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

LAND BRANDENBURG

LDA

Schutz der
- *Persönlichkeitsrechte*
- *Informationsfreiheit*

Tätigkeitsbericht 2016/2017

- 19. Tätigkeitsbericht -

Tätigkeitsbericht

der Landesbeauftragten für den Datenschutz

und für das Recht auf Akteneinsicht

zum 31. Dezember 2017

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 12. April 2016 vorgelegten Tätigkeitsbericht 2014/2015 an und deckt den Zeitraum vom 1. Januar 2016 bis zum 31. Dezember 2017 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

Am 27. April 2016 verabschiedeten das Europäische Parlament und der Rat der Europäischen Union die Verordnung zum Schutz natürlicher Personen für die Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung). Nach über vierjährigen Verhandlungen wurde damit in der gesamten Europäischen Union ein einheitliches, unmittelbar geltendes Datenschutzrecht vereinbart. Die Verordnung trat im Mai 2016 in Kraft und wird am 25. Mai 2018 in ganz Europa wirksam werden und damit zur Anwendung kommen. Die Berichtsjahre 2016 und 2017 waren insofern bei Unternehmen, Verwaltungen und Aufsichtsbehörden sowie den nationalen Gesetzgebern geprägt durch die notwendigen Vorbereitungen für die Anwendung der Verordnung.

Die Grundverordnung setzt einen wichtigen Impuls für einen hohen Standard im Datenschutz. Mit ihr wurde nicht nur eine Grundlage für einen besseren, einheitlichen grenzüberschreitenden Datenschutz geschaffen. Schon heute ist zu sehen, dass die ersten international agierenden Unternehmen europäische Datenschutzanforderungen als Vorbild nutzen und ihre gesamte, weltweite Geschäftstätigkeit daran ausrichten.

Wir erleben zurzeit einen Umbruch, wie es ihn seit der industriellen Revolution nicht mehr gegeben hat. Das Thema Digitalisierung stellt sowohl für Behörden als auch für die Wirtschaft eine große Herausforderung dar. Bei vielen diesbezüglichen Projekten fallen personenbezogene Daten an, deren Verknüpfungsmöglichkeiten nicht nur ungeahnte neue Möglichkeiten für die Datennutzung schaffen. Unternehmen eröffnen sich auch neue Geschäftsfelder, die z. B. mit der Auswertung des Verhaltens oder der Wünsche der Kunden einhergehen, um personalisierte Dienstleistungen erbringen zu können. Seit einiger Zeit wird deshalb die Frage des Eigentums an personenbezogenen Daten verstärkt diskutiert. Wem gehören unsere personenbezogenen Daten? Werden sie Eigentum eines Unternehmens, weil dieses sie für seine Zwecke nutzt und die Daten den Wert des Unternehmens ausmachen? Neue Begriffe werden geprägt wie zum Beispiel der Begriff der „Datensouveränität.“ Brauchen wir neben den Regelungen der Datenschutz-Grundverordnung schon wieder eine Diskussion über die Rechte der Betroffenen, um deren Daten es geht? Ich bin der Auffassung, dass die Entwicklung zukunftsfähiger Lösungen im Rahmen des digitalen Fortschritts immer eng mit dem Schutz der Betroffenen und ihrer Rechte verbunden sein muss. Die neuen Chancen, die mit der Digitalisierung unzweifelhaft einhergehen, dürfen nur unter Wahrung der Persönlichkeitsrechte jedes Einzelnen genutzt werden.

Eine zentrale Bedeutung für einen modernen Datenschutz kommt dem Grundsatz „Datenschutz durch Technikgestaltung“ zu. Jedes Projekt, in dem personenbezogene Daten verarbeitet werden, muss diesen von Anfang an beachten. Ich erlebe leider seit langem immer wieder, dass genau den damit verbundenen Fragen nicht genügend Aufmerksamkeit gewidmet wird. Wissen, Zeit und Geld spielen auch allgemein bei der Einhaltung der gesetzlichen Vorschriften zur Datensicherheit eine große Rolle. Und genau an diesen drei Faktoren fehlt es vielen Verantwortlichen zuweilen. Aber gerade die Gewährleistung der Sicherheit bei der Verarbeitung personenbezogener Daten, verbunden mit Datensparsamkeit, ist für das Vertrauen der Menschen in eine rechtskonforme Verarbeitung ihrer Daten von entscheidender Bedeutung. Dies gilt für staatliche Stellen genauso wie für Unternehmen. Allerdings stehen Behörden hier in einer besonderen Pflicht, da der Einzelne nicht die Freiheit hat, sich gegen eine Verarbeitung seiner Daten durch den Staat zu entscheiden, soweit diese auf einer gesetzlichen Grundlage beruht. Verletzungen des Datenschutzes durch Hackerangriffe haben in der Vergangenheit immer wieder deutlich gemacht, wie wichtig Datensicherheit für Datenschutz ist. Sie ist damit ein zentrales Thema, das auch in Zukunft aktuell bleiben wird.

Durch die steigende Gefahr terroristischer Angriffe wurde in den letzten beiden Jahren auch der Ruf nach mehr Befugnissen für die Sicherheitsbehörden erneut lauter. In Bund und Ländern wurden zahlreiche Sicherheitsgesetze novelliert und dem Staat weitreichende neue Befugnisse eingeräumt. Hierbei steht immer wieder das Spannungsverhältnis zwischen Freiheit und Sicherheit im Fokus. Der Staat muss seinen Bürgern beides zugleich gewährleisten. Bevor neue Eingriffe in die Freiheitsrechte der Bürger in Erwägung gezogen werden, bedarf es stets einer Analyse der bestehenden Regelungen. Wo haben diese nicht ausgereicht? Welche neuen Befugnisse sind tatsächlich erforderlich? Als Datenschutzbeauftragte unseres Landes wünsche ich mir vor der Schaffung neuer Eingriffsbefugnisse eine ergebnisoffene Prüfung, warum bestehende Befugnisse nicht ausgereicht oder versagt haben. Für die Bewertung der Verfassungsgemäßheit neuer Eingriffsbefugnisse muss stets der verfassungsrechtliche Grundsatz der Verhältnismäßigkeit mit den Fragen der Geeignetheit, Erforderlichkeit und Angemessenheit beachtet werden.

Liebe Leserinnen und Leser, mein Tätigkeitsbericht für die Jahre 2016 und 2017 zeigt Ihnen wieder einen bunten Strauß an Fällen, die meine Dienststelle sowohl im Bereich des Datenschutzes als auch im Bereich des Akteneinsichts- und Informationszugangsgesetzes bearbeitet hat. Zum Teil sind wir auf Behörden und Unternehmen gestoßen, die die gesetzlichen Regelungen vorbildlich einhalten. Zum Teil gab es Lücken oder klare Rechtsverstöße. In einigen Fällen konnten wir Verbesserungen erreichen – nicht immer jedoch in

dem Umfang und der Zeit, wie wir es uns vorgestellt haben. Ich wünsche Ihnen eine interessante Lektüre.

Kleinmachnow, den 18. April 2018

Dagmar Hartge

Teil A

Brennpunkte

1 Orientierung bei der Anwendung der Datenschutz-Grundverordnung

Muss mein Unternehmen einen betrieblichen Datenschutzbeauftragten benennen? Unter welchen Voraussetzungen ist eine Datenschutz-Folgenabschätzung notwendig? Was bedeutet Datenübertragbarkeit und was versteht man unter dem „Recht auf Vergessenwerden“? Welche Aufsichtsbehörde ist federführend und wann spricht man von grenzüberschreitender Datenverarbeitung? Diese und viele andere Fragen stellen sich im Zusammenhang mit der ab dem 25. Mai 2018 geltenden europäischen Datenschutz-Grundverordnung (DS-GVO).[1] Natürlich ergeben sich auch bei jedem anderen neu geschaffenen Gesetz Auslegungsfragen, die sich erst im Laufe der Zeit aufgrund der Praxis und mithilfe der Rechtsprechung klären lassen. Die Herausforderung im vorliegenden Fall besteht jedoch darin, dass hier ein EU-weiter Rechtsrahmen geschaffen worden ist, der von Aufsichtsbehörden aller Mitgliedstaaten übereinstimmend angewendet werden muss. Nur so lassen sich einheitliche Anforderungen für die Wirtschaft wie die öffentliche Hand schaffen und auch für die Bürger in der EU gleiche Bedingungen für ihre Datenschutzrechte garantieren. Im föderalen Deutschland ergibt sich als weitere Herausforderung, dass auch die 18 unabhängigen Aufsichtsbehörden des Bundes und der Länder sich auf eine möglichst gleichmäßige Anwendung der Verordnung verständigen, wobei sie zusätzlich die nationalen Regelungen, insbesondere das neue Bundesdatenschutzgesetz und die jeweiligen Landesdatenschutzgesetze zu berücksichtigen haben.

1.1 Leitlinien der Artikel-29-Datenschutzgruppe

Die Datenschutz-Grundverordnung sieht selbst verschiedene Verfahren und Instrumente vor, die dazu beitragen sollen, dass die Regelungen der Verordnung in allen Mitgliedstaaten möglichst einheitlich angewendet werden. Dazu gehört vor allem der Europäische Datenschutzausschuss, in dem jeder Mitgliedstaat mit dem Leiter einer seiner Datenschutzbehörden vertreten ist (Art. 68 DS-GVO). Der Ausschuss hat die Aufgabe, für eine einheitliche

[1] Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung), (ABl. EU L 119/1).

Anwendung der Grundverordnung zu sorgen. Ihm obliegt es beispielsweise, ihre ordnungsgemäße Anwendung in den Mitgliedstaaten zu überwachen, Meinungsverschiedenheiten zwischen Datenschutzbehörden zu schlichten und die Kommission zu beraten, einschließlich etwaiger Vorschläge zur Änderung der Verordnung. Der Europäische Datenschutzausschuss ist außerdem aufgefordert, zur Sicherstellung der einheitlichen Anwendung der Verordnung Leitlinien und Empfehlungen bereitzustellen. Allerdings konstituiert er sich erst mit dem Wirksamwerden der Datenschutz-Grundverordnung.

Um dennoch die zweijährige Übergangsphase bis zur Geltung der Verordnung zu nutzen und den Verantwortlichen frühzeitig Hilfestellungen an die Hand zu geben, hat es die Gruppe für den Schutz von Personen bei der Verarbeitung personenbezogener Daten (Artikel-29-Datenschutzgruppe) übernommen, erste Leitlinien zu entwickeln und nach Durchführung eines Anhörungsverfahrens zu veröffentlichen. Die Artikel-29-Datenschutzgruppe wurde auf der Grundlage des Artikels 29 der Datenschutzrichtlinie (Richtlinie 95/46/EG) errichtet. Sie setzt sich aus Vertretern der nationalen Datenschutzbehörden, des Europäischen Datenschutzbeauftragten und der Europäischen Kommission zusammen. Ihre Hauptaufgaben sind die Beratung der Europäischen Kommission in Datenschutzfragen und die Förderung einer einheitlichen Anwendung der Datenschutzrichtlinie in allen EU-Mitgliedstaaten. Sowohl in ihrer Zusammensetzung als auch in ihrer Aufgabenstellung ist sie mit dem zukünftigen Europäischen Datenschutzausschuss vergleichbar und daher berufen, im Vorgriff auf das Wirksamwerden der Datenschutz-Grundverordnung erste Auslegungshinweise zu geben.

Thematisch spezialisierte Untergruppen haben bereits verschiedene Empfehlungen und Stellungnahmen ausgearbeitet, die die Artikel-29-Datenschutzgruppe der Öffentlichkeit in Konsultationsverfahren präsentiert hat. Sie werden jeweils nach Durchführung der öffentlichen Anhörung und unter Berücksichtigung der eingegangenen Stellungnahmen abschließend von dem Gremium beschlossen und veröffentlicht. Diese sog. Guidelines bzw. Leitlinien befassen sich vertieft und umfassend mit einzelnen Bestimmungen der Grundverordnung, setzen sich mit unterschiedlichen Sachverhaltsvarianten auseinander und enthalten zumeist einen zusammenfassenden Annex mit Antworten auf „Häufig gestellte Fragen“.

Die bislang ausgearbeiteten Leitlinien haben beispielsweise das Recht auf Datenportabilität und die Datenschutz-Folgenabschätzung zum Gegenstand. Außerdem befassen sie sich mit der Frage, wie die federführende Aufsichtsbehörde zu bestimmen ist, und geben Hinweise zu den Datenschutzbeauftragten, die von den Verantwortlichen zu benennen sind, sowie zur Anwendung der Bußgeldvorschriften. Weitere Leitlinien, etwa zum Grundsatz der Transparenz, zur Einwilligung und zum Profiling, werden derzeit erarbeitet oder liegen bereits der Öffentlichkeit zur Anhörung vor.

1.2 Kurzpapiere der deutschen Aufsichtsbehörden

Da die Leitlinien der Artikel-29-Datenschutzgruppe und zukünftig des Europäische Datenschutzausschuss in einem ausgesprochen zeitaufwendigen Verfahren erarbeitet werden müssen, hat sich die Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder darauf verständigt, eigene Auslegungshinweise zur Datenschutz-Grundverordnung, sog. Kurzpapiere, untereinander abzustimmen und zu veröffentlichen. Sie stehen unter dem ausdrücklichen Vorbehalt einer zukünftigen – möglicherweise abweichenden – Auslegung durch den Ausschuss und sollen als erste Orientierung insbesondere für den nicht öffentlichen Bereich dienen. Den Kurzpapieren ist zu entnehmen, wie nach Auffassung der Konferenz die Verordnung in der Praxis angewendet werden sollte.

Die inzwischen vorliegenden Kurzpapiere geben Hinweise zu höchst unterschiedlichen Regelungsbereichen der Datenschutz-Grundverordnung, wie beispielsweise dem Verzeichnis von Verarbeitungstätigkeiten, der Verarbeitung personenbezogener Daten für Werbung, dem Auskunftsrecht der Betroffenen, der Auftragsverarbeitung und der Videoüberwachung. Ein weiteres Kurzpapier gibt den Unternehmen zudem einen sog. Maßnahmenplan an die Hand, der die erforderlichen Schritte auflistet, denen die Geschäftsleitungen folgen sollten, um ihre Unternehmen fit für das neue Datenschutzrecht zu machen.

Auch wenn sich die Kurzpapiere in erster Linie an private Unternehmen richten, empfiehlt es sich auch für öffentliche Stellen, diese heranzuziehen, soweit für sie keine speziellen Vorschriften gelten. Gerade die technisch-organisatorischen Hinweise lassen sich überwiegend auch auf öffentliche Stellen übertragen. Gleiches gilt für den Maßnahmenplan.

Die Leitlinien der Artikel-29-Datenschutzgruppe und die Kurzpapiere der unabhängigen Datenschutzbehörden des Bundes und der Länder sind wichtige Beiträge zur einheitlichen Anwendung der Datenschutz-Grundverordnung. Es empfiehlt sich, in Zweifelsfällen auf diese Auslegungshilfen zurückzugreifen, da sie die aktuelle, unter den Aufsichtsbehörden der EU-Mitgliedstaaten bzw. unter den deutschen Aufsichtsbehörden abgestimmte Rechtsauffassung zur Anwendung der Verordnung wiedergeben.

2 Wichtige Neuerungen der Datenschutz-Grundverordnung

2.1 Dokumentations- und Nachweispflichten

Bewährte Grundprinzipien des Datenschutzes, wie sie seit vielen Jahren in Deutschland Gesetzeskraft haben, bleiben auch mit der Datenschutz-Grundverordnung (DS-GVO) bestehen. Allerdings werden die Anforderungen für Verantwortliche und Auftragsverarbeiter zur Dokumentation und zum Nachweis der Einhaltung dieser Prinzipien in Zukunft höher.

Die allgemeinen Grundsätze, die bei jeder Verarbeitung personenbezogener Daten einzuhalten sind, werden im Art. 5 Abs. 1 DS-GVO zusammengefasst. Verantwortliche (in bisheriger Terminologie: verantwortliche Stellen bzw. Daten verarbeitende Stellen) müssen insbesondere die Rechtmäßigkeit der Verarbeitung, die Transparenz gegenüber Betroffenen und die Zweckbindung gewährleisten. Sie sind weiter verpflichtet, Daten nur im unbedingt erforderlichen Umfang zu verarbeiten (Datenminimierung), die Rechte Betroffener z. B. auf Berichtigung oder Löschung ihrer Daten zu beachten sowie geeignete technische und organisatorische Maßnahmen für die Sicherheit der Datenverarbeitung umzusetzen. Gemäß Art. 5 Abs. 2 DS-GVO muss der Verantwortliche die Einhaltung dieser Anforderungen nachweisen können (Rechenschaftspflicht).

Die allgemeine Nachweispflicht wird für einige spezielle Fälle im weiteren Verlauf der Verordnung konkretisiert. So darf z. B. ein Auftragsverarbeiter personenbezogene Daten gemäß Art. 28 Abs. 3 DS-GVO nur auf dokumentierte Weisung des Verantwortlichen verarbeiten, müssen Verantwortlicher und Auftragsverarbeiter gemäß Art. 30 DS-GVO schriftliche Verzeichnisse der Verarbeitungstätigkeiten führen oder sind Datenschutzverletzungen gemäß Art. 33 Abs. 5 DS-GVO durch den Verantwortlichen zu dokumentieren. Auch muss der Verantwortliche die Einwilligung Betroffener nachweisen können, falls die Datenverarbeitung darauf beruht (Art. 7 Abs. 1 DS-GVO).

Dem Nachweis der Einhaltung der Verordnung dient auch ein Sicherheitskonzept, in dem der Verantwortliche (ggf. gemeinsam mit dem Auftragsverarbeiter) die technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Datenverarbeitung beschreibt und deren Umsetzung dokumentiert. Hierbei sind gemäß Art. 24 und 32 DS-GVO die Art, der Umfang, die Umstände und die Zwecke der Datenverarbeitung, die Risiken für die Rechte und Freiheiten Betroffener, der Stand der Technik und die Implementierungskosten für die Maßnahmen zu berücksichtigen. Ziel ist, ein dem Risiko angemessenes Schutzniveau bei der Datenverarbeitung zu erreichen. Ein Sicherheitskonzept sollte stets in schriftlicher (oder elektronischer) Form vorliegen, damit es nachvollziehbar ist, seine Rechenschaftsfunktion erfüllen

und von der Aufsichtsbehörde geprüft werden kann. Gleiches gilt auch für die Datenschutz-Folgenabschätzung gemäß Art. 35 DS-GVO.[2]

Darüber hinaus ist zu empfehlen, dass der Verantwortliche (und ggf. der Auftragsverarbeiter) seine Aktivitäten zur Einhaltung der Datenschutz-Grundverordnung durch die Beschreibung des internen Datenschutzmanagements dokumentiert. Dies betrifft sowohl aufbau- als auch ablauforganisatorische Aspekte. Zu Ersteren gehören z. B. Festlegungen zu Rollen und Verantwortlichkeiten, zu internen Beratungs-, Entscheidungs-, Umsetzungs- und Kontrollstrukturen bei Datenschutzfragen oder zur Stellung des behördlichen bzw. betrieblichen Datenschutzbeauftragten. Bei der Ablauforganisation ist insbesondere an die Planung, Beschreibung und Kontrolle interner Prozesse zur Umsetzung der Datenschutz-Grundverordnung zu denken. Dabei sind einheitliche, behörden- bzw. unternehmensweite Vorgaben zu treffen, in denen das Vorgehen z. B. zur Erfüllung von Informations- und Transparenzpflichten, zur Bearbeitung von Auskunfts-, Berichtigungs- oder Löschanfragen Betroffener, zum Umgang mit Beschwerden oder zur Abgabe von Meldungen bei Datenschutzverletzungen festgelegt wird. Auch Maßnahmen zur Sensibilisierung und Schulung der Beschäftigten in Datenschutzfragen gehören in diesen Bereich.

Je nach Behörden- bzw. Unternehmensgröße sowie den internen Strukturen kann die Beschreibung des Datenschutzmanagements verschieden umfangreich und komplex sein. Im Regelfall wird sie sich z. B. in Datenschutzleitlinien, Richtlinien, Betriebs- und Organisationsanweisungen, vorgegebenen und standardisierten Prozessabläufen, Schulungsunterlagen u. Ä. manifestieren.

Die Erfüllung der Rechenschaftspflichten der Datenschutz-Grundverordnung sollte nicht auf die leichte Schulter genommen werden. Datenschutzaufsichtsbehörden werden sich von Verantwortlichen oder Auftragsverarbeitern oftmals zunächst Unterlagen zur allgemeinen Datenschutzorganisation in der Behörde oder im Unternehmen bzw. Dokumentationen für konkrete Datenverarbeitungsprozesse vorlegen lassen, bevor sie detailliertere Prüfungen beginnen. Bei nicht vorhandenen oder lückenhaften Beschreibungen können sie von ihren Abhilfebefugnissen Gebrauch machen (wie Warnung, Verwarnung, Weisung, Untersagung) oder ggf. eine Geldbuße verhängen.

2.2 Die Einwilligungserklärung

Mit Geltung der Datenschutz-Grundverordnung (DS-GVO) unterliegt auch die Einwilligung als eine mögliche Voraussetzung für die Rechtmäßigkeit der Verarbeitung personenbezogener Daten teilweise neuen An-

[2] Siehe A 2.5.

forderungen. Sie ist als einer der bedeutsamsten, da weitreichendsten Erlaubnistatbestände ausgestaltet. An ihre Wirksamkeit sind daher strenge Anforderungen zu stellen.

Was unter einer Einwilligung der betroffenen Person zu verstehen ist, regelt Art. 4 Nr. 11 DS-GVO. Hiernach ist jede freiwillig für den bestimmten Fall, in informierter Weise und unmissverständlich abgegebene Willensbekundung in Form einer Erklärung oder einer sonstigen eindeutigen bestätigenden Handlung, mit der die betroffene Person zu verstehen gibt, dass sie mit der Verarbeitung der sie betreffenden personenbezogenen Daten einverstanden ist, als Einwilligung zu qualifizieren.

Aus dieser Formulierung folgt bereits, dass die Datenschutz-Grundverordnung, anders als das bislang geltende Bundesdatenschutzgesetz, nicht mehr grundsätzlich die Schriftform erfordert. Damit sind neben eigenhändig unterschriebenen, schriftlichen Erklärungen auch mündliche Einwilligungen oder Einwilligungen etwa durch das Markieren eines Auswahlfeldes oder per E-Mail möglich. Da der Verantwortliche aber zugleich einer weitreichenden Rechenschaftspflicht[3] unterliegt und im Einzelfall nachweisen muss, dass die Verarbeitung rechtmäßig erfolgt, wird sich wohl auch zukünftig die Einholung einer schriftlichen Einwilligung oder einer protokollierten elektronischen Einwilligung als bevorzugte Lösung etablieren, um dieser Nachweispflicht genügen zu können.

Hervorzuheben ist an dieser Stelle, dass eine Einwilligung nach ErwGr. 32 DS-GVO ebenso durch technische Voreinstellungen z. B. im Internetbrowser erteilt werden kann.

Der Verordnungstext zeigt aber auch, dass das Erfordernis einer aktiven und unmissverständlichen Willensbekundung einer Einwilligung durch Stillschweigen entgegensteht. Es reicht damit – anders als bisher – nicht mehr aus, dem Betroffenen lediglich die Möglichkeit zu geben, vorformulierte Einwilligungserklärungen zu streichen oder ein voreingestellt gesetztes Häkchen zu entfernen.

Die Einwilligung muss ferner freiwillig und in informierter Weise erfolgen. Die Mindestvorgaben für die Informiertheit erschöpfen sich in der Nennung des Verantwortlichen und in Angaben zu den Zwecken, denen die Datenverarbeitung dient. Soweit eine Verarbeitung mehreren Zwecken dient, ist auf jeden dieser Zwecke hinzuweisen. Gemäß Art. 7 Abs. 2 DS-GVO kann die Einwilligung auch Bestandteil einer längeren Erklärung sein, die sich auch auf noch andere Sachverhalte beziehen kann. Gemeint ist damit insbesondere, dass die Einwilligung auch Bestandteil von Allgemeinen Geschäftsbedingungen

[3] Siehe A 2.1.

sein kann. Dies verlangt aber, dass die Erklärung im Text deutlich hervorgehoben und verständlich formuliert ist.

Zu betonen ist, dass in der bisherigen Praxis häufig zu allgemein gefasste „Datenschutzerklärungen“ zur Erteilung von Einwilligungen genutzt werden, aus denen weder hervorgeht, dass der Betroffene überhaupt eine eigene Erklärung abgeben soll noch worauf diese sich konkret bezieht. In diesen Fällen wird es daher mangels Verständlichkeit häufig an der erforderlichen Informiertheit der betroffenen Person fehlen, sodass keine wirksame Einwilligung vorliegt. Außerdem werden nach unserer Erfahrung vielfach Einwilligungen für Verarbeitungsschritte eingeholt, die bereits von Gesetzes wegen erlaubt sind und daher keiner Einwilligung bedürfen.

Aus dem Erfordernis der Freiwilligkeit folgt, dass die Einwilligung auf dem uneingeschränkten freien Willen der betroffenen Person beruhen muss. Im Zusammenhang mit Verträgen führt die Datenschutz-Grundverordnung daher ein allgemeines Kopplungsverbot ein. Wird die Erteilung der Einwilligung zur Vorbedingung für den Abschluss eines Schuldverhältnisses gemacht („friss oder stirb“), wäre die Einwilligung jedenfalls dann unwirksam, wenn durch sie auch Datenverarbeitungen, die über das für die Vertragserfüllung Erforderliche hinausgehen, legitimiert werden sollen. Ebenso soll eine Einwilligung als Erlaubnistatbestand ausscheiden, wenn zwischen dem Betroffenen und dem Verantwortlichen ein klares Ungleichgewicht besteht. Dies dürfte insbesondere im Zusammenhang mit Beschäftigtenverhältnissen relevant sein.

Hieran zeigt sich, dass insbesondere „Dienstleistung gegen Daten“-Geschäftsmodelle oder Vertragsschlüsse, die an Datenverarbeitungen gekoppelt werden, die mit der eigentlichen Erbringung der Leistung nicht in Zusammenhang stehen, zukünftig deutlich erschwert werden. Hier besteht stets die Gefahr unwirksamer Einwilligungen und damit gegebenenfalls rechtswidriger Datenverarbeitungen. Unternehmen kann nur geraten werden, die bestehenden Prozesse zu analysieren und zu prüfen, inwieweit die Datenverarbeitung auf Grundlage gesetzlicher Erlaubnisse in rechtmäßiger Weise umzustellen ist.

Wie auch bisher kann eine wirksam erteilte Einwilligung jederzeit widerrufen werden. Nach einem Widerruf kann die Datenverarbeitung nicht mehr auf die bisherige Einwilligung gestützt werden. Der Betroffene ist auf sein Widerspruchsrecht bereits vor Abgabe der Einwilligungserklärung hinzuweisen.

Soweit die Verarbeitung personenbezogener Daten von Kindern auf eine Einwilligung gestützt werden soll, enthält Art. 8 DS-GVO eine weitere Neuregelung. Die Norm verlangt für eine telemediengestützte Verarbeitung der Daten von Kindern bis zur Vollendung des 16. Lebensjahres die Einwilligung der Erziehungsberechtigten. Es ist nicht erforderlich, dass sich das Angebot

speziell an Kinder und Jugendliche richtet. Ausreichend ist vielmehr, dass das Angebot „auch“ einem Kind gemacht wird. Der verantwortliche Anbieter muss in diesen Fällen sicherstellen, dass die Identität der Erziehungsberechtigten und die Authentizität der Einwilligungserklärung festgestellt und gewährleistet werden kann. Hier eine praxistaugliche, zulässige Vorgehensweise zu entwickeln, stellt eine große Herausforderung dar.

Was für eine rechtswirksame Einwilligung gemäß Art. 8 DS-GVO nicht genügt, liegt auf der Hand: das bloße Anklicken eines Kästchens. Einigkeit besteht dagegen, dass das sog. Double-opt-in-Verfahren grundsätzlich einen sinnvollen Mechanismus darstellt. Allerdings sind auch hier die Missbrauchsrisiken nicht von der Hand zu weisen, etwa durch gefälschte E-Mail Adressen oder unmittelbare unberechtigte Nutzung des elterlichen Accounts durch die Kinder. In Betracht kommen darüber hinaus

- unterschriebene Dokumente,
- Telefon- oder Videokonferenzen,
- Abfrage von Kreditkartendaten zur Legitimation von Transaktionen.

Der notwendige Prüfungsgrad wird auch davon abhängen, wie sensitiv die jeweiligen Datenbestände sind.

Die bisher in großer Zahl in Unternehmen vorhandenen Einwilligungen als Grundlage für die Datenverarbeitung sollen nach ErwGr. 171 DS-GVO grundsätzlich auch weiterhin Bestand haben, soweit sie der Art nach bereits den Bedingungen der Datenschutz-Grundverordnung entsprechen.

Auch zukünftig wird die Einwilligung eine der wesentlichen Rechtmäßigkeitsvoraussetzungen für die Verarbeitung personenbezogener Daten darstellen. Da an ihre Wirksamkeit jedoch strenge Anforderungen zu stellen sind, sollten Unternehmen ihre bestehenden Prozesse und Verfahren analysieren. Alte Einwilligungen sollten ebenso auf den Prüfstand gestellt und gegebenenfalls aktualisiert werden. Bei neuen Einwilligungen ist auf die Einhaltung der rechtlichen Anforderungen genau zu achten.

2.3 Informations- und Transparenzpflichten

Unter den Rechten der betroffenen Person versteht die Datenschutz-Grundverordnung (DS-GVO) die Rechte des Einzelnen gegenüber dem für die Verarbeitung Verantwortlichen. Diese Rechte lassen sich grundsätzlich nach zwei Kategorien unterscheiden: solche, die einen entsprechenden Antrag oder ein Ersuchen der betroffenen Person voraussetzen, und solche, die sich an den Verantwortlichen richten und ihn ver-

pflichten, proaktiv umfassende Informationen zu der Datenverarbeitung zur Verfügung zu stellen.

Die Informationspflichten finden sich in Art. 12, 13, 14 und 19 DS-GVO. Art. 12 enthält allgemeine Grundlagen und Anforderungen an eine transparente Information und Kommunikation zwischen Betroffenen und Verantwortlichen. Die Art. 13 und 14 regeln konkrete Transparenzverpflichtungen gegenüber der betroffenen Person in Abhängigkeit davon, ob personenbezogene Daten bei dieser selbst erhoben werden (Direkterhebung, Art. 13) oder bei Dritten (Dritterhebung, Art. 14). Art. 19 normiert zudem eine Mitteilungspflicht gegenüber Empfängern, denen personenbezogene Daten offengelegt wurden, bei der Berichtigung oder Löschung dieser Daten oder der Einschränkung der Verarbeitung.

Im Fall der Direkterhebung ist der Verantwortliche zunächst verpflichtet, die Namen und Kontaktdaten des Verantwortlichen sowie gegebenenfalls seines Vertreters zur Verfügung zu stellen. Die bloße Mitteilung der Identität der verantwortlichen Stelle reicht also nicht mehr aus. Auch müssen die Kontaktdaten eines gegebenenfalls vorhandenen Datenschutzbeauftragten mitgeteilt werden. Neben der Angabe der jeweiligen Zwecke, für die die Verarbeitung erforderlich ist, ist nunmehr auch die konkrete Rechtsgrundlage zu nennen, auf die die Verarbeitung gestützt wird. Soweit sie auf Grundlage eines berechtigten Interesses gemäß Art. 6 Abs. 1 Buchst. f DS-GVO erfolgen soll, ist auch das konkrete Interesse zu benennen. Ohne Einschränkung sind daneben die Empfänger oder Kategorien von Empfängern personenbezogener Daten mitzuteilen.

Ebenfalls neu ist die Pflicht zur Information über die Absicht, personenbezogene Daten an ein Drittland oder eine internationale Organisation zu übermitteln. In diesen Fällen muss die betroffene Person darüber in Kenntnis gesetzt werden, welche Maßnahmen ergriffen wurden, um die Angemessenheit des Datenschutzniveaus im Empfängerland sicherzustellen.

Darüber hinaus sind zusätzlich solche Informationen zur Verfügung zu stellen, die eine faire und transparente Verarbeitung personenbezogener Daten gewährleisten. Dies können im konkreten Einzelfall zunächst Informationen über die Speicherdauer der jeweiligen Daten sein. Ebenso können Informationen über die Betroffenenrechte, insbesondere das Recht auf Auskunft, auf Datenübertragbarkeit und das Widerspruchsrecht, notwendig sein. Erfolgt die Verarbeitung im Wege einer automatisierten Entscheidungsfindung, sind aussagekräftige Informationen über die verwendete Logik, die Tragweite und die angestrebten Auswirkungen einer derartigen Verarbeitung anzugeben. Sämtliche Informationen sind der betroffenen Person bereits zum Zeitpunkt der Erhebung der Daten mitzuteilen oder sonst zur Verfügung zu stellen.

Auch wenn Daten bei Dritten erhoben werden, unterscheidet die Datenschutz-Grundverordnung zwischen mitzuteilenden Informationen und zusätzlichen Informationen, die zur Gewährung einer fairen und transparenten Verfahrensweise zur Verfügung zu stellen sind. Art und Inhalt der Informationen entsprechen in wesentlichen Teilen denjenigen, die auch im Falle einer Direkterhebung mitzuteilen sind. Da die betroffene Person allerdings nicht an der Datenerhebung mitgewirkt hat und somit auch keine Kenntnis darüber hat, welche personenbezogenen Daten erhoben wurden, hat der Verantwortliche zusätzlich auch die Kategorien der verarbeiteten Daten mitzuteilen. Diese Information muss so konkret sein, dass für die betroffene Person erkennbar wird, welche Folgen die Verarbeitung haben kann. Zudem ist nach Art. 14 Abs. 2 DS-GVO die Quelle der Daten anzugeben.

Die Informationen sind der betroffenen Person im Falle der Dritterhebung durch den Verantwortlichen nachträglich innerhalb einer angemessenen Frist nach Erlangung der Daten, spätestens jedoch innerhalb eines Monats, mitzuteilen. Diese Maximaldauer kann nicht pauschal als Frist angesetzt werden. Sie bestimmt sich vielmehr nach den konkreten Umständen des Einzelfalles und dürfte regelmäßig kürzer zu bemessen sein.

Ausnahmen von der Informationspflicht, etwa wenn die betroffene Person bereits über die Informationen verfügt (Art. 13 Abs. 4, 14 Abs. 5 Buchst. a DS-GVO) oder die Information einen unverhältnismäßigen Aufwand erfordern würde, sind im Sinne größtmöglicher Transparenz grundsätzlich eng auszulegen. Ein Verstoß gegen die Informationspflicht kann nach Art. 83 Abs. 5 Buchst. b DS-GVO mit einer Geldbuße geahndet werden.

Nur wenn die betroffene Person weiß, dass personenbezogene Daten über sie verarbeitet werden, kann sie die ihr zustehenden Rechte auch ausüben. Es ist für Verantwortliche aber auch im eigenen Interesse ratsam, rechtzeitig die erforderlichen Maßnahmen für eine zügige und korrekte Erfüllung der Informationspflichten zu treffen.

2.4 Datenschutz durch Technikgestaltung und durch datenschutzgerechte Voreinstellungen

Immer wieder stellen Datenschutzaufsichtsbehörden im Rahmen ihrer Beratungs- und Kontrolltätigkeit fest, dass Verantwortliche bei der Planung und Einführung von Verfahren zur Verarbeitung personenbezogener Daten Fragen des Datenschutzes und der Informationssicherheit gar nicht oder erst sehr spät im Projektverlauf betrachten. Dies erfordert in der Regel zeit- und kostenintensive Nachbesserungen, damit das Verfahren rechtskonform eingesetzt werden kann. Neue rechtliche Anforde-

rungen in der Datenschutz-Grundverordnung (DS-GVO) sollen die genannten Mängel und die Folgeprobleme verhindern.

Gemäß Art. 25 Abs. 1 DS-GVO muss der Verantwortliche sowohl zum Zeitpunkt der Festlegung der Mittel für die Verarbeitung als auch zum Zeitpunkt der eigentlichen Verarbeitung geeignete technische und organisatorische Maßnahmen treffen, die dafür ausgelegt sind, die Datenschutzgrundsätze wirksam umzusetzen und notwendige Garantien für die Einhaltung der Anforderungen der Verordnung und der Rechte Betroffener bieten. Er hat dabei den Stand der Technik, die Implementierungskosten, Art, Umfang, Umstände und Zwecke der Datenverarbeitung sowie die Risiken für die Rechte und Freiheiten natürlicher Personen zu berücksichtigen.

Die eigentliche Neuerung besteht in der Pflicht, bereits während der Konzeption und Entwicklung eines Verfahrens – also weit vor dessen Einsatz – Fragen des technischen und organisatorischen Datenschutzes zu klären (Datenschutz durch Technikgestaltung – Data protection by design). Somit können später notwendige Änderungen, die in der Regel aus der Nichtbeachtung dieser Fragen resultieren, vermieden werden.

Die Forderung nach Datenschutz durch Technikgestaltung wird durch die Verpflichtung des Verantwortlichen gemäß Art. 25 Abs. 2 DS-GVO ergänzt, geeignete technische und organisatorische Maßnahmen zu treffen, dass durch Voreinstellung grundsätzlich nur personenbezogene Daten verarbeitet werden, die für den beabsichtigten Zweck erforderlich sind (Datenschutz durch datenschutzgerechte Voreinstellungen – Data protection by default). Dies betrifft sowohl die Menge der Daten als auch den Umfang ihrer Verarbeitung, ihre Speicherfrist und die Zugänglichkeit zu den Daten.

Obwohl beide Regelungen den Verantwortlichen, der ein Verfahren zur Verarbeitung personenbezogener Daten einführen möchte, verpflichten, sind indirekt auch Verfahrenshersteller und Softwareproduzenten angesprochen. Sie sollten ihre Produkte von Anfang an so gestalten, dass diese die Anforderungen der Verordnung erfüllen bzw. sich entsprechend der gesetzlichen Vorgaben konfigurieren lassen. Nur so können sie langfristig im Wettbewerb bestehen.

Insgesamt sind mit den neuen Vorschriften bereits in frühen Phasen eines Projekts zur Einführung eines neuen Verfahrens zur Verarbeitung personenbezogener Daten und daran anschließend regelmäßig im weiteren Projektverlauf eine Reihe datenschutzrechtlicher Fragen zu betrachten und zu beantworten – ggf. in enger Abstimmung mit dem Verfahrenshersteller. Zu nennen sind in diesem Zusammenhang beispielsweise:

- In welchen Rollen werden Nutzer in dem Verfahren aktiv und welche Rechte sind für sie zur Erfüllung ihrer Aufgaben unbedingt erforderlich? Wie lässt sich das Rollen- und Berechtigungskonzept wirksam und nicht umgehbar implementieren?

- Welche Anforderungen werden an die Identifizierung und Authentisierung von Nutzern gestellt? Werden im Verfahren sensitive personenbezogene Daten verarbeitet oder bestehen bei unberechtigtem Zugriff besondere Risiken für Betroffene, sodass besondere Authentisierungsmechanismen vorzusehen sind? Wie werden diese umgesetzt?

- Welche Anforderungen bzgl. Verschlüsselung und digitaler Signatur ergeben sich aus der beabsichtigten Datenverarbeitung? Welche Vorkehrungen müssen hierfür in der verwendeten technischen Infrastruktur getroffen werden? Wie erfolgt die Verwaltung der kryptografischen Schlüssel?

- Wie wird der Grundsatz der Datensparsamkeit im Verfahren umgesetzt? Sind alle personenbezogenen Daten, die erhoben werden sollen, tatsächlich erforderlich? Können personenbezogene Daten frühzeitig pseudonymisiert oder anonymisiert werden?

- Welche technischen Komponenten bzw. Systembestandteile können zur Realisierung von Datenschutz und Sicherheitsfunktionen eingesetzt werden? Liegen diese bereits vor, sind sie getestet und können wiederverwendet werden? Über welche Schnittstellen können die Komponenten kommunizieren und Daten austauschen?

- Welche Entwicklungsumgebungen, Programmiersprachen bzw. Softwarebibliotheken unterstützen die sichere Entwicklung von neuen Komponenten, falls Eigenprogrammierungen erforderlich sind?

- Ist das Verfahren so gestaltet, dass die Einwilligung Betroffener z. B. in die Erhebung ihrer Daten, die Übermittlung an Dritte oder die Änderung des Verarbeitungszweckes eine bewusste, aktive Handlung erfordert? Werden Betroffene über die Konsequenzen der Einwilligung hinreichend aufgeklärt?

- Wird bei der Datenerhebung in Formularen bzw. in Eingabemasken – wenn möglich – auf Freitextfelder verzichtet? Werden stattdessen Auswahlfelder mit vorgegebenen Auswahlalternativen verwendet?

- Werden insbesondere für Betroffene die Schritte und Funktionen der Verarbeitung ihrer Daten transparent dargestellt? Besteht für Betroffene

eine einfache Möglichkeit, ihre Rechte z. B. auf Auskunft auszuüben? Welche Komponenten des Softwaresystems unterstützen dies?

- Wie erfolgt am Ende von Aufbewahrungsfristen technisch die Löschung von personenbezogenen Daten im Verfahren? Wie lassen sich die Berichtigung oder Sperrung von Daten oder ein Widerspruch des Betroffenen gegen die weitere Verarbeitung seiner Daten nachvollziehbar technisch umsetzen?

Hinzuweisen ist auch auf Folgendes: Wenn Verantwortliche gegen die Festlegungen des Art. 25 DS-GVO verstoßen, können Aufsichtsbehörden von ihren Abhilfebefugnissen wie Warnung, Verwarnung, Weisung oder Untersagung Gebrauch machen oder ggf. eine Geldbuße verhängen.

Der zeitliche, finanzielle und personelle Aufwand, um Verfahren zur Verarbeitung personenbezogener Daten erst nachträglich in Einklang mit den rechtlichen Bestimmungen zu bringen, kann durch die Einhaltung der Prinzipien des Datenschutzes durch Technikgestaltung und durch datenschutzgerechte Voreinstellungen minimiert werden. Verantwortlichen ist zu empfehlen, derartige Vorgaben bereits in Ausschreibungen für neue Verfahren zu integrieren. Verfahrenshersteller können die Einhaltung der Anforderungen durch Zertifikate für ihre Produkte nachweisen.

2.5 Datenschutz-Folgenabschätzung

Auch eine rechtmäßige Datenverarbeitung kann Risiken für die Rechte und Freiheiten der betroffenen Personen verursachen. Wenn dieses Risiko voraussichtlich hoch ist, sieht die Datenschutz-Grundverordnung (DS-GVO) die Durchführung einer Datenschutz-Folgenabschätzung vor, die Risiken der Datenverarbeitung untersucht und bewertet sowie Maßnahmen zur Risikobewältigung festlegt.

Eine Datenschutz-Folgenabschätzung ist gemäß Art. 35 DS-GVO durchzuführen, wenn die Form der Verarbeitung, insbesondere bei der Verwendung neuer Technologien, aufgrund der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung voraussichtlich ein hohes Risiko zur Folge hat. Ob dies der Fall ist, ergibt sich aus einer Abschätzung der Risiken der Verarbeitungsvorgänge (Schwellwertanalyse). Wird festgestellt, dass der Verarbeitungsvorgang kein hohes Risiko aufweist, dann ist eine Folgenabschätzung nicht zwingend erforderlich. In jedem Fall ist die Entscheidung über ihre Durchführung oder Nichtdurchführung mit Angabe der maßgeblichen Gründe für den konkreten Verarbeitungsvorgang schriftlich zu dokumentieren, um die Rechenschaftspflichten nach Art. 5 Abs. 2 DS-GVO zu erfüllen.

Eine Datenschutz-Folgenabschätzung ist vor der Aufnahme der zu betrachtenden Verarbeitungsvorgänge durchzuführen, kann aber bei wesentlichen Änderungen oder neu auftretenden Bedrohungen auch für bestehende Verfahren verpflichtend sein. Da sie einen intensiven Arbeitsprozess erfordert, muss sie rechtzeitig auf den Weg gebracht werden. Ein Datenschutz-Managementsystem kann dabei unterstützen.

Aufbauend auf Kriterien, die in einem europäischen Prozess abgestimmt wurden,[4] werden die Datenschutzaufsichtsbehörden eine nicht abschließende Liste mit Verarbeitungstätigkeiten, bei denen eine Datenschutz-Folgenabschätzung durchzuführen ist, veröffentlichen. Die Verordnung selbst enthält in Art. 35 Abs. 3 einige Beispiele. Genannt werden u. a. die umfangreiche Verarbeitung besonderer Kategorien personenbezogener Daten gemäß Art. 9 Abs. 1 DS-GVO oder die systematisch umfangreiche Überwachung öffentlich zugänglicher Bereiche.

Die formellen Anforderungen an die Durchführung einer Datenschutz-Folgenabschätzung ergeben sich aus Art. 35 DS-GVO, sowie den Erwägungsgründen 84, 90, 91, 92 und 93. Über die verwendete Methode können die Verantwortlichen entscheiden. Werden bestehende Methoden oder Standards eingesetzt, ist jedoch zu beachten, dass sie den Anforderungen der Datenschutz-Grundverordnung entsprechen müssen, d. h. ggf. anzupassen sind.

Die Resultate der Folgenabschätzung sind wegen der umfassenden Nachweis- und Dokumentationspflichten aus Art. 5 Abs. 2 DS-GVO in einem Bericht darzulegen. Dieser muss nach Art. 35 Abs. 7 DS-GVO mindestens eine systematische Beschreibung der geplanten Verarbeitungsvorgänge, eine Bewertung der Notwendigkeit und Verhältnismäßigkeit der Verarbeitung, die Beschreibung und Bewertung der Risiken sowie die Festlegung der Abhilfemaßnahmen zur Bewältigung der Risiken enthalten.

Ergibt eine Datenschutz-Folgenabschätzung, dass trotz technischer und organisatorischer Maßnahmen zur Risikoeindämmung weiterhin ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen besteht (Restrisiko), muss nach Art. 36 DS-GVO der Verantwortliche die zuständige Aufsichtsbehörde konsultieren. Er trifft unter Berücksichtigung der Empfehlungen der Aufsichtsbehörde eine Entscheidung, ob die Verarbeitungsvorgänge angesichts der verbleibenden Restrisiken durchgeführt werden können und ggf. welche zusätzlichen Abhilfemaßnahmen in diesem Fall zum Einsatz kommen sollen. Die Aufsichtsbehörde kann ihrerseits die in Art. 58 DS-GVO

[4] Siehe Artikel-29-Datenschutzgruppe, Leitlinien zur Datenschutz-Folgenabschätzung (DSFA) und Beantwortung der Frage, ob eine Verarbeitung im Sinne der Verordnung 2016/679 „wahrscheinlich ein hohes Risiko mit sich bringt“.

genannten Befugnisse ausüben und z. B. eine Warnung, Anweisung oder Untersagung der Verarbeitung aussprechen.

Die Datenschutz-Folgenabschätzung ist ein sinnvolles Instrument zur systematischen Risikoeindämmung und stellt eine wichtige Neuerung der Datenschutz-Grundverordnung dar. Rechtzeitig auf den Weg gebracht hilft sie nicht nur, die eigenen Prozesse bei der Verarbeitung personenbezogener Daten besser zu verstehen, sondern auch die Pflichten nach der Grundverordnung umzusetzen. Die Aufsichtsbehörden werden die Anwendung dieses Instruments mit der Veröffentlichung von Vorgaben, Hinweisen und Empfehlungen unterstützen.

2.6 Mitteilung der Kontaktdaten des Datenschutzbeauftragten

Bislang sind die verantwortlichen Stellen nicht verpflichtet, der Aufsichtsbehörde Kontaktdaten ihrer Datenschutzbeauftragten mitzuteilen. Dies ändert sich jedoch mit Geltung der Datenschutz-Grundverordnung (DS-GVO).

Gemäß Art. 37 Abs. 7 DS-GVO haben der Verantwortliche oder der Auftragsverarbeiter die Kontaktdaten des jeweiligen Datenschutzbeauftragten zu veröffentlichen und diese Daten der Aufsichtsbehörde mitzuteilen. Die Veröffentlichungs- und Mitteilungspflicht besteht nicht nur bezüglich des nach der Verordnung zu bestellenden Datenschutzbeauftragten, sondern auch, soweit sie nach dem weitergehenden, ab Mai 2018 geltenden § 38 BDSG zu bestellen sind.

Die Veröffentlichung der Kontaktdaten durch die Verantwortlichen entspricht dem Transparenzgrundsatz und ergänzt die Pflicht zur Bekanntgabe der Kontaktdaten an den jeweiligen Betroffenen gemäß Art. 13 und 14 DS-GVO. Die Kontaktdaten des Datenschutzbeauftragten sollten Angaben enthalten, die die Betroffenen ebenso wie die Aufsichtsbehörde in die Lage versetzen, den Datenschutzbeauftragten auf einfachem und direktem Weg zu erreichen. Dies kann durch Bekanntgabe einer postalischen Anschrift, einer persönlichen Telefonnummer oder einer persönlichen E-Mail-Adresse erfolgen.

Wir werden spätestens mit Geltung der Datenschutz-Grundverordnung in unserem Internetangebot über alle Möglichkeiten, der Meldepflicht nachzukommen, informieren.

Mit Geltung der Datenschutz-Grundverordnung haben der Verantwortliche und der Auftragsverarbeiter die Kontaktdaten des Datenschutzbeauftragten zu veröffentlichen und der Aufsichtsbehörde mitzuteilen.

2.7 Zertifizierung und Akkreditierung

Mit der Datenschutz-Grundverordnung (DS-GVO) wird auf EU-Ebene der Grundstein für datenschutzspezifische Zertifizierungsverfahren, Datenschutzsiegel und -prüfzeichen gelegt. Bis zur Umsetzung und Anwendung der Verordnung müssen die geforderten Mechanismen und Kriterien länderübergreifend entwickelt und abgestimmt werden.

Mit Art. 42 und 43 DS-GVO hat der europäische Gesetzgeber die Voraussetzungen geschaffen, die notwendig sind, um europaweit einheitliche Akkreditierungs- und Zertifizierungsverfahren zu etablieren. Die Zertifizierung ermöglicht den Nachweis, dass sich personenbezogene Verarbeitungsvorgänge im Einklang mit der Datenschutz-Grundverordnung befinden. Sie kann durch die zuständige Aufsichtsbehörde oder durch eine akkreditierte Zertifizierungsstelle für maximal 3 Jahre mit der Option auf Verlängerung erteilt werden. Die genannten Stellen können die Zertifizierung auch widerrufen, wenn die Voraussetzungen für die Zertifizierung nicht oder nicht mehr erfüllt werden. Grundlage eines jeden Zertifizierungsverfahrens ist die Bereitstellung der für dieses Verfahren notwendigen Informationen durch den Verantwortlichen bzw. Auftragsverarbeiter sowie die Gewährung des in diesem Zusammenhang erforderlichen Zugangs zu den Verarbeitungstätigkeiten. Die Zertifizierungskriterien, die das Verfahren im Wesentlichen bestimmen, werden durch die Zertifizierungsstelle der zuständigen Aufsichtsbehörde zur Genehmigung vorgelegt.

Die Befugnis, als Zertifizierungsstelle tätig zu werden (Akkreditierung), wird in Deutschland nach den Regelungen des ab Mai 2018 geltenden Bundesdatenschutzgesetzes durch die zuständige Aufsichtsbehörde auf Grundlage einer Akkreditierung durch die Deutsche Akkreditierungsstelle GmbH erteilt. Sie ist die bereits bestehende, nationale Akkreditierungsstelle der Bundesrepublik Deutschland. Um ihre hoheitlichen Akkreditierungsaufgaben ausfüllen zu können, wurde sie vom Bund beliehen und steht unter dessen Aufsicht.

Das Akkreditierungsverfahren erfolgt in zwei Stufen: Die erste Stufe besteht aus einer Prüfung des Antrag stellenden Unternehmens durch die Deutsche Akkreditierungsstelle, die unter Beteiligung von für den Prüfbereich fachkundigen Gutachtern der Aufsichtsbehörden durchgeführt werden soll. Danach entscheidet ein Akkreditierungsausschuss über den Erfolg einer Akkreditierung. Dieser Ausschuss wird zu zwei Dritteln von den Aufsichtsbehörden besetzt sein und kann nur einstimmig über den Erfolg des Verfahrens entscheiden. In einer zweiten Stufe vergibt die zuständige Aufsichtsbehörde im Rahmen eines Verwaltungsaktes die Befugnis, als Zertifizierungsstelle tätig zu werden.

Die unabhängigen Datenschutzbehörden des Bundes und der Länder stimmen derzeit Kriterien und Prozesse für Akkreditierungsverfahren nach der Datenschutz-Grundverordnung ab. Eine Arbeitsgruppe koordiniert auch die Abstimmungsprozesse mit der Deutschen Akkreditierungsstelle und fungiert als Schnittstelle zur Artikel-29-Datenschutzgruppe, die derzeit eine Leitlinie zur Zertifizierung und Akkreditierung erarbeitet.

Eine erfolgreiche Zertifizierung befreit einen Verantwortlichen oder Auftragsverarbeiter nicht von der Verantwortung für die Einhaltung der Datenschutz-Grundverordnung. Auch bleiben gemäß Art. 42 Abs. 4 DS-GVO unsere Aufgaben und Befugnisse als Aufsichtsbehörde von einer Zertifizierung unberührt. Diese kann jedoch, sofern ein genehmigtes Zertifizierungsverfahren durchgeführt wurde, unsere Kontroll- und Prüftätigkeit in beiderseitigem Interesse erleichtern.

Die Einführung von Datenschutz-Zertifizierungen ist ein wesentlicher Beitrag zur Anwendung und Einhaltung der Datenschutz-Grundverordnung. Sie soll betroffenen Personen auch einen raschen Überblick über das Datenschutzniveau einschlägiger Produkte und Dienstleistungen ermöglichen.

2.8 Sanktionen nach der Datenschutz-Grundverordnung

Nach wie vor halten einige öffentliche und nicht öffentliche Stellen datenschutzrechtliche Regelungen nur unzureichend ein. Grund hierfür mag unter anderem die geringe Sanktionsgefahr sein. Mit der Datenschutz-Grundverordnung (DS-GVO) soll sich dies nun ändern. Außerdem sind erheblich höhere Bußgelder als bislang, nämlich von bis zu 20 Millionen Euro oder 4 % des weltweiten Konzernjahresumsatzes, vorgesehen. Zudem verpflichtet die Verordnung die Verantwortlichen und Auftragsverarbeiter zu deutlich mehr Transparenz und Dokumentation im Umgang mit personenbezogenen Daten. Damit steigt zugleich die Gefahr, bei Nichteinhaltung der datenschutzrechtlichen Regelungen eher entdeckt zu werden, als dies in der Vergangenheit der Fall war.

Um die Einhaltung datenschutzrechtlicher Bestimmungen konsequent durchzusetzen, stellt Art. 58 DS-GVO den Aufsichtsbehörden einen umfassenden Katalog von Untersuchungs- und Abhilfebefugnissen (Sanktionen) zur Verfügung.

Im Rahmen ihrer Untersuchungsbefugnisse (Art. 58 Abs. 1 DS-GVO) kann die Aufsichtsbehörde den Verantwortlichen und Auftragsverarbeiter bzw. deren jeweilige Vertreter insbesondere anweisen, alle Informationen bereitzustellen, die für die Erfüllung der Aufgaben der Aufsichtsbehörde erforderlich sind. Daneben ist ihr der Zugang zu allen personenbezogenen Daten und

Informationen zu gewähren, die zur Aufgabenerfüllung notwendig sind. Von den in Art. 58 Abs. 2 DS-GVO genannten Abhilfebefugnissen sind vor allem die Verwarnung, die Anweisung zur Herstellung datenschutzkonformer Zustände, die Beschränkung bzw. das Verbot der Datenverarbeitung und die Verhängung von Bußgeldern hervorzuheben.

Die Verwarnung kann – nach dem Willen des europäischen Gesetzgebers – im Fall eines geringfügigeren Verstoßes oder wenn eine voraussichtlich zu verhängende Geldbuße eine unverhältnismäßige Belastung für eine natürliche Person bedeuten würde, ausgesprochen werden (ErwGr. 148). Für die Entscheidung, wann ein Verstoß als geringfügig anzusehen ist, können die Kriterien aus Art. 83 Abs. 2 S. 2 DS-GVO herangezogen werden. Da die Verwarnung eine verbindliche Feststellung darüber trifft, dass ein Rechtsverstoß vorliegt, ist sie als feststellender Verwaltungsakt zu klassifizieren.

Die Anweisung der Aufsichtsbehörde, datenschutzkonforme Zustände herzustellen, kann sich sowohl an den Verantwortlichen als auch an den Auftragsverarbeiter richten. Die Aufsichtsbehörde kann dabei konkrete Vorgaben machen, auf welche Weise der Einklang mit den Vorschriften der Datenschutz-Grundverordnung hergestellt werden soll. Weitere Anweisungen können z. B. die Einhaltung der Betroffenenrechte oder die Benachrichtigung von einem Datenschutzverstoß betroffener Personen beinhalten. Da es sich bei den aufsichtsbehördlichen Anweisungen um belastende Verwaltungsakte handelt, können sie mit Zwangsmitteln, wie z. B. Zwangsgeldern, durchgesetzt werden.

Zusätzlich zu den oder anstelle der in Art. 58 Abs. 2 DS-GVO genannten Maßnahmen können Verstöße gegen die Grundverordnung mit Geldbußen geahndet werden. Für nahezu jeden Verstoß gegen die Regelungen wird eine Geldbuße angedroht. Der Sanktionsrahmen aus Art. 83 Abs. 4 bis 6 DS-GVO ist dabei deutlich höher als bisher. Zukünftig können Geldbußen bis zu 20 Millionen Euro bzw. 4 % des gesamten, weltweit erzielten Jahresumsatzes eines Unternehmens verhängt werden, je nachdem, welcher der Beträge höher ist.

Besonderes Augenmerk ist dabei auf den Begriff des Unternehmens zu legen. Nach dem Willen des europäischen Gesetzgebers soll der weite, funktionale Unternehmensbegriff aus dem Kartellrecht gelten.[5] Danach werden Mutter- und Tochtergesellschaften als wirtschaftliche Einheit betrachtet. Verstöße in einem kleineren konzernangehörigen Unternehmen können somit dazu führen, dass der Jahresumsatz des gesamten Konzerns als Bemessungsgrundlage für die Höhe der prozentual zu verhängenden Geldbuße gilt. Die Anwendung des funktionalen Unternehmensbegriffs wirkt sich aber auch

[5] ErwGr. 150, Art. 101, 102 Vertrag über die Arbeitsweise der Europäischen Union.

auf haftungsrechtliche Fragen aus. Denn nach der hierfür maßgeblichen kartellrechtlichen Rechtsprechung genügt für die Verantwortlichkeit eines Unternehmens bzw. einer Unternehmensvereinigung die Handlung einer Person, die berechtigt ist, für das Unternehmen bzw. die Unternehmensvereinigung tätig zu werden. Erfasst sind daher nicht nur wie bisher die gesetzlichen Vertreter oder Leitungspersonen, sondern sämtliche Beschäftigte oder auch Beauftragte außerhalb des Unternehmens oder der Unternehmensvereinigung. Eine Kenntnis der Inhaber oder Geschäftsführer des Unternehmens von der konkreten Handlung oder eine Verletzung der Aufsichtspflicht ist für die Zuordnung der Verantwortlichkeit nicht erforderlich. Exzesse sind davon ausgenommen. Bei einem Exzess wäre zu prüfen, ob der Beschäftigte selbst Verantwortlicher im Sinne der Datenschutz-Grundverordnung ist und er demzufolge für die festgestellten Datenschutzverstöße belangt und persönlich mit einem Bußgeld belegt werden könnte.

Bei der Bemessung der Geldbuße gilt der Grundsatz aus Art. 83 Abs. 1 DS-GVO, dass eine Geldbuße wirksam, verhältnismäßig und abschreckend sein muss. In Art. 83 Abs. 2 Satz 2 DS-GVO werden eine Reihe von Kriterien aufgezählt, die bei der Entscheidung über die Verhängung der Geldbuße und über deren Höhe berücksichtigt werden. So ist neben Art, Schwere und Dauer des Verstoßes u. a. einzubeziehen, welche Art von Daten rechtswidrig verarbeitet wurde und ob finanzielle Vorteile durch die Datenverarbeitung erlangt wurden. Zu beachten ist ebenfalls, ob und wie der Verantwortliche oder Auftragsdatenverarbeiter mit der Aufsichtsbehörde zusammengearbeitet hat, um dem Verstoß abzuhelfen und seine möglichen nachteiligen Auswirkungen zu mindern, und ob die Stellen die Verstöße eigenständig der Aufsichtsbehörde mitgeteilt haben. Dies kann eine Abmilderung der Geldbuße bewirken. Insofern sollte nicht vergessen werden, dass es auch finanziell lohnenswert sein kann, sich im Falle einer entdeckten Datenschutzverletzung unverzüglich bei der Aufsichtsbehörde zu melden und so viel wie möglich gegen die Folgen für Betroffene zu unternehmen.

Um ein einheitliches Vorgehen der Aufsichtsbehörden auf europäischer Ebene bei der Bemessung von Geldbußen zu erreichen, hat die Artikel-29-Datenschutzgruppe zuletzt eine diesbezügliche Leitlinie erlassen.[6]

Neben der Datenschutz-Grundverordnung enthält auch das neue Bundesdatenschutzgesetz (BDSG) Regelungen zu Sanktionen. Diese erfolgten aufgrund des in Art. 84 Abs. 1 DS-GVO eröffneten Regelungsspielraums, wonach die Mitgliedstaaten die Vorschriften über andere Sanktionen für Datenschutzverstöße festlegen. In § 43 Abs. 1 BDSG sind daher Bußgeldvorschriften zu den Regelungen über Verbraucherkredite enthalten. Von dem Rege-

6 Artikel-29-Datenschutzgruppe, „Guidelines on the application and setting of administrative fines for the purposes of the Regulation 2016/679“.

lungsspielraum ist ebenfalls die Ermächtigung zur Schaffung strafrechtlicher Vorschriften umfasst. Hiervon hat der deutsche Gesetzgeber Gebrauch gemacht und in § 42 BDSG unbefugtes gewerbsmäßiges Handeln und solches in Bereicherungs- bzw. Schädigungsabsicht oder gegen Entgelt unter Strafe gestellt.

Die Verhängung von Geldbußen gegen Behörden wird durch § 43 Abs. 3 BDSG ausgeschlossen. Hierbei ist allerdings zu beachten, dass der europarechtliche Behördenbegriff zugrunde zu legen ist. Danach sind alle Unternehmen, die am Wettbewerb teilnehmen, ungeachtet ihrer nach nationalem Recht möglicherweise als öffentlich-rechtlich anzusehenden Rechtsform, keine Behörden oder öffentlichen Stellen i. S. v. Art. 83 Abs. 7 DS-GVO. Dies hat zur Folge, dass u. a. gegen staatliche Krankenhäuser oder Sparkassen Bußgelder verhängt werden können.

Die Sanktionsmöglichkeiten bei Datenschutzverstößen erschöpfen sich jedoch nicht in den Abhilfe- und Untersuchungsbefugnissen der Aufsichtsbehörde aus Art. 58 DS-GVO und der Verhängung von Bußgeldern. Zukünftig drohen den Verursachern von Datenschutzverstößen noch ganz andere Maßnahmen, die finanziell sehr einschneidend sein können. Exemplarisch seien hier nur die Abmahnung durch Datenschutzvereine und Verbraucherschutzverbände nach Art. 80 Abs. 1 und 2 DS-GVO genannt.

Die Datenschutz-Grundverordnung droht für nahezu jeden Datenschutzverstoß empfindliche Geldbußen an. Verantwortliche und Auftragsverarbeiter sind daher gut beraten, die notwendigen Veränderungen zeitnah umzusetzen.

3 Umsetzungsempfehlungen und Maßnahmeplan

Mit Erscheinen dieses Berichts neigt sich die zweijährige Übergangsfrist seit dem Inkrafttreten der Datenschutz-Grundverordnung (DS-GVO) dem Ende entgegen – die Verordnung ist ab dem 25. Mai 2018 verbindlich anzuwenden. Denjenigen Behörden und Unternehmen, die sich bisher gar nicht oder nur wenig mit der Umsetzung der neuen Anforderungen befasst haben, werden nachfolgend Hinweise für ein systematisches Vorgehen gegeben.

Grundsätzlich sind alle Prozesse und IT-Verfahren einer Behörde oder eines Unternehmens, in denen personenbezogene Daten verarbeitet werden, daraufhin zu prüfen, welche Anpassungen an die Regelungen der Daten-

schutz-Grundverordnung (bzw. der nationalen Umsetzungsgesetze)[7] vorgenommen werden müssen. Da hierbei ein erheblicher Planungs-, Koordinierungs- und Umsetzungsaufwand entstehen kann und verschiedene Beteiligte aus unterschiedlichen Organisationseinheiten einzubeziehen sind, empfiehlt sich eine projektorientierte Herangehensweise. Gleichzeitig ist auch davon auszugehen, dass die Ergebnisse des Anpassungsprozesses künftig regelmäßig zu überprüfen und zu aktualisieren sind. Dies wird beispielsweise aufgrund der Änderungen der Rechtslage, wechselnder Rahmenbedingungen oder der Fortentwicklung des Standes der Technik erforderlich. Das entspricht auch den Vorgaben der Verordnung, die z. B. in Art. 24, 32 und 35 DS-GVO zu finden sind. Insofern sollte ein iteratives Vorgehen geplant werden, z. B. in Anlehnung an den PDCA-Zyklus (PDCA – Plan, Do, Check, Act), eine bewährte Methode, die ursprünglich zur Qualitätssicherung in Produktionsprozessen entwickelt wurde.

In einem ersten Schritt sollte zunächst der Ist-Zustand der aktuell in der Behörde oder dem Unternehmen durchgeführten Verarbeitungen von personenbezogenen Daten erfasst werden. Insbesondere sind hierbei zu prüfen: zurzeit bestehende Rechtsgrundlagen für die Datenverarbeitungen, existierende Dokumentationen (wie Verfahrensverzeichnisse, Sicherheitskonzepte, Vorabkontrollen, verfahrensspezifische Dienst- oder Betriebsanweisungen) einschließlich ihrer Vollständigkeit, Aussagekraft und Aktualität, vertragliche Beziehungen zu externen Auftragsverarbeitern, allgemeine interne datenschutzrelevante Vorgaben (wie allgemeine Richtlinien, Anweisungen, Vorgaben für Prozessabläufe usw.).

Daran anschließend kann unter Berücksichtigung und Analyse der neuen Anforderungen der Datenschutz-Grundverordnung der Soll-Zustand für die Behörde oder das Unternehmen definiert werden. Durch einen Vergleich von Ist- und Soll-Zustand lassen sich bestehende Lücken und damit der Handlungsbedarf zur Anpassung der jeweiligen Verarbeitungen an die Verordnung identifizieren. Hierbei ist auch zu beachten, dass der Geltungsbereich der neuen Vorschriften nach Art. 2 Abs. 1 DS-GVO nicht nur (ganz oder teilweise) automatisierte Verarbeitungen personenbezogener Daten umfasst, sondern ebenso nicht-automatisierte Verarbeitungen von strukturierten Sammlungen solcher Daten, die nach bestimmten Kriterien zugänglich sind. Damit können sich im Vergleich zur bisherigen Rechtslage neue Dokumentations- und Nachweispflichten ergeben (z. B. bei der Erstellung des Verzeichnisses der Verarbeitungstätigkeiten nach Art. 30 DS-GVO).

Aus inhaltlicher Sicht ist es in diesem Schritt u. a. erforderlich zu prüfen, ob die bisherigen Rechtsgrundlagen der Datenverarbeitung weiter gültig sind oder eine Anpassung erforderlich ist. Dies betrifft auch die Frage der Fortgel-

[7] Siehe B 1.

tung von Einwilligungen Betroffener, falls die Verarbeitung darauf beruht. Weiterhin ist zu untersuchen, ob die bestehenden Verfahrensverzeichnisse in Bezug auf die Festlegungen von Art. 30 DS-GVO fortzuschreiben sind; für ggf. neu zu dokumentierende Verarbeitungen ist die Erstellung der Verzeichnisse vorzusehen. Gleiches gilt für die Beschreibung der technischen und organisatorischen Maßnahmen gemäß Art. 32 DS-GVO in Sicherheitskonzepten. Hierbei sind sowohl die speziellen Anforderungen dieses Artikels (z. B. zu Pseudonymisierung und Verschlüsselung, Gewährleistung der Belastbarkeit der IT-Systeme oder Prüfung der Wirksamkeit der Maßnahmen) als auch die Vorgaben von Art. 25 DS-GVO (zu Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen)[8] zu berücksichtigen. Darüber hinaus sind alle Verträge mit externen Auftragsverarbeitern darauf zu überprüfen, ob sie den Anforderungen von Art. 28 DS-GVO gerecht werden. Für solche Verarbeitungen, die voraussichtlich ein hohes Risiko für die Rechte und Freiheiten Betroffener zur Folge haben, ist die Erarbeitung einer Datenschutz-Folgenabschätzung gemäß Art. 35 DS-GVO zu planen und in bestimmten Fällen gemäß Art. 36 DS-GVO auch die Konsultation der Aufsichtsbehörde erforderlich.[9] Und letztlich werden die Nachweispflichten aus Art. 5 DS-GVO im Regelfall eine Überprüfung und Aktualisierung der allgemeinen behörden- oder unternehmensinternen Vorgaben zur Datenschutzorganisation[10] verlangen. Von besonderer Bedeutung ist in diesem Zusammenhang die Beschreibung der Prozesse zur Erfüllung der Informations- und Transparenzpflichten sowie zur Gewährleistung der Rechte Betroffener z. B. auf Auskunft, Berichtigung oder Löschung.

Der so identifizierte Handlungsbedarf, um die Lücken zwischen dem Ist- und dem Soll-Zustand zu schließen, muss in einen Plan zur Umsetzung der erforderlichen Anpassungsmaßnahmen und zur Beseitigung der Defizite münden. Hierbei sind konkret jeweils die Verantwortlichen und die Fertigstellungstermine zu definieren. Die Abarbeitung des Plans ist zu kontrollieren, die Ergebnisse sind zu überprüfen. In Abhängigkeit von der Qualität der bestehenden Verfahrensdokumentationen, der Komplexität der Verarbeitungen und der zur Verfügung stehenden Ressourcen kann es für die Behörde oder das Unternehmen sinnvoll sein, Prioritäten zu setzen. So kann mit der Anpassung an die Datenschutz-Grundverordnung etwa bei solchen Verarbeitungen begonnen werden, bei denen die Lücke zwischen Ist und Soll relativ klein ist und damit schnell Erfolge zu erzielen sind. Eine andere Herangehensweise könnte darin bestehen, zuerst diejenigen Verfahren zu betrachten, die besondere Bedeutung für die Geschäftstätigkeit haben und bei denen Maßnahmen der Aufsichtsbehörde oder Bußgelder gravierende Konsequenzen hätten. Letztlich muss die Behördenleitung bzw. die Geschäftsführung hierüber entschei-

8 Siehe A 2.4.

9 Siehe A 2.5.

10 Siehe A 2.1.

den. Sie bleibt in jedem Fall für die Einhaltung aller gesetzlichen Vorschriften verantwortlich.

Öffentliche und private Stellen, welche die bislang geltenden datenschutzrechtlichen Regelungen konsequent beachtet haben, sollten mit der Anpassung ihrer internen Organisation, der Prozesse und Verfahren zur Verarbeitung personenbezogener Daten an die Vorgaben der Datenschutz-Grundverordnung wesentlich besser zurechtkommen als diejenigen, die in diesem Bereich erhebliche Versäumnisse aufweisen. Davon unabhängig sind im Anschluss an die Anpassung Maßnahmen vorzusehen, die eine kontinuierliche und dauerhafte Einhaltung der datenschutzrechtlichen Anforderungen gewährleisten.

Teil B

Datenschutz

1 Entwicklung des Datenschutzrechts

Nach Inkrafttreten der europäischen Datenschutz-Grundverordnung (DS-GVO)[11] im Mai 2016 und der Datenschutzrichtlinie für den Bereich von Justiz und Inneres (JI-Richtlinie)[12] verblieb den Mitgliedstaaten eine Übergangszeit von zwei Jahren, um im nationalen Recht die aus den europäischen Bestimmungen folgenden Konsequenzen zu ziehen. Sowohl der Bundesgesetzgeber als auch der brandenburgische Landesgesetzgeber waren aufgefordert, die Bundes- und Landesgesetze auf ihre Kompatibilität mit der EU-Gesetzgebung zu überprüfen und die notwendigen Anpassungsgesetze auf den Weg zu bringen – ein ambitioniertes Vorhaben, das in wesentlichen Teilen rechtzeitig mit dem Wirksamwerden der Datenschutz-Grundverordnung abgeschlossen sein wird.

Bereits im April 2016, als der zwischen der Europäischen Kommission, dem Europäischen Parlament und dem Rat der Europäischen Union abgestimmte, endgültige Wortlaut der Datenschutz-Grundverordnung und der JI-Richtlinie vorlag, sprach sich die Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder dafür aus, das bestehende Datenschutzniveau, auch im Lichte der jüngeren Entscheidungen des Europäischen Gerichtshofs, zu erhalten und zu verstärken.[13] Sie appellierte an Bundes- und Landesgesetzgeber, die in der Datenschutz-Grundverordnung enthaltenen Öffnungs- und Konkretisierungsklauseln zugunsten des Rechts auf informationelle Selbstbestimmung zu nutzen, und empfahl beispielsweise, die durch die Verordnung weiterentwickelten Grundsätze des Datenschutzes durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen sowie das Erfordernis von Datenschutz-Folgenabschätzungen möglichst wirksam auszugestalten.

---

11 Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung) (ABl. EU L 119/1).

12 Richtlinie (EU) 2016/680 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr und zur Aufhebung des Rahmenbeschlusses 2008/977/JI des Rates (ABl. EU L 119/89).

13 Entschließung „Stärkung des Datenschutzes in Europa – nationale Spielräume nutzen“ vom 6. und 7. April 2016, siehe Anlage Nr. 1.6.1.

1.1 Datenschutz-Anpassungs- und -Umsetzungsgesetz des Bundes

Zu einem ersten, außerhalb eines offiziellen Verfahrens an die Öffentlichkeit gelangten Gesetzentwurf des Bundes mit Stand vom 5. August 2016 äußerte sich die Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder in einem umfassenden datenschutzrechtlichen Eckpunktepapier vom 28. September 2016,[14] das sie dem Bundesinnenministerium zuleitete. Darin kritisierte sie insbesondere die Vermischung der Regelungen zur Anpassung des Bundesdatenschutzgesetzes an die Datenschutz-Grundverordnung einerseits und zur Umsetzung der JI-Richtlinie andererseits. Eine solche Verschränkung sei höchst problematisch; sie sei intransparent und berge das Risiko einer fehlerhaften Anwendung. Insbesondere sei die Trennung der den öffentlichen Bereich betreffenden Bestimmungen von solchen, die für nicht öffentliche Stellen gelten, für den Gesetzesanwender oftmals nicht zu erkennen. Ein wesentlicher Kritikpunkt betraf zudem die Ausnutzung der in der Verordnung gewährten Regelungsspielräume für die nationalen Gesetzgeber. Deren Rahmen würde der Bundesgesetzgeber – unterstellt, das Gesetz würde in der Fassung dieses Gesetzentwurfs in Kraft treten – deutlich überschreiten und das bisherige Datenschutzniveau in Deutschland dadurch beträchtlich senken. Daneben äußerte sich die Konferenz auch kritisch zur zukünftigen Stellung der unabhängigen Datenschutzaufsichtsbehörden, wie etwa zum fehlenden Klagerecht der Datenschutzbehörden gegen Entscheidungen der EU-Kommission, zu der aus Ländersicht unzureichenden Regelung der Vertretung im Europäischen Datenschutzausschuss und zur Einrichtung einer zentralen Anlaufstelle.

Im November 2016 lag der Referentenentwurf eines Gesetzes zur Anpassung des Datenschutzrechts an die Verordnung (EU) 2016/679 und zur Umsetzung der Richtlinie (EU) 2016/680 – kurz: Datenschutz-Anpassungs- und -Umsetzungsgesetz EU – offiziell vor. Die Landesinnenminister hatten den Entwurf jeweils den Landesdatenschutzbehörden zur Stellungnahme übermittelt. Einige der ursprünglichen Kritikpunkte waren in diesem Gesetzentwurf ausgeräumt. Insbesondere war die empfohlene Trennung zwischen der Anpassung an die Datenschutz-Grundverordnung einerseits und der Umsetzung der JI-Richtlinie andererseits vorgenommen worden. Auch ließ sich nun nicht mehr nur der Gesetzesbegründung, sondern auch dem eigentlichen Gesetzestext entnehmen, ob eine Regelung für alle Verantwortlichen und ausschließlich für öffentliche oder nicht öffentliche Stellen gelten soll.

---

[14] Datenschutzrechtliche Eckpunkte zu den in die Öffentlichkeit gelangten Überlegungen des BMI für ein Gesetz zur Anpassung des Datenschutzrechts an die Datenschutzgrundverordnung und zur Umsetzung der Richtlinie (EU) 2016/680 (Datenschutz-Anpassungs- und -Umsetzungsgesetz EU – DSAnpUG-EU) vom 28. September 2016, siehe http://www.lda.brandenburg.de.

Mangels Zeit, eine umfassende inhaltliche Stellungnahme unter den unabhängigen Datenschutzbehörden des Bundes und der Länder abzustimmen, äußerte sich die Landesbeauftragte im Dezember 2016 gegenüber dem Ministerium des Innern und für Kommunales des Landes Brandenburg zu dem Gesetzentwurf, und zwar insbesondere zu dessen Artikel 1, der das neue Bundesdatenschutzgesetz enthält. Sie regte an, ihre Kritikpunkte, sofern das Ministerium sie teilt, aufzugreifen und in dessen eigene Stellungnahme gegenüber dem Bund zu übernehmen. Ein Schwerpunkt der Stellungnahme der Landesbeauftragten war die nach ihrer Auffassung rechtswidrige Ausfüllung der Regelungsspielräume der Datenschutz-Grundverordnung, die nicht nur extensiv, sondern in einem Maße ausgenutzt wurden, das die durch die Grundverordnung gesetzten Grenzen bei Weitem überschreitet. Ein Verstoß gegen EU-Recht im Falle des Inkrafttretens dieses Gesetzentwurfs schien offensichtlich. Dies betraf u. a. die erheblichen Beschränkungen der Betroffenenrechte und die unverhältnismäßige Durchbrechung des strengen Zweckbindungsgrundsatzes. Auf Kritik stieß auch, dass speziell bei den technisch-organisatorischen Regelungen die Bestimmungen der Verordnung und diejenigen des bisherigen Bundesdatenschutzgesetzes so miteinander verwoben wurden, dass daraus teilweise inkonsistente, schlimmstenfalls in sich widersprüchliche Regelungen erwuchsen.

