzt. Auch der Patientenbe-

auftragte der Bundesregierung sowie die Unabhängige Patientenberatung Deutschland (UPD) haben an dieser Praxis starke Kritik geübt.

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

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

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

1.4.4 Entschließung vom 5. Februar 2015: Keine Cookies ohne Einwilligung der Internetnutzer

Cookies und verschiedene andere Technologien ermöglichen die Verfolgung des Nutzerverhaltens im Internet. Sie werden immer häufiger zur Bildung von anbieter-übergreifenden Nutzungsprofilen verwendet, um Nutzern dann z. B auf sie zugeschnittene Werbung anzuzeigen. Die Datenschutzrichtlinie für elektronische Kommunikation (E-Privacy-Richtlinie, Art. 5 Abs. 3, RL 2002/58/EG) gestattet die Speicherung von Informationen oder den Zugriff auf Informationen, die bereits im Endgerät eines Nutzers gespeichert sind, jedoch nur, wenn der Nutzer dazu seine Einwilligung gegeben hat. Außerdem müssen die Diensteanbieter die Nutzer vor der Speicherung von Informationen mittels Cookies, Web Storage oder ähnlichen Instrumenten klar und umfassend über deren Zweck informieren. Dies gilt auch für den Zugriff auf Browser- oder Geräteinformationen zur Erstellung von sog. Device Fingerprints. Der europäische Gesetzgeber misst dem Einsatz dieser Technologien zu Recht ein hohes Gefährdungspotential für die Persönlichkeitsrechte der Nutzer bei.

Das Telemediengesetz (TMG) setzt diese europarechtlichen Vorgaben allerdings nur unvollständig in deutsches Recht um. Darauf haben die Datenschutzbeauftragten von Bund und Ländern die Bundesregierung bereits wiederholt hingewiesen. Dies hat bisher jedoch nicht zu einer Änderung des TMG geführt. Die Bundesregierung hält vielmehr die derzeit geltenden Vorgaben des Telemediengesetzes für ausreichend. Diese Auffassung ist unzutreffend. So ist die europarechtlich geforderte Einwilligung bereits in den Zugriff auf in den Endgeräten der Nutzer gespeicherte Informationen (Cookies) im deutschen Recht nicht enthalten.

Die fortgesetzte Untätigkeit der Bundesregierung und des Gesetzgebers hat zur Folge, dass gegenwärtig die Betroffenen ihre Ansprüche zur Wahrung der Privatsphäre aus Art. 5 Abs. 3 der E-Privacy-Richtlinie gegenüber Anbietern in Deutschland, bei denen das TMG zur Anwendung kommt, nur unzureichend wahrnehmen können. Damit wird den Bürgerinnen und Bürgern faktisch ein europarechtlich vorgesehenes, wesentliches Instrument zur Wahrung ihrer Privatsphäre bei der Nutzung des Internets vorenthalten. Die Datenschutzbeauftragten des Bundes und der Länder halten diesen Zustand für nicht hinnehmbar. Sie fordern die Bundesregierung auf, die E-Privacy-Richtlinie nun ohne weitere Verzögerungen vollständig in das nationale Recht zu überführen. Gerade die Weiterentwicklung von neuen Technologien zur Sammlung und Analyse des Nutzerverhaltens im Internet macht moderne und effiziente Regelungen zum Schutz der Privatsphäre der Nutzer unabdingbar.

1.5 88. Konferenz vom 8. bis 9. Oktober 2014 in Hamburg

1.5.1 Effektive Kontrolle von Nachrichtendiensten herstellen!

Die Enthüllungen über die Spähaktivitäten ausländischer Nachrichtendienste haben verdeutlicht, wie viele Kommunikationsdaten in der digitalisierten Welt anfallen, welche Begehrlichkeiten diese Daten offensichtlich auch bei Nachrichtendiensten demokratischer Länder wecken und mit welchen weitreichenden Methoden die Nachrichtendienste Informationen erfassen, sammeln und analysieren. Auch die deutschen Nachrichtendienste haben weitreichende Befugnisse zur Erhebung, Sammlung und Auswertung personenbezogener Daten sowie zum Austausch dieser untereinander bzw. mit Polizeibehörden. Die Befugnisse der Nachrichtendienste schließen auch die Überwachung der Telekommunikation ein. Damit einher geht im Bereich der strategischen Auslandsüberwachung des BND ein Kontrolldefizit. Auch eine Beteiligung des Bundesnachrichtendienstes durch Datenaustausch mit ausländischen Diensten steht im Raum. In den vergangenen Jahren wurden die gesetzlichen Befugnisse der Nachrichtendienste stetig erweitert. So wurden die Antiterrordatei und die Rechtsextremismusdatei als gemeinsame Dateien von Polizei und Nachrichtendiensten eingeführt sowie gemeinsame Zentren von Nach-

richtendiensten und Polizeibehörden errichtet. Die Berichte der NSU-Untersuchungsausschüsse des Deutschen Bundestages und einiger Landesparlamente haben darüber hinaus erhebliche Kontrolldefizite auch bei den Verfassungsschutzämtern offengelegt. Nach der Einschätzung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder ist daher eine Reform der rechtsstaatlichen Kontrolle der deutschen Nachrichtendienste dringend geboten.

Für die Betroffenen ist die aufgrund der Befugnisse der Nachrichtendienste und Sicherheitsbehörden vorgenommene Datenverarbeitung in weitem Maße intransparent, daher ist auch der Individualrechtsschutz faktisch eingeschränkt. Umso wichtiger ist die Kontrolle durch unabhängige Stellen. In der Entscheidung zum Antiterrordateigesetz vom 24. April 2013 hat das Bundesverfassungsgericht insoweit hervorgehoben, dass der Verhältnismäßigkeitsgrundsatz bei Datenverarbeitungen, die für die Betroffenen nur eingeschränkt transparent sind, gesteigerte Anforderungen an eine wirksame Ausgestaltung der Kontrolle sowohl auf der Ebene des Gesetzes als auch der Verwaltungspraxis stellt. Eine wichtige Rolle kommt dabei den Datenschutzbeauftragten des Bundes und der Länder zu, die neben den parlamentarischen Kontrollinstanzen die Kontrolle über die Nachrichtendienste ausüben. Bestimmte Bereiche nachrichtendienstlicher Tätigkeiten sind der Eigeninitiativkontrolle durch die Datenschutzbeauftragten des Bundes und der Länder von vornherein entzogen. Es ist sinnvoll, das bei den Datenschutzbeauftragten des Bundes und der Länder bereits vorhandene Fachwissen auch in diesem Bereich zu nutzen und die Datenschutzbehörden mit den entsprechenden Prüfbefugnissen und den hierfür erforderlichen personellen Ausstattung und Sachmitteln auszustatten.

Das Bundesverfassungsgericht hat mit der Entscheidung vom 24. April 2013 zum Zusammenwirken zwischen den Datenschutzbeauftragten und den parlamentarischen Kontrollinstanzen festgestellt: „Wenn der Gesetzgeber eine informationelle Kooperation der Sicherheitsbehörden vorsieht, muss er auch die kontrollierende Kooperation zugunsten des Datenschutzes ermöglichen.“ In diesem Sinne darf die Verteilung der Kontrolle auf mehrere Stellen nicht die Effektivität der Kontrolle einschränken. Für den Bereich der Telekommunikationsüberwachung nach dem Gesetz zur Beschränkung des Brief-, Post- und Fernmeldegeheimnisses ist die Kontrolle durch die G10-Kommission aus eigener Initiative derzeit gesetzlich nicht vorgesehen. Ebenso fehlt ein Kontrollmandat der Datenschutzbeauftragten für Beschränkungen des Fernmeldegeheimnisses. Vor dem Hintergrund der Ausführungen des Bundesverfassungsgerichtes erscheint eine Einbindung der Datenschutzbeauftragten neben den parlamentarischen Kontrollinstanzen aber erforderlich.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder fordert daher den Gesetzgeber auf, die Datenschutzbehörden mit entsprechenden Prüfbefugnissen auszustatten, damit das bei ihnen vorhandene Fachwissen auch in diesem Bereich genutzt werden kann.

1.5.2 Marktmacht und informationelle Selbstbestimmung

Die Konzentration wirtschaftlicher Macht und der Missbrauch marktbeherrschender Stellungen ist bisher Gegenstand des Wettbewerbs- und insbesondere des Kartellrechts. So untersucht gegenwärtig die Europäische Kommission mögliche Verstöße von Google gegen das Europäische Wettbewerbsrecht wegen mangelhafter Neutralität der Suchergebnisse.

Darüber hinaus ist jedoch zu lange übersehen worden, dass die zunehmenden Unternehmenskäufe vor allem im Bereich der Internetwirtschaft zu einer massiven Anhäufung von personenbezogenen Daten bis hin zur Monopolbildung in bestimmten Bereichen führen können. Datenmacht wird zur Marktmacht. Im April 2007 kaufte Google für 3,1 Mrd. US-Dollar das Werbeunternehmen Double-Click. Die Übernahme wurde sowohl von den Kartellbehörden in den USA und in Europa gebilligt, ohne dass die Auswirkungen dieser Übernahme auf den Datenschutz der Nutzer in diesen Entscheidungen berücksichtigt worden wäre. Facebook hat im vergangenen Jahr für die Übernahme von WhatsApp 18 Mrd. US-Dollar gezahlt. Auch dieser Zusammenschluss ist inzwischen sowohl in den USA als auch in der EU genehmigt worden, ohne dass es wirksame Garantien gegen eine weitere Verschlechterung des Datenschutzes gibt.

Sowohl der Europäische Datenschutzbeauftragte als auch die deutsche Monopolkommission haben inzwischen auf die möglichen Auswirkungen der Zusammenschlüsse gerade von solchen Internet-Unternehmen auf die informationelle Selbstbestimmung hingewiesen, deren Geschäftsmodelle wesentlich auf der Anhäufung von personenbezogenen Daten beruhen. Die massive Ausweitung von scheinbar kostenlosen Diensten und die wachsende Bedeutung von „Big Data“ erfordert nach Ansicht des Europäischen Datenschutzbeauftragten einen intensiveren Dialog zwischen den Datenschutz- und den Kartellbehörden, um die Wahlfreiheit wie auch die informationelle Selbstbestimmung der Nutzer angesichts abnehmender Konkurrenz aufrechtzuerhalten oder wiederherzustellen und um die Aufsichtsbefugnisse koordiniert einzusetzen. Die Monopolkommission hat in ihrem XX. Hauptgutachten (2012/2013 – Kapitel I) für eine verstärkte Kooperation von Datenschutz- und Wettbewerbsbehörden plädiert und sich für eine schnelle Verabschiedung der europäischen Datenschutzgrundverordnung eingesetzt.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder setzt sich ebenfalls für eine Datenschutzgrundverordnung auf hohem Niveau

ein. Sie ist davon überzeugt, dass insbesondere das Recht auf Datenportabilität sowohl die Souveränität des einzelnen Nutzers stärken als auch die auf der Sammlung personenbezogener Daten beruhende Machtposition einzelner Marktteilnehmer begrenzen kann.

Die Konferenz der Datenschutzbeauftragten weist darauf hin, dass eine stärkere Zusammenarbeit mit den Kartellbehörden sinnvoll ist. Ziel muss es dabei zugleich sein, den Datenschutz im Wettbewerb besser zu fördern.