Nachdem absehbar war, dass auch zu dem im Januar 2017 vorgelegten dritten Referentenentwurf eine unter den unabhängigen Datenschutzbehörden der Länder abgestimmte Stellungnahme vor der Befassung im Bundeskabinett nicht mehr möglich sein würde, beschlossen sie einen neuen Weg zu beschreiten, um ihre Bedenken gegen den Gesetzentwurf in das parlamentarische Verfahren einzubringen.[15] Angesichts der Vielzahl von Kritikpunkten einigten sie sich zunächst auf 13 Themenschwerpunkte und legten hierzu konkret formulierte Änderungsanträge einschließlich Begründung vor. Diese Änderungsvorschläge betrafen u. a. die Vertretung der Landesaufsichtsbehörden im Europäischen Datenschutzausschuss, die Rechte der betroffenen Personen, die Verarbeitung von besonderen Kategorien von Daten (insbes. von Gesundheitsdaten), die Einschränkungen der Aufsichtsbefugnisse gegenüber Berufsgeheimnisträgern und die fehlende Möglichkeit, Anordnungen der Aufsichtsbehörde gegenüber Behörden mithilfe von Zwangsvollstreckungsmaßnahmen durchzusetzen. Die einzelnen Landesdatenschutzbehörden leiteten die Änderungsvorschläge sodann ihren jeweils zuständigen Landesministerien mit der Bitte zu, sie in den Beratungen der zuständigen Ausschüsse des Bundesrats zu berücksichtigen und ggf. als eigene Anträge zu übernehmen. Der Bundesrat griff in seiner Stellungnahme zum Gesetz-

[15] Die Bundesbeauftragte nahm hieran nicht teil, da sie bereits Gelegenheit gehabt hatte, eine eigene Stellungnahme zu dem aktuellen Gesetzentwurf gegenüber dem Bundesinnenministerium abzugeben.

entwurf[16] verschiedene Vorschläge auf, im Ergebnis fanden sie jedoch nur zu einem sehr geringen Teil Eingang in das vom Bundestag am 27. April 2017 verabschiedete Gesetz.[17] Damit hat der Bundesgesetzgeber das Bundesdatenschutzgesetz rechtzeitig vor Anwendbarkeit der Datenschutz-Grundverordnung ab dem 25. Mai 2018 novelliert und auch die JI-Richtlinie im Rahmen seiner Zuständigkeit innerhalb der zweijährigen Umsetzungsfrist in nationales Recht umgesetzt.

1.2 Gesetz zur Änderung des Bundesversorgungsgesetzes und anderer Vorschriften

Die Umsetzung der Datenschutz-Grundverordnung durch den Bund beschränkte sich keineswegs auf die Novellierung des Bundesdatenschutzgesetzes. Hinter der zunächst harmlos klingenden Gesetzesbezeichnung „Gesetz zur Änderung des Bundesversorgungsgesetzes und anderer Gesetze“ verbarg sich eine Überraschung.

Ursprüngliches Ziel dieses aus zunächst nur drei Artikeln bestehenden Gesetzentwurfs[18] war es, die Höhe der sog. Vermögensschonbeträge im Bundesversorgungsgesetz und in der Verordnung zur Kriegsopferfürsorge der Erhöhung vergleichbarer Vermögensschonbeträge in der Sozialhilfe anzupassen. Das Gesetz, das schließlich nach Durchlaufen des parlamentarischen Gesetzgebungsverfahrens verabschiedet wurde, war demgegenüber auf erstaunliche 32 Artikel angewachsen. Das mag verfassungsrechtlich unproblematisch sein, solange sich die Ergänzungen im Rahmen des ursprünglichen Regelungsbereichs halten und sich an dem Gesetzesziel orientieren. Hieran hat sich der Bundestag jedoch nicht gehalten. Denn Zweck der meisten hinzugekommenen Artikel ist die Umsetzung der Datenschutz-Grundverordnung, noch dazu in Regelungsbereichen, die das eigentliche sozialpolitische Sachgebiet überhaupt nicht berühren. Zur Illustration sei auf die neu hinzugekommenen Änderungen des Handelsgesetzbuchs und des Genossenschaftsgesetzes (Art. 7 und 8), auf Änderungen des Patentgesetzes (Art. 9), des Halbleiterschutzgesetzes (Art. 12), des Urheberrechtsgesetzes (Art. 13) sowie der Abgabenordnung (Art. 17) hingewiesen. Ebenfalls geändert wurden verschiedene Bücher des Sozialgesetzbuches, darunter, aus datenschutzrechtlicher Sicht vor allem interessant, die Neuregelung des Sozialdatenschutzes im Zehnten Buch Sozialgesetzbuch (Art. 24).

16 Stellungnahme des Bundesrats vom 10. März 2017, Bundesrats-Drs. 110/17 (Beschluss).

17 Gesetz zur Anpassung des Datenschutzrechts an die Verordnung (EU) 2016/679 und zur Umsetzung der Richtlinie (EU) 2016/680 (Datenschutz-Anpassungs- und -Umsetzungsgesetz EU – DSAnpUG-EU) vom 30. Juni 2017 (BGBl. I S. 2097).

18 Gesetzentwurf der Bundesregierung vom 24. April 2017, Bundestags-Drs. 18/12041.

Kritikwürdig ist das Hauruck-Verfahren, in dem dieses Gesetz zustande gekommen ist. Durch kurzfristige und umfangreiche Ergänzungen mutierte es faktisch zu einem Gesetz zur Umsetzung und Ergänzung der Datenschutz-Grundverordnung. Auf die Anhörung im federführenden Bundestagsausschuss für Arbeit und Soziales am 29. Mai 2017, zu der u. a. kurzfristig immerhin die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit sowie der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit als Sachverständige geladen waren, folgte die Beschlussempfehlung bereits am 31. Mai 2017.[19] Weder der für den Datenschutz zuständige Bundestagsausschuss für Inneres noch der für die Abgabenordnung zuständige Finanzausschuss wurden beteiligt. Der Bundestag verabschiedete das Gesetz in zweiter und dritter Beratung in seiner 237. Sitzung am 1. Juni 2017. Für Reaktionen vonseiten der unabhängigen Datenschutzbehörden oder gar inhaltliche Stellungnahmen blieb angesichts der rasanten Abläufe kein Raum.

Die Landesbeauftragte, die ihrerseits erstmals am 31. Mai 2017 Kenntnis von dem Gesetzgebungsverfahren erhielt, kritisierte die „Nacht- und Nebelaktion“ des Bundesgesetzgebers.[20] Sie wandte sich aber nicht nur gegen das intransparente „Huckepackverfahren“, sondern auch gegen die durch das Gesetz bewirkte unverhältnismäßig starke Beschränkung der Rechte der Betroffenen, darunter vor allem des Rechts auf Auskunft, das gerade durch die neuen Vorschriften in der Abgabenordnung und in den Sozialgesetzbüchern erheblich verkürzt wird. Besonders kritisch sieht die Landesbeauftragte die Übertragung der Datenschutzaufsicht über die Landesfinanzbehörden in Steuerangelegenheiten von den Landesbeauftragten auf die Bundesbeauftragte für den Datenschutz, ohne dass dafür eine nachvollziehbare Begründung gegeben worden wäre. Welche Verbesserungen sich durch die Zentralisierung der Aufsicht für die betroffenen Bürgerinnen und Bürger ergeben sollen, ist nicht ersichtlich, zumal Ad-hoc-Prüfungen vor Ort zukünftig die Ausnahme sein dürften.

Ähnlich äußerten sich auch die unabhängigen Datenschutzbehörden der Länder in ihrem Positionspapier zum „Gesetz zur Änderung des Bundesversorgungsgesetzes und anderer Vorschriften (BR-Drs. 450/17)“ vom 20. Juni 2017, das dem Bundesrat mit Schreiben vom 20. Juni 2017 übermittelt wurde. Vorab wenden auch sie sich darin gegen die höchst undemokratische „Geheimgesetzgebung“. In dem Positionspapier wird sodann u. a. hingewiesen auf die erheblichen Einschränkungen der Informations- und Auskunftsrechte in der Abgabenordnung und im Zehnten Buch Sozialgesetzbuch, die angesichts der unbestimmten Formulierungen nahezu entfallen, ebenso wie auf die davon nicht zu trennenden Berichtigungs- und Widerspruchsmöglich-

19 Bundestags-Drs. 18/12611.

20 Presseinformation „Verschlechterung beim Datenschutz in Nacht- und Nebelaktion vom Deutschen Bundestag verabschiedet“ vom 2. Juni 2017, siehe http://www.lda.brandenburg.de.

keiten. Kritisiert werden außerdem die unklaren und teilweise beschränkten Befugnisse der Aufsichtsbehörden im Rahmen der Neuregelung des Sozialdatenschutzes im Zehnten Buch Sozialgesetzbuch. Ein weiterer wesentlicher Kritikpunkt ist wiederum die neue Zuständigkeit der Bundesbeauftragten für den Datenschutz und die Informationsfreiheit für die Datenschutzaufsicht über die Finanzbehörden der Länder im Anwendungsbereich der Abgabenordnung. Für diese Zuständigkeitsverlagerungen habe die bisherige Aufsicht keinerlei Anlass gegeben. Die Landesbeauftragten seien ihren Aufsichtspflichten kompetent, effektiv und flexibel nachgekommen. Zudem seien sie aufgrund ihrer örtlichen Nähe kurzfristig ansprechbar und gerade bei aktuellem Klärungs- und Beratungsbedarf sowie bei akuten Vorfällen sofort handlungsfähig. Da die Neuregelung außerdem eine Aufspaltung der Zuständigkeit für die Datenschutzaufsicht über die Finanzbehörden und Kommunen zur Folge haben werde, sei absehbar, dass die Abgrenzung der Zuständigkeiten zwischen Bundes- und Landesbeauftragten zu erheblichen Reibungsverlusten führen werde. Kompetenzstreitigkeiten, die Gefahr von Aufsichtslücken und eine unflexible, mit den Konstellationen vor Ort wenig vertraute Aufsicht seien als Konsequenz der Zentralisierung der Datenschutzaufsicht vorprogrammiert.

Ungeachtet dessen stimmte der Bundesrat dem Gesetzentwurf am 7. Juli 2017 zu. Er verband seine Zustimmung jedoch mit einer längeren Entschließung, die insbesondere das Gesetzgebungsverfahren, die Außerachtlassung des verfassungsrechtlichen Mitwirkungsrechts der Länder und Zweifel an der Gesetzgebungszuständigkeit des Bundes betraf. Trotz seiner erheblichen, zum Teil verfassungsrechtlich begründeten Zweifel dürfte letztlich die Rücksicht auf die ablaufende Wahlperiode des Bundestags ein Grund für die Zustimmung des Bundesrats gewesen sein.

1.3 Datenschutz-Anpassungs- und -Umsetzungsgesetz des Landes Brandenburg

Die europäische Datenschutz-Grundverordnung stellt nicht nur für den Bundesgesetzgeber eine besondere Herausforderung dar. Auch auf Landesebene bedarf es einer Überarbeitung aller den Datenschutz betreffenden gesetzlichen Regelungen, allen voran des Brandenburgischen Datenschutzgesetzes.

Schon im Oktober 2016 wandte sich das zuständige Ministerium des Innern und für Kommunales mit ersten Überlegungen zur Novellierung des Brandenburgischen Datenschutzgesetzes an die Landesbeauftragte. Diese sehr frühe Beteiligung war kein einmaliges Entgegenkommen des Ministeriums gegenüber der Landesbeauftragten, sondern der Beginn eines ausgesprochen transparenten Verfahrens aufseiten der Exekutive. Die Landesbeauftragte erhielt mehrfach Gelegenheit, zum Gesetzentwurf in seinem jeweiligen

Stadium nicht nur schriftlich Stellung zu nehmen, sondern diese Stellungnahmen dem Ministerium auch in Gesprächen zu erläutern. Die Vorschläge und Anregungen der Landesbeauftragten wurden, wenn auch nicht vollständig, so doch zu einem großen Teil aufgegriffen und umgesetzt.

Der Gesetzentwurf wurde am 12. September 2017 in den Landtag Brandenburg eingebracht[21] und dort am 28. September 2017 in erster Lesung behandelt. Die Anhörung zum Gesetzentwurf soll am 1. März 2018 vom Ausschuss für Inneres und Kommunales durchgeführt werden; dort wird auch die Landesbeauftragte Gelegenheit erhalten, nicht berücksichtigte und ihr besonders wichtige Anregungen zur Änderung des Gesetzentwurfs noch einmal vorzutragen. Der Landtag beabsichtigt, das Gesetz so rechtzeitig zu verabschieden, dass es noch vor dem 25. Mai 2018 verkündet werden kann und somit den zeitlichen Vorgaben der Datenschutz-Grundverordnung genügt.

1.4 Gesetz zur Anpassung des bereichsspezifischen Datenschutzrechts des Landes Brandenburg an die Datenschutz-Grundverordnung

Angesichts der bereichsübergreifenden Geltung des Datenschutzes ist es erforderlich, neben der Novellierung des Brandenburgischen Datenschutzgesetzes sämtliche Landesgesetze daraufhin zu überprüfen, ob bzw. inwieweit bestehende Datenschutzbestimmungen anzupassen oder neu aufzunehmen sind.

Das koordinierende Ministerium des Innern und für Kommunales leitete der Landesbeauftragten erstmalig im Oktober 2017 den (Arbeits-)Entwurf eines Gesetzes zur Anpassung des bereichsspezifischen Datenschutzrechts an die Verordnung (EU) 2016/679 zu. Zu dem anschließenden überarbeiteten Entwurf konnte die Landesbeauftragte ebenfalls – neben anderen – Stellung nehmen. Inzwischen liegt der Gesetzentwurf dem Landtag Brandenburg seit dem 15. Januar 2018 vor.[22]

Die in dem Gesetzentwurf vorgesehenen Änderungen in 31 Landesgesetzen finden vielfach in der Weise statt, dass sprachliche Anpassungen an die in der Datenschutz-Grundverordnung verwendeten Begrifflichkeiten vorgenommen werden. Soweit darüber hinausgehende inhaltliche Änderungen vorgesehen sind, wurden die Anregungen und Ergänzungsvorschläge der Landesbeauftragten – anders als in dem Verfahren zur Brandenburgischen Datenschutzgesetz – kaum aufgegriffen. Insoweit ist sie darauf verwiesen, ihre wesentlichen Bedenken im parlamentarischen Gesetzgebungsverfahren einzubringen.

21 Landtags-Drs. 6/7365.

22 Landtags-Drs. 6/7947.

1.5 Ausblick: Forderungen der Datenschutzkonferenz an den Bundestag und die neue Bundesregierung

Anlässlich der Neuwahl des Deutschen Bundestags hat die Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder im Oktober 2017 elf handlungsorientierte Grundforderungen für die neue Legislaturperiode vorgelegt.[23] Sie wurden allen im neuen Bundestag vertretenen Fraktionen zugeleitet und auch der Öffentlichkeit vorgestellt. Es handelt sich um Grundsatzpositionen und Forderungen zum Datenschutz, deren Berücksichtigung und ggf. Umsetzung die Konferenz angesichts der laufenden Diskussionen und rechtlichen wie technischen Entwicklungen als besonders aktuell und vordringlich bewertet. Das Grundsatzpapier soll dazu beitragen, das Datenschutzrecht weiterzuentwickeln sowie dessen Durchsetzung und Akzeptanz zu fördern. Gleichzeitig soll es verdeutlichen, dass ein wirksamer Daten- und zugleich Grundrechtsschutz kein Hindernis für die fortschreitende Digitalisierung sein muss. Vielmehr ist der Datenschutz als integraler und förderlicher Bestandteil politischer, wirtschaftlicher und gesellschaftlicher Fortentwicklung zu verstehen und sollte auch so gelebt werden.

Die einzelnen Grundsatzpositionen betreffen höchst unterschiedliche gesellschaftliche und politische Lebensbereiche, wie beispielsweise die Kriminalitäts- und Terrorismusbekämpfung, den Beschäftigtendatenschutz, die Digitalisierung des Gesundheitswesens („E-Health“), die Auswertung von Gesundheitsdaten („Big Data“) und die Digitalisierung der Verwaltung („E-Government“). Generell fordert die Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder, die Ziele der Datenschutz-Grundverordnung nicht aufzuweichen, sondern sie im Gegenteil weiterzuverfolgen und zu fördern. Letztlich zeigen ihre Grundsatzpositionen, dass mit der zunehmenden Digitalisierung der Gesellschaft bis hinein in die persönlichen Lebensbereiche auch die Notwendigkeit wächst, dem Datenschutz Geltung zu verschaffen und angemessene rechtliche wie technische und organisatorische Maßnahmen zu treffen, um einen angemessenen Ausgleich zwischen dem allgemeinen Interesse an der Datenverarbeitung und der Notwendigkeit des individuellen Grundrechtsschutzes zu finden.

[23] Grundsatzpositionen und Forderungen der Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder für die neue Legislaturperiode vom 16. Oktober 2017, siehe Anlage 1.7.

Bedingt durch das Inkrafttreten der Datenschutz-Grundverordnung und der JI-Richtlinie waren sowohl der Bundesgesetzgeber als auch der Landesgesetzgeber zu erheblichen gesetzgeberischen Aktivitäten aufgefordert. Sowohl das novellierte Bundesdatenschutzgesetz als auch das kurz vor der Verabschiedung stehende neue Brandenburgische Datenschutzgesetz werden rechtzeitig mit dem Wirksamwerden der Datenschutz-Grundverordnung am 25. Mai 2018 in Kraft treten. Auch die Datenschutzbestimmungen in den speziellen Bundes- und Landesgesetzen sind teilweise bereits angepasst. Hier bedarf es aber noch weiterer Anstrengungen, bis der gesamte einschlägige Gesetzesbestand vollständig entsprechend den EU-Vorgaben geändert sein wird.

2 Technisch-organisatorische Entwicklungen

2.1 Elektronische Identitätsnachweise

Am 15. Juli 2017 ist das Gesetz zur Förderung des elektronischen Identitätsnachweises[24] in Kraft getreten. Dadurch soll u. a. die Nutzung der Online-Ausweisfunktion des elektronischen Personalausweises erleichtert werden.

Seit dem Jahr 2010 werden in Deutschland neue Personalausweise ausgegeben, die u. a. eine Funktion zum elektronischen Identitätsnachweis (eID-Funktion) bereitstellen. Gleiches gilt für elektronische Aufenthaltstitel. Bürger sowie aufenthaltsberechtigte Ausländer sollen so die Möglichkeit erhalten, sich mit dem Personalausweis bzw. dem elektronischen Aufenthaltstitel gegenüber Behörden und Unternehmen elektronisch (z. B. über das Internet) auszuweisen. Die eID-Funktion bietet eine sichere und verlässliche gegenseitige Identifizierung zwischen Ausweisinhabern einerseits und Behörden und Unternehmen andererseits. Zur Durchführung eines elektronischen Identitätsnachweises benötigt der Nutzer neben dem neuen amtlichen Dokument mit aktivierter eID-Funktion, ein Ausweislesegerät und eine entsprechende Software. Die Behörde bzw. das Unternehmen weist die Befugnis, Identitätsdaten aus dem neuen Personalausweis auslesen zu dürfen, durch ein so genanntes Berechtigungszertifikat nach, das zuvor vom Bundesverwaltungsamt erteilt wurde.

Das ursprüngliche Ziel des Gesetzgebers, bei der Nutzung elektronischer Behörden- oder Unternehmensdienstleistungen die Identifizierungsfunktion des Personalausweises flächendeckend zum Einsatz zu bringen, konnte

[24] Gesetz zur Förderung des elektronischen Identitätsnachweises vom 7. Juli 2017 (BGBl. I S. 2310).

bislang nicht erreicht werden. Als Gründe werden u. a. die Freiwilligkeit der Freischaltung der eID-Funktion durch den Ausweisinhaber und das aufwendige Verfahren zur Beantragung und Erteilung von Berechtigungszertifikaten genannt.

Vor diesem Hintergrund brachte die Bundesregierung den Entwurf des o. g. Gesetzes in den Bundestag ein, um die Verbreitung und Nutzung der eID-Funktion zu fördern. Er sah eine Reihe von Änderungen u. a. im Personalausweisgesetz und im Aufenthaltsgesetz vor. Zu den wichtigsten gehört, dass die Aktivierung der eID-Funktion auf Ausweisen bzw. Aufenthaltstiteln verbindlich festgeschrieben wird. Der Ausweisinhaber hat keine Möglichkeit mehr, sie zu deaktivieren. Darüber hinaus wurden für Behörden und Unternehmen, die die eID-Funktion in Online-Dienstleistungen nutzen wollen, Vereinfachungen im Verfahren der Beantragung und Erteilung von Berechtigungszertifikaten vorgesehen. Weitere Ziele des Gesetzes waren u. a. die Anpassung des Personalausweisrechts an die Vorgaben der eIDAS-Verordnung der Europäischen Union[25] und die Vereinfachung des Verfahrens zur Ausstellung von Pässen und Personalausweisen.

Die Konferenz der unabhängigen Datenschutzbeauftragten des Bundes und der Länder hat in einer Entschließung[26] zu dem Gesetzentwurf u. a. darauf hingewiesen, dass eine obligatorische Aktivierung der eID-Funktion nur dann hinnehmbar ist, wenn dauerhaft sichergestellt wird, dass ihre Nutzung freiwillig und das Selbstbestimmungsrecht der Bürger gewahrt bleibt. Auch sollten Ausweisbehörden wie bisher verpflichtet sein, Bürger schriftlich und in verständlicher Form über die eID-Funktion zu informieren. Nach Meinung der Konferenz müssen Nutzer vor der Übermittlung ihrer Identitätsdaten aus dem Ausweis über den Zweck und den konkreten Kontext dieser Übermittlung unterrichtet werden sowie die Möglichkeit haben, einzelne Datenkategorien von der Weitergabe auszuschließen. Weiterhin müssen Antragsteller für Berechtigungszertifikate den Datenschutz und die Datensicherheit gewährleisten sowie die Einhaltung der entsprechenden Anforderungen schriftlich bestätigen und nachweisen.

Nicht alle Kritikpunkte der Entschließung wurden im weiteren Gesetzgebungsverfahren berücksichtigt. Insbesondere wurden für Behörden und Unternehmen, die Identitätsdaten aus dem Ausweis auslesen wollen und hierfür ein Berechtigungszertifikat beantragen, Pflichten gegenüber dem Bundesverwaltungsamt zum Nachweis der Gewährleistung von Datenschutz und Datensicherheit sowie zur Information über den Zweck der Identitätsfest-

[25] Verordnung (EU) Nr. 910/2014 des Europäischen Parlaments und des Rates vom 23. Juli 2014 über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt und zur Aufhebung der Richtlinie 1999/93/EG (ABl. EU L 257/73).

[26] Siehe Anlage 1.3.4.

stellung gestrichen. Letzterer muss auch nicht – wie bisher – dem Ausweisinhaber mitgeteilt werden.

Im Land Brandenburg wurden die Arbeiten zur Etablierung einer eID-Infrastruktur, über deren Anfänge wir in unserem letzten Tätigkeitsbericht[27] informiert hatten, wieder aufgenommen und im Rahmen eines kommunalen Pilotprojekts fortgeführt.[28]

Zwar werden mit dem Gesetz zur Förderung des elektronischen Identitätsnachweises einige Vereinfachungen bei der Nutzung der eID-Funktion vorgenommen. Allerdings geht dies zulasten der Transparenz von Datenübermittlungen für Ausweisinhaber sowie des Nachweises der Einhaltung datenschutzrechtlicher Anforderungen bei Inhabern von Berechtigungszertifikaten.

2.2 Risiken von Big-Data-Anwendungen, insbesondere im Gesundheitswesen

Die Digitalisierung schreitet insbesondere im Gesundheitswesen mit wachsender Geschwindigkeit voran. Große Datenmengen werden mit immer komplexeren und effizienteren technischen Systemen verknüpft und analysiert. Gleichzeitig steigt das Risiko, dass personenbeziehbare Daten in unzulässiger Weise verarbeitet werden.

Unter dem Begriff „Big Data“ versteht man die Kumulierung umfangreicher (Volume) strukturierter und unstrukturierter (Variety) Datenmengen sowie deren (wissenschaftliche) Analyse, mit dem Ziel, neue Erkenntnisse zu gewinnen. Technisch basieren Big-Data-Analysen in der Regel auf hoch performanten Rechnersystemen, kombiniert mit leistungsfähigen und spezialisierten Analyseprogrammen. Mechanismen des Cloud Computings ermöglichen zudem eine effiziente Verknüpfung der Ressourcen, mit dem Ergebnis, dass Daten in Echtzeit oder zumindest sehr schnell (Velocity) verarbeitet werden können (3-V-Modell von Gartner).

Mit dem technischen Fortschritt und der umfangreichen Digitalisierung in fast allen Lebensbereichen ist es denkbar, dass Big-Data-Analysen und -Technologien flächendeckend Einzug halten. Aus Gründen des Datenschutzes stehen wir dieser Entwicklung jedoch skeptisch gegenüber, da es u. a. wahrscheinlicher wird, dass Daten ohne erkennbaren Personenbezug auf Grund von Verknüpfungen und Analysen personenbeziehbar werden. Deshalb sollten z. B. bei der Verarbeitung hoch schutzbedürftiger Patientendaten im Gesundheitsbereich nur in Ausnahmefällen Big-Data-Methoden zur Anwendung kommen. Voraussetzung ist, dass sie primär den Patienten dienen

[27] Tätigkeitsbericht 2014/15, B 8.5.

[28] Siehe B 11.5.

und die Prüfungs- und Deutungshoheit bei medizinisch kompetenten Akteuren verbleibt. Dabei darf nicht pauschal von der Nützlichkeit von Big-Data-Verfahren ausgegangen werden, sondern der Nutzen sollte gerade in jedem Einzelfall geprüft werden und sich im Einklang mit den rechtlichen Vorschriften (z. B. Datenschutz-Grundverordnung, Sozialgesetzbuch, Bundesdatenschutzgesetz) befinden. Insbesondere sind die Prinzipien einer informierten Einwilligung, der Datenvermeidung und Datensparsamkeit, der Transparenz, der Erforderlichkeit, des Auskunftsrechts, des Datenschutzes durch Technikgestaltung sowie datenschutzfreundlicher Voreinstellungen und des Verbotes der automatisierten Einzelentscheidung zu berücksichtigen.

Methoden der Anonymisierung und Pseudonymisierung sind in diesem Zusammenhang die wichtigsten Instrumente. Werden sie berücksichtigt und nach dem Stand der Technik implementiert, sind wesentliche datenschutzrechtliche Grundprinzipien – wie Erforderlichkeit und Datensparsamkeit – erfüllt. Erst der Einsatz dieser Verfahren ermöglicht oftmals eine datenschutzgerechte Umsetzung von Big Data bei der Analyse umfangreicher Datenbestände im Gesundheitsbereich. Wie wirksam eine Anonymisierung ist, hängt immer vom Stand der Technik und der Menge der zur Verfügung stehenden Daten ab. Gerade die Verfügbarkeit großer Datenmengen unterschiedlichster Datenquellen, deren Verknüpfung sowie der Einsatz komplexer Analysewerkzeuge und -algorithmen erhöhen das Risiko, dass bei scheinbar anonymisierten Daten der Bezug zu einer Person nachträglich doch herstellbar wird. Die Anonymität ist daher kein statischer Zustand. Das Risiko einer Reidentifizierung muss deshalb regelmäßig ermittelt werden. Welche Technik letztendlich zuverlässig die Kriterien einer wirksamen Anonymisierung erfüllt, sollte immer auf der Grundlage einer Einzelfallentscheidung getroffen werden.

Im medizinischen Bereich kann es auch vorkommen, dass Big-Data-Analysen berechtigterweise personenbezogene Informationen enthalten müssen, um beispielsweise den Patienten über die Analyseergebnisse einer u. U. lebenswichtigen Therapie informieren zu können. Umso notwendiger werden in diesem Fall die umfassende informierte und freiwillige Einwilligung des Patienten. Darüber hinaus können Sicherheitslücken und Angriffe auf große Datenbanken mit sensitiven personenbezogenen Daten weitreichende Konsequenzen für den Schutz der Privatsphäre haben. Es müssen daher erweiterte Anforderungen an die Informationssicherheit von Big-Data-Anwendungen gestellt werden, die mit adäquaten technischen und organisatorischen Maßnahmen umzusetzen sind. Nur mit einer starken Verschlüsselung, geschlossenen und dezentralen Systemen sowie dem Einsatz von Treuhändermodellen kann die im Patientenverhältnis notwendige Vertraulichkeit gewahrt bleiben.

Die Verknüpfung unterschiedlicher Datenbestände einzelner Institutionen und Beteiligter darf aus unserer Sicht zukünftig nur auf Basis spezieller rechtlicher Regelungen erfolgen, da die Verarbeitung von Gesundheitsdaten bisher auf unterschiedlichen Rechtsgrundlagen (z. B. Bundesdatenschutzgesetz, Landesdatenschutzgesetze, Krankenhausgesetz, Sozialgesetzbuch) basiert und diese oftmals nicht den notwendigen Rahmen für Big-Data-Lösungen bieten können. Es gilt, neben den häufig berechtigten Interessen der Gesellschaft, der Behandler, Kostenträger und Forscher, insbesondere die Wahrung der Persönlichkeitsrechte der einzelnen Betroffenen zu beachten und eine angemessene Abwägung zwischen den verschiedenen Interessen zu treffen. Selbst bei einer Datenverarbeitung auf gesetzlicher Grundlage sollte aus Datenschutzgründen regelmäßig der Wille des Einzelnen, ob seine Daten tatsächlich zu einer Datensammelstelle gelangen dürfen, berücksichtigt werden. Beim Widerruf einer Einwilligungserklärung ist zudem immer zu klären, wie eine wirksame und datenschutzgerechte Löschung der personenbezogenen Daten erreicht werden kann. Ein Widerruf sollte jedenfalls nicht dazu führen, dass gerade eine Pseudonymisierung bzw. Anonymisierung der Gesundheitsdaten aufgehoben wird, um diese löschen zu können.

Die Verarbeitung personenbezogener Daten im Big-Data-Umfeld birgt erhebliche Risiken für die Rechte und Freiheiten der Betroffenen. Big-Data-Lösungen sollten, insbesondere im Gesundheitswesen, nur im Einzelfall und unter strenger Beachtung der gesetzlichen Anforderungen und grundlegender Datenschutzprinzipien eingesetzt werden.

2.3 Windows 10

Das weitverbreitete Betriebssystem Windows 10 sammelt eine Vielzahl von teilweise personenbezogenen Daten und sendet diese an den Hersteller Microsoft. Dessen erklärtes Ziel besteht u. a. darin, das Produkt durch die Datenauswertung weiterzuentwickeln und eine verbesserte personalisierte Nutzung zu ermöglichen. Allerdings ist dabei fraglich, ob die Datensammlung und Übermittlung für Anwender hinreichend transparent und konfigurierbar ist.

Das Betriebssystem Windows 10 ist seit Juli 2015 u. a. in den Versionen Home, Pro und Enterprise erhältlich. Insbesondere die Versionen Home und Pro sind auf den Markt der privaten Nutzer ausgerichtet und finden sich daher hauptsächlich auf PCs, Laptops und Tablets für den Heimgebrauch. Die Version Windows 10 Enterprise dagegen wird zumeist auf Computern in Unternehmen eingesetzt. Windows 10 gehört zu den sogenannten clouduntersützten Betriebssystemen.[29]

[29] Tätigkeitsbericht 2014/2015, B 2.5.

Auf jedem Gerät, auf dem Windows 10 installiert ist, sammelt das Betriebssystem kontinuierlich eine Reihe technischer Daten, die als Telemetriedaten bezeichnet und standardmäßig an Microsoft übermittelt werden. Dazu gehören beispielsweise Angaben über die eingerichtete Hard- und Software sowie die mit dem Computer verbundenen Peripheriegeräte (wie z. B. Monitor, Drucker, externe Datenspeicher). Zum Teil werden diese Daten ergänzt um Informationen zur Konfiguration und Nutzung von Apps (wie z. B. Zeitpunkt und Zeitdauer der Nutzung, parallel geladene Programme, Seitenaufrufe in Microsofts App Store). Im Regelfall ist davon auszugehen, dass derselbe Computer meist von derselben Person oder einem kleinen Personenkreis genutzt wird; außerdem kann Microsoft über die enge Integration von nutzerspezifischen Cloud-Diensten (s. u.) im Allgemeinen relativ leicht einen Personenbezug der Daten herstellen – sie sind somit zumindest teilweise datenschutzrelevant.

In den unterschiedlichen Versionen und in Abhängigkeit vom konkreten Aktualisierungsstand des Betriebssystems existieren mehrere, aufeinander aufbauende Telemetriestufen, z. B. „Sicherheit“, „Einfach“ und „Vollständig.“ Dabei umfassen die Telemetriedaten einer höheren Stufe stets die Daten der niedrigeren Stufe(n) und ergänzen diese. Hervorzuheben ist, dass ein einfaches Abschalten der Erhebung und Übermittlung der Telemetriedaten zurzeit in keiner Version von Windows 10 möglich ist. In den Versionen Home und Pro kann zwar der Datenumfang durch Auswahl der Stufe „Einfach“ beschränkt werden, aber auch hier erfolgt noch eine Sammlung und Weiterleitung personenbezogener Daten.

Lediglich in der hauptsächlich von Unternehmen genutzten Version Windows 10 Enterprise lässt sich die Telemetriestufe „Sicherheit“ auswählen. Diese enthält immer noch eine geringe Anzahl gerätespezifischer Informationen sowie Daten zur Erkennung und zum Entfernen von Schadsoftware. Selbst in dieser Version kann die Übertragung von Daten an Microsoft vermutlich nicht vollständig unterbunden werden, zumindest nicht ohne aufwendige Eingriffe in die interne Konfiguration des Betriebssystems und des umgebenden Netzwerkes.

Weiterhin ist festzuhalten, dass bei Neuinstallationen von Windows 10 Home und Pro die Telemetriestufe standardmäßig auf „Vollständig“ gesetzt und durch den Nutzer aktiv geändert werden muss. Insofern ist fraglich, ob Microsoft hiermit das Grundprinzip der datenschutzfreundlichen Voreinstellungen (Data protection by default) einhält. Auch hinsichtlich der Transparenz der Verarbeitung von Telemetriedaten ist Kritik angebracht: Nutzer finden auf den Webseiten der Firma Microsoft zwar Informationen hierüber, diese sind jedoch nur schwer verständlich, z. T. widersprüchlich bzw. nicht auf dem aktuellen Stand sowie an manchen Stellen lediglich beispielhaft und ohne ab-

schließende Nennung der jeweiligen Daten und Datenkategorien bzw. Zwecke der Verarbeitung.

Ein weiterer datenschutzrechtlich relevanter Aspekt von Windows 10 ist seine Cloud-Zentrierung. Viele der neuen und modernen Funktionen wie z. B. die digitale Assistentin Cortana, die Nutzung des Webbrowsers Edge oder des App Stores bedeuten Übertragungen von personenbezogenen Daten in die Microsoft Cloud, also auf Server im Internet mit Standorten u. a. in den USA. Zu diesen Daten können auch sehr sensitive Informationen gehören, etwa über politische und religiöse Überzeugungen, die Gesundheit oder das Sexualleben des Nutzers. Ein Missbrauch kann zu erheblichen Risiken für die informationelle Selbstbestimmung führen. Microsoft selbst sammelt die Daten nicht nur, sondern nutzt sie auch für Zwecke der personalisierten Werbung.

Wiederum sind die Standardeinstellungen für die genannten Dienste in Windows 10 nicht datenschutzfreundlich, da Nutzer bei der Windowsinstallation aktiv Entscheidungen gegen die Cloud-Integration treffen müssen. Die Benutzerführung während der Installation ist im Gegenteil so gestaltet, dass die Cloud-Nutzung als empfohlene Einstellung verstanden werden muss. Dass Windows 10 auch ohne Cloud-Anbindung verwendbar ist, wird eher versteckt und ist für unsichere Nutzer gegebenenfalls nur unter Schwierigkeiten zu verstehen und umzusetzen.

Aus gegenwärtiger Sicht begegnet die Nutzung von Windows 10 Home und Pro als Betriebssystem auf Arbeitsplatz-PCs in Behörden und Unternehmen erheblichen datenschutzrechtlichen Bedenken. Die Sammlung und Übermittlung personenbezogener Nutzungsdaten durch den Hersteller ist aus unserer Sicht nicht erforderlich. Auch mangelt es an einer hinreichenden Transparenz und einfachen Konfigurierbarkeit.

2.4 Modernisierung des IT-Grundschutzes

Der IT-Grundschutz des Bundesamtes für Sicherheit in der Informationstechnik (BSI) ist eine bewährte Methode, um ein angemessenes Informationssicherheitsniveau zu erreichen. Nun wurde er grundlegend überarbeitet. Im Herbst 2017 stellte das BSI modernisierte Bausteine sowie neue Vorgehensweisen vor.

Die neuen BSI-Standards 200-1 (Managementsysteme für Informationssicherheit), 200-2 (IT-Grundschutz-Vorgehensweise) und 200-3 (Risikomanagement) ersetzen die bisherigen Standards 100-1, 100-2 und 100-3. Eine interessante Neuerung der Grundschutz-Vorgehensweise ist dabei die neu eingeführte Unterscheidung zwischen Basis-, Kern- und Standard-Absicherung. Die Standard-Absicherung beschreibt den bei normalem

Schutzbedarf standardmäßig anzustrebenden Schutzgrad. Die anderen beiden Vorgehensweisen sollen einen leichteren Einstieg in den IT-Grundschutz ermöglichen, indem entweder zunächst die wichtigsten Systeme und Prozesse geschützt werden (Kern-Absicherung) oder schnell im gesamten System die grundlegenden Sicherheitsmaßnahmen umgesetzt werden, um den höchsten Risiken vorzubeugen (Basis-Absicherung). Darauf aufbauend ist dann jeweils die vollständige Analyse der Sicherheitsanforderungen anzuschließen, um die Standard-Absicherung zu erreichen. Mit dem "Leitfaden zur Basis-Absicherung" sollen speziell kleine und mittlere Unternehmen in diesem Prozess unterstützt werden.

Die früheren IT-Grundschutzkataloge wurden durch das IT-Grundschutz-Kompendium ersetzt, das die überarbeiteten Bausteine in verschlankter und neu strukturierter Form beinhaltet. Jeder Baustein enthält für einen bestimmten Bereich der Informationssicherheit eine Beschreibung der Gefährdungslage und bewährte Sicherheitsmaßnahmen. Ab Februar 2018 wird das Kompendium als Prüfgrundlage für Zertifizierungen nach IT-Grundschutz dienen.

Aus Sicht des Datenschutzes ist der neue Baustein „CON.2 - Datenschutz“ von besonderem Interesse. Dieser stellt nun eine Verknüpfung zwischen IT-Grundschutz und dem von den Datenschutzbehörden entwickelten Standard-Datenschutzmodell[30] (SDM) her, indem er die vollständige Umsetzung des SDM als Basisanforderung für alle Grundschutzanwender vorschreibt.

Eine wichtige Entwicklung sind die neuen IT-Grundschutz-Profile. Diese sollen von Anwendergruppen erstellt werden und als Schablone für einen bestimmten Einsatzbereich dienen. Beispiele hierfür könnten Kommunalverwaltungen oder auch eine klar abgegrenzte Wirtschaftsbranche sein, die jeweils ähnliche Herausforderungen und Strukturen haben. In den Grundschutz-Profilen soll eine verallgemeinerte Strukturanalyse, Schutzbedarfsfeststellung und Modellierung vorweggenommen, standardisiert dargestellt und so die spätere Anpassung an die eigene Institution mit möglichst geringem Arbeitsaufwand ermöglicht werden. Es laufen bereits verschiedene Initiativen zur Erstellung spezifischer IT-Grundschutz-Profile. Diese werden vom BSI begleitet, das auch über die weiteren Entwicklungen sowie Beteiligungsmöglichkeiten informiert.

30 Tätigkeitsbericht 2014/2015, B 2.2.

Mit den überarbeiteten BSI-Standards und dem neu konzipierten IT-Grundschutz-Kompendium stellt das BSI ein modernisiertes Standardwerk für die Etablierung eines angemessenen Informationssicherheitsniveaus zur Verfügung. Das von den Datenschutzbehörden entwickelte Standard-Datenschutzmodell wird dabei als wichtiges Element mit einbezogen. IT-Grundschutz-Profile für bestimmte Anwendungsbereiche können in Zukunft die Umsetzung unterstützen.

2.5 Praktische Probleme und neue Ansätze bei der Nutzung von Passwörtern

Schlechte oder an mehreren Stellen genutzte Passwörter sind immer noch eine der häufigsten Ursachen für Sicherheitsvorfälle im IT-Bereich. Auch klare Vorgaben zur Länge und Komplexität von Passwörtern werden in der Praxis von Nutzern häufig umgangen.

Eine sichere Authentifizierung der Anwender – meist durch Eingabe eines Passworts – ist die Grundlage für fast alle Sicherheitsmaßnahmen in einer Organisation. Neben einer geregelten Vergabe und Entziehung von Zugriffsrechten sowie der sicheren Speicherung und Übertragung von Zugangsdaten ist dabei die Qualität der genutzten Passwörter ein entscheidender Faktor.

Das Bundesamt für Sicherheit in der Informationstechnik empfiehlt für Passwörter normaler Benutzer eine Mindestlänge von acht Zeichen, darunter Großbuchstaben, Kleinbuchstaben, Sonderzeichen und Zahlen sowie ein Verbot von Trivialpasswörtern und leicht erratbaren Kombinationen wie Namen, Geburtsdaten oder Autokennzeichen. Außerdem ist ein regelmäßiges Wechseln des Passworts zu beachten.

Ein in der Praxis häufig zu beobachtendes Problem ist jedoch, dass die Vorgaben durch Anwender nicht richtig umgesetzt oder sogar bewusst umgangen werden. Rein organisatorische Vorschriften zu sicheren Passwörtern werden oft ignoriert. Aber auch wenn Teile der Vorgaben technisch durchgesetzt werden, heißt das noch nicht, dass daraus tatsächlich sichere Passwörter folgen. Bei erzwungenen Passwortänderungen wird häufig nur eine laufende Nummer geändert. Und auch ein Passwort, das Groß- und Kleinbuchstaben, Zahlen und Sonderzeichen enthält, kann einfach zu erraten sein, wenn es z. B. aus aufeinanderfolgenden Zeichen besteht oder auf einem Wort beruht, das sich im Wörterbuch findet (z. B. „Abc123!“ oder „Passwort1!“).

Um untaugliche Passwörter besser zu erkennen und auszufiltern, sollten also zusätzlich enthaltene Wörter, Namen, aufeinanderfolgende oder sich wiederholende Zeichen automatisch zurückgewiesen werden. Außerdem können

Listen häufig genutzter oder durch Sicherheitsvorfälle an die Öffentlichkeit geratener Passwörter genutzt werden, um schlechte Kennwörter herauszufiltern.

Da vor allem die Notwendigkeit, sich mehrere unterschiedliche Passwörter für verschiedene Aufgaben merken zu müssen, ein Umgehen der Regeln wahrscheinlicher macht, kann es unter Umständen sinnvoll sein, ein Programm zum verschlüsselten Speichern und Verwalten von Passwörtern (Passwort-Manager) zur Verfügung zu stellen. Ein Ansatz zur Verbesserung der Merkbarkeit ist es, auf Vorgaben zu den verwendeten Zeichen (Zahlen, Sonderzeichen etc.) zu verzichten und stattdessen die Mindestlänge deutlich zu erhöhen sowie die beschriebenen Filter gegen bekannte Passwörter anzuwenden. Als Richtlinie in Organisationen ist dies allerdings bisher in Deutschland keine offizielle Empfehlung.

Bei hohem Schutzbedarf und insbesondere bei Anmeldung aus einem externen Netz heraus sollte vor allem zur Authentifizierung von Nutzern nicht nur ein Passwort, sondern zusätzlich ein im Besitz des Nutzers befindliches Hardware-Element (Security Token) erforderlich sein, wie etwa eine Chipkarte (Zwei-Faktor-Authentifizierung).

Daneben fällt der Sensibilisierung von Mitarbeitern eine essenzielle Rolle zu, denn ohne ihre aktive Mithilfe bringen die Vorgaben wenig. Die Relevanz sicherer Authentifizierung muss daher immer wieder deutlich gemacht werden. Der Unterschied zwischen einem sicheren und einem unsicheren Passwort ist nicht immer intuitiv erkennbar, daher sind neben festen Vorgaben auch Hilfestellungen und Ansprechpartner wichtig.

Ein durchdachtes und auf die Anwender sowie den Schutzbedarf zugeschnittenes Konzept zur Authentifizierung ist insbesondere bei erhöhten Sicherheitsanforderungen essenziell für alle weiteren Schutzmaßnahmen. Soweit möglich sollten gute Passwörter technisch erzwungen werden, gleichwohl ist für die konsequente Beachtung der Vorgaben die Sensibilisierung der Mitarbeiter unverzichtbar.

2.6 BSI-Mindeststandards für die Verwaltung mobiler Endgeräte

Wenn in Behörden und Unternehmen mobile Endgeräte eingesetzt werden sollen, müssen sie in die IT-Sicherheitsstruktur der verantwortlichen Stelle eingebunden werden. Hierfür wird in der Regel eine Software zur Verwaltung der Mobilgeräte eingesetzt, ein sog. Mobile Device Management (MDM). Das Bundesamt für Sicherheit in der Informationstechnik (BSI) hat hierzu einen Mindeststandard herausgegeben.

Von Mobile Device Management-Software verwaltete mobile Endgeräte sind in der Regel Smartphones und Tablets. Tragbare Computer (Laptops) liegen außerhalb des Fokus.

Der Mindeststandard benennt eine Reihe funktionaler Sicherheitsanforderungen, die ein MDM erfüllen muss. Dazu gehören unter anderem:

- zentrale Verteilung, Installation und Deinstallation von Applikationen und Updates auf den Mobilgeräten aus der Ferne („Over The Air“ – OTA),
- Protokollierung der Konfigurationshistorie und der sicherheitsrelevanten Ereignisse inkl. Abrufmöglichkeit der aktuellen Gerätekonfiguration,
- Erstellung von sicheren Konfigurationsprofilen, die von den Nutzern nicht verändert werden können,
- Einrichtung und wirksame Durchsetzung komplexer Kennwörter und Gerätecodes inkl. Vorgaben zur Anzahl der möglichen Fehleingaben, nach denen die Daten automatisch vom Gerät gelöscht werden,
- Möglichkeit zur Fernlöschung (Remote Wipe),
- Einrichtung und wirksame Durchsetzung automatischer Gerätesperren nach Zeitvorgabe,
- Aktivierung der Geräteverschlüsselung.

Zudem sollte ein MDM vollständig und nachvollziehbar dokumentiert sein, sodass unter anderem deutlich wird, welche Betriebssystemversionen der mobilen Endgeräte unterstützt werden, welche Funktionalitäten das MDM bietet, welche Schutzeinrichtungen für personenbezogene Daten und für die Verwaltung von kryptografischem Material (wie Zertifikaten, Schlüsseln und Kennwörtern) sowie welche Protokolle und Kanäle zur sicheren Kommunikation vorhanden sind. Wichtig ist auch die Angabe, wie Jailbreak- und Rooting-Aktivitäten auf den verwalteten Geräten verhindert werden und wie die Applikationsverteilung bzw. Identifikation freigegebener Applikationen funktioniert.

Neben Vorgaben zu Anforderungen an sichere Mobile Device Management-Software gibt der BSI-Mindeststandard auch Empfehlungen zu den jeweiligen technischen und organisatorischen Maßnahmen für den sicheren Betrieb eines MDM. Er richtet sich zwar an Stellen des Bundes, kann jedoch auch Hilfestellung und Anregung für andere verantwortliche Stellen bei der Umsetzung der Informationssicherheit für mobile Endgeräte sein.

Verantwortliche Stellen, die mobile Endgeräte wie Smartphones und Tablets einsetzen, sollten sich im aktuellen Mindeststandard des BSI für Mobile Device Management über technische und organisatorische Kriterien zur Auswahl und zum sicheren Einsatz eines MDM informieren und eine Anwendung des Standards in ihrer Institution prüfen.

2.7 Datenschutz im Kraftfahrzeug – automatisiertes und vernetztes Fahren

Die Kraftfahrzeuge der Zukunft werden sich nach dem Willen von Wirtschaft und Politik erheblich von herkömmlichen Autos unterscheiden: Sie können automatisch untereinander und mit der Verkehrsinfrastruktur kommunizieren, um sich z. B. über Staus, Verkehrshindernisse oder andere Gegebenheiten zu informieren oder eine Fahrstrecke automatisiert ohne Zutun der menschlichen Fahrzeugführer fahren. In jedem Fall werden immense Datenmengen erzeugt, die zum großen Teil unter das Datenschutzrecht fallen.

Bereits heute kann ein Kraftfahrzeug als großes Computernetzwerk auf Rädern angesehen werden. In einer Vielzahl von elektronischen Komponenten und Steuergeräten werden unzählige Daten generiert und verarbeitet, die zu einem großen Teil als personenbezogen anzusehen sind. Die Entwicklung und Einführung vernetzter Fahrzeuge führt damit zu datenschutzrechtlichen Herausforderungen, da die Gefahr der Erstellung personenbezogener Bewegungs- und Verhaltensprofile besteht.

In der Europäischen Union wird seit einigen Jahren die Strategie „Cooperative Intelligent Transport Systems (C-ITS)“ vorangetrieben. Danach sollen Fahrzeuge zukünftig mit der Verkehrsinfrastruktur und untereinander Nachrichten austauschen, um sich gegenseitig über die Umgebung und den eigenen Zustand zu informieren. Ziel ist es, Staus und Unfälle zu vermeiden und den Verkehrsfluss zu verbessern. Die ausgetauschten Nachrichten enthalten Daten wie Geschwindigkeit, Geoposition, Beschleunigung und Lenkverhalten und sollen den Empfängerkomponenten die Erstellung eines Verkehrslagebildes ermöglichen, sodass auf bestimmte Verkehrssituationen geeignet reagiert werden kann. Beispiele für die geplanten ersten Dienste, die auf der C-ITS-Strategie basieren, sind die Warnung vor langsamen oder stehenden Fahrzeugen, vor Straßenarbeiten, vor Einsatzfahrzeugen oder die Anzeige von Verkehrszeichen im Fahrzeug.

Technische Nachrichtenformate für derartige Dienste wurden bereits festgelegt. Dazu zählen die „Cooperative Awareness Message (CAM)“ und die „Decentralized Environmental Notification Message (DENM)“. DENMs werden in potenziell gefährlichen Situationen versandt und beinhalten Nachrich-

ten über Typ und Ort des Verkehrsereignisses wie z. B. Staus, Verkehrshindernisse oder schlechte Wetterbedingungen. Wegen ihrer ereignisorientierten Aussendung und des fehlenden Personenbezugs sind sie datenschutzrechtlich unproblematisch. CAMs dagegen werden von Fahrzeugen oder Infrastrukturkomponenten regelmäßig in kurzen Zeitabständen von 0,1 bis 1 Sekunde verschickt und enthalten unter anderem Informationen über Ort, Geschwindigkeit, Länge und Breite der absendenden Station. Zur Sicherstellung von Authentizität, Integrität und Pseudonymität werden sie mit wechselnden Zertifikaten digital signiert. Allerdings sind sie dennoch datenschutzrechtlich problematisch, da sie unverschlüsselt übertragen werden und Kennungen sowie andere statische Informationen enthalten, über die eine Identifizierung von Fahrzeugen möglich ist. Die Zuordnung zu Personen und die Erstellung von Bewegungs- und Verhaltensprofilen können eine Folge sein. Um dem entgegenzuwirken, sollten die Prinzipien der Datenminimierung, der Transparenz und der datenschutzfreundlichen Voreinstellungen eingehalten werden. Eine Aufzeichnung von CAMs sollte technisch verhindert und den Nutzern die Möglichkeit der Deaktivierung des Versands von CAMs eingeräumt werden.

Datenschutzrechtlich ebenfalls relevant ist die Entwicklung hoch- und vollautomatisierter Fahrzeuge. Nur durch eine erhebliche Menge an Sensoren und Kameras im und am Fahrzeug können diese Automobile alle erforderlichen Daten zur Bestimmung des eigenen Zustands und der Verkehrsumgebung erhalten, um daraus die richtigen Entscheidungen für ihre Steuerung ableiten zu können. Aufgrund einer Novellierung des Straßenverkehrsgesetzes im Jahr 2017[31] müssen bei Nutzung automatisierter Fahrfunktionen auf Deutschlands Straßen Daten in einer Blackbox aufgezeichnet werden, mit denen sich nach einem Unfall klären lassen kann, ob die Technik und damit der Hersteller oder der Fahrer für einen Unfall verantwortlich war. Welche Daten dies sind und wie das Speichermedium ausgestaltet werden soll, bleibt ungeregelt.

Die Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder hat dies in einer Entschließung[32] kritisiert und darauf hingewiesen, dass in Kraftfahrzeugen mit hoch- oder vollautomatisierter Fahrfunktion die Gefahr elektronischer Fahrtenschreiber besteht, mit denen personenbezogene Profile gebildet werden können. Sie fordert u. a., Folgendes klar zu regeln:

- die abschließende Aufzählung derjenigen Daten, die aufgezeichnet und gespeichert werden dürfen,

31 Achtes Gesetz zur Änderung des Straßenverkehrsgesetzes vom 16. Juni 2017 (BGBl. I S. 1648).

32 Siehe Anlage 1.3.2.

- die Bestimmung des für die Verarbeitung Verantwortlichen,
- die Ergänzung einer Übermittlungs-/Zugriffsregelung für den Fahrer/Halter,
- die datenschutzgerechte Ausgestaltung des Speichermediums, insbesondere die Festlegung einer angemessenen Speicherdauer anhand der Erforderlichkeit und des Zwecks der Beweisführung für die Haftung,
- die Konkretisierung der Zwecke für die Übermittlung der gespeicherten Daten,
- die Nennung des Adressaten für das Übermittlungsverlangen,
- die abschließende Nennung berechtigter Übermittlungsempfänger und ihrer jeweiligen Verarbeitungsbefugnisse mit im Übrigen strikter Zweckbindung und
- die Konkretisierung des Löschzeitpunkts der übermittelten Daten.

Dass eine gesetzliche Regelung zur Datenverarbeitung in vernetzten und teilautonomen Fahrzeugen möglich ist, die IT-Sicherheits- und Datenschutz-Aspekte gleichermaßen berücksichtigt, zeigt der sog. Self-Drive Act, den das US-Repräsentantenhaus im September 2017 verabschiedet hat.

Bei der Weiterentwicklung von Kraftfahrzeugen zu automatisierten und vernetzten Automobilen müssen die dabei anfallenden großen Datenmengen weitgehend als personenbezogen angesehen werden. Eine Berücksichtigung der datenschutzrechtlichen Vorgaben ist für Hersteller und Politik daher unumgänglich. Sowohl auf technischer als auch auf rechtlicher Ebene besteht allerdings noch ein erheblicher Nachbesserungsbedarf, um das Grundrecht auf Datenschutz für die Nutzer ausreichend sicherzustellen.

2.8 RFID-Anwendungen in der Praxis – Bargeldlose Zahlungen auf Musikfestivals

Im Berichtszeitraum informierte uns ein Bürger darüber, dass der Veranstalter eines Musikfestivals bargeldlose Bezahlvorgänge mit Hilfe von in Armbändern integrierten RFID-Chips (RFID – Radio Frequency Identification) umsetzt. Hierzu wurde beim Kauf der Festivaltickets ein einzurichtendes Guthabenkonto des Käufers mit der eindeutigen Nummer eines RFID-Chips verknüpft, sodass beim Erwerb weiterer Dinge vor Ort (z. B. Getränke, Speisen, Fan-Artikel) nur der Chip ausgelesen werden

musste und die Bezahlung über eine Abbuchung vom Guthabenkonto erfolgte.

Weder auf der Internetseite des Festivalveranstalters noch auf der des Dienstleisters für die Abwicklung der Bezahlvorgänge war eine ausreichende Beschreibung der Verarbeitung der personenbezogenen Daten entsprechend den Anforderungen des Bundesdatenschutzgesetzes (BDSG) vorhanden. Auch die Datenschutzbestimmungen des Dienstleisters konnten nicht eingesehen werden, da die entsprechende Verknüpfung in dessen Internetauftritt nicht aktiv war.

Gemäß § 6c Abs. 1 BDSG sind Diensteanbieter bei der Nutzung von mobilen personenbezogenen Speicher- und Verarbeitungsmedien verpflichtet, den Betroffenen in allgemein verständlicher Form über die Funktionsweise des Mediums einschließlich der Art der verarbeiteten Daten zu unterrichten. Weiterhin müssen sie darüber aufklären, wie Nutzer ihre Rechte nach §§ 19, 20, 34 und 35 BDSG ausüben können, sowie welche Maßnahmen bei Verlust oder Zerstörung des Mediums zu treffen sind.

Nachdem wir mit dem Festivalveranstalter Kontakt aufgenommen und ihn auf seine Informationspflichten hingewiesen hatten, stellte dieser umgehend die Datenschutzrichtlinie für die Nutzung der auf dem Festival verwendeten RFID-Chips online bereit. Außerdem übergab er uns auch die Vertragsunterlagen zur Auftragsdatenverarbeitung gemäß § 11 BDSG durch seinen Dienstleister für die Abwicklung der Bezahlvorgänge.

Mithilfe der Unterlagen konnten wir nachvollziehen, dass für die Abwicklung der Bezahlvorgänge nur die eindeutige Nummer des RFID-Chips sowie das jeweils entstehende Umsatzvolumen genutzt wurden. Auf dem Chip erfolgte keine Speicherung weiterer personenbezogener Daten. Sowohl der Veranstalter als auch dessen Dienstleister kamen ihren Informationspflichten somit nach.

Grundsätzlich ist darauf hinzuweisen, dass beim Einsatz mobiler personenbezogener Speicher- und Verarbeitungsmedien je nach Gestaltung des konkreten Systems ggf. die Möglichkeit der Überwachung des Verhaltens oder der Bildung von Bewegungsprofilen Betroffener bestehen kann. Für die Erbringung der Dienste ist eine solche Verarbeitung in der Regel nicht erforderlich und damit ohne explizite Einwilligung der Betroffenen datenschutzrechtlich unzulässig. Betreiber müssen das unbefugte Auslesen der Daten aus den Medien ggf. mit technischen und organisatorischen Maßnahmen ausschließen.

Ein bargeldloser Zahlungsverkehr bei öffentlichen Veranstaltungen über in Armbändern integrierte RFID-Chips kann ein Mehr an Sicherheit und Schutz vor Diebstahl bieten. Betroffene sind jedoch im Vorfeld über die Art und die Funktionsweise der verwendeten Technik und die Verarbeitung ihrer personenbezogenen Daten zu informieren.

2.9 Mängel bei Verträgen zur Auftragsdatenverarbeitung

Die Auslagerung der Verarbeitung von personenbezogenen Daten einer verantwortlichen Stelle an andere Personen oder Stellen wird als Datenverarbeitung im Auftrag bezeichnet. Sie darf nur auf der Basis schriftlicher vertraglicher Regelungen erfolgen. Im Zuge der Beratung und Kontrolle öffentlicher Stellen des Landes fallen uns hierbei häufig Mängel auf.

Die wesentlichen Anforderungen an Auftragsdatenverarbeitungsverhältnisse öffentlicher Stellen werden im § 11 Brandenburgisches Datenschutzgesetz (BbgDSG) beschrieben. Insbesondere bleibt die Auftrag gebende Stelle für die Verarbeitung der personenbezogenen Daten verantwortlich. Der Auftragnehmer darf die Daten nur auf Weisung des Auftraggebers verarbeiten. Er muss die Vorschriften des Gesetzes beachten und jederzeit Kontrollen des Auftraggebers ermöglichen. Gegenstand und Umfang der Auftragsdatenverarbeitung, technisch-organisatorische Maßnahmen und ggf. Unterauftragsverhältnisse sind im Rahmen des Vertrags schriftlich festzulegen.

In der Praxis ist häufig festzustellen, dass öffentliche Stellen des Landes ihrer Verantwortung bei der Formulierung der erforderlichen Vereinbarungen nicht in vollem Umfang gerecht werden. Sie möchten gern eine angebotene Dienstleistung nutzen, unterwerfen sich dabei allerdings den Geschäftsbedingungen und Datenschutzvorgaben des Auftragnehmers, indem sie vorgefertigte Verträge akzeptieren.

Zwar ist es aus praktischer Sicht nachvollziehbar, dass der Dienstleister vorformulierte und für viele Kunden gleichlautende Verträge verwenden möchte. Allerdings entstehen dadurch mehrere Probleme. Zum einen ist dem Auftragnehmer oft nicht bewusst, nach welcher Rechtsgrundlage sich der Vertrag zur Auftragsdatenverarbeitung richtet und welche Folgen damit verbunden sind. In den meisten Fällen werden die Regelungen des Bundesdatenschutzgesetzes angeführt – diese sind aber für die öffentlichen Stellen des Landes Brandenburg nicht anwendbar. Der vorgefertigte Vertrag ist für sie somit nicht nutzbar.

Als weiteres Problem lässt sich die Ausrichtung der Vertragsinhalte zugunsten des Diensteanbieters identifizieren. In mehreren Fällen mussten wir

anhand vorgelegter Verträge feststellen, dass diese einseitig anbieterorientiert formuliert waren und die Rechtsposition der öffentlichen Stelle als Auftraggeber schwächten. Eine angebotene Leistung wurde nur zu konkreten, durch den Auftragnehmer bestimmten Bedingungen umgesetzt. Dies ist insbesondere bei solchen Diensteanbietern problematisch, die spezielle Fachanwendungen bereitstellen oder eine Monopolstellung haben.

Öffentliche Stellen des Landes, die personenbezogene Daten im Auftrag verarbeiten lassen wollen, müssen immer prüfen, ob die Einhaltung der gesetzlichen Anforderungen von § 11 BbgDSG vertraglich fixiert ist. Sie sind in diesem Zusammenhang gehalten, die ihnen zustehenden Kontrollrechte gegenüber dem Auftragnehmer konsequent auszuüben. Auch in diesem Punkt mussten wir feststellen, dass häufig Defizite bestehen und Kontrollen gar nicht oder erst im Fall von Vorkommnissen durchgeführt wurden.

Mit der im Mai 2018 wirksam werdenden Datenschutz-Grundverordnung (DS-GVO) wird auch ein einheitlicher Rechtsrahmen für die Gestaltung und Umsetzung von Auftragsverarbeitungstätigkeiten geschaffen. Alle Auftraggeber und Auftragnehmer müssen dann die Anforderungen insbesondere von Art. 28 DS-GVO beachten und ihre Verträge entsprechend gestalten. Unterschiedliche Vorschriften, wie sie zurzeit in Bund und Ländern bestehen, entfallen dann.

Lässt eine öffentliche Stelle personenbezogene Daten im Auftrag verarbeiten, bleibt sie weiterhin verantwortlich. Es ist unerlässlich, die jeweiligen rechtlichen Regelungen zu beachten und u. a. den Gegenstand, die Dauer, die Art und den Umfang der Auftragsdatenverarbeitung, die erforderlichen technisch-organisatorischen Maßnahmen sowie die Rechte und Pflichten der Vertragspartner festzuschreiben.

2.10 E-Postbrief der Deutschen Post AG

Mit dem Verfahren E-Postbrief stellt die Deutsche Post AG einen elektronischen Dienst bereit, der die Abwicklung des bisher in Papierform durchgeführten Schriftverkehrs vereinfachen soll. Falls der vorgesehene Empfänger eine elektronische E-Post-Adresse besitzt, wird ihm die Nachricht auf elektronischem Weg verschlüsselt zugestellt. Anderenfalls wird sie von einem Tochterunternehmen der Deutschen Post AG ausgedruckt, kuvertiert und als herkömmlicher Brief an die postalische Adresse versendet. Im Berichtszeitraum erhielten wir Anfragen mehrerer Kommunen, unter welchen datenschutzrechtlichen Voraussetzungen dieser Dienst genutzt werden kann.

Datenschutzrechtlich ist die Inanspruchnahme der Dienstleistung (entweder elektronische Zustellung oder Druck-, Kuvertier- und Versanddienst) als Datenverarbeitung im Auftrag zu betrachten. Hierbei sind die Regelungen des § 11 Brandenburgisches Datenschutzgesetz (BbgDSG) einzuhalten. Grundsätzlich war sich die Deutsche Post AG dessen zwar bewusst, verwies jedoch in den entsprechenden vertraglichen Unterlagen lediglich auf das Bundesdatenschutzgesetz. Damit war eine Nutzung durch brandenburgische Kommunen nicht möglich. Mit Änderung der Geschäftsbedingungen wurden die landesrechtlichen Vorschriften Brandenburgs nunmehr anerkannt und dieser Mangel beseitigt.

Zu klären war weiterhin die Frage, für welche Datenkategorien die Nutzung des E-Postbriefs der Deutschen Post AG (bzw. auch vergleichbarer Produkte anderer Diensteanbieter) überhaupt datenschutzrechtlich zulässig ist. Insbesondere wollten die Kommunen hoch schutzbedürftige personenbezogene Daten versenden, u. a. Daten, die Privatgeheimnisse gemäß § 203 Strafgesetzbuch darstellen, dem Steuergeheimnis gemäß § 30 Abgabenordnung oder dem Sozialgeheimnis gemäß § 35 Erstes Buch Sozialgesetzbuch unterliegen.

Im Ergebnis ist der Einsatz des Verfahrens E-Postbrief grundsätzlich auch für die Zustellung hoch schutzbedürftiger personenbezogener Daten zulässig, soweit der Datenverarbeitung im Auftrag nicht spezialgesetzliche Regelungen ausdrücklich entgegenstehen oder deren Bedingungen erfüllt werden. Als weitere Voraussetzung sind sowohl beim Auftraggeber (der Kommune) als auch beim Auftragnehmer (der Deutschen Post AG und ggf. ihrem Unterauftragnehmer) technische und organisatorische Maßnahmen gemäß § 10 BbgDSG umzusetzen, die dem Schutzzweck angemessen sind und sich nach den im Einzelfall zu betrachtenden Risiken sowie dem jeweiligen Stand der Technik richten. Die Maßnahmen sind im Rahmen eines Sicherheitskonzepts gemäß § 7 Abs. 3 BbgDSG zu beschreiben. Sollen hoch schutzbedürftige Daten verarbeitet werden, sind die besonderen Risiken im Konzept zu berücksichtigen und entsprechend zusätzliche Maßnahmen umzusetzen.

Gerade die Prüfung der Datenschutz- und Informationssicherheitskonzepte des Verfahrens E-Postbrief stellt die Kommunen und die Aufsichtsbehörden für den Datenschutz vor große Herausforderungen. Durch die Deutsche Post AG wurden bisher lediglich verschiedene Zertifikate (z. B. nach ISO 27001 auf der Basis von IT-Grundschutz oder TÜV-IT) vorgelegt, mit denen die Beherrschung der Risiken insbesondere bei der Verarbeitung von Daten hohen Schutzbedarfs nicht vollumfänglich nachgewiesen werden konnte. Insofern besteht ein weiterer Prüfbedarf sowohl der Konzepte als auch ihrer Umsetzung.

Nach Rücksprache mit der Deutschen Post AG werden dem Arbeitskreis Verwaltungsmodernisierung der Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder die erforderlichen Unterlagen zur abschließenden datenschutzrechtlichen Bewertung vorgelegt.

Die Nutzung des E-Postbriefs (bzw. vergleichbarer Dienste zur Zustellung von behördlichem Schriftverkehr) ist als Datenverarbeitung im Auftrag zu klassifizieren. Eine solche ist nur möglich, wenn spezialgesetzliche Vorschriften ihr nicht ausdrücklich entgegenstehen und darüber hinaus dem Schutzbedarf angemessene technische und organisatorische Maßnahmen beim Auftraggeber und Auftragnehmer umgesetzt werden.

3 Arbeit und Soziales

3.1 Prüfungen kommunaler Jobcenter

Im vorigen Berichtszeitraum prüften wir insgesamt sechs kommunale Träger der Grundsicherung für Arbeitssuchende (Jobcenter) im Land Brandenburg. Dabei stellten wir teils erhebliche Mängel im technischen und organisatorischen Datenschutz sowie bei der Erfüllung von Dokumentationspflichten fest, deren Behebung wir einforderten.[33] Die Ergebnisse sind insgesamt nicht zufriedenstellend. Ähnliches zeigte sich bei der Prüfung eines weiteren Jobcenters, die wir im Berichtszeitraum durchführten.

In sieben brandenburgischen Landkreisen nehmen die Jobcenter selbstständig die Aufgaben nach dem Zweiten Buch Sozialgesetzbuch (SGB II) wahr. Sie sind jeweils die für die Einhaltung des Datenschutzes verantwortliche Stelle. Damit tragen sie selbst die Verantwortung für eine zulässige Erhebung, Verarbeitung und Nutzung von Sozialdaten und haben die Pflicht, Datensicherungsmaßnahmen zu ergreifen.

Gemäß § 78a Zehntes Buch Sozialgesetzbuch sind kommunale Jobcenter verpflichtet, technische und organisatorische Maßnahmen zu treffen, um die Ausführung der Vorschriften dieses Gesetzbuches, insbesondere die in der Anlage zu dieser Vorschrift genannten Anforderungen zu gewährleisten. Darüber hinaus muss gemäß § 7 Abs. 3 Brandenburgisches Datenschutzgesetz vor dem erstmaligen Einsatz oder der wesentlichen Änderung eines Verfahrens eine schriftliche Freigabe erfolgen. Diese darf nur erteilt werden, wenn ein aus einer Risikoanalyse entwickeltes Sicherheitskonzept ergeben hat, dass die von dem Verfahren ausgehenden Gefahren für die Rechte und

[33] Tätigkeitsbericht 2014/2015, A 3.2, B 3.1.

Freiheiten der Betroffenen durch technisch-organisatorische Maßnahmen beherrscht werden können. Darüber hinaus ist hier eine Vorabkontrolle durch den jeweiligen behördlichen Datenschutzbeauftragten erforderlich.

3.1.1 Weitere Entwicklungen im Ergebnis der früheren Prüfungen

In unserem letzten Tätigkeitsbericht[34] hatten wir für die ersten Prüfungen ausführlich dargestellt, welche Mängel im technischen und organisatorischen Datenschutz festgestellt worden waren. Viele der dort aufgeführten Punkte sind nach nunmehr über zwei Jahren weiterhin offen.

Nach unserer Aufforderung haben zwar alle betroffenen Jobcenter damit begonnen, ein IT-Sicherheitskonzept zu erstellen und damit einen wichtigen Schritt hin zu einem gesetzeskonformen Verfahrensbetrieb getan. Fast alle bisher von uns geprüften Sicherheitskonzepte weisen jedoch weiterhin große Lücken auf. Wichtige Maßnahmen wurden entweder in die ferne Zukunft verschoben oder ganz ausgespart. Eine erweiterte Risikoanalyse, die auf den hohen Schutzbedarf der verarbeiteten Sozialdaten eingeht und nachvollziehbar macht, dass die vorgenommenen Maßnahmen ausreichen, fehlt meist vollständig. Ein IT-Sicherheitskonzept, das auch eine erweiterte Risikoanalyse enthält, wird von uns aktuell noch geprüft.

Auch beim Einsatz von dem Stand der Technik entsprechender Verschlüsselung hat sich wenig getan. Weiterhin speichern alle Jobcenter die Sozialdaten der Fachverfahren im Klartext. Auch bei der verschlüsselten Übertragung von personenbezogenen Daten wurden kaum Fortschritte erreicht. Zum aktuellen Zeitpunkt hat nur eines der Jobcenter, wie von uns gefordert, ein Kryptokonzept vorgelegt, das den Einsatz von Verschlüsselung systematisch dokumentiert und Umsetzungspläne festhält.

In allen geprüften Jobcentern stellten wir fest, dass eine datenschutzgerechte Protokollierung im Verfahren nicht gewährleistet ist. Unsere Forderung nach dienstlichen Regelungen, die bestimmen, was genau protokolliert wird, sowie wer die Protokolle unter welchen Umständen auswerten darf, wurde nur teilweise umgesetzt. Technische Maßnahmen zur Sicherung von Revisionssicherheit, Zugriffsbeschränkungen und Auswertbarkeit wurden nicht, wie gefordert, vorgenommen.

Die von uns angemahnte Vergabe abgestufter Lese- und Schreibrechte, die sich auf das zur Aufgabenerfüllung der Mitarbeiter notwendige Maß beschränken, stieß auf großen Widerstand. Oft wurde uns mitgeteilt, dass der Verwaltungsaufwand zu hoch sei, wenn im Falle von Vertretungen kurzfristig Lese- und Schreibrechte geändert werden müssten. Einzelne Jobcenter

[34] Tätigkeitsbericht 2014/2015, A 3.2.

haben kleine Verbesserungen vorgenommen, wie die Unterteilung eines Standortes in zwei Teams mit unterschiedlichen Zugriffsrechten. Weitere Einschränkungen wurden mit Verweis auf die mangelnde Unterstützung in der genutzten Software kategorisch abgelehnt. Unsere Auffassung ist weiterhin, dass der Zugriff auf sensitive Sozialdaten den Mitarbeitern nur so weit möglich sein darf, wie es für die Erfüllung ihrer Aufgaben im Rahmen der Leistungsgewährung nach dem Zweiten Buch Sozialgesetzbuch unbedingt notwendig ist.

Verbesserungen wurden dahingehend erreicht, dass die meisten Jobcenter inzwischen geregelte Verfahren etabliert haben, um personenbezogene Daten, deren Kenntnis nicht mehr erforderlich ist, zu löschen. Auch unsere Forderungen zur automatischen Umsetzung von Vorgaben für sichere Passwörter wurden größtenteils realisiert.

Die Zusammenarbeit mit den Jobcentern zur Behebung der Mängel gestaltete sich insgesamt schwierig. Informationen und Verbesserungen folgten häufig erst nach mehrfacher Aufforderung, auf einige Forderungen wurde gar nicht eingegangen. Als Grundproblem zeigte sich, dass in allen Fällen das Verfahren in Betrieb genommen wurde, ohne vorher die Einhaltung des Datenschutzes sicherzustellen. Nachträgliche Verbesserungen sind nun aufgrund der Abhängigkeit von der verwendeten Software nur mit großem Aufwand erreichbar.

Deutlich wurde auch, dass bei den verantwortlichen Stellen Fragen der Informationssicherheit und des Datenschutzes häufig keine hohe Priorität haben. So sind die IT-Abteilungen der betroffenen Landkreise meist nicht mit ausreichenden personellen und finanziellen Ressourcen ausgestattet, um ihre Aufgaben angemessen erfüllen zu können. Die Landkreise sind daher aufgefordert, für eine bessere personelle Ausstattung der zuständigen Abteilungen zu sorgen und diese im erforderlichen Umfang zu unterstützen.

3.1.2 Prüfung eines weiteren Jobcenters

Im Berichtszeitraum prüften wir ein weiteres Jobcenter unter besonderer Berücksichtigung der bisher aufgetretenen Problemfelder im technischen und organisatorischen Datenschutz sowie der datenschutzgerechten Aktenführung.

3.1.2.1 Technische und organisatorische Maßnahmen

Ein verfahrensspezifisches IT-Sicherheitskonzept konnte uns im Vorfeld der Prüfung nicht vorgelegt werden. Ein übergreifendes Sicherheitskonzept für die Infrastruktur des Landkreises existierte zwar, wies aber noch erhebliche Lücken auf. Wie bei den bisherigen Prüfungen wurde das Fachverfahren

eingeführt, ohne dass vorher eine Risikoanalyse und eine Vorabkontrolle stattfanden.

Die in der Folge aufgetretenen Mängel sind trotz der Verwendung eines alternativen Softwareprodukts denen, die in anderen Jobcentern festgestellt wurden, sehr ähnlich. Sie betreffen unter anderem die Verschlüsselung von Sozialdaten, die Rechtevergabe, die Verwendung sicherer Passwörter sowie die datenschutzgerechte Protokollierung.

Wir haben die Verantwortlichen aufgefordert, die beschriebenen Mängel zeitnah zu beheben und uns darüber zu informieren.

3.1.2.2 Aktenführung

Bereits in unserem letzten Tätigkeitsbericht[35] erläuterten wir die datenschutzrechtlichen Anforderungen an eine korrekte Aktenführung und die Erforderlichkeit der Vorlage einzelner Unterlagen.

Der Grundsatz der Datenvermeidung und Datensparsamkeit gilt als allgemeines Regelungsprinzip bei jeder Datenerhebung, -verarbeitung und -nutzung. Er verpflichtet jede verantwortliche Stelle, somit auch die Jobcenter, ihre Prozesse sowie die hierfür genutzten IT-Systeme so auszuwählen und zu gestalten, dass so wenig personenbezogene Daten wie möglich verwendet werden.

Der Antragsteller ist nur zur Vorlage von Dokumenten verpflichtet, die das Jobcenter für seine Aufgabenerfüllung nach dem Zweiten Buch Sozialgesetzbuch unbedingt benötigt. Kopien dieser Dokumente dürfen nur in dem Umfang angefertigt werden, wie es für die weitere Bearbeitung der Anträge erforderlich ist. Die anschließende Speicherung der Dokumente in den Akten ist nur soweit zulässig, als sie für die Aufgabenbearbeitung in den Jobcentern unerlässlich ist. Die Landesbeauftragte sieht daher Vermerke über die notwendigen Angaben als datenschutzrechtlich vorzugswürdig an.

In diesem Sinne haben wir auch die Aktenführung im geprüften Jobcenter auf die Einhaltung der datenschutzrechtlichen Regelungen kontrolliert. Dazu wählten wir Akten aus dem Leistungs- und Vermittlungsbereich nach dem Zufallsprinzip aus und stellten dabei einzelne Verstöße fest.

Bezüglich der Vorlage von bestimmten Dokumenten wie zum Beispiel Kontoauszügen, Mietverträgen oder Arbeitsunfähigkeitsbescheinigungen wird auf unsere Ausführungen im letzten Tätigkeitsbericht verwiesen.[36] Darüber hin-

---

35 Tätigkeitsbericht 2014/2015, B 3.1.3.

36 Tätigkeitsbericht 2014/2015, B 3.1.3.1 und B 3.1.3.2.

aus sind bei unserer Prüfung eine Wohnungsgeberbestätigung sowie ein Scheidungsurteil in den Akten aufgefallen.

Eine Wohnungsgeberbestätigung gemäß § 19 Abs. 1 Bundesmeldegesetz wird zur Vorlage bei der Meldebehörde benötigt. Diese Bescheinigung ist für die Bearbeitung eines Antrages auf Leistungsgewährung nach dem Zweiten Buch Sozialgesetzbuch nicht erforderlich.

Dem Beschluss des Familiengerichts zur Ehescheidung der Betroffenen waren der Tenor, der Tatbestand und die Entscheidungsgründe zu entnehmen. Inwieweit dies für die Feststellung der Leistungsberechtigung notwendig war, ist uns nicht ersichtlich. Allenfalls halten wir Angaben zu Unterhaltsansprüchen der Leistungsempfänger für erforderlich.

Das Jobcenter wurde aufgefordert, die Akten zukünftig datenschutzgerecht zu führen.

Der technisch-organisatorische Datenschutz in kommunalen Jobcentern wird weiterhin oft vernachlässigt. Seit Beginn der Prüfungen wurden Verbesserungen der teils erheblichen Mängel in diesem Bereich nur vereinzelt und schleppend erreicht. Bei einer weiteren Prüfung zeigten sich trotz Nutzung eines anderen Softwareprodukts ähnliche Probleme. Die Landesbeauftragte wird auf die Beseitigung der Mängel hinwirken.

3.2 Vertraulichkeit beginnt bei der Datenschutzorganisation

Im Berichtszeitraum kontrollierten wir aufgrund von Beschwerden von Bürgern bauliche und organisatorische Vorkehrungen zur Sicherung der Vertraulichkeit bei Sozialleistungsträgern und anderen öffentlichen Stellen. Eine Prüfung führte uns in das Bürgerbüro einer Stadtverwaltung, eine weitere zum Anmeldebereich eines Jobcenters.

Bereits in unserem letzten Tätigkeitsbericht[37] haben wir bauliche und organisatorische Maßnahmen erläutert, die verantwortliche Stellen treffen müssen, um den Datenschutz für Betroffene zu gewährleisten. Für die Stadtverwaltung ergibt sich dies aus § 10 Brandenburgisches Datenschutzgesetz, für Jobcenter aus § 78a Zehntes Buch Sozialgesetzbuch.

Der Umgang mit den personenbezogenen Daten der Bürger in den von uns geprüften Bereichen beider öffentlichen Stellen entsprach überwiegend den datenschutzrechtlichen Bestimmungen. Sowohl die Stadtverwaltung als auch

[37] Tätigkeitsbericht 2014/2015, B 3.1.1.

das Jobcenter mussten lediglich aufgefordert werden, kleinere Mängel zu beheben.

Die Aufbewahrung der Akten hat so zu erfolgen, dass Unbefugte ihre Inhalte nicht zur Kenntnis nehmen können. In der Regel kommen hierfür Schränke zum Einsatz, die verschließbar sein müssen. Das Bürgerbüro der Stadtverwaltung kam diesen Anforderungen nach.

Für die Leerung der Papierkörbe waren die Mitarbeiter selbst verantwortlich, die hierzu einen verschlossenen Metallbehälter im oberen Flurbereich des Gebäudes nutzten. Schriftliche Anweisungen zur Entsorgung oder Vernichtung von Schriftstücken existierten nicht. Bei der Vor-Ort-Begehung fanden wir auch an unbesetzten Arbeitsplätzen Unterlagen mit Personenbezug in den Papierkörben. Die Stadtverwaltung wurde deshalb aufgefordert, Regelungen zur datenschutzgerechten Entsorgung von Papierdokumenten zu erstellen und dabei insbesondere auf den unterschiedlichen Schutzbedarf der Daten zu achten.

Zur Sicherstellung der Vertraulichkeit gehört auch, dass Bildschirminhalte für Unbefugte nicht einsehbar sind. Deshalb wurde in der Stadtverwaltung zum Wartebereich hin eine Trennwand mit ausreichendem Abstand zu den Arbeitsplätzen eingezogen. Auch die Arbeitsplätze zur Fensterfront befanden sich in einer größeren Entfernung und waren so ausgerichtet, dass eine Kenntnisnahme der Bildschirminhalte von außen nicht möglich war.

Nicht zu kritisieren war das System zum Aufruf der Wartenden im Bürgerbüro der Stadtverwaltung. Es verfügt über eine differenzierte Rechtevergabe für die Mitarbeiter, sodass diese ausschließlich auf die Daten derjenigen Betroffenen zugreifen können, die im eigenen Bereich ein Anliegen klären möchten.

Kundengespräche im Jobcenter unterliegen der Vertraulichkeit. In einem Fall hatte das geprüfte Jobcenter ein Plakat mit Informationen so angebracht, dass Gespräche im nahe gelegenen Anmeldebereich beim Lesen des Aushangs mitgehört werden konnten. Wir forderten es deshalb auf, das Plakat umzuhängen.

Des Weiteren müssen Kunden die Möglichkeit haben, mit den zuständigen Mitarbeitern vertrauliche Gespräche zu führen. Dazu muss entweder ein eigener Beratungsraum zur Verfügung stehen oder die Möglichkeit existieren, auf separate abgeschirmte Arbeitsplätze auszuweichen. Betroffene sollten bei jedem Termin auf diese Möglichkeit der Gesprächsführung hingewiesen werden, zumal ein Mithören von Gesprächen im selben Raum gerade zu weniger ausgelasteten Zeiten (geringer Geräuschpegel) nicht ganz ausge-

schlossen werden kann. Eine entsprechende Information sollte jede Behörde in ihrem Empfangsbereich bereitstellen.

Im Anmeldebereich des geprüften Jobcenters waren keine Papierakten vorhanden. Dort wurden jedoch Posteingänge in einem entsprechenden Fach unverschlossen aufbewahrt. Um zu vermeiden, dass Unbefugte Einblick in personenbezogene Daten von Leistungsempfängern erhalten, sollten Posteingänge jedoch in einem abgeschlossenen Schrank gelagert werden. Im Übrigen sollten generell die Kunden eines Jobcenters nicht alleine in Büros zurückgelassen werden.

Verantwortliche Stellen haben Maßnahmen zur Gewährleistung der Vertraulichkeit bei der Datenverarbeitung umzusetzen. Dazu sind unter anderem die Unterlagen der Bürger gesichert aufzubewahren und die Diskretion bei Gesprächen sicherzustellen.

3.3 Jugendberufsagenturen

Im gesamten Bundesgebiet werden seit einigen Jahren sogenannte Jugendberufsagenturen eingerichtet – so auch im Land Brandenburg. Dies sind keine neuen, eigenständigen Behörden, sondern spezielle Kooperationsformen zwischen den Agenturen für Arbeit, den Jobcentern sowie den Trägern der Jugendhilfe, um Jugendliche unter 25 Jahren beim Start ins Berufsleben zu unterstützen. Aus datenschutzrechtlicher Sicht stellen sich hierbei insbesondere Fragen der Zulässigkeit von Datenerhebungen, Datenübermittlungen und Datennutzungen. Wir haben dazu im Berichtszeitraum mehrere Landkreise sowie die Regionaldirektion Berlin-Brandenburg der Bundesagentur für Arbeit beraten.

Grundsätzlich richtet sich die datenschutzrechtliche Zulässigkeit der genannten Prozesse nach den Festlegungen des Sozialgesetzbuches, insbesondere seines Zehnten Buches (SGB X). Gemäß § 67a Abs. 1 SGB X ist das Erheben von Sozialdaten durch einen Leistungsträger nur dann zulässig, wenn ihre Kenntnis zur Erfüllung der Aufgaben der jeweiligen Stelle erforderlich ist. Eine anschließende Datenübermittlung (als Teil der Datenverarbeitung) und Datennutzung ist gemäß § 67b Abs. 1 SGB X nur zulässig, wenn sie durch eine Rechtsvorschrift oder die Einwilligung des Betroffenen legitimiert wird. Nach § 69 Abs. 1 SGB X ist eine Datenübermittlung u. a. dann erlaubt, wenn sie zur Aufgabenerfüllung der übermittelnden Stelle nach dem Sozialgesetzbuch oder der empfangenden Stelle, wenn diese selbst Sozialleistungsträger ist, erforderlich ist. Insofern sind auch die in den anderen Büchern des Sozialgesetzbuches jeweils definierten Aufgaben der an den Jugendberufsagenturen beteiligten Kooperationspartner zu beachten – für die Jobcenter das Zweite Buch, für die Arbeitsagenturen das Dritte Buch, für die Jugendämter

das Achte Buch. Aufgabenzuständigkeiten der einzelnen Behörden dürfen hierbei nicht durchbrochen werden.

Die anfragenden Landkreise haben wir deshalb dahingehend beraten, dass die einzelnen Übermittlungen personenbezogener Daten von Jugendlichen sich an den Aufgaben zu orientieren haben, die den jeweils beteiligten Stellen durch Gesetz zugewiesen sind. Eine Datenübermittlung durch ein Jugendamt ohne Einwilligung des Betroffenen kann also nur zulässig sein, wenn diese für die Erfüllung der gesetzlichen Aufgaben des Jugendamtes selbst nach dem Achten Buch Sozialgesetzbuch, der Bundesagentur für Arbeit nach dem Dritten Buch Sozialgesetzbuch oder des Jobcenters nach dem Zweiten Buch Sozialgesetzbuch erforderlich ist. Auch darf es nicht zu einer Vermischung der Aufgabenerfüllung kommen. So kann beispielsweise das Jugendamt nur im Rahmen seiner eigenen Aufgaben tätig werden. Eine Erledigung von Aufgaben des Jobcenters oder der Arbeitsagentur ist ausgeschlossen. Dies gilt auch umgekehrt.

Ob im Einzelfall eine Befugnis besteht, Daten eines Jugendlichen an die Bundesagentur für Arbeit oder das Jobcenter zu übermitteln, ist vom Jugendamt zu prüfen. Der Jugendliche ist hieran zu beteiligen. In jedem Fall, in dem ein Jugendlicher vom Jugendamt betreut wird, ist zu entscheiden, ob eine Kontaktaufnahme und Weiterleitung der Daten zum Jobcenter überhaupt notwendig ist. Nicht alle dem Jugendamt bekannten Jugendlichen werden Leistungen nach dem Zweiten Buch Sozialgesetzbuch beantragen wollen oder einen Anspruch auf derartige Leistungen haben. Ebenso wird es zahlreiche Fälle geben, in denen ein Jugendlicher Leistungen vom Jobcenter bezieht, ohne gleichzeitig von einem Jugendamt betreut zu werden. In allen diesen Fällen wäre eine Datenübermittlung zur Erfüllung der Aufgaben des Jobcenters nicht erforderlich und damit nach § 69 SGB X unzulässig.

Als Alternative für die Legitimierung der Datenübermittlung an Kooperationspartner in der Jugendberufsagentur und die anschließende Datennutzung kommt nach § 67b Abs. 1 SGB X ferner eine Einwilligung des betroffenen Jugendlichen in Betracht. Auf diese Weise können auch Schulen frühzeitig in den Unterstützungsprozess eingebunden werden. Die Regionaldirektion Berlin-Brandenburg der Bundesagentur für Arbeit bat uns um eine Beratung zu Mustern für entsprechende Einwilligungserklärungen. Wir haben ihr empfohlen, die Betroffenen über den Verwendungszweck der Daten (z. B. weitere Betreuung durch das Jugendamt oder das Jobcenter) umfassend zu informieren – am besten über ein separates Hinweisblatt. Ferner muss aus dem Formular klar hervorgehen, welche Daten konkret an welche Stellen weitergegeben werden sollen.

Zusätzliche Informationen können der „Arbeitshilfe zum Sozialdatenschutz in Jugendberufsagenturen“, die unter Federführung des Bundesministeriums für

Arbeit und Soziales herausgegeben wurde, entnommen werden. Sie enthält Hinweise nach Bundesrecht zur rechtlichen Zulässigkeit des Informationsaustausches unter den Sozialleistungsträgern und zu den Anforderungen an wirksame Einwilligungserklärungen.

Im Rahmen der Kooperation verschiedener Sozialleistungsträger und ggf. anderer öffentlicher Stellen in Jugendberufsagenturen sind die Vorschriften zum Sozialdatenschutz in jedem Einzelfall zu beachten. Dies gilt insbesondere für Datenübermittlungen. Sollen diese auf einer Einwilligung des betroffenen Jugendlichen basieren, sind hohe Anforderungen an die Transparenz der Datenweitergabe und der Datenverwendung einzuhalten.

3.4 Babyfone in Gemeinschaftsräumen einer Seniorenwohnanlage

Die Landesbeauftragte hatte den Fall zu beurteilen, ob handelsübliche Babyfone in den Gemeinschaftsräumen einer Seniorenwohnanlage zur Nachtzeit eingesetzt werden dürfen.

Im Rahmen einer Überprüfung durch das Landesamt für Soziales und Versorgung war bei einer Seniorenwohnanlage der Betrieb zweier Babyfone in Gemeinschaftsräumen dieser Einrichtung aufgefallen. Sie wurden während des Nachtdienstes eingesetzt und dienten dazu, Auffälligkeiten möglichst frühzeitig zu bemerken und Bewohnern bei Bedarf möglichst schnell helfen zu können. Die akustischen Signale konnten zum Teil einzelnen Bewohnern zugeordnet werden. Auch ließ sich nicht ausschließen, dass die unmittelbar angrenzenden, der Privatsphäre zuzurechnenden Bewohnerzimmer miterfasst wurden und sogar das gesprochene Wort mitgehört werden konnte.

Unabhängig von einer eventuellen Strafbarkeit wegen Verletzung der Vertraulichkeit des Wortes (§ 201 Strafgesetzbuch) haben wir die Einrichtung auf die datenschutzrechtliche Unzulässigkeit der Verwendung der Babyfone hingewiesen. Bei den Tonaufnahmen handelt es sich um personenbezogene Daten im Sinne des Bundesdatenschutzgesetzes (BDSG). Zwar hatte die Einrichtung ein berechtigtes Interesse, die Sicherheit ihrer Bewohner möglichst umfassend zu gewährleisten. Dieses musste aber angesichts der Schwere des Eingriffs in die Rechte der Bewohner zurückstehen, zumal derselbe Effekt mit milderen Mitteln hätte erreicht werden können. Zu denken ist etwa an den Einsatz von Notfallknöpfen, die gefährdete Bewohner in der Nacht bei sich tragen, oder an zusätzliche Kontrollgänge des Personals.

Eine Nutzung der Babyfone wäre allenfalls zulässig, wenn alle Bewohner nach § 4a BDSG einwilligten. Denn jeder Einzelne ist Betroffener im Sinne des Bundesdatenschutzgesetzes. Sobald auch nur einer von ihnen sein

Einverständnis nicht erteilt oder von seinem Recht auf Widerruf Gebrauch macht, ist die akustische Überwachung rechtswidrig.

Voraussetzung einer Einwilligung ist zudem, dass die Betroffenen sich grundsätzlich höchstpersönlich mit der Verarbeitung ihrer Daten, d. h. mit der Nutzung der Babyfone, einverstanden erklären. Die Abgabe einer Einwilligung durch einen Bevollmächtigten ist nach unserer Auffassung nur zulässig, wenn ergänzend eine ausdrückliche Bevollmächtigung durch den Betroffenen für die Abgabe solcher Einwilligungserklärungen vorliegt.

Schließlich haben wir die Einrichtung noch auf ein weiteres Problem hingewiesen: Den Herstellerangaben ließ sich nicht entnehmen, ob die übertragenen Daten mit einem sicheren kryptographischen Verfahren verschlüsselt werden. Kombiniert mit einer Reichweite von bis zu 300 Metern bestand also die Gefahr, dass Unbefugte, die sich außerhalb des Geländes befinden, mithören können. Leider haben viele Geräte, die den DECT-Standard zur Übertragung nutzen, keine diesbezügliche Kennzeichnung. Betroffen hiervon sind auch viele handelsübliche Telefone an Festnetzanschlüssen. Wer solche Geräte einsetzen will, um personenbezogene Daten zu übertragen, muss sich vorher informieren, ob die Übertragung verschlüsselt stattfindet und hierbei Verfahren nach dem aktuellen Stand der Technik eingesetzt werden.

Die betroffene Einrichtung hat sich im Ergebnis entschieden, die verwendeten Geräte zu entfernen.

Tonaufnahmen, die Betroffenen zugeordnet werden können, sind personenbezogene Daten. Der Einsatz von akustischen Überwachungsgeräten – hier von Babyfonen – in Gemeinschaftsräumen einer Seniorenwohnanlage setzt regelmäßig die Einwilligung aller betroffenen Bewohner voraus und verlangt zudem technische Sicherheitsvorkehrungen, die das Abhören durch Dritte ausschließen.

3.5 Übermittlung von Daten zu Impfschäden

Das Robert-Koch-Institut (RKI) plante ein bundesweites Projekt, bei dem kontinuierlich Anträge auf Versorgung nach einem Impfschaden und anerkannte Impfschäden erfasst sowie bei den Versorgungsämtern gestellte Impfschadensanträge und deren Anerkennung seit dem Jahr 2000 retrospektiv ausgewertet werden sollten. In Brandenburg war angedacht, dass das Landesamt für Soziales und Versorgung Angaben zu anerkannten Impfschäden an das RKI meldet. Es sollte dem RKI insbesondere medizinische Angaben verbunden mit den Initialen des Namens, dem vollständigen Geburtsdatum und dem Geschlecht des Patienten per E-Mail übersenden.

Das RKI ging davon aus, dass dem Projekt aus Sicht des Datenschutzes nichts entgegenstehe, da es sich bei den zu meldenden Daten um anonymisierte Daten handele. Diese Einschätzung teilten wir nicht. Gemäß § 67 Abs. 8 Zehntes Buch Sozialgesetzbuch (SGB X) sind Sozialdaten dann anonym, wenn sie derart verändert wurden, dass die Einzelangaben über persönliche oder sachliche Verhältnisse nicht mehr oder nur mit einem unverhältnismäßig großen Aufwand an Zeit, Kosten und Arbeitskraft einer bestimmten oder bestimmbaren natürlichen Person zugeordnet werden können. Die geringe Fallzahl und die Angabe des Geburtsdatums verbunden mit umfangreichen Gesundheitsangaben ließen hier jedoch die Möglichkeit einer Zuordnung des Datensatzes zu einer bestimmten Person als sehr wahrscheinlich erscheinen. Somit handelte es sich lediglich um pseudonymisierte Daten. Dafür sprach auch die Absicht des RKI, die gelieferten Datensätze mit anderen externen Datenbeständen zu verknüpfen und abzugleichen.

Handelt es sich also wie hier um personenbezogene Daten im Sinne von § 67 Abs. 1 S. 1 SGB X, so bedarf es einer Rechtsgrundlage für die Datenübermittlung oder der Einwilligung der Betroffenen. Dem Infektionsschutzgesetz selbst lässt sich eine Befugnis für die Übermittlung der in Rede stehenden Daten an das RKI nicht entnehmen. Dagegen erlaubt § 75 SGB X die Übermittlung von Sozialdaten für ein ganz bestimmtes Verfahren zum Zweck der wissenschaftlichen Forschung und Planung im Sozialleistungsbereich. Das Projekt muss demnach einen erkennbaren thematischen Bezug zu Inhalten, Trägern oder Strukturen des Systems der sozialen Sicherung aufweisen. Es muss deutlich werden, welche konkreten Erkenntnisse sich für den Sozialleistungsbereich ergeben.

Vor einer Übermittlung ist außerdem zu prüfen, ob der Zweck des Forschungsvorhabens auch auf andere Weise erreicht werden kann, etwa über die Weitergabe der Informationen in anonymisierter Form. Soll vom Grundsatz der vorrangigen Anonymisierung abgewichen werden, so ist dies nur zulässig, wenn die Erforderlichkeit des Personenbezugs für das Forschungsprojekt dargelegt wird. Ein solcher Grund wurde jedoch nicht vorgetragen. Damit verblieb nur die Option zu prüfen, ob es zumutbar war, die Einwilligung der Betroffenen in die Datenweitergabe einzuholen.

Nach Mitteilung des Landesamtes für Soziales und Versorgung hat das RKI die begehrten Daten angesichts der datenschutzrechtlichen Einwendungen nicht wieder angefragt.

Für eine Übermittlung von personenbezogenen Angaben zu Impfschäden an das Robert-Koch-Institut besteht keine gesetzliche Befugnis. Die Daten dürfen nur vollständig anonymisiert oder mit der Einwilligung der Betroffenen weitergegeben werden.

4 Bauen, Wohnen und Verkehr

4.1 Keine dauerhafte Speicherung der Daten von Rufbus-Kunden

Um den Aufwand bei regelmäßiger Bestellung eines Rufbusses zu reduzieren, hatte ein Verkehrsunternehmen die Kundendaten nicht sofort nach Abschluss des Beförderungsvertrages gelöscht.

Wir wurden von Kunden eines Verkehrsunternehmens gebeten, die Erhebung und Verarbeitung der personenbezogenen Daten im Zusammenhang mit dem Rufbus-Service aus datenschutzrechtlicher Sicht zu bewerten. Bei der Bestellung eines Busses würden der Name, das Fahrziel und die Telefonnummer erfragt. Die Kunden vermuteten, dass diese Angaben auch nach Erledigung der Fahrt gespeichert würden. Dies leiteten sie daraus ab, dass z. B. gefragt worden sei, ob es wieder von A nach B gehen solle, sobald die eigene Telefonnummer wiederholt angegeben wurde. Der eigene Name sei dann auch bereits bekannt. So könne das Verkehrsunternehmen in der Rückschau ein Bewegungsprofil erstellen.

Unsere Prüfung ergab, dass die Rufbuszentrale den Namen des jeweiligen Kunden, sein Geburtsdatum oder Alter, die Kontakt- und Adressdaten sowie den Fahrwunsch (Ausgangs- und Zielhaltestelle, Fahrtzeit, Datum) erhob. Diese Daten wurden nach Erledigung des Fahrauftrags weiter gespeichert, um den Aufwand bei wiederkehrenden Fahraufträgen zu reduzieren.

Personenbezogene Daten sind zu löschen, sobald ihre Kenntnis für die Erfüllung des eigenen Geschäftszwecks nicht mehr erforderlich ist (§ 35 Abs. 2 Nr. 3 Bundesdatenschutzgesetz). In bestimmten Fällen müssen die Daten zwar darüber hinaus noch gespeichert bleiben, wenn etwa gesetzliche oder vertragliche Aufbewahrungsfristen einer Löschung entgegenstehen. Die Nutzung der Daten ist dann jedoch auf den konkreten Zweck beschränkt, dem die Speicherung dient. So ergeben sich z. B. steuerrechtliche Aufbewahrungspflichten aus der Abgabenordnung. Die Daten dürfen in diesem Fall aber auch nur für steuerrechtliche Zwecke genutzt werden.

Nach Erörterung der Rechtslage hat das Unternehmen seine Verarbeitungspraxis umgestellt. Die personenbezogenen Daten der abgeschlossenen Bestellvorgänge beim Rufbus-Service wurden umgehend gelöscht. Die Trennung von Fahr- und Kundendaten wurde organisiert. Mit dem Ziel, den Aufwand bei regelmäßiger Bestellung zu reduzieren, wurde für die Kunden eine Einwilligungslösung implementiert, mit der einer Speicherung der persönlichen Daten über 90 Tage zugestimmt werden kann. Die Kunden können ihre Einwilligung jederzeit widerrufen.

Personenbezogene Daten sind grundsätzlich zu löschen, sobald ihre Kenntnis für die Erfüllung des eigenen Geschäftszwecks nicht mehr erforderlich ist. Eine darüber hinausgehende Speicherung kann mit ausdrücklicher Einwilligung der Betroffenen erfolgen.

4.2 Facility Management in der Landesverwaltung

Der Brandenburgische Landesbetrieb für Liegenschaften und Bauen (BLB) führt seit 2015 ein durch externe Dienstleister zur Verfügung gestelltes neues IT-System für seine Liegenschaftsverwaltung (Computer Aided Facility Management – CAFM) ein, mit dem auch personenbezogene Daten verarbeitet werden. Dabei wurden die datenschutzrechtlichen Vorgaben zu den erforderlichen technischen und organisatorischen Maßnahmen lange Zeit nicht berücksichtigt.

Der BLB unterfällt als Landesbetrieb teilweise den Regelungen des Bundesdatenschutzgesetzes (BDSG). Er hat gemäß § 9 BDSG die innerbetriebliche Organisation datenschutzgerecht zu gestalten und technische und organisatorische Maßnahmen zu ergreifen, die die in der Anlage zu dieser Vorschrift genannten Kontrollziele (Zutritts-, Zugangs-, Zugriffs-, Weitergabe-, Eingabe-, Auftrags-, Verfügbarkeits-, Trennungskontrolle) gewährleisten. Zudem ist der BLB aufgrund der IT-Standards der Brandenburgischen Landesverwaltung verpflichtet, ein IT-Sicherheitskonzept gemäß den Vorgaben des Bundesamtes für Sicherheit in der Informationstechnik (BSI) zu erstellen. Trotz unserer mehrfachen Hinweise zu den datenschutzrechtlichen Anforderungen erfüllte der BLB diese jedoch weder bis zur Produktivsetzung des CAFM-Systems noch in den Monaten danach, sodass die Landesbeauftragte eine Prüfung einleitete.

In der folgenden Zeit wurden verschiedene Dokumente zu einem IT-Sicherheitskonzept und schließlich auch ein Vertrag zur Auftragsdatenverarbeitung nach § 11 BDSG vorgelegt. Nach Prüfung der Unterlagen stellten wir fest, dass nicht alle erforderlichen technischen und organisatorischen Maßnahmen ergriffen wurden, um die Anforderungen des § 9 BDSG zu erfüllen. Zudem war kein Realisierungsplan vorhanden, der verbindliche Termine und Verantwortliche für die Umsetzung der noch fehlenden Maßnahmen festlegt. In unserer Stellungnahme haben wir daher die fehlende Rechtmäßigkeit des CAFM-Systembetriebs konstatiert. Der BLB legte unter Vorlage einer verbindlichen Realisierungsplanung dar, welche Fortschritte bei der Umsetzung der technischen und organisatorischen Maßnahmen gemacht wurden und wie die noch vorhandenen Mängel in der nahen Zukunft behoben werden sollten. Zudem konnten Vereinbarungen zur Vorlage der erforderlichen Nachweise getroffen werden. Außerdem wurde bei den Verantwortlichen das Verständnis für die datenschutzrechtlichen Anforderungen gestärkt.

In der Folge wurden nachgebesserte Dokumente zur Auftragsdatenverarbeitung und zur Realisierungsplanung vorgelegt, die eine positive Entwicklung hin zu einem ausgewogenen Sicherheitskonzept belegen. Wir werden den Prozess im Sinne der Umsetzung der datenschutzrechtlichen Anforderungen weiter kritisch begleiten.

Bei der Einführung von IT-Systemen in der Landesverwaltung, mit denen personenbezogene Daten verarbeitet werden, sind die Anforderungen der Datenschutzgesetze an die Realisierung von technischen und organisatorischen Maßnahmen vor Produktivsetzung zu erfüllen.

4.3 Kontrolle eines Wohnungsunternehmens

Eine anlassunabhängige datenschutzrechtliche Prüfung eines großen Unternehmens der Gebäudewirtschaft offenbarte Handlungsbedarf bei der Entwicklung eines Löschkonzepts.

Die Prüfung beschränkte sich im Wesentlichen auf die Erhebung, Verarbeitung und Nutzung von personenbezogenen Daten zum Zwecke der Anbahnung, Begründung, Durchführung und Beendigung von Mietverhältnissen. Im Ergebnis der Prüfung konnte eine überwiegend positive Bilanz gezogen werden. Allerdings konnte kein Konzept zur Löschung der personenbezogenen Daten von Mietinteressenten und ehemaligen Mietern vorgelegt werden.

In einem Löschkonzept legt eine verantwortliche Stelle fest, wie sie die datenschutzrechtlichen Pflichten zur Löschung von personenbezogenen Daten erfüllt. Sofern ein Mietverhältnis beendet ist und keine Zahlungsrückstände mehr bestehen, sind die Daten zu löschen, wenn nicht vertragliche oder gesetzliche Aufbewahrungsfristen entgegenstehen. Dasselbe gilt für die Daten, die im Rahmen von Vertragsanbahnungen erhoben wurden, wie z. B. bei Mietanfragen oder schriftlich erteilten Selbstauskünften. Kommt das Vertragsverhältnis nicht zustande, sind diese Daten umgehend zu löschen, es sei denn, der Betroffene willigt in die weitere Verarbeitung ausdrücklich ein. Eine Löschung hatte das geprüfte Unternehmen zwar in regelmäßigen Abständen vorgenommen. Die Löschfrist hätte aber stärker an der Erforderlichkeit ausgerichtet und die Löschung früher umgesetzt werden müssen.

Im Umgang mit personenbezogenen Daten sind die Prinzipien der Erforderlichkeit, der Datenvermeidung und der Datensparsamkeit zu beachten. Um eine rechtskonforme Löschung der Daten zu gewährleisten, muss die verantwortliche Stelle unter Berücksichtigung der jeweiligen einschlägigen Rechtsvorschriften und der zulässigen Zwecke der Datenerhebung, -verarbeitung und -nutzung ein Regelwerk für die Löschung der Daten entwickeln und umsetzen.

5 Beschäftigtendatenschutz

5.1 Übermittlungen von Beschäftigtendaten im Konzern

Immer wieder werden wir gefragt, unter welchen Voraussetzungen die Daten von Beschäftigten eines Unternehmens an andere Unternehmen weitergegeben werden dürfen. In der Regel handelt es sich dabei um Datenübermittlungen zwischen rechtlich selbstständigen Unternehmen innerhalb eines Konzerns oder einer Unternehmensgruppe.

Im Berichtszeitraum wandte sich z. B. ein Unternehmen an uns, das zusammen mit seiner Muttergesellschaft mit Sitz im europäischen Ausland durch ein US-Unternehmen aufgekauft wurde. Für die Etablierung von Projekt- und Kommunikationsstrukturen zwischen den Beteiligten sollten zunächst die wichtigsten Beschäftigtendaten wie Name, Organisationseinheit, telefonische Erreichbarkeit und E-Mail-Adresse in die USA übermittelt werden. In einem anderen Fall kontaktierte uns der Betriebsrat des brandenburgischen Tochterunternehmens eines weltweit tätigen Konzerns mit Hauptsitz in den USA. Er monierte u. a., dass der Arbeitgeber Übermittlungen von Beschäftigtendaten zur Konzernmutter lediglich pauschal und summarisch rechtfertigte, ohne jedoch für einzelne Datenkategorien genau zu begründen, warum die Übermittlung jeweils erforderlich ist und warum schutzwürdige Interessen der Betroffenen ihr nicht entgegenstehen.

In beiden Fällen geht es um Datentransfers in das nicht europäische Ausland. Aufgrund der Begriffsbestimmungen im Bundesdatenschutzgesetz (BDSG) kann es sich hierbei nicht um eine Auftragsdatenverarbeitung handeln, bei der die Datenweitergabe an den Auftragnehmer privilegiert ist und der Auftraggeber die volle Kontrolle (und Verantwortung) über die Datenverarbeitung behält.

Dementsprechend bedarf es für die Datentransfers in den genannten Fällen jeweils einer eigenen Rechtsgrundlage. Diese kann sich z. B. aus § 32 Abs. 1 BDSG ergeben. Danach ist die Übermittlung zulässig, wenn sie für die Begründung oder Durchführung des Beschäftigungsverhältnisses selbst erforderlich ist. Ein solcher Fall liegt beispielsweise bei sog. konzerndimensionalen Arbeitsverträgen vor. Der Vertrag weist einen eindeutigen Konzernbezug auf – der Beschäftigte ist sich bei Vertragsschluss der Verflechtungen der beteiligten Unternehmen bewusst und weiß, dass er flexibel auch in anderen Unternehmen der Gruppe eingesetzt werden kann. Seine Daten müssen somit in übergreifenden, zentralen Personalverwaltungssystemen zur Verfügung stehen.

Auch § 28 Abs. 1 Nr. 2 BDSG kann eine Rechtsgrundlage für die Datenübermittlung liefern. Sie ist nach dieser Regelung zulässig, wenn sie zur

Wahrung berechtigter Interessen der verantwortlichen Stelle erforderlich ist und keine Anhaltspunkte bestehen, dass schutzwürdige Interessen des betroffenen Beschäftigten am Ausschluss der Übermittlung überwiegen. Berechtigte Interessen der übermittelnden Stelle können z. B. in der Zentralisierung und effizienten Erfüllung von Aufgaben der Personalverwaltung und der Personalplanung, in der unternehmensübergreifend einheitlichen Wahrnehmung spezieller Funktionen oder in der zentralen Durchsetzung ausgefeilter Datenschutz- und IT-Sicherheitskonzepte liegen. Im Rahmen der Abwägung mit den schutzwürdigen Interessen der Betroffenen sind jeweils für den konkreten Fall z. B. die Kategorien der übermittelten Daten und ihr Schutzbedarf, die Vorkehrungen beim Empfänger zur Gewährleistung der Zweckbindung der Datenverarbeitung, die Möglichkeiten für Betroffene, ihre Rechte auf Auskunft, Berichtigung und Löschung wahrzunehmen, oder die beim Empfänger realisierten Maßnahmen zur Gewährleistung der Informationssicherheit zu beachten. In jedem Fall muss der Arbeitgeber die jeweiligen Datenübermittlungs- und -verarbeitungsprozesse transparent machen.

Alternativ könnte auch eine Einwilligung jedes Beschäftigten in die Datenübermittlung als Rechtsgrundlage dienen. Allerdings werden hieran gemäß § 4a BDSG hohe Anforderungen gestellt. Insbesondere muss die Einwilligung freiwillig sein, also auf der freien Entscheidung des Betroffenen beruhen. Wegen des ungleichen Kräfteverhältnisses zwischen Arbeitgeber und Arbeitnehmer wird in der Regel davon auszugehen sein, dass bei einer solchen Konstellation nur in wenigen Fällen eine echte Freiwilligkeit vorliegt (z. B. wenn Beschäftigte durch die Einwilligung Vorteile erlangen).

Wenn Klarheit über die Rechtsgrundlage der Übermittlung von Beschäftigtendaten in das nicht europäische Ausland besteht, ist ein zweiter Prüfschritt durchzuführen. Gemäß § 4b Abs. 2 BDSG muss die Übermittlung unterbleiben, wenn beim Empfänger kein angemessenes Datenschutzniveau besteht. Die Bewertung der Angemessenheit des Datenschutzniveaus erfolgt entweder jeweils im Einzelfall unter Berücksichtigung aller Umstände, z. B. der Art der Daten, der Zweckbestimmung, der Dauer der Verarbeitung, des Herkunfts- und des Empfängerlandes, der dort geltenden Rechtsnormen oder der umgesetzten Sicherheitsmaßnahmen. Alternativ kann auch Entscheidungen der Europäischen Kommission gefolgt werden, die für bestimmte Empfängerländer die Angemessenheit des Datenschutzniveaus festgestellt hat. Zu diesen Ländern gehören u. a. Argentinien, Kanada, Israel, Neuseeland oder die Schweiz. Für die USA wird eine Angemessenheit des Datenschutzniveaus nur dann angenommen, wenn sich das betreffende US-Unternehmen

(als Datenempfänger) den Regelungen des EU-US Privacy Shield[38] unterwirft.

Ausnahmsweise darf gemäß § 4c BDSG eine Datenübermittlung an einen Empfänger, bei dem kein angemessenes Datenschutzniveau vorliegt, u. a. auch dann erfolgen, wenn die Einwilligung des Betroffenen vorliegt oder (nach Genehmigung der zuständigen Aufsichtsbehörde) hinreichende Garantien für den Schutz der Persönlichkeitsrechte der Betroffenen beim Empfänger bestehen. Diese Garantien können sich z. B. ergeben aus verbindlichen Unternehmensregelungen (sog. BCRs, Binding Corporate Rules) oder bei Verwendung von durch die Europäische Kommission erarbeiteten Vertragsklauseln zwischen übermittelndem und empfangendem Unternehmen.

Nach alledem war in den beiden geschilderten Fällen jeweils nachzubessern. Im zuerst beschriebenen Fall fehlte es an hinreichenden Vorkehrungen zur Gewährleistung eines angemessenen Datenschutzniveaus beim Empfänger. Da das in Rede stehende US-Unternehmen weder dem EU-US Privacy Shield unterfiel, noch unternehmensinterne BCRs hatte, empfahlen wir den Abschluss eines Vertrages nach den EU-Standardvertragsklauseln zwischen den Beteiligten. Im zweiten dargestellten Fall bestand zwar ein solcher Vertrag, allerdings hatte der Betriebsrat zu Recht eine detailliertere Betrachtung der Rechtsgrundlagen der Datenübermittlung und eine transparente Information der betroffenen Beschäftigten gefordert.

Unternehmen, die Beschäftigtendaten in das nicht europäische Ausland übermitteln wollen, müssen immer eine zweistufige Prüfung durchführen. Eine solche Übermittlung ist nur dann überhaupt zulässig, wenn es eine klare Rechtsgrundlage für die Datenweitergabe gibt. Darüber hinaus muss gewährleistet sein, dass beim Empfänger ein angemessenes, mit europäischen Standards vergleichbares Datenschutzniveau herrscht. Ist eine dieser Bedingungen nicht erfüllt, muss die Übermittlung unterbleiben.

5.2 Background Checks für Mitarbeiter beim Betriebsübergang – welche Überprüfungen sind dem neuen Arbeitgeber erlaubt?

Im Berichtszeitraum wandte sich ein Beschäftigter einer Berliner Firma an uns, nachdem diese von einem brandenburgischen Unternehmen aufgekauft wurde. Im Zuge des Betriebsübergangs führte der neue Arbeitgeber Hintergrundüberprüfungen der zu übernehmenden Beschäftig-

[38] Durchführungsbeschluss (EU) 2016/1250 der Kommission vom 12. Juli 2016 gemäß der Richtlinie 95/46/EG des Europäischen Parlaments und des Rates über die Angemessenheit des vom EU-US-Datenschutzschild gebotenen Schutzes (bekannt gegeben unter Aktenzeichen C(2016) 4176) (ABl. EU L 207/1).

ten durch. Unser Petent hatte Bedenken hinsichtlich des Datenumfangs und der Verfahrensweise.

Konkret wurden die Beschäftigten der Berliner Firma aufgefordert, in einem Online-Fragebogen persönliche Grundinformationen (Name, Geburtsdatum, Adresse), die Wohnanschriften der vergangenen sieben Jahre, Informationen zum höchsten Bildungsabschluss sowie die beruflichen Stationen letzten drei Jahre zusammen mit der jeweiligen Tätigkeit und dortigen Kontaktpersonen anzugeben. Zur Bestätigung der Daten sollten sie eine Kopie des Bildungsabschlusses sowie eines Personaldokuments (Personalausweis, Reisepass, Führerschein) in elektronischer Form auf die Online-Plattform hochladen. Außerdem sollten sie der Überprüfung ihrer Angaben zustimmen, die allerdings nicht durch den neuen Arbeitgeber selbst, sondern durch einen Auftragnehmer mit Sitz in den USA erfolgte. Die in diesem Zusammenhang erteilten Informationen für die Beschäftigten waren ausschließlich in englischer Sprache verfügbar, z. T. in sich widersprüchlich und schwer verständlich. Die Beschäftigten wurden außerdem darüber im Unklaren gelassen, welche Folgen es gehabt hätte, wenn sie nicht an der Datenerhebung teilgenommen hätten.

Auf unsere Nachfragen hin nahm das Unternehmen umfangreich Stellung: Es sah die Erhebung und Überprüfung der persönlichen Daten der Beschäftigten grundsätzlich vom Fragerecht des Arbeitgebers gedeckt. Nach der ständigen Rechtsprechung der Arbeitsgerichte waren auch Plausibilitätskontrollen und Verifizierungen der Angaben – z. B. durch Rückfragen bei ehemaligen Arbeitgebern – zulässig. Im konkreten Fall war außerdem zu berücksichtigen, dass das Unternehmen aufgrund seiner Geschäftstätigkeit insbesondere strafrechtliche Risiken nach dem Außenwirtschaftsgesetz sowie Risiken für die Unternehmensreputation zu vermeiden hatte. Aus diesem Grund führte es anhand der früheren Wohnanschriften auch Abgleiche der Beschäftigtennamen mit öffentlich zugänglichen Sanktionslisten der EU und des UN-Sicherheitsrates durch. Die Spezifik der Arbeitsaufgaben erforderte derartige Überprüfungen für alle zu übernehmenden Beschäftigten. Dieser Auffassung schlossen wir uns an – die Background Checks waren für die Begründung und Durchführung des Beschäftigungsverhältnisses erforderlich und damit nach § 32 Abs. 1 Bundesdatenschutzgesetz zulässig.

Als rechtswidrig bewerteten wir allerdings die Erhebung der Kopie der Personalausweise bzw. Reisepässe der Betroffenen. Sie war nicht nur nicht erforderlich, sondern stand auch im Widerspruch zu den damaligen Regelungen des Personalausweisgesetzes bzw. des Passgesetzes.[39] Das Unternehmen erkannte dies ebenfalls als Mangel, stellte die Praxis – die auch für alle Be-

[39] Die hier einschlägigen gesetzlichen Normen wurden mittlerweile geändert (§ 20 Abs. 2 Personalausweisgesetz bzw. § 18 Abs. 3 Passgesetz).

werber galt – mit sofortiger Wirkung ein und wies den Dienstleister an, bereits dort gespeicherte Personalausweis- oder Passdaten unverzüglich zu löschen. Auch die allgemeinen Unternehmensprozesse bei der Einstellung wurden insofern geändert, als dass neue Beschäftigte sich nun am ersten Arbeitstag durch Vorlage eines Identitätsdokuments ausweisen müssen und hierüber lediglich ein Aktenvermerk angefertigt wird.

Kritik übten wir des Weiteren an der unzureichenden Transparenz des Verfahrens zur Durchführung der Background Checks. Das Unternehmen erläuterte zwar, dass alle Beschäftigten aufgrund der internationalen Ausrichtung der Tätigkeit die englische Sprache beherrschen müssen. Die Beschwerde bei uns hat jedoch gezeigt, dass selbst Sprachkundige Schwierigkeiten beim Verständnis hatten. Insbesondere wurde nicht hinreichend deutlich, welche Abschnitte des mehrteiligen Informationsblattes für die Betroffenen anwendbar waren, welche Konsequenzen sich aus dem Ausfüllen des Formulars ergaben und welche Folgen eine entsprechende Weigerung gehabt hätte. Das Unternehmen folgte unserer Kritik und überarbeitete kurzfristig sowohl das Online-Formular als auch die Verfahrensinformationen vollständig. Sie liegen nun auch in deutscher Sprache vor.

Als weiteren Mangel identifizierten wir im Verlaufe unserer Untersuchungen, dass keine hinreichende Rechtsgrundlage für die Übermittlung der Beschäftigtendaten an den Dienstleister für die Background Checks mit Sitz in den USA existierte.[40] Von einer freiwilligen und informierten Einwilligung konnte nach dem oben Gesagten nicht ausgegangen werden. Das Unternehmen verwies einerseits auf Binding Corporate Rules (BCRs) für die Übermittlung von Beschäftigtendaten in die USA. Diese galten jedoch nur bezüglich der dort firmierenden Konzernmutter (bzw. anderer Unternehmen der Gruppe) als Empfänger und nicht bezüglich des Dienstleisters. Andererseits wurde uns ein Vertrag zwischen der Konzernmutter und dem Dienstleister vorgelegt, der zwar viele geeignete und angemessene Datenschutz- bzw. Informationssicherheitsmaßnahmen enthielt, die vom Dienstleister umzusetzen waren. Allerdings war nicht das unserer Aufsicht unterstehende Unternehmen Vertragspartner. Auch in diesem Punkt wurde kurzfristig Abhilfe geschaffen: Mittlerweile existieren direkte vertragliche Beziehungen zwischen den europäischen Unternehmen der Gruppe und dem US-Dienstleister, die inhaltlich die Standardvertragsklauseln der EU-Kommission für solche Fälle einhalten.

[40] Für allgemeine rechtliche Ausführungen zu solchen Übermittlungen siehe B 5.1.

Unternehmen, die Background Checks für Beschäftigte durchführen, müssen die Datenerhebungen und die eigentlichen Überprüfungen auf das erforderliche Maß beschränken. Hierbei sind u. a. die zukünftigen Arbeitsaufgaben der Beschäftigten sowie der Prüfzweck, mögliche Schäden für das Unternehmen zu verhindern, zu berücksichtigen. Sollen externe Dienstleister in die Prüfungen einbezogen werden, ist dies nur unter Beachtung der gesetzlichen Vorschriften der Auftragsdatenverarbeitung und ggf. der Datenübermittlung ins Ausland möglich.

5.3. Zeiterfassungsdaten und Abwesenheitsgründe auf freier Flur

Arbeitgeber gehen nicht immer sorgsam mit den Daten ihrer Beschäftigten um. So z. B. gewährte eine öffentliche Stelle allen Mitarbeitern Zugriff auf die elektronischen Zeiterfassungsdaten und Abwesenheitsgründe der Kollegen. In einem anderen Fall präsentierte ein Geschäftsführer mittels einer Magnettafel die Abwesenheiten und Krankenstände seiner Mitarbeiter im öffentlich zugänglichen Flur des Verwaltungsgebäudes. Außerdem hatte ein Betriebsrat die Absicht, sich mittels einer Betriebsvereinbarung Leserechte für die elektronischen Zeiterfassungsdaten aller Mitarbeiter zu sichern.

5.3.1 Zeiterfassungssystem mit Übermaß an Informationen

Eine Interessenvertretung bei einer öffentlichen Stelle bat uns, den Einsatz des dort verwendeten Zeiterfassungssystems zu überprüfen. Dieses war so konfiguriert, dass sich jeder Mitarbeiter über die An- und Abwesenheit aller Beschäftigten informieren konnte. Der Grund für die Abwesenheit war jeweils zusätzlich mittels Farbkodierungen hinterlegt. Folgende Informationen waren den Farbkodierungen zu entnehmen: nicht oder noch nicht anwesend, anwesend, abwesend jeweils mit Grund (u. a. krank, Kind krank, Bildungsurlaub, Gleitzeitausgleich, Elternzeit, Urlaub, Sonderurlaub) sowie abwesend – war aber schon anwesend. Sobald der Mauszeiger auf dem Bildschirm eine kurze Zeit unbewegt über dem Namen eines Mitarbeiters verweilte, erschien außerdem eine kontextsensitive, temporär aufscheinende Zusatzinformation, die die Zeit der letzten Buchung anzeigte, sodass sich eine Abfolge von Kommen und Gehen ableiten ließ.

Nicht nur, dass alle Mitarbeiter voneinander die Abwesenheitsgründe und damit Personalaktendaten unerlaubt zur Kenntnis nehmen konnten, war es durch diese Funktionalitäten auch auf einfachste Weise möglich, Verhaltensprofile zu erstellen und Verhaltenskontrollen durchzuführen.

Die diesem System zugrunde liegende Dienstvereinbarung war unter datenschutzrechtlichen Gesichtspunkten rechtswidrig, weil entgegen anders lautenden Rechtsvorschriften zur Verarbeitung von Personaldaten (hier: Zeiterfassungsdaten) und Personalaktendaten (Abwesenheitsgründe) diese Daten Dritten (allen Beschäftigten der Dienststelle) zugänglich gemacht wurden, ohne dass der Dienstverkehr dies erfordert hätte (vgl. § 29 Abs. 1 Satz 2 Brandenburgisches Datenschutzgesetz) oder die Voraussetzungen der §§ 94 ff. Landesbeamtengesetz vorgelegen hätten.

Die öffentliche Stelle hat unsere Kritik zum Anlass genommen, in Zusammenarbeit mit ihrem behördlichen Datenschutzbeauftragten und dem Hersteller der Software alle aufgezeigten Mängel zu beheben. Auch die für die Einführung eines IT-Fachverfahrens erforderlichen Dokumente wurden –leider erst verspätet – erstellt (u. a. Verfahrensverzeichnis, Berechtigungskonzept, Freigabeerklärung); die Dienstvereinbarung wurde entsprechend angepasst.

5.3.2 Aushang von Beschäftigtendaten auf dem Flur

Durch eine anonyme Eingabe erhielten wir den Hinweis, dass in einem Unternehmen im Land Brandenburg eine Tafel öffentlich ausgehängt wurde, die alle Urlaubs- und Krankentage der Mitarbeiter enthält. Das war für uns Anlass, vor Ort eine unangekündigte Kontrolle durchzuführen.

Der Geschäftsführer gewährte uns sofort Zugang zu dem Aushang, der Gegenstand der Beschwerde war. Es handelte sich um eine beschreibbare Magnettafel mit Kalenderfunktion, die in einem Flur des Verwaltungsgebäudes angebracht war, der zur Werkshalle führt. Der Geschäftsführer hatte ein System entwickelt, um mithilfe der Tafel sowohl die Personalsachbearbeitung als auch seine Personalplanung durchzuführen. Folgende Informationen waren handschriftlich auf der Tafel abgebildet: die Namen aller Mitarbeiter sowie deren Tätigkeit, personenscharf der Resturlaub aus 2016 und die Summe der Krankentage des Jahres 2017. Mit farbigen Magneten wurden für jeden einzelnen Beschäftigten die Urlaubstage für das Jahr 2017 sowie die Abwesenheiten durch Krankheit im Kalender markiert. Alle Mitarbeiter konnten die Daten über Kollegen jederzeit zur Kenntnis nehmen. Datenschutzrechtlich stellt dies eine Übermittlung durch den Geschäftsführer dar.

Das öffentliche Aushängen von Beschäftigtendaten (hier insbesondere Resturlaub, Krankheit, Summe der Krankentage) entbehrt jeder Rechtsgrundlage. Nach § 32 Abs. 1 Satz 1 Bundesdatenschutzgesetz dürfen personenbezogene Daten eines Beschäftigten für Zwecke des Beschäftigungsverhältnisses verarbeitet (hier: übermittelt) werden, wenn dies für die Durchführung des Beschäftigungsverhältnisses erforderlich ist. Für Mitarbeiter bzw. Kollegen untereinander ist es allenfalls wichtig zu wissen, welche Kollegen aktuell oder

zukünftig abwesend sind (ohne Nennung des Grundes), damit Arbeitsabläufe im Unternehmen gesteuert werden können.

Wir haben dem Geschäftsführer dringend empfohlen, die Tafel mit den Abwesenheiten der Beschäftigten aus dem öffentlich zugänglichen Flur zu entfernen. Da es ihm wichtig war, sie weiterhin für seine Personalsachbearbeitung und -planung zu benutzen, hatten wir keine Bedenken, wenn der Aushang in seinem Büro so erfolgt, dass Unberechtigte die personenbezogenen Daten der Kollegen nicht einsehen können.

Der Geschäftsführer hat sofort nach unserer Kontrolle reagiert und die Tafel aus dem Flur entfernt, um sie in seinem Büro anzubringen.

5.3.3 Lesezugriff des Betriebsrats auf die Zeiterfassungsdaten aller Mitarbeiter

Um eine Betriebsvereinbarung zum Thema Arbeitszeit abzuschließen und sich dabei seine Informationsrechte nach dem Betriebsverfassungsgesetz zu sichern, bat uns ein Betriebsrat um Unterstützung. Er war der Ansicht, dass die Interessenvertretung Einsicht in alle Zeiterfassungsdaten benötigt, um die Einhaltung der gesetzlichen Regelungen insbesondere mit Blick auf Beginn und Ende der Arbeitszeit und die Einhaltung der Pausenzeiten zu überprüfen. Diese gesetzliche Aufgabe könnte, so war seine Meinung, durch den Erhalt von umfassenden Leserechten für die elektronische Zeiterfassung wahrgenommen werden.

Wir haben dem Betriebsrat mitgeteilt, dass uns nicht ersichtlich ist, aus welchem Grund es unerlässlich wäre, im Rahmen seiner Überwachungsaufgaben nach § 80 Betriebsverfassungsgesetz Arbeitszeiten aller Mitarbeiter personenscharf durch Einräumen von Leserechten zu kontrollieren. Unseres Erachtens kommt der Arbeitgeber seiner Auskunftsverpflichtung ausreichend nach, wenn er den Betriebsrat, zunächst ohne Personenbezug (anonymisiert) oder auch pseudonymisiert, über die Zeiterfassungsdaten regelmäßig unterrichtet. Erst in einer zweiten Stufe wäre im Falle einer Rechtsverletzung die Namensnennung bzw. die Auflösung des Pseudonyms vorzunehmen.

Aus datenschutzrechtlicher Sicht wäre der Einsatz eines Zeiterfassungssystems angezeigt, welches die Verstöße gegen arbeitszeitrechtliche Regelungen bereits systemtechnisch separat auflisten kann. Einer personenbezogenen Darstellung der Verstöße würde nichts entgegenstehen; dem Grundsatz der Datensparsamkeit ebenso wie der Überwachungsfunktion des Betriebsrats würde dadurch Rechnung getragen.

Sowohl öffentlichen als auch privaten Arbeitgebern mangelt es häufig am Bewusstsein, dass Personaldaten nur verarbeitet werden dürfen, wenn eine Rechtsvorschrift es erlaubt. Gerade Zeiterfassungsdaten und Abwesenheitsgründe der Mitarbeiter sind Dritten ohne Erlaubnisnorm nicht zugänglich zu machen. Ein Betriebsrat hingegen hat im Rahmen seiner Überwachungsfunktion den Anspruch, bei festgestellten Arbeitszeitverletzungen Zeiterfassungsdaten personenscharf vom Arbeitgeber zu erhalten.

6 Gesundheit

6.1 Gesundheitsdaten am Handgelenk

Die Landesbeauftragte beteiligte sich an einer unter den Aufsichtsbehörden deutschlandweit abgestimmten Prüfaktion von sogenannten Wearables mit Gesundheitsfunktionen. Ergebnis ist, dass keines der 16 getesteten Geräte die datenschutzrechtlichen Anforderungen vollständig erfüllt.

Unter der Federführung des Bayerischen Landesamtes für Datenschutzaufsicht fand im Berichtszeitraum eine koordinierte Prüfaktion zum Datenschutz bei Wearables mit Gesundheitsfunktionen (z. B. Fitness-Armbänder, Smart Watches, Activity Tracker) statt. Neben unserer Dienststelle waren die Datenschutzaufsichtsbehörden aus Schleswig-Holstein, Niedersachsen, Nordrhein-Westfalen und Hessen sowie die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit daran beteiligt. Geprüft wurden 16 Wearables von unterschiedlichen Herstellern, die einen Marktanteil von ca. 70 % in Deutschland haben.

Diese Armbänder sollen den Nutzer zu einer gesunden Lebensweise motivieren und die Bewegung im Alltag fördern. Neben den gängigen Messungen der Schritte, der zurückgelegten Kilometer sowie der verbrauchten Energie, bieten die aktuellen und geprüften Geräte erheblich mehr Funktionen. Sie können zusätzlich u. a. die Herzfrequenz, die Körpertemperatur und den Schlafrhythmus erfassen und auswerten. Informationen, die auch immer mehr Versicherer und Unternehmen der Gesundheitsbranche interessieren. Zwar sind die Einzelinformationen für sich betrachtet oftmals wenig aussagekräftig. In der Regel werden diese Daten jedoch mit eindeutig zugewiesenen Personenkennungen verbunden. Bei einer dauerhaften Nutzung fallen derart viele Informationen an, dass sich daraus ein erstaunlich präzises Bild des Tagesablaufs und Gesundheitszustands des Nutzers ergibt, insbesondere wenn diese Informationen mit Standortdaten verknüpft werden.

Nach detaillierter Vorplanung und Abstimmung fand die Prüfung zu großen Teilen in drei Prüfzentren der Aufsichtsbehörden statt. Dort wurden die Geräte sowie die zum Gerät empfohlenen oder zum zugehörigen Smartphone mitgelieferten (Hersteller-) Apps für die Betriebssysteme iOS und Android unter Laborbedingungen getestet. Neben den rechtlichen Fragestellungen, wie z. B. die ausreichende Aufklärung über den Umgang mit den Daten, stand auch die technische Umsetzung auf dem Prüfstand. Mit speziellen Versuchsaufbauten, Softwarekomponenten und Softwareanalysetools (z. B. Kali Linux, Wireshark, Burp Suite, CyanogenMod, Android SDK) wurden u. a. die Datenflüsse, die Speicher- und Zugriffsmechanismen, die Sicherheitskomponenten und das Tracking für alle systemzugehörigen Komponenten (Wearable, Smartphone, App, Webportal) dynamisch und statisch analysiert. Insbesondere die zugehörigen Apps waren von Interesse, da ohne diese die meisten Wearables in ihrer Funktion erheblich eingeschränkt oder sogar unbrauchbar sind. Die Prüfergebnisse spiegelten teilweise die mangelhafte Umsetzung von technischen Standardsicherheitsmaßnahmen wider. So stellten wir u. a. eine fehlerhafte Auflistung von Berechtigungen, die Nutzung unsicherer Verschlüsselungsalgorithmen bei der Netzkommunikation, die Speicherung von Passwörtern im Klartext oder gar fehlenden Passwortschutz, die Nutzungsmöglichkeit trivialer Passwörter sowie eine nicht implementierte Löschmöglichkeit der Daten durch den Nutzer fest.

Wir müssen auch konstatieren, dass die meisten Datenschutzerklärungen nicht die gesetzlichen Anforderungen erfüllen. Sie sind häufig viele Seiten lang, schwer verständlich, enthalten auf wesentliche Datenschutzfragen nur pauschale Hinweise und sind teilweise nicht einmal in deutscher Sprache vorhanden. So erfährt der Nutzer oftmals nicht im ausreichenden Maße, wer konkret Zugriff auf die Daten hat und wie lange sie an welchem Ort und zu welchem Zweck gespeichert werden. Neben den Hardware-Herstellern und App-Anbietern werden oft Dienstleister mit einbezogen, die auch teilweise im Ausland sitzen. Fast kein Gerätehersteller klärt zudem über die besonders schützenswerten Gesundheits- und Standortdaten auf. Sie sind sogar teilweise der Auffassung, dass es sich um anonyme Daten handele.

Vielfach werden auch Tracking-Tools amerikanischer Unternehmen eingesetzt. Damit haben die Hersteller die Möglichkeit zu registrieren, wie welche Geräte und welche Software genutzt werden, diese Daten mit anderen aus unterschiedlichen Nutzungsszenarien zu verknüpfen und zur Profilbildung zu verwenden.

Besondere Vorsicht ist geboten, wenn Komponenten des Gesamtsystems, z. B. das Wearable selbst oder das Smartphone mit der zugehörigen App, verkauft werden sollen oder verloren gehen. Sie bieten dem Nutzer meist keine Möglichkeit, seine Daten selbstständig, komplett und datenschutzgerecht zu löschen.

Die Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder hat sich mit der Entschließung „Wearables und Gesundheits-Apps – Sensible Gesundheitsdaten effektiv schützen!“[41] an die Hersteller gewandt und u. a. die Beachtung der Grundsätze der Datenvermeidung und Datensparsamkeit, den Einsatz datenschutzfreundlicher Technologien und Voreinstellungen, Transparenz, informierte Einwilligungen und Verantwortungsübernahme eingefordert.

Eine datenschutzgerechte Nutzung der meisten Wearables ist derzeit nicht möglich. Unsere Prüfung hat an vielen Stellen gezeigt, dass die notwendigen technischen und organisatorischen Sicherheitsmaßnahmen nicht wirksam und vollständig umgesetzt worden sind und rechtliche Fragestellungen zum Datenschutz nur ungenügend beantwortet werden konnten.

6.2 Telemedizinische Versorgung für insulinpflichtige Diabetiker bei der AOK Nordost

Die AOK Nordost bietet ihren Versicherten ein Verfahren an, welches umfassend und automatisch den individuellen Krankheitsverlauf von Diabetes mellitus mit telemedizinischer Unterstützung dokumentiert. Spezielle Hard- und Softwarekomponenten, die auch über das Internet und das Mobilfunknetz kommunizieren, kommen zum Einsatz.

Für Patienten mit insulinpflichtigem, schwer einstellbaren Diabetes mellitus Typ 1 und Typ 2 bietet die AOK Nordost seit etwa einem Jahr ein Versorgungsprogramm an, welches die Blutzuckerselbstkontrolle und die Selbstinjektion von Insulin mit telemedizinischer Technologie unterstützt. Automatisiert und ohne zusätzlichen Aufwand wird ein Diabetes-Tagebuch elektronisch geführt, auf das der Patient und mit seiner Einwilligung auch der behandelnde Arzt jederzeit zugreifen kann, um den Stoffwechsel besser einzustellen.

Die AOK Nordost hat für den Einsatz eines entsprechenden Systems mit einem externen Unternehmen einen Vertrag zur besonderen ambulanten Versorgung nach § 140a Fünftes Buch Sozialgesetzbuch abgeschlossen. Die zentrale Komponente des Systems bildet das digitale Diabetes-Tagebuch, welches als Web-Anwendung oder per Smartphone-App über das Internet erreichbar ist und als Sammelstelle für alle Daten fungiert. Die Behandlungswerte werden durch ein Blutzuckermessgerät und einen Insulin-Pen erfasst und per integrierter Funkschnittstelle, mittels einer lokal installierten „Vermittlerstation“, über das Mobilfunknetz an das Web-Portal versendet.

41 Siehe Anlage 1.6.2.

Um bewerten zu können, ob dieses Verfahren allen datenschutzrechtlichen Anforderungen entspricht und keine Risiken für die Rechte und Freiheiten der Betroffenen existieren, forderten wir die AOK Nordost auf, uns dieses per Dokumentation und der Beantwortung von dedizierten Fragen nachzuweisen. Angefordert haben wir u. a. den Vertrag zur besonderen ambulanten Versorgung, die Einwilligungserklärung der Patienten, die Patienteninformation, das vollständige IT-Sicherheitskonzept (inkl. der erweiterten Risikoanalyse sowie der referenzierten Unterlagen), die Vorabkontrolle gemäß § 4d Abs. 5 Bundesdatenschutzgesetz (BDSG), das Verfahrensverzeichnis gemäß § 4e BDSG, das ISO/IEC 27001 Zertifikat inkl. vollständigem Zertifizierungsreport, die Bestellungsurkunde des Beauftragten für den Datenschutz gemäß § 4f BDSG sowie die Verträge zur Auftragsdatenverarbeitung gemäß § 11 BDSG.

Die AOK Nordost hat uns unter Mitwirkung des Dienstleisters die geforderten Unterlagen größtenteils zugesandt. Eine abschließende Bewertung, ob alle technischen und organisatorischen Maßnahmen in dem Verfahren getroffen wurden, die erforderlich sind, um die Ausführungen der Vorschriften des Bundesdatenschutzgesetzes, insbesondere die in der Anlage zu diesem Gesetz genannten Anforderungen, gewährleistet sind, konnten wir bisher noch nicht vornehmen, da das IT-Sicherheitskonzept und der angeforderte aussagekräftige Zertifizierungsreport nicht vollständig vorlagen.

Mit der telemedizinischen Versorgung insulinpflichtiger Diabetiker bietet die AOK Nordost ein innovatives Versorgungsprogramm an. Der Nachweis einer vollständigen datenschutzgerechten Umsetzung konnte bisher noch nicht erbracht werden.

6.3 Modellprojekt Schulgesundheitsfachkräfte

In einem Modellprojekt kümmern sich zehn Gesundheitsfachkräfte an ausgewählten brandenburgischen Schulen um kranke oder verletzte Schüler. Ziel ist es, den Kinder- und Jugendgesundheitsdienst der Landkreise sowie Lehrkräfte und Eltern zu entlasten. Vor Beginn des Projekts hat das federführende Ministerium für Arbeit, Soziales, Gesundheit, Frauen und Familie die Landesbeauftragte beteiligt, um rechtliche sowie technisch-organisatorische Voraussetzungen für eine datenschutzgerechte Durchführung zu klären.

Neben Brandenburg nimmt auch Hessen an dem zweijährigen Modellprojekt teil. Während die hessischen Fachkräfte Mitarbeiter der Schulen sind, hat sich das Land Brandenburg für die Anbindung an einen privatrechtlich organisierten, gemeinnützigen Träger entschieden. Die Situation bedurfte daher besonderer datenschutzrechtlicher Beratung.

Der Schwerpunkt unserer Empfehlungen lag auf der Erforderlichkeit und Gestaltung von Einwilligungen. Zunächst bedarf es einer grundsätzlichen Einwilligungserklärung der Eltern oder der sonstigen Sorgeberechtigten zur Teilnahme der Kinder an dem Modellprojekt. Sowohl die Schule als auch der Projektträger haben sicherzustellen, dass die Gesundheitsfachkräfte nur dann zum Einsatz kommen, wenn für das zu versorgende Kind eine solche Einwilligung vorliegt.

Soweit Lehrkräfte oder sonstiges Schulpersonal durch die Projektmitarbeiter zu einem Schulkind beraten werden sollen, bedarf es einer separaten Einwilligung der Eltern oder der sonstigen Sorgeberechtigten in eine entsprechende Übermittlung der gesundheitsbezogenen Daten der betroffenen Kinder. Eine anonyme Beratung dürfte im schulischen Umfeld schließlich kaum möglich sein, da bereits die Schilderung der näheren Umstände eines Falles zumeist Rückschlüsse auf die jeweiligen Schüler erlaubt.

Nachdem das Ministerium für Arbeit, Soziales, Gesundheit, Frauen und Familie uns das Konzept für das Modellprojekt vorgelegt hatte, haben wir darüber hinaus empfohlen, Vorgaben für den technisch-organisatorischen Datenschutz bei den eingesetzten Gesundheitsfachkräften zu konkretisieren und eine getrennte Aktenführung zwischen Schule und Fachkräften auch im Falle von Unfällen zu gewährleisten.

Der Projektträger hat im Ergebnis unserer Beratung die vorgesehene Einwilligungserklärung entsprechend unseren Empfehlungen erweitert, die Informationen für die Betroffenen deutlich verbessert und die Löschregeln vervollständigt. Darüber hinaus werden für weitere Anlässe gesonderte Einwilligungserklärungen vorgehalten.

Gesundheitsbezogene Informationen über die Schulkinder dürfen nur dann zwischen Schule und Gesundheitsfachkräften ausgetauscht werden, wenn die Eltern oder Sorgeberechtigten in die Projektteilnahme und in die Beratung des Schulpersonals durch die Gesundheitsfachkräfte eingewilligt haben.

6.4 Übermittlung von Patientendaten zum Zweck der Qualitätssicherung?

Das Gesundheitsministerium bat uns um Klärung der Frage, auf welcher Rechtsgrundlage Krankenhäuser zum Zweck der Qualitätssicherung Patientendaten an Dritte übermitteln dürfen.

Die bei der Landesärztekammer Brandenburg eingerichtete Landesgeschäftsstelle Qualitätssicherung erfüllt verschiedene Aufgaben, um die Qualität der stationären Versorgung zu sichern und weiterzuentwickeln. An ihr sind

Vertreter der Krankenkassenverbände, der Landeskrankenhausgesellschaft und der Landesärztekammer beteiligt. In einem jährlichen Datenvalidierungsverfahren soll die Landesgeschäftsstelle die von den Krankenhäusern im Rahmen der stationären externen Qualitätssicherung an das Institut für Qualitätssicherung und Transparenz im Gesundheitswesen übermittelten Daten auf Vollständigkeit und Plausibilität überprüfen. Davon umfasst ist u. a. ein Stichprobenverfahren, in dem die Qualitätsdokumentation mit der Dokumentation im Krankenhaus (Patientenakte) abgeglichen wird. Die Landesgeschäftsstelle benötigt dafür den Zugriff auf Patientenakten. Das Brandenburgische Krankenhausentwicklungsgesetz enthält jedoch keine entsprechende Befugnis zur Übermittlung personenbezogener Patientendaten.

Das Ministerium für Arbeit, Soziales, Gesundheit, Frauen und Familie hat uns gebeten, vor diesem Hintergrund eine Empfehlung für eine mögliche Ergänzung des Krankenhausentwicklungsgesetzes zu unterbreiten. Daraufhin haben wir eine konkrete Formulierung vorgeschlagen, die bereits die Anforderungen der künftig geltenden Datenschutz-Grundverordnung erfüllt und die dort vorgesehenen Regelungsspielräume berücksichtigt. Voraussetzung für eine Datenübermittlung zum Zweck der Qualitätssicherung muss sein, dass es sich beim Empfänger um einen Arzt oder eine ärztlich geleitete Stelle handelt und dass überwiegende schutzwürdige Interessen der Betroffenen gewahrt bleiben. Die Datenübermittlung muss sich in jedem Fall am Grundsatz der Erforderlichkeit ausrichten. Patientendaten sind daher vor ihrer Weitergabe, soweit möglich, zu anonymisieren oder zu pseudonymisieren. Dies trägt auch dem in der Datenschutz-Grundverordnung festgelegten Prinzip der Datenminimierung Rechnung.

Eine Übermittlung von Patientendaten an Dritte zum Zweck der Qualitätssicherung bedarf einer gesetzlichen Übermittlungsvorschrift. Aus dem Prinzip der Datenminimierung folgt, dass die Angaben, soweit möglich, anonymisiert oder pseudonymisiert zu übermitteln sind.

6.5 Rezepte auf Abwegen – Mängel bei der Datenverarbeitung im Auftrag von Apotheken

Nachdem ein Apothekenrechenzentrum uns den Verlust eines Paketes mit Originalrezepten anzeigte, haben wir diesen Fall nicht nur datenschutzrechtlich bewertet, sondern auch zum Anlass genommen, stichprobenartig die Aufträge zur Datenverarbeitung zwischen Apotheken und deren Rechenzentren zu prüfen.

Das Apothekenrechenzentrum teilte mit, dass ein Paket mit Originalrezepten nicht bei der AOK Nordost angekommen sei und man über den Paketdienst, der den Transport übernommen hatte, dessen Verbleib versuche zu klären.

Letztlich war das Paket wohl bei einem Einbruch in einem Depot des Paketdienstes verschwunden. Die verantwortliche Apotheke erfuhr davon nichts und konnte so nicht prüfen, ob sie verpflichtet war, uns den Datenverlust wegen drohender schwerwiegender Beeinträchtigungen der betroffenen Kunden gemäß § 42a Bundesdatenschutzgesetz (BDSG) zu melden. Es stellte sich zudem heraus, dass erforderliche Vereinbarungen zwischen Apotheke und Rechenzentrum nicht bestanden.

Bei der Abrechnung der Apotheken mit den Krankenkassen ist das dafür von den Apotheken eingeschaltete Rechenzentrum lediglich Auftragnehmer einer Datenverarbeitung im Auftrag. Für diese ist ein schriftlicher Vertrag gemäß § 11 BDSG erforderlich. Darin ist u. a. zu regeln, dass der Auftragnehmer den Auftraggeber über Verletzungen des Datenschutzes zu informieren hat. Dieser bleibt nämlich dafür verantwortlich, eine Meldepflicht gemäß § 42a BDSG zu prüfen. Im konkreten Fall konnte die Apotheke der Pflicht nicht nachkommen, da sie von dem Diebstahl nicht erfuhr. Das Rechenzentrum sagte zu, nunmehr alle erforderlichen Vereinbarungen mit seinen Auftraggebern zu treffen.

Wir nahmen den Fall zum Anlass, bei ausgewählten Apotheken eine Stichprobe zur Einhaltung datenschutzrechtlicher Anforderungen bei der Beauftragung von Rechenzentren vorzunehmen. Diese kam im Wesentlichen zu folgendem Ergebnis:

- Schriftlicher Vertrag

  Alle Apotheken der Stichprobe hatten von der im Fünften Buch Sozialgesetzbuch eingeräumten Möglichkeit Gebrauch gemacht, ein Rechenzentrum in die Abrechnung mit den Krankenkassen einzubeziehen. Eine Apotheke hielt dabei die Vorschrift des Sozialgesetzbuches für ausreichend und hatte keinen schriftlichen Vertrag über eine Datenverarbeitung im Auftrag geschlossen. Sie hat jedoch erklärt, jetzt auf eine solche Vereinbarung zu drängen.

- Auswahlkriterien für den Vertragspartner

  Bei den Auswahlkriterien für einen Dienstleister standen Erfahrung, Qualität, Service und Vertragskonditionen im Allgemeinen im Vordergrund, zugleich legte immerhin die Hälfte der Apotheker auch ausdrücklich Wert auf angemessenen Datenschutz beim Apothekenrechenzentrum.

- Unterauftragsverhältnisse

  Unterauftragsverhältnisse sind bei einem Drittel der Apotheken grundsätzlich vertraglich ausgeschlossen und bei einem Drittel möglich; ein Drittel konnte hierzu keine Aussage treffen. Unterauftragnehmer, sofern es sie denn gibt, waren den Apotheken nicht bekannt. In einzelnen Verträgen wurde die Entsorgung von Datenträgern zudem nicht als Unterauftragsverhältnis qualifiziert, obwohl sie ein ganz typisches Beispiel für eine Datenverarbeitung im Auftrag ist – es sei denn, die Kenntnisnahme personenbezogener Daten wäre dabei ausgeschlossen. Nach unserer Auffassung lässt das Sozialgesetzbuch jedoch überhaupt keine Unterauftragsverhältnisse zu.

- Kontrollpflichten

  Die Mehrzahl der Apotheken war in der Vergangenheit ihrer regelmäßigen Pflicht zur Kontrolle der vom Rechenzentrum einzuhaltenden technischen und organisatorischen Maßnahmen nicht nachgekommen. Zum Teil wurde auf die Entfernung zum Auftragnehmer oder die sehr große Kundenzahl des Dienstleisters hingewiesen, die eine Vor-Ort-Kontrolle schwierig machten; zum Teil wurde dies mit der fehlenden Fachkunde der Apotheker für eine solche Prüfung begründet. Eine Apotheke hatte allerdings eine Besichtigung bei ihrem Rechenzentrum vorgenommen. Für sie war die nötige strikte Trennung ihrer Daten von denen anderer Apotheken ein wesentliches Auswahlkriterium gewesen.

  Etwa die Hälfte der Apotheken sprach sich für ein schriftliches Kontrollverfahren aus bzw. für einen Abruf eines aussagekräftigen Zertifikats auf der Website des Rechenzentrums. Verständlich ist der darin zum Ausdruck kommende Gedanke, grundsätzlich einen praktikablen Weg für Kontrollen zu wählen, nicht zuletzt wegen der oben genannten Gründe. Auch wird dem Auftragnehmer bei einem großen Kundenstamm ggf. die Koordinierung einer Vielzahl von Kontrollen erleichtert. Insofern sind Vorlagen von Prüfprotokollen und speziellen Zertifikaten (inklusive der Zertifizierungsberichte) grundsätzlich ein guter Ansatz.

  In zwei Verträgen fanden wir Regelungen, wonach das Überlassen von objektiv ausreichenden Prüfprotokollen zu technisch-organisatorischen Maßnahmen im Rechenzentrum das Kontrollrecht des Auftragnehmers vor Ort ersetzt. Es kann allerdings unseres Erachtens nicht sein, dass der Auftragnehmer durch interne Prüfprotokolle jegliche Vor-Ort-Kontrolle durch den Auftraggeber abwenden kann. Die Prüfprotokolle sollten daher von unabhängigen Stellen oder Behörden stammen. Auch darf diese Vereinbarung nur im Regelfall greifen, ein Vor-Ort-Kontrollrecht jedoch nicht absolut ausgeschlossen werden.

- Informationspflichten nach § 42a BDSG

  Alle Apotheken, die eine schriftliche Vereinbarung nach § 11 BDSG getroffen hatten, versicherten, dass sie vom Rechenzentrum bei einer Gefährdung ihrer Patientendaten zeitnah informiert würden, um ihren Meldepflichten umgehend nachkommen zu können.

Wir werden die Prüfergebnisse zum Anlass nehmen, mit dem Apothekerverband Brandenburg e. V., bei dem fast alle Apotheken im Land Brandenburg Mitglieder sind, insbesondere die Problemfelder „Unterauftragsverhältnisse“ und „Ausübung der Kontrollpflichten der Apotheken gegenüber den Rechenzentren“ zu erörtern.

Das Sozialgesetzbuch gestattet es den Apotheken, Rechenzentren mit der Abrechnung zu betrauen. Zwischen den Vertragspartnern ist dazu eine schriftliche Vereinbarung über eine Datenverarbeitung im Auftrag zu treffen. Vor Beginn der Datenverarbeitung und regelmäßig während der Vertragslaufzeit hat sich die Apotheke von den beim Auftragnehmer getroffenen technischen und organisatorischen Maßnahmen zu überzeugen. Sie bleibt in diesem Verhältnis die verantwortliche Stelle für die Daten der Krankenversicherten.

6.6 Überführung von Daten zum Infektionsschutz in ein neues Softwaresystem durch Externe

Die Überführung von Datenbanken eines Gesundheitsamtes mit u. a. namentlichen Infektionsmeldungen in ein neues Softwaresystem sollte nach Vorstellung des Landkreises von dem programmanbietenden Unternehmen im Rahmen einer Datenverarbeitung im Auftrag vorgenommen werden. Der behördliche Datenschutzbeauftragte hatte sich längere Zeit darum bemüht, zum Schutz der Gesundheitsdaten und zur Wahrung der ärztlichen Schweigepflicht eine Konvertierung durch eigene Mitarbeiter des Gesundheitsamtes zu erreichen, bevor er unsere Unterstützung erbat.

Nach dem Brandenburgischen Gesundheitsdienstgesetz gilt für die Datenverarbeitung im Auftrag das Brandenburgische Datenschutzgesetz. Nicht sensitive personenbezogene Daten des Gesundheitsamtes, z. B. aus dem Modul „Kommunalhygiene“, können danach problemlos von einem externen Unternehmen im Auftrag verarbeitet werden. Hinsichtlich der sensitiven Gesundheitsdaten ist demgegenüber die besondere Schweigepflicht der Mitarbeiter des Gesundheitsamtes zu beachten. Ihre Verarbeitung im Auftrag war zum damaligen Zeitpunkt nur dann zulässig, wenn durch technische oder organisatorische Maßnahmen eine Kenntnisnahme dieser Angaben durch

den Auftragnehmer sicher ausgeschlossen werden konnte. Insbesondere bei der geplanten Altdatenanalyse durch das Unternehmen, der Übermittlung von Korrekturhinweisen dorthin und der Endkonvertierung schien diese Voraussetzung nicht gewährleistet zu sein. Für namentliche Infektionsmeldungen lehnten wir daher die vom Landkreis angestrebte Lösung ab.

Erst der deutliche Hinweis, dass die Offenbarung von Patientendaten an einen externen Dienstleister zum damaligen Zeitpunkt[42] unter Strafe stand, überzeugte die Kreisverwaltung davon, der Empfehlung der Landesbeauftragten zu folgen.

Letztlich entschloss sich der Landkreis, die Überführung der personenbezogenen Gesundheitsdaten des Sachgebietes Infektionsschutz selbst zu erledigen.

Der Umstand, dass bei der Verarbeitung von Gesundheitsdaten neben datenschutzrechtlichen Anforderungen die ärztliche Schweigepflicht eine zusätzliche Hürde darstellt, wurde in der Vergangenheit häufig verkannt. Für die Datenverarbeitung im Auftrag hat sich der Gesetzgeber dieses Themas nun endlich angenommen.

6.7 Einsatz externer Dienstleister durch Berufsgeheimnisträger – Änderung des Strafgesetzbuches

Im Berichtszeitraum wurde das Strafgesetzbuch dahingehend geändert, dass Ärzte, Zahnärzte oder Apotheker durch die Beauftragung externer IT-Dienstleister künftig nicht mehr gegen ihre besondere Schweigepflicht verstoßen und sich dadurch strafbar machen. Im Gegenzug unterliegen ihre Auftragnehmer ihrerseits der Schweigepflicht und sind strafrechtlich selbst für deren Durchbrechung verantwortlich. Auf eine solche Regelung hatten die unabhängigen Datenschutzbehörden des Bundes und der Länder lange gedrungen.