1.5.3 Unabhängige und effektive Datenschutzaufsicht für Grundrechtsschutz unabdingbar

Die Bundesregierung hat am 27. August 2014 einen Gesetzentwurf zur Stärkung der Unabhängigkeit der Datenschutzaufsicht im Bund beschlossen (siehe BR Drs. 395/14). Er sieht vor, dass die bisher beim Bundesministerium des Innern eingerichtete Bundesbeauftragte für den Datenschutz und die Informationsfreiheit in eine eigenständige oberste Bundesbehörde umgewandelt wird.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder begrüßt, dass nunmehr auch der Bundesgesetzgeber die vom Europäischen Gerichtshof in mehreren Urteilen konkretisierten Voraussetzungen für eine völlig unabhängige Datenschutzaufsicht herstellen will. Es ist erfreulich, dass die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit künftig keiner Aufsicht durch eine andere Behörde mehr unterliegen wird und aufgrund ihres Status‘ als eigenständiger oberster Bundesbehörde ohne jeden Einfluss anderer Behörden selbst über ihren eigenen Haushalt und ihr eigenes Personal verfügen kann.

Die Konferenz weist jedoch auf wesentliche Punkte hin, denen auch der Gesetzesentwurf keine beziehungsweise nur unzureichend Rechnung trägt:

- Eine effektive Datenschutzaufsicht setzt die rechtliche Stärkung der Durchsetzungsbefugnisse der Bundesbeauftragten für den Datenschutz und die Informationsfreiheit zwingend voraus. Ihr müssen in ihrem Zuständigkeitsbereich gegenüber den Post- und Telekommunikationsanbietern die gleichen Anordnungs- und Untersagungsbefugnisse eingeräumt werden, wie sie den Aufsichtsbehörden der Länder gegenüber der Privatwirtschaft schon seit Jahren zustehen. Der Bundesbeauftragten ist in diesem Bereich auch die Stellung einer Obersten Bundes – und Bußgeldbehörde einzuräumen. Nur dann stehen auch ihr wirksame Eingriffsbefugnisse, wie sie die Europäische Datenschutzrichtlinie fordert, zur Verfügung.

- Eine unabhängige, funktionsfähige und effektive Datenschutzkontrolle setzt zudem voraus, dass die BfDI als künftige oberste Bundesbehörde mit ausreichenden personellen und sächlichen Mitteln ausgestattet ist, um ihren gesetzlichen Kontroll- und Beratungsaufgaben nachkommen zu können. Entsprechendes gilt für alle Datenschutzbehörden in den Ländern. Ebenso wie in vielen Ländern ist dies für die Bundesbeauftragte für den Datenschutz und Information im vorliegenden Entwurf des Bundesdatenschutzgesetzes nicht der Fall.

- Die Genehmigung, als Zeugin auszusagen, wird durch den Gesetzesentwurf in problematischer Weise eingeschränkt. Zwar wird der generelle Genehmigungsvorbehalt des BMI aufgehoben, das Gesetz sieht aber weite Ausnahmen hiervon vor, diese sind zu streichen. Zumindest muss das Letztentscheidungsrecht bei der Bundesbeauftragten für den Datenschutz und die Informationsfreiheit verbleiben.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder appelliert an den Bundesgesetzgeber, der Bundesbeauftragten sowohl effektive Sanktionsmöglichkeiten an die Hand zu geben als auch die nötigen Personalmittel für eine den Aufgaben entsprechende Personalausstattung zur Verfügung zu stellen. Die Konferenz erinnert auch die Länder daran, dass auch sie ihren Datenschutzaufsichtsbehörden ausreichend Personalmittel zur Verfügung stellen müssen, um die bereits bestehenden Kontrolldefizite zu Lasten der Bürgerinnen und Bürger und deren Grundrechtsschutz abzubauen.

1.5.4 Zum Recht auf Sperrung von Suchergebnissen bei Anbietern von Suchmaschinen

Der Europäische Gerichtshof (EuGH) hat mit seinem Urteil vom 13. Mai 2014 – C-131/12 „Google Spain“ einen fundamentalen Beitrag zum Schutz der Persönlichkeitsrechte im Internet geleistet. Die Namenssuche in Suchmaschinen kann erhebliche Auswirkungen auf die Persönlichkeitsrechte haben. Mit Suchmaschinen lassen sich weltweit in Sekundenschnelle detaillierte Profile von Personen erstellen. Oft sind Einträge über eine unbegrenzte Zeit hinweg abrufbar. Sie können dann zu sozialen und wirtschaftlichen Nachteilen für die Betroffenen führen, die ggf. ein Leben lang mit früheren oder vermeintlichen Verfehlungen konfrontiert bleiben. Das Urteil stellt nun klar, dass die Betreiber von Suchmaschinen ein Recht Betroffener auf Sperrung von Suchergebnissen bei Anbietern von Suchmaschinen umzusetzen haben. Künftig bleiben die Betroffenen daher nicht nur darauf angewiesen, ihre Ansprüche unmittelbar gegenüber den Informationsanbietern zu verfolgen, die häufig nur schwer oder auch gar nicht zu realisieren sind.

Betroffene können sich nun auch direkt an die Suchmaschinenbetreiber wenden und verlangen, dass bei der Suche einzelne Links zu ihrem Namen künftig nicht mehr angezeigt werden. Das Urteil ordnet dabei allerdings nicht an, bestimmte Inhalte, wie Presseartikel oder Artikel aus der Wikipedia, zu löschen oder ihre Auffindbarkeit im Internet unmöglich zu machen. Vielmehr soll – nach einer erfolgreichen Beschwerde des Betroffenen – der entsprechende Link lediglich bei Eingabe eines bestimmten Personennamens nicht mehr angezeigt werden. Der betroffene Inhalt bleibt mit allen anderen Suchbegriffen weiterhin frei zugänglich (für Inhalte, die regelmäßig durch Eingabe des Namens einer Person in eine Suchmaschine gefunden werden, weil es sich um eine Person des öffentlichen Lebens handelt, hat der EuGH ausdrücklich eine Ausnahme vorgesehen).

Zu Recht wird in der Debatte auf die erhebliche Macht der Anbieter von Suchmaschinen hingewiesen, über die Veröffentlichung von Suchergebnissen zu entscheiden. Diese Macht besteht jedoch nicht erst seit der Entscheidung des EuGH. Tatsächlich haben Inhalteanbieter keinen Rechtsanspruch am Nachweis ihrer Inhalte durch Suchmaschinen. Anbieter von Suchmaschinen sind keine neutralen Sachwalter der Informationsgesellschaft, sondern kommerziell handelnde Wirtschaftsunternehmen. Welche Suchergebnisse den Nutzern angezeigt wurden, bestimmt sich damit jedenfalls auch nach den kommerziellen Interessen von Suchmaschinen und ihren Vertragspartnern. Darüber hinaus unterlagen Suchmaschinen auch bereits vor der Entscheidung des EuGH bei der Gestaltung der Suchergebnisse äußeren Beschränkungen (z. B. durch das Urheberrecht). Mit dem Urteil wird klargestellt, dass Suchmaschinen neben diesen Erwägungen jetzt auch die Grundrechte der Betroffenen zu berücksichtigen haben.

Das Urteil konkretisiert die Kriterien, unter welchen sich ausländische Unternehmen an europäisches bzw. nationales Datenschutzrecht halten müssen. Dieses für den Grundrechtsschutz maßgebliche Urteil muss nunmehr von den Suchmaschinenbetreibern umfassend umgesetzt werden.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder weist in diesem Zusammenhang auf folgende Punkte hin:

- Die effektive Wahrung der Persönlichkeitsrechte des Betroffenen setzt voraus, dass Anbieter von Suchmaschinen die Suchergebnisse bei einem begründeten Widerspruch weltweit unterbinden. Angesichts der territorialen Unbeschränktheit des Internet muss der Schutz des Einzelnen vor einer unberechtigten Verbreitung personenbezogener Daten universell gelten.

- Der verantwortliche Betreiber der Suchmaschine hat regelmäßig die Rechte der Betroffenen gegen die Interessen der Öffentlichkeit an einem

freien und umfassenden Informationszugang im Einzelfall abzuwägen. Dabei ist insbesondere auf die Schwere der Persönlichkeitsrechtsbeeinträchtigung, die Stellung des Betroffenen im öffentlichen Leben sowie auf den zeitlichen Ablauf zwischen der Veröffentlichung und dem Antrag des Betroffenen beim Suchmaschinenbetreiber abzustellen.

- Die Entscheidung über die Verbreitung von Suchergebnissen, die Umsetzung von Widersprüchen und die Abwägungsentscheidung mit dem öffentlichen Interesse treffen zunächst die Suchmaschinenbetreiber. Die Kontrolle dieser Entscheidungen obliegt den jeweiligen Aufsichtsbehörden für den Datenschutz oder den staatlichen Gerichten. Alternative Streitbeilegungs- oder Streitschlichtungsverfahren dürfen das verfassungsmäßige Recht der Betroffenen auf eine unabhängige Kontrolle durch die dafür vorgesehenen staatlichen Institutionen nicht beschneiden.

- Eine Befugnis der Anbieter von Suchmaschinen, Inhaltsanbieter routinemäßig über die Sperrung von Suchergebnissen zu informieren, besteht nicht. Dies gilt auch dann, wenn die Benachrichtigung nicht ausdrücklich den Namen des Betroffenen enthält.

1.5.5 Datenschutz im Kraftfahrzeug – Automobilindustrie ist gefordert

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder weist auf die datenschutzrechtlichen Risiken hin, die mit der zunehmenden Datenverarbeitung in Kraftfahrzeugen und ihrer Vernetzung untereinander, mit ihrer Umgebung und mit dem Internet entstehen. Die Datenverarbeitung in modernen Fahrzeugen schafft Begehrlichkeiten, die dort anfallenden Daten für die verschiedensten Zwecke nutzen zu wollen – etwa bei Arbeitgebern und Versicherungen. Dabei besteht die Gefährdungslage bereits im Zeitpunkt des Erfassens von Daten in den im Auto integrierten Steuergeräten und nicht erst mit deren Auslesen oder Übermitteln. Bereits diese personenbezogenen Daten geben Auskunft über Fahrverhalten und Aufenthaltsorte und können zur Informationsgewinnung über den Fahrer bzw. den Halter bis hin zur Bildung von Persönlichkeitsprofilen herangezogen werden.

Um eine selbstbestimmte Fahrzeugnutzung frei von Furcht vor Überwachung zu gewährleisten, sind Automobilhersteller, Händler, Verkäufer, Werkstätten ebenso wie Anbieter von Kommunikations- und Telediensten rund um das Kraftfahrzeug im Rahmen ihres Wirkungskreises in der Pflicht, informationelle Selbstbestimmung im und um das Kraftfahrzeug zu gewährleisten.

Dazu gehört:

- Bereits in der Konzeptionsphase sind bei der Entwicklung neuer Fahrzeugmodelle und neuer auf Fahrzeuge zugeschnittene Angebote für Kommunikations- und Teledienste die Datenschutzgrundsätze von privacy by design bzw. privacy by default zu verwirklichen.

- Datenverarbeitungsvorgängen im und um das Fahrzeug muss das Prinzip der Datenvermeidung und Datensparsamkeit zu Grunde liegen. Daten sind in möglichst geringem Umfang zu erheben und umgehend zu löschen, nachdem sie nicht mehr benötigt werden.

- Die Datenverarbeitungen müssen entweder vertraglich vereinbart sein oder sich auf eine ausdrückliche Einwilligung stützen.

- Für Fahrer, Halter und Nutzer von Fahrzeugen muss vollständige Transparenz gewährleistet sein. Dazu gehört, dass sie umfassend und verständlich darüber zu informieren sind, welche Daten beim Betrieb des Fahrzeugs erfasst und verarbeitet sowie welche Daten über welche Schnittstellen an wen und zu welchen Zwecken übermittelt werden. Änderungen sind rechtzeitig anzuzeigen. Die Betroffenen müssen in die Lage versetzt werden, weitere Nutzer ebenfalls zu informieren.