§ 203 Strafgesetzbuch bestimmte bislang, dass das Teilen geschützter Geheimnisse u. a. durch einen Arzt, Zahnarzt, Apotheker mit seinen eigenen berufsmäßig tätigen Gehilfen oder den bei ihm zur Vorbereitung auf den Beruf tätigen Personen kein unbefugtes Offenbaren dieser Geheimnisse darstellt und mithin nicht strafbar ist. Für sonstige Personen, die an der beruflichen oder dienstlichen Tätigkeit eines Berufsgeheimnisträgers mitwirken, soweit eine Offenbarung für die Inanspruchnahme der Tätigkeit der sonstigen Person erforderlich ist, galt dies jedoch nicht. Damit machten sich Ärzte, Zahnärzte oder Apotheker durch die Weitergabe von der Schweigepflicht unterliegenden Informationen an externe Dienstleister strafbar, auch wenn sie

[42] Zur aktuellen Rechtslage siehe B 6.7.

auf diese Dienstleistungen angewiesen waren. Umgekehrt konnten die Auftragnehmer strafrechtlich nicht zur Verantwortung gezogen werden, da sie nicht der Schweigepflicht unterlagen.

Die Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder hatte bereits im Jahre 2015 eine Anpassung dieser Regelung gefordert, fand zunächst jedoch beim Gesetzgeber kein Gehör.[43] Nachdem die Bundesregierung im Jahre 2017 doch noch einen entsprechenden Gesetzentwurf vorlegte, forderte die Konferenz eine Harmonisierung des Datenschutzrechts und des Strafrechts sowie eine Ausweitung der Zeugnisverweigerungsrechte und des Beschlagnahmeschutzes auf alle Dienstleister.[44] Durch die inzwischen weitgehend in Kraft getretenen Änderungen des § 203 Strafgesetzbuch hat der Gesetzgeber die Rechtslage an die realen Verhältnisse angepasst und so mehr Rechtsklarheit geschaffen.[45]

Entscheidende Bedeutung kommt in der Neuregelung dem Oberbegriff der „mitwirkenden Person“ zu. Er umfasst die Gehilfen der primär Schweigepflichtigen, die bei ihnen zur Vorbereitung auf den Beruf tätigen Personen sowie weitere Mitarbeiter und Helfer (z. B. eigenes Reinigungspersonal), aber auch externe Dienstleister, die an der beruflichen oder dienstlichen Tätigkeit eines Berufsgeheimnisträgers mitwirken. Dieser Personengruppe gegenüber sind Ärzte, Zahnärzte und Apotheker künftig befugt, fremde Geheimnisse, die der Schweigepflicht unterliegen, zu offenbaren, soweit dies für die Inanspruchnahme der Tätigkeit erforderlich ist. Gleichzeitig ist die unbefugte Preisgabe von Patientengeheimnissen nun auch für jegliche mitwirkende Person strafbar. Zusätzlich macht sich ein Berufsgeheimnisträger strafbar, wenn eine sonstige mitwirkende Person die Schweigepflicht verletzt und er sie nicht zur Geheimhaltung verpflichtet hatte. Nur, wenn beispielsweise ein Dienstleister selbst Arzt, Zahnarzt oder Apotheker ist, hat die fehlende Verpflichtung keine Auswirkungen auf den Auftraggeber. Letzterer kann sich darauf verlassen, dass der Auftragnehmer seine gesetzlichen Pflichten kennt. Parallel zur Änderung des Strafgesetzbuches wurden auch das Zeugnisverweigerungsrecht auf alle mitwirkenden Personen ausgedehnt und das grundsätzliche Beschlagnahmeverbot einheitlich geregelt.

Um sicherzustellen, dass durch die Gewährung des Zugangs zu fremden Geheimnissen künftig auch nicht gegen berufsrechtlich festgelegte Verschwiegenheitspflichten verstoßen wird, sollten zum einen die standesrechtlichen Bestimmungen zur Verschwiegenheitspflicht angepasst werden, zum anderen sind ergänzende gesetzliche Befugnisnormen erforderlich, die die

43 Tätigkeitsbericht 2014/2015, A 2.1.

44 Siehe Anlage 1.3.3.

45 Gesetz zur Neuregelung des Schutzes von Geheimnissen bei der Mitwirkung Dritter an der Berufsausübung schweigepflichtiger Personen vom 30. Oktober 2017 (BGBl. I S. 3618).

Voraussetzungen und Grenzen der Inanspruchnahme von Dienstleistungen Dritter näher regeln. Für Rechts- und Patentanwälte, Notare, Steuerberater und Wirtschaftsprüfer hat der Bundesgesetzgeber bereits Regelungen getroffen. Für den Gesundheitsbereich ist der Landesgesetzgeber noch in der Pflicht, entsprechende Normen zu schaffen.

Nachdem der Bundesgesetzgeber die strafrechtlichen Regelungen für die Einbeziehung externer Dienstleister durch Berufsgeheimnisträger in sinnvoller Weise geändert hat, bedarf es nunmehr der Anpassung landesgesetzlicher Regelungen im Gesundheitsbereich.

6.8 Akten- und Datenträgervernichtung im Gesundheitsbereich

Mit der Verarbeitung hoch schutzbedürftiger Daten im Gesundheitsbereich müssen auch Prozesse und Maßnahmen etabliert werden, die eine datenschutzgerechte Vernichtung von Dokumenten und elektronischen Datenträgern sicherstellen. Welche sind das?

Öffentliche und nicht öffentliche Daten verarbeitende Stellen sind nach dem einschlägigen Vorschriften über den Datenschutz dazu verpflichtet, Datenträger, auf denen personenbezogene Daten gespeichert sind, dann zu löschen, wenn ihre Speicherung unzulässig oder ihre Kenntnis für die Aufgabenerfüllung bzw. zur Erfüllung des Zwecks der Speicherung nicht mehr erforderlich ist. Das Löschen oder Vernichten muss ein irrreversibler Prozess sein, der sicherstellt, dass die Daten nicht mehr zurückgewonnen werden können.

Im Gesundheitsbereich erhalten wir immer wieder Anfragen zur Umsetzung der Löschpflicht, insbesondere zur datenschutzgerechten Entsorgung durch externe Auftragnehmer. Für Krankenhäuser in Brandenburg gelten sowohl die Vorschriften des Brandenburgischen Datenschutzgesetzes (BbgDSG) als auch die landesrechtlichen Vorschriften über Krankenhäuser im Krankenhausentwicklungsgesetz. Da im zuletzt Genannten keine Regelungen zur Datenverarbeitung im Auftrag getroffen worden sind, kommen die Vorschriften des § 11 BbgDSG zur Anwendung. Die Patientendaten unterliegen darüber hinaus der ärztlichen Schweigepflicht gemäß § 203 Strafgesetzbuch. Sie dürfen gemäß Abs. 3 Satz 2 dieser Regelung gegenüber sonstigen mitwirkenden Personen nur offenbart werden, soweit diese für die Inanspruchnahme der Tätigkeit dieser Personen erforderlich ist. Eine solche Erforderlichkeit sehen wir für die Tätigkeit eines Entsorgungsdienstes jedoch nicht, sodass technische und organisatorische Maßnahmen zu treffen sind, die eine Wahrung des Geheimnisses sicherstellen. Hat nun der Dienstleister im Zuge des Entsorgungsprozesses (z. B. beim Öffnen einer verschlossenen Entsorgungstonne mit Papierunterlagen) die Möglichkeit, patientenbezogene Anga-

ben über die Gesundheit zur Kenntnis zu nehmen, ist dies nach § 11 Abs. 2 Satz 3 BbgDSG unzulässig. Eine Einwilligungslösung dazu wäre zwar theoretisch möglich, ist aber nach unserer Einschätzung praktisch kaum umzusetzen. Die datenschutzkonforme Vernichtung von Patientendaten sollte deshalb vor Ort, entweder durch das Krankenhaus selbst oder mittels eines beaufsichtigten Dienstleisters (z. B. mobile Datenträgervernichtung) erfolgen und entsprechend der DIN 66399 „Büro- und Datentechnik – Vernichtung von Datenträgern“ nach der Schutzklasse 3 und der Sicherheitsstufe 5 (besser 6) umgesetzt werden.

Gleiches gilt auch für Stellen des Gesundheitsbereichs, die außerhalb von Krankenhäusern Patientendaten verarbeiten (z. B. Arztpraxen). Üblicherweise kommen hier Aktenvernichter mit der o. g. Sicherheitsstufe zum Einsatz. In jedem Fall sollte darauf geachtet werden, dass dem Gerät eine ausreichende Mindestmenge an zu vernichtenden Dokumenten zugeführt und das Vernichtungsgut stichprobenartig kontrolliert wird.

Sollen patientenbezogene Daten im Gesundheitsbereich datenschutzgerecht vernichtet werden, ist immer darauf zu achten, dass die gewählte Sicherheitsstufe dem hohen Schutzbedarf angemessen ist und die ärztliche Schweigepflicht auch gegenüber einem Dienstleister gewahrt bleibt.

6.9 Akteneinsicht Betroffener bei Körperschaften des öffentlichen Rechts

Mit Auskunfts- und Akteneinsichtsrechten Betroffener bei berufsständischen Kammern und anderen Körperschaften des öffentlichen Rechts im Gesundheitswesen waren wir im Berichtszeitraum verstärkt befasst.

6.9.1 Aufsichtsrechtliche und berufsgerichtliche Verfahren einer Kammer

Mit einer Kammer haben wir erörtert, inwieweit verletzte oder geschädigte Patienten Auskunfts- bzw. Einsichtsrechte gegenüber dieser Körperschaft haben, wenn der von ihnen angezeigte Pflichtverstoß eines Therapeuten zu einem aufsichtsrechtlichen oder berufsgerichtlichen Verfahren führt. Dabei geht es beispielsweise um die Einsicht in Verfahrensunterlagen (z. B. Stellungnahmen eines Arztes) oder um die Auskunft zum Ergebnis des Verfahrens.

Die Kammer ging davon aus, dass während eines laufenden aufsichtsrechtlichen Verfahrens nur ein Verfahrensbeteiligter auf der Grundlage des vorrangig anzuwendenden Verwaltungsverfahrensgesetzes Akteneinsicht erhalten könne. Da der Beschwerde führende Patient aber kein Verfahrensbeteiligter

in diesem Sinne ist und das Verwaltungsverfahrensrecht den datenschutzrechtlichen Auskunftsanspruch verdränge, komme eine Auskunft an den betroffenen Patienten nicht infrage. Vielmehr trete dessen Wunsch hinter das Interesse des Therapeuten zurück.

Grundsätzlich hat ein Betroffener (z. B. Patient) nach § 18 Brandenburgisches Datenschutzgesetz einen Auskunfts- bzw. Akteneinsichtsanspruch hinsichtlich seiner eigenen Daten. Selbst wenn ein Vorrang des Verwaltungsverfahrensrechts gegenüber diesem Anspruch angenommen werden sollte, hat nach unserer Auffassung ein Patient stets Anspruch auf eine pflichtgemäße Ermessensentscheidung über seinen Auskunfts- bzw. Akteneinsichtsantrag. Das Verwaltungsverfahrensgesetz schließt „die Gewährung der Akteneinsicht und die Erteilung von Auskünften durch die Behörde an Dritte nicht aus, sofern ein Geheimhaltungsbedürfnis (§ 30) dem nicht entgegensteht.“[46] Es darf zudem nicht automatisch davon ausgegangen werden, dass das Geheimhaltungsinteresse der Beteiligten nach dem Verwaltungsverfahrensrecht stets das Einsichtsinteresse nicht beteiligter Betroffener überwiegt.

Ergänzend bezog sich die Kammer auf gerichtliche Entscheidungen,[47] nach denen Dritte, wie beispielsweise Beschwerde führende Patienten, keinen Anspruch darauf haben zu erfahren, ob und welche Maßnahmen gegen ein Kammermitglied ergriffen werden. Diese Ansicht teilen wir und haben in einem vergleichbaren Fall eine andere Stelle auch bei der Verweigerung der Auskunftserteilung gegenüber einem Antragsteller unterstützt. Dabei geht es nämlich um Angaben über den Arzt, gegen den das Verfahren geführt wurde, nicht jedoch um Daten des Auskunftsbegehrenden. Dieser hat nur dann einen Auskunfts- bzw. Akteneinsichtsanspruch, soweit der Arzt im Rahmen des aufsichtsrechtlichen Verfahrens Angaben über ihn mitgeteilt hat.

Im Zusammenhang mit berufsgerichtlichen Verfahren halten wir Einsichtsrechte eines Betroffenen aufgrund des allgemeinen Datenschutzrechts für ausgeschlossen. Schon der Umstand, dass nach § 59 Abs. 3 Heilberufsgesetz des Landes Brandenburg nur in besonderen Fällen auf eine Veröffentlichung der Entscheidung erkannt werden kann, spricht gegen voraussetzungslose, umfassende Informationen an andere Stellen oder Personen. Außerdem sind Entscheidungen nach dem Heilberufsgesetz nur dem Beschuldigten, seinem Beistand und den Antragsberechtigten, also der Kammer oder einer Aufsichtsbehörde zuzustellen. Im Übrigen verweist das Heilberufsgesetz auf die Vorschriften der Strafprozessordnung. Danach kann ein Rechtsanwalt für den Verletzten die Akten, die dem Gericht vorliegen oder

---

46 Beschluss des Bundesverwaltungsgerichts vom 21. März 1986, BVerwG 7C 71.83 (BVerwGE 74, 115, 119).

47 Urteil des Verwaltungsgerichts Hannover vom 19. September 2007, 5 A 3261/05, und Beschluss des Oberverwaltungsgerichts Niedersachsen vom 29. Januar 2008, 11 LA 448/07.

diesem im Falle der Erhebung der öffentlichen Klage vorzulegen wären, einsehen sowie amtlich verwahrte Beweisstücke besichtigen, soweit er hierfür ein berechtigtes Interesse darlegt. Die Einsicht in Akten ist zu versagen, soweit überwiegende schutzwürdige Interessen des Beschuldigten oder anderer Personen entgegenstehen. Unter Umständen können dem Verletzten Auskünfte und Abschriften aus den Akten erteilt werden. Im Einzelfall ist es daher denkbar, dass Auskunfts- oder Einsichtsrechte von Verletzten in oder nach berufsgerichtlichen Verfahren auf der Grundlage der Strafprozessordnung erfolgreich geltend gemacht werden. Dies sah auch die Kammer so.

6.9.2 Versand aus Datenschutzgründen nur per Einschreiben?

In einem anderen Fall hatte ein Betroffener nach einem Schriftwechsel mit einer öffentlichen Stelle einen Antrag auf Akteneinsicht gestellt. Die Stelle hielt es aus Datenschutzgründen für erforderlich, Unterlagen mit sensitiven Daten nur als Einschreiben zu versenden. Um die daraus entstehenden Versandkosten einzusparen, sollten Betroffene grundsätzlich die Kopien vor Ort abholen.

Eine vom Antragsteller eines Auskunftsbegehrens angegebene postalische Anschrift, die der Daten verarbeitenden Stelle vor dem Auskunftsantrag bereits bekannt war, darf regelmäßig für die Zusendung von Schriftstücken mit Sozial- und Patientendaten genutzt werden. Ein Identitätsmissbrauch scheint in einem solchen Fall eher unwahrscheinlich. Zum Schutz sensitiver Daten genügt aus unserer Sicht der einfache postalische Versand in einem – ohnehin dem Briefgeheimnis unterliegenden – verschlossenen Umschlag. Dieser sollte mit gut lesbaren Absenderangaben versehen sein, um zu vermeiden, dass die Sendung im Falle der Nichtzustellbarkeit geöffnet wird.

In einem Flächenland wie Brandenburg ist die Forderung, Akten vor Ort einzusehen oder Kopien dort abzuholen, problematisch, weil sie insbesondere bei langen Anfahrtswegen eine Hürde für die Ausübung der Rechte der Betroffenen darstellt. Wenn die Antragsteller aus Zeit-, Entfernungs- oder sonstigen persönlichen Gründen eine andere Variante bevorzugen, sollte deren Wunsch im Hinblick auf das Recht auf informationelle Selbstbestimmung grundsätzlich gefolgt werden.

6.9.3 Auskunft über vom Betroffenen selbst übermittelte Daten

In einem weiteren Fall erhielt ein Antragsteller auf sein Auskunftsbegehren hin nur die Information, in welchen Datenfeldern Informationen über ihn gespeichert waren. Dies hielt die Daten verarbeitende Stelle für ausreichend, weil die Angaben vom Betroffenen selbst stammten.

Werden einem Antragsteller die konkret zu seiner Person gespeicherten Daten vorenthalten, kann er nicht feststellen, ob seine Angaben korrekt erfasst wurden. Schon im Hinblick auf mögliche Berichtigungs- und Löschungsansprüche ist es für den Betroffenen daher wichtig, nicht nur allgemeine Informationen zu erhalten.

Dem grundrechtlichen Anspruch eines datenschutzrechtlich Betroffenen auf Auskunft oder Akteneinsicht kann auch während eines laufenden Verwaltungsverfahrens zur Geltung verholfen werden. In vielen Fällen ist die Auskunftserteilung Voraussetzung für die Inanspruchnahme weiterer Betroffenenrechte wie z. B. des Rechts auf Berichtigung oder Löschung.

6.10 Anforderung von Patientenunterlagen eines Verstorbenen durch eine Krankenkasse

Eine Krankenkasse beabsichtigte, im Interesse der Erben eines verstorbenen Versicherten Einsicht in dessen Patientenakte zu nehmen. Sie bezog sich auf ihre gesetzlich geregelte Aufgabe, Versicherte bei der Verfolgung von Schadensersatzansprüchen, die aus vermuteten Behandlungsfehlern entstanden sind, zu unterstützen. Ihren Anspruch auf Einsicht in die Patientendokumentation stützte die Krankenkasse auf § 630g Abs. 3 Bürgerliches Gesetzbuch (BGB), nach dem Erben Einsicht in die Patientendokumentation nehmen können. Der um Auskunft ersuchte Arzt beschwerte sich bei uns über das Ansinnen der Kasse.

Eine Datenverarbeitung durch eine Krankenkasse mit dem Ziel, einen Versicherten bei Behandlungsfehlern nach § 66 Fünftes Buch Sozialgesetzbuch (SGB V) zu unterstützen, lässt sich auf § 284 SGB V stützen. Die Geltendmachung eines zivilrechtlichen Akteneinsichtsanspruchs ist in dieser gesetzlichen Grundlage zur Datenverarbeitung jedoch nicht aufgeführt. Ob der Versicherte selbst in diesem Zusammenhang die Krankenkasse beauftragen könnte, sein Recht auf Akteneinsicht geltend zu machen, ist schon fraglich.

Unserer Ansicht nach kommt als Unterstützungsleistung regelmäßig die Information des Versicherten über Kenntnisse und Erfahrungen der Krankenkasse in Frage, die die Geltendmachung und Durchsetzung seiner Ansprüche erleichtern oder überhaupt erst ermöglichen. Als unterstützende Maßnahme bei einer Akteneinsicht genügt es deshalb, den Antragsberechtigten auf dieses ihm zustehende Recht und dessen rechtliche Grundlage hinzuweisen sowie nach Möglichkeit auf ein Musterschreiben, das er für seinen Antrag verwenden kann.

Das Versicherungsverhältnis war im vorliegenden Fall aber durch den Tod des Versicherten beendet. Schadensersatzansprüche eines Verstorbenen

gehen nach § 1922 BGB auf seine Erben über, Unterstützungsleistungen nach § 66 SGB V jedoch nicht. Schon der Versicherte selbst hat nur einen Anspruch auf fehlerfreie Ermessensausübung, ob sich die Krankenkasse für seine Unterstützung entscheidet. Die Frage, ob Krankenkassen sich z. B. für vererbte Schmerzensgeldforderungen, die gar nicht mehr ihren Versicherten zugutekommen können, einsetzen dürfen, ist zu verneinen. Dies ergibt sich aus § 59 Erstes Buch Sozialgesetzbuch, wonach Ansprüche auf Sozialleistungen mit dem Tode des Berechtigten erlöschen.

Nach dem Sozialgesetzbuch dürfen Sozialdaten Verstorbener zwar von Sozialleistungsträgern unter erleichterten Voraussetzungen verarbeitet oder genutzt werden. Eine Datenerhebung ist dabei aber nicht vorgesehen. Auch dies spricht gegen eine Befugnis der Krankenkasse, die Erben bei der Durchsetzung seines Akteneinsichtsbegehrens zu unterstützen, da damit zwangsläufig die Erhebung von Daten einherginge.

Aufgrund unserer Intervention beabsichtigt die Krankenkasse, nun ganz darauf zu verzichten, Behandlungsunterlagen Versicherter oder Verstorbener auf zivilrechtlicher Grundlage anzufordern. Vorsorglich informierten wir noch die anderen Krankenkassen in unserem Zuständigkeitsbereich sowie das Ministerium für Arbeit, Soziales, Gesundheit, Frauen und Familie über unsere Auffassung.

Regelmäßig haben Erben eines verstorbenen Versicherten zur Wahrnehmung vermögensrechtlicher Interessen selbst einen Akteneinsichtsanspruch gegen den Behandler des Verstorbenen, sofern dies nicht dem (mutmaßlichen) Willen des Verstorbenen widerspricht (§ 630g Abs. 3 BGB). Eine Datenverarbeitungsbefugnis einer Krankenkasse für die Unterstützung der Erben bei der Durchsetzung ihres Anspruchs sieht das Sozialgesetzbuch aber nicht vor.

6.11 Wohngruppenzuschlag – Erhebung von Daten der Mitbewohner von Versicherten durch eine Pflegekasse

Zum Zweck der Beantragung eines Wohngruppenzuschlags durch pflegebedürftige Versicherte verwendete eine Pflegekasse ein Antragsformular, mit dem Daten weiterer Mitbewohner einer ambulant betreuten Wohngruppe erhoben werden sollten.

Pflegebedürftige in ambulanten Wohngruppen können auf Antrag einen pauschalen, monatlichen Wohngruppenzuschlag erhalten, wenn u. a. mindestens drei Bewohner dieser Gruppe ebenfalls pflegebedürftig sind. Bereits vor Jahren hatten wir uns – damals vorrangig gegenüber der AOK Nordost – für eine datenschutzgerechte Ausgestaltung der Erhebungsbögen für den

sog. Wohngruppenzuschlag eingesetzt.[48] In der Zwischenzeit hat der Gesetzgeber mit § 38a Abs. 2 Elftes Buch Sozialgesetzbuch (SGB XI) eine spezielle Datenerhebungsbefugnis geschaffen. Nunmehr genügt eine Bestätigung des Antragstellers, dass die gesetzlichen Kriterien einer ambulant betreuten Wohngruppe vorliegen. Angaben zu Pflegekasse und Pflegestufe der einzelnen Mitbewohner bedarf es nicht mehr.

Trotz der veränderten Rechtslage verwendete die Innungskrankenkasse Brandenburg und Berlin ein veraltetes Antragsformular für Wohngruppenzuschläge. Nachdem wir sie auf das Versäumnis aufmerksam gemacht hatten, der Neuregelung Rechnung zu tragen, änderte sie unverzüglich das Formular. Sie leitete zudem alle erforderlichen Schritte in die Wege, um die ihr bereits vorliegenden Angaben zu Mitbewohnern von Antragstellern zu löschen. Bei einer internen Überprüfung stellte sie fest, dass solche Anträge verhältnismäßig selten waren und die Antragsteller in den meisten Fällen auch gar keine Angaben zu Mitbewohnern gemacht hatten. Vereinzelt nutzten die Antragsteller veraltete Fremdformulare, sodass die fehlerhafte Datenerhebung nicht einmal von der Pflegekasse zu vertreten war. Soweit sie Daten zu Mitbewohnern gespeichert hatte, waren diese weder recherchierbar noch wurden sie von der Kasse in irgendeiner Weise verwendet.

Die Pflegekasse stellte fest, dass es zunächst einen Auftrag zur Anpassung der Formulare an die neue Rechtslage gegeben hatte, der jedoch – vermutlich infolge verschiedener Umstrukturierungen – in Vergessenheit geriet. Sie konnte auch nicht mehr ermitteln, wer für die mangelnde Umsetzung der Formularänderung Verantwortung trug. Die Pflegekasse sagte zu, für die Zukunft insoweit Konsequenzen zu ziehen und zugleich ihre Mitarbeiter in Datenschutzangelegenheiten zu belehren.

Um unzulässige Datenerhebungen zu vermeiden, sind entsprechende Formulare bei Änderungen der Rechtsgrundlagen unverzüglich anzupassen.

7 Informationsverarbeitung in der Landesverwaltung

7.1 Informationssicherheitsmanagement in der Landesverwaltung

Das Informationssicherheitsmanagementteam (ISMT) ist das oberste Arbeitsgremium zu Fragen der Informationssicherheit in der Landesverwaltung. Es besteht aus den Informationssicherheitsbeauftragten der Ressorts und wird vom IT-Sicherheitsmanager des Landes geleitet. Seit

48 Tätigkeitsbericht 2012/2013, B 6.3.

seiner Gründung im Jahr 2008 wirkt unsere Behörde beratend in diesem Gremium mit.[49]

Die wesentlichen Aufgaben des ISMT werden in der Informationssicherheitsleitlinie der Landesverwaltung definiert. Sie bestehen u. a. darin, ressortübergreifende landesweite Sicherheitsrichtlinien und -standards zu entwickeln und fortzuschreiben, den ressortübergreifenden Sicherheitsprozess zu initiieren und zu begleiten, die Umsetzung der zentralen Informationssicherheitsleitlinie der Landesverwaltung zu kontrollieren und die Schulung und Sensibilisierung für Informationssicherheit zu unterstützen.

Zu den landesweiten Richtlinien für die Informationssicherheit, die im Berichtszeitraum mit unserer beratenden Unterstützung erörtert und zum Teil verabschiedet wurden, gehören z. B. ein landesweites Kryptokonzept mit zentralen Vorgaben für den Einsatz kryptografischer Verfahren sowie Richtlinien zum Umgang mit mobilen Datenträgern, zur Verhinderung ungesicherter Netzzugänge und zur Behandlung von Sicherheitsvorfällen. Die bereits bestehenden Richtlinien zum Virenschutz in der Landesverwaltung sowie zum Umgang mit mobilen Endgeräten wurden aktualisiert und fortgeschrieben.

Das ISMT befasste sich weiterhin mit der Vorbereitung einer umfassenden Bestandsaufnahme zum Informationssicherheitsmanagement in allen Bereichen der Landesverwaltung. Es wurde ein Fragenkatalog u. a. zur Existenz und Umsetzung behördenspezifischer Sicherheitsrichtlinien, zum Stand der Informationssicherheit in Fachverfahren, zur organisatorischen Stellung der IT-Sicherheitsbeauftragten sowie zu personellen und finanziellen Ressourcen für die Informationssicherheit erarbeitet. Der Katalog wurde zur Beantwortung an die jeweils zuständigen IT-Sicherheitsbeauftragten verteilt. Mit dieser Bestandsaufnahme sollen insbesondere landesweite und vergleichbare Aussagen zum Stand des Sicherheitsmanagements bereitgestellt und gemeinsame Handlungsschwerpunkte für eine bessere Koordination der zukünftigen Arbeiten im Gremium identifiziert werden. Mittlerweile liegen die Antworten vor, sie werden aktuell ausgewertet.

Hervorzuheben sind weiterhin die Aktivitäten im ISMT, Beschäftigte der Landesverwaltung – einschließlich der Führungskräfte – verstärkt für das Thema Informationssicherheit zu sensibilisieren und entsprechende Schulungsveranstaltungen zu organisieren und zu begleiten. Insgesamt nahmen bislang mehrere tausend Verwaltungsmitarbeiter an solchen Veranstaltungen teil. Dazu gehören auch die Beschäftigten unserer Behörde.

---

49 Tätigkeitsbericht 2014/2015, B 8.2.

Vor dem Hintergrund der zunehmenden Komplexität und Vernetzung der Datenverarbeitungsprozesse in der Landesverwaltung sowie der steigenden Gefährdungen durch Angriffe oder Datenmissbrauch wachsen auch die Anforderungen zur Gewährleistung der Informationssicherheit und zur landesweiten Koordination der Aktivitäten im Sicherheitsmanagementteam. Wir werden die erfolgreiche Arbeit dieses Gremiums auch in Zukunft beratend unterstützen.

7.2 E-Akte für Schwerbehindertenangelegenheiten

Mit einem Projekt zur Einführung elektronischer Akten im Schwerbehindertenbereich wandte sich das Landesamt für Soziales und Versorgung an die Landesbeauftragte und bat um Unterstützung und Austausch zur Umsetzung des Datenschutzes.

Auch bei der elektronischen Aktenführung sind ebenso wie bei der Papieraktenführung die geltenden Gesetze zum Datenschutz zu beachten. Dementsprechend dürfen z. B. nur Daten gespeichert werden, die zur Aufgabenerfüllung erforderlich sind. Weiterhin muss die Löschung und Schwärzung nicht notwendiger Informationen möglich sein.

Darüber hinaus müssen die spezifischen Risiken der rein digitalen Datenverarbeitung behandelt werden. Es sind Maßnahmen festzulegen, die die Vertraulichkeit, Integrität, Verfügbarkeit, Authentizität, Revisionsfähigkeit und Transparenz während der Verarbeitung sowie über möglicherweise lange Aufbewahrungszeiträume sicherstellen. Gemäß § 7 Abs. 3 Brandenburgisches Datenschutzgesetz muss vor Inbetriebnahme eines solchen Verfahrens eine schriftliche Freigabe erfolgen, die nur erteilt werden darf, wenn ein aus einer Risikoanalyse entwickeltes Sicherheitskonzept ergeben hat, dass die von dem Verfahren ausgehenden Gefahren für die Rechte und Freiheiten der Betroffenen durch technisch-organisatorische Maßnahmen beherrscht werden können sowie ggf. eine Vorabkontrolle durch den behördlichen Datenschutzbeauftragten stattgefunden hat.

Im konkreten Vorhaben des Landesamtes bestehen aufgrund des hohen Schutzbedarfs bei der Verarbeitung von Schwerbehindertendaten besondere Anforderungen gerade im technisch-organisatorischen Bereich. Hierzu gehören das rechtssichere Scannen eingehender Dokumente,[50] ein angemessenes Rechte- und Rollenkonzept mit sicherer Authentisierung der Mitarbeiter, die verschlüsselte Speicherung und Übertragung sensitiver Daten, digitale Signaturen sowie organisatorische Festlegungen und die Beteiligung des

[50] Siehe auch Technische Richtlinie des Bundesamtes für Sicherheit in der Informationstechnik BSI TR-03138 Ersetzendes Scannen (RESISCAN).

Personalrates insbesondere bezüglich der datenschutzgerechten Protokollierung.[51]

Bereits 2006 hatte die damalige Konferenz der Datenschutzbeauftragten des Bundes und der Länder die Orientierungshilfe “Datenschutz bei Dokumentenmanagementsystemen”[52] veröffentlicht. Dieser sowie dem vom Bundesministerium des Inneren publizierten Organisationskonzept elektronische Verwaltungsarbeit[53] können ausführliche Informationen zur elektronischen Aktenführung entnommen werden.

Viele dieser Aspekte wurden im vorliegenden Konzept des Landesamtes bereits berücksichtigt. Insbesondere begrüßen wir, dass auf einen externen Dienstleister für das Scannen von Dokumenten verzichtet sowie Verschlüsselung und digitale Signierung der Dokumente von Anfang an eingeplant wurden.

Verbesserungsbedarf haben wir allerdings hinsichtlich der datenschutzgerechten Aktenvernichtung sowie der Schwärzung in elektronischen Dokumenten gesehen. Insbesondere dürfen geschwärzte Informationen nicht in die Volltextsuche einbezogen und nicht wieder hergestellt werden können. Außerdem wiesen wir auf die Notwendigkeit regelmäßiger Stichprobenkontrollen der Korrektheit des Scanvorgangs hin.

Einige wichtige Elemente des Konzepts befinden sich noch im Entwicklungsstadium. Die Landesbeauftragte wird das Projekt daher weiterhin begleiten.

Bei Einführung der E-Akte sind die datenschutzrechtlichen Rahmenbedingungen und angemessene Informationssicherheit zwingend zu beachten. Das Landesamt für Soziales und Versorgung hat ein gutes Konzept für die elektronische Aktenführung erarbeitet. Durch die frühzeitige Einbindung der Landesbeauftragten konnten einige Verbesserungen angeregt werden.

7.3 Nutzung externer Plattformen für Datenaustausch und Fortbildung

Das gestiegene Problembewusstsein vieler Beschäftigter der Landesverwaltung für datenschutzrechtliche Fragen äußert sich auch darin, dass unsere Behörde immer häufiger Anfragen von Betroffenen zur Verarbeitung ihrer persönlichen Daten im dienstlichen Zusammenhang erhält. Im Berichtszeitraum betraf dies z. B. die Nutzung von Diensten, die

[51] Siehe dazu auch die Orientierungshilfe „Protokollierung“ der Datenschutzkonferenz, siehe http://www.lda.brandenburg.de.

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

[53] https://www.verwaltung-innovativ.de.

durch Dritte außerhalb der Landesverwaltung angeboten wurden, für den Datenaustausch und die Kollaboration mit Externen sowie für Fortbildungszwecke.

In einem Fall hatte eine Behörde Kooperationsbeziehungen zu einem Unternehmen, die mit dem Austausch von Dateien, ihrer gemeinsamen Bearbeitung und herkömmlicher Projektkommunikation einhergingen. Zur Unterstützung der Zusammenarbeit betrieb das Unternehmen eine Kollaborationsplattform. Hierfür nutzte es ein Softwareprodukt eines ausländischen Herstellers, bei dessen Anwendung nutzerspezifische Daten nicht nur an die Plattform selbst (und damit das Unternehmen), sondern auch an den Produktanbieter ins außereuropäische Ausland übertragen wurden. Dabei handelte es sich mindestens um die Namen der Beschäftigten, ihre dienstliche Erreichbarkeit und die Zugehörigkeit zu Organisationseinheiten. Dies ging aus den Nutzungsbedingungen hervor, die vor dem Beginn der Verwendung der Plattform zu bestätigen waren.

In einem anderen Fall bediente sich eine Behörde einer externen Fortbildungsplattform, um dort Schulungsunterlagen bereitzustellen und Beschäftigten zu ermöglichen, sich mit den Dokumenten auch in ihrer Freizeit zu befassen bzw. darüber auf der Plattform zu diskutieren. Die Plattform ist Produkt eines deutschen Unternehmens und wird auch in einem Rechenzentrum in Deutschland betrieben. Auch hier flossen Daten über die Beschäftigten an den Plattformbetreiber. Die Nutzungsbedingungen, deren Kenntnisnahme von jedem Anwender zu bestätigen war, enthielten auch eine Einwilligung zur Datenweitergabe an den Betreiber sowie eine detaillierte Information zu Umfang und Einzelheiten der Datenverarbeitung. Zu erwähnen ist, dass die elektronische Fortbildungsplattform lediglich ergänzend zu den herkömmlichen Fortbildungsangeboten der Behörde bereitgestellt wurde – Beschäftigte waren somit nicht verpflichtet, sie zu benutzen.

In beiden Fällen kann sich die jeweilige Behörde ihrer datenschutzrechtlichen Verantwortung nicht dadurch entziehen, dass sie die eigentliche Verarbeitung von einem anderen erledigen lässt. Sie muss deshalb zunächst prüfen, ob eine Rechtsgrundlage die Verarbeitung von Beschäftigtendaten erlaubt. In den konkreten Fällen war hierzu § 29 Brandenburgisches Datenschutzgesetz (BbgDSG) heranzuziehen. Danach ist die Verarbeitung personenbezogener Daten von Beschäftigten u. a. dann erlaubt, wenn sie zur Durchführung des Dienstverhältnisses erforderlich oder in einer Rechtsvorschrift, einem Tarifvertrag oder einer Dienstvereinbarung vorgesehen ist. Alternativ käme auch eine Einwilligung des Betroffenen in Betracht, die gemäß § 4 BbgDSG freiwillig, informiert und widerrufbar sein muss. Zu den weiteren Vorschriften des Gesetzes, die die Behörde beachten muss, gehört auch der Abschluss eines schriftlichen Vertrages gemäß § 11 BbgDSG über die Datenverarbeitung im Auftrag, wenn bei der Verarbeitung ein externer Dienstleister einbezogen

werden soll. Dieser muss die Regelungen des Brandenburgischen Datenschutzgesetzes einhalten und darf die Daten nur auf Weisung des Auftraggebers verarbeiten. Insofern behält Letzterer die Kontrolle über die Datenverarbeitung.

In den beiden geschilderten Fällen gingen wir davon aus, dass der Betrieb der Kollaborationsplattform bzw. des Fortbildungsangebots grundsätzlich zulässig war; im einen Fall auf der Basis der gesetzlichen Rechtsgrundlage, im anderen Fall auf Basis der Einwilligung. Allerdings gab es weder hier noch da Verträge gemäß § 11 BbgDSG. Deren Abschluss war nachzuholen. In der Regel stellt dabei die vollständige Einhaltung der brandenburgischen Rechtsvorschriften durch den Auftragnehmer dann keine Hürde dar, wenn er seinen Sitz in Deutschland oder Europa hat.

Kritisch sahen wir jedoch im Falle der Kollaborationsplattform die zusätzliche Weitergabe der Beschäftigtendaten an den Hersteller der Software. Dieser hatte seinen Sitz außerhalb Europas. Es bestand die begründete Annahme (auch aus ähnlich gelagerten Fällen in der Vergangenheit), dass der Abschluss eines Vertrages gemäß § 11 BbgDSG mit dem Hersteller scheitern würde. In einem solchen Fall ist der Empfänger der Daten kein Auftragsverarbeiter, sondern Dritter. Wegen der fehlenden vertraglichen Bindung hat die Behörde keine Einflussmöglichkeiten mehr auf die weitere Datenverarbeitung beim Empfänger.

Aus rechtlicher Sicht handelt es sich dann bei der Datenweitergabe an den Softwarehersteller um eine Übermittlung. Diese ist nach § 29 BbgDSG nur zulässig, wenn der Empfänger ein rechtliches Interesse darlegt, der Dienstverkehr es erfordert oder der Betroffene eingewilligt hat. Wir sahen keine der drei Voraussetzungen als erfüllt an. Insbesondere war die einfache Bestätigung der Nutzungsbedingungen nicht mit einer freiwilligen, informierten und widerrufbaren Einwilligung vergleichbar. Insofern stuften wir diese Übermittlung als unzulässig ein.

Wenn öffentliche Stellen des Landes Dienste Externer bei der Verarbeitung von Daten Beschäftigter in Anspruch nehmen, bleiben sie grundsätzlich für die Einhaltung der datenschutzrechtlichen Vorschriften verantwortlich. Insbesondere ist ein schriftlicher Vertrag über die Datenverarbeitung im Auftrag zu schließen. Schlägt dies fehl, muss die Stelle prüfen, ob die strengeren rechtlichen Anforderungen einer Datenübermittlung an Dritte erfüllt sind.

7.4 Mangelnde Aktualisierung eines Verfahrensverzeichnisses

Ein Hobbynutztierhalter hatte von seinem Landkreis ein Formular erhalten, in dem er Auskunft zur Tierhaltung erteilen sollte. Darin wurde er befragt, ob er in der entsprechenden Fachanwendung bereits registriert sei. Der Petent wandte sich an uns, um nähere Informationen zu diesem System zu erhalten. Er wollte u. a. erfahren, welche personenbezogenen Daten in dem Verfahren gespeichert sind und wann diese wieder gelöscht werden.

Bei dem Fachverfahren handelt es sich um ein landesweit verwendetes Softwaresystem zur behördlichen Überwachung im Lebensmittel- und Veterinärbereich, das vom zuständigen Ministerium eingeführt wurde. Das nachgeordnete Landesamt administriert dieses und die Landkreise sind für die Pflege der Daten verantwortlich. Dem Ministerium obliegt die Fachaufsicht sowohl über das Landesamt als auch über die Landkreise hinsichtlich der Fachanwendung. In dieser Rolle bestimmt es alle wesentlichen Aspekte des Verfahrenseinsatzes.

Aufgrund der Anfrage des Petenten haben wir mit dem Landkreis als Daten verarbeitende Stelle Kontakt aufgenommen. Da wir mit diesem nicht alle Aspekte klären konnten, wandten wir uns an das zuständige Ministerium. Insbesondere interessierten wir uns für die Regelfristen zur Sperrung und Löschung der Daten. Hierzu konnten jedoch auch die dortigen Mitarbeiter keine verbindliche Aussage treffen.

Gemäß § 8 Abs. 1 Nr. 8 Brandenburgisches Datenschutzgesetz (BbgDSG) müssen die Regelfristen für die Sperrung und Löschung der Daten in einem Verfahrensverzeichnis schriftlich oder elektronisch festgelegt werden. Unsere Überprüfung des aus dem Jahr 2005 stammenden Verfahrensverzeichnisses ergab, dass Angaben zu den Löschfristen darin von Beginn an nicht enthalten waren. Des Weiteren ist uns aufgefallen, dass bestimmte Sicherheitsmaßnahmen nicht mehr dem Stand der Technik entsprachen. Das Ministerium teilte uns mit, dass die eingesetzte Software trotz fehlender Überarbeitung des Verzeichnisses kontinuierlich den technischen und rechtlichen Erfordernissen angepasst würde. Allerdings wurde die gesetzlich geforderte Fortschreibung des Verfahrensverzeichnisses unterlassen.

Auch fehlte eine Freigabeerklärung für das Verfahren. Diese wird seit der Neufassung des Brandenburgischen Datenschutzgesetzes vom 15. Mai 2008 gefordert. Die Freigabe erfolgt gemäß § 7 Abs. 3 BbgDSG durch die Daten verarbeitende Stelle. Sie kann auch durch die zuständige oberste Landesbehörde oder eine von ihr bestimmte Stelle erteilt werden.

Im konkreten Fall sind die festgestellten Mängel nicht den Landkreisen, sondern dem Aufsicht führenden Ministerium anzulasten. Wir forderten es deshalb auf, das mehr als zehn Jahre alte Verfahrensverzeichnis zu überarbeiten und die Freigabe zu erklären. Trotz mehrfacher Nachfragen wurden uns weder die Regelfristen für die Sperrung und Löschung der Daten mitgeteilt, noch das überarbeitete Verfahrensverzeichnis vorgelegt. Wir sahen uns daher veranlasst, die Leitungsebene des Ministeriums auf die gravierenden Probleme aufmerksam zu machen und forderten diese auf, umgehend mit der Mängelbeseitigung zu beginnen.

Legt eine zuständige oberste Landesbehörde im Rahmen der Fachaufsicht für andere Stellen Einzelheiten der Einführung und des Betriebs eines Fachverfahrens fest, muss sie selbst die damit verbundenen datenschutzrechtlichen Pflichten vollständig erfüllen.

8 Inneres

8.1 Unter welchen Voraussetzungen sind Widersprüche gegen Datenübermittlungen der Meldebehörden wirksam?

Oft möchten Betroffene die Übermittlung ihrer personenbezogenen Daten durch Meldebehörden an andere Stellen dadurch verhindern, dass sie der Weitergabe widersprechen. Doch nicht immer führt ein solcher Widerspruch auch zum gewünschten Ziel.

Immer wieder wenden sich Bürger an unsere Dienststelle und teilen mit, sie hätten bei ihrer Meldebehörde der Weitergabe ihrer personenbezogenen Daten widersprochen. Ziel solcher Widersprüche ist meist die Verhinderung der Datenübermittlung an bestimmte Stellen oder für bestimmte Zwecke. Verärgerung stellt sich dann oft ein, wenn doch ein Brief ins Haus flattert und es naheliegt, dass die Adressdaten von der Meldebehörde stammen. Wir müssen dem Betroffenen in solchen Fällen regelmäßig mitteilen, dass auch, wenn tatsächlich eine Übermittlung stattgefunden hat, ein rechtswidriges Verhalten der Meldebehörde nicht erkennbar ist. Kann die Meldebehörde sich ohne Weiteres über den Willen des Betroffenen hinwegsetzen?

Beim Datenschutz handelt es sich um ein Grundrecht (Art. 11 Verfassung des Landes Brandenburg), in das nur durch Gesetz oder aufgrund von Gesetzen eingegriffen werden darf. Diesem Prinzip entspricht im einfachen Recht das sog. Verbot mit Erlaubnisvorbehalt, nach dem eine Datenverarbeitung nur dann erlaubt ist, wenn ein Gesetz sie vorsieht (vgl. § 4 Abs. 1 Brandenburgi-

sches Datenschutzgesetz). Im Melderecht finden sich solche Rechtsgrundlagen etwa in der Befugnis zur Weitergabe von Meldedaten an öffentliche Stellen, soweit diese Daten für die Arbeit der empfangenden Stelle erforderlich sind – insbesondere in § 34 Bundesmeldegesetz (BMG) und in § 36 Abs. 1 BMG in Verbindung mit der landesrechtlichen Verordnung über regelmäßige Datenübermittlungen der Meldebehörden (MeldDÜV).

Diese Übermittlungsbefugnis wird im Melderecht in verschiedenen Fällen eingeschränkt. So muss die Meldebehörde etwa – auf Antrag des Betroffenen oder von Amts wegen – eine sog. Auskunftssperre (§ 51 Abs. 1 BMG) ins Melderegister eintragen, wenn Tatsachen vorliegen, die die Annahme rechtfertigen, dass der betroffenen oder einer anderen Person durch eine Melderegisterauskunft eine Gefahr für Leben, Gesundheit, persönliche Freiheit oder ähnliche schutzwürdige Interessen erwachsen kann. Sind solche Umstände glaubhaft gemacht und ist eine Auskunftssperre eingetragen, so unterbleibt die Melderegisterauskunft an Private. Gemäß § 8 Abs. 3 MeldDÜV entfällt auch die Regelübermittlung an den Rundfunk Berlin-Brandenburg, nicht jedoch die Melderegisterauskunft im konkreten Einzelfall. Auch wenn der Betroffene nicht in einer persönlichen Gefahrensituation lebt, kann er, wenn ein Gesetz dies bestimmt, einzelnen Datenübermittlungen widersprechen. Das betrifft beispielsweise die Übermittlung von Daten an Parteien, Wählergruppen und andere Träger von Wahlvorschlägen im Zusammenhang mit Wahlen und Abstimmungen, an Adressbuchverlage sowie zur Bekanntgabe von Alters- und Ehejubiläen (§ 50 Abs. 5 BMG).

Die Meldebehörden sind verpflichtet, einmal jährlich ihre Bürger durch ortsübliche Bekanntmachung auf die Widerspruchsrechte hinzuweisen. Die Landesbeauftragte stellt in ihrem Internetangebot Musterschreiben zur Verfügung, um diese Rechte auszuüben. Den Meldebehörden bleibt zu raten, Betroffene möglichst frühzeitig darauf aufmerksam zu machen, wenn ein Antrag erfolglos bleiben muss, weil die gesetzlichen Voraussetzungen nicht vorliegen.

Widersprüche gegen Datenübermittlungen der Meldebehörden sind nur wirksam, wenn die gesetzlichen Voraussetzungen vorliegen. Um die Wahrnehmung dieser Widerspruchsrechte zu erleichtern, stellt die Landesbeauftragte in ihrem Internetangebot entsprechende Musterschreiben zur Verfügung.

8.2 Melderegisterauskünfte bei nicht eindeutigen Anfragen

Uns erreichte die Beschwerde einer Betroffenen, die ein Schreiben eines Inkassodienstes mit einer Zahlungsaufforderung erhalten hatte, aber nicht die Schuldnerin war. Es stellte sich heraus, dass die für sie zustän-

dige Meldebehörde in unzulässiger Weise bei der Feststellung eines mutmaßlichen Schuldners „assistiert“ hatte und dadurch die Daten einer Unbeteiligten – der Betroffenen – herausgegeben hatte.

Der wahre Schuldner der in Streit befindlichen Forderung hatte offensichtlich bei Abschluss eines Vertrages über Telekommunikationsdienstleistungen falsche Angaben zur eigenen Identität gemacht. Da die aus dem Vertrag resultierende Forderung nicht beglichen wurde, überstellte die Gläubigerin den Vorgang an ein Inkassounternehmen zu Schuldnerermittlung und Einzug der Forderung. Dieses stellte eine Meldedatenanfrage gemäß § 44 Bundesmeldegesetz (BMG) mit den vorliegenden, falschen Daten bei der Meldebehörde der amtsfreien Gemeinde, die als angeblicher Wohnsitz des vermeintlichen Schuldners den Daten zu entnehmen war. Diese Anfrage ergab jedoch keine Treffer.

Daraufhin half die Meldebehörde bei der Klärung, indem sie im Zusammenwirken mit dem Inkassounternehmen aus dem ihr übergebenen Datensatz nach und nach Kriterien ausschied, bis ein Treffer – die Daten der Betroffenen – dem übersandten Datensatz entsprach. Es handelte sich bei den zugrunde gelegten Daten nur noch um das Geburtsdatum und die Wohnstraße ohne Hausnummer. Wegen der Übereinstimmung des angegebenen Geburtsdatums mit dem der Betroffenen, welches in der Gemeinde kein zweites Mal existierte, sowie der relativen Namensähnlichkeit des von dem Schuldner verwandten Namens mit dem der Betroffenen, ging die Meldebehörde von Schreibfehlern hinsichtlich der abweichenden Nachnamen und Hausnummer aus. Hierauf gestützt übermittelte die Meldebehörde die Daten der Betroffenen an das Inkassounternehmen, welches diese für ein Vorgehen gegen die Betroffene nutzte. Nachdem sich herausgestellt hatte, dass es sich bei der Betroffenen nicht um die Schuldnerin handelte, unterließ das Inkassounternehmen weitere Beitreibungsversuche.

Personenbezogene Daten dürfen nur weitergegeben werden, wenn hierfür eine Rechtsgrundlage vorhanden ist (§ 4 Abs. 1 Nr. 2 Brandenburgisches Datenschutzgesetz – BbgDSG). Eine solche stellt § 44 BMG mit der Befugnis zur Erteilung einfacher Melderegisterauskünfte zwar zur Verfügung. Allerdings ist eine Erteilung nur rechtmäßig, wenn die Identität der Person, über die eine Auskunft begehrt wird, auf Grund der in der Anfrage mitgeteilten Angaben eindeutig festgestellt werden kann (§ 44 Abs. 3 Nr. 1 BMG). Die Identität muss also durch die vom Antragsteller angegebenen, gesetzlichen Suchkriterien bereits eindeutig bestimmt sein.

Dies war hier nicht der Fall. Es obliegt dem Antragsteller, hier dem Inkassounternehmen, die Daten zu benennen, auf deren Grundlage eine Auskunft erfolgen soll. Ergibt der darauffolgende Abgleich, dass die angefragten Daten keiner Person zugeordnet werden können, hat die Meldebehörde dies – und

nur dies – dem Antragsteller mitzuteilen. Keinesfalls darf sie – und sei ein Fehler auch noch so naheliegend – Angaben des Antragstellers selbstständig korrigieren. Nur so lässt sich die Übermittlung unrichtiger personenbezogener Daten mit den hier eingetretenen – nicht nur datenschutzrechtlichen – Folgeproblemen vermeiden.

Die Gemeinde reagierte in der Folge vorbildlich; ihre Mitarbeiter wurden sensibilisiert und zu rechtmäßigem Handeln angeleitet. Für eine Beanstandung nach § 25 BbgDSG bestand daher keine Veranlassung. Soweit die Rechtmäßigkeit der Datennutzung durch den Inkassodienstleister zu prüfen war, wurde der Vorgang an die insoweit örtlich zuständige Aufsichtsbehörde nach § 38 Bundesdatenschutzgesetz abgegeben.

Um die rechtswidrige Weitergabe personenbezogener Daten zu verhindern, dürfen Meldebehörden Anträge auf Auskunft aus dem Melderegister nur dann beantworten, wenn die Identität der Person auf Basis der Antragsdaten zweifelsfrei feststeht. Etwaige Unklarheiten sind durch den Antragsteller zu klären und nicht mithilfe des Melderegisters.

8.3 Abgleich von Finanz- mit Meldedaten innerhalb einer Stadtverwaltung

Eine Stadt fragte an, ob es zulässig sei, eine Schnittstelle zwischen Melderegisterverfahren und Finanzverfahren in der Weise einzurichten, dass die im Finanzverfahren gespeicherten personenbezogenen Daten regelmäßig automatisiert mit den Meldedaten abgeglichen würden, um Erstere auf dem neuesten Stand zu halten.

Die Kämmereien der Kommunen haben vielfach das Problem, Steuern und Abgaben zu erheben, wenn sich Adressdaten der Schuldner ändern. Daher besteht häufig das Interesse an der Durchführung eines anlassunabhängigen, wiederkehrenden, automatisierten Abgleichs mit dem gesamten Datenbestand, um diesen jederzeit aktuell zu halten. Bei Planungen solcher Art kommt es oft vor, dass den technisch-organisatorischen Möglichkeiten der Einrichtung einer Schnittstelle mehr Aufmerksamkeit geschenkt wird als der rechtlichen Zulässigkeit.

Die Zulässigkeit, ein automatisiertes Abrufverfahren einzurichten, ergibt sich aus § 37 Abs. 2 i. V. m. §§ 39, 40 Bundesmeldegesetz (BMG). Es bedarf der Zulassung durch den Hauptverwaltungsbeamten. Dieser hat die abrufberechtigten Stellen sowie die erforderlichen technischen und organisatorischen Maßnahmen schriftlich festzulegen. Die Meldebehörde hat u. a. die Umstände jedes Abrufs zu protokollieren und ggf. stichprobenartig auszuwerten. Diese Voraussetzungen wären für die Stadt erfüllbar gewesen.

Allerdings ist jeder Abruf nach Art und Umfang nur zulässig, wenn für ihn eine Rechtsgrundlage existiert. Eine Rechtsgrundlage speziell für das in Rede stehende Szenario ist nicht ersichtlich, sodass auf § 37 Abs. 2 S. 1 BMG i. V. m. § 3 Abs. 1 Meldedaten-Übermittlungsverordnung (MeldDÜV) zurückgegriffen werden muss. Danach darf ein Abruf nur erfolgen, wenn dies im Einzelfall zur Erfüllung der Aufgaben der abrufenden Stelle erforderlich ist. Zwar ist es keinesfalls ausgeschlossen, eine Vielzahl von Datensätzen gleichzeitig rechtmäßig abzurufen. Der Abruf muss jedoch hinsichtlich jedes einzelnen Betroffenen zur Erfüllung einer gesetzlichen Aufgabe erforderlich sein. Gesetzliche Aufgabe ist die Sicherung der Möglichkeit, Zustellungen an einzelne Adressen vorzunehmen. Hierzu ist der – in der vorliegenden Form in einem Großteil von Fällen unvermeidliche – Abruf von Daten bei nicht geänderten Datensätzen jedoch nicht erforderlich.

Mit der „Verhinderung der Erosion des Datenbestands“ kann ein solcher Abgleich nicht gerechtfertigt werden. Nicht der Datenbestand ist unrichtig, sondern einzelne Daten. Probleme mit der Richtigkeit von Daten sind daher in Ermangelung einer speziellen Rechtsgrundlage im Einzelfall zu beheben.

Die Alternative, die Meldedaten durch aktives Handeln der Meldebehörde zu übermitteln, verbessert die Situation nicht. Zunächst sind turnusmäßig wiederkehrende, initiative Datenübermittlungen durch die Meldebehörde unzulässig, wenn sie nicht in der Meldedaten-Übermittlungsverordnung erlaubt sind. § 9 MeldDÜV erlaubt den Meldebehörden, den für ihren Bereich zuständigen Finanzämtern zur Sicherung des Steueraufkommens Daten eines Betroffenen zu übermitteln, wenn sich dieser in das Ausland abmeldet. Die Stadtkämmerei ist jedoch weder ein Finanzamt, noch umfasst die Rechtsgrundlage den gesamten Fallkomplex, den die Stadt abdecken will. Selbst Übermittlungen im Einzelfall auf Bitten des Empfängers sind gemäß § 37 Abs. 1 i. V. m. § 34 Abs. 1 BMG nur zulässig, wenn sie erforderlich sind. Die Landesbeauftragte verneinte im Ergebnis die Frage der Stadt nach der Zulässigkeit des von ihr beabsichtigten Abgleichs des gesamten Datenbestands.

Der Abgleich aller Datensätze eines Verfahrens mit dem Melderegister zum Zwecke der Bestandspflege von Personendaten ist regelmäßig nur zulässig, wenn hierfür eine ausdrückliche Rechtsgrundlage besteht. Fehlt eine solche, ist ein vollständiger Abgleich unzulässig, weil er typischerweise Datensätze umfassen würde, die ganz überwiegend bereits richtig sind und keiner Korrektur bedürfen.

8.4 Herausgabe von Informationen durch Katasterämter an Privatpersonen oder Makler

Im Berichtszeitraum erreichte uns eine Vielzahl von Beschwerden Betroffener, deren personenbezogene Daten von Katasterämtern der Landkreise und kreisfreien Städte an Private – typischerweise am Grundstück der Betroffenen interessierte Käufer oder Makler – herausgegeben wurden. Dies nahm die Landesbeauftragte zum Anlass, die Voraussetzungen der Weitergabe personenbezogener Daten mit der Landesregierung und im Einzelfall mit den Landkreisen und kreisfreien Städten zu klären.

Bei der Verarbeitung von Geodaten können das Rechtsgefühl von Betroffenen, die Rechtslage und die Praxis manchmal weit auseinanderklaffen. Eine Vielzahl von Beschwerden kam von Grundstückseigentümern, die überraschend Post von privaten Kaufinteressenten oder Maklern erhielten. Diese erkundigten sich nach Verkaufsabsichten, ohne dass die Betroffenen solche jemals geäußert hätten. Nachdem die Eigentümer ihr Recht auf Auskunft gemäß § 34 Abs. 1 Nr. 1 Bundesdatenschutzgesetz gegenüber den Interessenten ausgeübt und in diesem Zusammenhang nach der Herkunft der Daten gefragt hatten, stellte sich regelmäßig heraus, dass die Quelle das zuständige Katasteramt war. Die Landesbeauftragte hatte die Zulässigkeit der Herausgabe zu klären.

Gemäß § 10 Abs. 1 S. 1 Brandenburgisches Vermessungsgesetz (BbgVermG) sind Geobasisinformationen, zu denen die Katasterdaten gehören, grundsätzlich allen bereitzustellen. § 10 Abs. 1 S. 2 bis 4 der Vorschrift präzisiert jedoch, dass zur Einsicht in personenbezogene Geobasisinformationen – soweit nicht die Einwilligung des Eigentümers vorliegt – ein berechtigtes Interesse des Antragstellers erforderlich ist, welches er in der Regel der Behörde gegenüber glaubhaft machen muss. Berechtigtes Interesse ist allgemein jedes – auch wirtschaftliche – durch die Sachlage gerechtfertigte und von der Rechtsordnung ansonsten gebilligte Interesse. Der Begriff des berechtigten Interesses ist insbesondere weniger restriktiv als der des rechtlichen Interesses, bei dem der Antragsteller die Daten benötigen muss, um etwa einen zivilrechtlichen Anspruch gegen den Betroffenen durchzusetzen.

Nicht ausreichend ist daher das Motiv der bloßen Neugier. Ebenfalls zu verneinen ist das berechtigte Interesse in Fällen, in denen der Behörde bekannt ist, dass ein Verkauf nicht stattfinden kann oder soll. Unzweifelhaft besteht andererseits ein Einsichtsanspruch bei nachweisbar bereits laufenden Verhandlungen erst recht in Fällen eines rechtlichen Interesses, wenn etwa bereits bestehende (vor-)vertragliche gegenseitige Pflichten konkret durchgesetzt werden müssen.

Fraglich bleiben diejenigen Fälle, in denen zwar beim Antragsteller ein Kaufinteresse besteht, jedoch zum Verkaufsinteresse des Betroffenen keine Hinweise vorliegen. Die Landesbeauftragte hatte gegenüber dem zuständigen Ministerium die Auffassung vertreten, dass der Tatbestand des berechtigten Interesses in § 10 Abs. 1 S. 2 BbgVermG restriktiv auszulegen ist, sodass er jedenfalls solche Fälle ausschließt, in denen keinerlei Kontakt mit dem Eigentümer nachweisbar ist.

In weiteren Absprachen mit dem Ministerium wurde Folgendes vereinbart:

- In Fällen, in denen Makler und andere einschlägig gewerblich Tätige keinen Kontakt mit dem Betroffenen nachweisen können, ist die Auskunft hinsichtlich personenbezogener Daten des oder der Eigentümer zu verweigern. Dies gilt auch und insbesondere, wenn sich die Anfrage gleichzeitig auf mehrere Datensätze bezieht. In diesem Fall ist einerseits der Eingriff, den die Weitergabe für den Betroffenen bedeutet, in der Regel weitergehend, weil die Interaktion mit einem professionellen Makler erfahrungsgemäß auch die Intensität der Nutzung der Daten erhöht. Im Fall der Abfrage mehrerer Datensätze liegt zudem der Verdacht nahe, dass sich ein Makler eine private Datenbank zulegen möchte, ohne dass eine Absicht, das Grundstück zu vermakeln, unmittelbar bevorsteht. In der Praxis soll ein Makler zunächst auf die nicht personenbezogenen Inhalte des Katasters verwiesen werden, deren Kenntnisnahme im Umkehrschluss zu § 10 Abs. 1 S. 2 BbgVermG kein berechtigtes Interesse voraussetzt.

- In Fällen, in denen Privatpersonen in der Absicht, ein Grundstück selbst zu erwerben, um Katastereinsicht nachsuchen, soll die Auskunft zu personenbezogenen Daten jedenfalls nicht schon deswegen verweigert werden, weil der Betroffene bisher nicht in Verhandlungen getreten ist. Abgeleitet wird dies aus der grundsätzlichen Publizität nach § 10 Abs. 1 S. 1 BbgVermG im Verhältnis zu dem grundsätzlich als niedriger eingeschätzten Eingriff in die Rechte des Betroffenen durch die weitere Nutzung der Daten. Eine Verweigerung der Auskunft aus anderen Gründen, z. B. wegen fehlender Konkretisierung der Kaufabsicht, bleibt aber möglich.

Das Ministerium hat den Katasterbehörden diese Hinweise übermittelt. Allerdings war bei unseren Nachfragen festzustellen, dass die vorstehende Differenzierung den meisten Behörden nicht bewusst war. Der Landesbeauftragten sind sowohl Landkreise und kreisfreie Städte bekannt, die den Tatbestand des berechtigten Interesses eher weiter auslegen, als auch solche, die eine restriktivere Auslegung anwenden.

Wurden Daten über die vorgenannten Grundsätze hinaus an Kauf- oder Makelinteressenten übermittelt, haben wir auf die beschriebene Vorgehensweise hingewiesen. Auf Beanstandungen gemäß § 25 Brandenburgisches Datenschutzgesetz haben wir in allen Fällen verzichtet, da davon ausgegangen werden konnte, dass die Vorgaben des Ministeriums in Zukunft beachtet werden.

Die Frage, in welchen Fällen Katasterbehörden bei einseitigem Kaufinteresse personenbezogene Daten übermitteln dürfen, ist differenziert zu beantworten. Neben anderen denkbaren Umständen ist entscheidend, ob der die Auskunft Ersuchende ein Makler oder in ähnlicher Weise geschäftsmäßig mit Immobilien befasst ist.

8.5 Die elektronische Gesundheitskarte für Flüchtlinge

In enger Zusammenarbeit mit den Krankenkassen, Ärztekammern, Landkreisen und kreisfreien Städten wurde im Land Brandenburg im Berichtszeitraum die elektronische Gesundheitskarte für Flüchtlinge eingeführt, um diesen den Zugang zur Gesundheitsversorgung zu vereinfachen.

Den rechtlichen Rahmen für die gesundheitliche Versorgung von geflüchteten Menschen bildet das Asylbewerberleistungsgesetz, das den Leistungsanspruch bei Krankheit, Schwangerschaft und Geburt regelt. Bisher mussten sich Asylbewerber in ihrer jeweiligen Kommune von den zuständigen Sozialämtern einen Behandlungsschein ausstellen lassen. Dabei lag die Entscheidung beim einzelnen Behördenmitarbeiter. Bei Unklarheiten war ein Amtsarzt hinzuzuziehen.

Um ein landesweit einheitliches Verfahren der Gesundheitsversorgung für Flüchtlinge zu schaffen und den Verwaltungsaufwand der Kommunen zu reduzieren, schloss das Land Brandenburg mit verschiedenen Krankenkassen eine Rahmenvereinbarung zur Übernahme der Krankenbehandlung ab. In diesem Kontext werden an Asylbewerber elektronische Gesundheitskarten ausgegeben.

Die Landkreise und kreisfreien Städte übermitteln hierzu die erforderlichen Daten der Betroffenen an die Krankenkassen in eigener Verantwortung. Mangels einschlägiger bereichsspezifischer Normen im Sozialrecht ist das Brandenburgische Datenschutzgesetz (BbgDSG) anzuwenden. Soweit mit der Erhebung und Übermittlung von Daten der Flüchtlinge an die Krankenkassen ein automatisiertes Verfahren zur Anwendung kommt, müssen die Landkreise und kreisfreien Städte insbesondere die Regelungen dieses

Gesetzes zu Sicherheitskonzept, Verfahrensverzeichnis, Vorabkontrolle und Verfahrensfreigabe beachten.

Neben diesen rechtlichen Erwägungen hatten wir aufgrund einer Anfrage zu klären, ob für die erforderlichen Datenübermittlungen (Anmeldungen, Veränderungsmeldungen, Abmeldungen) die spezielle Software einer Krankenkasse verwendet werden könne. Der dazu erstellte Leitfaden sah vor, dass die personenbezogenen Daten in einer verschlüsselten Datei gespeichert und diese per E-Mail an die Krankenkasse gesendet werden sollte. Das hierbei verwendete symmetrische Verschlüsselungsverfahren war zwar nicht zu kritisieren, allerdings war das Schema zur Bildung des Passwortes im Programm hinterlegt und leicht reproduzierbar. Wir empfahlen, zusätzlich auf asymmetrische Verschlüsselungsverfahren zurückzugreifen, da ein leicht bestimmbares Passwort die Sicherheit der Verschlüsselung deutlich verringert.

Nach dem Leitfaden sollten zudem Bilddateien mit Passbildern der Betroffenen für die Gesundheitskarten in einer komprimierten Datei gespeichert und unverschlüsselt per E-Mail zur Krankenkasse übertragen werden. Wir wiesen darauf hin, dass die elektronische Übermittlung der Daten nur verschlüsselt erfolgen darf. Dieses Erfordernis ergibt sich aus § 10 BbgDSG.

Für die weitere Datenverarbeitung durch die Krankenkassen sind die Landkreise und kreisfreien Städte hingegen nicht verantwortlich. Bei der Übernahme der Krankenbehandlung handelt es sich um eine sog. Aufgabenübertragung; die Regelungen zur Datenverarbeitung im Auftrag finden keine Anwendung.

Bei allen Übermittlungen der Daten von Leistungsberechtigten nach dem Asylbewerberleistungsgesetz an die Krankenkassen ist das Brandenburgische Datenschutzgesetz zu beachten. Für die elektronische Übertragung von Daten muss ein sicheres Verschlüsselungsverfahren genutzt werden.

8.6 Übermittlung von Daten unbegleiteter minderjähriger Ausländer

Dürfen Ausländerbehörden den Familiengerichten und Jugendämtern Angaben zu ausländerrechtlichen Angelegenheiten von unbegleiteten Minderjährigen übermitteln?

Nachdem eine ausländische Minderjährige ohne Begleitung nach Deutschland eingereist war, übermittelte die Ausländerbehörde des zuständigen Landkreises Daten an das Familiengericht und an das Jugendamt. Letzteres hatte die Amtsvormundschaft übernommen. Die Ausländerbehörde informier-

te das Jugendamt im weiteren Verlauf über die Feststellung der Ausreisepflicht, die Ausreiseaufforderung und die Androhung der Abschiebung der Minderjährigen. Daraufhin beschwerte sich eine Rechtsanwältin gegen die Datenübermittlung durch die Ausländerbehörde an das Familiengericht sowie das Jugendamt. Sie selbst verfügte über eine anwaltliche Vollmacht der im Ausland lebenden, sorgeberechtigten Mutter der Minderjährigen. Durch die Datenübermittlung sei ihre anwaltliche Vollmacht missachtet worden.

Die Landesbeauftragte konnte keinen datenschutzrechtlichen Verstoß feststellen und verwies die Rechtsanwältin auf die folgenden Rechtsgrundlagen:

Das Jugendamt nimmt einen ausländischen Minderjährigen, der unbegleitet nach Deutschland kommt, nach § 42 Abs. 1 S. 1 Nr. 3 Achtes Buch Sozialgesetzbuch (SGB VIII) in Obhut, wenn sich weder Personensorge- noch Erziehungsberechtigte im Inland aufhalten. Nach § 42 Abs. 3 S. 2 SGB VIII hat das Jugendamt unverzüglich die Bestellung eines Vormunds zu veranlassen und dazu das Familiengericht anzurufen.

Im Falle der unbegleiteten Minderjährigen hatte das Familiengericht festgestellt, dass die elterliche Sorge (hier: der allein sorgeberechtigten Mutter der Minderjährigen) ruhte, weil die Mutter diese mangels Aufenthalts in Deutschland nicht ausüben konnte. Das Familiengericht bestellte darauf hin gemäß § 14 Abs. 1 Nr. 10 Rechtspflegergesetz eine Mitarbeiterin des zuständigen Jugendamtes zum Amtsvormund.

Die Übermittlung von Informationen über die unbegleitete Minderjährige durch die Ausländerbehörde an das Familiengericht war nach § 22a Abs. 2 Gesetz über das Verfahren in Familiensachen und in den Angelegenheiten der freiwilligen Gerichtsbarkeit zulässig. Nach dieser Vorschrift dürfen Behörden dem Familien- oder Betreuungsgericht personenbezogene Daten übermitteln, wenn deren Kenntnis aus ihrer Sicht für familien- oder betreuungsgerichtliche Maßnahmen erforderlich ist und keine überwiegenden schutzwürdigen Interessen des Betroffenen entgegenstehen. Diese Rechtsgrundlage gilt auch für Ausländerbehörden. Die Ausländerbehörde durfte daher die für die Abwicklung aufenthaltsrechtlicher Angelegenheiten erforderlichen Daten der unbegleiteten Minderjährigen dem Familiengericht übermitteln, damit u. a. die rechtliche Handlungsfähigkeit eintreten konnte.

Auch die Übermittlung der Entscheidungen der Ausländerbehörde über die Feststellung der Ausreisepflicht, die Ausreiseaufforderung und die Androhung der Abschiebung der Minderjährigen an das Jugendamt war für dessen Aufgabenerfüllung als Amtsvormund erforderlich und damit rechtmäßig.

Behörden dürfen dem Familiengericht in der Regel personenbezogene Daten übermitteln, wenn deren Kenntnis aus ihrer Sicht für familiengerichtliche Maßnahmen erforderlich ist. Sofern das Jugendamt als Amtsvormund bestellt wird, werden ihm Bescheide als Vertreter der Minderjährigen bekannt gegeben.

8.7 Digitale Einsatzplanung der Freiwilligen Feuerwehr

Im Bereich des Brand- und Katastrophenschutzes sind die Freiwilligen Feuerwehren unverzichtbar. Um die Einsatzplanung und auch die fachliche Aus- und Weiterbildung der Kameraden zu erleichtern, setzen die Freiwilligen Feuerwehren zunehmend auf den Einsatz von webbasierten Diensten, die durch Drittanbieter zur Verfügung gestellt werden.

Die Freiwilligen Feuerwehren sind organisatorisch den Städten und Gemeinden angegliedert. Sie unterliegen somit als Teil der öffentlichen Stelle den Bestimmungen des Brandenburgischen Datenschutzgesetzes (BbgDSG). Im Falle der Nutzung externer Softwareprodukte oder Rechenzentrumsdienste geben sie personenbezogene Daten ihrer Mitglieder im Rahmen einer Datenverarbeitung im Auftrag gemäß § 11 BbgDSG an ihre Dienstleister weiter. Diese müssen ihrerseits vertraglich zusichern, die Vorschriften des Gesetzes einzuhalten. Hinzu kommt, dass bei dem Outsourcing unter Umständen auch Gesundheitsdaten mit hohem Schutzbedarf verarbeitet werden, und somit besondere Anforderungen an die umzusetzenden technisch-organisatorischen Maßnahmen aufseiten des Diensteanbieters zu stellen sind.

Bei der Vorbereitung einer solchen Datenverarbeitung im Auftrag stellte sich heraus, dass die erforderlichen vertraglichen Voraussetzungen nicht erfüllt wurden. Zwar hatten Drittanbieter, die dem Bundesdatenschutzgesetz unterliegen, die entsprechenden Vertragsentwürfe und Datenschutzvorgaben nach dem Bundesdatenschutzgesetz umgesetzt. Da die Freiwilligen Feuerwehren jeweils nur die kostenfreie Basisversion des angebotenen Produktes zu nutzen beabsichtigten, hatten die Dienstleister nur ein geringes Interesse an der Anpassung der vertraglichen Bedingungen an das Brandenburgische Datenschutzgesetz sowie an der Umsetzung der erforderlichen, ggf. zusätzlichen technisch-organisatorischen Maßnahmen.

Aufgrund der nicht erfüllten Voraussetzungen für eine Auftragsdatenverarbeitung gemäß § 11 BbgDSG war die Verarbeitung der personenbezogenen Daten der Mitglieder der Freiwilligen Feuerwehr durch Dritte datenschutzrechtlich nicht zulässig. Die Nutzung der entsprechenden Webdienste kam deshalb in mehreren Fällen bisher nicht zustande.

Als verantwortliche Daten verarbeitende Stelle bleibt die Gemeinde für die Verarbeitung der personenbezogenen Daten der Mitglieder der Freiwilligen Feuerwehr verantwortlich. Solange keine vertraglichen Regelungen nach dem Brandenburgischen Datenschutzgesetz vorliegen, ist eine Datenverarbeitung durch Dritte datenschutzrechtlich unzulässig.

9 Jugend

9.1 Darf eine Kita vor Aufnahme eines Kindes eine detaillierte ärztliche Tauglichkeitsbescheinigung anfordern?

Einer aufmerksamen Kinderärztin ist es zu verdanken, dass wir von vier Fällen erfuhren, in denen ihr Eltern die von verschiedenen Kitas ausgegebenen Formularvordrucke für die erstmalige Aufnahme in deren Einrichtung vorgelegt hatten. Darin sollten beispielsweise einzelne Krankheiten (wie z. B. Hepatitis B) und konkret durchgeführte Schutzimpfungen angegeben werden.

Nach § 11 Abs. 2 Kindertagesstättengesetz Brandenburg (KitaG) ist vor Aufnahme in eine Kita zwar eine ärztliche Untersuchung erforderlich. Diese soll aber im Ergebnis nur eine grundsätzliche Kitatauglichkeit ohne nähere Angaben zu konkreten Krankheiten attestieren. Inwieweit darüber hinaus detaillierte gesundheitliche Angaben für die Betreuung des Kindes in der Einrichtung wichtig sind, ist zwischen den Eltern und der Kita zu klären.

Auf Nachfrage zeigten die jeweiligen Kitas für die teilweise Unzulässigkeit der Datenerhebungen in der Regel nur geringes Verständnis. In einem Fall sei versehentlich das falsche, veraltete Formular ausgedruckt worden.

Die vier Vorfälle nahmen wir zum Anlass, das Ministerium für Bildung, Jugend und Sport zu informieren. Es weist nunmehr in seinem Internetangebot sowie in entsprechenden Fach- und Multiplikatorenrunden explizit auf sein veröffentlichtes Musterformular „Ärztliche Bescheinigung für die Aufnahme in Kindertagesstätten nach § 11 Abs. 2 Kindertagesstättengesetz Brandenburg“ hin.[54]

Den Kitas, die unzulässig Daten erhoben hatten, haben wir dringend empfohlen, das Musterformular des Ministeriums zu verwenden.

[54] https://mbjs.brandenburg.de.

Als Nachweis der generellen Kitatauglichkeit ist lediglich die ärztliche Bestätigung, dass keine Bedenken gegen die Aufnahme eines bestimmten Kindes in eine Kita bestehen, zulässig. Im Rahmen des individuellen Betreuungsvertrages zwischen den Eltern und der Kita kann nach vorhandenen Impfungen oder gesundheitlichen Beeinträchtigungen, wie z. B. lebensbedrohlichen Allergien, gefragt werden.

9.2 Darf die Gemeinde für die Anmeldung zur Hortbetreuung einen Nachweis des Sorgerechtsstatus verlangen?

Eine Mutter sollte der Gemeinde für die Anmeldung ihres Kindes zur Hortbetreuung den Gerichtsbeschluss zum Sorgerecht einreichen. Die Petentin hielt dies für nicht erforderlich, da die Entscheidung für die Hortbetreuung der sog. Alltagssorge unterfalle, die auch bei gemeinsamem Sorgerecht von ihr alleine getroffen werden könne.

Das Sorgerecht ist im Bürgerlichen Gesetzbuch (BGB) geregelt. Berührt war in diesem Fall die Ausübung der gemeinsamen elterlichen Sorge bei getrennt lebenden Eltern nach § 1687 BGB. Diese Vorschrift unterscheidet zwischen Angelegenheiten, deren Regelung für das Kind von erheblicher Bedeutung und für die ein gegenseitiges Einvernehmen beider Sorgeberechtigter erforderlich ist. Dem gegenüber hat für Angelegenheiten des täglichen Lebens jener Elternteil, bei dem sich das Kind mit Einwilligung des anderen Elternteils oder aufgrund einer gerichtlichen Entscheidung gewöhnlich aufhält, die Befugnis zur alleinigen Entscheidung. Entscheidungen in Angelegenheiten des täglichen Lebens sind in der Regel solche, die häufig vorkommen und die keine schwer abzuändernden Auswirkungen auf die Entwicklung des Kindes haben.

Unabhängig von der zivilrechtlichen Frage, ob die Anmeldung des Kindes zum Hort der Alltagssorge unterfällt oder nicht, sprechen verschiedene Gründe für das Recht der Gemeinde, den Nachweis der Sorgeberechtigung zu erheben. So müssen die Gemeinde und die Betreuer stets wissen, wer als Ansprechpartner für Angelegenheiten des Kindes infrage kommt. Dies betrifft beispielsweise die Berechtigung zur Anmeldung des Kindes, die Zahlungsverpflichtung für Elternbeiträge, den Besuch von Elternabenden, die Teilnahme an Ausflügen oder auch medizinische Notfälle.

Ein Nachweis des Sorgerechtsstatus kann schon bei der Anmeldung oder beim Abschluss des Betreuungsvertrages, aber auch bei eingetretenen Änderungen zulässig sein. In Einzelfällen ist auch eine spätere Erhebung möglich, wenn die Angaben nicht vollständig vorliegen oder Widersprüche auftreten.

9.3 Bescheid über Kita-Gebühren an getrennt lebende Eltern

Eine Mutter beklagte sich, dass eine Gemeinde den Bescheid über die Elternbeiträge für die Kita-Betreuung ihres Kindes nicht nur ihr, sondern auch dem anderen, von ihr getrennt lebenden Elternteil übermittelt hatte. Sie befürchtete, diesem würden dadurch Rückschlüsse auf ihr Einkommen und ihre Arbeitszeit ermöglicht, die ihn nichts angingen, zumal sie die Zahlung stets vollständig alleine vornimmt.

Solche und ähnliche Anfragen sowie Beschwerden erreichen uns immer wieder. Teilweise gehen die Gemeinden als Träger der Kindertageseinrichtung davon aus, dass die Personensorgeberechtigten nach § 17 Kindertagesstättengesetz (KitaG) als Gesamtschuldner für Kita-Beiträge haften, sodass der Bescheid beiden Elternteilen bekannt zu geben sei.

Diese Auffassung teilen wir nicht. Vielmehr vertreten wir die Ansicht, dass § 17 Abs. 1 KitaG durch die Formulierung „die Personensorgeberechtigten“ nicht zwingend ein Gesamtschuldverhältnis unterstellt. Diese Regelung umschreibt lediglich den Kreis der als Beitragspflichtige in Betracht kommenden Personen. Näheres regelt die jeweilige kommunale Satzung. Die Möglichkeit, dass nur eine Person zur Zahlung herangezogen wird, ist nicht ausgeschlossen.

Wenn – wie im vorliegenden Fall – die Zahlung stets durch die Mutter allein erfolgt, gibt es in der Regel keinen Grund, dem getrennt lebenden Elternteil, der an der Zahlung ohnehin nicht beteiligt ist, die Beitragshöhe mitzuteilen. Dem Vater würde dadurch vielmehr in unzulässiger Weise die Möglichkeit eröffnet, Rückschlüsse auf das Einkommen und die Arbeitszeit der Mutter zu ziehen.

Die Rechtsauffassung hatten wir bereits im Zusammenhang mit früheren Fällen mit dem Ministerium für Bildung, Jugend und Sport abgestimmt.

Leben Eltern getrennt oder sind geschieden und entrichtet ein Elternteil den kompletten Kita-Beitrag, ist der entsprechende Bescheid lediglich an diesen zu richten.

10 Justiz und Rechtspflege

Darf das Versorgungswerk der Rechtsanwälte von seinen Mitgliedern den Einkommensteuerbescheid verlangen?

Das Versorgungswerk der Rechtsanwälte in Brandenburg hat die Aufgabe, seinen Mitgliedern – den in Brandenburg ansässigen Rechtsanwälten – eine beitragsfinanzierte Versorgung im Alter und bei Berufsunfähigkeit zu leisten. Dazu erhebt es Beiträge, deren Höhe sich nach dem Einkommen des jeweiligen Rechtsanwalts richtet. Ein selbstständig tätiger Rechtsanwalt wehrte sich dagegen, dass er dem Versorgungswerk zum Nachweis seines Einkommens eine Kopie seines Einkommensteuerbescheids ohne Schwärzungen übersenden sollte.

Dem Rechtsanwalt leuchtete es nicht ein, dass das Versorgungswerk die von ihm übersandte unvollständige Kopie seines Einkommensteuerbescheids nicht akzeptierte. Für sein Recht, den Bescheid nur teilweise zu kopieren und im kopierten Teil Schwärzungen vorzunehmen, spreche, dass sich aus dem Bescheid nicht nur sein Arbeitseinkommen aus der selbstständigen Tätigkeit als Rechtsanwalt ergebe, sondern auch die Einkünfte aus seiner sonstigen Tätigkeit und zudem – wegen der Zusammenveranlagung – die Einkünfte seiner Ehefrau. Für die Beitragsbemessung ist aber allein das Einkommen aus seiner Rechtsanwaltstätigkeit maßgeblich.

Die Satzung, die sich das Versorgungswerk aufgrund gesetzlicher Ermächtigung gegeben hat, sieht die Vorlage des Einkommensteuerbescheids vor. Derartige Satzungen öffentlich-rechtlicher Körperschaften sind als gesetzliche Grundlage für die Datenverarbeitung geeignet, sodass die Erhebung der Daten durch die Vorlage des Einkommensteuerbescheids bzw. die Übersendung einer Kopie auf die spezielle Vorschrift in der Satzung gestützt werden kann. Die Regelung lässt sich damit rechtfertigen, dass allein das Versorgungswerk abschließend beurteilen kann, welche Informationen es für die Beitragsbemessung benötigt. Auch muss es beispielsweise prüfen können, inwieweit der jeweilige Bescheid ggf. nur vorläufig ist.

Allerdings fehlt es in der Satzung an einer Regelung, die die Speicherung von Daten erlaubt. Die Zulässigkeit der Speicherung der Daten aus dem Einkommensteuerbescheid ist daher auf der Grundlage des Brandenburgischen Datenschutzgesetzes zu beurteilen. Eine Speicherung ist danach nur zulässig, wenn dies zur rechtmäßigen Erfüllung der Aufgaben des Versorgungswerks erforderlich ist. Das Versorgungswerk ist folglich nur befugt, solche Daten aus einem vorgelegten Einkommensteuerbescheid zu speichern, die es für die Ermittlung der Beitragspflicht tatsächlich benötigt. Rein praktisch

bedeutet das, dass der Einkommensteuerbescheid zwar in vollem Umfang vorzulegen ist, das Versorgungswerk jedoch nur die Informationen daraus für sich festhalten darf, die es für die Ermittlung der Beitragshöhe benötigt, und den Bescheid im Übrigen zurückgeben muss.

Kommt das Versorgungswerk dem Rechtsanwalt entgegen und räumt ihm die Möglichkeit ein, statt der Vorlage des Originals eine Kopie zu übersenden, so darf es auch in diesem Fall nur die für die Ermittlung der Beitragspflicht erforderlichen Daten speichern und muss die Kopie im Übrigen vernichten oder alternativ zurücksenden.

Auch wenn es auf den ersten Blick nicht einleuchten mag, wozu das Versorgungswerk den gesamten Einkommensteuerbescheid benötigt, besteht gleichwohl eine durch die Aufgabe des Versorgungswerks gerechtfertigte gesetzliche Pflicht zur Vorlage. Dagegen ist die Speicherung von Daten aus dem Einkommensteuerbescheid auf das unbedingt notwendige Maß zu beschränken.

11 Kommunales

11.1 Fertigung von Protokollen aus Tonaufzeichnungen einer Sitzung der Stadtverordnetenversammlung zur Beweisgewinnung

Tonaufzeichnungen der menschlichen Stimme stellen gewichtige Eingriffe in das Recht auf Datenschutz dar. Anfertigung und Nutzung ist öffentlichen Stellen gesetzlich nur zu bestimmten Zwecken erlaubt. Die Landesbeauftragte musste 2016 eine Beanstandung aussprechen, weil eine kreisfreie Stadt eine solche Tonaufzeichnung entgegen der gesetzlichen Zweckbindung weiterverarbeitet hatte.

Bereits im Jahre 2015 erreichte uns die Beschwerde eines Stadtverordneten einer kreisfreien Stadt. Ihm war vorgeworfen worden, im Rahmen einer persönlichen Erklärung in einer nicht öffentlichen Sitzung der Stadtverordnetenversammlung Interna einer stadteigenen Gesellschaft, deren Aufsichtsratsmitglied er war, verraten zu haben. Eine von der Sitzungsleitung gefertigte Tonaufnahme wurde daraufhin genutzt, um neben der Niederschrift der Sitzung ein separates Protokoll der Erklärung des Betroffenen im Wortlaut anzufertigen und der strafantragsberechtigten Gesellschaft zuzuleiten. Der Betroffene hielt das Vorgehen der Stadt für datenschutzrechtlich unzulässig, wobei er angab, ihm sei nicht bewusst gewesen, dass nicht öffentliche Sitzungen überhaupt mitgeschnitten würden.

§ 42 Abs. 1 S. 1 Brandenburgische Kommunalverfassung (BbgKVerf), hier in Verbindung mit § 27 Abs. 1 S. 2, schreibt vor, dass über jede Sitzung der Gemeindevertretung eine Niederschrift zu fertigen ist. § 42 Abs. 2 S. 3 BbgKVerf erlaubt die Tonaufzeichnung der Sitzung zur Erleichterung der Niederschrift. Die Stadt hat im Laufe der Korrespondenz bezweifelt, dass es sich um eine datenschutzrechtliche Vorschrift handele, da die Mitglieder der Stadtverordnetenversammlung ihre Wortbeiträge nicht als Privatleute abgeben würden, sondern im Rahmen der Erfüllung öffentlich-rechtlicher Pflichten. Die Landesbeauftragte stellte hingegen fest, dass der Anwendungsbereich des Datenschutzrechts eröffnet ist. Zunächst sind öffentliche Stellen bei der Erhebung von personenbezogenen Daten gleich welcher Art an datenschutzrechtliche Vorschriften gebunden (§ 2 Abs. 1 S. 1 i. V. mit §§ 12 ff. Brandenburgisches Datenschutzgesetz – BbgDSG). Sowohl Gesetzesbegründung als auch Schrifttum machen zudem deutlich, dass die Beschränkung der Aufzeichnungsbefugnis ausdrücklich den Eingriff in datenschutzrechtliche Rechtspositionen begrenzen sollte. Dies gilt insbesondere, wenn – wie im vorliegenden Fall – ein ersichtlich freier, unangemeldeter Wortbeitrag in Rede steht.

Es handelt sich bei § 42 Abs. 2 S. 3 BbgKVerf um eine sog. Zweckbindungsvorschrift: Die Tonaufzeichnung ist zwar zulässig, aber nur, wenn sie ausschließlich dazu dient, die Niederschrift gemäß Abs. 1 S. 1 der Vorschrift anzufertigen. Bei Beginn der Aufzeichnung war dieser Zweck unzweifelhaft gegeben. Auch differenziert die Vorschrift nicht zwischen Aufzeichnungen in öffentlicher und nicht öffentlicher Sitzung, sodass eine durchgängige Aufzeichnung rechtmäßig ist, ohne dass die Betroffenen auf das Weiterlaufen des Bandes im nicht öffentlichen Teil gesondert aufmerksam gemacht werden müssten.

Allerdings bedeutet die Zweckbindung in § 42 Abs. 2 S. 3 BbgKVerf auch, dass eine spätere Nutzung der rechtmäßig hergestellten Aufzeichnung grundsätzlich ausschließlich den dort festgelegten Zweck verfolgen darf, nämlich die Anfertigung der offiziellen Niederschrift (§ 42 Abs. 3 BbgKVerf). Hiergegen verstieß die Stadt in Kenntnis der abweichenden Rechtslage, indem sie ein separates Wortprotokoll zum Zweck der Weitergabe fertigte, das zu keinem Zeitpunkt Teil der Niederschrift gemäß § 42 Abs. 1 BbgKVerf war und von der Stadtverordnetenversammlung auch nicht als solcher genehmigt werden sollte.

Die Nutzung der Tonaufzeichnung entgegen der erkennbaren gesetzlichen Zweckbindung und ohne nähere Zulässigkeitsprüfung stellte sich für die Landesbeauftragte als erheblicher Rechtsverstoß dar, den sie gemäß § 25 Abs. 1 S. 1 Nr. 2 und S. 2 BbgDSG bei der kreisfreien Stadt und dem für die Kommunalaufsicht zuständigen Ministerium beanstandete.

Die nachfolgende Weitergabe der Daten war nicht Gegenstand der Beanstandung. Da die übermittelten Daten jedoch unter Verstoß gegen Datenschutzrecht zustande gekommen waren und daher grundsätzlich einer Löschpflicht unterlagen, konnten sie nicht ohne Weiteres weitergegeben werden. Die datenschutzrechtliche Problematik stellte sich hier als weniger schwerwiegend dar, weil die eigentliche Information auch auf rechtmäßigem Weg an die strafantragsberechtigte Stelle hätte gelangen können.

Die Tonaufzeichnung ist öffentlichen Stellen nur in wenigen Fällen und zu bestimmten festgelegten Zwecken erlaubt. Legt das Gesetz einen solchen fest, darf von diesem grundsätzlich nicht abgewichen werden. Die Nutzung von Tonaufzeichnungen zu anderen Zwecken kann auch dann einen Datenschutzverstoß darstellen, wenn die Wortbeiträge im Rahmen der Ausübung eines öffentlichen Amtes aufgezeichnet werden.

11.2 Transparenz beim Verkauf des gemeindlichen „Tafelsilbers“

Transparenz ist als Zielrichtung des Verwaltungshandelns in aller Munde. Dies gilt erst recht für fiskalisches Handeln öffentlicher Stellen. Doch wie weit geht die Offenheit, wenn personenbezogene Daten Dritter betroffen sind?

Immer wieder erreichen uns Anfragen von Gemeinden, inwieweit sie Daten zu Grundstückskaufverträgen, bei denen die Gemeinde als Verkäuferin auftritt, veröffentlichen dürfen. Ausgangspunkt ist der Umstand, dass beim Verkauf von Immobilien durch Gemeinden regelmäßig die Gemeindevertretung entscheiden muss (vgl. § 28 Abs. 2 Nr. 17 Brandenburgische Kommunalverfassung – BbgKVerf). Der Wunsch der Gemeinde nach Transparenz kollidiert in diesen Fällen oft mit dem Wunsch des betroffenen Käufers, nicht in der Öffentlichkeit aufzutreten. Insbesondere geht es in vielen Fällen darum,

- ob solche Verträge im öffentlichen Teil der Sitzung verhandelt werden können und

- ob Beschlüsse über Grundstückskaufverträge einschließlich Namen und Kaufpreis veröffentlicht werden dürfen.

Gemäß § 36 Abs. 2 BbgKVerf sind die Sitzungen der Gemeindevertretung grundsätzlich öffentlich. Die Öffentlichkeit ist allerdings auszuschließen, wenn berechtigte Interessen Einzelner es erfordern. Wann letzteres der Fall ist, kann nur im Einzelfall entschieden werden. Problematisch ist, dass ein unberechtigter Ausschluss der Öffentlichkeit die Unwirksamkeit der gefassten

Beschlüsse nach sich ziehen kann. Die Landesbeauftragte empfiehlt das folgende Vorgehen:

Zunächst ist es ratsam, im Vorfeld Kontakt mit dem Betroffenen aufzunehmen, um zu klären, ob dieser überhaupt Vorbehalte gegen die Verhandlung in öffentlicher Sitzung hegt. Ist dies nicht der Fall, ist auch ein entgegenstehendes Interesse gemäß § 36 Abs. 2 BbgKVerf nicht feststellbar. Äußert der Betroffene Bedenken, können diese zur Grundlage der erforderlichen Einschätzung der Schutzbedürftigkeit im Einzelfall gemacht werden.

Wir schließen uns zudem der Auffassung des Landesbeauftragten für Datenschutz und Informationsfreiheit Mecklenburg-Vorpommern an, der in seiner insoweit nach wie vor aktuellen Orientierungshilfe „Datenschutz in kommunalen Vertretungen“[55] ausführt, dass bei Grundstücksangelegenheiten, etwa bei Grundstückskäufen und -verkäufen, solche Angaben nicht offen zu legen sind, die Aufschluss über die Vermögensverhältnisse und Geschäftsabsichten der Beteiligten geben. Diese Gegenstände gehören in der Regel in den nicht öffentlichen Teil der Sitzung. Gleiches gilt für Beschlüsse über die etwaige Ausübung eines gemeindlichen Vorkaufsrechts, in denen oftmals Kalkulationsgrundlagen offengelegt werden müssen, deren Interesse für die Öffentlichkeit in keinem Verhältnis zu dem damit verbundenen Eingriff in das Recht auf Datenschutz des Betroffenen steht.

Es muss jedoch darauf hingewiesen werden, dass es sich hierbei nicht um feste Vorgaben handelt. Besondere Umstände des Einzelfalls können das Interesse des Betroffenen verstärken oder – zum Beispiel wenn das Grundstücksgeschäft durch eigenes Handeln des Käufers bereits zuvor Gegenstand der öffentlichen Diskussion gewesen ist oder die Transaktion einen besonders großen Umfang annimmt – im Einzelfall auch wieder zurücktreten lassen. Auf die Einzelfallbetrachtung kann daher nicht verzichtet werden.

§ 39 Abs. 3 BbgKVerf bestimmt, dass die Beschlüsse der Gemeindevertretung oder deren wesentlicher Inhalt in ortsüblicher Weise der Öffentlichkeit zugänglich zu machen sind, soweit nicht im Einzelfall u. a. zur Wahrung von Rechten Dritter etwas anderes beschlossen wird. Die Veröffentlichung im Volltext ist der Regelfall. Zwischen in öffentlicher und in nicht öffentlicher Sitzung gefassten Beschlüssen unterscheidet die Vorschrift nicht; Geheimbeschlüsse darf es nicht geben.

Personenbezogene Daten dürfen die Veröffentlichungen, die eine Form der Datenübermittlung (§ 3 Abs. 2 Nr. 4 Brandenburgisches Datenschutzgesetz) darstellen, nur enthalten, soweit dies zur Erreichung des Zwecks der Veröf-

[55] Landesbeauftragter für Datenschutz und Informationsfreiheit Mecklenburg-Vorpommern, Orientierungshilfe „Datenschutz in kommunalen Vertretungsorganen“, S. 6 - 7, Stand Januar 2003, siehe http://datenschutz-mv.de.

fentlichung erforderlich ist. Sie müssen daher aus Beschlüssen ausgesondert werden, solange ihr wesentlicher Inhalt erhalten bleibt. Dies gilt insbesondere für in nicht öffentlicher Sitzung gefasste Beschlüsse. Denn es wäre nicht erklärbar, dass personenbezogene Daten erst vor der Öffentlichkeit durch Verhandlung in geschlossener Sitzung geschützt werden, dann aber durch eine – insbesondere bei Veröffentlichung im Internet – viel einschneidendere Veröffentlichung des Beschlusses doch wieder in die Öffentlichkeit gelangen.

Die Landesbeauftragte sieht den wesentlichen Inhalt des Beschlusses bei Grundstücksgeschäften darin, dass der Leser erkennen können muss, zu welchen Konditionen die Gemeinde ihre eigenen Grundstücke veräußert hat. Zu löschen sind daher alle personenbezogenen Daten, die zur Klärung dieser Frage nichts beitragen. Hierfür bedarf es weder des Namens noch weiterer Daten des Käufers, es sei denn, er hat bei entsprechender Gelegenheit keine Bedenken gegen eine Veröffentlichung erhoben. Ein weiteres irrelevantes Datum kann die genaue Adresse des Grundstücks darstellen, wenn etwa die Angabe der Straße für die Einschätzung der wirtschaftlichen Tragweite des Grundstücksgeschäfts genügt.

Zwar mag der Kaufpreis eine für die Einschätzung der wirtschaftlichen Tragweite eines Beschlusses wichtige Information sein, dennoch sollte, wenn der Beschluss in nicht öffentlicher Sitzung getroffen wurde, auch erwogen werden, diesen entweder nur grob oder pauschalierend anzugeben oder einen Beschluss nach § 39 Abs. 3 letzter Halbsatz BbgKVerf zu treffen und die Veröffentlichung insoweit zu beschränken. Zu einem solchen Beschluss ist die Gemeindevertretung verpflichtet, wenn die überwiegenden Interessen des Betroffenen eine solche Maßnahme erforderlich machen.

Insgesamt kann das datenschutzgerechte Vorgehen bei aller Bildung von Fallgruppen und Faustregeln nur im Einzelfall bestimmt werden. Neben einer Abstimmung mit dem Betroffenen über die Öffentlichkeit der Sitzung und die Veröffentlichung des Beschlusses steht auch die Landesbeauftragte Kommunen wie Betroffenen gerne zur Lösung einschlägiger Fragen zur Verfügung.

Transparenz beim Verkauf des gemeindlichen „Tafelsilbers“ ist ein hohes Gut – aber auch sie muss in den Rechten des Käufers ihre Grenze finden. Bei der Frage der öffentlichen Verhandlung muss das Öffentlichkeitsprinzip beachtet werden – aber auch die Möglichkeit für den Betroffenen bestehen, seine finanziellen Verhältnisse lediglich in einem angemessen begrenzten Umfeld offenzulegen. Bei der Veröffentlichung von Beschlüssen dürfen regelmäßig nur so viele personenbezogene Daten des Käufers erkennbar sein, dass der Leser die wirtschaftliche Tragweite der Transaktion ermessen kann. Je nach den Umständen kann jedoch auch der Kaufpreis als Ausdruck der finanziellen Verhältnisse eines bestimmbaren Betroffenen zu vergröbern oder gänzlich von der Veröffentlichung auszunehmen sein.

11.3 Veröffentlichung personenbezogener Daten in Beschlussvorlagen

Die Landesbeauftragte beschäftigte sich im Berichtszeitraum mit der Frage, ob und inwieweit personenbezogene Daten in Beschlussvorlagen bzw. Sitzungsunterlagen für die Stadtverordnetenversammlung zur Verfügung zu stellen sind.

Eine kreisangehörige Stadt bat uns um Einschätzung der dort üblichen Praxis zur Veröffentlichung von Beschlussvorlagen. Diese wurden Interessierten genauso wie den Stadtverordneten über das Ratsinformationssystem zur Verfügung gestellt. Wegen der Einsehbarkeit für jedermann wurden die personenbezogenen Daten – etwa von Einwendern in baurechtlichen Verfahren – geschwärzt, was auf Unmut der Stadtverordneten stieß. Sie wollten sich nicht mit dem Hinweis zufriedengeben, die ungeschwärzten Dokumente seien in der Stadtverwaltung einsehbar, zumal die Geschäftsordnung eine elektronische Bereitstellung der Sitzungsunterlagen vorsah.

§ 36 Abs. 4 Brandenburgische Kommunalverfassung (BbgKVerf) bestimmt, dass jeder das Recht hat, Beschlussvorlagen zu den in öffentlicher Sitzung zu behandelnden Tagesordnungspunkten einzusehen. Schon bei der Erstellung der Beschlussvorlagen ist folglich auf Datensparsamkeit zu achten und das Dokument frei von für das Verständnis nicht erforderlichen personenbezogenen Daten Dritter zu halten. Dabei ist ein strenger Maßstab anzulegen. Personenbezogene Daten dürfen nur dann Teil der Beschlussvorlage werden, wenn ohne sie die Gesamtaussage des Dokuments schlechterdings nicht nachvollziehbar wäre. Vielmehr muss es ausreichen, das Beschlussthema selbst nebst Hinweisen zum Verständnis aufzunehmen, personenbezogene Daten jedoch nach Möglichkeit in nicht öffentlich zugängliche Anlagen auszugliedern. Über ein Ratsinformationssystem können Beschlussvorlagen der Öffentlichkeit nur zur Verfügung gestellt werden, soweit sie überhaupt keine personenbezogenen Daten enthalten, da es sich insoweit um einen Abruf und nicht um eine bloße Einsicht handelt.

Vom Vorstehenden vollkommen zu trennen ist die Bereitstellung der Sitzungsunterlagen für die Stadtverordneten. Ihnen können die Beschlussvorlagen einschließlich der Anlagen über ein Ratsinformationssystem – den erforderlichen Passwortschutz vorausgesetzt – in der Regel vollständig zum Abruf bereitgestellt werden. Auch hier kann allerdings eine vorläufige Schwärzung von für die Arbeit der Stadtverordneten nicht erforderlichen personenbezogenen Daten notwendig sein. Die Aufdeckung der auf diese Weise geschützten Identitäten kann bei Vorliegen der gesetzlichen Voraussetzungen unter Umständen durch den Akteneinsichtsanspruch nach § 29 BbgKVerf individuell erfolgen.

Personenbezogene Daten sollten nach Möglichkeit bereits bei Erstellung aus den Beschlussvorlagen ausgesondert werden – insbesondere durch die Verlagerung in nicht öffentlich zugängliche Anlagen, solange die Beschlussvorlagen schlüssig bleiben. Diese können der Öffentlichkeit über ein Ratsinformationssystem nur zur Verfügung gestellt werden, soweit sie überhaupt keine personenbezogenen Daten enthalten.

11.4 Überprüfung der Abstimmung über Bürgerhaushalte mittels Meldedaten

Ein in den letzten Jahren immer beliebteres Mittel zur Einbindung von Bürgern in die Gestaltung der Zukunft ihrer Gemeinde ist der sogenannte Bürgerhaushalt. Hierbei können sie darüber abstimmen, welches aus einer Reihe von Kandidatenprojekten mit einem fixen, dem Haushalt entnommenen Geldbetrag finanziert werden soll. Bei Vorbereitung und Durchführung der Abstimmung entstehen oft Fragen, die zu beantworten die Landesbeauftragte im Berichtszeitraum mehrfach Gelegenheit hatte.

Der Bürgerhaushalt wird von der Literatur einhellig als neue Form kommunaler Öffentlichkeitsarbeit klassifiziert. Dementsprechend bildet § 13 S. 2 Brandenburgische Kommunalverfassung (BbgKVerf) die Rechtsgrundlage dafür, den Bürgerhaushalt in der Hauptsatzung als Mittel der Einwohnerbeteiligung festzuschreiben. Kernproblem ist – wie bei allen Abstimmungen – die Anforderung, Abstimmungen durch Unberechtigte und Doppelabstimmungen zu verhindern. Die Satzung legt fest, wer abstimmungsberechtigt ist. Dies sind üblicherweise die am Ort gemeldeten Einwohner, die ein bestimmtes Lebensalter überschritten haben müssen.

Gemäß §§ 12, 13 Brandenburgisches Datenschutzgesetz (BbgDSG) sind Erhebung und Verarbeitung personenbezogener Daten grundsätzlich dann zulässig, wenn sie erforderlich, d. h. unumgänglich sind, um eine der Daten verarbeitenden Stelle obliegende Aufgabe zu erfüllen. Ginge es nur darum, die Abstimmung durch Unberechtigte zu verhindern, wäre es ausreichend und mithin auch zulässig, die Abstimmungsberechtigung der Betroffenen anlässlich der Stimmabgabe zu überprüfen. Der Landesbeauftragten ist jedoch bewusst, dass es im Sinne eines fairen Wettbewerbs auch erforderlich ist, eine Doppelabstimmung mit geeigneten Maßnahmen zu unterbinden.

Die Kommunen waren in vielen Fällen schnell auf die Idee gekommen, Abstimmungslisten aus dem Melderegister zu erstellen, indem sie schlicht die Namen und Geburtsdaten aller nach der Satzung abstimmungsberechtigten Einwohner erhoben. Bei der Abstimmung würde ein Identifikationspapier des jeweiligen Abstimmenden eingesehen und der Name aus der Liste gestrichen.

Gegen dieses Verfahren hatte die Landesbeauftragte keine Einwände. Da die Festlegung der Kriterien der Abstimmungsberechtigung eine von § 13 S. 3 BbgKVerf gedeckte Aufgabe ist, muss dies auch für die Überprüfung anlässlich der Abstimmung gelten. Da die Erhebung der Meldedaten aller Abstimmungsberechtigten die breiteste denkbare Datenverarbeitungsmaßnahme darstellt, war zunächst zu prüfen, ob eine gleich geeignete, aber weniger einschneidende Maßnahme zur Verfügung steht. Dies war jedoch nicht der Fall. Die Erhebung der Meldedaten durch die Organisatoren schien auch in Bezug auf diejenigen Bürger, die sich nicht an der Abstimmung beteiligen, nicht unangemessen, zumal ihnen dadurch die Möglichkeit abzustimmen eröffnet wird und im Übrigen die Daten strikt zweckgebunden eingesetzt und nach Abschluss der Abstimmung und ggf. erneuter Prüfung der Listen auf Schlüssigkeit gelöscht würden. Eine weitere Nutzung der Daten findet nicht statt.

Auch aus melderechtlicher Sicht war die Weitergabe von Namen und Geburtsdaten innerhalb einer Kommune gemäß § 37 Abs. 1 i. V. mit § 34 Abs. 1 S. 1 Nr. 1, 3 und 8 Bundesmeldegesetz zulässig.

Daher ist die zweckgebundene Erhebung und Nutzung dieser Daten als Voraussetzung für die Stimmabgabe erforderlich zur Erfüllung einer öffentlichen Aufgabe i. S. von § 12 Abs. 1 und § 13 Abs. 1 S. 1 BbgDSG und somit zulässig.

Eine kreisangehörige Stadt erklärte uns gegenüber ihre Absicht, Private mit der Durchführung des Bürgerhaushalts zu beauftragen. Die Inhalte und Umstände des dafür gemäß § 11 BbgDSG erforderlichen Auftragsdatenverarbeitungsvertrags waren zu klären. Der Vertrag konnte daraufhin rechtzeitig geschlossen werden. Schließlich sind bei der Behandlung der Listen erforderliche technisch-organisatorische Maßnahmen gemäß § 10 BbgDSG zur Sicherstellung des Datenschutzes einzuhalten.

Der Gesetzgeber erkennt den Bürgerhaushalt als neue Form der Einwohnerbeteiligung an. Die zu seiner Durchführung erforderlichen Daten dürfen unter Einhaltung der Grundsätze der Erforderlichkeit und Zweckbindung verarbeitet werden.

11.5 Kommunale Zusammenarbeit bei der Zulassung von Kraftfahrzeugen per Internet

Seit dem 1. Oktober 2017 haben die Kraftfahrzeug-Zulassungsbehörden die Möglichkeit der internetbasierten Abmeldung und Wiederzulassung von Kraftfahrzeugen auf denselben Halter umzusetzen[56]. Die Landkreise und kreisfreien Städte bieten diese bürgernahe Online-Dienstleistung an. Um die Identifikation des Bürgers zu ermöglichen, setzt das Verfahren die Nutzung des elektronischen Identitätsnachweises (eID-Funktion) des elektronischen Personalausweises voraus.

Um den örtlichen Zulassungsstellen in den Landkreisen und kreisfreien Städten die Umsetzung des Verfahrens zu erleichtern, hat der Zentrale IT-Dienstleister des Landes Brandenburg (ZIT-BB) mit Unterstützung des Ministeriums des Innern und für Kommunales die Entwicklung einer mandantenbasierten Online-Plattform in Erwägung gezogen. Diese ermöglicht eine nach verantwortlichen Stellen getrennte Datenverarbeitung in einer gemeinsamen, einheitlichen Systemumgebung. Gleichzeitig können der Aufwand der Entwicklung und die Implementierungskosten für die einzelnen Behörden gesenkt werden. Der ZIT-BB betreibt hierbei das Online-Portal für die internetbasierte Kfz-Zulassung im Rahmen einer Datenverarbeitung im Auftrag gemäß § 11 Brandenburgisches Datenschutzgesetz (BbgDSG) für die jeweilige, örtlich zuständige Kfz-Zulassungsstelle.

Der ZIT-BB hat die Landesbeauftragte bereits frühzeitig in das Projekt eingebunden, da es bei der Umsetzung des Identitätsnachweises mithilfe des elektronischen Personalausweises datenschutzrechtliche Fragen gab. Für das Auslesen des Ausweises bedarf es eines Berechtigungszertifikates für die verantwortliche Stelle. Im Rahmen des mandantenorientierten Verfahrens war zu entscheiden, ob jeder Mandant ein entsprechendes Berechtigungszertifikat benötigt oder aber, ob der Einsatz eines einzigen, gemeinsamen Berechtigungszertifikats möglich ist. Aus datenschutzrechtlicher Sicht und in Abstimmung mit der für die Vergabe der Berechtigungszertifikate zuständigen Stelle, dem Bundesverwaltungsamt, kam hier nur eine delegierende öffentlich-rechtliche Vereinbarung gemäß § 5 Gesetz über kommunale Gemeinschaftsarbeit im Land Brandenburg in Betracht. Damit wird die Aufgabe der Identitätsfeststellung an eine zu bestimmende verantwortliche Stelle verlagert. Konkret haben die Kfz-Zulassungsbehörden diese Kernkomponente des Verfahrens an den Landkreis Elbe-Elster delegiert, sodass dieser nach einer erfolgreich durchgeführten Identifikation des Antragstellers dessen Identitätsdaten an die verantwortliche Daten verarbeitende Stelle übermittelt.

---

56 Dritte Verordnung zur Änderung der Fahrzeug-Zulassungsverordnung und anderer straßenverkehrsrechtlicher Vorschriften vom 23. März 2017 (BGBl. I S. 522).

Ausdrücklich soll an dieser Stelle darauf hingewiesen werden, dass der Bürger die Abmeldung oder Wiederzulassung seines Fahrzeugs nicht selbstständig durchführt. Er stellt lediglich online einen Antrag, welcher im Nachgang durch die zuständige Kfz-Zulassungsstelle fachlich bearbeitet wird.

Die verantwortliche Stelle erhebt mithilfe eines Web-Formulars die erforderlichen Daten für den jeweiligen Zweck (Kfz-Abmeldung, Kfz-Wiederzulassung) und übermittelt diese an das Kraftfahrt-Bundesamt. Die Übermittlung der Antragsdaten von dort an die Fachanwendung der örtlich zuständigen Kfz-Zulassungsstelle zur Weiterbearbeitung des elektronischen Antrages erfolgt durch ein automatisiertes Abrufverfahren. Zur Abwicklung der gebührenpflichtigen Verwaltungsvorgänge wurde auch eine elektronische Bezahlplattform für die Fachanwendung implementiert, um einen Medienbruch bei der Gebührenentrichtung zu vermeiden.

Da es sich bei dem Verfahren der internetbasierten Kfz-Zulassung um ein bedeutendes, flächendeckendes E-Government-Verfahren im Land Brandenburg handelt, wirkte die Landesbeauftragte insbesondere an der datenschutzrechtlichen Verfahrensdokumentation mit und konnte bereits frühzeitig Einfluss auf die Gestaltung und Umsetzung der vertraglichen Regelungen zwischen den Teilnehmern und die erforderlichen technisch-organisatorischen Maßnahmen nehmen. Ziel war es auch, für zukünftige E-Government-Anwendungen eine Musterdokumentation zu entwerfen und diese allen teilnehmenden Behörden zur Verfügung zu stellen.

Im Ergebnis konnte in Kooperation mit der Pilotkommune (Landkreis Elbe-Elster), dem ZIT-BB und allen beteiligten Landkreisen und kreisfreien Städten eine vollständige Verfahrensbeschreibung als Muster erstellt werden. Die Beteiligten sind damit in der Lage, dass Verfahren einer Vorabkontrolle gemäß § 10a BbgDSG zu unterziehen. Damit liegt auch eine wesentliche Voraussetzung für eine Verfahrensfreigabe gemäß § 7 Abs. 3 BbgDSG vor.

Neben der vorgestellten Lösung einer gemeinsamen Online-Plattform für die internetbasierte Kfz-Zulassung hat eine Minderheit der Zulassungsbehörden eigenständige Bürgerportale für E-Government-Anwendungen implementiert und dort die Möglichkeit der internetbasierten Kfz-Zulassung integriert. In Bezug auf die datenschutzgerechte Umsetzung von permanenten Bürgerkonten in Bürgerportalen und die Erforderlichkeit der Online-Registrierung für die Nutzung von elektronischen Verwaltungsdienstleistungen besteht noch Abstimmungsbedarf mit den zuständigen Stellen.

Bürgernahes E-Government ist eine Herausforderung der kommenden Jahre. Das Verfahren der internetbasierten Kfz-Zulassung zeigt, wie Kooperation und vertrauensvolle Zusammenarbeit zwischen verantwortlichen Stellen, Dienstleistern und Aufsichtsbehörden zu einem positiven Ergebnis führen können.

12 Polizei und Verfassungsschutz

12.1 Gemeinsames Kompetenz- und Dienstleistungszentrum für Telekommunikationsüberwachung

Am 19. Juli 2017 wurde in Leipzig der Staatsvertrag über die Errichtung eines Gemeinsamen Kompetenz- und Dienstleistungszentrums der Polizeien der Länder Berlin, Brandenburg, Sachsen, Sachsen-Anhalt und Thüringen auf dem Gebiet der polizeilichen Telekommunikationsüberwachung als rechtsfähige Anstalt öffentlichen Rechts unterzeichnet. Der Landtag Brandenburg hat dem Staatsvertrag am 16. November 2017 zugestimmt.

Wie wir bereits in unserem letzten Tätigkeitsbericht[57] ausgeführt haben, beabsichtigen die Polizeien der Länder Berlin, Brandenburg, Sachsen, Sachsen-Anhalt und Thüringen die Errichtung des Gemeinsamen Kompetenz- und Dienstleistungszentrums, um IT-Systeme zur Telekommunikationsüberwachung zentral zur Verfügung zu stellen. Dadurch werden technisches Know-how gebündelt und Kosten gespart. Die Polizeien der beteiligten Länder bleiben weiterhin für die polizeiliche Fallbearbeitung zur Gefahrenabwehr und Strafverfolgung zuständig. Das Zentrum wird redundant in den Standorten Dresden und Leipzig aufgebaut. Die Aufnahme des Wirkbetriebes soll nach derzeitigem Kenntnisstand zum Ende des Jahres 2019 erfolgen.

Die Datenschutzbeauftragten der betroffenen Länder waren konstruktiv an den Beratungen über den Staatsvertrag beteiligt. Das Ergebnis stellt einen tragbaren Kompromiss zwischen datenschutzrechtlichen Forderungen und dem Ziel einer effizienten und zukunftssicheren Telekommunikationsüberwachung dar. Es wurden u. a. folgende Punkte im Staatsvertrag festgeschrieben:

- Die Grundsätze der Datenminimierung, Datenvermeidung und Datensparsamkeit sind zu beachten.

[57] Tätigkeitsbericht 2014/2015, B 12.4.

- Die nach dem jeweiligen Stand der Technik zu treffenden personellen, technischen und organisatorischen Maßnahmen zur Datensicherheit sind auf der Grundlage eines IT-Sicherheitskonzepts zu ermitteln.

- Die Polizeibehörden der Trägerländer dürfen auch bei der zentralen Datenvorhaltung in der Anstalt ausschließlich auf die in ihrem Zuständigkeitsbereich und auf ihre Veranlassung hin erhobenen Daten zugreifen. Insoweit ist eine strikte und zuverlässige Mandantentrennung zu gewährleisten.

- Soweit ein Landesrecht präventive Telekommunikationsüberwachung zulässt, sind die Speicherbereiche von zu repressiven Zwecken erhobenen Daten zu trennen.

- Der verfassungsrechtliche Schutz des Kernbereiches privater Lebensgestaltung ist zu gewährleisten.

- Die Anstalt bestellt einen behördlichen IT-Sicherheitsbeauftragten.

- Verarbeitet die Anstalt personenbezogene Daten im Auftrag, gelten die Vorschriften über den Datenschutz in dem Auftrag gebenden Land. Der Datenschutzbeauftragte des jeweiligen Landes überwacht die Einhaltung dieser Vorschriften, berät die Anstalt insoweit in Fragen des Datenschutzes und nimmt das Kontrollrecht, darunter auch ein Betretungsrecht, gegenüber der Anstalt wahr.

Bei der weiteren technischen Ausgestaltung des Systems zur Telekommunikationsüberwachung ist die Trennung der Daten nach den jeweils verfolgten Zwecken und nach unterschiedlichen Betroffenen eine der grundlegenden Forderungen. Aus technisch-organisatorischer Sicht kann eine Trennung der Datenbestände der beteiligten Länder entweder physikalisch oder logisch erfolgen. Die Konferenz der unabhängigen Datenschutzbeauftragten des Bundes und der Länder hat in der Orientierungshilfe „Mandantenfähigkeit“ die technischen und organisatorischen Anforderungen an die Trennung von automatisierten Verfahren bei der Benutzung einer gemeinsamen IT-Infrastruktur zusammengefasst. Diese sollten bei der Systemgestaltung berücksichtigt werden.

Der Staatsvertrag legt fest, dass das o. g. Sicherheitskonzept von der Anstalt vor einer Entscheidung über den Einsatz oder eine wesentliche Änderung der Datenverarbeitung zu erstellen ist. Darüber hinaus ist auch eine Datenschutz-Folgenabschätzung hinsichtlich möglicher Gefahren für das Recht auf informationelle Selbstbestimmung vorzunehmen. Entsprechend der technischen Entwicklung ist die Ermittlung und ggf. Anpassung der Sicherheitsmaßnahmen in angemessenen Abständen zu wiederholen. Sollten Risiken für Be-

troffene verbleiben, die nicht durch entsprechende Sicherheitsmaßnahmen oder eine Modifizierung der Datenverarbeitung verhindert werden können, darf das zugehörige Verfahren nicht eingesetzt werden. Diese Regelungen entsprechen der datenschutzrechtlichen Gesetzeslage. Nach unserer Auffassung müssen die Länder jederzeit in die sie betreffenden Teile des Sicherheitskonzepts, der Datenschutz-Folgenabschätzung und ggf. weiterer relevanter Dokumente der Anstalt Einblick nehmen können.

Aufgrund der Komplexität der im Gemeinsamen Kompetenz- und Dienstleistungszentrum zu betreibenden IT-Systeme spielt die Aus- und Fortbildung der Administratoren für die Gewährleistung von Informationssicherheit eine entscheidende Rolle. Datenschutzrechtliche Kontrollen der letzten Jahre haben hier Defizite gezeigt.[58] Ihnen ist durch entsprechende Schulungsmaßnahmen entgegenzuwirken.

Das Gemeinsame Kompetenz- und Dienstleistungszentrum auf dem Gebiet der polizeilichen Telekommunikationsüberwachung darf nur unter der Voraussetzung eines wirksamen technischen Datenschutzes in Betrieb genommen werden. Es muss gewährleistet sein, dass die Daten einer strengen Zweckbindung unterliegen und die Datensicherheit nicht beeinträchtigt ist. Insbesondere ist darauf zu achten, dass die Art, der Umfang und die Verschlüsselung der zu verarbeitenden personenbezogenen Daten, die Trennung der länderspezifischen Datenbestände und die Regelungen zur Datenverarbeitung im Auftrag datenschutzgerecht ausgestaltet werden.

12.2 Mitteilungen der Kommunen über sog. „Reichsbürger“ und „Selbstverwalter“ an Polizei und Verfassungsschutz

Bundesweit sind in den letzten Monaten sog. „Reichsbürger“ oder „Selbstverwalter“ in den Fokus der öffentlichen Aufmerksamkeit geraten. Diesen von ihrer ideologischen Überzeugung her teilweise sehr unterschiedlichen Gruppen und Untergruppen ist gemeinsam, dass sie die Bundesrepublik Deutschland als rechtmäßigen Staat verneinen und sich vielfach den behördlichen Anordnungen widersetzen. Der brandenburgische Verfassungsschutz stuft Teile der „Reichsbürgerbewegung“, die seit 2016 beobachtet werden, als rechtsextremistisch ein, während sich andere diesem Spektrum zuzuordnende Personen lediglich verbal oder durch ihr provokatives Verhalten von der Bundesrepublik distanzieren und die herrschende Rechtsordnung nicht anerkennen.

[58] Tätigkeitsbericht 2014/2015, B 12.3.

Bekanntgeworden sind Fälle, in denen Mitglieder dieser Gruppen die Zahlung von Steuern, Bußgeldern oder Gebühren verweigern, die Tätigkeit von Gerichten und Behörden behindern oder Mitarbeiter bedrohen. Andere nutzen selbst erwählte Titel und Berufsbezeichnungen, maßen sich Hoheitsgewalt an, verweigern die Vorlage von Personalausweisen zur Identifikation oder sprechen „Grundstücksbetretungsverbote“ aus. Neben einer staatsfeindlichen Gesinnung fallen sie zunehmend durch verbale Aggressivität auf. In einzelnen Fällen wurden „Reichsbürger“ gegenüber staatlichen Mitarbeitern auch gewalttätig. Vereinzelt kam es zu bewaffneten Handlungen, denen im Jahr 2016 auch ein Polizeibeamter in Bayern zum Opfer fiel. Laut Bundesregierung sollen mehrere hundert Mitglieder dieser Gruppierungen eine waffenrechtliche Erlaubnis besitzen.[59]

Verfassungsschutz und Polizei reagierten auf diese Entwicklung mit einer verstärkten Beobachtung und Informationssammlung über diese Gruppen. Da bei kommunalen Verwaltungen, die häufig direkten dienstlichen Kontakt zu „Reichsbürgern“ und „Selbstverwaltern“ haben, Einzelinformationen zu diesem Personenkreis vorliegen können, scheint es naheliegend, Erkundigungen dort einzuholen. In einigen Kommunen gingen Schreiben sowohl der Polizei als auch des Verfassungsschutzes ein, in denen in sehr allgemeiner Form gebeten wurde, über alle Sachverhalte zu informieren, bei denen Mitarbeiter verbalen oder körperlichen Angriffen von „Reichsbürgern“ ausgesetzt waren, und darüber hinaus weitere Kenntnisse über mögliche Anhänger dieser Gruppierungen weiterzugeben. Mehrere Kommunen wandten sich daraufhin an uns und baten um eine Stellungnahme, ob und wann personenbezogene Daten zu „Reichsbürgern“ übermittelt werden dürften. Das Polizeipräsidium hatte für die geplanten Informationssammlungen bereits einen Erlass entworfen, der uns allerdings erst im Zuge unserer Recherchen bekannt wurde.

Das Bedürfnis von Verfassungsschutz und Sicherheitsbehörden, Gefährdungen für das Gemeinwesen oder Personen, die die öffentliche Sicherheit gefährden könnten, im Blick zu haben, ist nachvollziehbar. Dennoch müssen die gesetzlichen Vorgaben für Datenerhebungen durch Polizei und Verfassungsschutz auf der einen und Übermittlungsbefugnisse der Kommunen auf der anderen Seite gewahrt werden. Dabei ist zwischen den deutlich voneinander unterschiedenen Aufgaben der Polizei- und Verfassungsschutzbehörden zu unterscheiden.

Als besondere Ausprägung der Gewaltenteilung sind in Deutschland die Aufgaben und Funktionen von Polizeibehörden und Nachrichtendiensten deutlich voneinander zu trennen (Trennungsgebot). Den Nachrichtendiensten

[59] Antwort der Bundesregierung auf die Kleine Anfrage zum Thema „Reichsbürger“ vom Februar 2017, Bundestags-Drs. 18/11246.

kommt die Aufgabe zu, Aufklärung bereits im Vorfeld von Gefährdungslagen zu betreiben. Ihre Tätigkeit dient dem Schutz weit gefasster Ziele, wie dem Schutz vor Bestrebungen, die gegen die freiheitlich demokratische Grundordnung, den Bestand oder die Sicherheit des Bundes oder eines Landes gerichtet sind (vgl. § 3 Abs. 1 Nr. 1 Brandenburgisches Verfassungsschutzgesetz – BbgVerfSchG). Entsprechend diesem vorfeldbezogenen Aufgabenspektrum haben Nachrichtendienste weitreichende Befugnisse zur (verdeckten) Datensammlung. Im Gegenzug zu den Erhebungsbefugnissen, die weit ins Vorfeld eines gefährdenden Handelns reichen, sind die operativen Befugnisse der Verfassungsschutzbehörden auf Information und Beratung beschränkt. Dagegen obliegt der Polizei die Verhütung, Verhinderung und Verfolgung von Straftaten sowie die Abwehr von sonstigen Gefahren für die öffentliche Sicherheit und Ordnung. Sie handelt grundsätzlich offen und trägt operative Verantwortung. Ihrer Aufgabenwahrnehmung entsprechend sind polizeiliche Datenverarbeitungsbefugnisse enger und präziser gefasst, erlauben auch zur Gefahrenabwehr nur ausnahmsweise verdeckte Erhebungen und setzen stets einen konkreten Anlass, etwa einen Tatverdacht, voraus.

Unter Berücksichtigung dieser Unterschiede waren sowohl Erhebungs- als auch Übermittlungsbefugnisse zu prüfen, denn in datenschutzrechtlicher Hinsicht bedarf es für die Übermittlung personenbezogener Daten einer gesetzlichen Grundlage auf Übermittler- und auf Empfängerseite.

Die polizeiliche Anfrage war unspezifisch formuliert und benannte keine Rechtsgrundlage für die gewünschten Datenübermittlungen. Wir konnten darin kein polizeiliches Ersuchen an öffentliche Stellen auf der Grundlage des § 45 Abs. 2 Brandenburgisches Polizeigesetz (BbgPolG) erkennen. Aber auch ohne Ersuchen können öffentliche Stellen personenbezogene Daten, die zu anderen Zwecken erhoben wurden, an die Polizei übermitteln (§ 45 Abs. 1 BbgPolG i. V. m. § 14 i. V. m. § 13 Abs. 2 S. 1 Buchst. a bis g Brandenburgisches Datenschutzgesetz). Dies ist zum Beispiel der Fall, wenn sich bei der rechtmäßigen Aufgabenerfüllung Anhaltspunkte für Straftaten, wie Bedrohung, Nötigung oder Widerstand gegen Vollstreckungsbeamte oder für Ordnungswidrigkeiten ergeben und die Unterrichtung der zuständigen Polizeibehörde geboten erscheint. Gleiches gilt, wenn es zur Abwehr erheblicher Nachteile für das Gemeinwohl oder einer sonst unmittelbar drohenden Gefahr für die öffentliche Sicherheit oder zur Abwehr einer schwerwiegenden Beeinträchtigung der Rechte einer anderen Person erforderlich ist. Die übermittelnde Stelle ist in diesen Fällen gehalten, eine konkrete Prüfung vorzunehmen, und trägt die Verantwortung für die Zulässigkeit der Übermittlung. Das bedeutet für die Praxis: Wird etwa im Zusammenhang mit angekündigten rechtmäßigen Vollzugshandlungen gegen einen Bürger erkennbar, dass dieser sich seiner Überzeugung gemäß auf sein Widerstandsrecht beruft, kann eine Datenübermittlung im Einzelfall geboten sein. Aber nicht jedes den Verwaltungsablauf unzweifelhaft störende oder provokante Verhalten, die Vorlage

ungültiger Papiere oder ein vorgebrachtes abstruses politisches Bekenntnis berechtigt zu Übermittlungen von personenbezogenen Daten des Betroffenen an die Polizei. Diese Art „Widerstand gegen die bestehende Rechtsordnung“ kann mit dem Instrumentarium des Verwaltungsverfahrens sachlich beschieden werden.

Auch auf der Empfängerseite erlaubt § 30 Abs. 1 Nr. 1 BbgPolG die Erhebung personenbezogener Daten nur, wenn dies zur Gefahrenabwehr, insbesondere zur vorbeugenden Bekämpfung von Straftaten, erforderlich ist. Dabei hat das Gesetz eine im Einzelfall bestehende konkrete Gefahr im Blick. Dies stellt auch die Verwaltungsvorschrift des Ministeriums des Innern zum Brandenburgischen Polizeigesetz klar. Es bedarf daher in jedem Einzelfall der Feststellung, dass in absehbar zeitlicher Nähe durch die fragliche Person ein Schaden für die öffentliche Sicherheit und Ordnung mit hinreichender Wahrscheinlichkeit verursacht wird. Gefahrverursachendes Verhalten ist von nonkonformem, möglicherweise auch querulatorischem Handeln zu unterscheiden, das die Schwelle zu bußgeldbewehrtem oder strafrechtlich relevantem Tun gerade nicht überschreitet. Unsachliches oder provokatives Auftreten gegenüber Amtspersonen, verbale oder schriftliche Äußerungen zu vermeintlichen Befugnissen, unkooperatives Verhalten bei Melde- oder Erlaubnisverfahren und Gebührenverweigerung sind aus unserer Sicht allein noch kein ausreichender Anlass, um Personen, die der „Reichsbürger-“ und „Selbstverwalterszene“ zuzuordnen sind, polizeilich zu erfassen. Wir haben daher dem Plan der Polizei, gefahrenabwehrrechtlich noch nicht relevante Sachverhalte und personenbezogene Daten verdeckt bei den Kommunen zu sammeln, nicht zugestimmt.

Das gegenüber den öffentlichen Stellen geäußerte Anliegen der Verfassungsschutzbehörde, ihr alle bekannt gewordenen Tatsachen im Zusammenhang mit „Reichsbürgern“ und „Selbstverwaltern“ einschließlich personenbezogener Daten zu übermitteln, ist nach den speziellen Übermittlungsvorschriften in § 14 BbgVerfSchG zu beurteilen: Gemäß § 14 Abs. 1 BbgVerfSchG unterrichten Behörden und Einrichtungen und damit auch die Kommunen von sich aus die Verfassungsschutzbehörde über Bestrebungen, wenn diese sich gegen die freiheitliche demokratische Grundordnung, den Bestand oder die Sicherheit des Bundes oder eines Landes richten. Derartige Bestrebungen können sowohl von einem Personenzusammenschluss als auch von Einzelperson ausgehen. Voraussetzung ist aber, dass die Gruppe oder die Einzelperson erkennen lässt, dass sie ihre Ziele unter Anwendung von Gewalt erreichen will. Eine konkrete Gewalttat muss dafür nicht vorliegen. Bei Gruppierungen kommt es zudem nicht zwingend auch auf die Gewaltbereitschaft des einzelnen Mitglieds einer solchen Bewegung an. Es genügt vielmehr, dass aufgrund von Tatsachen erkennbar ist, dass der Personenzusammenschluss insgesamt seine Ziele auch unter Anwendung von Gewalt durchsetzen würde. Die Verfassungsschutzbehörde sieht die Reichsbürger-

bewegung offenbar als eine derartige Bestrebung mit Gewaltpotenzial an. Die Beurteilung, ob eine Person einer solchen Gruppierung angehört, liegt jedoch weiterhin in der Verantwortung der Kommune.

Anders ist der Sachverhalt allerdings zu beurteilen, wenn sich eine Einzelperson losgelöst von derartigen Personenzusammenschlüssen individuell als sog. Reichsbürger oder Selbstversorger zu erkennen gibt. Eine Meldung an die Verfassungsschutzbehörde aus eigener Initiative kommt in diesem Fall nur in Betracht, wenn die Person begründeten Anlass zu der Annahme gibt, dass sie selbst auch unter Anwendung von Gewalt ihre verfassungsfeindlichen Ziele durchsetzen würde. Nur dann wäre eine Mitteilung über diese Person an die Verfassungsschutzbehörde von der gesetzlichen Übermittlungsbefugnis gedeckt.

Wir empfehlen den kommunalen Verantwortungsträgern bei zweifelhaften Sachverhalten den Verfassungsschutz zu kontaktieren und relevante Informationen ohne Personenbezug vorzutragen. Bei Interesse kann die Verfassungsbehörde ein Ersuchen gemäß § 14 Abs. 3 BbgVerfSchG stellen. Keinesfalls sind die Kommunen gehalten, Datensammlungen über den Personenkreis intern vorzuhalten oder gezielt Recherchen durchzuführen.

Mitarbeiter kommunaler Verwaltungsträger dürfen personenbezogene Daten zu sog. „Reichsbürgern“ und „Selbstverwaltern“ sowohl an die Polizei als auch den Verfassungsschutz übermitteln, wenn die jeweiligen Voraussetzungen im Polizei- oder im Verfassungsschutzgesetz oder in anderen spezifischen Rechtsgrundlagen vorliegen. Während der Verfassungsschutz zum Zweck politischer Vorfeldaufklärung sehr weitreichende, verdeckte Datenerhebungsbefugnisse hat, sind die der Polizei enger und präziser gefasst. Sie darf Daten nur erheben, wenn Anhaltspunkte für einen Tatverdacht oder eine konkrete Gefahr vorliegen. Handeln, das eine allgemeine Missachtung des Staates und der bestehenden Rechtsordnung ausdrückt, reicht dafür nicht aus.

12.3 Passbilderhebung zur Ermittlung von Fahrzeugführern

Immer wieder erreichen uns Beschwerden von Betroffenen, die eine vermeintlich unzulässige Anforderung von Pass- oder Personalausweisfotos im Zuge von Fahrerermittlungen beklagen. Es handelt sich dabei meist um Fälle, in denen kommunale Behörden der Verkehrsüberwachung oder die Zentrale Bußgeldstelle der Polizei wegen Ordnungswidrigkeiten im Straßenverkehr ermitteln und in denen ein Beweisfoto des Fahrers vorliegt. Über das Kennzeichen können zwar die Halterdaten abgefragt werden, Fahrzeughalter und -führer sind jedoch nicht notwendig identisch. Insbesondere wenn als Halter eine juristische Person (z. B.

Unternehmen) eingetragen ist oder das Messfoto des Fahrzeugführers nicht plausibel zu den Halterdaten passt, müssen weitere Ermittlungen angestellt werden. Die Bußgeldbehörden oder die in Amtshilfe vor Ort ermittelnden Polizeibeamten wenden sich dann teilweise an die lokalen Meldeämter, um über die dort hinterlegten Passbilder einen Abgleich durchzuführen.

Scheidet der Halter als Fahrzeugführer aus, ist er zunächst als Zeuge zu befragen, ob er Auskünfte zum Fahrer geben kann. Allerdings bleibt die Befragung des Halters vor allem im Familienumfeld häufig ergebnislos, weil die Bereitschaft, an der Aufklärung des tatsächlichen Fahrzeugführers mitzuwirken, gering ist. Auch bei einer juristischen Person lässt sich der Fahrer vielfach nicht ermitteln.

Grundsätzlich darf die Verfolgungsbehörde zum Zweck einer sicheren Zuordnung des gesuchten Fahrzeugführers zwar ein Personalausweis- oder Passfoto des zuständigen Meldeamtes anfordern. Dabei müssen jedoch die Vorgaben des § 22 Abs. 2 Passgesetzes (PassG), bzw. § 24 Abs. 2 Personalausweisgesetzes (PAuswG) beachtet werden. Die Übersendung eines Lichtbildes stellt datenschutzrechtlich eine Datenübermittlung dar, für deren Zulässigkeit die ersuchende Behörde die Verantwortung trägt. Voraussetzung ist, dass sie erstens berechtigt ist, solche Daten zu erhalten, und zweitens ohne deren Kenntnis nicht in der Lage wäre, eine ihr obliegende Aufgabe zu erfüllen (Grundsatz der Erforderlichkeit). Diese Voraussetzungen liegen in den beschriebenen Fällen regelmäßig vor. Insbesondere kann die Erforderlichkeit aus unserer Sicht in der Regel nicht mit dem Argument verneint werden, dass versäumt wurde, Vorortermittlungen durch Mitarbeiter der Bußgeldstellen oder Polizeibeamte am Wohnort und ggf. unter Einbeziehung des persönlichen Wohnumfelds des Halters durchzuführen. Denn diese Maßnahmen greifen in das Grundrecht auf Datenschutz des Betroffenen als auch in das allgemeine Persönlichkeitsrecht stärker ein als ein Lichtbildabgleich. Bei solchen Umfragen würde die dem Betroffenen vorgeworfene Ordnungswidrigkeit gegenüber Dritten verbreitet, ohne dass dieser die Möglichkeit hätte, dies zu verhindern oder zuvor gerichtlich klären zu lassen. Die Verfolgungsbehörde ist stets gehalten, das mildere Mittel anzuwenden.

Um dem Grundsatz des Vorrangs der Direkterhebung von Daten beim Betroffenen zu genügen, verlangen wir von der ermittelnden Behörde, dass sie vor einem Lichtbildabgleich zunächst versucht, mit dem Betroffenen telefonisch, schriftlich oder auf sonstige Weise Kontakt aufzunehmen, um diesem die Gelegenheit zur Äußerung zu geben. Bleibt dies ergebnislos, darf eine direkte Datenerhebung als gescheitert gelten und das Lichtbild kann angefordert und rechtmäßig übermittelt werden.

Anders lag ein Amtshilfefall, in dem die Polizei eines anderen Bundeslandes einen unbekannten Fahrzeugführer wegen angezeigter Nötigung im Straßenverkehr suchte. Die ermittelte Halterin, eine GmbH aus Brandenburg, hatte wie schon in früheren Fällen ihre Mitwirkung bei der Aufklärung der Identität des verantwortlichen Fahrzeugführers verweigert. Ein Beweisfoto existierte nicht, sondern lediglich die Personenbeschreibung durch einen Zeugen. Bei zurückliegenden Fahrerermittlungen im Rahmen von Verkehrsordnungswidrigkeitenverfahren in Brandenburg war zu dem fraglichen Fahrzeug mehrfach eine Mitarbeiterin der Firma und in Einzelfällen ihr Ehemann als Nutzer des Fahrzeugs ermittelt worden. Da in der Anzeige ein männlicher Fahrer beschrieben wurde und die Möglichkeit bestand, dass der Ehemann zum Tatzeitpunkt der Fahrzeugführer war, forderte die Polizei bei der Meldebehörde ein Lichtbild an, um dieses mit der Personenbeschreibung aus der Anzeige abzugleichen. Sie verzichtete auf eine Kontaktaufnahme und Anhörung des möglichen verantwortlichen Fahrers, weil sie davon ausging, keine Auskunft zu erhalten.

Anders, als in den Fällen des Lichtbildabgleichs mit Beweisfotos aus Anlagen zur Geschwindigkeitsmessung, existierte ein solches Vergleichsfoto hier nicht. Die ermittelnde Polizei konnte sich lediglich auf eine äußerst vage Personenbeschreibung mit Angaben zu Geschlecht, Haarfarbe und Alter mit erheblicher Spannbreite stützen. Wie sich später herausstellte, wären die Zeugen gar nicht in der Lage gewesen, den Fahrzeugführer mithilfe eines Passfotos zu identifizieren. Die Lichtbildanforderung war daher im Ergebnis kein geeignetes Mittel für Identifizierungszwecke und damit nicht erforderlich. Durch das Versäumnis, den Betroffenen selbst zu der Tat zu befragen, wurde außerdem die Chance, den Fahrzeugführer durch eine weniger einschneidende Maßnahme zu ermitteln, nicht genutzt.

Ist bei einem Verkehrsverstoß der Fahrzeugführer unbekannt, richtet sich die Fahrerermittlung zunächst stets an den Halter des Fahrzeugs – entweder als Betroffener oder in Fällen, in denen der Halter als Fahrzeugführer aus Plausibilitätsgründen ausscheidet, als Zeuge. Wirkt der Halter bei der Ermittlung des verantwortlichen Fahrzeugführers nicht mit, sind weitere Recherchen der Verfolgungsbehörde erforderlich. Bevor das Lichtbild eines verdächtigten Fahrers angefordert wird, um es mit dem vorliegenden Beweisfoto abzugleichen, ist zunächst der Versuch zu unternehmen, Daten direkt beim vermuteten Fahrzeugführer zu erheben.

12.4 Verwendung von Cookies im Internetangebot der Polizei

Im Berichtszeitraum informierte uns ein Petent darüber, dass im Internetangebot der Polizei Brandenburg entgegen der dortigen Datenschutzhinweise dauerhafte Cookies verwendet werden.

Bei Cookies handelt es sich um kleine Textdateien, die im Zuge der Webnutzung auf dem Computer des Nutzers gespeichert werden. Man unterscheidet prinzipiell zwischen dauerhaften und temporären Cookies. Mit dauerhaften Cookies besteht die Möglichkeit, das Surfverhalten des Nutzers über einen längeren Zeitraum zu analysieren und die Ergebnisse z. B. für Zwecke der Marktforschung und Werbung einzusetzen. Diese Art der Cookies darf nur nach vorheriger Einwilligung des Nutzers (Opt-in-Lösung) verwendet werden. Im Gegensatz dazu werden temporäre Cookies nur während des Besuches der Webpräsenz (Sitzung) abgelegt. So können beispielsweise Authentisierungsdaten eines Nutzers durch temporäre Cookies gespeichert werden, sodass nicht auf jeder Unterseite eine neue Anmeldung erforderlich ist.

In ihrem Internetangebot stellt die Polizei Brandenburg Informationen zu verwendeten Cookies bereit. Sie weist darin ausdrücklich darauf hin, dass keine dauerhaften Cookies verwendet werden. Wir nahmen die Diskrepanz zwischen dieser Erklärung und den Beobachtungen unseres Petenten zum Anlass, das Internetangebot der Polizei zu prüfen. Dabei stellte sich heraus, dass tatsächlich dauerhafte Cookies verwendet wurden. Wir haben daraufhin die Verantwortlichen aufgefordert, deren Speicherung zu beenden. Die erforderlichen Änderungen nahm die Polizei Brandenburg umgehend vor, sodass jetzt, wie in ihren Hinweisen angegeben, nur noch temporäre Cookies verwendet werden.

Bei der Erstellung von datenschutzfreundlichen Internetangeboten sollte darauf geachtet werden, dass grundsätzlich nur temporäre Cookies eingesetzt werden. Dauerhafte Cookies dürfen nur nach Einwilligung des Nutzers gespeichert werden.

13 Schule

13.1 Digitalisierung im Klassenzimmer – von Schul-Cloud bis WhatsApp

Der Einsatz digitaler Lehr- und Lernmittel, z. B. über Online-Lernplattformen, wird in der schulischen Praxis künftig weiter an Bedeutung gewinnen. Die Beachtung der datenschutzrechtlichen Voraussetzungen bedeutet dabei für viele Schulen eine große Herausforderung – nicht zuletzt deshalb, weil gegenwärtig entsprechende Leitlinien bzw. Handlungsempfehlungen fehlen. Gleiches gilt auch für die Nutzung elektronischer Kurznachrichtendienste, die im privaten Bereich längst etabliert sind.

13.1.1 Online-Lernplattformen

Online-Lernplattformen können vielfältig genutzt werden. Sie ermöglichen meist einen einfachen, webbasierten Zugang zu digitalen Lehr- und Lerninhalten. Weitere Funktionalitäten wie Diskussionsforen, das Bearbeiten von Übungsaufgaben, das Durchführen von Tests oder das Bereitstellen von Vertretungsplänen gehören oft zum praktischen Leistungsumfang dieser Programme. Gern greifen Schulen auf Angebote von Herstellern oder Dienstleistern zurück, extern bereitgestellte Online-Lernplattformen (z. B. als cloudbasierte Lösungen) zu nutzen, da sie so den Aufwand der technischen Wartung und Pflege sparen. „Befördert“ werden solche Entscheidungen zum Teil dadurch, dass Hersteller ihre Hard- und Software kostenlos für ganze Schulklassen bereitstellen.

Auch wenn viele Vorteile für den Einsatz von Lernplattformen sprechen, fallen bei deren Nutzung regelmäßig personenbezogene Daten an, u. a. durch die personalisierte Anmeldung der Nutzer oder die Protokollierung ihres Verhaltens. Darüber hinaus legen externe Plattformanbieter oft nicht vollständig offen, welche Informationen sie zusätzlich im Hintergrund speichern und auswerten. Es besteht die Gefahr der Erstellung von Persönlichkeitsprofilen der Schüler oder Lehrer. Die jeweiligen Schulen müssen als Daten verarbeitende Stellen daher die besonderen datenschutzrechtlichen Anforderungen beim Einsatz von Lernplattformen beachten.

Gemäß § 11 Abs. 1 Datenschutzverordnung Schulwesen ist der Schulleiter für die Einhaltung des Datenschutzes verantwortlich. Er gibt Hinweise zur Datenverarbeitung, organisiert und kontrolliert die Beachtung der datenschutzrechtlichen Bestimmungen und bestellt einen behördlichen Datenschutzbeauftragten. Vielfach verfügen die Leiter allerdings nicht über ausreichende Datenschutzkenntnisse. Auch existiert an vielen Schulen kein be-

hördlicher Datenschutzbeauftragter.[60] Aus unserer Sicht ist es dringend geboten, dass das zuständige Ministerium verstärkt auf die Einhaltung dieser Vorschriften hinwirkt.

Für den Einsatz von Online-Lernplattformen stellt sich zunächst die Frage nach der Rechtsgrundlage der Verarbeitung personenbezogener Daten. Nach § 65 Abs. 2 Brandenburgisches Schulgesetz dürfen Schulen personenbezogene Daten von Schülern oder Lehrkräften nur verarbeiten, soweit dies zur rechtmäßigen Erfüllung des Erziehungs- und Bildungsauftrages der Schule und für einen jeweils damit verbundenen Zweck oder zur Durchführung schulorganisatorischer Maßnahmen erforderlich ist. Beide Voraussetzungen erfüllen Online-Lernplattformen nach unserer Auffassung jedoch nicht. Deshalb kann ihr Einsatz gegenwärtig nur auf freiwilliger Basis erfolgen.

Schüler bzw. bei Minderjährigen deren Eltern müssen daher vorab ausreichend über den konkret geplanten Einsatz der Lernplattform, die beteiligten Institutionen (z. B. externe Dienstleister oder Hersteller digitaler Lehr- und Lernmittel), die Einzelheiten der Datenverarbeitung und die entsprechenden Konsequenzen informiert werden. Erst dann können sie freiwillig entscheiden, ob sie eine rechtsgültige Einwilligung in die Datenverarbeitung geben. Diese muss auch widerrufbar sein. Schulen, die Lernplattformen einsetzen wollen, sind deshalb aufgefordert, Vorkehrungen zu treffen, damit diejenigen, die nicht in deren Nutzung einwilligen, keine Nachteile im Unterricht haben.

Darüber hinaus müssen Schulen vor dem Einsatz von Online-Lernplattformen auch die übrigen datenschutzrechtlichen Vorschriften einhalten. Dies betrifft z. B. die Freigabe des Verfahrens gemäß § 7 Abs. 3 Brandenburgisches Datenschutzgesetz (BbgDSG), die Erstellung eines Verfahrensverzeichnisses gemäß § 8 BbgDSG, die Umsetzung technischer und organisatorischer Maßnahmen gemäß § 10 BbgDSG oder ggf. den Abschluss schriftlicher Verträge mit externen Dienstleistern zur Datenverarbeitung im Auftrag gemäß § 11 BbgDSG.

Im Berichtszeitraum waren wir mehrfach beratend bei der Einführung von Online-Lernplattformen tätig. In einem Fall arbeitet ein Potsdamer Forschungsinstitut gegenwärtig an einem Pilotprojekt zur Bereitstellung einer Cloud-Plattform für webbasierte Lehr- und Lerninhalte, das in insgesamt 13 Bundesländern an jeweils mehreren Schulen erprobt werden soll – darunter auch an einem brandenburgischen Gymnasium. In virtuellen Klassenräumen können Lehrkräfte u. a. Arbeitsmaterialien und Aufgaben anbieten, welche die Schüler dann in der Schule und zu Hause selbstständig bearbeiten. Gleichzeitig sollen die nutzungsbezogenen Daten der Schüler und Lehrkräfte für ein vom Bundesministerium für Bildung und Forschung gefördertes For-

[60] Siehe B 13.4.

schungsvorhaben zu Evaluationszwecken verwendet werden. Nach unserer intensiven Beratung hat das Institut für beide Teilprojekte wirksame schriftliche Einwilligungserklärungen formuliert, die die Anforderungen von § 4 Abs. 2 BbgDSG erfüllen. Die Einholung der Einwilligungen obliegt im Fall des Einsatzes der Lernplattform der jeweiligen Schule, im Fall der Datennutzung zu Evaluationszwecken dem Institut selbst.

Darüber hinaus haben wir gemeinsam mit dem Institut einen Mustervertrag für die Datenverarbeitung im Auftrag gemäß § 11 BbgDSG entwickelt. Dieser ist erforderlich, da die am Projekt teilnehmende Schule den Service „SchulCloud“ des Instituts nutzt. Der Mustervertrag enthält den Vertragsgegenstand, den Umfang und die Art der Datenverarbeitung sowie die gegenseitigen Vertragspflichten der Schule als Auftraggeber (u. a. Kontrollpflichten) und des Instituts als Auftragnehmer (u. a. Weisungsgebundenheit). Bedeutsam ist, dass die Schule allein für die Einhaltung des Datenschutzgesetzes, vor allem für die Rechtmäßigkeit der Datenverarbeitung und der Datenweitergabe an den Auftragnehmer, verantwortlich ist. Durch die Bereitstellung eines Mustervertrages werden die am Projekt teilnehmenden Schulen wesentlich entlastet.

In einer Orientierungshilfe[61] beschreiben die unabhängigen Datenschutzbehörden des Bundes und der Länder, welche datenschutzrechtlichen Mindestkriterien Online-Lernplattformen erfüllen müssen. Sie soll auch den Anbietern derartiger Systeme die Möglichkeit geben, ihr jeweiliges Produkt so zu gestalten oder anzupassen, dass eine Nutzung durch Schulen datenschutzrechtlich zulässig ist.

13.1.2 Nutzung von WhatsApp

Immer wieder erhalten wir Anfragen sowohl von Lehrern als auch von Eltern, ob und unter welchen Voraussetzungen Kurznachrichtendienste wie WhatsApp an Schulen genutzt werden dürfen.

Ähnlich vielen sozialen Netzwerken, wie z. B. Facebook, verarbeitet auch der Messengerdienst WhatsApp personenbezogene Daten auf Servern in Ländern, die weder dem Telekommunikationsgesetz unterliegen noch ein akzeptables Datenschutzniveau nachweisen können. Bereits aus diesem Grund bestehen erhebliche Zweifel an einem datenschutzgerechten Umgang mit den personenbezogenen Daten.

Für einen solchen Eingriff in das Recht der Schüler sowie unbeteiligter Dritter auf informationelle Selbstbestimmung enthalten weder das Brandenburgische Schulgesetz noch die Datenschutzverordnung Schulwesen eine Rechts-

[61] Orientierungshilfe der Datenschutzaufsichtsbehörden für Online-Lernplattformen im Schulunterricht, siehe http://www.lda.brandenburg.de.

grundlage. Eine Datenverarbeitung ohne Rechtsgrundlage ist nur mit Einwilligung der betroffenen Personen zulässig.

Die Einwilligung in die Datenverarbeitung scheitert im konkreten Fall jedoch schon an der fehlenden Freiwilligkeit: Ohne Nutzung des Dienstes würden den Schülern wichtige Informationen aus dem Klassenchat (wie z. B. Mitteilungen zu Hausaufgaben, Klausuren oder Terminen) vorenthalten. Aufgrund des faktischen Gruppenzwanges können Schüler, die den Dienst nicht nutzen, zudem schnell als Außenseiter stigmatisiert werden. Lehrpersonal kann deshalb den ihm anvertrauten Schülern nicht „nahelegen“ oder sie dazu verpflichten, den Dienst WhatsApp für schulische Zwecke, wie das Erteilen von Hausaufgaben, die Korrespondenz untereinander, die Versendung von Lösungen oder Noten usw. zu nutzen. Vielmehr empfehlen wir den Lehrkräften, alternative, datenschutzrechtlich unproblematische Kommunikationsplattformen zu verwenden.

Im Ergebnis vertreten wir die Auffassung, dass die Nutzung von WhatsApp für die dienstliche Kommunikation der Lehrkräfte mit der Schülerschaft aus den vorgenannten Gründen unzulässig ist. Dies schließt die Einrichtung von WhatsApp-Gruppen für Schulklassen ein. Gegenwärtig sieht das zuständige Ministerium jedoch immer noch keinen Handlungsbedarf, den Schulen klare Richtlinien und Hinweise zur Nutzung von Messengerdiensten zu geben.

Um mit der rasanten Entwicklung der Informationstechnik Schritt zu halten und Online-Verfahren im Zusammenhang mit der Nutzung digitaler Medien im Unterricht oder elektronische Kurznachrichtendienste im schulischen Kontext zu nutzen, müssen eindeutige rechtliche und technische Rahmenbedingungen geschaffen werden. Die Verantwortlichen in den Schulen dürfen mit der Umsetzung der datenschutzrechtlichen Anforderungen nicht allein gelassen werden. Das zuständige Ministerium ist gefordert, zentral entsprechende Regelungen zu treffen und Hinweise zu geben.

13.2 Keine Eile bei der Förderung der Medienkompetenz

Schulische Medienbildung hat unter anderem zum Ziel, Schüler für einen selbstbestimmten und verantwortungsvollen Mediengebrauch zu befähigen. Dabei spielt das Recht des Einzelnen, selbst über die Preisgabe und Verwendung seiner personenbezogenen Daten zu bestimmen, eine bedeutende Rolle. Um dieses Ziel zu erreichen, definieren die Rahmenlehrpläne fächerübergreifend Schwerpunkte und Maßnahmen zur Medienbildung. Zur Umsetzung des Basiscurriculums Medienbildung hat die Landesbeauftragte im Berichtszeitraum mit dem zuständigen Landesinstitut für Schule und Medien Berlin-Brandenburg Gespräche geführt.

Die vom Landesinstitut herausgegebene Handreichung "Cybermobbing ist nicht cool" enthält unter anderem Handlungsempfehlungen für Maßnahmen der Prävention und Intervention bei Vorfällen von Cybermobbing. In einem Beitrag zu dieser Veröffentlichung hatten wir die Gelegenheit, die datenschutzrechtlichen Bezüge dieses Themas darzustellen. Die Broschüre wurde allen Schulen in Brandenburg und Berlin zur Verfügung gestellt und ist auf dem Bildungsserver Berlin-Brandenburg abrufbar.[62]

Darüber hinaus schlug das Landesinstitut vor, ein Arbeitspapier mit Praxisfällen zum Datenschutz in der digitalen Medienbildung herauszugeben und den Schulen zur Verfügung zu stellen. Obwohl die Landesbeauftragte die hierfür vorgesehenen Beiträge wie vereinbart erstellt und dem Landesinstitut angeboten hatte, kam das Papier bislang nicht zustande. Auch ein Workshop mit Schulleitern und Schulberatern, auf dem datenschutzrechtliche Grundsätze zu vermitteln wir uns gerne bereit erklärt hatten, fand noch nicht statt.

Die in der Kooperation zwischen dem Landesinstitut und unserer Dienststelle bisher erreichten Ergebnisse sind überschaubar. Aufgrund entsprechender Zusagen gehen wir davon aus, künftig intensiver in Projekte eingebunden zu werden und auf eine angemessene Berücksichtigung der Anliegen des Datenschutzes in der schulischen Medienbildung hinwirken zu können.

13.3 Auskunftsrechte getrennt lebender Eltern gegenüber der Schule ihres Kindes

Ein Vater, der sich das gemeinsame Sorgerecht mit seiner geschiedenen Frau teilt, beschwerte sich über die Schulleiterin der Grundschule seines bei der Mutter lebenden Sohnes. Er hatte u. a. Zeugniskopien des letzten Halbjahres, die Dokumentation über die Fehlstunden und Leistungseinschätzungen seines Sohnes begehrt. Die Schulleiterin verweigerte die Auskünfte mit der Begründung, dass nur die Person, bei der sich das Kind aufhält, Informationen erhält.

§ 65 Abs. 8 Satz 1 Brandenburgisches Schulgesetz (BbgSchulG) räumt den Eltern ein Recht auf Einsicht in die sie betreffenden Unterlagen und auf unentgeltliche Auskünfte über die sie betreffenden Daten ein. Das Recht minderjähriger Schüler üben ihre Eltern aus. Gemäß § 65 Abs. 8 Satz 4 BbgSchulG können die Einsichtnahme und die Auskunft nur dann eingeschränkt oder versagt werden, wenn der Schutz des betroffenen Schülers, seiner Eltern, von Lehrkräften oder von Personen des sonstigen Schulperso-

62 „Cybermobbing ist nicht cool! Projektbericht und Handlungsempfehlungen für Maßnahmen der Prävention und Intervention bei Vorfällen von Cybermobbing“, http://bildungsserver.berlin-brandenburg.de.

nals sowie von Dritten dies erforderlich macht. Solche Verweigerungsgründe lagen konkret nicht vor.