- Auch bei einer vertraglich vereinbarten oder von einer Einwilligung getragenen Datenübermittlung an den Hersteller oder sonstige Diensteanbieter sind Fahrer, Halter und Nutzer technisch und rechtlich in die Lage zu versetzen, Datenübermittlungen zu erkennen, zu kontrollieren und ggf. zu unterbinden. Zudem muss Wahlfreiheit für datenschutzfreundliche Systemeinstellungen und die umfangreiche Möglichkeit zum Löschen eingeräumt werden.

- Schließlich muss durch geeignete technische und organisatorische Maßnahmen Datensicherheit und -integrität gewährleistet sein. Dies gilt insbesondere für die Datenkommunikation aus Fahrzeugen heraus.

Auf dieser Grundlage wirkt die Konferenz der Datenschutzbeauftragten des Bundes und der Länder darauf hin, dass Automobilhersteller, Zulieferer und ihre Verbände bundesweit einheitliche Datenschutzstandards auf hohem Niveau setzen, die dazu beitragen, dass Innovation auch mit gesellschaftlicher Akzeptanz einhergeht.

1.6 Entschließung zwischen der 87. und 88. Konferenz

Entschließung vom 25. April 2014: Ende der Vorratsdatenspeicherung in Europa!

Der Europäische Gerichtshof hat in seinem Urteil vom 8. April 2014 die Europäische Richtlinie zur Vorratsspeicherung von Telekommunikations-Verkehrsdaten (Richtlinie 2006/24/EG) für ungültig erklärt. Dieses Urteil hat weitreichende Folgen für den Datenschutz in Europa.

Die Datenschutzbeauftragten des Bundes und der Länder haben die anlasslose und massenhafte Speicherung von Verkehrsdaten der Telekommunikation stets abgelehnt. Sie begrüßen die Entscheidung des Europäischen Gerichtshofs als wichtigen Schritt zur Bekräftigung der informationellen Selbstbestimmung und des Telekommunikationsgeheimnisses.

Der Europäische Gerichtshof hat in seinem Urteil der undifferenzierten und automatischen Totalerfassung solcher Daten eine klare Absage erteilt. Er hat darauf hingewiesen, dass schon die Pflicht zur anlasslosen Speicherung einen besonders schwerwiegenden Eingriff großen Ausmaßes in das Recht auf Privatleben und den Datenschutz der Betroffenen darstellt. Diese in der Europäischen Grundrechte-Charta verbrieften Rechte dürften nur eingeschränkt werden, soweit dies absolut notwendig ist.

Die für ungültig erklärte Richtlinie entsprach diesen Vorgaben nicht, weil sie ohne jede Differenzierung, Einschränkung oder Ausnahme zur pauschalen Totalerfassung der Verkehrsdaten verpflichtete. Nach dem Urteil des Gerichtshofs kann eine undifferenzierte Pflicht zur anlasslosen und flächendeckenden Vorratsdatenspeicherung unionsrechtlich nicht mehr neu begründet werden. Die Absichtserklärung der Bundesregierung, zurzeit kein Gesetz zur Speicherung von Verkehrsdaten einzuführen, wird von der Konferenz der Datenschutzbeauftragten des Bundes und der Länder begrüßt. Etwaige Diskussionen auf europäischer Ebene sollten abgewartet werden.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder weist ausdrücklich darauf hin, dass der Maßstab des EuGH auch für das anlasslose exzessive Überwachen durch sämtliche Nachrichtendienste gelten muss.

Zudem hält der Gerichtshof die Pflicht zur großflächigen Speicherung von personenbezogenen Daten nur dann für zulässig, wenn die Daten in der Europäischen Union gespeichert werden und damit unter die Kontrolle unabhängiger Datenschutzbehörden fallen. Dies zwingt auch zu einer Neubewertung z. B. der Fluggastdaten-Übermittlung in die USA und des Safe-Harbor-Abkommens.

1.7 87. Konferenz vom 27. bis 28. März 2014 in Hamburg

1.7.1 Beschäftigtendatenschutzgesetz jetzt!

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

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

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

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

Hierfür müssen künftig gesetzliche Standards geschaffen werden, um sowohl die Rechtssicherheit für die Arbeitgeber zu erhöhen als auch einen wirksamen Grundrechtsschutz für die Beschäftigten zu schaffen.

1.7.2 „Biometrische Gesichtserkennung durch Internetdienste – Nur mit Wahrung des Selbstbestimmungsrechts Betroffener!“

Die Nutzung biometrischer Daten wird zunehmend zu einem Phänomen des Alltags. Dies gilt in besonderer Weise für die biometrische Gesichtserkennung, die in sozialen Medien auf dem Vormarsch ist. Für den Zweck der Auswertung von Personenfotos werden die Gesichter der Nutzer biometrisch erfasst, so dass ein späterer Abgleich mit anderen Fotos die Identifizierung einzelner Personen ermöglicht. Dazu werden sogenannte Templates erstellt. Dies sind mathematische Modelle der wesentlichen Merkmale des Gesichts wie etwa dem Abstand von Augen, Mundwinkel und Nasenspitze. Es darf nicht verkannt werden, dass die Vermessung der Gesichtsphysiognomie in hohem Maße die schutzwürdigen Interessen Betroffener berührt, denn stets ist die dauerhafte Speicherung eines Referenz-Templates des eigenen Gesichts erforderlich.

Dass die Templates dann in den Datenbanken global agierender Internetunternehmen gespeichert werden, stellt nicht erst seit den Enthüllungen über das Überwachungsprogramm Prism, das den US-Geheimdiensten den Zugriff auf die Datenbanken der US-Anbieter erlaubt, ein erhebliches Risiko für das Persönlichkeitsrecht des Einzelnen dar.

Die biometrische Gesichtserkennung ist eine Technik, die sich zur Ausübung von sozialer Kontrolle eignet und der damit ein hohes Missbrauchspotential immanent ist. Mit ihrer Hilfe ist es möglich, aus der Flut digitaler Fotografien im Internet gezielt Aufnahmen von Zielpersonen herauszufiltern. Darüber hinaus könnten durch den Abgleich von Videoaufnahmen mit vorhandenen Templates in Echtzeit Teilnehmerinnen und Teilnehmer etwa von Massenveranstaltungen sowie von Demonstrationen oder einfach nur Passanten individualisiert und identifiziert werden. Der Schutz der Anonymität des Einzelnen in der Öffentlichkeit lässt sich damit zerstören, ohne dass die Betroffenen ihre biometrische Überwachung kontrollieren oder sich dieser entziehen können.

An die Erzeugung biometrischer Templates der Gesichter von Personen durch Internet-Dienste sind daher hohe rechtliche Anforderungen zu stellen, die das informationelle Selbstbestimmungsrecht von Betroffenen in höchst möglicher Weise berücksichtigen:

- Die Erhebung, Verarbeitung und/oder Nutzung biometrischer Daten zur Gesichtserkennung zum Zweck der Erstellung eines dauerhaften biomet-

rischen Templates kann nur bei Vorliegen einer wirksamen Einwilligung des Betroffenen i. S. d. § 4 a BDSG rechtmäßig erfolgen.

- Die Einwilligung in die Erstellung biometrischer Templates zur Gesichtserkennung muss aktiv und ausdrücklich durch den Betroffenen erteilt werden. Die Betroffenen müssen vor der Erteilung der Einwilligung über die Funktionsweise der Erstellung und Nutzung der sie möglicherweise betreffenden Templates und die damit verfolgten Zwecke und Risiken in klarer und verständlicher Weise umfassend informiert werden. Eine Zweckänderung ist unzulässig. Sie bedarf einer Einwilligung, die dem Standard an die Einwilligungen bei der Verarbeitung besonderer personenbezogener Daten, § 4 a Abs. 3 BDSG, entspricht.

- Die Einwilligung kann nicht durch den Verweis auf entsprechende Klauseln in allgemeinen Nutzungsbedingungen oder Datenschutzerklärungen ersetzt werden.

- Für eine logische Sekunde kann es nach § 28 Abs. 1 Satz 1 Nr. 2 bzw. Nr. 3 BDSG auch ohne Einwilligung zulässig sein, ein Template zu erstellen, mit dem ein Abgleich mit bereits vorhandenen, zulässigerweise gespeicherten Templates im Rahmen des von der Einwilligung abgedeckten Zwecks möglich ist. Betroffene sind über den Umstand, dass Bilder zum Abgleich mit bestehenden Templates verwendet werden, zu informieren.

- Derartige biometrische Templates zum automatischen Abgleich, bei denen eine Einwilligung fehlt, sind unverzüglich nach dem Abgleich zu löschen.

- Die Speicherung von biometrischen Templates von Dritten, die – anders als die Nutzer von sozialen Medien – regelmäßig nicht einwilligen können, ist ausgeschlossen.

1.7.3 Struktur der künftigen Datenschutzaufsicht in Europa

Ein zentrales Verhandlungsthema bei den Beratungen im Rat der EU betrifft die Frage, welche Aufgaben die Datenschutzbehörden künftig haben und wie sie in Fällen, die mehrere Mitgliedstaaten oder die gesamte EU betreffen, besser zusammenarbeiten können. Die Europäische Kommission hatte hierzu das Prinzip einer einheitlichen An-laufstelle („One-Stop-Shop“) vorgeschlagen, wonach die Datenschutzbehörde am Sitz der Hauptniederlassung EU-weit zuständig ist für die Aufsicht über alle Niederlassungen eines Unternehmens innerhalb der EU. Daneben schlug sie die Einführung eines Kohärenzverfahrens vor, das es den Datenschutzbehörden ermöglichen soll, in

grenz-überschreitenden Fällen zu einheitlichen Entscheidungen im Rahmen des europäischen Datenschutzausschusses zu gelangen.

Vor dem Hintergrund der aktuell im Rat erörterten unterschiedlichen Modelle plädieren die Datenschutzbeauftragten des Bundes und der Länder für einen effektiven und bürgernahen Kooperations- und Entscheidungsmechanismus, der folgende Kernelemente beinhalten sollte:

1. Die Datenschutzbeauftragten des Bundes und der Länder bekräftigen den Grundsatz, dass jede Aufsichtsbehörde im Hoheitsgebiet ihres Mitgliedstaats die ihr mit der Verordnung übertragenen Aufgaben und Befugnisse über alle Datenverarbeitungen ausübt, durch welche Personen dieses Mitgliedstaates betroffen sind, unabhängig davon, ob die verantwortliche Stelle über eine Niederlassung innerhalb dieses Mitgliedstaates verfügt oder nicht.

2. Die Datenschutzbeauftragten des Bundes und der Länder befürworten die Ein-führung eines One-Stop-Shop-Mechanismus für Fälle, in denen der Datenverarbeiter über mehrere Niederlassungen in unterschiedlichen EU-Mitgliedstaaten verfügt. In diesem Fall fungiert die Aufsichtsbehörde am Ort der Hauptniederlassung als federführende Behörde, die mit den Aufsichtsbehörden der Mitgliedstaaten, in denen der Verantwortliche über weitere Niederlassungen verfügt oder in denen Personen betroffen sind, eng kooperiert. Es bleibt damit den betroffenen Personen unbenommen, sich an die Aufsichtsbehörden ihres Heimatlandes zu wenden.

3. Die federführende Behörde und die mit zuständigen nationalen Aufsichtsbehörden kooperieren mit dem Ziel einer einheitlichen Entscheidungsfindung. Im Falle der Einigkeit erlässt die federführende Behörde die erforderlichen Maßnahmen gegenüber der Hauptniederlassung des Verantwortlichen. Der Verantwortliche ist verpflichtet, die Maßnahmen in allen Niederlassungen innerhalb der EU umzusetzen.

4. Sofern eine nationale Behörde dem Maßnahmenentwurf der federführenden Behörde widerspricht, ist der Europäische Datenschutzausschuss mit dem Fall zu befassen, der hierzu verbindliche Leitlinien erlassen oder sonstige verbindliche Maßnahmen treffen kann.