Weder aus den Regelungen des Brandenburgischen Schulgesetzes noch aus der Datenschutzverordnung Schulwesen ergeben sich Bestimmungen, die die Pflicht zur Auskunftserteilung von dem jeweiligen Aufenthaltsort des Kindes abhängig machen. Vielmehr gilt der gemeinsam sorgeberechtigte Vater als Elternteil i. S. d. § 2 Nr. 5 BbgSchulG mit der Folge, dass auf ihn genauso wie auf die Kindesmutter die Bestimmungen des Brandenburgischen Schulgesetzes und der Datenschutzverordnung Schulwesen anzuwenden sind. Ihm stehen damit dieselben Einsichts- und Auskunftsrechte zu.

Der vom Kind getrennt lebende, aber zugleich gemeinsam sorgeberechtigte Elternteil hat die gleichen Einsichts- und Auskunftsrechte wie der Elternteil, bei dem sich das Kind gewöhnlich aufhält.

13.4 Übereilte Bestellung des behördlichen Datenschutzbeauftragten einer Schule

Aufgrund eines datenschutzrechtlichen Vorfalls baten wir eine Schule um die Benennung des behördlichen Datenschutzbeauftragten. Die Schulleiterin sandte uns eine vom Bürgermeister unterschriebene Bestellungsurkunde des gemeindlichen behördlichen Datenschutzbeauftragten, der zeitgleich und ohne vorherige Absprachen von seiner Berufung erfuhr.

Nach § 11 Abs. 1 Datenschutzverordnung Schulwesen (DSV) hat jede Schule einen behördlichen Datenschutzbeauftragten zu bestellen. Dieser kann in begründeten Einzelfällen mit seinem Einverständnis für mehrere Schulen bestellt werden, wenn dadurch die Erfüllung seiner Aufgaben nicht beeinträchtigt wird. Er ist in diesem Fall von der jeweiligen Schule gesondert zu bestellen.

Eine gesonderte Bestellung durch die betreffende Grundschule erfolgte hier jedoch nicht; diese wurde von der Gemeinde vorgenommen. Zudem hatte der behördliche Datenschutzbeauftragte der Gemeinde, der ohne sein Wissen bestellt worden war, dies nachträglich abgelehnt. Die Grundschule hat nunmehr einen solchen Beauftragten aus ihren eigenen Reihen bestellt.

Soweit sich die jeweilige Schule eines gemeindlichen behördlichen Datenschutzbeauftragten bedient, muss ihn die Schulleitung selbst bestellen.

13.5 Heimarbeitsplatz einer Schulleiterin

Immer wieder gibt es Anfragen zur Heimarbeit von Lehrkräften. Im konkreten Fall wollte eine Grundschulleiterin wissen, ob sie von zu Hause über ihren privaten PC auf das Netzwerk der Schule zugreifen darf.

Zur Telearbeit an häuslichen Arbeitsplätzen haben wir uns bereits in früheren Tätigkeitsberichten geäußert.[63]

§ 65 Abs. 5 Brandenburgisches Schulgesetz verlangt, dass personenbezogene Daten von Schülern, deren Eltern, Lehrkräften und sonstigem Schulpersonal in der Regel nur in der Schule verarbeitet werden dürfen. Der Schulleiter kann in begründeten Fällen gestatten, dass Lehrkräfte oder sonstiges pädagogisches Personal Daten von Schülern auf Datenverarbeitungsgeräten außerhalb der Schule verarbeiten. Die Kategorien der hierfür zugelassener Daten können der Anlage 1 zur Datenschutzverordnung Schulwesen (DSV) entnommen werden. Dort ist auch festgelegt, für welche Daten eine Verarbeitung außerhalb der Schule ausgeschlossen ist.

Für die Genehmigung bedarf es nach § 5 DSV weiterhin folgender Voraussetzungen:

- Die Datenverarbeitung muss der konkreten Aufgabenerfüllung im unmittelbaren pädagogischen Verantwortungsbereich der Lehrkraft oder der Person des sonstigen pädagogischen Personals dienen.

- Es muss ein Sicherheitskonzept gemäß § 7 Abs. 3 des Brandenburgischen Datenschutzgesetzes (BbgDSG) existieren, das auch die besonderen Risiken der Datenverarbeitung außerhalb der Schule und auf privaten Geräten berücksichtigt.

- Die Umsetzung technischer und organisatorischer Maßnahmen ist nach dem Sicherheitskonzept sowie gemäß § 10 Abs. 1 und 2 BbgDSG nachzuweisen und durch die Schulleiterin oder den Schulleiter zu bestätigen.

- In einer vorherigen schriftlichen Einverständniserklärung hat die Lehrkraft sich der Kontrolle der Landesbeauftragten für den Datenschutz und für das Recht auf Akteneinsicht zu unterwerfen. Die Schule bleibt Daten verarbeitende Stelle und ist für die Einhaltung der Voraussetzungen nach § 8 BbgDSG verantwortlich. Für die Beantragung und Genehmigung des Verfahrens ist die Anlage 7 zur DSV zu verwenden.

63 Tätigkeitsbericht 2008/2009, A 2.5 und Tätigkeitsbericht 2012/2013, B 3.3.

Die Einrichtung eines Heimarbeitsplatzes für Lehrkräfte ist unter bestimmten Voraussetzungen grundsätzlich zwar möglich. Im Rahmen der Sicherheitsbetrachtungen müssen jedoch die bei der Telearbeit entstehenden, zusätzlichen Risiken beachtet werden. Durch technische und organisatorische Maßnahmen ist ein dem dienstlichen Arbeitsplatz vergleichbares Sicherheitsniveau zu gewährleisten.

14 Finanzen

14.1 Löschkonzept für das Verfahren des Neuen Finanzmanagements

Im Rahmen des Neuen Finanzmanagements (NFM) in der Landesverwaltung wird für das Haushalts-, Kassen- und Rechnungswesen ein SAP-System eingesetzt. Wir hatten die bereits einige Jahre zurückliegende Einführung des Systems datenschutzrechtlich begleitet und schon zum damaligen Zeitpunkt auf die Notwendigkeit eines Löschkonzeptes hingewiesen. Auch wenn im Finanzbereich lange Aufbewahrungsfristen bestehen, sind rechtzeitig Vorkehrungen zu treffen.

Gemäß § 19 Abs. 2 Buchst. b Brandenburgisches Datenschutzgesetz sind personenbezogene Daten zu löschen, wenn ihre Kenntnis für die Daten verarbeitende Stelle zur Aufgabenerfüllung nicht mehr erforderlich ist. Buchhaltungsdaten, die im NFM verarbeitet werden, sind im Regelfall nach Ablauf der gesetzlichen Aufbewahrungsfristen nicht mehr erforderlich. Eine Löschung nach Fristablauf ist daher vorzusehen. Es gibt jedoch kein einfaches Schema, mit dem die für jeden einzelnen Buchungssatz gültige Löschfrist bestimmt werden kann. Zudem ist die Umsetzung von Löschungen in der Standardkonfiguration des SAP-Systems nicht vorgesehen. Insofern hat das Ministerium der Finanzen als Verfahrensbetreiber zu prüfen, ob es das System selbst anpassen kann oder ob der Hersteller nachbessern muss.

Unsere Sachstandsanfrage zur Erstellung eines Löschkonzepts ergab zunächst, dass bislang keine Aktivitäten in diese Richtung entfaltet worden sind. Ein sensibilisierendes Gespräch zur datenschutzrechtlichen Erforderlichkeit des Löschens personenbezogener Daten in SAP hat dann aber schnell dazu geführt, dass das Ministerium ein entsprechendes, qualitativ hochwertiges Masterkonzept erstellt hat, welches ein systematisches Vorgehen zur Bestimmung von zu löschenden Daten, Löschfristen, Löschklassen und Löschregeln enthält. Zudem hat es einen Prozess zur Erstellung eines detaillierten Löschkonzeptes gestartet. Da hierzu sämtliche verantwortlichen Stellen in der Landesverwaltung, die das Verfahren verwenden, zuarbeiten müssen, hat

das Ministerium für die notwendigen Informationsveranstaltungen und das Zusammenführen der Ergebnisse ungefähr ein Jahr eingeplant. Berücksichtigt man, dass es Dutzende Belegarten mit unterschiedlichen Aufbewahrungsfristen in der Buchhaltung der Landesverwaltung zu beachten gibt, die wiederum von einer Vielzahl verschiedener verantwortlicher Stellen zu identifizieren sind, erscheint diese Frist nicht zu lang.

Personenbezogene Daten in der Finanzverwaltung sind nach Ablauf der gesetzlichen Aufbewahrungsfristen zu löschen. Verantwortliche Stellen und Verfahrensbetreiber haben daher dafür Sorge zu tragen, dass dafür alle erforderlichen Maßnahmen ergriffen werden. Bei einem komplexen Verfahren, wie dem Neuen Finanzmanagement, muss hierfür ein umfassendes Löschkonzept erstellt werden. Das Ministerium der Finanzen setzt diese Aufgabe derzeit um.

14.2 Darf das Finanzamt der Krankenkasse Auskunft über persönliche Daten geben?

Eine Krankenkasse erkundigte sich bei dem zuständigen Finanzamt nach den Einkommensteuerbescheiden eines ihrer freiwillig Versicherten, der selbstständig erwerbstätig war, um dessen Beiträge zur gesetzlichen Kranken- und Pflegeversicherung festzulegen. Das Finanzamt gab Auskunft, ob und wann Steuerbescheide erlassen worden waren.

Die Krankenkasse ermittelt als zuständiger Sozialversicherungsträger im Sinne des Zehnten Buches Sozialgesetzbuch zum Zwecke der Festsetzung der Beiträge zur gesetzlichen Kranken- und Pflegeversicherung für freiwillige Mitglieder, die hauptberuflich selbstständig erwerbstätig sind, die beitragspflichtigen Einnahmen. Im Regelfall dient hierfür die Beitragsbemessungsgrenze. Der freiwillig Versicherte kann allerdings eine Beitragsreduzierung erreichen, wenn er geringere Einnahmen nachweist (§ 240 Abs. 4 Satz 2 Fünftes Buch Sozialgesetzbuch). Die aus dem zuletzt vorgelegten Einkommenssteuerbescheid abgeleitete Beitragsbemessung bleibt dann bis zur Erteilung des nächsten Einkommenssteuerbescheides maßgebend.

In unserem Fall erklärte der Versicherte seiner Krankenkasse auf Nachfrage, ihm sei seit mehr als 18 Monaten kein Steuerbescheid zugegangen. Aus diesem Grund richtete die Krankenkasse ihr Auskunftsersuchen nunmehr an das Finanzamt. Dieses teilte der Krankenkasse unter Angabe des Datums des Bescheides und des Veranlagungszeitraumes mit, welche Einkommenssteuerbescheide in den letzten 18 Monaten erlassen wurden.

Nach § 31 Abs. 2 Abgabenordnung sind die Finanzbehörden gegenüber den gesetzlichen Krankenkassen als Träger der gesetzlichen Sozialversicherung

auskunftspflichtig. Hierzu hat das Bundesministerium der Finanzen in einem Anwendungserlass festgelegt: Erklärt ein freiwillig Versicherter, der selbstständig erwerbstätig ist und eine Beitragsreduzierung erreichen möchte, seiner Krankenkasse auf Nachfrage, ihm sei seit mehr als 18 Monaten kein Steuerbescheid zugegangen, ist der Krankenkasse auf Ersuchen mitzuteilen, ob innerhalb dieses Zeitraums ein Steuerbescheid erteilt wurde; im Idealfall ist auch dessen Datum und das jeweilige Veranlagungsjahr mitzuteilen. Somit handelte es sich bei den vom Finanzamt an die Krankenkasse erteilten Auskünften um eine rechtmäßige Datenübermittlung.

Soweit die Kenntnis von im Besteuerungsverfahren bekannt gewordenen Verhältnissen eines Versicherten für die zu treffende Beitragsfestsetzung der gesetzlichen Krankenkasse erforderlich ist, sind die Finanzbehörden hierüber grundsätzlich auskunftspflichtig.

14.3 Muss ein Auskunftsersuchen zu den eigenen Daten gegenüber dem Finanzamt begründet werden?

Der Antragsteller begehrte gemäß § 18 Brandenburgisches Datenschutzgesetz (BbgDSG) vom Finanzamt Auskunft über die zu seiner Person gespeicherten Daten. Das Finanzamt verlangte, dass er zunächst den Grund für sein Auskunftsersuchen angibt.

Allgemein gilt, dass je nach begehrter Information und dem Stand des Verfahrens für Auskunftsverlangen unterschiedliche Anspruchsgrundlagen zur Anwendung kommen. Die begehrte Auskunft des Antragstellers bezog sich ausschließlich auf seine eigenen Daten, sodass der Sachverhalt nach dem Brandenburgischen Datenschutzgesetz zu prüfen war.

Das Finanzamt hielt jedoch das Akteneinsichts- und Informationszugangsgesetz (AIG) für einschlägig. Es lehnte den Antrag ab und berief sich auf § 4 Abs. 2 Nr. 4 AIG. Danach soll ein Antrag auf Akteneinsicht abgelehnt werden, wenn die ordnungsgemäße Erfüllung der Aufgaben der öffentlichen Stelle erheblich beeinträchtigt würde, es sei denn, dass das Interesse an der Einsichtnahme das entgegenstehende öffentliche Interesse im Einzelfall überwiegt. Da der Antragsteller sein Interesse nicht dargelegt hatte, fiel die Abwägung zu seinen Lasten aus und führte zur Ablehnung seines Antrags.

Das Finanzamt hatte allerdings außer Acht gelassen, dass das Akteneinsichts- und Informationszugangsgesetz gar nicht zur Anwendung kommt, vielmehr war § 18 Abs. 1 BbgDSG einschlägig. Auch das Bundesverfassungsgericht hatte bereits mit Entscheidung vom 10. März 2008 (1 BvR 2388/03) festgestellt, dass der Anspruch auf Informationen aus der eigenen Steuerakte verfassungsrechtlich geboten ist. Mangels spezialgesetzlicher

Regelungen hierzu greift daher auch im Abgabenrecht § 18 BbgDSG bei Ersuchen auf Zugang zu Daten, die zur eigenen Person gespeichert sind.

Wir erläuterten dem Finanzamt die Rechtslage sowie die einzelnen Bestimmungen des § 18 BbgDSG, der jedem Betroffenen ohne Nennung eines besonderen Grundes einen grundsätzlichen Anspruch auf Auskunft über die zu seiner Person gespeicherten Daten und über die Herkunft und mögliche Empfänger dieser Daten gewährt. Die begehrten Informationen waren unserem Petenten somit gemäß § 18 BbgDSG ohne Angabe eines Grundes zu erteilen.

Auch gegenüber einem Finanzamt muss für ein Auskunftsersuchen nach § 18 BbgDSG keine Begründung dargelegt werden.

15 Telekommunikation und Telemedien

15.1 Internationale Zusammenarbeit am Beispiel sync.me

Aus einer Beschwerde über die Sammlung von personenbezogenen Daten durch einen in Israel ansässigen App-Anbieter wurde ein andauerndes Projekt europäischer Aufsichtsbehörden, an dem die Landesbeauftragte bis heute mitarbeitet – eine von mehreren von uns angeregten Kooperationen in einer zusammenwachsenden Datenschutzwelt.

Im August 2015 erreichte uns die Beschwerde eines Petenten, dessen Name und Telefonnummer in der Datenbank einer App namens sync.me aufgetaucht war. Die App funktioniert in der Weise, dass sie die Telefonverzeichnisse der Mobiltelefone ihrer Nutzer nebst Namen und anderen dort verfügbaren Informationen in das eigene System lädt und sie zu einer Datenbank zusammenfasst. Wird der App-Nutzer von einer Person angerufen, die in dieser Datenbank, nicht aber im lokalen Telefonverzeichnis des App-Nutzers gelistet ist, sorgt sync.me dafür, dass statt der Telefonnummer die aus der Datenbank bekannten Angaben, insbesondere der Name, ausgegeben werden. Der Dienst kann auch über ein Web-Portal genutzt werden. Betreiber und Anbieter der App ist eine Firma aus Ramat Gan, Israel. Würde die App in Deutschland betrieben, bestünden erhebliche datenschutzrechtliche Zweifel an der Vorgehensweise der Betreiber. Insbesondere wurden die in den Adressverzeichnissen aufgeführten Personen weder um Einwilligung in die Hinzufügung zu der Datenbank gebeten, noch wurde diese Datenerhebung ihnen gegenüber transparent gemacht. So hatte auch unser Petent von seiner Aufnahme in die Datenbank nur zufällig erfahren.

Da der Diensteanbieter selbst keine Niederlassung außerhalb Israels hat, war von der alleinigen Aufsichtszuständigkeit der beim israelischen Justizministerium angesiedelten Datenschutzaufsicht (ILITA) auszugehen. Israel ist zwar nicht Mitglied der Europäischen Union, sodass die Richtlinie 95/46/EG (sog. Datenschutzrichtlinie) dort nicht gilt. Gemäß der Entscheidung 2011/61/EU der Europäischen Kommission ist das Datenschutzniveau in Israel aber als gleichrangig mit dem in der EU anzusehen. Wir hielten es für Erfolg versprechend, den Kontakt herzustellen, um eine rechtliche Einschätzung zu bitten und ein koordiniertes Vorgehen anzubieten. Auf unser Schreiben vom September 2015 erhielten wir zunächst die Bestätigung, dass die datenschutzrechtliche Rechtswidrigkeit des vorgestellten Geschäftsmodells jedenfalls im Hinblick auf israelische Betroffene bereits festgestellt worden sei. Eine weitere Zusammenarbeit in Bezug auf Betroffene in der EU wurde in Aussicht gestellt.

Im folgenden Jahr wurden wir eingeladen, uns an einer Serie von Telefonkonferenzen zum weiteren Vorgehen zu beteiligen. Es stellte sich heraus, dass die niederländische Datenschutzbehörde unabhängig von unserem Haus die ILITA ebenfalls mit der Bitte um Einschätzung kontaktiert hatte. Schließlich bildete sich vonseiten der EU-Mitgliedsstaaten eine Ad-hoc-Arbeitsgruppe von Datenschutzbehörden, die federführend von der britischen Aufsichtsbehörde (The Information Commissioner’s Office) geleitet wurde. Weitere Mitglieder waren die niederländische Autoriteit Persoonsgegevens, die italienische Garante per la protezione dei dati personale sowie die Landesbeauftragte. Gemeinsam ermutigten wir die israelische Behörde mit Hinblick auf die Richtlinie 2002/58/EG (sog. E-Privacy-Richtlinie), ihre Vollzugsaktionen auf die Daten von EU-Bürgern auszuweiten, und leisteten die dafür notwendige rechtliche Zuarbeit. Gleichzeitig nahm die Arbeitsgruppe mehrere andere gleichartige Apps in den Blick, die von unterschiedlichen EU-Mitgliedsstaaten aus betrieben wurden.

Da die Bemühungen der israelischen Kollegen Zeit benötigten, wurde unterdessen in Koordination mit einem Unterausschuss der Arbeitsgruppe nach Art. 29 der Datenschutzrichtlinie und unter Beteiligung der Vorsitzenden dieser Arbeitsgruppe, der Präsidentin der französischen Commission Nationale de l’Informatique et des Libertés, im Jahr 2017 ein Anschreiben an die verschiedenen App-Betreiber, darunter auch diejenigen von sync.me, erarbeitet, um ihnen die rechtlichen Bedenken gegen ihr Geschäftsmodell unmittelbar mitzuteilen. Eine Evaluation des Effekts dieser Maßnahme steht derzeit noch aus.

Auch ansonsten ist in Fällen der Verarbeitung personenbezogener Daten durch im Ausland ansässigen Stellen die Kooperation zwischen Aufsichtsbehörden im Berichtszeitraum wesentlich verstärkt worden. Dies betrifft nicht nur die zuständigkeitsbedingte Abgabe von Vorgängen an Aufsichtsbehörden

im EU-Ausland, sondern etwa auch Gespräche mit der amerikanischen Federal Trade Commission und dem belgischen Ausschuss für den Schutz des Privatlebens zu einer Immobilienwebseite, die detaillierte Grundstücksprofile einschließlich Fotos mit unbestimmter Veröffentlichungsbefugnis und einer Vielzahl von detaillierten, in der Summe für Betroffene höchst belastenden Grundstücksdaten zur Verfügung stellte.

Insbesondere bei einem Bezug zu Staaten außerhalb der EU gelingt es wegen des teilweise abweichenden Rechtsverständnisses nicht in jedem Fall, eine für den Petenten vollkommen zufriedenstellende Lösung zu finden – Verbesserungen lassen sich dennoch oft erzielen. Die Kooperationen sind daneben von unschätzbarem Wert für uns, da wir auf diese Weise die datenschutzrechtlichen Zustände in anderen Ländern kennenlernen und den Betroffenen zutreffende Auskünfte und Ratschläge geben können. Die Landesbeauftragte wird diese Aktivitäten außerhalb und innerhalb der EU auch in der Zukunft fortsetzen – nicht zuletzt, weil die Datenschutz-Grundverordnung mit dem Europäischen Datenschutzausschuss und dem Marktortprinzip zwangsläufig eine verstärkte internationale Kooperation fordert.

Auch wenn eine Stelle, über die sich Petenten beschweren, außerhalb der Europäischen Union liegt, stehen der Landesbeauftragten verschiedene Möglichkeiten zur Lösung datenschutzrechtlicher Probleme zur Verfügung. Soweit ein Vorgang nicht zuständigkeitshalber an eine andere Datenschutzbehörde abgegeben werden kann, können Kontakte zu Kollegen im Ausland helfen, eine Lösung des Problems oder zumindest eine Klärung des Sachverhalts herbeizuführen. Die Landesbeauftragte wird diesen Weg – auch und gerade aufgrund der Datenschutz-Grundverordnung – weiter beschreiten.

15.2 Zusammenarbeit auf Landesebene – Medienkompetenz, Verbraucherschutz und mehr

Im Bereich Telemedien wurde im Berichtszeitraum die Beratungstätigkeit und Koordination mit verschiedenen Akteuren des Landes im öffentlichen und privaten Bereich erheblich verstärkt.

Die Landesbeauftragte beteiligte sich beispielsweise im Januar 2017 mit einem Vortrag nebst Diskussion an einer Veranstaltung der Eltern-Medien-Beratung zum Datenschutz in sozialen Netzwerken, in der Erzieher zu Fragen der Medienkompetenz geschult wurden. Der Vortrag beschäftigte sich mit der deutschen und europäischen Rechtslage sowie der vielfach davon abweichenden Rechtswirklichkeit, zeigte mögliche Kontrollverluste und Konsequenzen ungesteuerter Mediennutzung, aber auch Möglichkeiten für einen bewussten Umgang auf. Die interaktive Gestaltung und aktive Mitarbeit der Beteiligten führte nach beiderseitigem Eindruck zu einem hohen Erkenntnis-

gewinn und einer effektiven Sensibilisierung für die datenschutzrechtlichen Probleme bei der Nutzung sozialer Medien.

Bereits im Jahr 2016 waren die für Telemedien und für Schulen zuständigen Mitarbeiter unserer Dienststelle auf Einladung des Landesfachverbands Medienbildung Brandenburg e. V. zur Netzwerktagung Medienkompetenz eingeladen. Die Referenten der Landesbeauftragten leiteten und moderierten die Diskussionen mit Lehrern, Schulleitern und anderen Entscheidungsträgern im Bildungsbereich zum Thema Nutzung sozialer Medien für schulische Inhalte. Besonders gefragt war die Einschätzung zu den Möglichkeiten und Grenzen der Nutzung des in Deutschland besonders verbreiteten Messenger-Dienstes WhatsApp für schulische Inhalte. Hier konnte die Landesbeauftragte entgegen manchen Tendenzen im schulischen Bereich im Sinne des bewussten, reflektierten Umgangs mit den neuen Medien wirken.[64]

Ebenfalls wurde die Zusammenarbeit mit der Verbraucherzentrale Brandenburg entscheidend verstärkt. Zu diesem Zweck fanden im Jahr 2016 Beratungen in unserem Hause – insbesondere zum eCommerce im Rahmen des Projekts Digitaler Marktwächter – statt. In Rede standen allgemein Kennzeichen der datenschutzrechtlichen Vertrauenswürdigkeit von Webshops und elektronischen Zahlungsdienstleistern und im Besonderen die Auskunfts- und Löschrechte sowie das Recht zur Anrufung der Aufsichtsbehörden im Konfliktfall und deren Handlungsmöglichkeiten im nationalen und europäischen Rahmen.

Auch soweit gegen Datenschutzverstöße vorgegangen werden muss, findet nunmehr eine verstärkte Koordinierung zwischen der Landesbeauftragten und der Verbraucherzentralen im Telemedienbereich statt. Insbesondere wird eine Harmonisierung der Einschätzungen zu bestimmten sowohl verbraucherschutzrechtlich als auch telemedienrechtlich relevanten Fragen sowie ein abgestimmtes Vorgehen angestrebt. Ziel ist, für die Verbraucher ein gleichmäßiges Datenschutzniveau in Brandenburg zu gewährleisten und gleichzeitig sicherzustellen, dass Anbieter von Telemediendiensten, wie Webseitenbetreiber oder App-Entwickler, einheitliche und transparente Bedingungen für ihre Arbeit in Brandenburg vorfinden.

Es steht zu erwarten, dass mit Wirksamwerden der Datenschutz-Grundverordnung sowie der noch zu verabschiedenden ePrivacy-Verordnung die Kooperations- und Vermittlungstätigkeit stetig weiterzuentwickeln sein wird. Handlungsfelder werden dabei unter anderem die Förderung des Datenschutzbewusstseins bei öffentlichen und nicht öffentlichen Stellen und die Stärkung der Medienkompetenz der Bürger sein.

---

64 Siehe B 13.1.2.

Die Datenschutzbeauftragte kam auch im Telemedienbereich im Berichtszeitraum ihrem Aufklärungsauftrag in einer Vielzahl von Formaten nach – in Diskussionsrunden, Fortbildungsveranstaltungen, Vorträgen und anderen Formen der Zusammenarbeit. Aufgrund der alsbald wirksam werdenden Datenschutz-Grundverordnung kommt einer Fortführung dieser Arbeit hohe Priorität zu.

15.3 Fanpages öffentlicher Stellen bei Facebook

Immer wieder erreichten uns im Berichtszeitraum Anfragen, inwieweit es zulässig ist, dass öffentliche Stellen – etwa Gemeinden – sog. Fanpages, also für alle eingeloggten Nutzer sichtbare und zur Kommentierung nutzbare Seiten des sozialen Netzwerks Facebook einrichten. Eine endgültige Antwort auf die Frage ist heute schwieriger denn je.

Viele Bürger nutzen heute für das Auffinden von Informationen vorrangig soziale Netzwerke, manche meinen gar, ohne diese Dienste wichtige Informationen zu verpassen. Dass hieraus auch ein Wunsch öffentlicher Stellen folgt, auf sozialen Medien – insbesondere bei Facebook – präsent zu sein, verwundert nicht.

Problematisch wird dies angesichts der Tatsache, dass die großen sozialen Netzwerke nur schwer zu bewegen sind, sich an geltendes deutsches bzw. europäisches Datenschutzrecht zu halten und die Vorgaben einer deutschen Aufsichtsbehörde nur sehr eingeschränkt akzeptieren. Um Werbeeinnahmen zu generieren, werden regelmäßig Profile von Betroffenen erstellt, die in ihrer Eingriffstiefe weit über das hinausgehen, was das europäische Recht nach den geltenden Richtlinien vorsieht. Dies betrifft auch das Setzen von Cookies und die Ausführung von Skripten, die den Betroffenen auch beim Navigieren jenseits von Facebook verfolgen. Die Daten der Nutzer, die eigentlich nur mit der öffentlichen Stelle interagieren möchten, gelangen so – zu anderen Zwecken – immer auch zu dem Diensteanbieter selbst.

Gemäß Artikel 2 Buchst. d der Richtlinie EG/95/46 (Datenschutzrichtlinie) ist derjenige für die Verarbeitung von Daten verantwortlich, der allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet. Nach Auffassung der Datenschutzbehörden der Länder schließt dies auch den Betreiber einer Fanpage ein. Er trägt im Rahmen seines Beitrags zur Datenverarbeitung eine eigene Verantwortung für das Schicksal der Daten seiner Besucher. Diese Frage ist derzeit beim Europäischen Gerichtshof anhängig (Aktenzeichen C‑210/16). Bei Redaktionsschluss lag das Plädoyer des Generalanwalts vor. Er bejaht den von den Datenschutzbehörden vertretenen Verantwortlichkeitsbegriff grundsätzlich, da nur so Verantwortlichkeitslücken vermieden werden können. Die

Entscheidung in der Sache steht noch aus, ebenso das abschließende Urteil des Bundesverwaltungsgerichts, das die Frage dem Europäischen Gerichtshof im Vorabentscheidungsverfahren vorgelegt hat. Erfahrungsgemäß hat das Wort des Generalanwalts erhebliches Gewicht bei der Beantwortung der Vorlagefragen.

Der Betrieb einer Fanpage findet nach alledem nicht im rechtsfreien Raum statt und bedarf in jedem Fall weiterer Regeln. Die Entscheidung des Europäischen Gerichtshofs und das auf sie gestützte Urteil des Bundesverwaltungsgerichts werden in diesem Zusammenhang Bindungswirkung entfalten und – in Zusammenschau mit der Datenschutz-Grundverordnung und ggf. auch der in Arbeit befindlichen ePrivacy-Verordnung – eine Neueinschätzung erforderlich machen.

In Erwartung des abschließenden Urteils hat die Landesbeauftragte einen vorläufigen Mindeststandard für das Verhalten öffentlicher Stellen auf sozialen Netzwerken definiert. Bis zu einer endgültigen Klärung durch die Gerichte wird dieser Anforderungskatalog bei der datenschutzrechtlichen Bewertung von Fanpages öffentlicher Stellen zugrunde gelegt. Wegen besonderer schulrechtlicher Vorschriften gilt er nicht für die Schulen.

- Kein Übergriff in Kernbereiche der Verwaltung

  Gesetzliche Aufgaben von Behörden dürfen nicht über die sozialen Medien wie z. B. Facebook, WhatsApp oder Google+ abgewickelt werden, wenn die Betroffenen hierfür personenbezogene Daten preisgeben sollen – sei es gegenüber der Behörde selbst, sei es gegenüber dem Diensteanbieter oder gegenüber Dritten. Dies bedeutet in der Praxis eine Beschränkung auf reine Bereitstellung von Informationen. Behörden, die ihre gesetzlichen Aufgaben unter Verarbeitung personenbezogener Daten – also interaktiv – elektronisch vollziehen möchten, müssen dies im Rahmen eines Verfahrens tun, in dem sie selbst oder von ihr ständig überwachte Auftragsdatenverarbeiter gemäß § 11 Brandenburgisches Datenschutzgesetz (BbgDSG) die Einhaltung datenschutzrechtlicher Standards durch technisch-organisatorische Maßnahmen sicherstellen.

- Verlagerung des Dialogs auf datenschutzgerechte Kommunikationskanäle

  Für den Dialog mit den Betroffenen sind ausschließlich datenschutzgerechte Mechanismen zu nutzen. Es sollte insbesondere keine Diskussion zu konkreten Fällen mithilfe der Kommentarfunktion geführt werden; Betroffene dürfen keinesfalls dazu aufgefordert oder ermuntert werden, in Kommentaren personenbeziehbare Einzelfälle zu schildern, Anfragen sollten so schnell wie möglich in „ordnungsgemäße Kanäle“ umgeleitet

werden. Auch Auskünfte unter Einschluss personenbezogener Daten verbieten sich in sozialen Netzwerken.

Eine stetige Moderation der Kommentare ist erforderlich, um solche, in denen personenbeziehbare Einzelfälle behandelt werden, nach Umleitung auf andere Kanäle zu löschen. Dasselbe gilt selbstverständlich für rechtlich problematische Fälle, wie etwa das Posten fremder personenbezogener Daten durch Nutzer (sog. doxing) oder solcher Inhalte, die in anderer Weise das Persönlichkeitsrecht von Betroffenen berühren.

- Kein Zwang zum Besuch sozialer Netzwerke durch exklusive Inhalte

  Für den Erhalt von Informationen dürfen Betroffene nicht auf die Nutzung sozialer Medien, die sie in ihrem Recht auf informationelle Selbstbestimmung gefährden, angewiesen sein. Alle Informationsinhalte müssen auch auf der Behördenwebseite veröffentlicht werden. Darüber hinaus empfehlen wir, die bei dem sozialen Netzwerk abgelegten Inhalte auf das erforderliche Minimum zu reduzieren. Insbesondere sollte dort ein Link auf die Behördenwebseite vorhanden sein.

- Information der Nutzer, Datenschutzhinweis, Impressum

  Es empfiehlt sich der deutliche Hinweis seitens der öffentlichen Stelle, dass der Betreiber des sozialen Netzwerks möglicherweise personenbezogene Daten des Betroffenen zu Geschäfts- oder Werbezwecken erhebt, verarbeitet und nutzt. Für nähere Informationen kann auf die Datenschutzerklärung des jeweiligen Netzwerks verwiesen werden. Alle Angebote in sozialen Netzwerken müssen klar erkennen lassen, welche öffentliche Stelle für die Fanpage verantwortlich ist. Eine Nennung des Behördennamens mit Verlinkung auf die Anbieterkennzeichnung der Behördenwebseite ist insoweit ausreichend.

- Förderung datenschutzfreundlicher Hostinglösungen

  Inhalte sollten vorzugsweise in einer Umgebung vorgehalten werden, in der die Standards der Datenschutzrichtlinie und des nationalen Rechts jederzeit durchsetzbar sind. Dies betrifft sowohl die Nutzung datenschutzfreundlicher sozialer Netzwerke in der Europäischen Union oder in Staaten, für die die Europäische Kommission ein vergleichbares Datenschutzniveau festgestellt hat, als auch das lokale oder auf Grundlage eines Auftragsdatenverarbeitungsvertrags nach § 11 BbgDSG rechtmäßig an Dritte übertragene Hosting.

- Prüfung der Rechtsgrundlagen für die Verarbeitung personenbezogener Daten

  Personenbezogene Daten dürfen von öffentlichen Stellen nur durch oder aufgrund eines Gesetzes verarbeitet werden. Dies gilt auch für den Betrieb von Fanpages. Werden trotz des Vorstehenden dennoch personenbezogene Daten veröffentlicht, muss hierfür im Einzelfall eine Rechtsgrundlage vorliegen (in der Regel gemäß § 16 BbgDSG, ggf. in Verbindung mit spezielleren Rechtsnormen). Soweit Bilder verwendet werden, ist in der Regel eine Einwilligung gemäß § 22 S. 1 des Kunsturhebergesetzes bzw. § 4 Abs. 1 Nr. 1 in Verbindung mit Abs. 2 und 3 BbgDSG erforderlich. Dies gilt im Übrigen unabhängig von dem Ausgang des vorgenannten Gerichtsverfahrens über die Mitverantwortung von Fanpagebetreibern an den Verarbeitungstätigkeiten von Facebook.

Es sei ausdrücklich angemerkt, dass dieser Katalog nicht als Empfehlung zum Betrieb einer Fanpage verstanden werden soll. Wir gehen vielmehr davon aus, dass öffentliche Stellen, die an Recht und Gesetz gebunden sind, keinesfalls solche Anbieter zur Verarbeitung eigener oder fremder Daten nutzen sollten, die sich – offen oder versteckt – weigern, die hiesigen Datenschutzvorschriften anzuerkennen. Die Landesbeauftragte setzt sich insoweit nachdrücklich für die Nutzung gesetzeskonformer Lösungen bei der Selbstdarstellung öffentlicher Stellen ein und berät interessierte Stellen gerne.

Wurden die vorstehenden Kriterien eingehalten, hat die Landesbeauftragte bisher in keinem Fall den Betrieb einer Fanpage gemäß § 25 BbgDSG beanstandet. Je nach dem, wie die Entscheidung des Europäischen Gerichtshofs und des Bundesverwaltungsgerichts ausfällt, bleibt dies jedoch ausdrücklich vorbehalten. Die Datenschutz-Grundverordnung bringt den Aufsichtsbehörden zudem neue Befugnisse zur Einschränkung der Datenverarbeitung, von denen die Landesbeauftragte entsprechend der neuen Rechtslage Gebrauch machen wird. Die öffentlichen Stellen im Land bleiben aufgerufen, ihre Pläne zur Präsenz auf sozialen Medien genau zu prüfen und im Zweifel in Absprache mit dem behördlichen Datenschutzbeauftragten Änderungen vorzunehmen.

Betreiber von Seiten in sozialen Netzwerken agieren nicht im rechtlichen Vakuum, sondern sind für große Teile der Datenverarbeitungsmaßnahmen, die durch ihre Tätigkeit ausgelöst werden, verantwortlich. Im öffentlichen Bereich unterliegt eine Nutzung der sozialen Medien besonderen Beschränkungen, die eine Prüfung des Konzepts und der veröffentlichten Inhalte im Einzelfall erforderlich machen. Die Landesbeauftragte setzt sich für datenschutzrechtskonforme Lösungen ein und berät öffentlichen Stellen bei der Einrichtung solcher Lösungen.

15.4 Klarnamenpflicht beim Bezug eines Newsletters

Im Februar 2016 wurde beim Ministerium der Justiz und für Europa und Verbraucherschutz ein Newsletter zum Bezug von Informationen über neue Gesetze und Verordnungen eingerichtet – zweifellos eine gute Sache. Allerdings wurden bei der Anmeldung Daten abgefragt, die weder zum Versand des Newsletters erforderlich waren noch überhaupt genutzt werden sollten.

Der genannte Dienst ging zum 1. Februar 2016 online. Bereits am 2. Februar lag der Landesbeauftragten die Beschwerde eines Betroffenen vor, der sich am Bezug des Newsletters vorläufig gehindert sah, weil bei der Anmeldung in einem Webformular seinen Namen eingeben musste. Er rügte einen Verstoß gegen das Telemediengesetz (TMG) und das sog. Gebot der Datensparsamkeit. Die Landesbeauftragte prüfte dieses Formular ebenso wie ein weiteres, das auf der gleichen Vorlage beruhte und zum Bezug eines Newsletters zum Thema Elektronischer Rechtsverkehr diente. Sie stellte Folgendes fest:

Zum Bezug des Newsletters war die Anlage eines Nutzerkontos erforderlich. Dazu mussten personenbezogene Daten hinterlegt werden, um eine Wiedererkennung zu ermöglichen. Dies sollte bestimmte Einstellungen zum Abonnement des Newsletters ermöglichen und war datenschutzrechtlich letztlich unproblematisch. Zur Anlage des Nutzerkontos waren allerdings neben der E-Mail-Adresse und der Festlegung eines Passworts der Vor- und Nachname anzugeben. Waren die entsprechenden Felder nicht ausgefüllt, ließ sich das Abonnement nicht einrichten.

Da jede Datenerhebung durch öffentliche Stellen einen Eingriff in das Grundrecht der Betroffenen auf Datenschutz darstellt, muss dieser in jedem Fall verhältnismäßig sein. Die öffentliche Stelle darf insbesondere nur diejenigen Daten erheben, die zur Erfüllung ihrer jeweiligen Aufgabe erforderlich sind. Für Telemedien wie den Newsletter gilt zudem § 14 TMG, nach dem Anbieter von Telemedien personenbezogene Daten eines Nutzers (hier sog. Bestandsdaten) nur erheben und verwenden dürfen, soweit diese für die Begründung, inhaltliche Ausgestaltung oder Änderung eines Vertragsverhältnisses über die Nutzung von Telemedien erforderlich sind.

Welche Daten waren nun für die Bereitstellung des Newsletters erforderlich? Die Landesbeauftragte sah es zunächst als nachvollziehbar und datenschutzrechtlich nicht problematisch an, dass der Bezug des Newsletters überhaupt die Anlegung eines Accounts erforderte. Die zusätzlich angebotenen Einstellungen zur Verwaltung des Abonnements, die anders schwerlich hätten realisiert werden können, boten insoweit eine ausreichende Begründung. An die E-Mail-Adresse sollte der Newsletter gesandt werden; sie war schon deswegen ein erforderliches Datum. Aus technisch-organisatorischen Grün-

den (§ 10 Brandenburgisches Datenschutzgesetz) war auch die Speicherung eines Passworts zusätzlich zum Benutzernamen erforderlich – dies diente gleichzeitig der Umsetzung der gesetzlichen Forderung in § 13 Abs. 4 Nr. 3 TMG, dass die Nutzung von Telemedien unter Ausschluss der Kenntnisnahme durch Dritte ermöglicht werden muss. Welchen Zweck die Erhebung von Vor- und Nachnamen dienen sollte, war dagegen nicht ersichtlich, da der Newsletter ohne Weiteres ausschließlich aufgrund der Angabe einer validen E-Mail-Adresse bereitgestellt werden konnte.

Das Ministerium räumte ein, dass es sich um ein bloßes Problem des Formulardesigns handele. Die über das Formular erhobenen Namen seien nicht auf Plausibilität geprüft worden. Die Formulare wurden in der Folge so geändert, dass zwar die Eingabefelder „Vorname“ und „Nachname“ aus technischen Gründen bestehen blieben, die Nutzer aber im Begleittext informiert wurden, dass die Eingabe ihres tatsächlichen Namens nicht erforderlich sei und beliebige Eintragungen vorgenommen werden könnten. Die Landesbeauftragte stimmte der Lösung zu, da das Formulardesign in naher Zukunft überarbeitet und datenschutzgerecht ausgestaltet wird. Sie wies jedoch darauf hin, dass eingegebene Namen anschließend mangels Erforderlichkeit zu löschen sind. Seitdem ist für Nutzer eindeutig erkennbar, dass der Bezug beider Newsletter ohne Namensnennung möglich ist.

Anbieter von Webservices – gleich, ob öffentliche oder nicht öffentliche Stellen – müssen bei der Bereitstellung jeglicher Online-Dienstleistung beachten, dass Daten von Nutzern grundsätzlich nur erhoben werden dürfen, wenn dies zur Durchführung der aus dem Anbieter-Nutzer-Verhältnis folgenden Aufgaben erforderlich ist. Die zweckfreie Erhebung von Daten „auf Halde“ ohne konkrete Weiterverarbeitungsabsicht verbietet sich in jedem Fall.

15.5 Prüfung der Webseiten von Hotels und Pensionen auf Verschlüsselung

Viele Hotels und Pensionen bieten auf ihren Internetseiten Kontakt- oder Buchungsformulare an. Bei Nutzung der Formulare durch Kunden werden personenbezogene Daten wie Name, Anschrift und Reisezeiträume über das Internet übertragen. Wir haben bei ausgewählten Webseiten die Verschlüsselung der Formulardaten während des Transports überprüft.

Hotels und Pensionen, die Webseiten im Internet bereitstellen, gelten nach dem Telemediengesetz (TMG) als geschäftsmäßige Diensteanbieter und sind daher verpflichtet, durch technische und organisatorische Vorkehrungen sicherzustellen, dass die von ihnen angebotenen Webseiten und Übertragungen von Formulardaten gegen Verletzungen des Schutzes personenbezoge-

ner Daten gesichert sind. Entsprechende Maßnahmen müssen den Stand der Technik berücksichtigen. Eine Maßnahme, die diesen Vorgaben entspricht, ist insbesondere die Anwendung eines als sicher anerkannten Verschlüsselungsverfahrens.

Wir haben eine Stichprobe von ca. 170 Webseiten ausgewählter Hotels und Pensionen im Land auf ihre Verschlüsselungsfähigkeiten hin geprüft. Als Stand der Technik gilt hier die Anwendung des Protokolls TLS (Transport Layer Security). 130 Webseiten aus der Stichprobe binden Kontakt- oder Buchungsformulare ein. Davon senden 104 Webseiten – das sind 80 Prozent – die Formulardaten völlig unverschlüsselt, also im Klartext lesbar, über das Internet. 26 Webseiten bzw. 20 Prozent verschlüsseln die Übertragung der Formulardaten. Jedoch hat eine nähere Untersuchung ergeben, dass bei acht dieser Webseiten verschiedene Sicherheitsprobleme bei der Verschlüsselung auftreten, die sie für Angriffe anfällig machen, z. B. weil veraltete Verschlüsselungsalgorithmen bevorzugt oder schwache Schlüsselaustauschparameter verwendet werden. Insofern wird die Vorgabe des Telemediengesetzes, ein Verschlüsselungsverfahren zu verwenden, zwar erfüllt, jedoch ist es in den genannten Fällen nicht sicher genug. Auch für die verantwortlichen Stellen, die überhaupt keine Transportverschlüsselung anbieten, ist es unabdingbar, ihre Datenübertragung an den Stand der Technik anzupassen. Wir werden uns für eine entsprechende Umsetzung der erforderlichen technischen Maßnahmen bei dem Deutschen Hotel- und Gaststättenverband Brandenburg einsetzen.

Werden personenbezogene Daten durch geschäftsmäßige Telemedienanbieter über das Internet übertragen, muss eine dem Stand der Technik entsprechende Verschlüsselung eingesetzt werden, um Datenschutzverletzungen zu verhindern.

15.6 Die Tücken des E-Mail-Verkehrs

15.6.1 Versand eines Vereinsberichts an die Mitglieder per E-Mail

Der Vorsitzende eines Vereins versandte den Vereinsbericht per E-Mail an die aktiven und zum Teil auch ausgeschiedenen Vereinsmitglieder. Durch die Verwendung des CC-Feldes (Carbon Copy) waren für alle Empfänger die Namen und dazugehörigen E-Mail-Adressen der anderen Empfänger sichtbar.

Nicht nur die ausgeschiedenen sondern auch die aktiven Mitglieder eines Vereins sind im Verhältnis zum Verein Dritte im Sinne des Bundesdatenschutzgesetzes (BDSG). Die durch die Verwendung CC-Feldes bei der Adressierung erfolgte Weitergabe von Namen und E-Mail-Adressen an alle

aktiven und ehemaligen Vereinsmitglieder stellt damit eine Übermittlung personenbezogener Daten an Dritte dar. Gemäß § 4 Abs. 1 BDSG ist jedoch das Erheben, Verarbeiten (wozu auch das Übermitteln zählt) und Nutzen personenbezogener Daten nur zulässig, soweit dieses Gesetz oder eine andere Rechtsvorschrift dies erlaubt oder anordnet oder der Betroffene eingewilligt hat.

Der Vereinsvorstand versicherte uns, dass es sich bei dem Versenden der E-Mail mit der Adressfeldoption CC um eine einmalige und unbeabsichtigte Ausnahme gehandelt habe. Sämtlicher E-Mail-Verkehr zwischen dem Vorstand und den Vereinsmitgliedern werde normalerweise ausschließlich über eine Adressierung per BCC-Feld (Blind Carbon Copy) ausgeführt.

Ergänzend wirkten wir mit Nachdruck darauf hin, dass die personenbezogenen Daten der ausgeschiedenen Vereinsmitglieder gemäß § 35 Abs. 2 BDSG zu löschen sind, sobald ihre Kenntnis für die Erfüllung des Zwecks der Speicherung nicht mehr erforderlich ist. Alternativ können diese Daten auch gesperrt werden, also so gekennzeichnet werden, dass ihre weitere Verarbeitung oder Nutzung eingeschränkt ist, wenn einer Löschung gesetzliche, satzungsmäßige oder vertragliche Aufbewahrungsfristen entgegenstehen.

Die Angabe der Adressaten einer E-Mail im CC-Feld des Nachrichtenkopfes führt zu einer Datenübermittlung an Dritte. Durch die Nutzung der Option BCC lässt sich diese Übermittlung von vornherein vermeiden.

15.6.2 E-Mail-Adressen im Kundenverteiler

Ein selbstständiger Handelsvertreter nutzte die E-Mail-Adressen seiner Kunden, um auf einen vermeintlichen Verbraucherskandal aufmerksam zu machen. Zahlreiche Stromabrechnungen seien infolge einer fehlerhaft berechneten Umlage nach dem Erneuerbare-Energien-Gesetz (EEG-Umlage) falsch und damit nachteilig für die Verbraucher. Der Verantwortliche verschickte die entsprechende E-Mail an sich selbst und setzte die Adressen seiner sämtlichen Kunden ins CC-Feld.

Durch die Nutzung des CC-Adressfeldes wurden insgesamt 243 E-Mail-Adressen allen Adressaten übermittelt und zur Kenntnis gebracht. Eine Übermittlung personenbezogener Daten – und um solche handelt es sich grundsätzlich bei E-Mail Adressen – ist jedoch wiederum nur zulässig, soweit das Gesetz dies erlaubt oder die Betroffenen eingewilligt haben. Eine wirksame Einwilligung lag allerdings nicht vor und auch auf eine gesetzliche Grundlage konnte die Übermittlung nicht gestützt werden. Für die Durchführung der jeweils mit den Kunden abgeschlossenen Verträge war eine solche jedenfalls nicht erforderlich und es bestand auch kein berechtigtes Interesse

des Handelsvertreters an einer derartigen Verarbeitung personenbezogener Daten.

Wir wiesen den Handelsvertreter darauf hin, dass die gewählte Versandart nicht im Einklang mit datenschutzrechtlichen Bestimmungen steht und sich eine rechtswidrige Verarbeitung als Ordnungswidrigkeit darstellt, die mit Bußgeld geahndet werden kann. Uns wurde versichert, dass es sich in diesem Fall um einen bedauerlichen Fehler gehandelt habe und sonst keine Übermittlung von Adressen stattfinde. Man werde jedoch zukünftig ganz auf derartige „Newsletter“ verzichten.

Die Offenbarung von E-Mail-Adressen eines Kundenverteilers an alle Kunden stellt eine Datenverarbeitung dar, die der Einwilligung der Betroffenen oder einer Rechtsgrundlage bedarf. Ein berechtigtes Interesse an einer solchen Datenübermittlung kann grundsätzlich nicht angenommen werden.

15.6.3 Übersendung von Listen mit Übernachtungsgästen durch Hotelbetreiber per E-Mail an eine Gemeinde

Eine Stadt forderte die ansässigen Hotelbetreiber auf, ihr für Kontrollzwecke per E-Mail Listen der Gäste zu übersenden, soweit deren Aufenthalt beruflich veranlasst war und deshalb keine Übernachtungssteuer anfiel.

Aus datenschutzrechtlicher Sicht haben die Hotelbetreiber als steuerpflichtige (natürliche oder juristische) Personen bei der Übermittlung § 9 i. V. m. Nr. 4 der Anlage zum Bundesdatenschutzgesetz (BDSG) einzuhalten. Hierin wird bestimmt, dass dem jeweiligen Schutzzweck angemessene technisch-organisatorische Maßnahmen zu ergreifen sind, um zu verhindern, dass personenbezogene Daten während des Transports von Unbefugten eingesehen werden können (sog. Weitergabekontrolle). Da die Gästelisten personenbezogene Daten enthalten, ist ihre Übermittlung per E-Mail nur zulässig, wenn allen Steuerpflichtigen die erforderliche Verschlüsselung möglich und zumutbar sowie deren Beachtung wirksam sichergestellt ist.

Da unverschlüsselte E-Mails auch im geschäftlichen Verkehr den Regelfall darstellen, hätte die Stadt aus unserer Sicht auf die erforderliche Weitergabekontrolle gesondert hinweisen müssen. Sie versicherte uns, dass sie auf die Übersendung von Gästelisten per E-Mail künftig verzichten und einen sicheren Transportweg (insbesondere per Post) vereinbaren werde.

Wer personenbezogene Daten übermittelt, hat bei der Wahl des Übermittlungswegs die erforderlichen technisch-organisatorischen Maßnahmen zu ergreifen, um zu verhindern, dass die Daten während des Transports von Unbefugten eingesehen werden können. Bei dem Versenden von Daten per E-Mail kann hierfür eine Transportverschlüsselung erforderlich sein.

16 Umwelt

Vor-Ort-Begehung durch eine Behörde, und jeder darf mit!

Bei einem Vor-Ort-Termin zur Kontrolle der Einhaltung naturschutzrechtlicher Vorschriften waren nicht nur der zu Kontrollierende und Vertreter der Behörde, sondern auch noch ein Ornithologe und zwei Jäger anwesend.

Aufgrund des Verdachts eines Verstoßes gegen naturschutzrechtliche Vorschriften vereinbarte die überwachende Behörde einen Vor-Ort-Termin auf der betroffenen landwirtschaftlich genutzten Fläche mit dem vermutlichen Verursacher. Ein Ornithologe, der Auskünfte zur ökologischen Wertigkeit der Fläche beibringen sollte, wurde ebenfalls über den Termin informiert, jedoch nicht ausdrücklich eingeladen. Er begleitete die Begehung vor Ort auf eigene Initiative. Am Tag des Termins hielten sich zufällig auch noch ein Jäger und dessen Frau auf der entsprechenden Fläche auf. Sie wurden auf die Gruppe aufmerksam und stießen zu der Vor-Ort-Kontrolle hinzu.

Durch die Teilnahme unbeteiligter Dritter an dem Vor-Ort-Termin wurden diesen der Name des Betroffenen und seine Stellung als mutmaßlicher Verursacher eines naturschutzrechtlichen Verstoßes offenbart. Die spezialgesetzliche Ermächtigungsnorm für eine Datenübermittlung nach § 38 Brandenburgisches Naturschutzausführungsgesetz war im vorliegenden Fall nicht einschlägig, sodass auf die allgemeinen Vorschriften des Brandenburgischen Datenschutzgesetzes (BbgDSG) zurückzugreifen war.

Bei der Übermittlung personenbezogener Daten an den Ornithologen, den Jäger und seine Frau handelte es sich um eine Datenübermittlung an Personen außerhalb des öffentlichen Bereichs. Sie ist gemäß § 16 BbgDSG nur zulässig, wenn die Übermittlung zur rechtmäßigen Erfüllung der in der Zuständigkeit der übermittelnden Stelle liegenden Aufgaben erforderlich ist und die zusätzlichen Voraussetzungen des § 13 Abs. 1 BbgDSG vorliegen.

Die Datenübermittlung an die genannten Personen war zur rechtmäßigen Aufgabenerfüllung durch die Behörde nicht erforderlich. Die Aufgabe des Ornithologen war es, Informationen zur ökologischen Wertigkeit der Fläche beizubringen. Hierzu benötigte er keine personenbezogenen Daten des Nutzers der landwirtschaftlichen Fläche. Auch seine Teilnahme an der behördlichen Begehung war nicht erforderlich und somit datenschutzrechtlich unzulässig.

Gleiches galt für den Jäger und seine Frau. Auch diese waren nicht zum Termin geladen, sondern befanden sich aus eigener Initiative vor Ort. Die Behörde hätte dafür Sorge tragen müssen, dass auch sie bei der Begehung keine Kenntnis von personenbezogenen Daten erlangen.

Sind nichtgeladene Personen bei Vor-Ort-Terminen anwesend, muss sichergestellt sein, dass diese keine Kenntnis von personenbezogenen Daten erlangen können.

17 Videoüberwachung

17.1 Auf gute Nachbarschaft!

Spätestens wenn der Nachbar eine Überwachungskamera installiert und diese auch auf ein fremdes Grundstück, den Gehweg oder die Straße richtet, hört der Spaß auf. Wer möchte schon gerne beim Sonnenbad im eigenen Garten oder beim Spazierengehen ständig durch Überwachungskameras beobachtet oder gar aufgezeichnet und damit einem permanenten Überwachungsdruck ausgesetzt werden? Nachbarn und Anwohner fühlen sich dann häufig in ihrem Grundrecht auf informationelle Selbstbestimmung verletzt und fragen sich, ob die Videoüberwachung zulässig ist.

Grundsätzlich ist eine auf andere Personen gerichtete Videoüberwachung durch nicht öffentliche Stellen – und damit auch durch Privatpersonen – nur zulässig, wenn sie auf eine Erlaubnisnorm gestützt werden kann. Erstreckt sich eine Videoüberwachung auf öffentlich zugängliche Bereiche wie z. B. Wege und Straßen, müssen immer die strengen Voraussetzungen des § 6b Abs. 1 Nr. 2 oder Nr. 3 Bundesdatenschutzgesetz erfüllt sein. Danach ist die Videoüberwachung zulässig, wenn sie zur Wahrnehmung des Hausrechts oder berechtigter Interessen für konkret festgelegte Zwecke erforderlich ist und keine Anhaltspunkte dafür bestehen, dass schutzwürdige Interessen der Betroffenen überwiegen. Diese Voraussetzungen sind in Nachbarschaftsangelegenheiten jedoch selten erfüllt. Dies bedeutet regelmäßig, dass die

Überwachung des eigenen, erkennbar abgegrenzten Grundstücks datenschutzrechtlich zulässig sein kann, nicht aber eine Videoüberwachung angrenzender Straßen, Plätze oder Gehwege. In Einzelfällen sind Ausnahmen möglich.

Besteht der Verdacht, dass das eigene Grundstück durch eine andere Person videoüberwacht wird, bietet sich neben einer unmittelbaren Klärung mit dieser Person eine Klärung durch das zuständige Zivilgericht an. Das von einer (vermuteten) Videoüberwachung beeinträchtigte allgemeine Persönlichkeitsrecht findet seine rechtliche Ausprägung in verschiedenen Rechtsgebieten – neben dem Bundesdatenschutzgesetz etwa in §§ 823, 1004 Bürgerliches Gesetzbuch (Schadensersatzpflicht, Beseitigungs- und Unterlassungsanspruch), §§ 22, 23, 33 Kunsturheberrechtsgesetz (Recht am eigenen Bild) und §§ 201, 201a Strafgesetzbuch (Verletzung der Privatsphäre durch Bild- und Tonaufnahmen). Ein zivilgerichtliches Vorgehen kann sogar dann erfolgreich sein, wenn es sich um eine Kameraattrappe handelt.

Bei sogenannten Dome-Kameras kann aufgrund der Bauart der tatsächliche Erfassungsbereich von Außenstehenden nicht nachvollzogen werden. Daher empfehlen wir selbst bei einer zulässigen Videoüberwachung, auf den Einsatz solcher Kameras gänzlich zu verzichten.

Um Beschwerden von Nachbarn und Anwohnern zu vermeiden, empfehlen wir, den Erfassungsbereich von Geräten zur Videoüberwachung auf das eigene, familiär genutzte und erkennbar abgegrenzte Grundstück zu beschränken und die unmittelbaren Nachbarn über den Erfassungsbereich zu informieren.

17.2 Wetterbeobachtung wird zur dauerhaften Videoüberwachung

Durch einen Hinweis der örtlichen Polizeidienststelle wurden wir auf den Betrieb einer Wetter-Webcam aufmerksam, deren Bilder im Internet abrufbar waren. Auf der Internetseite konnten nahezu in Echtzeit ein anliegendes Wohngebiet mit Straßen, Gehwegen und Nachbargrundstücken sowie alle sich dort aufhaltenden Personen beobachtet werden.

Der private Webcam-Betreiber berief sich zunächst darauf, dass der Anwendungsbereich des Bundesdatenschutzgesetzes gar nicht eröffnet sei, da die Erhebung und Verarbeitung der Bilder der Webcam ausschließlich für persönliche Zwecke erfolge. Dies traf jedoch nicht zu, denn die Webcam übermittelte personenbezogene Daten über das Internet weltweit an einen unbegrenzten Empfängerkreis. Anwohner, Passanten und Verkehrsteilnehmer hatten keine Möglichkeit, sich einer solchen Dauerbeobachtung zu entziehen.

Durch die Echtzeitübertragung konnte beobachtet werden, wer wann sein Haus verließ, sein Auto bewegte oder einen Spaziergang machte. Diese unzulässige, permanente Videobildübertragung, von der zahlreiche Personen betroffen waren, stellte einen besonders intensiven Eingriff in das allgemeine Persönlichkeitsrecht der Betroffenen dar und verstieß gegen das Bundesdatenschutzgesetz. Daher forderten wir den Betreiber auf, die Webcam so einzustellen, dass keine personenbezogenen Daten erhoben und übertragen werden. Ein datenschutzkonformer Betrieb der Webcam hätte sich z. B. durch die Änderung des Erfassungsbereiches der Kamera oder das Verpixeln der nahen Bereiche des Wohngebietes erreichen lassen.

Aufgrund der Weigerung des Webcam-Betreibers diese Aufforderung umzusetzen, erließen wir eine Anordnung gemäß § 38 Abs. 5 Bundesdatenschutzgesetz, die ihm aufgab, den Erfassungsbereich der Kamera so einzustellen, dass nahe Bereiche des Wohngebietes und die dort befindlichen Personen nicht oder jedenfalls nicht erkennbar erfasst werden. Der Webcam-Betreiber kam jedoch auch der Anordnung nicht nach. Zu deren Durchsetzung haben wir ein Vollstreckungsverfahren eingeleitet, um den Kamerabetreiber mithilfe eines Zwangsgeldes zu einem rechtskonformen Handeln zu bewegen.

Wer Bilder einer privaten Webcam ins Internet überträgt, muss die Vorschriften des Bundesdatenschutzgesetzes einhalten. Die Erhebung und Übermittlung personenbezogener Daten mit einer Webcam kann nicht auf die Annahme persönlicher oder familiärer Tätigkeiten gestützt werden, da weltweit jeder auf die Bilder zugreifen kann.

17.3 Videoüberwachung zum Schutz vor „Eventualitäten“

Ein Unternehmer hatte in seinen Büroräumen sowie auf dem angrenzenden Parkplatz Videokameras installiert. Auf die aufgenommen Bilder griff er nach Belieben mithilfe einer auf seinem geschäftlichen Mobiltelefon installierten App zu.

Im Rahmen unserer Vor-Ort-Prüfung stellten wir fest, dass der Geschäftsführer zwei aktive Kameras für die Videoüberwachung nutzte. Eine Kamera war auf den Außenbereich gerichtet und erfasste den an die Geschäftsräume angrenzenden Parkplatz. Eine weitere Kamera erfasste weitläufig den Geschäftsraum, zu dem auch Kunden Zugang haben. Die Videobeobachtung durch die beiden Kameras erfolgte in Echtzeit, wofür der Geschäftsführer eine App auf seinem Mobiltelefon nutzte. Die App umfasste auch die Funktionalität, Videobilder auf Knopfdruck zu speichern.

Grundsätzlich ist eine Videoüberwachung durch nicht öffentliche Stellen, von der andere Personen betroffen sind, nach § 4 Abs. 1 Bundesdatenschutzge-

setz (BDSG) nur zulässig, wenn alle Betroffenen eingewilligt haben oder die Überwachung auf eine Erlaubnisnorm gestützt werden kann. Eine solche Norm für die Überwachung öffentlich zugänglicher Räume ist § 6b BDSG. Nach Abs. 1 Nr. 2 oder Nr. 3 dieser Vorschrift ist die Videoüberwachung durch nicht öffentliche Stellen nur zulässig, wenn sie zur Wahrnehmung des Hausrechts oder zur Wahrnehmung berechtigter Interessen für konkret festgelegte Zwecke erforderlich ist und keine Anhaltspunkte dafür bestehen, dass schutzwürdige Interessen der Betroffenen überwiegen.

Als Zwecke nannte der Betreiber der Kameras u. a. den Schutz vor Straftaten. Außerdem diene ihm die Videoüberwachung für „Eventualitäten“. Insbesondere für die Mitarbeiter stand dem Überwachungsinteresse des Betreibers eine unerträgliche Situation gegenüber. Denn die Beschäftigten konnten nicht erkennen, wann eine Überwachung stattfindet. Durch die permanente Möglichkeit des Zugriffs auf die Bilder der Videokameras entstand ein dauerhafter Überwachungsdruck, dem sich die Mitarbeiter nicht entziehen konnten. Da sich der Betreiber zur Begründung des von ihm mit der Videoüberwachung verfolgten Zwecks auf keinerlei konkrete Anlässe in der Vergangenheit berufen konnte, überwogen die Interessen der Mitarbeiter deutlich. Aber auch die Interessen sonstiger anlasslos erfasster Personen, wie Kunden und Parkplatznutzer, fielen stärker ins Gewicht als seine Überwachungsinteressen.

Wir erörterten mit dem Betreiber umfassend die gesetzlichen Voraussetzungen einer Videoüberwachung. Aufgrund unserer datenschutzrechtlichen Bedenken gegen die Zulässigkeit nahm er vom weiteren Betrieb der Kameras Abstand und baute sie ab.

Die auf eine gesetzliche Erlaubnisnorm gestützte Videoüberwachung ist nur zulässig, wenn schutzwürdige Interessen Betroffener nicht entgegenstehen. Hierfür bedarf es einer umfassenden Interessenabwägung. Um von der Unzulässigkeit auszugehen, genügt es bereits, wenn Anhaltspunkte für ein Überwiegen der Betroffeneninteressen nicht ausgeräumt werden können.

17.4 Schöner Wohnen – für alle sichtbar

Durch die Beschwerde eines Bürgers wurden wir auf eine Webcam aufmerksam, die ein Bahnhofsgebäude in einer größeren Stadt und dessen Vorplatz mit allen sich dort befindenden Verkehrsteilnehmern und Passanten erfasste sowie ins Internet übertrug. Im Laufe des Verfahrens stellte sich heraus, dass die für die Videoüberwachung verantwortliche Stelle – eine Wohnungsbaugesellschaft – noch zwei weitere Webcams zu Werbezwecken betrieb. Diese erfassten zwei sanierte Wohngebiete, teilweise mit Grünanlagen. Die Livebilder sollten als Aushängeschild für die Wohnungsbaugesellschaft dienen.

Der Betreiber der Webcams vertrat die Auffassung, dass der Betrieb datenschutzgerecht sei, da die gezeigten Bilder von sehr weit oben, mit geringer Auflösung aufgenommen und nur alle 14 Sekunden aktualisiert würden. Um eine Erhebung personenbezogener Daten handelt es sich aber auch, wenn Gesichter, individuelle Körpermerkmale, Bewegungsabfolgen einzelner Personen oder personenbezogene Sachumstände erfasst werden und dadurch Rückschlüsse auf Personen gezogen werden können. Bei allen drei Webcams wurden solche personenbezogene Daten im öffentlich zugänglichen Raum erhoben, sodass die Zulässigkeit der Webcams anhand des § 6b Abs. 1 Bundesdatenschutzgesetz (BDSG) zu prüfen war. Der benannte Werbezweck stellte kein berechtigtes Interesse im Sinne des § 6b Abs. 1 Nr. 3 BDSG dar. Für den Zweck der Werbung bedarf es keiner Videoüberwachung über das Internet. Fotos der beworbenen Orte sind vollkommen ausreichend. Zudem standen die überwiegenden Interessen der Passanten und Anwohner dem Werbeinteresse der Gesellschaft gegenüber. Die großflächige und dauerhafte Beobachtung der betroffenen Bereiche stellten einen erheblichen Eingriff in das allgemeine Persönlichkeitsrecht einer Vielzahl betroffener Personen dar.

Datenschutzrechtlich unbedenklich sind Webcams nur, wenn keine personenbezogenen Daten erhoben und übertragen werden. Dies kann durch eine gezielte Auswahl und gute Kombination des konkreten Erfassungsbereichs, eine möglichst weite Entfernung der Kamera, eine herabgesetzte Bildqualität und die Einstellung kontextbezogener Zeitintervalle der Bildaktualisierung beeinflusst werden. Im konkret zu untersuchenden Fall reichten die entsprechenden Maßnahmen des Kamerabetreibers hierzu nicht aus.

Die drei Webcams der Wohnungsbaugesellschaft hätten nach den genannten Kriterien, gegebenenfalls auch durch Verpixeln einiger Bereiche, datenschutzgerecht eingestellt werden können. Die Gesellschaft entschied sich jedoch aus eigenem Bestreben für ihre Abschaltung.

Werden personenbezogene Daten zu Werbezwecken durch eine Webcam erhoben und übertragen, liegt darin kein berechtigtes Interesse im Sinne des § 6b Abs. 1 Nr. 3 BDSG. Webcams sind in der Regel nur dann datenschutzrechtlich unbedenklich, wenn keine personenbezogenen Daten erhoben und übertragen werden.

17.5 Aufruf zur Videoüberwachung von Wahlplakaten

Wahlkampf erfolgt zum Teil auch mit unfairen Mitteln. Um Wahlplakate vor Vandalismus zu schützen, rief ein Politiker Bürger dazu auf, diese mit Videokameras zu überwachen. Sogar ein Taschengeld wurde den Freiwilligen für ihre Dienste in Aussicht gestellt.

Die Videoüberwachung von Wahlplakaten im öffentlich zugänglichen Raum ist gemäß § 6b Bundesdatenschutzgesetz nur zulässig, wenn sie zur Wahrnehmung berechtigter Interessen für konkret festgelegte Zwecke erforderlich ist und keine Anhaltspunkte bestehen, dass schutzwürdige Interessen Betroffener überwiegen.

Der Schutz der Plakate vor Vandalismus und damit der Schutz des Eigentums kann als berechtigtes Interesse nur von der jeweiligen Partei geltend gemacht werden, in deren Eigentum sich die Plakate befinden, nicht hingegen von Bürgern. Bei der erforderlichen Interessenabwägung überwiegen aber in aller Regel die schutzwürdigen Interessen der anlasslos erfassten Personen, womit eine entsprechende Videoüberwachung als datenschutzrechtlich unzulässig zu bewerten ist. Sollte im Einzelfall eine solche Plakatüberwachung zulässig sein, wären weitreichende technisch-organisatorische Maßnahmen erforderlich, die der Kamerabetreiber sicherzustellen hätte. Es war zu bezweifeln, dass dies in der beschriebenen Lage eine realistische Option darstellte.

Nach unserem Kenntnisstand wurde trotz des Aufrufs keine Kamera zur Überwachung von Wahlplakaten in Betrieb genommen. Bürgern ist auch dringend davon abzuraten, solchen Aufrufen nachzukommen. Wer das Vorhaben in die Tat umsetzt und damit gegen das Datenschutzgesetz verstößt, hat unter Umständen mit einem Bußgeldverfahren zu rechnen.

Ein Aufruf zur Überwachung von Wahlplakaten mittels Videokameras gegen Entlohnung liest sich wie schnell verdientes Geld. Die Umsetzung in die Tat kann jedoch zu einem Bußgeldverfahren führen. Aus datenschutzrechtlicher Sicht ist davon dringend abzuraten.

18 Wirtschaft und Versicherungen

18.1 eBay Kleinanzeigen – Niederlassungswechsel und erste Erfahrungen

Seit dem 1. Juli 2017 wird der Telemediendienst eBay Kleinanzeigen nicht mehr von den Niederlanden, sondern von Brandenburg aus betrieben. In den ersten Monaten nach Übernahme der datenschutzrechtlichen Aufsicht hatte die Landesbeauftragte zumeist Fragen zu Betroffenenrechten zu klären.

Solange die Internetplattform eBay Kleinanzeigen, zugehörig zum eBay-Konzern, von der Marktplaats B. V. in Amsterdam betrieben wurde, lag die

Aufsichtszuständigkeit bei den niederländischen Kollegen. Zum 1. Juli wechselte der Betrieb in die Verantwortung der neuen eBay Kleinanzeigen GmbH, die ihren Sitz in Brandenburg hat. Damit liegt die Aufsichtszuständigkeit nunmehr bei unserer Behörde. Für die Abwicklung des Übergangs bat die Landesbeauftragte die bisher zuständige niederländische Aufsichtsbehörde um Mitteilung offener Beschwerden – eine Bitte, der diese nachkam.

In der kurzen Zeit unserer Aufsichtstätigkeit hatten wir die Gelegenheit, anhand von Fällen das Funktionieren der Verfahren zur Durchsetzung der Betroffenenrechte auf Auskunft, Berichtigung und Löschung (§§ 34, 35 BDSG) zu prüfen. Wir setzten uns – wie bei anderen Unternehmen auch – für eine intensivere Schulung des Kundenservices, der für den Erstkontakt mit Beschwerdeführern zuständig ist, zu Datenschutzfragen im Allgemeinen und den Betroffenenrechte im Besonderen ein. Auch regten wir eine stärkere Einbeziehung des betrieblichen Datenschutzbeauftragten in das Beschwerdemanagement an.

Alle mit Datenverarbeitung befassten Unternehmen sind verpflichtet, ein effizientes System zur Bearbeitung von Auskunftsansprüchen (§ 34 BDSG), zur Berichtigung unrichtiger Daten (§ 35 Abs. 1 BDSG) und zur (ggf. auch abschlägigen) Bescheidung von Löschungsverlangen zumindest hinsichtlich selbst verantworteter Inhalte (§ 35 Abs. 2 ff. BDSG) einzurichten. Gerade bei Internetplattformen, bei denen ein Großteil der entstehenden Daten von Dritten erzeugt wird, bietet sich an, gleichzeitig auch eine mögliche Haftung für rechtswidrige nutzergenerierte Daten in den Blick zu nehmen.

Eine gewissenhafte Einhaltung der Rechtsvorschriften (Compliance) hilft auch, Bußgelder zu vermeiden, die bereits heute für eine nicht, nicht richtig, nicht vollständig oder nicht rechtzeitig erteilte Auskunft (§ 43 Abs. 1 Nr. 8a BDSG) verhängt werden können. Mit Inkrafttreten der Datenschutz-Grundverordnung werden Bußgelder auf weitere Tatbestände – etwa die unterlassene Löschung – ausgeweitet und der Höhe nach deutlich empfindlicher. Gleichzeitig hilft eine Verbesserung der datenschutzrechtlichen Qualität des Kundenservices, Vertrauen aufzubauen und zu erhalten und so die Kundenzufriedenheit zu verbessern. Insoweit kann ein vorbildlicher Datenschutz, nicht zuletzt in einer vertrauensabhängigen Branche wie dem eCommerce, durchaus einen Marktvorteil darstellen.

Für jedes Unternehmen in der Europäischen Union gilt: Die Einrichtung von effektiven Verfahren zur Erfüllung der elementaren Betroffenenrechte (insbesondere auf Auskunft, Berichtigung und Löschung) ist Pflicht und ein Grundbaustein der Compliance. Dazu gehört es unter anderem, die mit dem Erstkontakt im Beschwerdemanagement betrauten Mitarbeiter datenschutzrechtlich zu schulen. Sind keine funktionierenden Prozesse vorhanden, drohen Bußgelder und – vielleicht schlimmer – der Vertrauensverlust der Nutzer. Gute Prozesse dagegen stärken das Vertrauen und können zu einem messbaren Vorteil am Markt beitragen.

18.2 Kundendaten beim Betriebsübergang – Hindert Datenschutz die Übertragung?

Ein wichtiges Thema für Unternehmen, Handelsvermittler und Makler ist die Übertragung von Kundenbeständen bei einem Betriebsübergang. Immer wieder erreichen uns Beschwerden, in denen die Betroffenen berichten, Post von ihnen bis dahin unbekannten Unternehmen erhalten zu haben, wonach diese nunmehr etwa einen bestehenden Versicherungsvertrag betreuen. Erst auf Nachfrage wird den Betroffenen mitgeteilt, dass die Kundendatei von dem Vorgänger übernommen worden sei.

Die Weitergabe von Kundendaten – datenschutzrechtlich gesehen eine Verarbeitung personenbezogener Daten – kann ohne ausdrückliche Einwilligung der Betroffenen zulässig sein, wenn sie zur Wahrung berechtigter Interessen erforderlich ist und kein Grund zu der Annahme besteht, dass das schutzwürdige Interesse der Betroffenen an einem Ausschluss der Verarbeitung überwiegt. Die jeweiligen berechtigten Interessen können sowohl wirtschaftlicher wie auch ideeller Art sein. Der Verkauf des Kundenbestandes sowie die Übernahme und Weiterführung der Verträge zur Erzielung eines wirtschaftlichen Erlöses ist als ein solches berechtigtes Interesse anzuerkennen. Im Rahmen der Abwägung dieses wirtschaftlichen Interesses mit den Interessen der Betroffenen ist jedoch zu beachten, dass das Grundrecht auf informationelle Selbstbestimmung Letzteren die Befugnis einräumt, grundsätzlich selbst über die Preisgabe und Verwendung ihrer persönlichen Daten zu bestimmen. Da die Vertragsdaten mitunter weitgehende Rückschlüsse auf die Lebensumstände der Betroffenen zulassen, sind diesen bereits im Vorfeld der Übermittlung hinreichende Informationen zum geplanten Vorgehen zur Verfügung zu stellen. In diesem Zusammenhang sollte zugleich ein Widerspruchsrecht eingeräumt werden, um den Betroffenen die Möglichkeit zur Wahrung ihrer schutzwürdigen Interessen zu geben. Über diese Möglichkeit des Widerspruchs und die damit verbundenen Konsequenzen sind die Kunden rechtzeitig zu informieren.

Unabhängig davon haben Kundendaten für Unternehmen oft auch einen erheblichen wirtschaftlichen Wert wegen der Möglichkeit der persönlichen werblichen Ansprache. Soll neben der Weiterführung der bisherigen Verträge durch das neue Unternehmen zugleich eine werbliche Ansprache der neuen Kunden etwa per E-Mail oder Telefon erfolgen, ist zu beachten, dass hierfür in jedem Falle eine ausdrückliche Werbeeinwilligung erforderlich ist.

Seinen Vertragspartner sucht man sich im Regelfall selbst aus. Im Falle des Betriebsübergangs kann der Betroffene daher nicht gezwungen sein, seine wirtschaftlichen, beruflichen oder sozialen Daten einem ihm unbekannten Nachfolger offenbaren zu müssen. Liegt im Vorfeld keine Einwilligung in die konkrete Weitergabe der Daten vor, ist den Kunden zumindest ein Widerspruchsrecht in Hinblick auf die Übermittlung einzuräumen, um ihre schutzwürdigen Interessen zu wahren.

18.3 Von den Schwierigkeiten, bei übereinstimmendem Namen und gleichem Geburtsdatum eine Personenverwechslung nachzuweisen

Ein Bürger erhielt – für ihn vollkommen überraschend – von einer Rechtsanwaltskanzlei eine Mahnung über eine Gesamtforderung von ca. 800 Euro, die im Namen eines großen Energieversorgers versandt worden war. Für den Fall, dass der Bürger die Forderung nicht innerhalb von 14 Tagen begleicht, wurde ihm ein gerichtliches Mahnverfahren angedroht, dessen Kosten wiederum zu seinen Lasten gehen würden. Das Schreiben enthielt weder Angaben über den Sachverhalt, der der Forderung zugrunde lag, noch eine Aufschlüsselung der Forderung im Einzelnen.

Der vermeintliche Schuldner, der eine Personenverwechslung oder einen missbräuchlichen Umgang mit seinen Daten vermutete, machte zunächst den ihm zustehenden datenschutzrechtlichen Auskunftsanspruch gegenüber der Rechtsanwaltskanzlei geltend. Er fragte insbesondere, welche Daten über seine Person gespeichert seien und wann und von wem die Kanzlei seine Daten erhalten habe. Statt auf das Auskunftsersuchen zu antworten, teilte sie ihm mit, dass es um die Abrechnung einer Verbrauchsstelle in einer von ihm genutzten Wohnung gehe. Zum Beweis berief sich die Rechtsanwaltskanzlei auf eine Aussage der Eigentümerin des entsprechenden Hauses. Die Kanzlei fügte ihrem Schreiben noch die Schlussrechnung mit Angabe der Adresse der Verbrauchsstelle bei, setzte eine neue Zahlungsfrist und teilte zudem mit, dass sich die Gesamtforderung zwischenzeitlich weiter erhöht habe.

Nach einem Hinweis der Landesbeauftragten auf die sich aus dem Bundesdatenschutzgesetz ergebende Pflicht zur Auskunftserteilung teilte uns die

Anwaltskanzlei mit, dass sie, nachdem der Schuldner der maßgeblichen Verbrauchsstelle nicht mehr zu erreichen war, einen Adressdienstleister mit einer Adressrecherche beauftragt habe. Die zunächst mitgeteilte Adresse sei jedoch erfolglos angeschrieben worden. Auf eine zweite Adressrecherche hin habe der Adressdienstleister die Anschrift unseres Petenten übermittelt. Die Rechtsanwaltskanzlei sicherte zu, sich nunmehr mittels einer Melderegisterabfrage Sicherheit über den eigentlichen Schuldner verschaffen zu wollen.

Der vermeintliche Schuldner blieb ebenfalls nicht tatenlos, sondern wandte sich an die Quelle der falschen Daten, nämlich an besagten Adressdienstleister. Der reagierte anfangs zögerlich. Nach Einschaltung der für ihn zuständigen anderen Datenschutzaufsichtsbehörde konnte schließlich festgestellt werden, dass der über unseren Petenten gespeicherte Datenbestand fehlerhaft war. Er wurde für die Weitergabe an Kunden gesperrt; zudem wurden die bisherigen Empfänger der Daten entsprechend unterrichtet. Nachdem auch die Rechtsanwaltskanzlei hiervon Kenntnis erlangt hatte, löschte sie die Daten unseres Petenten und sah von weiteren Nachforschungen ab.

Stellt man fest, dass ein Unternehmen falsche Daten über die eigene Person gespeichert hat oder gar eine Personenverwechslung vorliegt, so ist der datenschutzrechtliche Auskunftsanspruch ein geeignetes, wenn nicht sogar das einzig Erfolg versprechende Instrument, um der falschen Datenspeicherung auf den Grund zu gehen. Dies kann sich allerdings zu einer wahren Odyssee ausweiten, wenn die Daten verarbeitenden Stellen ihrer gesetzlichen Pflicht, Auskunft über die personenbezogenen Daten, ihre Herkunft und ihre Empfänger zu erteilen, nicht oder nur ungenügend nachkommen.

18.4 Zum Wohle der Besucher – Protokollierung der Parkplatznutzung

Uns erreichten wiederholt Anfragen von Bürgern, die ihre Verwunderung darüber zum Ausdruck brachten, dass verschiedene Unternehmen die Kfz-Kennzeichen der Nutzer des eigenen Besucherparkplatzes und die Namen von Gästen dokumentierten.

Zahlreiche Unternehmen stellen ihren Kunden oder Besuchern eigene Parkplatzflächen zur Nutzung für gewisse Zeit zur Verfügung. Einige gehen dabei aber einen Schritt weiter, indem sie das Kennzeichen jedes Fahrzeugs und den Namen des jeweiligen Fahrers erfassen. Bei beiden Angaben handelt es sich um personenbezogene Daten. Gemäß § 3 Abs. 1 Bundesdatenschutzgesetz (BDSG) sind alle Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren Person Daten mit Personenbezug. Dazu zählt insbesondere auch das Kfz-Kennzeichen. Zwar offenbart die Buchstaben-Zahlen-Kombination aus sich heraus nicht die Identität

des Fahrzeughalters. Dieser ist jedoch etwa durch eine Abfrage aus dem Fahrzeugregister bestimmbar.

Da in den uns vorgetragenen Fällen von den Besuchern keine Einwilligung für die Erhebung und Verarbeitung personenbezogener Daten eingeholt wurde, wäre sie nur auf Grundlage einer gesetzlichen Bestimmung zulässig gewesen. Eine solche ist § 28 Abs. 1 Nr. 2 BDSG, die eine Datenverarbeitung erlaubt, wenn sie zur Wahrung berechtigter Interessen der verantwortlichen Stelle erforderlich ist und kein Grund zu der Annahme besteht, dass das schutzwürdige Interessen der Betroffenen an einem Ausschluss der Verarbeitung überwiegt. Hervorzuheben ist, dass es sich bei den berechtigten Interessen um solche der verantwortlichen Stelle handeln muss.

In einem Fall wurde argumentiert, dass bei einer Beschädigung eines Fahrzeuges der Unfallverursacher nur anhand des Kennzeichens ermittelt werden könne. So ließen sich die Interessen des Eigentümers des beschädigten Fahrzeugs schützen. Dies sind jedoch vornehmlich Interessen der Besucher und nicht der verantwortlichen Stelle. Sie müssen daher bei der anzustellenden Interessenabwägung außer Betracht bleiben.

Andere Interessen, wie die Abwehr von Gefahren für hergestellte Produkte, betreffen die verantwortliche Stelle und sind grundsätzlich zu berücksichtigen. Zur Wahrung der geforderten Standards in der Lebensmittelsicherheit war im konkreten Fall allerdings nur die Dokumentation der Namen der Besucher erforderlich, um eine mögliche Verunreinigung durch diese aufklären zu können. Sie war damit zulässig. Auf die unzulässige Aufzeichnung der Kfz-Kennzeichen verzichtet das Unternehmen dagegen nunmehr.

Bei der Abwägung der Interessen sind nur solche der verantwortlichen Stelle sowie der Betroffenen zu berücksichtigen. Öffentliche Interessen oder solche Dritter müssen außer Betracht bleiben. Eine Dokumentation von Besuchern kann im Einzelfall zulässig sein, wobei jedoch der Grundsatz der Erforderlichkeit strikt zu beachten ist.

19 Wissenschaft und Forschung

Audio- und Videomitschnitte in Lehrveranstaltungen an Hochschulen

Zunehmend ist zu beobachten, dass Studenten in Vorlesungen, Seminaren und Übungen heimlich oder auch offen Audio- oder Videoaufnahmen von den Vorträgen der Dozenten fertigen. Die Aufzeichnungen dienen vermutlich eigenen Lernzwecken und ersetzen offenbar die früher üblichen Mitschriften. Die Dozenten sind häufig mit dem Aufnehmen ihrer Vorträge und Präsentationsfolien nicht einverstanden.

Zwar stellen Videoaufnahmen von Dozenten ebenso wie akustische Mitschnitte ihres gesprochenen Wortes personenbezogene Daten dar. Allerdings gelten die Vorschriften des Bundesdatenschutzgesetzes (BDSG) für Private nicht, sofern sie diese Daten ausschließlich für persönliche oder familiäre Tätigkeiten erheben, verarbeiten oder nutzen.

Fertigen Studenten die Video- oder Audioaufnahmen ausschließlich zu eigenen Lernzwecken, ist diese Tätigkeit ihrem persönlichen Lebensbereich zuzuordnen. Dies ist jedenfalls dann unzweifelhaft, wenn die Aufnahmen im persönlichen Herrschaftsbereich verbleiben, wenn also nur der Student eigene und abgesicherte Zugriffsrechte auf seine Aufnahmen hat und ein Zugriff regelmäßig nur durch ihn selbst erfolgen kann. Etwas anderes muss gelten, wenn der Student die Aufnahmen z. B. zu gewerblichen Zwecken fertigt oder sie an Dritte übermittelt, die ihrerseits die Aufnahmen zu eigenen unternehmerischen Zwecken verarbeiten. Denn sobald neben persönlichen oder familiären Zwecken auch andere Ziele verfolgt werden, liegt keine ausschließlich private Nutzung mehr vor. Entscheidend ist also, dass die Verwendung der Daten auf den privaten Aktionsradius beschränkt bleibt.

Wie ist es aber, wenn ein Student die Aufnahmen an Kommilitonen übermittelt? Unbedenklich ist sicherlich die Weitergabe einer Aufnahme an einen einzelnen Kommilitonen, der – etwa krankheitsbedingt – am Besuch einer Vorlesung gehindert war. Eine Übermittlung an eine Mehrzahl von Studenten, noch dazu regelmäßig, dürfte dagegen schnell die Grenze der persönlichen Lebensführung überschreiten. Ist beabsichtigt, Video- oder Audioaufnahmen Dritten zu übermitteln, muss daher im Zweifelsfall die Einwilligung des jeweils betroffenen Dozenten eingeholt werden, da eine gesetzliche Erlaubnisnorm nicht existiert.

Insbesondere kann sich der Hersteller eines Mitschnitts nicht darauf berufen, dass die Aufnahmen für eigene Geschäftszwecke benötigt würden und damit die datenschutzrechtliche Erlaubnis des § 28 Abs. 1 BDSG anwendbar sei. Denn dies würde voraussetzen, dass kein Grund zu der Annahme besteht,

dass schutzwürdige Interessen des Betroffenen an dem Ausschluss der Verarbeitung oder Nutzung überwiegen. Ein solches schutzwürdiges Interesse des betroffenen Dozenten wäre sicherlich sein Urheberrecht an seinem Vortrag ebenso wie sein aus dem allgemeinen Persönlichkeitsrecht abgeleitetes Recht am eigenen Bild. Das Verbreitungsinteresse des Studenten muss demgegenüber hintanstehen.

Aus Gründen unserer auf den Datenschutz beschränkten Zuständigkeit mussten wir uns bei der Prüfung der Rechtmäßigkeit der Audio- und Videoaufnahmen auf die datenschutzrechtlichen Gesichtspunkte beschränken. Daneben sind aber vor allem auch urheberrechtliche Aspekte zu beachten.

Aus datenschutzrechtlicher Sicht sind Audio- und Videoaufnahmen in Lehrveranstaltungen solange unbedenklich, wie die Studenten diese Aufnahmen ausschließlich für ihre privaten (Lern-) Zwecke verwenden. Eine weitergehende Nutzung bedarf regelmäßig der Zustimmung des jeweils betroffenen Dozenten. Daneben sind die urheberrechtlichen Vorschriften zu beachten.

20 Betriebliche und behördliche Datenschutzbeauftragte

20.1 Darf eine juristische Person zum Datenschutzbeauftragten bestellt werden?

Unternehmen haben bei Vorliegen der gesetzlichen Voraussetzungen einen betrieblichen Datenschutzbeauftragten zu bestellen. Dieser muss dort nicht selbst beschäftigt sein. In letzter Zeit erreichte uns mehrfach die Frage, ob auch die Bestellung einer juristischen Person als externer Datenschutzbeauftragter zulässig ist. Gerade kleinere verantwortliche Stellen planen, durch die externe Vergabe der Aufgaben von der Expertise datenschutzrechtlich bzw. -technisch spezialisierter Rechtsanwaltskanzleien oder Beratungsunternehmen zu profitieren.

Die derzeit geltende Regelung des § 4f Bundesdatenschutzgesetz fordert vom zu bestellenden Datenschutzbeauftragten die zur Erfüllung seiner Aufgaben erforderliche Fachkunde (d. h. insbesondere datenschutzrechtliche sowie technische und organisatorische Kenntnisse) sowie Zuverlässigkeit – beides persönliche Eigenschaften. Außerdem ist der Datenschutzbeauftragte der Leitung der verantwortlichen Stelle unmittelbar zu unterstellen. Diese Voraussetzungen kann nach unserer Auffassung nur eine natürliche, nicht aber eine juristische Person erfüllen. Auch die Schutzvorschriften des Bundesdatenschutzgesetzes, wie beispielsweise der Grundsatz, dass der Datenschutzbeauftragte wegen der Erfüllung seiner Aufgaben nicht benachteiligt

werden darf, und das ihm zustehende Zeugnisverweigerungsrecht sind erkennbar auf eine natürliche Person zugeschnitten.

Die ab Mai 2018 geltende Datenschutz-Grundverordnung (DS-GVO) enthält ähnliche Festlegungen. So fordert Art. 37 Abs. 5 DS-GVO, dass der Datenschutzbeauftragte auf der Grundlage seiner beruflichen Qualifikation und insbesondere des Fachwissens benannt wird, das er auf dem Gebiet des Datenschutzrechts und der Datenschutzpraxis besitzt, sowie auf der Grundlage seiner Fähigkeit zur Erfüllung der von ihm nach Art. 39 DS-GVO wahrzunehmenden Aufgaben. Weiter regelt Art. 37 Abs. 6 DS-GVO, dass der Datenschutzbeauftragte Beschäftigter des Verantwortlichen (bzw. Auftragsverarbeiters) sein oder seine Aufgaben auf der Grundlage eines Dienstleistungsvertrages erfüllen kann.

Vor diesem Hintergrund hat die Artikel-29-Datenschutzgruppe der Datenschutzbeauftragten der Mitgliedsstaaten der Europäischen Union in einem Arbeitspapier ergänzende Hinweise veröffentlicht.[65] Danach kann der Dienstleistungsvertrag, auf dessen Grundlage die Funktion eines Datenschutzbeauftragten ausgeübt wird, mit einer natürlichen oder juristischen Person geschlossen werden. Im zuletzt genannten Fall ist es jedoch unverzichtbar, dass jedes Mitglied der Organisation, das Datenschutzaufgaben für den Auftraggeber wahrnimmt, sämtliche Anforderungen der Datenschutz-Grundverordnung erfüllt, insbesondere das erforderliche Fachwissen besitzt, unabhängig agiert und Interessenskonflikte ausgeschlossen werden. Darüber hinaus ist der Schutz vor ungerechtfertigter Kündigung des Dienstleistungsvertrages oder Entlassung beim Dienstleister wegen der Erfüllung von Datenschutzaufgaben zu sichern.

Auch wenn durch die Zusammenarbeit mehrerer externer Personen in einem „Datenschutz-Team“ deren individuelle Qualifikationen und Stärken kombiniert und die Tätigkeit damit effizienter gestaltet werden kann, empfiehlt die Artikel-29-Datenschutzgruppe, eine einzelne Person als primären Ansprechpartner für den jeweiligen Auftraggeber sowie eine klare Verteilung der Aufgaben und Verantwortlichkeiten im Team vertraglich festzulegen.

Wenn die Aufgaben des Datenschutzbeauftragten auf der Basis eines Dienstleistungsvertrages mit einer externen Organisation wahrgenommen werden sollen, ist zu gewährleisten, dass alle hierbei agierenden Personen die Anforderungen der Datenschutz-Grundverordnung erfüllen. Darüber hinaus ist in der vertraglichen Regelung eine natürliche Person als Hauptansprechpartner in Datenschutzfragen festzulegen.

[65] Artikel-29-Datenschutzgruppe, „Leitlinien in Bezug auf Datenschutzbeauftragte“ (Working Paper WP 243 rev.01, zuletzt überarbeitet und angenommen am 5. April 2017).

20.2 Beratungen mit den behördlichen Datenschutzbeauftragten

Einmal im Jahr laden wir die behördlichen Datenschutzbeauftragten der Landkreise, kreisfreien Städte und größeren kreisangehörigen Gemeinden zu einer ganztägigen Beratung in unsere Dienststelle ein. Im Berichtszeitraum fanden das 13. und 14. Treffen dieser Art statt.

Die diskutierten Themen werden regelmäßig von den behördlichen Datenschutzbeauftragten selbst vorgeschlagen. Sie entstammen ihrer täglichen Arbeit, beinhalten verschiedenste datenschutzrechtliche Fragestellungen und treten in ähnlicher Form bei vielen Teilnehmern der Beratungen auf. Im Austausch miteinander und mit Vertretern unserer Dienststelle werden z. B. Auslegungen von Rechtsvorschriften vorgenommen, Lösungsmöglichkeiten erörtert und bewertet sowie Empfehlungen und Hinweise zur Umsetzung in der Praxis gegeben. Die Veranstaltungen haben sich bewährt und ermöglichen den Beauftragten auch, von den Erfahrungen anderer Behörden zu profitieren. Auf diesem Wege können im jeweils eigenen Zuständigkeitsbereich frühzeitig Probleme bei der Verarbeitung personenbezogener Daten identifiziert und ggf. erforderliche Maßnahmen bzw. Korrekturen eingeleitet werden.

Inhaltliche Schwerpunkte der Beratungen im Berichtszeitraum waren z. B. Übermittlungen von Gesundheits- und Sozialdaten, insbesondere im Kinder- und Jugendbereich, Möglichkeiten der Überprüfung von dienstlichen E-Mail-Konten, der Umgang mit Bewerberdaten, elektronische Einwilligungserklärungen, Fragen der datenschutzgerechten Gestaltung der Zusammenarbeit zwischen Kommunen, Auftragsdatenverarbeitung und Fernwartung. Bei der zuletzt durchgeführten Veranstaltung standen darüber hinaus Fragen zur Anwendung und Umsetzung der Datenschutz-Grundverordnung, die ab dem 25. Mai 2018 auch für die öffentlichen Stellen des Landes gilt, und der daraus resultierenden Anpassungen des allgemeinen Datenschutzrechts im Land Brandenburg im Fokus.

21 Tätigkeit der Sanktionsstelle

21.1 Überblick zu den Ordnungswidrigkeitenverfahren

Im Berichtszeitraum hat die Landesbeauftragte 54 Ordnungswidrigkeitenverfahren wegen verschiedener Verstöße sowohl gegen das Brandenburgische als auch das Bundesdatenschutzgesetz geführt.

Von den 54 durchgeführten Verfahren haben wir in 21 Fällen ein Bußgeld verhängt. Die Summe der verhängten Bußgelder betrug 28.970 Euro. In fünf Fällen haben wir eine Verwarnung ausgesprochen und dabei in einem Fall ein Verwarngeld in Höhe von 35 € festgesetzt. Die übrigen 28 Verfahren waren einzustellen, weil unter anderem einzelne Tatbestandsvoraussetzungen, wie beispielsweise das subjektive Merkmal der vorsätzlichen Begehungsweise, nicht erfüllt wurden. Ein fahrlässiges Handeln kann nach § 38 Brandenburgisches Datenschutzgesetz (BbgDSG) nicht geahndet werden – im Gegensatz zum Bundesdatenschutzgesetz (BDSG). Zudem mussten wir teilweise Vorgänge mangels Zuständigkeit an die Staatsanwaltschaft oder Polizei zurückgeben.

Die Verfahren, die mit der Festsetzung von Bußgeldern bzw. einer Verwarnung abgeschlossen wurden, betrafen unter anderem – wie schon in früheren Berichtszeiträumen – den unbefugten Abruf personenbezogener Daten aus Datenbanken durch Polizeibedienstete und Mitarbeiter der öffentlichen Verwaltung. Teilweise wurden die unbefugt erlangten Daten zudem an Dritte weitergegeben. Auch die Nichterteilung von Auskünften gegenüber der Landesbeauftragten und die unsachgemäße Entsorgung von Datenmüll haben wir im Berichtszeitraum sanktioniert.

In letztgenanntem Fall wurden u. a. Arztrezepte, Überweisungsscheine und Krankenkassenkarten, auf denen sich Patientendaten befanden, lediglich grob zerkleinert in der Abfalltonne der Nachbarn entsorgt. Namen, Diagnosen und Anschriften der betroffenen Patienten waren gut lesbar. Daten verarbeitende Stellen müssen aber dafür Sorge tragen, dass die datenschutzrechtlichen Vorgaben auch beim Entsorgen der Daten eingehalten werden. Ein Verstoß hiergegen wird empfindlich sanktioniert.

Einen Fall der unbefugten Datenweitergabe im nicht öffentlichen Bereich sanktionierte die Landesbeauftragte ebenfalls mit der Verhängung eines Bußgelds. Der ehemalige Arbeitgeber der Betroffenen gab deren Namen, Anschrift und die Tatsache, dass das Beschäftigungsverhältnis beendet war, an einen befreundeten Dritten weiter. Daraufhin unterbreitete dieser ihr ein Arbeitsangebot. Selbst wenn die Übermittlung der Daten ohne Kenntnis und Einverständnis der Betroffenen nur „gut gemeint“ war, handelt es sich dennoch um eine unbefugte Vorgehensweise. Denn solange die Betroffene nicht ausdrücklich einwilligt oder die Datenweitergabe auf eine gesetzliche Grundlage gestützt werden kann, ist sie zu unterlassen.

Auch in einem anderen Fall wurden Beschäftigtendaten unzulässig übermittelt. Der Geschäftsführer eines Unternehmens zur Organisation von Veranstaltungen übersandte – zumindest unter Außerachtlassung der erforderlichen Sorgfalt – einer Mitarbeiterin im Anhang zur E-Mail eine Datei, die nicht nur deren eigene Entgeltabrechnung, sondern auch die Abrechnungen für 38

weitere Beschäftigte enthielt. Den Lohnzetteln waren nicht nur der Name, die Adresse, das Geburtsdatum und die Entgeltdaten sondern auch Kontodaten (IBAN, BIC), Steuerdaten (Steuer ID, Steuerklasse, ggf. Kinderfreibeträge und Konfession für Kirchensteuerabzug) sowie Sozialversicherungsdaten (Sozialversicherungsnummer, Krankenkasse) der Beschäftigten zu entnehmen. Obwohl der Geschäftsführer unmittelbar nach dem Versand der E-Mail an die Mitarbeiterin durch diese von der fehlerhaften Zustellung der Lohnzettel Kenntnis erhielt, unterließen er und die weiteren Geschäftsführer es, die Landesbeauftragte über den Vorfall in Kenntnis zu setzen. Zumindest aus mangelnder Sorgfalt erkannten sie nicht, dass sie hierzu nach § 42a BDSG verpflichtet gewesen wären. Der aus dieser Norm gleichfalls resultierenden Pflicht, die 38 betroffenen Mitarbeiter über den Vorfall zu informieren, kamen sie gleichfalls nicht nach. Für diese drei Verstöße haben wir gegen das Unternehmen insgesamt ein Bußgeld im vierstelligen Bereich ausgesprochen.

Mehrere Bußgelder mussten gemäß § 43 Abs. 1 Nr. 10 BDSG erlassen werden, da die verantwortlichen Stellen sich vehement weigerten, einem Auskunftsverlangen der Landesbeauftragten zu entsprechen bzw. nur verspätet antworteten. Daten verarbeitende Stellen sind gemäß § 38 Abs. 3 Satz 1 BDSG aber gesetzlich dazu verpflichtet, der Landesbeauftragten die für die Erfüllung ihrer gesetzlichen Aufgaben erforderlichen Auskünfte zu erteilen.

Nach § 34 BDSG hat der Betroffene ein Recht auf Auskunft, welche personenbezogenen Daten über ihn gespeichert sind. Zum Umfang der Auskunft gehört auch, zu welchem Zweck die Daten erhoben wurden, woher diese stammen und an welche Stellen diese übermittelt wurden. Die Auskunft muss nachvollziehbar und in allgemein verständlicher Form erteilt werden. Zudem erfordert die umfassende Auskunftspflicht auch, die Antragsteller darüber zu informieren, wenn über sie keine Daten gespeichert sind. Auch die Negativauskunft ist eine gebotene Form der Auskunftserteilung. Eine eindeutige, unmissverständliche Mitteilung an den Anfragenden, beispielsweise in der Form: „Wir haben keine Daten zu Ihrer Person vorliegen.“ wäre erforderlich, aber auch ausreichend. Eine verspätete oder unvollständige Auskunft an den Betroffenen kann gemäß § 43 Abs. 1 Nr. 8a BDSG mit einem Bußgeld geahndet werden. Dieses Mittel anzuwenden, sahen wir uns im Berichtszeitraum erneut gezwungen:

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

Im öffentlichen Bereich kam es auch im aktuellen Berichtszeitraum zu Datenschutzverstößen in Zusammenhang mit unbefugten Abrufen, die wir mit Bußgeldern geahndet haben. In der öffentlichen Verwaltung nutzte beispielsweise ein Bürgermeister seine Stellung als Vorgesetzter aus und wies seine ihm unterstellten Mitarbeiter an, die Namen von Kraftfahrzeughaltern aus der Datenbank des Kraftfahrt-Bundesamtes zu ermitteln und ihm dann vorzulegen. Diesem Ansinnen lagen aber keine dienstlichen Anlässe, wie z. B. die Ahndung von Verkehrsverstößen zugrunde, sondern rein private Motive. In einem anderen Fall gab es gleichfalls keinen ausreichenden dienstlichen Anlass, der eine Erhebung personenbezogener Daten gerechtfertigt hätte. Hier war es vor allem die Neugier, die dazu führte, dass sich der Amtsinhaber die Anträge auf Kita-Betreuung vorlegen ließ, um zu erfahren, wo die Eltern arbeiten. In beiden Fällen fehlte es sowohl an der Einwilligung der Betroffenen als auch an einer Rechtsgrundlage, die die Abfragen gerechtfertigt hätten. Personenbezogene Daten dürfen aus für dienstliche Zwecke zur Verfügung stehenden Datenbanken bzw. Akten nur aufgrund eines dienstlichen Anlasses und nur für dienstliche Zwecke verwendet werden.

Dies gilt ebenso für Polizeibedienstete. Zwar mag es verlockend sein, in dienstlich zur Verfügung gestellten Datenbanken aus privatem Anlass schnell Informationen zu erhalten. Allerdings stellt jeder einzelne Abruf, der nicht dienstlich veranlasst ist, eine Ordnungswidrigkeit dar und wurde von uns jeweils entsprechend sanktioniert. So war es auch in dem Fall, in dem eine Zeugin ihre private Telefonnummer für weitere Nachfragen zur Verfügung gestellt hatte und diese dann von einem Beamten zur Anbahnung persönlicher Kontakte verwendet wurde. Nicht nur eigene Interessen, sondern auch Freundschaftsdienste sind zwar ein Motiv, rechtfertigen es aber nicht, Daten von Betroffenen aus dienstlich zur Verfügung stehenden Datenbanken oder Unterlagen abzufragen.

Die Sanktionspraxis der Ordnungswidrigkeitenstelle wird sich mit Geltung der Datenschutz-Grundverordnung ab dem 25. Mai 2018 weitreichend verändern, da um ein Vielfaches höhere Bußgelder verhängt werden können. Es ist daher umso wichtiger, dass die verantwortlichen Stellen dafür Sorge tragen, dass die datenschutzrechtlichen Vorgaben eingehalten werden.

21.2 Verlust von Daten auf dem Postweg – Wer ist meldepflichtig?

Beim Auftreten einer Datenpanne muss die verantwortliche Stelle in bestimmten Fällen sowohl dem Betroffenen als auch der zuständigen Aufsichtsbehörde den Vorfall melden. Tut sie dies nicht, droht ihr ein Bußgeld. In diesem Zusammenhang hatten wir die Frage zu klären, wer nach § 42a Bundesdatenschutzgesetz (BDSG) meldepflichtig ist, wenn ein

Absender (also die verantwortliche Stelle) eine Postsendung mit personenbezogenen Daten mehrerer Betroffener mittels eines Postdienstleisters verschicken will, die Sendung aber auf dem Postweg verloren geht.

Kernproblem des dargestellten Sachverhalts ist die Frage, ob der Absender nach der Abgabe des Pakets mit den personenbezogenen Daten an den Postdienstleister weiterhin als meldepflichtige Stelle anzusehen ist. Das ist gemäß § 42a BDSG dann der Fall, wenn die Daten bei ihm gespeichert sind. In der Abgabe des Pakets an den Postdienstleister könnte eine Beendigung des Speicherns beim Absender gesehen werden. Allerdings speichert der Postdienstleister seinerseits die Daten nicht, weil er wegen des Postgeheimnisses keine Kenntnis davon hat, dass sich personenbezogene Daten in dem Paket befinden. Diese Kenntnis ist aber Voraussetzung dafür, selbst Daten speichern zu können. Würde in der Abgabe des Pakets eine Beendigung des Speicherns des Absenders gesehen, da er tatsächlich keinen Zugriff mehr auf die Daten hat und kann aber gleichzeitig keine neue Speicherung durch den Postdienstleister eintreten, wäre niemand die meldepflichtige Stelle im Sinne des § 42a BDSG. Diese Auslegung würde dem Gesetzeszweck, nämlich die Betroffenen eines Datenlecks und die Aufsichtsbehörde davon unverzüglich in Kenntnis zu setzen, widersprechen.

Für jede gesetzlich geregelte Aktivität muss es zudem immer einen Verantwortlichen geben, sodass kein Raum für eine „unverantwortete“ Aktivität bleibt. Die Eigenschaft als verantwortliche Stelle ist dabei nicht streng an den Besitz der Daten gebunden, sondern bleibt auch beim Transport von Datenträgern durch Dritte erhalten. Dies führt dazu, dass der Absender so lange als speichernde und damit verantwortliche Stelle angesehen wird, bis die jeweilige Postsendung mit den personenbezogenen Daten beim Empfänger ankommt. Erreicht die Postsendung den Empfänger nicht, ist der Absender verpflichtet, sowohl der Aufsichtsbehörde als auch den Betroffenen den Verlust der Daten unverzüglich zu melden, sobald er davon Kenntnis erlangt. Unterlässt er die Meldung, kann dies als Ordnungswidrigkeit mit einem Bußgeld geahndet werden.

Die Versendung personenbezogener Daten unter Zuhilfenahme eines Postdienstleisters entbindet den Absender nicht von seiner Meldepflicht bei Datenschutzverletzungen. Ab Geltung der Datenschutz-Grundverordnung (DS-GVO) richtet sich diese Pflicht zukünftig nach Art. 33 und 34 DS-GVO.

Teil C

Akteneinsicht und Informationszugang

1 Entwicklung des Informationszugangsrechts

1.1 Bundesrepublik Deutschland

Am 7. Dezember 2016 hat die Bundesregierung nach langem Zögern die Teilnahme der Bundesrepublik Deutschland an der Open Government Partnership (OGP) erklärt. Diese internationale Initiative wurde im Jahr 2011 gegründet; die Teilnehmerstaaten setzen sich für die Förderung von offenem Regierungs- und Verwaltungshandeln (Open Government) ein. Aus Sicht der Bundesregierung ist die Teilnahme Deutschlands ein wichtiges Signal für den Veränderungsprozess in der Verwaltung hin zu einer Digitalisierung, Öffnung, Zusammenarbeit und Weiterentwicklung im Sinne von Open Government. Auch eine Akzentuierung von Reformprojekten, darunter beispielsweise Open Data, wird angestrebt. Als wichtiges Instrument dienen der Open Government Partnership nationale Aktionspläne, die alle zwei Jahre unter Einbeziehung der Zivilgesellschaft erstellt und anschließend evaluiert werden. Diese Pläne sollen Vorhaben in Form von Selbstverpflichtungen aller staatlichen Ebenen (Bund, Länder, Kommunen) unter anderem zu Transparenzfragen bündeln. In dem ersten, im Sommer 2017 veröffentlichten Nationalen Aktionsplan 2017–2019 bekennt sich die Bundesregierung zu hehren Ambitionen: „Die Bundesregierung will Vorreiter bei Open Data werden. Die Veröffentlichung von Daten als Open Data soll Teil des täglichen Verwaltungshandelns werden. Das daraus entstehende Daten-Ökosystem der Verwaltung soll Grundlage für Transparenz und Innovation sein und den Bedarfen der Nutzer entsprechen.“ Der erste Nationale Aktionsplan richtet sich nur an Bundesbehörden; eine Einbeziehung der Landes- und Kommunalverwaltungen in den OGP-Prozess ist im Rahmen der Erstellung des zweiten Nationalen Aktionsplans vorgesehen. Dies ist eine Chance, Informationszugangsgesetze und Open Data auch in Brandenburg weiterzuentwickeln.

Der Deutsche Bundestag hat am 18. Mai 2017 die erste – auch als Open-Data-Gesetz bezeichnete – Änderung des E-Government-Gesetzes beschlossen. Nach einer vorangegangen Vereinbarung der Regierungschefs von Bund und Ländern sollen auch die Länder solche Gesetze erlassen, um bundesweit vergleichbare Standards für den Zugang zu öffentlichen Datenpools zu erreichen. Das Open-Data-Gesetz erklärt die öffentliche Bereitstellung von Daten zum Standard; Ausnahmen müssen begründet werden („Open Data by default“). Bundesbehörden werden verpflichtet, Rohdaten entgeltfrei und zur uneingeschränkten Weiterverwendung für jedermann zur Verfügung zu stellen. Zusammenhängende Texte, wie zum Beispiel Verträge,

Gutachten, Stellungnahmen und ähnliche Dokumente, sind davon nicht umfasst. Außerdem gehen die Ausnahmen des Open-Data-Gesetzes sogar noch über die im Informationsfreiheitsgesetz geregelten Ausnahmen hinaus. Beispielsweise sollen nur Daten veröffentlicht werden, die außerhalb der jeweiligen Behörde liegende Verhältnisse betreffen. Einen individuellen Anspruch auf Veröffentlichung enthält das Gesetz zudem nicht. Die Informationsfreiheitsbeauftragten der Länder haben dies während des Gesetzgebungsprozesses kritisiert und eine Weiterentwicklung des Informationsfreiheitsgesetzes des Bundes hin zu einem Transparenzgesetz gefordert, das die dazugehörigen Open-Data-Regelungen einschließt. Eine Vorbildfunktion für die Länder sahen sie in dem verabschiedeten Bundesgesetz nicht.[66] Zuvor hatte bereits die Konferenz der Informationsfreiheitsbeauftragten in Deutschland die Gesetzgeber in Bund und Ländern aufgefordert, nicht bei Open Data stehenzubleiben, sondern flächendeckend Transparenzgesetze zu schaffen.[67] Das Ministerium des Innern und für Kommunales des Landes Brandenburg stellte der Landesbeauftragten in Aussicht, dass es die Kritikpunkte der Informationsfreiheitsbeauftragten in die – indes noch ausstehende – Fortschreibung der Open-Data-Strategie des Landes sowie in die Erarbeitung eines E-Government-Gesetzes einfließen lassen werde.

Das seit dem Jahre 2015 betriebene nationale Datenportal GovData soll die Daten aus den Behörden der Bundes-, Landes- und Kommunalverwaltungen auffindbar machen und künftig als Portal für die nach dem Open-Data-Gesetz verpflichtende Bereitstellung von Daten dienen. GovData ist eine Anwendung des IT-Planungsrates. Verantwortlich für das Portal ist eine Geschäfts- und Koordinierungsstelle mit Sitz in Hamburg. Inzwischen beteiligen sich neben dem Bund elf Bundesländer, darunter auch Brandenburg, an dem Portal. Die Konferenz der Informationsfreiheitsbeauftragten in Deutschland hat an die verbleibenden Länder appelliert, der Verwaltungsvereinbarung ebenfalls beizutreten, und forderte alle Vereinbarungspartner zur verstärkten Bereitstellung von Daten auf.[68] Zu dem letztgenannten Punkt teilte das Ministerium des Innern und für Kommunales des Landes Brandenburg mit, es arbeite an der Fortentwicklung des Metadatenstandards für das Angebot von Daten auf dem Portal.

Von der höchstrichterlichen Rechtsprechung gingen auch im Berichtszeitraum wieder wesentliche Akzente für die Anwendung des Informationsfrei-

---

66 Entschließung der Informationsfreiheitsbeauftragten der Länder vom 24. April 2017, „Open Data: Gesetzentwurf der Bundesregierung greift zu kurz!“, siehe Anlage 4.3.

67 Entschließung der Konferenz der Informationsfreiheitsbeauftragten in Deutschland vom 2. Dezember 2016, „Nicht bei Open Data stehenbleiben: Jetzt auch Transparenzgesetze in Bund und Ländern schaffen!“, siehe Anlage 3.2.

68 Entschließung der Konferenz der Informationsfreiheitsbeauftragten in Deutschland vom 15. Juni 2016, „GovData: Alle Länder sollen der Verwaltungsvereinbarung beitreten und Daten auf dem Portal bereitstellen!“, siehe Anlage 3.3.

heitsgesetzes aus. So stellte das Bundesverfassungsgericht in einer Entscheidung[69] ausdrücklich fest, dass die Informationsfreiheit aus Artikel 5 Grundgesetz auch den Zugang zu allgemein zugänglichen Informationsquellen schützt, wenn eine im staatlichen Verantwortungsbereich liegende Informationsquelle aufgrund rechtlicher Vorgaben zur öffentlichen Zugänglichkeit bestimmt ist. Anders formuliert: Wenn der Gesetzgeber ein Informationsfreiheitsgesetz erlassen hat, kommt der Informationsfreiheit Verfassungsrang zu. Die Entscheidung, ob Einsicht gewährt wird oder insbesondere die Geheimhaltungsinteressen Dritter gewichtiger sind, muss somit im Rahmen einer Güterabwägung zwischen gleichrangigen Interessen getroffen werden. Personenbezogene Daten oder Betriebs- und Geschäftsgeheimnisse sind damit nicht mehr per se höherwertigere Grundrechte im Verhältnis zum Recht auf Akteneinsicht. Allerdings trifft dies nicht zu, wenn der Gesetzgeber gar kein Informationsfreiheitsgesetz erlassen hat. In ähnlicher Weise argumentierte im Übrigen auch der Verfassungsgerichtshof Rheinland-Pfalz:[70] Nimmt der Gesetzgeber bestimmte Bereiche oder Informationen aus dem Zugangsanspruch heraus, fehle es an der allgemeinen Zugänglichkeit im Sinne der Verfassung. Anders sei es bei Einschränkungen, die erst in Abhängigkeit vom Einzelfall zum Tragen kommen; diese Einschränkungen sind zwar im Rahmen einer Güterabwägung zu berücksichtigen, stellten aber nicht infrage, dass die dem Zugangsanspruch unterstellten Informationen nach der Entscheidung des Gesetzgebers der Öffentlichkeit zugänglich sein sollen und damit dem Verfassungsrecht der Informationsfreiheit unterfallen. Strittig waren Regelungen des Landestransparenzgesetzes Rheinland-Pfalz, die die Zugänglichkeit von Informationen im Bereich von Wissenschaft, Forschung und Lehre einschränkten. Den Beschluss des Bundesverfassungsgerichts nahmen die Informationsfreiheitsbeauftragten der Länder zum Anlass, zu fordern, die Informationsfreiheit nicht im Belieben des jeweiligen Gesetzgebers zu belassen, sondern sie ausdrücklich im Grundgesetz zu normieren. Damit wäre auch für die Länder, die immer noch kein Recht auf voraussetzungslosen Zugang gewähren, die Pflicht verbunden, ein solches Recht einfachgesetzlich zu verankern.[71]

In einem viel beachteten Urteil[72] entschied das Bundesverwaltungsgericht, dass einem Journalisten Einsicht in ein Gutachten über die politische Belastung ehemaliger Mitarbeiter eines Bundesministeriums in der NS-Zeit zu gewähren ist, soweit die Mitarbeiter bereits verstorben sind. Der postmortale Persönlichkeitsschutz stehe dem nicht entgegen. Die Herausgabe von Angaben zu noch lebenden Mitarbeitern jedoch stehe unter dem Vorbehalt ihrer

69 Beschluss des Bundesverfassungsgerichts vom 20. Juni 2017, 1 BvR 1978/13.

70 Beschluss des Verfassungsgerichtshofs Rheinland-Pfalz vom 27. Oktober 2017, VGH B 37/16.

71 Grundsatzpositionen der Landesbeauftragten für die Informationsfreiheit vom 9. Oktober 2017, siehe Anlage 4.1,

72 Urteil des Bundesverwaltungsgerichts vom 29. Juni 2017, 7 C 24.15.

Einwilligung. Ein entsprechendes Drittbeteiligungsverfahren sei immer dann durchzuführen, wenn ein Versagungsgrund durch eine solche Einwilligung überwunden werden kann. Das Urteil befasst sich ausführlich mit dem Verhältnis zwischen Informationsfreiheitsgesetz und Bundesbeamtengesetz, das die hier relevanten Vorschriften zu Personalaktendaten enthält. Es kommt zu dem Ergebnis, dass der Regelungswille des Informationsfreiheitsgesetzes sich auch auf die Personalaktendaten erstreckt, beide gesetzlichen Bestimmungen also gleichrangig nebeneinander stehen.

Mit einer Reihe von Urteilen hat das Bundesverwaltungsgericht gegen ein Recht auf Informationszugang zu behördlichen Diensttelefonlisten – konkret ging es um Jobcenter – entschieden.[73] Es beendete damit eine Rechtsunsicherheit, die aufgrund unterschiedlicher Entscheidungen der Vorinstanzen entstanden war. Das Informationsfreiheitsgesetz enthält eine Ausnahme vom grundsätzlichen Schutz personenbezogener Daten für den Fall, dass Kontaktdaten von Bearbeitern betroffen sind. Hierzu stellte das Bundesverwaltungsgericht klar, dass Bearbeiter im Sinne des Informationsfreiheitsgesetzes nicht alle Bediensteten einer Behörde, sondern nur diejenigen sind, die mit einem bestimmten Verwaltungsvorgang befasst waren, zu dem Informationszugang begehrt wird. Die dienstlichen Telefonnummern würden als personenbezogene Daten der Mitarbeiter vom Schutzbereich des Grundrechts auf informationelle Selbstbestimmung erfasst. Das Bundesverwaltungsgericht argumentiert zudem, dass neben dem Datenschutz auch der Schutz der öffentlichen Sicherheit – hier der Funktionsfähigkeit staatlicher Einrichtungen – einer Herausgabe der Telefonlisten entgegenstehe. Deren Gefährdung sei bereits dann zu bejahen, wenn die effektive Aufgabenerledigung gestört und die Arbeit der betroffenen Bediensteten beeinträchtigt werden kann. Es erscheine plausibel, dass sowohl die schriftliche Erledigung von Verwaltungsvorgängen als auch Beratungsgespräche mit persönlich anwesenden Kunden durch Anrufe erheblich beeinträchtigt werden, da diese die Konzentration störten und dadurch Qualität und Quantität der Aufgabenerledigung verminderten.

In einer Entscheidung[74] über den Zugang zu einem Vorgang, der die Privatisierung eines Unternehmens betraf, stellte das Bundesverwaltungsgericht unter anderem fest, dass eine informationspflichtige Stelle Unterlagen nach Eingang eines Antrags auf Akteneinsicht nicht einfach vernichten oder weggeben darf, auch nicht an ein gesetzliches Archiv. Anderenfalls müsste sie sich die Unterlagen gegebenenfalls im Wege der Amtshilfe vorübergehend wieder übermitteln lassen, um den Informationszugangsanspruch zu prüfen.

---

73 Urteile des Bundesverwaltungsgerichts vom 20. Oktober 2016, 7 C 20.15, 7 C 23.15, 7 C 27.15, 7 C 28.15.

74 Urteil des Bundesverwaltungsgerichts vom 17. März 2016, 7 C 2.15.

Die Entscheidung über einen Antrag auf Informationszugang, der einen einheitlichen Lebenssachverhalt betrifft, ist nach einem weiteren Urteil des Bundesverwaltungsgerichts[75] im Hinblick auf die dafür anfallenden Gebühren auch dann als einheitliche Amtshandlung anzusehen, wenn die Behörde mit mehreren Bescheiden über den Antrag entschieden hat. Eine mehrfache Gebührenerhebung sei mit dem im Informationsfreiheitsgesetz angelegten Verbot einer abschreckend wirkenden Gebührenerhebung unvereinbar.

Das Informationsfreiheitsgesetz sieht vor, dass ein Anspruch auf Informationszugang nicht besteht, wenn die Information einer durch Rechtsvorschrift geregelten Geheimhaltungs- oder Vertraulichkeitspflicht unterliegt. Hierzu stellt das Bundesverwaltungsgericht[76] fest, dass auch eine Geheimhaltungsregelung in einer Rechtsverordnung vom Begriff der Rechtsvorschrift umfasst ist. Das Informationsfreiheitsgesetz enthalte keine Bestimmung, nach der Geheimhaltungspflichten in vom Parlament verabschiedeten Gesetzen enthalten sein müssten. Der Grundsatz, dass unter der Geltung des Informationsfreiheitsgesetzes geheim bleibt, was nach anderen Vorschriften geheim gehalten werden muss, gelte auch im Hinblick auf Rechtsverordnungen.

Auf der Grundlage des Informationsweiterverwendungsgesetzes erging ein weiteres Urteil des Bundesverwaltungsgerichts.[77] Es kommt zum Ergebnis, dass Informationen, die eine Behörde von sich aus veröffentlicht und damit allgemein zugänglich macht, der Anwendbarkeit des Informationsweiterverwendungsgesetzes unterfallen, und zwar ohne dass ein individueller Informationszugangsanspruch auf der Grundlage beispielsweise eines Informationsfreiheitsgesetzes bestehen muss. Konkret ging es um Ausschreibungstexte für öffentliche Aufträge, die von der zuständigen Stelle über eine von Dritten betriebene Vergabeplattform im Internet veröffentlicht werden. Die Texte müssen im Ergebnis des Urteils unverzüglich nach ihrer Veröffentlichung allen Interessenten zur Verfügung gestellt werden.

1.2 Länder

Die Tendenz, die klassischen, auf einem Antragsverfahren basierenden Informationsfreiheitsgesetze um die Verpflichtung zur aktiven Veröffentlichung von Informationen zu ergänzen, hielt auch im Berichtszeitraum an. Das Hamburgische Transparenzgesetz aus dem Jahr 2012 ist Vorreiter auf diesem Gebiet gewesen. Drei Jahre später wurde das Bremer Informationsfreiheitsgesetz in diesem Sinne novelliert. In Rheinland-Pfalz trat zu Beginn des Jahres 2016 das Landestransparenzgesetz in Kraft.[78] Es sieht – ähnlich wie

75 Urteil des Bundesverwaltungsgerichts vom 20. Oktober 2016, 7 C 6.15.

76 Urteil des Bundesverwaltungsgerichts vom 28. Juli 2016, 7 C 3.15.

77 Urteil des Bundesverwaltungsgerichts vom 14. April 2016, 7 C 12.14.

78 Landestransparenzgesetz (LTranspG) vom 27. November 2015 (GVBl. S. 383).

in Hamburg und Bremen – eine zentrale Transparenz-Plattform vor, auf der ausgewählte Informationen rheinland-pfälzischer Landesbehörden zu finden sein werden. Die Plattform wird schrittweise auf- und ausgebaut. Zudem werden Informationen, die von Landesbehörden auf Antrag herausgegeben wurden, auf der Transparenz-Plattform allgemein zugänglich gemacht. Mit dem Landestransparenzgesetz wurden das frühere Landesinformationsfreiheitsgesetz und das Landesumweltinformationsgesetz zusammengeführt; der Landesbeauftragte für den Datenschutz und die Informationsfreiheit ist damit auch für die Kontrolle des Umweltinformationszugangs zuständig.

In Schleswig-Holstein hat der Landtag das Informationszugangsgesetz novelliert.[79] Es verpflichtet die Landesbehörden künftig zur aktiven Veröffentlichung von Informationen und sieht die Einrichtung eines elektronischen Informationsregisters vor. Dieser einem Transparenzgesetz entsprechende Teil der Novellierung wird im Jahre 2020 in Kraft treten.

Seit Beginn des Berichtszeitraums ist in Baden-Württemberg das Landesinformationsfreiheitsgesetz in Kraft.[80] Die Aufgabe des Landesbeauftragten für die Informationsfreiheit wird dort – wie in allen übrigen Ländern mit entsprechenden Gesetzen – vom Landesbeauftragten für den Datenschutz wahrgenommen. Auch das Landesinformationsfreiheitsgesetz Baden-Württemberg enthält Veröffentlichungspflichten für die Landesbehörden.

Der Thüringer Landtag hat die Landesregierung zur Vorlage eines umfassenden Transparenzgesetzes bis zum 31. März 2017 aufgefordert.[81] Zum Redaktionsschluss dieses Tätigkeitsberichts stand dies jedoch noch aus. Das Thüringer Informationsfreiheitsgesetz enthält ebenfalls bereits jetzt gewisse Veröffentlichungspflichten.

Vorsichtige Schritte in Richtung Veröffentlichungspflichten ist das Land Berlin gegangen. Das Abgeordnetenhaus erweiterte die Pflicht, Aktenpläne, Aktenordnungen und dergleichen allgemein zugänglich zu machen, dahingehend, dass diese nunmehr auch im Internet zu veröffentlichen sind.[82] Darüber hinaus hat die neue Regierungskoalition vereinbart, das Berliner Informationsfreiheitsgesetz in Richtung eines Transparenzgesetzes weiterzuentwi-

---

79 Gesetz zur Änderung des Informationszugangsgesetzes für das Land Schleswig-Holstein vom 5. Mai 2017 (GVBl. S. 279).

80 Gesetz zur Regelung des Zugangs zu Informationen in Baden-Württemberg (Landesinformationsfreiheitsgesetz – LIFG) vom 17. Dezember 2015 (GBl. S. 1201).

81 Beschluss des Thüringer Landtags vom 23. Juni 2016: „Stärkung von Informationsfreiheit und Transparenz im Freistaat Thüringen“, Landtags-Drs 6/2369.

82 Viertes Gesetz zur Änderung des Berliner Informationsfreiheitsgesetzes vom 7. Juli 2016 (GVBl. S. 434).

ckeln. Nicht schützenswerte Daten sollen dann in der Regel auf dem Berliner Datenportal zur Verfügung gestellt werden.[83]

Der Landtag Sachsen-Anhalt hat die Landesregierung aufgefordert, das Informationszugangsgesetz weiterzuentwickeln, die Gebührenobergrenze für den Informationszugang zu senken, eine Bagatellgrenze in Höhe von 50 Euro einzuführen sowie das Landesportal um ein Landesinformationsregister zu ergänzen.[84]

Weder über ein Informationsfreiheits- noch über ein Transparenzgesetz verfügen somit nur noch die Länder Bayern, Hessen, Niedersachsen und Sachsen. Dies bedeutet jedoch nicht, dass es dort keine Entwicklung zu verzeichnen gäbe.

Zwar hatte die niedersächsische Landesregierung nach einer ausführlichen Verbändeanhörung bereits den Entwurf eines Transparenzgesetzes beschlossen, das öffentliche Stellen angehalten hätte, möglichst viele Informationen aktiv zu veröffentlichen, und das Grundlage für die Schaffung eines allgemein zugänglichen Informationsregisters gewesen wäre. Der Landesbeauftragten für den Datenschutz wäre nicht nur die Kontrollbefugnis für dieses, sondern auch für das Umweltinformationsgesetz übertragen worden.[85] Aufgrund der vorzeitigen Auflösung des niedersächsischen Landtags kam es jedoch nicht mehr zur Verabschiedung des Gesetzes. Die neue Landesregierung hat in ihrer Koalitionsvereinbarung lediglich die Evaluierung der Erfahrungen anderer Bundesländer mit einem Informationsfreiheits- und Transparenzgesetz verankert, um auf dieser Grundlage über die Einführung eines Informationsfreiheits- und Transparenzgesetzes in Niedersachsen zu entscheiden.[86]

Auf eine ganz ähnliche Formulierung hatten sich die Koalitionspartner in Hessen geeinigt. Inzwischen ist dort eine entsprechende Evaluierung erfolgt. Die Regierungsfraktionen haben daraufhin im Rahmen der Anpassung des hessischen Landesrechts an die Erfordernisse der Datenschutz-Grundverordnung einen Gesetzentwurf für ein hessisches Datenschutz- und

---

83 Koalitionsvereinbarung zwischen Sozialdemokratische Partei Deutschlands (SPD), Landesverband Berlin, und DIE LINKE, Landesverband Berlin, und BÜNDNIS 90/DIE GRÜNEN, Landesverband Berlin, für die Legislaturperiode 2016 – 2021, S. 154.

84 Beschluss des Landtages Sachsen-Anhalt vom 4. Mai 2017 zum Dritten Tätigkeitsbericht des Landesbeauftragten für die Informationsfreiheit für die Zeit vom 1. Oktober 2012 bis 30. September 2014, Landtags-Drs. 7/1363.

85 https://www.stk.niedersachsen.de/aktuelles/presseinformationen/ (Abruf am 20. November 2017).

86 Koalitionsvereinbarung zwischen der Sozialdemokratischen Partei Deutschlands (SPD) Landesverband Niedersachsen und der Christlich-Demokratischen Union (CDU) in Niedersachsen für die 18. Wahlperiode des Niedersächsischen Landtages 2017 bis 2022, S. 45.

Informationsfreiheitsgesetz vorgelegt.[87] Dieser sieht einen voraussetzungslosen Informationszugangsanspruch gegenüber den Landesbehörden vor; den Kommunen wird die Entscheidung über die Anwendung des Informationszugangsrechts überlassen. Bundesweit einzigartig wäre die Zusammenführung der beiden Rechtsmaterien Datenschutz und Informationsfreiheit in einem einheitlichen Gesetz.

Die Entscheidung des Sächsischen Landtages über einen Entwurf für ein Gesetz über die Transparenz von Informationen im Freistaat Sachsen[88] steht noch aus. Die Regierungsfraktionen hatten sich in ihrem Koalitionsvertrag auf ein Informationsfreiheitsgesetz verständigt.[89]

Während der Freistaat Bayern sich im vorigen Berichtszeitraum nur zu einem das dortige Datenschutzgesetz ergänzenden Auskunftsrecht durchringen konnte,[90] das vom Antragsteller die Darlegung eines berechtigten, nicht auf eine entgeltliche Weiterverwendung gerichteten Interesses verlangt, hat sich der Trend bayerischer Kommunen fortgesetzt, Informationsfreiheitssatzungen zu erlassen. Inzwischen haben fast 40 Prozent der Einwohner Bayerns ein Akteneinsichtsrecht auf der Grundlage kommunaler Informationsfreiheitssatzungen im Bereich des eigenen Wirkungskreises der Städte und Gemeinden.[91]

1.3 Brandenburg

Die Datenschutz-Grundverordnung, die das geltende Datenschutzrecht ab dem 25. Mai 2018 ersetzen wird, hat nicht nur Auswirkungen auf die Datenschutzgesetze des Bundes und der Länder. Auch das Informationsfreiheitsrecht ist von der Datenschutzreform betroffen. Bislang verweist das brandenburgische Akteneinsichts- und Informationszugangsgesetz bezüglich der Kontrollkompetenzen der Landesbeauftragten auf die gegenüber den öffentlichen Stellen im Brandenburgischen Datenschutzgesetz vorgesehenen Kontrollrechte. Da diese durch die Datenschutz-Grundverordnung geändert werden, bedarf es auch einer Anpassung des Informationszugangsrechts. Die Landesregierung beabsichtigt, die bisherigen Kontrollkompetenzen vollständig und inhaltlich unverändert direkt im Akteneinsichts- und Informations-

87 Gesetzentwurf der Fraktionen der CDU und BÜNDNIS 90/DIE GRÜNEN für ein Hessisches Gesetz zur Anpassung des Hessischen Datenschutzrechts an die Verordnung (EU) Nr. 2016/679 und zur Umsetzung der Richtlinie (EU) Nr. 2016/680 und zur Informationsfreiheit, Landtags-Drs. 19/5728.

88 Gesetzentwurf der Fraktion BÜNDNIS 90/DIE GRÜNEN. Gesetz über die Transparenz von Informationen im Freistaat Sachsen. Landtags-Drs. 6/10209.

89 Koalitionsvertrag 2014 bis 2019 zwischen der CDU Sachsen und der SPD Sachsen, S. 106.

90 Tätigkeitsbericht 2014/2015, C 1.3.

91 https://informationsfreiheit.org/ubersicht/ (Abruf am 20. November 2017).

zugangsgesetz zu regeln, sodass ein Rückgriff auf das Datenschutzrecht künftig nicht mehr erforderlich ist.[92]

Mit demselben Gesetzentwurf plant die Landesregierung, eine Lücke im bestehenden Akteneinsichts- und Informationszugangsgesetz zu schließen. Das Gesetz ermächtigt die Landesregierung bislang, im Benehmen mit dem Ausschuss für Inneres des Landtages die Gebührentatbestände und die Höhe der Gebühren durch Rechtsverordnung (Gebührenordnung) zu bestimmen. Da sich der Wortlaut auf die Gebühren beschränkt, fehlt es an einer Ermächtigung, auch die Kostenerhebung für Auslagen zu regeln. Vor dem Hintergrund einer vergleichbaren Rechtslage auf Bundesebene hatte das Bundesverwaltungsgericht die Rechtswidrigkeit der entsprechenden bundesrechtlichen Befugnis zur Erhebung von Auslagen festgestellt.[93] Künftig soll die Auslagenerhebung in Brandenburg von der Ermächtigung zum Erlass von Kostenregelungen umfasst sein. Die Entscheidung des Landtages über einen entsprechenden Gesetzentwurf stand zum Redaktionsschluss dieses Berichts noch aus.

Weitere gesetzgeberische Aktivitäten des Landtags Brandenburg auf dem Gebiet des Akteneinsichts- und Informationszugangsgesetzes waren im Berichtszeitraum nicht zu verzeichnen. Befremdlich ist, dass im Rahmen der Anpassung an die Datenschutz-Grundverordnung ausgerechnet eine Gesetzeslücke geschlossen werden soll, welche die Kosten für die Informationsfreiheit betrifft und das Land begünstigt. Die zahlreichen von den Bürgern hinzunehmenden Defizite, die von der Landesbeauftragten bereits in der Vergangenheit geltend gemacht wurden, blieben weiterhin unberücksichtigt.

Weder eine Weiterentwicklung des Akteneinsichts- und Informationszugangsgesetzes zu einem Transparenzgesetz noch eine Ergänzung des Gesetzes um aktive Veröffentlichungspflichten sind in Brandenburg derzeit zu erwarten. Dasselbe gilt für eine angemessene Berücksichtigung der sich aus dem Umweltinformationsrecht ergebenden Herausforderungen[94] sowie für die Erweiterung des Anwendungsbereichs des Akteneinsichts- und Informationszugangsgesetzes auf juristische Personen des Privatrechts, die öffentliche Aufgaben wahrnehmen und der Kontrolle durch öffentliche Stellen unterliegen. Die Ausnahmetatbestände vom Anwendungsbereich sowie zum Schutz überwiegender öffentlicher Interessen bleiben unverhältnismäßig streng und zahlreich und eine Interessenabwägung im Einzelfall bleibt weiterhin in vielen

92 Entwurf der Landesregierung für ein Gesetz zur Anpassung des Allgemeinen Datenschutzrechts an die Verordnung (EU) 2016/679 und zur Umsetzung der Richtlinie (EU) 2016/680 (Landtags-Drs. 6/7365).

93 Urteil des Bundesverwaltungsgerichts vom 20. Oktober 2016, 7 C 6.15.

94 Siehe hierzu C 9.

Fällen versagt. Auch die Vorschriften zum Umgang mit Unternehmensdaten gehören auf den Prüfstand.

Angesichts der beschriebenen Entwicklungen in anderen Ländern bleibt völlig offen, ob und wie das Land Brandenburg gedenkt, seine ursprüngliche Vorreiterrolle als erstes Land, das sich ein Akteneinsichts- und Informationszugangsgesetz gegeben hat, auch nur annähernd wieder zu erlangen.

Von den im Berichtszeitraum ergangenen Gerichtsentscheidungen zum Akteneinsichts- und Informationszugangsgesetz sind zwei Entscheidungen des Oberverwaltungsgerichts Berlin-Brandenburg besonders erwähnenswert.

Das Oberverwaltungsgericht hat in einem Klageverfahren gegen einen Sozialversicherungsträger (eine Körperschaft des öffentlichen Rechts), der neben Brandenburg noch für zwei weitere Länder zuständig ist, die Ausnahme des § 2 Abs. 3 Akteneinsichts- und Informationszugangsgesetz differenziert ausgelegt.[95] Nach dieser Ausnahme vom Anwendungsbereich des Akteneinsichts- und Informationszugangsgesetzes ist der Anspruch gegenüber Verwaltungseinrichtungen des Landes, deren Zuständigkeitsbereich sich auch auf andere Bundesländer erstreckt, auf die Akten beschränkt, die sich ausschließlich auf das Land Brandenburg beziehen. In Bezug auf den beklagten Sozialversicherungsträger komme, so das Oberverwaltungsgericht, diese Ausnahme jedoch nicht zum Tragen. Die Akten führende Stelle sei nicht unmittelbar in den Verwaltungsaufbau eingegliedert, eine Weisungsbefugnis gegenüber dem Träger bestehe nicht und die Rechtsaufsicht liege ohnehin beim Land Brandenburg. Der Schutzzweck der Ausnahmevorschrift, nämlich die Wahrung der Hoheitsrechte der beteiligten Länder, sei somit nicht erfüllt. Eine weitere, ebenfalls strittige Ausnahme von der Anwendbarkeit des Gesetzes für Stellen, die nach § 2 Abs. 5 Nr. 1 Akteneinsichts- und Informationszugangsgesetz am Wettbewerb teilnehmen, sei zudem eng auszulegen. Die Voraussetzungen lägen nicht bereits vor, wenn eine im Wirtschaftsverkehr tätige öffentliche Institution im Wettbewerb mit Dritten steht. Die Ausnahmeregelung sei vielmehr nur einschlägig, wenn die erbetene Information selbst Wettbewerbsrelevanz hat.

In einer weiteren Entscheidung[96] stellte das Oberverwaltungsgericht Berlin-Brandenburg fest, dass sich eine gegenteilige Auslegung des Begehrens verbiete, wenn eine rechtskundige Person ausdrücklich erklärt, dass sie ihren Antrag nicht auf das Akteneinsichts- und Informationszugangsgesetz stützt. Ohne vorherige Klärung dieser Situation habe die beklagte Behörde nicht von der Begründung eines Verwaltungsrechtsverhältnisses ausgehen und einen

95 Urteil des Oberverwaltungsgerichts Berlin-Brandenburg vom 14. Juli 2016, 12 B 33.14.

96 Beschluss des Oberverwaltungsgerichts Berlin-Brandenburg vom 6. Juli 2016, 12 N 18.16.

Bescheid auf der Grundlage des Akteneinsichts- und Informationszugangsgesetzes erlassen dürfen.

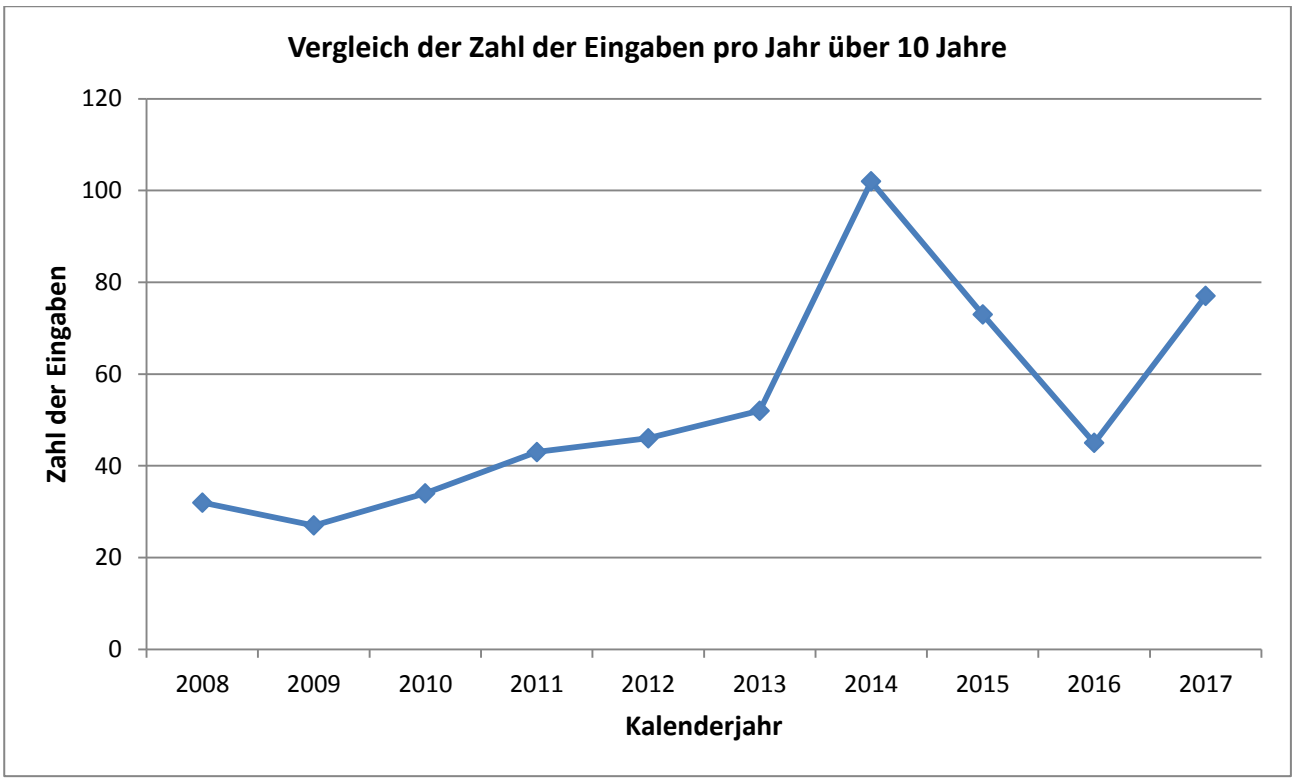
2 Eingaben bei der Landesbeauftragten

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. Da die Statistik jahresweise erstellt wird, beziehen sich die Angaben im Wesentlichen auf das Jahr 2017, nicht auf den gesamten Berichtszeitraum.

Nach ihrem Höchststand im Jahr 2014 (102 Eingaben) hatte sich die Zahl der Beschwerden im darauf folgenden Jahr bereits erheblich reduziert; eine ähnliche Entwicklung war im Jahr 2016 zu verzeichnen. Seither stieg die Zahl der Beschwerden jedoch wieder erheblich an, und zwar um 71 Prozent auf 77 Vorgänge im Jahr 2017.

Der massive Anstieg der Beschwerden im Jahr 2014 war mit einer verstärkten Nutzung der Internet-Plattform www.fragdenstaat.de einhergegangen. Seinerzeit, also erst ein Jahr nach der Ausweitung von www.fragdenstaat.de auf das Land Brandenburg, hatten 68 Prozent der Petenten ihre Beschwerden über die Plattform eingereicht. Zwischenzeitlich war diese Quote erstaunlicherweise auf nur vier Prozent aller Eingaben (2016) gesunken. Im Jahr 2017 wurden aber wieder 17 Prozent der Eingaben auf diese Weise eingereicht.

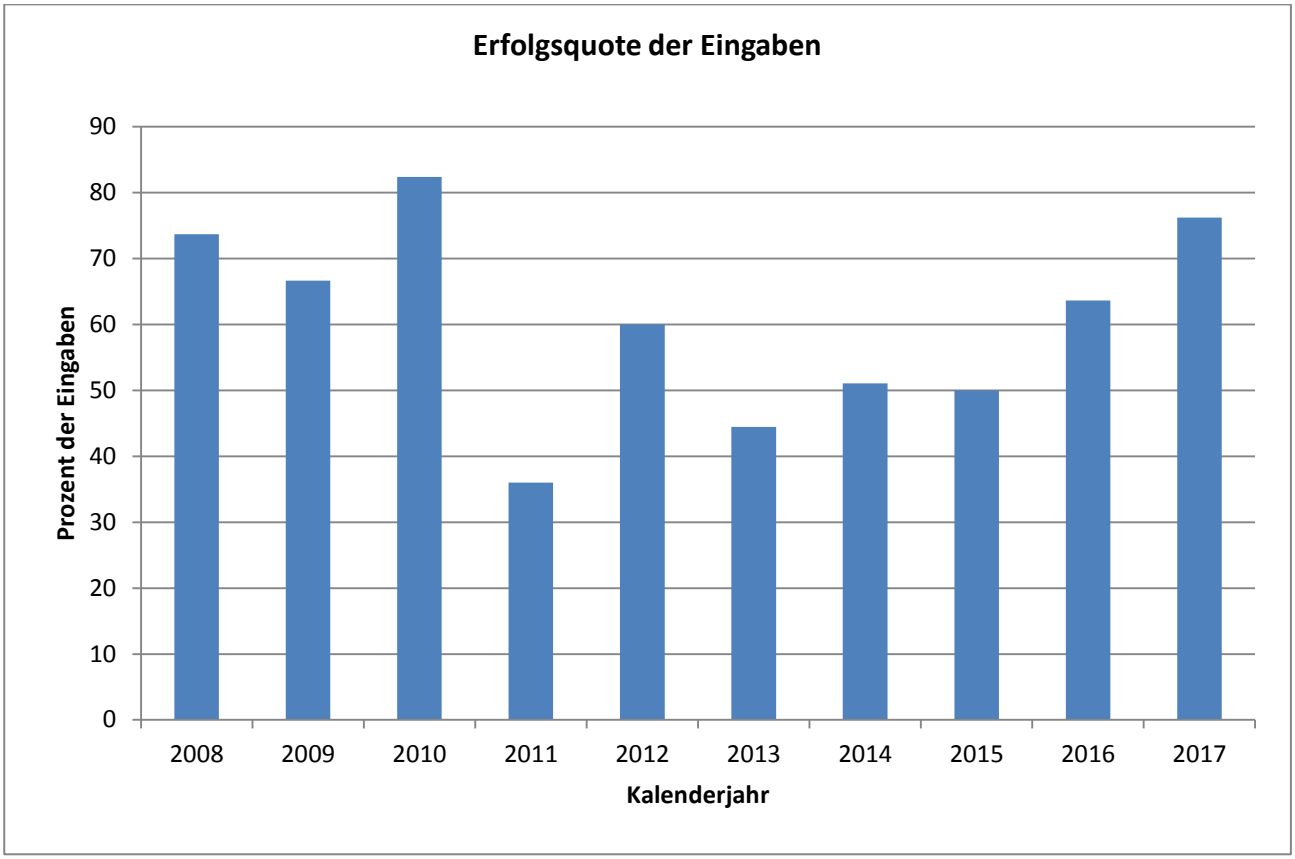


Bereits seit längerer Zeit beobachten wir in unserer täglichen Arbeit, dass informationspflichtige Stellen immer routinierter mit auf der Plattform eingereichten Anträgen auf Akteneinsicht umzugehen verstehen. Die im Vergleich zur Startphase von www.fragdenstaat.de in Brandenburg geringere Beschwerdezahl mag ihre Ursache also auch in der verbesserten Routine der Verwaltungen im Umgang mit der Plattform haben.

Vergleicht man die absoluten Zahlen der Eingaben, die nicht über die Plattform eingereicht wurden, zeigt sich folgendes Bild: 2013 – 46 Eingaben, 2014 – 38 Eingaben, 2015 – 53 Eingaben, 2016 – 43 Eingaben, 2017 – 64 Eingaben.

Lohnt es sich überhaupt, die Landesbeauftragte bei Schwierigkeiten mit der Wahrnehmung des Informationszugangsrechts anzurufen? Im Jahr 2017 ist der Anteil der offenen Fälle von 51 im Vorjahr auf 45 Prozent zurückgegangen. Offen bleiben Fälle zum Beispiel, wenn der Abschluss aufwendigerer oder spät im Jahr gestellter Beschwerden erst im Folgejahr möglich ist. 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 2017 wurde der Informationszugang in 76 Prozent der Beschwerden, deren Ergebnis vorliegt, nach unserem Tätigwerden gewährt. Dies stellt eine erneute Steigerung im Vergleich zu den Vorjah-

reswerten (2016: 64 Prozent, 2015: 50 Prozent) dar. 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.

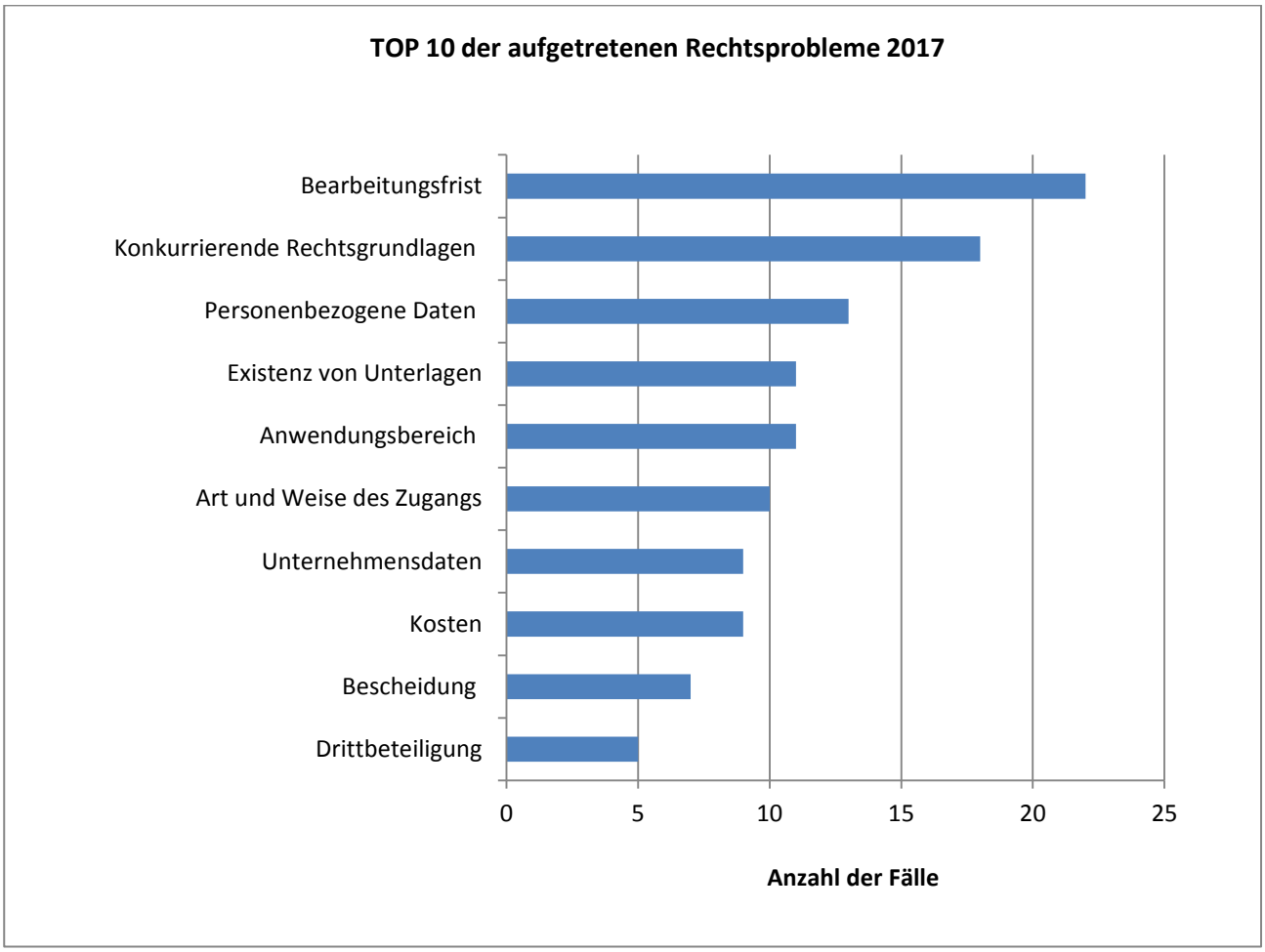


Bei der Beurteilung des Erfolgs macht sich die Statistik den Blickwinkel der Antragsteller zu eigen: Eingaben, in deren Ergebnis die gewünschten Informationen ganz oder teilweise offen gelegt werden, gelten als Erfolg; wird die Offenlegung zu Recht oder auch – aus unserer Sicht – zu Unrecht verweigert, wird dies als Misserfolg verbucht.

Der Dauerbrenner in der Beschwerdepraxis ist nach wie vor die teilweise erhebliche Überschreitung der regelmäßigen, einmonatigen Höchstbearbeitungsfrist für Anträge auf Akteneinsicht durch informationspflichtige Stellen. Häufig hatten wir auch zu klären, welche Rechtsgrundlage für den Informationszugang überhaupt infrage kommt. Nach wie vor stellt das im Falle beantragter Umweltinformationen gegenüber dem Akteneinsichts- und Informationszugangsgesetz vorrangig anzuwendende Umweltinformationsrecht hier den Hauptanwendungsfall dar. Die Frage der Abgrenzung der Rechtsgrundlagen betrifft in geringerem Umfang auch das Verwaltungsverfahrensrecht, das Archivrecht oder Ansprüche aus dem Datenschutzrecht.

In erstaunlich vielen Fällen machten die Verwaltungen geltend, dass die zur Einsicht beantragten Unterlagen überhaupt nicht existierten. Nicht selten

spielten Missverständnisse zwischen Antragsteller und Behörde oder eine mangelnde Bereitschaft, bereits im Vorfeld der Antragstellung oder Entscheidung ein Gespräch zu führen, in diesem Zusammenhang eine Rolle.



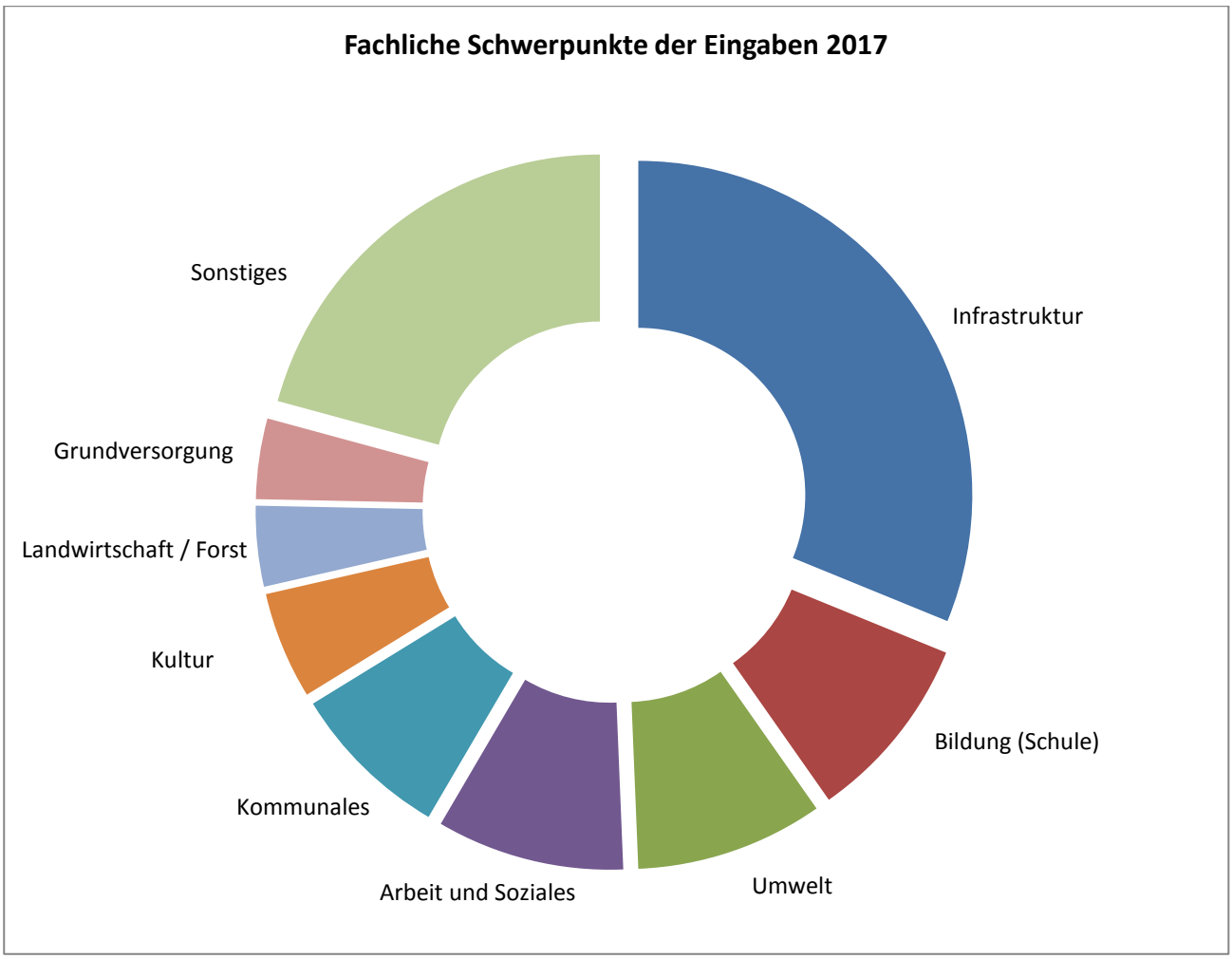
Das Hauptproblem des Vorjahres – der Anwendungsbereich des Akteneinsichts- und Informationszugangsgesetzes – stand im Jahr 2017 erst auf Platz fünf. Dazu gehört auch der Ausschluss von Akteneinsichten aufgrund eines noch nicht abgeschlossenen Verfahrens. Obwohl das Akteneinsichts- und Informationszugangsgesetz mittlerweile seit vielen Jahren ein weitgehendes Wahlrecht des Antragstellers enthält, ob er beispielsweise Kopien erhalten oder Einsicht nehmen möchte, war die Art und Weise des Informationszugangs im Jahr 2017 durchaus weiterhin in zahlreichen Fällen strittig. Dabei ging es auch um die Möglichkeit, Informationen in elektronischer Form zu erhalten. Kosten, also Gebühren und Auslagen für die mit der Bearbeitung des Antrags und der Einsichtnahme selbst verbundene Tätigkeit, waren tendenziell häufiger als zuvor Gegenstand von Beschwerden. Bei Streitigkeiten über die Bescheidung eines Antrags ging es zumeist um das Schriftformerfordernis für einen – auch teilweise – ablehnenden Bescheid sowie um die Notwendigkeit, Ablehnungsgründe darin nachvollziehbar darzulegen.