5. Die Datenschutzbeauftragten des Bundes und der Länder befürworten die in dem Verordnungsentwurf enthaltenen Elemente zur Stärkung der Verantwortlichkeit der Unternehmen zur Einhaltung des Datenschutzrechts. Hierzu zählen die EU-weite Einführung betrieblicher Datenschutzbeauftragter, Datenschutz-Folgeabschätzungen, Privacy-by-Design und Privacy-by-Default, Zertifizierungen, Datenschutzsiegel und Verhaltensregeln. Fragen zur Rechtskonformität einer Datenverarbeitung

können im Rahmen der vorherigen Zurateziehung mit den Aufsichtsbehörden geklärt werden.

6. Für die Einführung formeller, fristgebundener Verfahren zur Erlangung EU-weit gültiger Compliance-Entscheidungen besteht aus Sicht der Datenschutzbeauftragten des Bundes und der Länder daneben kein Bedarf. Insbesondere darf die Klärung von Compliance-Fragen nicht zu einer Verlagerung der Verantwortlichkeit auf die Aufsichtsbehörden und zur Einschränkung aufsichtsbehördlicher Maßnahmen im Falle von Datenschutzverstößen führen.

7. Ein originärer Schwerpunkt der Aufsichtstätigkeit in Bezug auf Zertifizierungsprozesse sollte darin liegen, im Rahmen der Norminterpretation Prüfstandards mitzugestalten, auf deren Grundlage die Vergabe von Zertifikaten geprüft wird.

1.7.4 „Öffentlichkeitsfahndung mit Hilfe sozialer Netzwerke – Strenge Regeln erforderlich!“

Mit zunehmender Beliebtheit sozialer Netzwerke bei Bürgerinnen und Bürgern steigt das Interesse von Strafverfolgungsbehörden, diese sozialen Netzwerke auch zur Öffentlichkeitsfahndung zu nutzen. So gibt es in Deutschland bereits Polizeidienststellen, die mittels Facebook nach Straftätern suchen. Auch die 84. Konferenz der Justizministerinnen und Justizminister hat sich im November 2013 mit dem Thema befasst.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hält es erneut für notwendig darauf hinzuweisen, dass eine Nutzung sozialer Netzwerke privater Betreiber (wie z. B. Facebook) zur Öffentlichkeitsfahndung aus datenschutzrechtlicher Sicht sehr problematisch ist. Durch die weltweit recherchierbare Veröffentlichung von Fahndungsdaten wird in weitaus schwerwiegenderer Weise in die Grundrechte Betroffener (Tatverdächtiger oder auch Zeugen) eingegriffen, als dies bei der Nutzung klassischer Medien der Fall ist. Auch sind im Internet veröffentlichte Daten einer Fahndungsausschreibung nur sehr schwer bzw. gar nicht mehr zu löschen. Geben Nutzerinnen und Nutzer der sozialen Netzwerke in Diskussionsforen und Nutzerkommentaren öffentlich Spekulationen, Behauptungen und Diskriminierungen ab, beeinträchtigt dies die Persönlichkeitsrechte der Betroffenen erheblich. Solche Funktionen sind in von den Ermittlungsbehörden betriebenen Angeboten weder geeignet noch erforderlich, um die behördlichen Aufgaben zu erfüllen. Die Konferenz weist darauf hin, dass Öffentlichkeitsfahndung nur auf Diensten von Anbietern erfolgen darf, die die datenschutzrechtlichen Vorgaben des Telemediengesetzes zur Nutzungsdatenverarbeitung, insbesondere der Regeln zur Reichweitenmessung gemäß §§ 13 Abs. 4

Nr. 6, 15 Abs. 3 TMG, und das Recht auf anonyme und pseudonyme Nutzung gemäß § 13 Abs. 6 TMG beachten.

Sofern es Strafverfolgungsbehörden gleichwohl gestattet werden soll, zu Zwecken der Öffentlichkeitsfahndung auf soziale Netzwerke mit deaktivierter Kommentierungsfunktion zurückzugreifen, so darf dies – ungeachtet der generellen Kritik an der Nutzung sozialer Netzwerke durch öffentliche Stellen – nur geschehen, wenn folgende Maßgaben beachtet werden:

- Die Vorschriften der Strafprozessordnung (§ 131 Abs. 3, § 131 a Abs. 3, § 131 b StPO) zur Öffentlichkeitsfahndung kommen aufgrund der technikoffenen Formulierung als Rechtsgrundlage für die Öffentlichkeitsfahndung im Internet grundsätzlich in Betracht. Sie sind aber im Hinblick auf den Verhältnismäßigkeitsgrundsatz nur eingeschränkt anzuwenden. Eine entsprechende Klarstellung durch den Gesetzgeber wäre wünschenswert. Zumindest aber sind die besonderen Voraussetzungen der Fahndung im Internet, insbesondere in sozialen Netzwerken in Umsetzungsvorschriften zu konkretisieren. Änderungsbedarf besteht beispielsweise für die Anlage B der RiStBV.

- In materiell-rechtlicher Hinsicht haben die Strafverfolgungsbehörden den Verhältnismäßigkeitsgrundsatz strikt zu beachten. Die zu schaffenden Regelungen müssen den besonderen Gefahren der Öffentlichkeitsfahndung in sozialen Netzwerken gerecht werden. Insbesondere muss sichergestellt werden, dass eine solche Fahndung nur bei im Einzelfall schwerwiegenden Straftaten überhaupt in Betracht gezogen werden kann.

- In verfahrensrechtlicher Hinsicht müssen die Umsetzungsregelungen die Staatsanwaltschaft verpflichten, bereits im Antrag auf richterliche Anordnung der Maßnahme die Art, den Umfang und die Dauer der Öffentlichkeitsfahndung konkret anzugeben. Dies umfasst insbesondere die ausdrückliche Angabe, ob und warum die Anordnung auch die Öffentlichkeitsfahndung in sozialen Netzwerken umfassen soll.

- Es ist sicherzustellen, dass

  - die zur Öffentlichkeitsfahndung verwendeten personenbezogenen Daten von den Strafverfolgungsbehörden ausschließlich auf im eigenen Verantwortungsbereich stehenden Servern gespeichert und verarbeitet werden, nicht hingegen auf Servern der privaten Anbieter,

- die Weitergabe und der automatisierte Abruf der personenbezogenen Daten aus dem Internet durch Web-Crawler und ähnliche Dienste so weit als technisch möglich verhindert werden,

- die Kommunikation zwischen den Strafverfolgungsbehörden und den Nutzern nur außerhalb der sozialen Netzwerke erfolgt.

1.7.5 „Gewährleistung der Menschenrechte bei der elektronischen Kommunikation“

Die Enthüllungen des Whistleblowers Edward Snowden haben ein Ausmaß an geheimdienstlicher Überwachung aufgezeigt, das viele zuvor nicht für möglich gehalten hatten. Die tendenziell unbegrenzte und kaum kontrollierte Überwachung der elektronischen Kommunikation aller verletzt das auch im digitalen Zeitalter weltweit anerkannte Recht auf Privatheit in täglich wiederkehrender millionenfacher Weise. Dies beeinträchtigt zugleich die Wahrnehmung anderer Menschenrechte wie der Meinungs- und Versammlungsfreiheit. Es ist eine gesamtgesellschaftliche Aufgabe, berechtigtes Vertrauen in die prinzipielle Unverletzlichkeit der Kommunikation wieder herzustellen.

Die Datenschutzbeauftragten des Bundes und der Länder haben daher schon im September 2013 gefordert, auf diese neue Qualität der Überwachung rechtlich und politisch zu reagieren. Darüber hinaus sind aber auch technische und organisatorische Schutzmaßnahmen erforderlich. Der Schutz der informationellen Selbstbestimmung der in Deutschland lebenden Menschen sowie der Vertraulichkeit und Integrität informationstechnischer Systeme muss wiederhergestellt und dauerhaft gesichert werden.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder fordert daher die Prüfung und Umsetzung folgender Maßnahmen:

1. Sichere Verschlüsselung beim Transport und bei der Speicherung von Daten,

2. Bereitstellung einer einfach bedienbaren Verschlüsselungs-Infrastruktur,

3. Einsatz von Ende-zu-Ende-Verschlüsselung in Kombination mit Verfahren zur Verbindungsverschlüsselung,

4. Sichere und vertrauenswürdige Bereitstellung von Internetangeboten,

5. Weiterentwicklung innovativer Vorkehrungen zum Schutz von Verkehrsdaten,

6. Ausbau der Angebote und Förderung anonymer Kommunikation,

7. Angebot für eine Kommunikation über kontrollierte Routen,

8. Sichere Verschlüsselung der Mobilkommunikation und Einschränkung der Möglichkeiten der Geolokalisierung,

9. Beschränkung des Cloud Computing mit personenbezogenen Daten auf vertrauenswürdige Anbieter mit zertifizierter Informationssicherheit,

10. Förderung der Vertrauenswürdigkeit informationstechnischer Systeme durch Zertifizierung,

11. Sensibilisierung von Nutzerinnen und Nutzern moderner Technik,

12. Ausreichende Finanzierung von Maßnahmen der Informationssicherheit.

Der Arbeitskreis „Technische und organisatorische Datenschutzfragen“ der Datenschutzkonferenz hat einen Anforderungskatalog formuliert, der die hier genannten Maßnahmen konkretisiert (siehe Anlage zu dieser Entschließung).

Die Datenschutzbeauftragten des Bundes und der Länder fordern die Anbieter elektronischer Kommunikationsdienste auf, entsprechende Technologien und Dienste zur Verfügung zu stellen. Die Verwaltungen in Bund und Ländern, insbesondere die zuständigen Regulierungsbehörden, sind aufgefordert, auf die Durchsetzung der o. g. Maßnahmen zu dringen. Der Gesetzgeber ist aufgerufen, die zu ihrer Durchsetzung ggf. nötigen Änderungen und Präzisierungen an dem bestehenden Rechtsrahmen vorzunehmen.

Anlage zur Entschließung „Gewährleistung der Menschenrechte bei der elektronischen Kommunikation“

Die Anlage kann auch aus unserem Internetangebot unter http://www.lda.brandenburg.de abgerufen werden.

2 Beschlüsse der Aufsichtsbehörden für den Datenschutz im nicht öffentlichen Bereich (Düsseldorfer Kreis)

2.1 Beschluss vom 15./16. September 2015

Nutzung von Kameradrohnen durch Private

In jedem Elektronikmarkt sind sie mittlerweile zu finden: Drohnen mit Kameraausstattung zu einem erschwinglichen Preis. Drohnen kommen als unbemannte Luftfahrzeuge nicht nur in Krisengebieten oder in der Landwirtschaft zum Einsatz, sondern werden immer häufiger auch von Privaten für die Freizeitbeschäftigung gekauft und im nachbarschaftlichen Umfeld eingesetzt. Da können durchaus Begehrlichkeiten aufkommen: ein unbeobachteter Blick in den Garten des Nachbarn, auf die Sonnenterrasse oder in sonstige nicht einfach zugängliche Orte.

Der potentiell überwachbare Bereich wird nur von den technischen Gegebenheiten des eingesetzten Geräts begrenzt. Mauern, Zäune oder sonstige Abtrennungen, die Dritten das Betreten des so geschützten Bereichs oder den Einblick in diesen erschweren oder unmöglich machen sollen, stellen im Rahmen des Drohneneinsatzes kein Hindernis mehr dar. Darüber hinaus ist es für Betroffene auch regelmäßig nicht ohne weiteres möglich, den für den Drohneneinsatz Verantwortlichen zu erkennen. Aus diesen Gründen kann der Einsatz von mit Videokameras ausgerüsteten Drohnen im Vergleich zum Einsatz stationärer Videoüberwachungsmaßnahmen mit einem ungleich größeren Eingriff in das informationelle Selbstbestimmungsrecht der Betroffenen verbunden sein.

Auch wenn der Betrieb von Drohnen durch Privatpersonen zu Zwecken des Sports oder der Freizeitgestaltung mit Ausnahme von § 16 Abs. 1 Nr. 1 LuftVO keiner luftverkehrsrechtlichen Erlaubnis der zuständigen Landesluftfahrtbehörde bedarf und im Hinblick auf § 1 Abs. 2 Nr. 3 des Bundesdatenschutzgesetzes (BDSG) außerhalb des datenschutzrechtlichen Regelungsregimes erfolgen kann, sind Verwendungen von Drohnen mit Videotechnik denkbar, die in den Anwendungsbereich des BDSG fallen. In solchen Fällen sind Drohnen nur im Rahmen von datenschutzrechtlichen Erlaubnisnormen zu betreiben, wobei deren Voraussetzungen in der Mehrzahl der Fälle wegen des regelmäßigen Überwiegens von Interessen Betroffener nicht gegeben sind. Dies ist insbesondere dann der Fall, wenn die Aufnahmen für eine Veröffentlichung im Internet stattfinden oder ein zielgerichteter Drohneneinsatz zur kontinuierlichen Beobachtung öffentlich zugänglicher Räume im Sinne des § 6 b BDSG erfolgt. Wenn solche Drohnen innerhalb des Anwendungsbereiches des BDSG betrieben werden und hierbei unbefugt Daten

erhoben oder verarbeitet werden, kann die zuständige Behörde hierfür ein Bußgeld von bis zu 300.000 Euro verhängen.

Jedoch sind auch außerhalb des Anwendungsbereiches des BDSG rechtliche Rahmenbedingungen zu beachten. So sind auch hier das Recht am eigenen Bild, das Grundrecht der Betroffenen auf informationelle Selbstbestimmung im Besonderen sowie das Persönlichkeitsrecht im Allgemeinen zu wahren.

Dem mit dem Drohneneinsatz verbundenen Eingriff in das allgemeine Persönlichkeitsrecht Betroffener kann neben den Möglichkeiten der zuständigen Aufsichts- oder Bußgeldbehörde auch zivilrechtlich begegnet werden. Vor allem dann, wenn die Verletzung des allgemeinen Persönlichkeitsrechts in einem Eindringen in geschützte Bereiche, wie beispielsweise das befriedete und blickgeschützte Grundstück, besteht oder eine zielgerichtete Beobachtung erkennbar stattfindet. Dem Betroffenen kann in solchen Fällen ein Abwehranspruch aus § 823 in Verbindung mit § 1004 Abs. 1 des Bürgerlichen Gesetzbuches (BGB) analog zustehen. Auch das Kunsturhebergesetz (KUG), welches das Recht am eigenen Bild – als besondere Ausprägung des allgemeinen Persönlichkeitsrechts – schützt, kann tangiert sein (§§ 22, 23 KUG), sofern eine Verbreitung oder Veröffentlichung der Aufzeichnungen erfolgt.

Die Strafverfolgungsbehörden können eingeschaltet werden, wenn durch den Drohneneinsatz die Verwirklichung von Straftatbeständen droht, wie beispielsweise bei der Anfertigung von Bildaufnahmen höchstpersönlicher Lebensbereiche (§ 201 a des Strafgesetzbuches (StGB)), mithin Bereiche der Intimsphäre (im Einzelnen dazu: Bundestagsdrucksache 15/2466, S. 5.) oder der Aufzeichnung des nichtöffentlich gesprochenen Wortes (§ 201 StGB).

Der Düsseldorfer Kreis fordert daher Drohnenbetreiber auf, grundsätzlich niemanden ohne seine Einwilligung zu filmen und die Privatsphäre anderer zu achten. Private Nutzer dürfen Drohnen mit Foto- oder Videoausrüstung nur in solchen Bereichen einsetzen, in denen eine Verletzung von Rechten Dritter ausgeschlossen werden kann.

2.2 Beschluss vom 20. Mai 2014

Smartes Fernsehen nur mit smartem Datenschutz

Gemeinsame Position

der

Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich (Düsseldorfer Kreis)

und der

Datenschutzbeauftragten der öffentlich-rechtlichen Rundfunkanstalten

Moderne Fernsehgeräte (Smart-TV) bieten neben dem Empfang des Fernsehsignals u. a. die Möglichkeit, Internet-Dienste aufzurufen. Den Zuschauern ist es somit möglich, simultan zum laufenden TV-Programm zusätzliche Web-Inhalte durch die Sender auf dem Bildschirm anzeigen zu lassen (etwa durch den HbbTV-Standard). Auch Endgerätehersteller bieten über eigene Web-Plattformen für Smart-TV-Geräte verschiedenste Internet-Dienste an. Für die Zuschauer ist aufgrund der Verzahnung der Online- mit der TV-Welt oft nicht mehr erkennbar, ob sie gerade das TV-Programm oder einen Internet-Dienst nutzen. Überdies können sie vielfach nicht erkennen, um welchen Dienst es sich handelt.

Durch die Online-Verbindung entsteht – anders als beim bisherigen Fernsehen – ein Rückkanal vom Zuschauer zum Fernsehsender, zum Endgerätehersteller oder zu sonstigen Dritten. Das individuelle Nutzungsverhalten kann über diesen Rückkanal erfasst und ausgewertet werden.

Fernsehen ist ein maßgebliches Medium der Informationsvermittlung und notwendige Bedingung für eine freie Meinungsbildung. Das Recht auf freien Informationszugang ist verfassungsrechtlich geschützt und Grundbedingung der freiheitlich demokratischen Grundordnung. Die Wahrnehmung dieses Rechts würde durch die umfassende Erfassung, Auswertung und Nutzung des Nutzungsverhaltens empfindlich beeinträchtigt.

Aus datenschutzrechtlicher Sicht sind die folgenden Anforderungen zu beachten:

1. Die anonyme Nutzung von **Fernsehangeboten** muss auch bei Smart-TV-Nutzung gewährleistet sein. Eine Profilbildung über das individuelle Fernsehverhalten ist ohne informierte und ausdrückliche Einwilligung der Zuschauer unzulässig.

2. Soweit Web- oder HbbTV-Dienste über Smart-TV-Geräte genutzt werden, unterliegen diese als **Telemedien** den datenschutzrechtlichen Anforderungen des Telemediengesetzes. Endgerätehersteller, Sender sowie alle sonstigen Anbieter von Telemedien müssen entweder eine entsprechende Einwilligung der Betroffenen einholen oder zumindest die folgenden rechtlichen Vorgaben beachten:

   - Auch personenbeziehbare Daten der Nutzer dürfen nur verwendet werden, sofern dies zur Erbringung der Dienste oder zu Abrechnungszwecken erforderlich ist.

   - Spätestens bei Beginn der Nutzung müssen die Nutzer erkennbar und umfassend über die Datenerhebung und -verwendung informiert werden.

   - Anbieter von Telemedien dürfen nur dann Nutzungsprofile erstellen und analysieren, sofern hierzu Pseudonyme verwendet werden und die betroffene Nutzerin oder der betroffene Nutzer dem nicht widersprochen hat. Derartige Widersprüche sind wirksam umzusetzen, insbesondere im Gerät hinterlegte Merkmale (z. B. Cookies) sind dann zu löschen. Auf das Widerspruchsrecht sind die Nutzer hinzuweisen. IP-Adressen und Gerätekennungen sind keine Pseudonyme im Sinne des Telemediengesetzes.

   - Verantwortliche Stellen haben sicherzustellen, dass Nutzungsprofildaten nicht mit Daten über den Träger des Pseudonyms zusammengeführt werden.

3. Beachtung des Prinzips „privacy by default“: Die Grundeinstellungen der Smart-TV-Geräte und Web-Dienste sind durch die Hersteller und Anbieter derart zu gestalten, dass dem Prinzip der anonymen Nutzung des Fernsehens hinreichend Rechnung getragen wird. Der Aufruf der Web-Dienste und die damit einhergehende wechselseitige Kommunikation mit Endgerätehersteller, Sender oder sonstigen Anbietern per Internet dürfen erst nach umfassender Information durch die Nutzer selbst initiiert werden, z. B. die Red-Button-Aktivierung bei HbbTV. Die auf den Geräten gespeicherten Daten müssen der Kontrolle durch die Nutzer unterliegen. Insbesondere muss die Möglichkeit bestehen, Cookies zu verwalten.

4. Smart-TV-Geräte, die HbbTV-Angebote der Sender sowie sonstige Web-Dienste müssen über sicherheitstechnische Mechanismen verfügen, die die Geräte und den Datenverkehr vor dem Zugriff unbefugter Dritter schützen.

Diese Position wird von der Konferenz der Direktoren der Landesanstalten für Medien unterstützt.

2.3 Beschlüsse vom 25./26. Februar 2014

2.3.1 Unzulässigkeit von Videoüberwachung aus Fahrzeugen (sog. Dashcams)

Mittlerweile nimmt der Einsatz sog. Dashcams auch in Deutschland immer mehr zu, um, so die standardmäßige Begründung, im Falle eines Unfalls den Hergang nachvollziehen und das Video gegebenenfalls als Nachweis bei der Regulierung von Schadensfällen und der Klärung von Haftungsfragen heranziehen zu können.

Die Aufsichtsbehörden des Bundes und der Länder für den Datenschutz im nicht-öffentlichen Bereich machen darauf aufmerksam, dass der Einsatz solcher Kameras – jedenfalls sofern dieser nicht ausschließlich für persönliche oder familiäre Tätigkeiten erfolgt – datenschutzrechtlich unzulässig ist.

Soweit mit den Dashcams in öffentlich zugänglichen Bereichen gefilmt wird und als Hauptzweck der Aufnahmen die Weitergabe von Filmaufnahmen zur Dokumentation eines Unfallhergangs angegeben wird, ist der Einsatz – auch wenn die Kameras von Privatpersonen eingesetzt werden – an den Regelungen des Bundesdatenschutzgesetzes zu messen. Gemäß § 6 b Abs. 1 Nr. 3 und Abs. 3 des Bundesdatenschutzgesetzes (BDSG) 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.

Diese Voraussetzungen sind in aller Regel nicht erfüllt, da die schutzwürdigen Interessen der Verkehrsteilnehmer überwiegen. Das informationelle Selbstbestimmungsrecht umfasst das Recht des Einzelnen, sich in der Öffentlichkeit frei zu bewegen, ohne befürchten zu müssen, ungewollt und anlasslos zum Objekt einer Videoüberwachung gemacht zu werden. Dashcams zeichnen den Verkehr sowie Personen, die sich in der Nähe einer Straße aufhalten, ohne Anlass und permanent auf, so dass eine Vielzahl von Verkehrsteilnehmern betroffen ist, die sämtlich unter einen Generalverdacht gestellt werden, ohne dass sie von der Überwachung Kenntnis erlangen oder sich dieser entziehen können. Das Interesse des Autofahrers, für den eher theoretischen Fall eines Verkehrsunfalls Videoaufnahmen als Beweismittel zur Hand zu haben, kann diesen gravierenden Eingriff in das Persönlichkeitsrecht der Verkehrsteilnehmer nicht rechtfertigen.

Da selbst die Polizei Videokameras zur Verfolgung von Straftaten und Ordnungswidrigkeiten nur auf der Grundlage spezifischer Regelungen und ausschließlich dann einsetzen darf, wenn gegen die betroffene Person ein entsprechender Anfangsverdacht besteht, können erst recht sonstige Stellen nicht für sich beanspruchen, den öffentlichen Verkehrsraum anlass- und schrankenlos mittels Kameras zu überwachen.

2.3.2 Modelle zur Vergabe von Prüfzertifikaten, die im Wege der Selbstregulierung entwickelt und durchgeführt werden

I. Ausgangslage

Freiwillige Audits leisten einen bedeutenden Beitrag für den Datenschutz, weil sie als aus eigenem Antrieb veranlasste Maßnahme die Chance in sich bergen, zu mehr Datenschutz in der Fläche zu gelangen.

Datenschutz sollte ein Wettbewerbsvorteil sein. Unternehmen, die sich um einen hohen Datenschutzstandard bemühen, möchten dies auch anerkannt sehen. Ein Datenschutzzertifikat ist ein wichtiges Signal an diese Unternehmen.

Zugleich trägt ein Zertifikat dazu bei, das Vertrauen von Bürgerinnen und Bürgern, Verbraucherinnen und Verbraucher in den achtsamen Umgang mit ihren Daten zu fördern.

Eigenverantwortung ist eine wichtige Säule für einen funktionierenden Datenschutz.

Der Ruf nach einem Audit hat im Zuge der Diskussion um den Europäischen Rechtsrahmen weiteren Auftrieb erhalten. Initiativen auf Landesebene und nunmehr auch auf Bundesebene haben dieses Anliegen aufgegriffen.

II. Erprobung von Modellen, Anforderungen

Die Gesetzgeber haben bisher lediglich einzelne Teilregelungen zu Zertifizierungen getroffen.

Der Düsseldorfer Kreis unterstützt weitergehende Bemühungen, Erfahrungen mit Zertifizierungen zu sammeln, die in eigener Verantwortung im Wege der Selbstregulierung auf der Grundlage von Standards erfolgen, die die Aufsichtsbehörden befürworten.

Verlässliche Aussagen für Bürgerinnen und Bürger, für Verbraucherinnen und Verbraucher erfordern, dass Zertifizierungsdienste anbietende Stellen (Zertifizierungsdienste) geeignete inhaltliche und organisatorische Vorkehrungen

für derartige Verfahren mit dem Ziel treffen, eine sachgerechte und unabhängige Bewertung zu gewährleisten.

Dazu gehören im Kern folgende, von Zertifizierungsdiensten zu bearbeitende Strukturelemente:

- Prüffähige Standards, die von den Aufsichtsbehörden befürwortet werden, zu entwickeln, zu veröffentlichen und zur Nutzung für Dritte freizugeben,

- beim Zertifizierungsprozess zwischen verschiedenen Ebenen zu unterscheiden (Prüfung, Zertifizierung, Akkreditierung),

- für verschiedene auf Ebenen und/oder in Verfahrensabschnitten anfallende Aufgaben voneinander abzugrenzende Rollen der jeweils Mitwirkenden vorzusehen,

- Regelungen zur Vermeidung von Interessenkollisionen der an einem Zertifizierungsprozess Beteiligten zu treffen,

- Anforderungen an die Eignung als Prüferin und Prüfer festzulegen und diesen Personenkreis für Zertifizierungen zu qualifizieren,

- den geprüften Sachbereich so zu umschreiben, dass Bürgerinnen und Bürger, Kundinnen und Kunden die Reichweite der Prüfaussage ohne weiteres dem Zertifikat entnehmen können,

- Bedingungen für Erteilung, Geltungsdauer und Entzug von Zertifikaten zu bestimmen,

- Zertifikate zusammen mit den wesentlichen Ergebnissen der Prüfberichte zu veröffentlichen.

III. Abstimmung im Düsseldorfer Kreis

Der Düsseldorfer Kreis verfolgt die Entwicklung von sowohl auf Landesebene mit dieser Zielrichtung begleiteten Initiativen als auch auf Bundesebene begonnenen weiteren Initiativen. Er beteiligt sich an einer ergebnisoffenen Diskussion, um zu optimalen Verfahrensgestaltungen zu gelangen.

Die im Düsseldorfer Kreis zusammenwirkenden Aufsichtsbehörden sehen daher als gemeinsame Aufgabe, sich auf inhaltliche und verfahrensmäßige Anforderungen für Zertifizierungsverfahren zu verständigen und zu Bera-

tungsersuchen im Interesse einer bundesweit einheitlichen Aufsichtspraxis auf im Düsseldorfer Kreis abgestimmter Grundlage Stellung zu nehmen.

2.4 Beschluss vom 27. Januar 2014

Orientierungshilfe zur Einholung von Selbstauskünften bei Mietinteressenten

Vor der Vermietung von Wohnraum erheben Vermieter bei den Mietinteressenten zum Teil sehr umfangreiche persönliche Angaben, auf deren Basis sie ihre Entscheidung über den Vertragsabschluss treffen. An der Beantwortung solcher Selbstauskünfte muss der Vermieter jedoch ein berechtigtes Interesse haben und es dürfen nur solche Daten erhoben werden, die zur Durchführung des Mietvertrags erforderlich sind. Die legitimerweise zu stellenden Fragen basieren folglich auf einer Abwägung der Interessen des Vermieters gegenüber dem Recht des Mietinteressenten auf informationelle Selbstbestimmung.

Die Orientierungshilfe „Einholung von Selbstauskünften bei Mietinteressenten“ zeigt die wichtigsten Grundsätze auf. Für häufige Fallgestaltungen wird – ohne Anspruch auf Vollständigkeit – dargestellt, was zulässig ist.

Anlage: Orientierungshilfe zur Einholung von Selbstauskünften bei Mietinteressenten (Stand: Januar 2014)

Die Orientierungshilfe kann auch aus unserem Internetangebot unter http://www.lda.brandenburg.de abgerufen werden.

3 Entschließungen der Konferenz der Informationsfreiheitsbeauftragten in Deutschland

3.1 Entschließung zwischen der 30. und 31. Konferenz

Entschließung vom 4. Dezember 2015: Informationsfreiheit 2.0 – endlich gleiches Recht in Bund und Ländern!*

Vor zehn Jahren hat der Deutsche Bundestag das Informationsfreiheitsgesetz verabschiedet und damit für solche Länder, die bislang noch kein derartiges Gesetz kannten, ein Beispiel gegeben. Inzwischen besteht in elf Ländern ein Recht auf Zugang zu Verwaltungsinformationen, ohne dass die Antragsteller ihr Einsichtsinteresse begründen müssen.

Trotz einer flächendeckenden Entwicklung hin zu mehr Verwaltungstransparenz besteht weiterhin Handlungsbedarf. So zeigen weder Bayern noch Hessen Bestrebungen, Informationsfreiheitsgesetze zu schaffen. Die niedersächsische Landesregierung hat zwar beschlossen, einen Entwurf vorzulegen, berät aber noch über die Einzelheiten. In Sachsen soll bis spätestens 2019 ein Informationsfreiheitsgesetz geschaffen werden. Indes enttäuscht der lange erwartete Gesetzentwurf der baden-württembergischen Landesregierung durch viele überflüssige Einschränkungen. Das brandenburgische Beispiel zeigt, dass auch die Novellierung vorhandener Gesetze dazu dienen kann, das Rad durch die Schaffung neuer Ausnahmen zurückzudrehen. Die Umsetzung der Evaluation des Informationsfreiheitsgesetzes des Bundes steht noch aus. Ob dort – ebenso wie bereits in den Transparenzgesetzen von Hamburg und Bremen – Verwaltungen verpflichtet werden, bestimmte Informationen von sich aus im Internet zu veröffentlichen, ist ungewiss. In Rheinland-Pfalz tritt zum 1. Januar 2016 als erstem Flächenland ein solches Transparenzgesetz in Kraft. Es umfasst auch das im Übrigen bundesweit eingeführte Recht auf Zugang zu Umweltinformationen. Auch in Thüringen und Nordrhein-Westfalen ist laut Koalitionsvertrag beabsichtigt, das derzeitige Informationsfreiheitsgesetz zu einem Transparenzgesetz fortzuentwickeln.

Nach Auffassung der Informationsfreiheitsbeauftragten sollten moderne Regelungen über den Informationszugang in Form effektiver Transparenzgesetze

1. der herkömmlichen Informationserteilung auf Antrag eine Pflicht der Verwaltung zur proaktiven Veröffentlichung von Informationen in Open-Data-Portalen zur Seite stellen,

2. Ausnahmen vom freien Zugang zu Informationen nur in einem unbedingt erforderlichen Maß enthalten,

3. neben klassischen Verwaltungen auch Unternehmen der öffentlichen Hand einbeziehen und

4. der vorhandenen Rechtszersplitterung auf dem Gebiet der Informationsfreiheit entgegenwirken und das Umweltinformationsrecht mit dem Informationsfreiheitsrecht zusammenführen.

Sowohl bei der Novellierung vorhandener als auch bei der Schaffung neuer Regelungen muss die Erhöhung der Transparenz oberstes Ziel sein. Nach Auffassung der Informationsfreiheitsbeauftragten gibt es keinen vernünftigen Grund dafür, dass einige Länder noch immer kein Recht auf voraussetzungslosen Zugang zu Informationen haben.

Die Informationsfreiheit hat dort, wo sie eingeführt wurde, zu mehr staatlicher Transparenz, einer besseren Informiertheit der Bürger und einer offeneren Verwaltungskultur geführt. Transparenzgesetze und Open-Data-Plattformen im Internet haben diese Wirkung in erfreulicher Weise befördert. Die Befürchtung von Kritikern, dass Verwaltungen von einer Antragsflut überrannt würden, hat sich nicht bewahrheitet.

Die Konferenz der Informationsfreiheitsbeauftragten in Deutschland fordert die Gesetzgeber in Bund und Ländern auf, die positiven Erfahrungen mit der Informationsfreiheit in Deutschland anzuerkennen und die Einheitlichkeit der Lebensbedingungen auch im Bereich der Verwaltungstransparenz herzustellen.

* bei Stimmenenthaltung der Bundesbeauftragten für den Datenschutz und die Informationsfreiheit

3.2 30. Konferenz der Informationsfreiheitsbeauftragten am 30. Juni 2015 in Schwerin

3.2.1 Mehr Transparenz bei den Verhandlungen über das Transatlantische Freihandelsabkommen (TTIP)!

Die Bundesregierung hat sich dafür ausgesprochen, noch im Jahr 2015 das geplante Freihandelsabkommen (Transatlantic Trade and Investment Partnership, TTIP) zwischen der EU und den Vereinigten Staaten von Amerika zu verabschieden. Mit dem geplanten Abkommen würde die derzeit weltgrößte Freihandelszone entstehen.

Seit der Aufnahme der Verhandlungen zwischen der EU und den USA im Jahr 2013 wurden deren Intransparenz und der spärliche Informationsfluss

kritisiert. Als Reaktion auf diese Kritik hat die EU-Handelskommissarin Cecilia Malmström im November 2014 mehr Transparenz versprochen. In diesem Rahmen hat sich die Europäische Kommission dazu verpflichtet, die Öffentlichkeit darüber zu informieren, mit wem sich ihre führenden Politiker und höheren Beamten treffen und einen erweiterten Zugang zu Dokumenten im Zusammenhang mit den Verhandlungen über eine transatlantische Handels- und Investitionspartnerschaft mit den Vereinigten Staaten zu ermöglichen.

Die Konferenz der Informationsfreiheitsbeauftragten in Deutschland (IFK) sieht diese Initiative als einen wichtigen ersten Schritt hin zu mehr Offenheit und mahnt deren Fortführung und Ausweitung dringlich an. Sie hebt die Notwendigkeit größtmöglicher Transparenz in den Verhandlungen für eine lebendige öffentliche Debatte hervor, in der die Bürgerinnen und Bürger vollständig über die Auswirkungen auf ihr tägliches Leben informiert werden. Die Informationsfreiheitsbeauftragten fordern im Sinne von Open Government Data, der Öffentlichkeit neben zusammenfassenden und erläuternden Informationen vermehrt Originaldokumente zur Verfügung zu stellen, um es den Bürgerinnen und Bürgern zu ermöglichen, sich eine eigene Meinung von den Inhalten und dem Ablauf der Verhandlungen zu bilden. Hierzu gehören auch Informationen über die Positionen und Forderungen der USA sowie von Lobbyisten. Eine umfassende Offenlegung von Informationen zu TTIP auf EU- sowie auf Bundes-Ebene soll so früh und so weit wie möglich erfolgen. Erst wenn Originaldokumente aus den Bereichen Umwelt-, Arbeitnehmer- und Verbraucherschutz bekannt sind, kann beurteilt werden, ob es zu einer Absenkung europäischer Standards kommt.

Die IFK fordert die Bundesregierung und die Europäische Kommission dazu auf, in den Verhandlungen mit den USA darauf zu bestehen, dass für Streitigkeiten zwischen den Handelspartnern öffentlich tagende hoheitliche Gerichte geschaffen werden. Nur dadurch kann die notwendige Transparenz gewährleistet werden.

3.2.2 Auch Kammern sind zur Transparenz verpflichtet!

Immer wieder verweigern sich berufsständische Kammern den Transparenzanforderungen der jeweiligen Informationszugangsgesetze.

Berufsständische Kammern nehmen hoheitliche Aufgaben auf Bundes- und Länderebene wahr. Für die jeweiligen Berufsgruppen besteht eine gesetzliche Pflicht zur Mitgliedschaft, die Kammern sind für Berufszulassungen zuständig und haben oft weitgehende Sanktionsmöglichkeiten.

Informationen, die im Rahmen ihrer Tätigkeit anfallen, unterfallen den Informationszugangsgesetzen von Bund und Ländern. Dies gilt auch für Jahresabschlüsse und Angaben zu Einnahmen, Ausgaben und Rückstellungen der

Kammern. Für die Verpflichtung der Kammern ist es unerheblich, ob Antragstellende Kammermitglieder sind und welche Motive zur Antragstellung führten. Öffentlich-rechtliche Körperschaften befinden sich in weiten Bereichen nicht in Konkurrenz zu Marktteilnehmern – Wettbewerbsnachteile können sich zumeist nicht ergeben. Folglich stehen schutzwürdige Betriebs- und Geschäftsgeheimnisse einem Informationszugang in der Regel nicht entgegen.

Ansprüche auf Informationszugang sind unverzüglich, spätestens jedoch innerhalb der in den Informationszugangsgesetzen des Bundes bzw. der Länder genannten Fristen zu erfüllen. Eine Entscheidung darf nicht auf Gremiensitzungen verschoben, sondern sollte im Rahmen der regulären Geschäftsführung getroffen werden. Im Übrigen sind transparenzpflichtige Informationen der berufsständischen Kammern in den bereits vorhandenen Informationsregistern zu veröffentlichen.

Die Informationsfreiheitsbeauftragten in Deutschland fordern daher die berufsständischen Kammern auf, ihren Transparenzverpflichtungen nachzukommen.

3.3 29. Konferenz der Informationsfreiheitsbeauftragten am 9. Dezember 2014 in Hamburg

3.3.1 Mehr Transparenz bei technischen Ermittlungsmethoden – Vertrauen in den Rechtsstaat stärken!

In den vergangenen Jahren wurden die Ermittlungsbefugnisse für Polizeien, Strafverfolgungsbehörden und Nachrichtendienste kontinuierlich ausgeweitet. Ihnen steht ein beträchtliches Instrumentarium unterschiedlich eingriffsintensiver technischer Maßnahmen zur Verfügung, wie zum Beispiel Funkzellenabfragen, Einsatz von IMSI-Catchern, Telekommunikationsüberwachung und Verkehrsdatenerhebung. Im Rahmen der Erweiterung wurden in die Landespolizeigesetze und die Strafprozessordnung Berichterstattungspflichten aufgenommen. Dadurch sollte garantiert werden, dass die Gesellschaft sich der Auswirkungen dieser neuen Maßnahmen bewusst ist.

Eine kritische Überprüfung der Berichtspflichten zeigt, dass eine Transparenz der Auswirkungen solcher Ermittlungsmaßnahmen nicht erreicht wird. Die Berichterstattungspflichten sind nicht nur uneinheitlich geregelt: Zum Teil fehlen für einige Maßnahmen wie zum Beispiel die Bestandsdatenabfrage Berichtspflichten vollständig, zum Teil lassen die bestehenden Berichtspflichten keine hinlänglichen Erkenntnisse über das Ausmaß der Überwachung und insbesondere die Zahl der Betroffenen zu. Die Berichte über Funkzellenabfragen zu Strafverfolgungszwecken lassen etwa nicht erkennen, dass von einer einzelnen gerichtlichen Anordnung tausende Bürgerinnen und Bürger

betroffen sein können, die keinen Anlass für die Erhebung ihrer Daten gegeben haben. Das Bundesverfassungsgericht verlangt in seinem Urteil zur Vorratsdatenspeicherung aber gerade, dass der Gesetzgeber eine „Überwachungsgesamtrechnung“ betreibt und beim Erlass neuer Überwachungsregelungen berücksichtigt. Nur so könne verhindert werden, dass die Freiheitswahrnehmung der Bürger total erfasst und registriert wird, denn dies verstieße gegen die verfassungsrechtliche Identität Deutschlands. Deshalb ist es jedenfalls erforderlich, nicht nur die theoretisch bestehenden, vom Gesetz erlaubten Überwachungsmöglichkeiten in den Blick zu nehmen, sondern gerade auch das konkrete Ausmaß ihres Einsatzes sichtbar zu machen.

Auf der Grundlage der gegenwärtig veröffentlichten Statistiken und zum Teil schmalen Berichtspflichten ist es nicht möglich, die gesamtgesellschaftlichen Auswirkungen aller Maßnahmen differenziert zu erfassen. Die Konferenz der Informationsfreiheitsbeauftragten fordert die Gesetzgeber in Bund und Ländern daher auf, die bestehenden Verpflichtungen zur Erstellung und Veröffentlichung von Statistiken auf alle Maßnahmen im Rahmen verdeckter Ermittlungsmethoden auszudehnen und sie durch die Angabe der Anzahl der Betroffenen so aussagekräftig zu gestalten, dass sich der Effekt auf die Bevölkerung klar erkennen lässt.

Darüber hinaus muss eine gesetzliche Veröffentlichungspflicht für die Berichte der Bundesnetzagentur zur Bestandsdatenabfrage festgeschrieben werden.

Eine besondere Bedeutung kommt der Transparenz der Nachrichtendienste zu. Erforderlich ist die Verschärfung bestehender bzw. Schaffung neuer Berichtspflichten gegenüber parlamentarischen Kontrollgremien und Datenschutzbeauftragten und die Verpflichtung zur Aufnahme aussagekräftiger statistischer Angaben zu Überwachungsmaßnahmen in die Verfassungsschutzberichte von Bund und Ländern. Geboten ist insbesondere eine Berichterstattung für den gesamten Bereich der strategischen Auslands-Telekommunikationsüberwachung.

Die Transparenz beim Einsatz staatlicher, insbesondere geheimer Ermittlungsmethoden ist neben den datenschutzrechtlichen Anforderungen eine wesentliche Voraussetzung für eine effiziente demokratische Kontrolle sowie die Beurteilung der Angemessenheit des staatlichen Eingriffshandelns und damit eine unabdingbare Wissensgrundlage für das Vertrauen der Bürgerinnen und Bürger in ihren Rechtsstaat.

3.3.2 Umfassende und effektive Informationsfreiheitsaufsicht unabdingbar!

Mit den Informationsfreiheitsgesetzen des Bundes und der Länder wurde der Bundes- bzw. den Landesbeauftragten für Informationsfreiheit die Aufgabe eines „außergerichtlichen Streitschlichters“ im Bereich des allgemeinen Informationsfreiheitsrechts übertragen. Sie kontrollieren die Anwendung der Informationsfreiheitsgesetze, vermitteln in Streitfällen und wirken auf die Einhaltung des geltenden Rechts hin. Im Bund sowie in den meisten Bundesländern verfügen die Informationsfreiheitsbeauftragten jedoch nur über eine eingeschränkte Kontroll- und Beratungskompetenz. Sie überwachen nur die Einhaltung des allgemeinen Informationsfreiheitsrechts, nicht jedoch der besonderen Informationszugangsrechte, wie z. B. nach dem Umwelt- oder dem Verbraucherinformationsrecht.

Diese Situation ist unbefriedigend. Bürgerinnen und Bürger erwarten, dass ihr Informationsanliegen von den Informationsfreiheitsbeauftragten umfassend geprüft wird. Mangels umfassender Kontroll- und Beratungszuständigkeit ist dies jedoch zu häufig nicht der Fall, sodass es im Umwelt- und im Verbraucherinformationsrecht an einer unabhängigen Aufsichtsbehörde fehlt.

Auch die wissenschaftlichen Evaluierungsberichte zum Informationsfreiheitsgesetz des Bundes und einiger Länder haben sich dafür ausgesprochen, den Informationsfreiheitsbeauftragten zusätzlich die Kontrollkompetenzen für das besondere Informationsfreiheitsrecht zu übertragen. Im Bereich des Datenschutzes sind die Beauftragten bereits für das besondere Datenschutzrecht zuständig. Dieser Standard muss auch in der Informationsfreiheit hergestellt werden.

Die Konferenz der Informationsfreiheitsbeauftragten fordert daher die Gesetzgeber in Bund und Ländern auf, die Kontroll- und Beratungskompetenzen der Informationsfreiheits-beauftragten um das Umwelt- und das Verbraucherinformationsrecht – wo dies noch nicht geschehen ist – zu erweitern und die Informationsfreiheitsbeauftragten mit ausreichenden personellen und sachlichen Mitteln auszustatten, damit sie ihren gesetzlichen Kontroll- und Beratungsaufgaben nachkommen können. Nur so ist gesichert, dass Bürgerinnen und Bürger bei der Ausübung ihrer Informationsrechte umfassend beraten werden und die Einhaltung der verschiedenen Informationsgesetze unabhängig kontrolliert wird.

3.3.3 Open Data muss in Deutschland Standard werden!

Die Bundesregierung hat mit der Digitalen Agenda 2014 – 2017, der Digitalen Verwaltung 2020 und dem nationalen Aktionsplan zur Umsetzung der G8 Open-Data-Charta wesentliche Regierungsprogramme zur Etablierung von E- und Open-Government sowie zur Digitalisierung der Verwaltung auf den Weg gebracht. Die Regierungsprogramme sehen aus informationsfreiheitsrechtlicher Sicht u.a. die Einführung einer gesetzlichen Open-Data-Regelung, die Schaffung von Open-Data-Ansprechpartnern in den Behörden, die Einführung der elektronischen Verwaltungsakte und eine verstärkte Zusammenarbeit mit den Ländern vor.

Die Konferenz der Informationsfreiheitsbeauftragten betont in diesem Zusammenhang das Erfordernis weitgehender gesetzlicher Veröffentlichungspflichten und die Übertragung der Aufgabe des Open-Data-Ansprechpartners auf behördliche Informationsfreiheitsbeauftragte.

Insbesondere bei Planung und Einführung der eAkte sind Aspekte der Informationsfreiheit und des Datenschutzes frühestmöglich im Anforderungskatalog abzubilden. Schon bei Anlage einer Akte sollten personenbezogene Daten, Betriebs- und Geschäftsgeheimnisse und sonstige Beschränkungen vor einer weiteren Verwendung markiert werden, so dass sie automatisiert ersetzt oder hervorgehoben werden können. Dies erleichtert eine nachfolgende Weitergabe und Weiterverwendung erheblich und unterstützt die aktenführenden Stellen bei der effizienten Bearbeitung von IFG-Anträgen.

Es gilt jetzt, die Regierungsprogramme zügig in die Tat umzusetzen, damit Open Data in Deutschland zum Standard werden kann. Die Konferenz fordert die Länder und den Bund auf, soweit noch nicht geschehen, mit dieser Zielsetzung E- und Open-Government-Strategien gemeinsam zu entwickeln.

3.4 28. Konferenz der Informationsfreiheitsbeauftragten am 17. Juni 2014 in Hamburg

3.4.1 Das Urheberrecht dient nicht der Geheimhaltung!

Die Konferenz der Informationsfreiheitsbeauftragten in Deutschland betrachtet mit Sorge die Entwicklung, dass sich auskunftspflichtige Stellen zur Ablehnung von Anfragen auf das Urheberrecht oder andere Rechte des „Geistigen Eigentums“ berufen. Das Urheberrecht darf nicht dazu eingesetzt werden, staatliche Informationen zurück zu halten.

Amtliche Vermerke sind in aller Regel nicht urheberrechtlich geschützt. Gedankliche Inhalte können in ihrer politischen, wirtschaftlichen oder gesellschaftlichen Aussage nicht über das Urheberrecht monopolisiert werden,

sondern müssen vielmehr Gegenstand der freien geistigen Auseinandersetzung bleiben. Mit Steuermitteln finanzierte und für die Erfüllung einer öffentlichen Aufgabe erstellte Vermerke dürfen nicht unter Berufung auf Rechte des „Geistigen Eigentums“ zurückgehalten werden. Hintergrund insbesondere des urheberrechtlichen Schutzes ist die Garantie einer angemessenen Vergütung der Urheber. Diese ist aber nicht bedroht, wenn Werke betroffen sind, die in Erfüllung dienstlicher Pflichten erstellt wurden.

Nur in Ausnahmefällen kann es sein, dass von Dritten für staatliche Stellen erstellte Gutachten tatsächlich dem Urheberrecht unterfallen und die Dritten schutzbedürftig sind. Wer mit der Verwaltung Verträge schließt, muss wissen, dass diese an gesetzliche Transparenzpflichten gebunden ist, die sich nicht abbedingen lassen. Wo dies nicht bereits gesetzlich vorgeschrieben ist, sollen sich die staatlichen Stellen in solchen Fällen das Recht an einer Herausgabe einräumen lassen. Soweit diese Stellen einem Informationsfreiheitsgesetz unterliegen, ist es ihre Pflicht, dafür Sorge zu tragen, dass Rechte Dritter nicht einem gesetzlichen Informationszugang entgegenstehen. Was mit staatlichen Mitteln für die Verwaltung von staatlichen Stellen oder Dritten hergestellt wird, muss grundsätzlich zugänglich sein.

3.4.2 Keine Flucht vor der Informationsfreiheit ins Privatrecht!

Es ist für weite Bereiche der Rechtsordnung anerkannt, dass der Staat sich nicht durch Wahl einer privaten Rechtsform seiner verfassungsrechtlichen Bindungen entledigen kann. Für das Recht aller Bürgerinnen und Bürger, sich voraussetzungslos über staatliches oder kommunales Handeln zu informieren, gilt dies leider nicht in gleichem Maße. Entscheidet sich der Staat für eine formale Privatisierung und erledigt eine öffentliche Aufgabe durch eine juristische Person des Privatrechts, so ist diese nach vielen Informationsfreiheitsgesetzen nicht direkt auskunftsverpflichtet. Informationszugang muss für alle Unterlagen gelten, die im Zusammenhang mit der Erfüllung öffentlicher Aufgaben stehen. Dabei darf es nicht darauf ankommen, ob die Aufgaben durch Behörden oder durch Private, an denen die öffentliche Hand mehrheitlich beteiligt ist, wahrgenommen werden. Ebenso wenig kommt es auf die Rechtsform an, in der jeweils gehandelt wird.

Da häufig gerade die Bereiche privatisiert werden, die über große Finanzvolumina verfügen, ist hier die Herstellung von Transparenz hinsichtlich der Verwendung öffentlicher Steuermittel besonders wichtig. Bereits 2003 hatten die Informationsfreiheitsbeauftragten die Gesetzgeber im Bund und in den Ländern dazu aufgerufen, die Herstellung von Transparenz nicht davon abhängig zu machen, in welcher Form die öffentliche Aufgabe erledigt wird. Leider ist diese Forderung längst nicht überall umgesetzt worden. Es gilt weiterhin: Für die Auskunftsverpflichtung sollte allein entscheidend sein, ob es sich um eine staatliche oder kommunale Aufgabe, insbesondere eine der

Grundversorgung handelt. Bei der Erfüllung öffentlicher Aufgaben müssen Ansprüche auf Auskunft auch direkt gegenüber den Unternehmen geschaffen werden.

Die Anwendung der Informationsfreiheitsgesetze darf nicht von der Rechtsform abhängen, in der öffentliche Aufgaben erledigt werden. Eine Flucht vor der Informationsfreiheit in das Privatrecht ist mit einem modernen Staatsverständnis nicht zu vereinbaren.

3.4.3 Informationsfreiheit nicht Privaten überlassen!

Öffentliche Stellen vertreten vielfach die Auffassung, staatliche Transparenz könne durch die Bereitstellung amtlicher Informationen auf von Privaten nach deren Regularien betriebenen Plattformen wie Facebook, Twitter etc. hergestellt werden. Auch wenn derartige Internetdiensteanbieter einen großen Nutzerkreis erreichen, stehen kommerzielle Interessen der Betreiber vielfach einem bedingungslosen und freien Informationszugang entgegen.

Öffentlichkeit ist gekennzeichnet durch voraussetzungslose, für ausnahmslos alle Menschen bestehende Zugangsmöglichkeiten. Sie kann deshalb nicht durch die Bereitstellung von Inhalten auf Internetseiten und -diensten hergestellt werden, die zum Beispiel ausschließlich durch allgemeine Geschäftsbedingungen Privater geregelt sind, nur Mitgliedern offen stehen oder keinen unbeobachteten Zugang gewähren. Staatliche Transparenz darf nicht durch die Offenbarung personenbezogener Daten erkauft werden.

Nur die Veröffentlichung auf von öffentlichen Stellen steuerbaren und der Allgemeinheit kostenfrei und anonym zugänglichen Kanälen genügt den Anforderungen der Herstellung staatlicher Transparenz. Die Konferenz der Informationsfreiheitsbeauftragten fordert, die Veröffentlichung amtlicher Informationen auf ausschließlich von den öffentlichen Stellen selbst gesteuerten Veröffentlichungsmedien vorzunehmen. Eine Steuerung und Kontrolle in diesem Sinne kann beispielsweise auch durch Einzelverträge mit Privaten geschehen. Der im Hamburger Transparenzgesetz formulierte Grundsatz, wonach der Zugang zum Informationsregister kostenlos und anonym ist, sollte in alle Informationsfreiheits- und Transparenzgesetze aufgenommen werden.

4 Abkürzungsverzeichnis

Abs.	=	Absatz
AIG	=	Akteneinsichts- und Informationszugangsgesetz
AOK	=	Allgemeine Ortskrankenkasse
App	=	Applikation (Anwendungssoftware) für mobile Endgeräte
Art.	=	Artikel
ATD	=	Antiterrordatei
ATDG	=	Antiterrordateigesetz
BbgDSG	=	Brandenburgisches Datenschutzgesetz
BbgKVerf	=	Kommunalverfassung des Landes Brandenburg
BbgSchulG	=	Brandenburgisches Schulgesetz
BbgStatG	=	Brandenburgisches Statistikgesetz
BCR	=	Binding Corporate Rules
BDSG	=	Bundesdatenschutzgesetz
BEM	=	Betriebliches Eingliederungsmanagement
BGB	=	Bürgerliches Gesetzbuch
BGBl.	=	Bundesgesetzblatt
BSI	=	Bundesamt für Sicherheit in der Informationstechnik
BStatG	=	Bundesstatistikgesetz
bzgl.	=	bezüglich
bzw.	=	beziehungsweise
CERT	=	Computer Emergency Response Team
DDR	=	Deutsche Demokratische Republik
d. h.	=	das heißt
DSV	=	Datenschutzverordnung Schulwesen
DV	=	Datenverarbeitung
DViA	=	Datenverarbeitung im Auftrag
EDV	=	Elektronische Datenverarbeitung
eID	=	elektronische Identität
EU	=	Europäische Union
e. V.	=	eingetragener Verein

EWR	=	Europäischer Wirtschaftsraum
FeV	=	Fahrerlaubnis-Verordnung
ff.	=	folgende (Seiten)
gematik	=	Gesellschaft für Telematikanwendungen der Gesundheitskarte GmbH
ggf.	=	gegebenenfalls
GIW	=	Geoinformationswirtschaft
GKDZ	=	Gemeinsames Kompetenz- und Dienstleistungszentrum auf den Gebiet der Telekommunikationsüberwachung
GmbH	=	Gesellschaft mit beschränkter Haftung
GPG4Win	=	Privacy Guard for Windows
GVBl.	=	Gesetz- und Verordnungsblatt
HbbTV	=	Hybrid Broadcast Broadband Television
IaaS	=	Infrastructure as a Service
IMEI	=	International Mobile Equipment Identity
IMSI	=	International Mobile Subscriber Identity
inkl.	=	inklusive
INSPIRE	=	Infrastructure for Spatial Information in Europe
IP	=	Internet Protokoll
ISMS	=	Informationssicherheitsmanagementsystem
ISO	=	International Organization for Standardization
IT	=	Informationstechnik
i. V. m.	=	in Verbindung mit
JI-Richtlinie	=	Datenschutz-Richtlinie im Bereich von Justiz und Inneres
KESY	=	Kennzeichenerfassungssystem
Kita	=	Kindertagesstätte
LAufnG	=	Landesaufnahmegesetz
LDAP	=	Lightweight Directory Access Protocol
LDG	=	Landesdisziplinargesetz
LISUM	=	Landesinstitut für Schule und Medien Berlin-Brandenburg
MPU	=	Medizinisch-Psychologische Untersuchung

NADIS	=	Nachrichtendienstliches Informationssystem
Nr.	=	Nummer
NSA	=	National Security Agency
o. g.	=	oben genannt
OWiG	=	Ordnungswidrigkeitengesetz
PaaS	=	Platform as a Service
PGP	=	Pretty Good Privacy
PC	=	Personal Computer
PIN	=	persönliche Identifikationsnummer
RED	=	Rechtsextremismus-Datei
REDG	=	Rechtsextremismus-Datei-Gesetz
RFID	=	Radio Frequency Identification
RIO	=	Ressort Information Officer
SaaS	=	Software as a Service
SGB I	=	Erstes Buch Sozialgesetzbuch
SGB V	=	Fünftes Buch Sozialgesetzbuch
SGB X	=	Zehntes Buch Sozialgesetzbuch
StGB	=	Strafgesetzbuch
StPO	=	Strafprozessordnung
StVG	=	Straßenverkehrsgesetz
TKG	=	Telekommunikationsgesetz
TKÜ	=	Telekommunikationsüberwachung
TMG	=	Telemediengesetz
TTIP	=	Transatlantic Trade and Investment Partnership
URL	=	Uniform Resource Locator
USB	=	Universal Serial Bus
VV-Schulbetrieb	=	Verwaltungsvorschriften über die Organisation der Schulen in inneren und äußeren Schulangelegenheiten
WLAN	=	Wireless Local Area Network
z. B.	=	zum Beispiel
ZIT-BB	=	Brandenburgischer IT-Dienstleister
ZPO	=	Zivilprozessordnung