Im Hinblick auf die materiellen Ausnahmen vom Akteneinsichtsrecht stand der Umgang mit personenbezogenen Daten sowie mit Unternehmensdaten im Vordergrund. Damit hing die Frage von Drittbeteiligungen zusammen – nicht zuletzt die schwer zu vermittelnde Unterscheidung zwischen der Anhörung und der Zustimmung einer betroffenen Person bzw. eines betroffenen Unternehmens.

In den wenigsten Fällen ging es nur um ein einziges der genannten Probleme, d. h. pro Fall waren zumeist mehrere Schwierigkeiten zu verzeichnen.

In welchen Fachbereichen das Einsichtsinteresse der Antragsteller am größten war, lässt sich statistisch nur schwer kategorisieren. Insbesondere bereitet die Zuordnung der Anträge zu einzelnen Themen Schwierigkeiten.

Während in den Vorjahren Informationen zur Verwaltungsorganisation öffentlicher Stellen kurzzeitig auffällig gefragt waren, verebbte das Interesse der Antragsteller an derart internen Informationen im Jahr 2017. Stattdessen kamen die klassischen Prioritäten wieder zum Tragen: An erster Stelle standen erneut infrastrukturelle Aufgaben der öffentlichen Stellen, also vor allem Planen, Bauen, Wohnen und Verkehr. Es folgten die Bereiche Bildung (Schule), Umwelt, Arbeit und Soziales sowie Kommunales.



Dass der Umweltbereich, im dem das Umweltinformationsgesetz regelmäßig vorrangig anzuwenden ist, überhaupt in der Statistik zum Akteneinsichts- und Informationszugangsgesetz erscheint, liegt daran, dass sich in den fraglichen Fällen entweder der Antragsteller oder die Behörde auf das letztgenannte Gesetz berufen haben und daraus Probleme entstanden sind. Aus zahlreichen Anfragen und Gesprächen wissen wir aber, dass auch die Handhabung des Umweltinformationsgesetzes keineswegs reibungslos von statten geht. Für dessen Kontrolle fehlen der Landesbeauftragten aber gesetzliche Kompetenzen. Überschneidungen bestehen im Übrigen auch auf dem Gebiet der Infrastruktur – einige der auf diesem Gebiet erfassten Fälle dürften im Ergebnis dem Umweltinformationsrecht zuzuordnen sein.[97]

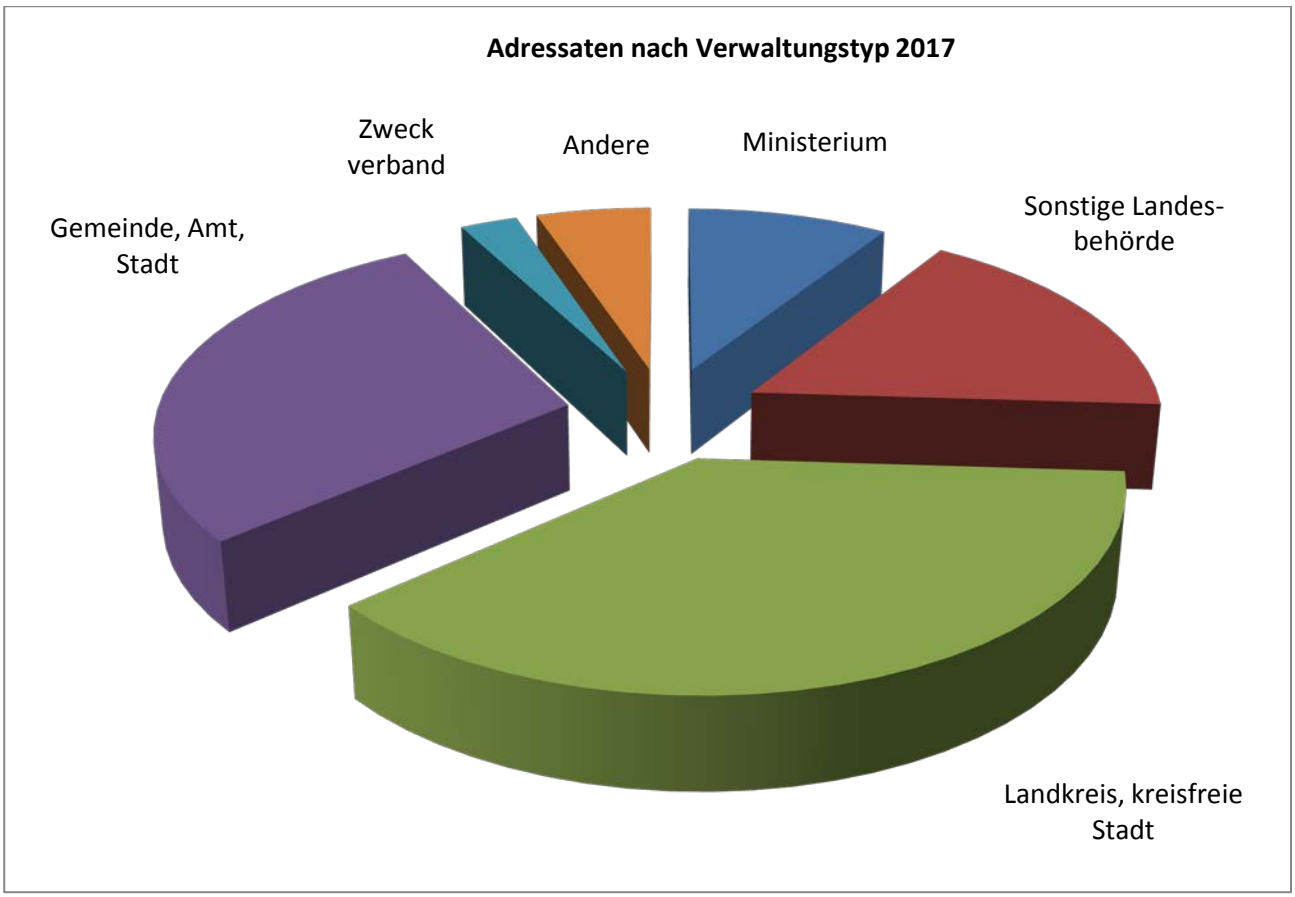
Kommunale Aufgaben gingen in die Statistik nur ein, soweit sie im weitesten Sinne mit kommunalrechtlichen Fragestellungen zusammenhingen, insbesondere in Bezug auf die kommunalen Vertretungskörperschaften. Fachaufgaben, die von den Kommunen erledigt werden, sind davon nicht umfasst.

[97] Zur Bedeutung des weiten Anwendungsbereichs des Umweltinformationsrechts und zur fehlenden gesetzlichen Kompetenzen der Landesbeauftragten auf diesem Gebiet siehe C 9.

Insbesondere im Bereich der Arbeits- und Sozialverwaltung – im Jahr 2017 standen hier besonders die Jobcenter der brandenburgischen Landkreise im Fokus der Antragsteller – bestehen zahlreiche Verwaltungsvorschriften zum Zweck der gleichmäßigen Auslegung sozialrechtlicher Bestimmungen. In der Regel sind diese nicht geheimhaltungsbedürftig. Erfreulich ist, dass immer mehr Verwaltungen dazu übergehen, diese Vorschriften aktiv in ihren Internetangeboten zu veröffentlichen.

Kurz nach Inkrafttreten des Akteneinsichts- und Informationszugangsgesetzes zeigte die Analyse der Eingaben, dass diese zu immerhin einem Drittel aus Beschwerden über Landesministerien bestanden. In den Folgejahren hat sich dieser Anteil wesentlich reduziert. Besonders die Kommunen (Gemeinden, Ämter, Landkreise) sind seither in der Regel Hauptadressat jener Einsichtsanträge, in deren Verlauf eine Eingabe an die Landesbeauftragte gerichtet wird. Dieser Schwerpunkt ist zwar nicht verwunderlich; schließlich werden Entscheidungen, die den Alltag der Bürgerinnen und Bürger unmittelbar prägen, vor allem auf der kommunalen Ebene gefällt. Dennoch fällt hier eine deutliche Steigerung im Vergleich der Vorjahre auf. Richteten sich im Jahr 2015 noch 41 Prozent der Beschwerden gegen Kommunen und Zweckverbände, waren dies im Jahr 2016 bereits 58 Prozent und im Jahr 2017 sogar 70 Prozent. Den Hauptanteil stellten dabei die Verwaltungen der kreisfreien Städte und Landkreise.

Im Jahr 2017 ist die Zahl der Fälle, in denen die Landesbeauftragte um Unterstützung gegenüber Ministerien gebeten wurde, geringfügig von 13 auf 9 Prozent gesunken. Sonstige Landesbehörden schlugen in 17 Prozent der Eingaben zu Buche (2016: 20 Prozent). Die mittelbare Staatsverwaltung – hier waren im Vorjahr insbesondere berufsständische Kammern involviert – spielte im Jahr 2017 überhaupt keine Rolle mehr. Wir werten dies als gutes Zeichen und gehen davon aus, dass die erst seit der Novellierung des Akteneinsichts- und Informationszugangsgesetzes im Jahr 2013 bestehende Anwendbarkeit der Informationsfreiheit auf die mittelbare Staatsverwaltung dort in der Zwischenzeit geräuschlos praktiziert wird.



3 Ausnahmetatbestände einfach mal behaupten

Viel hilft viel, dachte sich eine Stadtverwaltung und fuhr zur Abwehr eines Informationszugangsanspruchs fast sämtliche Ablehnungstatbestände des Akteneinsichts- und Informationszugangsgesetzes auf. Dabei wollte der Antragsteller lediglich die Ausschreibungsunterlagen für die Errichtung einer Brücke sehen, die den Bauunternehmen zum Zweck der Angebotsabgabe zur Verfügung gestellt worden waren.

Der Antragsteller interessierte sich für die an potenzielle Bieter herausgegebenen Ausschreibungsunterlagen zum inzwischen erfolgten Bau einer Brücke. Seinen Antrag wies die Stadtverwaltung als rechtsmissbräuchlich und damit unzulässig zurück. Sie bezog sich auf einen früheren Informationszugangsantrag, den eine Verwandte des Antragstellers und zugleich Eigentümerin des Grundstücks, auf dem die Brücke errichtet wurde, ausgelöst und den die Stadtverwaltung wegen einer unzutreffenden Anschrift abgelehnt hatte. Obwohl die Stadt selbst den Antragsteller aufgefordert hatte, die Zustimmung der Grundstückseigentümerin zur Einsicht in die Ausschreibungsunterlagen beizubringen, hielt sie ihm dies schließlich entgegen. Der Antrag des Petenten umgehe ein von der Grundstückseigentümerin eingeleitetes Klageverfahren; er verfolge kein eigenes Interesse. Der Antrag sei auch

unbegründet, da er nicht hinreichend bestimmt sei und die Behörde daher den Antragsgegenstand sowie eine gegebenenfalls anderweitige Zuständigkeit nicht erkennen könne. Überdies handele es sich um einen unzulässigen Ausforschungsantrag, mit dem sich der Antragsteller einen Überblick über das bei der Stadtverwaltung vorhandene Wissen verschaffen wolle. Dem Begehren nachzugehen, würde die Arbeitsfähigkeit der Verwaltung erheblich beeinträchtigen. Durch die Einsichtnahme in Ausschreibungsunterlagen würde zudem der Schutz personenbezogener Daten, von Urheberrechten sowie von Betriebs- und Geschäftsgeheimnissen verletzt. Insbesondere würde die Einsicht in Ausschreibungsunterlagen interne Kalkulationen der Bieter offenbaren. Da bereits die Grundstückseigentümerin Unterlagen zu ihrem Grundstück eingesehen habe, scheide eine erneute Einsichtnahme durch den Antragsteller aus.

Wir vertraten gegenüber der Stadtverwaltung die Auffassung, dass die Ablehnungsbegründung einer informationszugangsrechtlichen Überprüfung in keiner Weise standhielt. Der voraussetzungslose Anspruch auf Akteneinsicht hat unter anderem zur Folge, dass ein vermutetes Strohmannverhältnis auf der Grundlage des Akteneinsichts- und Informationszugangsgesetzes keine Rolle spielt. Ein Ausforschungsverbot ist dem Gesetz zudem fremd. Angesichts der Umweltrelevanz des Vorgangs machten wir die Stadtverwaltung darauf aufmerksam, dass das Umweltinformationsgesetz im Falle des Vorliegens von Umweltinformationen vorrangig vor dem Akteneinsichts- und Informationszugangsgesetz anzuwenden ist. Ausführlich wiesen wir darauf hin, dass die Akten führende Stelle einen Antrag erst unter Bezugnahme auf die nicht hinreichend erfolgte Bestimmung ablehnen kann, nachdem sie ihrer Verpflichtung nachgekommen ist, den Antragsteller zu beraten und zu unterstützen. Zudem bezweifelten wir, dass die vom Antragsteller ausdrücklich vorgenommene Beschränkung seines Begehrens auf das Ausschreibungsblankett noch einer Konkretisierung bedurfte. Für die Argumentation, die Bearbeitung des Antrags würde die Arbeitsfähigkeit der Verwaltung erheblich beeinträchtigen, sahen wir keinen gesetzlichen Ausnahmetatbestand, zumal die Stadtverwaltung selbst mangels Beratung des Antragstellers nichts dazu beigetragen hatte, eine aus ihrer Sicht erforderliche Konkretisierung des Antrags zu erreichen. Die Tatsache, dass die Stadtverwaltung ihre Ablehnung bereits auf konkrete Schutzinteressen stützte, gleichzeitig aber vorgab, nicht zu wissen, um welche Informationen es dem Antragsteller geht, erschien uns widersprüchlich. Auch die Behauptung der Stadt, die Grundstückseigentümerin habe die fraglichen Unterlagen bereits eingesehen, schien uns angesichts der Argumentation, die Stadt habe gar nicht gewusst, um welche Unterlagen es ging, zweifelhaft. Der pauschale Verweis auf entgegenstehende Schutzinteressen Dritter entsprach schließlich nicht dem Erfordernis einer nachvollziehbaren Begründung, zumal davon auszugehen war, dass eine entsprechende Beteiligung nicht erfolgt war.

Die Stadtverwaltung wies den Widerspruch des Antragstellers zurück. Sie äußerte die Auffassung, dass ihre ursprünglichen Ablehnungsgründe nur unzureichend gewürdigt worden seien, und wiederholte im Wesentlichen die bereits im Ablehnungsbescheid ausgeführte Argumentation. Allerdings argumentierte die Stadt nun nicht mehr mit einem bereits eingeleiteten Klageverfahren der Grundstückseigentümerin, sondern damit, dass das verwaltungsrechtlich an sich vorgesehene Vorverfahren bzw. Klageverfahren umgangen werde. In diesem Zusammenhang führte sie bestehende grundstücksrechtliche Auseinandersetzungen an und machte geltend, es handele sich um ein laufendes Verfahren, das nur Verfahrensbeteiligten zugänglich sei. Inwieweit davon das Ausschreibungsverfahren für die längst erbrachten Bauleistungen betroffen gewesen sein soll, klärte sie nicht. Den materiellen Schutzbedarf der beantragten Informationen beschränkte die Stadt nunmehr auf Betriebs- und Geschäftsgeheimnisse – ohne allerdings zu erläutern, weshalb diese in den vor der Angebotsabgabe versandten Ausschreibungsunterlagen überhaupt vorhanden sein sollen.

Sowohl der Ablehnungs- als auch der Widerspruchsbescheid beließen es mehr oder weniger bei der Aufzählung von Ablehnungstatbeständen, ohne nachvollziehbar zu erläutern, inwieweit diese der Akteneinsicht im konkreten Fall entgegenstehen.

Während des gesamten Verfahrens blieb völlig offen, worin der Geheimhaltungsbedarf für Ausschreibungsunterlagen, in denen noch gar keine Eintragungen der Bieter vorhanden waren, bestehen sollte. Schließlich beanstandete die Landesbeauftragte die genannten Verstöße der Stadtverwaltung gegen das Akteneinsichts- und Informationszugangsgesetz und unterrichtete die Kommunalaufsichtsbehörde hierüber. Sie empfahl eine Neubescheidung des Antragstellers und bat die Stadtverwaltung um eine Stellungnahme. Darin bestand die Stadtverwaltung auf der Rechtmäßigkeit ihres Vorgehens. Unsere Möglichkeiten, den Petenten zu unterstützen, waren damit erschöpft.

Werden gesetzliche Ablehnungstatbestände geltend gemacht, bedarf es einer schriftlichen und nachvollziehbaren Begründung, inwieweit diese dem Informationszugang im konkreten Fall entgegenstehen. Keinesfalls reicht es aus, Ausnahmen nur zu benennen.

4 Öffentlicher Nahverkehr – bitte nicht zu viel Öffentlichkeit!

Ein Landkreis rückte die begehrten Protokolle des ihn beratenden Nahverkehrsbeirates nach langem Hin und Her zwar schließlich heraus, suggerierte dem Antragsteller aber gleichzeitig, dass er über deren Inhalt Stillschweigen zu bewahren habe.

Der Nahverkehrsbeirat begleitet und berät den Landkreis bei der Wahrnehmung seiner Aufgaben nach dem ÖPNV-Gesetz. Ein Bürger beantragte beim Landkreis den Zugang zu den Protokollen dieses Fachbeirats. Darauf erhielt er die Antwort, der Nahverkehrsbeirat tage in nicht öffentlicher Sitzung, weshalb die Übersendung von Sitzungsunterlagen nur an die Mitglieder des Nahverkehrsbeirates erfolge. Weiterhin erging der Hinweis, dass regelmäßig im öffentlichen Teil der Sitzung des Ausschusses für Wirtschaft, Kreisentwicklung, Verkehr und Vergaben des Kreistags des Landkreises über die Themenbereiche des Nahverkehrsbeirates berichtet werde. Hier bestehe die Möglichkeit sich zu informieren.

Um die Angelegenheit bewerten zu können, baten wir den Landkreis um Übersendung einer etwaigen Geschäftsordnung des Nahverkehrsbeirates bzw. um Nennung einer anderen Regelung, die Aussagen zur Nichtöffentlichkeit der Sitzungen des Gremiums trifft. Außerdem wollten wir wissen, welche gesetzlichen Ausnahmetatbestände der Übersendung von Sitzungsunterlagen des Nahverkehrsbeirates an den Antragsteller entgegenstehen. Die Behörde ließ sich an die erbetene Stellungnahme mehrfach erinnern und übersandte schließlich einen 20 Jahre alten Kreistagsbeschluss, dessen Regelungssystematik nach ihrer Auffassung den Willen zur nicht öffentlichen Sitzung verdeutlichte. Um dies zu belegen, führte der Landkreis eine Vorschrift aus der Geschäftsordnung an, welche die Teilnahme von Interessenvertretern oder die Hinzuziehung von Sachverständigen und Auskunftspersonen regelt. Eine solche Regelung sei unnötig, wenn die Sitzungen von vornherein öffentlich wären. Weiterhin führte der Landkreis aus, dass die Geschäftsordnung keine Regelung zur Teilnahme bzw. Einladung der Öffentlichkeit enthalte. Im Ergebnis verstehe der Landkreis die Geschäftsordnung daher so, dass die Sitzungen nicht öffentlich stattzufinden haben. Zudem verwies der Landkreis darauf, dass es in jeder Sitzung des Nahverkehrsbeirates dazu kommen kann, dass betriebswirtschaftliche Daten von Unternehmen des öffentlichen Personennahverkehrs erörtert werden. Weiterhin legte er dar, dass die Ausführungen im öffentlichen Teil der Sitzung des Kreisausschusses, auf dem über die Arbeit und die wesentlichen Themen des Nahverkehrsbeirates informiert wird, für die Bürger denselben Informationswert hätten wie eine Akteneinsicht. Auf gesetzliche Ausnahmetatbestände des

Akteneinsichts- und Informationszugangsgesetzes ging die Behörde nicht ein, sondern hielt an der Ablehnung des Antrages fest.

Wir erläuterten dem Landkreis, dass es für die Frage der Einsehbarkeit von Protokollen der Nahverkehrsbeiratssitzungen nicht entscheidend ist, ob die Sitzungen öffentlich oder nicht öffentlich stattfinden. Vielmehr kommt es darauf an, ob zum Zeitpunkt der Antragstellung Ausnahmetatbestände zum Schutz überwiegender Geheimhaltungsinteressen erfüllt sind. Die Ablehnung eines Antrages ist schriftlich zu begründen, sodass erkennbar wird, welche gesetzlichen Ausnahmetatbestände einer Einsicht entgegenstehen und welche Erwägungsgründe im Einzelnen zugrunde gelegt wurden. Wir baten um Berücksichtigung dieser Hinweise sowie um eine Unterrichtung über das weitere Vorgehen. Wiederum bedurfte es mehrerer Erinnerungen, bis der Landkreis uns antwortete.

Schließlich gewährte der Landkreis dem Antragsteller die Einsicht in die Protokolle des Nahverkehrsbeirates. Allerdings verwehrte er die erbetene Übersendung von Kopien aufgrund eines deutlich höheren, jedoch nicht näher erläuterten Verwaltungsaufwands. Außerdem teilte er dem Antragsteller, der zufällig Gemeindevertreter in einer kreisangehörigen Gemeinde war, mit, dass ihm die Einsichtnahme ausdrücklich in seiner Funktion als gewählter Gemeindevertreter gewährt werde. Der Landkreis suggerierte somit das Vorliegen eines kommunalverfassungsrechtlichen Kontroll- und Informationsanspruchs, der im Verhältnis eines Gemeindevertreters zur Verwaltung eines Landkreises allerdings nicht gegeben ist. Dadurch war der Antragsteller daran gehindert, die Protokolle frei zu verwenden. Denn Gemeindevertreter sind, wenn ihnen auf kommunalverfassungsrechtlicher Grundlage Akteneinsicht gewährt wird, zur Verschwiegenheit verpflichtet. Das Akteneinsichts- und Informationszugangsgesetz hingegen kennt eine solche Beschränkung nicht. Zudem blieb offen, ob und inwieweit möglicherweise Ausnahmetatbestände des Akteneinsichts- und Informationszugangsgesetzes der vollständigen Herausgabe der Protokolle entgegenstehen. Nur eine Entscheidung des Landkreises, die ausdrücklich auf dem Akteneinsichts- und Informationszugangsgesetz beruht, lässt eine rechtssichere, freie Verwendung zu. Diese entspricht im Übrigen auch dem Ziel des Verfassungs- und Gesetzgebers des Landes Brandenburg, die Teilhabe an den politischen Mitgestaltungsrechten zu verbessern.

Wir fragten daher bei der Behörde nach der Rechtsgrundlage für das Vorgehen. Der Landkreis teilte mit, sich nicht weiter erklären zu wollen. Schließlich beanstandete die Landesbeauftragte die Verstöße des Landkreises gegen das Akteneinsichts- und Informationszugangsgesetz. Dies betraf auch die trotz bestehender Unterstützungspflicht und mehrfacher Aufforderung zunächst nur zögerliche, unvollständige und schließlich ausbleibende Beantwortung von Fragen, die zur Bewertung des Falls relevant waren. Die Landesbe-

auftragte unterrichtete das Ministerium des Innern und für Kommunales des Landes Brandenburg als Aufsichtsbehörde über die Beanstandung und empfahl eine Bescheidung des Antragstellers unter Berücksichtigung der oben erläuterten Rechtslage.

Die Kritikpunkte der Landesbeauftragten arbeitete der Landkreis vollständig ab und sicherte zu, künftig das Justiziariat zum Zweck der Qualitätssicherung mit Anträgen auf Informationszugang zu befassen. Er erstellte einen neuen Bescheid und lehnte die Akteneinsicht nunmehr unter Bezugnahme auf den Ausnahmetatbestand des Akteneinsichts- und Informationszugangsgesetzes zum Schutz der Willensbildung ab. Zwischenzeitlich lehnte der Kreistag eine Beschlussvorlage ab, mit der die Öffentlichkeit der Sitzungen des Nahverkehrsbeirats gefordert worden war.

Informationen, die auf der Grundlage des Akteneinsichts- und Informationszugangsrecht herausgegeben werden, kann ein Antragsteller in der Regel beliebig verwenden. Bei Akteneinsichten auf der Grundlage von Vorschriften, die nur für einen beschränkten Personenkreis gelten, ist dies oft nicht der Fall. Deshalb kommt es wesentlich darauf an, dass die jeweils einschlägige Regelung zur Entscheidung über den Informationszugang herangezogen wird.

5 Von Missverständnissen und solchen, die gar keine sind

Eine Stadtverwaltung lehnte einen Antrag auf Informationszugang ab. Bis zum Schluss ging sie davon aus, der Antrag richte sich auf möglicherweise schützenswerte Protokolle einer Stadtverordnetenversammlung. Tatsächlich wollte die Antragstellerin aber ganz reguläre Vorgänge der Stadtverwaltung sehen. Nur ein Missverständnis?

Handschriftlich begehrte eine Antragstellerin bei einer Stadtverwaltung Einsicht in die Vorgänge bezüglich der Übertragung von Anlagen durch die Stadt an den zuständigen Wasser- und Abwasserzweckverband. In ihrem Ablehnungsbescheid gab die Stadtverwaltung zunächst den Antrag mit einem ganz anderen Gegenstand (Protokolle nicht öffentlicher Sitzungen der Stadtverordnetenversammlung anstatt Vorgänge der Stadtverwaltung) wieder und hielt den Anwendungsbereich des Akteneinsichts- und Informationszugangsgesetzes nicht für eröffnet, da es sich um ein laufendes Verfahren handele. Außerdem überwiege hinsichtlich nicht öffentlicher Sitzungsprotokolle das Geheimhaltungsinteresse, da die Antragstellerin keine Schädigung vorweisen

könne, welche die angestrebte Prüfung eines Amtshaftungsanspruchs begründen könnte.

Wir erkundigten uns bei der Stadtverwaltung, ob die abweichende Bezeichnung des Einsichtsbegehrens das Ergebnis einer – in Zweifelsfällen verpflichtenden – Beratung der Antragstellerin gewesen sei, und baten außerdem um Informationen zu dem geltend gemachten, laufenden Verfahren. Wie in solchen Fällen üblich, baten wir anhand informationszugangsrechtlicher Hinweise um eine Überprüfung der Angelegenheit sowie um eine Stellungnahme. Nachdem wir an diese erinnert hatten, teilte die Stadtverwaltung mit, an ihrer ablehnenden Entscheidung festhalten zu wollen. Sie bezog sich dabei auf eine angebliche Empfehlung der Kommunalaufsicht zu der Vorschrift des Akteneinsichts- und Informationszugangsgesetzes, die den Umgang mit Protokollen aus nicht öffentlicher Sitzung regelt. Auf unsere Fragen und Hinweise ging sie nicht ein. Wir baten die Stadtverwaltung daher erneut, uns mitzuteilen, aus welchem Grund sie der Auffassung war, dass das öffentliche Geheimhaltungsinteresse das Einsichtsinteresse der Antragstellerin überwiegt. Außerdem erbaten wir die Übersendung einer Kopie der erwähnten Empfehlung der Kommunalaufsichtsbehörde. Nachdem die Stadtverwaltung fernmündlich mitteilte, über unser erstes Schreiben nicht mehr zu verfügen, übersandten wir dieses erneut, mussten aber wiederum an eine Beantwortung erinnern.

Schließlich bekräftigte die Stadtverwaltung ihre ablehnende Entscheidung, die sie nunmehr ausschließlich auf den Schutz nicht öffentlicher Sitzungen stützte. Sie stellte die Empfehlung der Kommunalaufsichtsbehörde zur Verfügung, die zwar die Einschätzung der Stadt teilte, dass eine Einsichtnahme der Sitzungsprotokolle abzulehnen sein dürfte, dem Anschein nach von dem eigentlichen Gegenstand des Einsichtsantrags aber gar nicht in Kenntnis gesetzt worden war.

Die zögerliche bzw. unvollständige Unterstützung der Landesbeauftragten durch die Stadtverwaltung erschwerte unsere informationszugangsrechtliche Bewertung der Angelegenheit. Auf der Grundlage der vorliegenden Informationen hielten wir den Ablehnungsbescheid, der sich auf den später gar nicht mehr geltend gemachten Ausnahmegrund eines laufenden Verfahrens stützte, für fehlerhaft. Bezüglich der Sitzungsprotokolle bemängelten wir, dass eine Darlegung der Abwägung zwischen dem Einsichtsinteresse der Antragstellerin und dem öffentlichen Geheimhaltungsinteresse ebenso wie jede weitere nachvollziehbare Ablehnungsbegründung fehlte. Vor allem aber wiesen wir darauf hin, dass der Schutz von Sitzungsprotokollen sich keineswegs auf Unterlagen richtet, die mit der Erörterung eines Sachverhalts durch die Stadtverordnetenversammlung im Zusammenhang stehen, sondern vielmehr ausschließlich auf den Verlauf der Erörterung selbst. Angesichts der Diskrepanz zwischen dem von der Petentin und der Behörde benannten

Antragsgegenstand bemängelten wir das Ausbleiben der verpflichtenden Beratung der Antragstellerin. Die Landesbeauftragte beanstandete die genannten Verstöße der Stadtverwaltung gegen das Akteneinsichts- und Informationszugangsgesetz und empfahl eine Neubescheidung der Antragstellerin. Zudem bat sie um eine Stellungnahme und informierte die Kommunalaufsichtsbehörde.

Unser Eindruck, dass sich die Stadtverwaltung auch für abwegige Argumentationen nicht zu schade war und dass die gesamte Ablehnungsbegründung entweder auf Missverständnissen oder vorgeblichen Missverständnissen basierte, bestätigte sich im weiteren Verlauf. Die Behörde wies die Beanstandung der Landesbeauftragten nämlich zurück und behauptete, ihr läge ein Antrag der Petentin auf Einsicht in Vorgänge der Stadtverwaltung gar nicht vor. Merkwürdigerweise gab sie in ihrem ursprünglichen Ablehnungsbescheid aber das Datum genau dieses Antrags an. Daraufhin übersandten wir der Stadt eine Kopie des uns vorliegenden Antrags und baten sie darum, uns im Gegenzug eine Kopie des ihr vorliegenden Antrags zwecks ergänzender Prüfung zu übersenden, falls es sich wider Erwarten um zwei unterschiedliche Anträge handeln sollte. Abschließend teilte die Stadtverwaltung mit, ihr liege kein zweiter Antrag vor. Sie berief sich auf die Bestandskraft ihres Ablehnungsbescheids.

Die Landesbeauftragte kann zwischen Antragstellern und Verwaltungen vermitteln und letztendlich Verstöße gegen das Akteneinsichts- und Informationszugangsgesetz beanstanden. Eine Weisungsbefugnis hat sie nicht. Gegen die robuste Blockadehaltung einiger weniger öffentlicher Stellen können diese Kompetenzen nichts ausrichten. Den Antragstellern bleibt dann nur die Beschreitung des langwierigen und unter Umständen kostenintensiven Rechtswegs.

6 Geschäfts- und Finanzdaten einer Kammer – Wo ein Wille ist, ist auch ein Weg

Als mittelbare Staatsverwaltung unterliegen Körperschaften des öffentlichen Rechts dem Akteneinsichts- und Informationszugangsgesetz erst seit dessen Novellierung im Jahr 2013. Im letzten Tätigkeitsbericht haben wir ausführlich über Schwierigkeiten berichtet, Informationen von einigen berufsständischen Kammern in Brandenburg zu erhalten. Insgesamt hatte die Landesbeauftragte gegenüber vier Kammern Beanstandungen ausgesprochen. Die Entwicklung im zurückliegenden Berichtszeitraum gibt nunmehr Anlass zur Hoffnung, dass der Informationszugang auch hier bald zum Alltag gehört.

Einen Antrag auf Informationszugang zu ihren Geschäfts- bzw. Finanzdaten sowie zu Angaben über Vergütungen, Nebentätigkeiten und Mandaten der Geschäftsführung beantwortete eine berufsständische Kammer zunächst nicht. Auch unseren Hinweis auf die Anwendbarkeit des Akteneinsichts- und Informationszugangsgesetzes sowie auf dessen bereits deutlich überschrittene Bearbeitungsfrist ignorierte die Kammer. Erst nach zweimaliger Erinnerung sicherte sie eine baldige Beantwortung zu. Diese bestand schließlich darin, einerseits infrage zu stellen, ob die Kammer überhaupt dem Anwendungsbereich des Akteneinsichts- und Informationszugangsgesetzes unterfällt. Andererseits teilte die Kammer mit, Geschäfts- bzw. Finanzdaten aus dem Zeitraum vor der Novellierung des Akteneinsichts- und Informationszugangsgesetzes nicht offenbaren zu wollen, da das Gesetz damals noch keine Geltung gegenüber den Kammern entfaltet habe. Angaben zu Vergütungen, Nebentätigkeiten und Mandaten der Geschäftsführung würden aus Datenschutzgründen – hier berief sich die Kammer auf das Brandenburgische Datenschutzgesetz – unterbleiben; in ihrem Internetangebot seien Jahresabschlüsse und Bilanzen veröffentlicht.

Wir hielten dieses Ergebnis nicht für rechtmäßig. Zwar bezweifelten wir nicht den grundsätzlichen Schutzbedarf der in Rede stehenden personenbezogenen Daten. Dieser ergibt sich jedoch unmittelbar aus dem Akteneinsichts- und Informationszugangsgesetz; ein Rückgriff auf das Brandenburgische Datenschutzgesetz war nicht erforderlich. Wir hielten das Akteneinsichts- und Informationszugangsgesetz zudem auch auf Daten für anwendbar, die vor der Ausweitung des Anwendungsbereichs auf die mittelbare Staatsverwaltung entstanden waren. Soweit auf das – im Übrigen recht umfangreiche – Internetangebot der Kammer verwiesen wurde, hielten wir die Nennung einer genauen Fundstelle für angebracht. Unsere eigene Recherche nach den begehrten Informationen war dort jedenfalls ohne Ergebnis verlaufen. Wir forderten die Kammer auf, die Angelegenheit erneut zu prüfen und uns gegenüber Stellung zu nehmen. Eine Reaktion erfolgte nicht. Im Ergebnis beanstandete die Landesbeauftragte die Verstöße der Kammer gegen das Akteneinsichts- und Informationszugangsgesetz. Das zuständige Ministerium als Aufsichtsbehörde wurde hierüber unterrichtet.

Die Beanstandung entfaltete eine durchaus positive Wirkung. So übersandte die Kammer dem Antragsteller im weiteren Verlauf sämtliche angefragten Geschäfts- bzw. Finanzdaten und versicherte, künftige Anträge mit der erforderlichen Gewissenhaftigkeit beantworten zu wollen. Außerdem sagte sie zu, die Geschäfts- und Finanzdaten künftig in ihrem Internetangebot zu veröffentlichen. Die Herausgabe der Angaben zu Vergütungen, Nebentätigkeiten und persönlichen Mandaten der Geschäftsführung, welcher der Geschäftsführer nicht zustimmte, lehnte die Kammer unter Bezugnahme auf den im Akteneinsichts- und Informationszugangsgesetz geregelten Schutz personenbezogener Daten zulässigerweise ab.

Die aktive Veröffentlichung von Informationen im eigenen Internetangebot ist nicht nur ein geeignetes Instrument zur Förderung der Transparenz. Sie erspart auch die aufwändige Bearbeitung von Anträgen auf Informationszugang. Kurzum: Ein Beispiel, das Schule machen sollte.

7 Mehr Transparenz in brandenburgischen Jobcentern – Zunehmende Veröffentlichung von Weisungen und Arbeitshilfen

Im Land Brandenburg gibt es sieben Optionskommunen, in denen die kommunalen Träger die Grundsicherung der Arbeitssuchenden übernommen haben. Hier ist – anders als bei anderen Landkreisen – nicht die Bundesagentur für Arbeit der zentrale Ansprechpartner, sondern das Jobcenter des jeweiligen Landkreises. Im Gegensatz zur Bundesagentur für Arbeit stellten die Jobcenter der Optionskommunen ihre Weisungen und Arbeitshilfen bislang in der Regel nicht öffentlich zur Verfügung. Um dennoch eine aktive Veröffentlichung dieser Dokumente zu erwirken, nutzten Bürger die Plattform www.fragdenstaat.de und stellten entsprechende Anträge.

In der Regel reagierten die angeschriebenen Jobcenter nicht auf die Anträge, sodass sich die Petenten mit der Bitte um Unterstützung ihres Einsichtsgesuchs an die Landesbeauftragte wandten. So erhielten wir im Berichtszeitraum für sechs der sieben brandenburgischen Optionskommunen Eingaben zu Anträgen auf Akteneinsicht beziehungsweise Veröffentlichung von Weisungen und Arbeitshilfen.

Da in der Regel die im Akteneinsichts- und Informationszugangsgesetz (AIG) festgelegten Bearbeitungsfristen nicht eingehalten wurden, wiesen wir die zuständigen Jobcenter bei der ersten Kontaktaufnahme auf die formalen Bearbeitungskriterien hin. An der Reaktion der Jobcenter wurde zudem deutlich, dass die Anträge aufgrund ihrer Formulierung „alle internen Weisungen und Arbeitshilfen“ oft missverständlich waren. Es war für die Antragsbearbeiter häufig nicht klar, dass die Petenten ausschließlich die Veröffentlichung von Dokumenten begehrten, bei denen ein Bezug zu sozialrechtlich relevanten Sachverhalten vorlag. Im weiteren Verlauf machten wir die Jobcenter darauf aufmerksam, dass wir davon ausgingen, dass es sich bei einer Vielzahl der Weisungen und Arbeitshilfen um Informationen handelt, deren Herausgabe kein Ausnahmetatbestand des Akteneinsichts- und Informationszugangsgesetzes entgegensteht. Zudem wiesen wir die Jobcenter darauf hin, dass sie gemäß § 6 Abs. 1 Satz 5 AIG verpflichtet sind, die Petenten hinsichtlich des Aktenbestandes zu beraten und bei der Formulierung ihres Antrags

zu unterstützen. Es wurde jeweils empfohlen, die begehrten Dokumente entsprechend den Anträgen herauszugeben oder die Dokumente aktiv auf der Internetseite zu veröffentlichen, um so das Verwaltungshandeln der Jobcenter transparenter zu gestalten. Die Veröffentlichung im Internet würde zudem den Aufwand der Behörden für die Bearbeitung von Informationsanträgen reduzieren und potenziellen Antragstellern Kosten ersparen.

Große Bedenken äußerten die Jobcenter hinsichtlich der Herausgabe von Kopien der Dokumente, da sie befürchteten, dass veraltete Versionen kursieren und damit weitere Missverständnisse zwischen Bürgern und dem Jobcenter entstehen könnten. Eine aktive Veröffentlichung der Dokumente auf den Webseiten der Jobcenter kann dieser Befürchtung entgegenwirken. Da die Webseiten jederzeit aktuell gepflegt werden können, ist der Umlauf veralteter Dokumente unwahrscheinlich.

Die Hälfte der beratenen Jobcenter ist unseren Anregungen bisher gefolgt und hat im Internet eine Vielzahl von Weisungen und Arbeitshilfen veröffentlicht und zunächst angekündigte Gebühren, die im Rahmen der Bearbeitung entstanden wären, nicht erhoben. Ein weiteres Jobcenter hat mit der Veröffentlichung bereits begonnen, dies jedoch noch nicht abschließend umgesetzt.

Die aktive Veröffentlichung von Arbeitsanweisungen im eigenen Internetangebot ermöglicht eine große Transparenz sowie eine stetige Kontrolle über die Aktualität der veröffentlichten Dokumente. Zudem können betroffene Bürger Amtsentscheidungen leichter nachvollziehen, sodass gegebenenfalls weitere Nachfragen bei den zuständigen Bearbeitern vermieden werden.

8 Braunkohlegeschäfte in der Lausitz – das Wort auf der Goldwaage

Worum ging es in den Verhandlungen zum Verkauf der Braunkohle-Sparte eines schwedischen Energiekonzerns mit potenziellen Investoren und dem Land Brandenburg? Die zuständige oberste Landesbehörde zierte sich zunächst, Information darüber zur Verfügung zu stellen.

Vor dem Hintergrund des von der Landesregierung begleiteten Verkaufs der Braunkohlegeschäfte der Vattenfall Europe Mining AG an einen tschechischen Investor beantragte eine bekannte Umweltschutzorganisation beim zuständigen Ministerium die Zusendung einer Liste aller hierzu wahrgenommenen Termine sowie sämtlicher Unterlagen und Entscheidungsergebnisse der Gespräche mit dem Verkäufer sowie mit den potenziellen Investoren bzw.

ihren Vertretern. Die Behörde beantwortete die Fragen und übersandte unter Berechnung einer Verwaltungsgebühr eine sorgfältig zusammengestellte Liste der über dreißig stattgefundenen Gesprächstermine. In Bezug auf die Unterlagen und Entscheidungsergebnisse der Gespräche lehnte sie den Antrag jedoch mit der Begründung ab, solche Unterlagen lägen nicht vor. Die Landesregierung sei kein Vertragspartner, und weder ihr noch dem Ministerium käme eine Entscheidungskompetenz in Bezug auf den Verkaufsprozess zu. Somit lägen auch keine Entscheidungsergebnisse vor. Die bisher geführten Gespräche hätten dem Zweck gedient, die Interessen des Landes in Bezug auf den künftigen Betrieb der Braunkohle-Sparte zu betonen. Darüber seien keine Gesprächsvermerke angefertigt worden.

Die politische Bedeutung des in Rede stehenden Verkaufsprozesses für die brandenburgische Wirtschaft und die Entwicklung in der Lausitz war zum Zeitpunkt der Antragstellung allgemein bekannt; die Thematik erfuhr in der Öffentlichkeit und seitens der Berichterstattung in den Medien ein hohes Maß an Aufmerksamkeit. Auch ohne Kenntnis des Aktenbestands der zuständigen obersten Landesbehörde hielten wir es vor diesem Hintergrund sowie angesichts des üblicherweise in der öffentlichen Verwaltung geltenden Gebots der Aktenführung für zumindest außergewöhnlich, dass keinerlei Vermerke oder weitere Unterlagen zu den Gesprächen existieren sollten. Wir wandten uns daher mit der Bitte an das Ministerium, zu prüfen, ob es sich um ein Missverständnis handeln könnte. Das Anliegen des Antragstellers verstanden wir jedenfalls so, dass er sich für sämtliche inhaltlich relevanten Unterlagen interessierte, die dem Ministerium im Zusammenhang mit den Gesprächen vorlagen. Wir haben der Behörde empfohlen, gegebenenfalls mit der Umweltschutzorganisation Kontakt aufzunehmen, um den Gegenstand ihres Einsichtsinteresses mit dem vorhandenen Informationsbestand abzugleichen. In diesem Zusammenhang wiesen wir darauf hin, dass das Akteneinsichts- und Informationszugangsgesetz eine Beratungs- und Unterstützungspflicht vorsieht, falls dem Antragsteller Angaben zur hinreichenden Bestimmung seines Antrags fehlen.

Das Ministerium teilte zwar mit, nicht ausschließen zu können, dass die Wortwahl des Antrages die Intention des Informationszugangsbegehrens nicht in Gänze wiedergibt. Gleichzeitig sah es im Hinblick auf die offensichtliche Sachkunde der Umweltschutzorganisation jedoch keine Hinweise darauf, dass diese einer Beratung und Unterstützung bedurfte. Da der ablehnende Bescheid bereits bestandskräftig war, stellte die Behörde dem Antragsteller aber anheim, einen neuen und gegebenenfalls weiter gefassten Antrag zu stellen.

Der Antragsteller wählte für seinen neuen Antrag eine Formulierung, die sich so eindeutig auf die inhaltlich relevanten Unterlagen zu den Verkaufsgesprä-

chen richtete, dass keine Missverständnisse mehr möglich waren. Im Ergebnis legte das Ministerium die begehrten Informationen offen.

Streit um die Bedeutung von Formulierungen in Anträgen auf Informationszugang kann durch eine kurze Rückfrage ohne großen Aufwand vermieden werden. Gerade wenn die grundsätzliche Interessenlage aller Akteure bekannt ist, verursacht das Beharren auf einer engen Auslegung von Einsichtsbegehren nur eine unnötige Verzögerung der Entscheidung über die Akteneinsicht.

9 Umweltinformationen: Keine Unterstützung durch die Landesbeauftragte

Wenn der Zugang zu Umweltinformationen beantragt wird, verdrängen die Regelungen des Umweltinformationsgesetzes jene des Akteneinsichts- und Informationszugangsgesetzes. Der Landesbeauftragten fehlen dann die gesetzlichen Kompetenzen, um Verwaltungen zu beraten oder Antragsteller zu unterstützen. Weil der Begriff der Umweltinformation inzwischen sehr weit ausgelegt wird, müssen wir in immer mehr Fällen auf unsere Unzuständigkeit verweisen – obwohl es in der Sache genauso um einen voraussetzungslosen Zugang zu Informationen geht. Den Schaden tragen vor allem die Antragsteller.

In der Praxis ist die Frage, ob ein Antrag auf Informationszugang auf der Grundlage des Akteneinsichts- und Informationszugangsgesetzes (AIG) oder des Umweltinformationsgesetzes (VIG) zu bearbeiten ist, keine Formalität. Obwohl es beiden Gesetzen um den Zugang zu Informationen geht, unterscheiden sie sich wesentlich in den Regelungen zu den Anwendungsbereichen, den Ausnahmetatbeständen und den Kosten. Erfahrungsgemäß stehen auf der Grundlage des Umweltinformationsrechts zumeist mehr Informationen aus einer größeren Zahl von informationspflichtigen Stellen zu niedrigeren Kosten zur Verfügung als nach dem Akteneinsichts- und Informationszugangsgesetz. Ein Wahlrecht, welches Gesetz anzuwenden ist, besteht jedoch nicht. Das Umweltinformationsgesetz geht dem Akteneinsichts- und Informationszugangsgesetz vielmehr nach § 1 AIG ausdrücklich vor, soweit sich ein Antrag auf Umweltinformationen richtet.

Im Rahmen der Novellierung des Akteneinsichts- und Informationszugangsgesetzes war die Zusammenführung der Rechtsgrundlagen eine unserer

Hauptforderungen an den Gesetzgeber.[98] Die Landesbeauftragte hat sich mit diesem Anliegen auch an den zuständigen Ausschuss des Landtags Brandenburg gewandt und dort dezidiert das Dilemma für die Antragsteller dargelegt. Sie stehen vor einem Paradoxon: Handelt es sich um allgemeine Informationen, kommt das Akteneinsichts- und Informationszugangsgesetz – mit in den meisten Fällen weniger zugangsfreundlichen Regelungen – zum Tragen. Allerdings können sie auf die Unterstützung durch die Landesbeauftragte rechnen. Beantragen sie Umweltinformationen, ist das Umweltinformationsrecht anzuwenden. Die Antragsteller haben dann zwar in den meisten Fällen einen weitergehenden Informationsanspruch, müssen aber auf die Unterstützung durch die Landesbeauftragte verzichten, da ihr hier keine gesetzlichen Kompetenzen zustehen.[99] Während sie auf dem Gebiet des Datenschutzes die Einhaltung sämtlicher Vorschriften über den Datenschutz kontrolliert, steht ihr auf dem Gebiet der Informationsfreiheit nach § 11 Abs. 2 AIG i. V. m. § 23 Abs. 1 Brandenburgisches Datenschutzgesetz nur die Kontrolle der Einhaltung des Akteneinsichts- und Informationszugangsgesetzes zu. Der Gesetzgeber ist darauf nicht eingegangen. Der Landesbeauftragten bleibt somit in der Regel keine andere Wahl, als auf ihre Unzuständigkeit für das Umweltinformationsrecht zu verweisen. Für Behörden, die sich mit Beratungsersuchen an uns wenden, ist das misslich; für Antragsteller, die eine unbürokratische Vermittlung erwarten, bedeutet es in der Praxis oft den Verzicht auf die begehrten Informationen. Ihnen steht zwar auch ohne Unterstützung durch die Landesbeauftragte die Beschreitung des Rechtsweges offen. Angesichts der nicht unerheblichen Prozess- und Kostenrisiken, vor allem aber wegen der im Hinblick auf zeitkritische Informationen untauglich langen Verfahrensdauer vor den Verwaltungsgerichten stellt dies oft keine praxisgerechte Lösung dar.

Über die Problematik haben wir schon in unserem letzten Tätigkeitsbericht informiert.[100] In ihrer Stellungnahme[101] teilte die Landesregierung unter anderem mit, den von uns vorgebrachten erheblichen Beratungs- und Unterstützungsbedarf für informationspflichtige Stellen nicht zu erkennen, weil er „so von behördlicher Seite auch bislang nicht an die Landesregierung herangetragen“ worden sei. An die Landesbeauftragte, von der viele informationspflichtige Stellen annehmen, sie sei selbstverständlich auch für den Umwel-

98 Stellungnahme der Landesbeauftragten zum Gesetz zur Änderung des Akteneinsichts- und Informationszugangsgesetzes und zur Aufhebung des Personalausweisgesetzes, Anlage 3 der Landtags-Drs. P-AI 5/41-1 sowie Tätigkeitsbericht 2012/2013, A 3.

99 Schreiben der Landesbeauftragten an den Landtagsausschuss für Ländliche Entwicklung, Umwelt und Landwirtschaft vom 26. März 2015 zu Praxisproblemen des Informationszugangsrechts in Brandenburg, Anlage 3 der Landtags-Drs. P-ALUL 6/5.

100 Tätigkeitsbericht 2014/2015, C 1.4.

101 Stellungnahme der Landesregierung zum Tätigkeitsbericht für die Jahre 2014 und 2015 der Landesbeauftragten für den Datenschutz und für das Recht auf Akteneinsicht, Landtags-Drs. 6/4740.

tinformationszugang zuständig, wird ein solcher Bedarf hingegen regelmäßig und intensiv herangetragen. Dass der Landesregierung hier eine vermittelnde Zuständigkeit zukommen könnte, nimmt vermutlich niemand an. Auch der Verweis der Landesregierung darauf, dass Antragsteller nach dem Umweltinformationsrecht einen von der Beschreitung des Verwaltungsrechtswegs unabhängigen Anspruch auf eine nochmalige Überprüfung der Entscheidung durch die informationspflichtige Stelle hätten, geht fehl. Dieser Anspruch bezieht sich ausschließlich auf privatrechtlich organisierte informationspflichtige Stellen, da für diese die Vorschriften der Verwaltungsgerichtsordnung über das Widerspruchsverfahren nicht gelten. Keinesfalls ist diese Vorschrift so zu verstehen, als könne ein Antragsteller unabhängig vom Verwaltungsrechtsweg bei Behörden um eine erneute Überprüfung der Entscheidung bitten. Selbst wenn dies so wäre, ist darauf hinzuweisen, dass es sich im Zweifelsfall um dieselbe Stelle handeln würde, die den Ablehnungsbescheid erstellt hat und nicht um eine unabhängige Kontrollbehörde. Zwar trifft die Feststellung der Landesregierung zu, dass sowohl die öffentlichen als auch die privaten informationspflichtigen Stellen beim Vollzug des Umweltinformationsgesetzes einer Aufsicht bzw. Überwachung unterliegen. Das ist aber eine Tatsache, die auch auf andere Rechtsgebiete zutrifft. Das Vorhandensein institutioneller Hierarchien in der Aufbauorganisation ist keineswegs gleichbedeutend mit der Beauftragung unabhängiger Stellen zum Zweck einer außergerichtlichen Streitschlichtung. Auch wenn die Landesregierung sich bemüht, diese Erkenntnis zu relativieren – eine solche Stelle gibt es schlicht nicht.

Im Verwaltungsalltag verdrängt das speziellere Umweltinformationsrecht das allgemeine Informationszugangsrecht als Anspruchsgrundlage – und damit die Möglichkeit einer Unterstützung durch die Landesbeauftragte – immer häufiger. Den letzten Meilenstein in dieser Entwicklung stellt ein im Berichtszeitraum ergangenes Urteil des Bundesverwaltungsgerichts dar, das ein weites, richtlinienkonformes Verständnis des Begriffs der Umweltinformation nach § 2 Abs. 3 UIG zugrunde gelegt hat.[102] Danach sind Umweltinformationen unter anderem alle Daten über Maßnahmen oder Tätigkeiten, die (wahrscheinlich) Umweltauswirkungen haben oder den Umweltschutz bezwecken. Zu den Maßnahmen gehören etwa politische Konzepte, Rechts- und Verwaltungsvorschriften, Abkommen, Umweltvereinbarungen, Pläne und Programme. Das Bundesverwaltungsgericht hat klargestellt, dass sich eine Maßnahme oder Tätigkeit auf Umweltbestandteile oder -faktoren lediglich auswirken oder wahrscheinlich auswirken muss, um eine Umweltinformation zu sein. Eines unmittelbaren Zusammenhangs der einzelnen Daten mit der Umwelt bedarf es hingegen nicht. Vielmehr ist es gerade Zweck der Transparenz, dass beispielsweise nicht nur zu Ergebnissen, sondern auch zu den in sie einfließenden Faktoren Zugang gewährt wird. Das Gesetz unterscheidet

[102] Urteil des Bundesverwaltungsgerichts vom 23. Februar 2017, 7 C 31.15.

zudem nicht zwischen mittelbaren oder unmittelbaren Auswirkungen einer Maßnahme auf die Umwelt. Für die Eigenschaft einer Umweltinformation genügt also jeglicher Zusammenhang mit der Maßnahme oder Tätigkeit. Von einer Geringfügigkeitsgrenze der Umweltauswirkungen ist keine Rede.

Für die Bearbeitung eines Antrags auf Informationszugang bedeutet das zum einen, dass nicht mehr, wie von uns bislang vertreten, unterschieden werden muss, ob beispielsweise innerhalb einer Projektakte Umwelt- oder allgemeine Informationen vorhanden sind. Vielmehr handelt es sich bei der gesamten Akte um eine Umweltinformation, wenn die entsprechende Projektmaßnahme umweltrelevant ist. Diese Vereinfachung bedeutet zum anderen, dass Informationszugangsansprüche zunehmend in das Umweltinformationsrecht verlagert und damit der Kontrollkompetenz der Landesbeauftragten entzogen werden. Dies steht der Absicht des Gesetzgebers entgegen, eine ausgleichende und bürgernahe Schlichtung in Streitfällen zu erreichen.

Der Landesbeauftragten sind dabei nicht nur die Hände gebunden, wenn es um Unterlagen aus der klassischen Umweltverwaltung geht. Vielmehr müssen Anträge auch dann auf der Grundlage des Umweltinformationsgesetzes bearbeitet werden, wenn beispielsweise Bauangelegenheiten, die Stadt-, Raum- oder Verkehrsplanung oder die Land- und Forstwirtschaft betroffen sind. Gerade Maßnahmen und Tätigkeiten in diesen Bereichen sind es, an denen Bürgerinnen und Bürger ein hohes Interesse haben, da sie deren Auswirkungen oft in ihrer unmittelbaren Nachbarschaft erleben. Ist die Umwelt im Spiel, kommt das Akteneinsichts- und Informationszugangsgesetz somit nur in Ausnahmefällen zum Tragen. Obwohl beide Gesetze im Wesentlichen dasselbe Ziel haben – die Offenlegung von Informationen – entscheidet die formale Frage, welches Gesetz anwendbar ist, darüber, ob die Landesbeauftragte überhaupt tätig werden darf. Dies verhindert nicht nur in vielen Fällen eine bürgernahe Problemlösung, sondern beeinträchtigt auch das Vertrauen der Bürger in die Tätigkeit der Landesbeauftragten, die gezwungen ist, sich auf ihre Unzuständigkeit zurückzuziehen.

Die geschilderte Problematik besteht auch in den meisten anderen Ländern sowie auf Bundesebene. Im Zusammenhang mit der laufenden Evaluierung des Umweltinformationsgesetzes des Bundes hat die Konferenz der Informationsfreiheitsbeauftragten des Bundes und der Länder daher den Bundes- und die Landesgesetzgeber aufgefordert, den Informationsfreiheitsbeauftragten – wo nicht schon geschehen – die Zuständigkeit für das Recht auf Umweltinformationszugang zu übertragen.

Angesichts der zunehmenden Verlagerung von Informationszugangsansprüchen in das Umweltinformationsrecht bleibt es unverständlich, weshalb der Gesetzgeber auf die Möglichkeit einer außergerichtlichen und bürgernahen Streitschlichtung durch die Landesbeauftragte auf diesem Gebiet verzichtet.

Teil D

Die Dienststelle

1 Die Dienststelle

Mit der Datenschutz-Grundverordnung, die am 25. Mai 2018 wirksam werden wird, sind zahlreiche neue Aufgaben und Befugnisse verbunden, die eine personelle Verstärkung der Aufsichtsbehörden zwingend erfordern. Neue Rechtsinstitute wie beispielsweise die Datenschutz-Folgenabschätzung, Akkreditierungs- und Zertifizierungsverfahren, die Anforderungen in Bezug auf Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen, stark erweiterte Beratungspflichten sowie die Pflicht, entsprechend der gesetzlichen Vorgaben Sanktionen zu verhängen, machen die Personalaufstockung in den Datenschutzaufsichtsbehörden unumgänglich. Dies gilt damit auch für meine Dienststelle.

Vor diesem Hintergrund hatte ich im Aufstellungsverfahren für den Doppelhaushalt 2017/2018 insgesamt 15 neue Stellen beantragt. Diese wären aus meiner Sicht erforderlich gewesen, um eine systematische Vorbereitung auf die mit der Datenschutz-Grundverordnung verbundenen neuen Aufgaben und Befugnisse sowie ab Mai 2018 deren Umsetzung sicherzustellen. Auch wenn der Landtag für meine Dienststelle nur einen Stellenzuwachs von acht Stellen – sechs für das Jahr 2017 und zwei für das Jahr 2018 – beschlossen hat, bin ich für diese Stärkung sehr dankbar.

Drei der sechs Stellen für 2017 konnten, wie vorgesehenen, mit Juristen besetzt werden. Im technischen Bereich sieht dies leider etwas anders aus. Hier konnte bisher nur eine der beiden Stellen im höheren Dienst auf Anhieb dauerhaft besetzt werden, die andere wurde nach kurzer Zeit wieder vakant. Für eine weitere Stelle im gehobenen Dienst ist eine Besetzung erst ab dem Jahr 2018 gelungen. Gerade im Bereich der IT-Stellen machen sich der Fachkräftemangel und der Wettbewerbsnachteil des Staates aufgrund seiner zur Privatwirtschaft vergleichsweise niedrigen Bezahlung stark bemerkbar. Umso mehr freue ich mich über die neu gewonnenen, engagierten Mitarbeiter.

Durch den Stellenzuwachs konnte erstmals ein Justiziariat eingerichtet werden. Dies war angesichts der Zunahme der Anordnungen und Bußgeldverfahren sowie damit auch der gerichtlichen Verfahren zwingend erforderlich.

Die Zahl der eingegangenen Beschwerden ist im Berichtszeitraum in allen Arbeitsgebieten erneut gestiegen, besonders bei der Videoüberwachung. Aus diesem Grund bin ich sehr froh, eine weitere Mitarbeiterin im juristischen Bereich befristet beschäftigen zu können.

Mithilfe der neuen Mitarbeiter ist es zwar möglich, den Übergang zur Datenschutz-Grundverordnung sicherzustellen. Allerdings sind auf verschiedenen Arbeitsgebieten bereits jetzt Personalengpässe zu verzeichnen. Dies betrifft insbesondere den Bereich der inneren Sicherheit, in dem der Bundesgesetzgeber verschiedene neue und umfassende Prüfpflichten für die Datenschutzkontrollstellen beschlossen hat. Darüber hinaus hat er durch die Ausschöpfung von Regelungsspielräumen der Datenschutz-Grundverordnung im nationalen Anpassungs- und Umsetzungsgesetz den Aufsichtsbehörden erst kürzlich zusätzliche Aufgaben zugewiesen, z. B. im Rahmen von Akkreditierungsverfahren.

Mit dem Doppelhaushalt 2017/2018 wurden meiner Dienststelle auch Finanzmittel für einen Umzug nach Potsdam bereitgestellt. Nach den vorangegangenen erfolglosen Bemühungen meiner zwei Vorgänger im Amt und meinen eigenen langjährigen Anstrengungen besteht nun endlich die Aussicht für die Dienststelle, in die Landeshauptstadt Potsdam umzuziehen. Der Personalzuwachs der Dienststelle und der damit verbundene Raumbedarf machen den Umzug in ein größeres Gebäude noch einmal dringlicher. Nach den bisherigen Planungen soll mit einem Umzug der Dienststelle nach Potsdam erst im Jahr 2019 zu rechnen sein.

2 Zusammenarbeit mit dem Landtag

Auch im Berichtszeitraum war die Zusammenarbeit mit dem Landtag Brandenburg wieder eng und vertrauensvoll. Mit der Entscheidung für einen Personalzuwachs hat der Landtag gegenüber meiner Dienststelle ein deutliches Signal dafür gesetzt, dass ihm ein starker Datenschutz und damit ein starkes Grundrecht auf informationelle Selbstbestimmung wichtig ist.

Vom Ausschuss für Inneres und Kommunales wurde ich als Sachverständige für Datenschutzfragen zu zwei Anhörungen eingeladen. Im Mai 2017 erläuterte ich in einem Fachgespräch meine Positionen zu Fragen der polizeilichen Videoüberwachung. Im Oktober 2017 wurde ich zum Entwurf eines Kreisneugliederungsgesetzes angehört. In weiteren Sitzungen des Ausschusses beantwortete ich den Abgeordneten Fragen zu datenschutzrelevanten Vorhaben wie beispielsweise dem Gemeinsamen Kompetenz- und Dienstleistungszentrum der Länder Berlin, Brandenburg, Sachsen, Sachsen-Anhalt und Thüringen für Telekommunikationsüberwachung. Weitere Datenschutzthemen wurden im Hauptausschuss beraten, so zum Beispiel der 19. Rundfunkänderungsstaatsvertrag, zu dem ich im April 2016 eine Stellungnahme abgegeben habe.

Mein Tätigkeitsbericht für die Jahre 2014/2015 wurde im zuständigen Ausschuss für Inneres und Kommunales beraten. Das Plenum verabschiedete in seiner Sitzung im Dezember 2016 auf der Grundlage der Ausschussberatungen einen Beschluss mit Forderungen an die Landesregierung zu diesem Bericht.[103]

Im Berichtszeitraum feierte meine Dienststelle im Plenarsaal des Landtags ihr 25-jähriges Gründungsjubiläum.[104] Für die Unterstützung dieser erfolgreichen Veranstaltung und die Erstellung der Festschrift bedanke ich mich bei der Präsidentin des Landtags und seiner Verwaltung.

Meine zweite sechsjährige Amtszeit als Landesbeauftragte endete im Juli 2017. Am 28. Juni 2017 wählte mich der Landtag nach einer öffentlichen Ausschreibung erneut mit großer Mehrheit für weitere sechs Jahre zur Landesbeauftragten für den Datenschutz und für das Recht auf Akteneinsicht. Ich freue mich über das mir damit ausgesprochene Vertrauen und die Fortsetzung der Arbeit mit meinen Mitarbeiterinnen und Mitarbeitern für die Grundrechte auf Datenschutz und Informationsfreiheit im Land Brandenburg.

3 Zusammenarbeit mit anderen Datenschutzbehörden

3.1 Konferenz der Datenschutzbehörden des Bundes und der Länder

In der Vergangenheit trafen sich die unabhängigen Datenschutzbehörden des Bundes und der Länder in der Regel zweimal im Jahr zu einer Konferenz und diskutierten dort über aktuelle Themen des Datenschutzes sowie verabschiedeten Entschließungen, Beschlüsse und Orientierungshilfen. Diese Frequenz reichte im Berichtszeitraum wegen der gravierenden Umwälzungen im Datenschutzrecht nicht mehr aus.

Im Jahr 2016 kam die Datenschutzkonferenz unter dem Vorsitz meines Kollegen Reinhard Dankert aus Mecklenburg-Vorpommern zu insgesamt fünf Konferenzen, zwei regulären Konferenzen und drei Sonderkonferenzen, zusammen. Die Sonderkonferenzen dienten dazu, sich bei wesentlichen Fragen der Umsetzung der Datenschutz-Grundverordnung abzustimmen. Die erste Sonderkonferenz fand bereits im Januar 2016 in Frankfurt am Main statt, noch vor Verabschiedung der Verordnung. Zwei weitere Sonderkonferenzen folgten in Berlin nach deren In-Kraft-Treten.

---

[103] Landtags-Drs. 6/5383-B.

[104] Siehe D 5.1.3.

In ihrer regulären Frühjahrskonferenz im April 2016 in Schwerin verabschiedeten die unabhängigen Datenschutzbehörden des Bundes und der Länder vier Entschließungen und eine Orientierungshilfe. Die Themen der Entschließungen reichten von der Umsetzung der Datenschutz-Grundverordnung über Freiheitsrechte bei der Bekämpfung des Terrorismus, Servicekonten der Verwaltung bis hin zu Wearables und Gesundheits-Apps. Die Orientierungshilfe wurde zu Online-Lernplattformen im Schulunterricht verabschiedet. Zwischen den beiden Hauptkonferenzen verabschiedete die Konferenz zwei weitere Entschließungen. Sie forderte ein Klagerecht für die Datenschutzbehörden zur gerichtlichen Überprüfung von EU-Kommissionsentscheidungen sowie zusätzliche personelle Ressourcen für die Erfüllung der neuen bzw. erweiterten Aufgaben im Zusammenhang mit der Datenschutz-Grundverordnung. Auf ihrer 92. Sitzung im Herbst 2016 in Kühlungsborn verabschiedete die Konferenz zwei Entschließungen. Mit einer Entschließung forderte sie den Bundesinnenminister auf, das Videoüberwachungsverbesserungsgesetz zurückzuziehen. Die zweite Entschließung betraf gravierende Mängel, die bei der gemeinsamen Prüfung der Falldatei Rauschgift aufgedeckt worden waren und forderte zu deren Behebung auf.

Im Jahr 2017 ging der Vorsitz der Konferenz an die Landesbeauftragte für den Datenschutz Niedersachsen, Barbara Thiel, über. Bereits vor der Frühjahrskonferenz in Göttingen verabschiedeten die Datenschutzbehörden vier Entschließungen. Sie betrafen den Einsatz externer Dienstleister durch Berufsgeheimnisträger, den Gesetzesentwurf zur Aufzeichnung von Fahrdaten bei der Nutzung automatisierter Fahrfunktionen in Kraftfahrzeugen, das neue Bundeskriminalamtgesetz sowie die Novellierung des Personalausweisgesetzes. In der 93. Konferenz in Göttingen verabschiedete die Konferenz die Erklärung „Vom Wert des Datenschutzes in der digitalen Gesellschaft“. Eine weitere Entschließung betraf den Einsatz von Videokameras zur biometrischen Gesichtserkennung und dessen Risiken. In der Herbstsitzung in Oldenburg wurden Entschließungen zur anlasslosen Vorratsdatenspeicherung von Reisedaten und zur Umsetzung der Datenschutz-Grundverordnung im Medienrecht verabschiedet.

Die Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder verabschiedete im Berichtszeitraum zudem Anwendungshilfen für die Wirtschaft zur Umsetzung der Datenschutz-Grundverordnung. Diese sogenannten Kurzpapiere sollen Verantwortlichen in jenen Fällen Hilfestellungen anbieten, in denen die Artikel-29-Datenschutzgruppe noch keine Leitlinien verabschiedet hat.

3.2 Zusammenarbeit mit weiteren Stellen

Nachdem mein langjähriger Berliner Amtskollege, Dr. Alexander Dix, im Januar 2016 in den Ruhestand gegangen ist, konnte die traditionell enge

Zusammenarbeit mit der dortigen Datenschutzbehörde unter der neuen Beauftragten für Datenschutz und Informationsfreiheit, Maja Smoltczyk, fortgesetzt werden. In regelmäßigen Kooperationsgesprächen stimmten wir uns beispielsweise über die Telekommunikationsüberwachung in dem derzeitigen, gemeinsam genutzten Zentrum in Berlin oder den Aufbau des neuen Gemeinsamen Kompetenz- und Dienstleistungszentrums der Länder Berlin, Brandenburg, Sachsen, Sachsen-Anhalt und Thüringen für Telekommunikationsüberwachung ab. In zahlreichen anderen Aufgabenfeldern arbeiten wir seit Jahren aufgrund von Staatsverträgen, die auch die datenschutzrechtliche Zuständigkeit regeln, eng zusammen.

Auch mit dem Ministerium des Innern und für Kommunales fanden im Berichtszeitraum wieder mehrere Arbeitstreffen statt. Das Ministerium hat die Regelungen für ein Landesgesetz zur Anpassung des allgemeinen Datenschutzrechts an die Datenschutz-Grundverordnung und die EU-Datenschutzrichtlinie für Justiz und Inneres bereits im Entwurfsstadium mit meiner Dienststelle besprochen. Viele meiner Anregungen wurden aufgegriffen. An dieser Stelle möchte ich den Mitarbeiterinnen und Mitarbeitern des Ministeriums ausdrücklich meinen Dank für die konstruktive Zusammenarbeit aussprechen. Das Umsetzungsgesetz befindet sich mittlerweile im Gesetzgebungsverfahren. Auch bei der Anpassung der spezialgesetzlichen Regelungen wurde ich vom Ministerium des Innern und für Kommunales frühzeitig beteiligt.

Im Berichtszeitraum leitete ich als dessen Vorsitzende vier Sitzungen des Beirats Marktwächter Digitale Welt. Der Marktwächter Digitale Welt ist ein auf Verbraucherbeschwerden und empirischen Untersuchungen basierendes Frühwarnsystem der Verbraucherzentralen und des Verbraucherzentrale Bundesverbandes. Eine konstruktive Zusammenarbeit der Datenschutzaufsichtsbehörden und Verbraucherzentralen ist hierbei von besonderer Bedeutung. So erfolgten beispielsweise Untersuchungen von Wearables und dazugehörigen Apps sowohl durch Datenschutzbehörden als auch durch Verbraucherzentralen, die sich hervorragend ergänzt haben. Ich freue mich, dass ich als Beiratsvorsitzende den Dialog zwischen den Beteiligten unterstützen kann.

4 Zusammenarbeit mit anderen Informationsfreiheitsbeauftragten

Die Konferenz der Informationsfreiheitsbeauftragten in Deutschland befasst sich mit aktuellen Fragen des Informationszugangs. Ihr gehören die Beauftragten des Bundes sowie derjenigen Länder an, in denen es ein Informationsfreiheitsgesetz gibt. Baden-Württemberg, dessen Landesinformationsfrei-

heitsgesetz am 1. Januar 2016 in Kraft trat, nahm im Berichtszeitraum erstmals an der Konferenz teil.

Im Jahr 2016 führte die Landesbeauftragte für Datenschutz und Informationsfreiheit Nordrhein-Westfalen, Helga Block, den Vorsitz. Vor dem Hintergrund eines Urteils des Bundesverwaltungsgerichts zur Offenlegung der Ausarbeitungen der Wissenschaftlichen Dienste des Deutschen Bundestages forderte die Konferenz in einer Entschließung die Verwaltungen der Landesparlamente auf, dem Beispiel der Bundestagsverwaltung in Sachen Transparenz und Open Data zu folgen. Der Landtag Brandenburg praktiziert diese Offenheit im Übrigen schon länger, das Landtagspräsidium beschloss inzwischen, auch die vor 2013 entstandenen Gutachten seines Parlamentarischen Beratungsdienstes zu veröffentlichen.

In einer weiteren Entschließung machten die Informationsfreiheitsbeauftragten auf die noch lückenhafte Beteiligung der Länder an dem Bund-Länder-Online-Portal GovData aufmerksam. Die Konferenz kritisierte, dass viele Daten, an deren Veröffentlichung ein großes öffentliches Interesse besteht, noch nicht abrufbar sind und das Potenzial von Open Data ungenutzt bleibt. Sie appellierte an die verbleibenden Länder, der Verwaltungsvereinbarung beizutreten, und forderte alle Vereinbarungspartner zur verstärkten Bereitstellung von Daten auf.

Die Pläne der Bundesregierung für ein Open-Data-Gesetz hielt die Konferenz für unzureichend. Sie forderte in einer Entschließung konkrete Veröffentlichungspflichten und eine Integration der Open-Data-Regelungen in Transparenzgesetze, anstatt separate Gesetze zu schaffen oder die Regelungen den eher informationstechnisch orientierten E-Government-Gesetzen zu überlassen. Bestehende Informationsfreiheitsgesetze sollten entsprechend erweitert werden.

Den Konferenzvorsitz der Informationsfreiheitsbeauftragten übernahm im Folgejahr der Landesbeauftragte für den Datenschutz und die Informationsfreiheit Rheinland-Pfalz, Prof. Dr. Dieter Kugelmann. Unter seiner Leitung forderten die Informationsfreiheitsbeauftragten der Länder den Deutschen Bundestag erneut auf, statt des zwischenzeitlich von der Bundesregierung vorgelegten Entwurfs eines Open-Data-Gesetzes das Informationsfreiheitsgesetz des Bundes zu einem umfassenden Transparenzgesetz zu entwickeln, und konkretisierten ihre Kernforderungen. Da sich die Länder verpflichtet hatten, Open-Data-Gesetze nach dem Beispiel der Bundesregelung zu erlassen, befürchteten sie durch die Ergebnisse auf Bundesebene erhebliche Auswirkungen auf die Landesgesetzgebung. Vor der Bundestagswahl appellierte die Konferenz an alle öffentlichen Stellen in Deutschland, sich ihrer Verantwortung für die Informationsfreiheit bewusst zu sein und durch größtmögliche Transparenz die Bürgerinnen und Bürger in ihrer politischen Wil-

lensbildung zu unterstützen. Damit soll zielgerichtet gestreuten Fehlinformationen aktiv entgegengetreten werden. An eine künftige Bundesregierung richteten sich die Grundsatzpositionen der Landesbeauftragten für die Informationsfreiheit. Sie forderten in diesem Papier unter anderem, die Informationsfreiheit in die Verfassungen aufzunehmen, den Informationszugang in einheitlichen Rechtsgrundlagen zu regeln und zu Transparenzgesetzen weiterzuentwickeln, die vollständige Herausnahme der Nachrichtendienste aus dem Anwendungsbereich sowie weitere unnötige Ausnahmen abzuschaffen und mehr Transparenz in der Drittmittelforschung herzustellen.

Schließlich forderte die Konferenz den Bundes- und die Landesgesetzgeber auf, den Informationsfreiheitsbeauftragten – wo nicht schon geschehen – die Zuständigkeit für die Umweltinformationen zu übertragen. Grund für diesen Appell ist, dass den Beauftragten weder auf Bundesebene noch in den meisten Ländern eine Kompetenz für das Umweltinformationsrecht zusteht und sich ihre Aufgabe deshalb auf den Zugangsanspruch nach dem Informationsfreiheitsgesetz beschränkt. Sie können den Bürgern in einer zunehmenden Zahl von Fällen somit keine Unterstützung bei der Einforderung ihrer Informationsrechte anbieten.

5 Öffentlichkeitsarbeit

5.1 Veranstaltungen der Landesbeauftragten

5.1.1 Der Europäische Datenschutztag

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 Datenschutzbehörden des Bundes und der Länder richten zu diesem Datum stets eine zentrale Veranstaltung aus.

Die zentrale Veranstaltung anlässlich des 10. Europäischen Datenschutztages fand am 28. Januar 2016 in Frankfurt am Main statt. Sie wurde vom Konferenzvorsitzenden des Vorjahres, dem Hessischen Datenschutzbeauftragten, unter dem Thema „Europäisches Datenschutzrecht – Vielfalt in Kohärenz" durchgeführt. Die Veranstaltung stand somit ganz im Zeichen der Reform des europäischen Datenschutzrechts. Sie rückte die Erforderlichkeit einer künftig noch stärkeren Zusammenarbeit nationaler und europäischer Datenschutzbehörden in den Blickpunkt. So wird beispielsweise der Europäische Datenschutzausschuss, dem Vertreter der Aufsichtsbehörden aller Mitgliedstaaten angehören, als neues und unabhängiges Gremium künftig bei

Datenverarbeitungen mit grenzüberschreitenden Auswirkungen zu einheitlichen und verbindlichen Entscheidungen gelangen müssen. Thematisiert wurden außerdem das Verhältnis zwischen der bisherigen Datenschutzrichtlinie und der Datenschutz-Grundverordnung sowie deren Umsetzung in nationales Recht.

Der Konferenzvorsitzende des Jahres 2016, der Landesbeauftragte für Datenschutz und Informationsfreiheit Mecklenburg-Vorpommern, organisierte die zentrale Veranstaltung der Datenschutzbehörden zum 11. Europäischen Datenschutztag, die am 30. Januar 2017 in Berlin stattfand. Sie trug den Titel „Diktatur der Daten? – Privatsphäre und Selbstbestimmung im Zeitalter von Big Data und Algorithmen.“ Anknüpfungspunkt war auch hier das Inkrafttreten der Datenschutz-Grundverordnung. Sie enthält eine Regelung, nach der sich niemand einer Entscheidung unterwerfen muss, die ausschließlich auf einer automatisierten Verarbeitung beruht. Angesichts der technischen Entwicklungen auf den Gebieten Big Data, künstliche Intelligenz und Algorithmen stand auf der Veranstaltung die Frage im Mittelpunkt, ob und wie diese Bestimmung praktisch umgesetzt werden kann.

5.1.2 Brandenburg-Tag am 3. und 4. September 2016 in Hoppegarten

Der 15. Brandenburg-Tag am 3. und 4. September 2016 in Hoppegarten fand auf dem dortigen Rennbahngelände sowie in dessen unmittelbarer Umgebung statt. Im Vergleich zu früheren Landesfesten handelte es sich dabei um ein relativ kompaktes Ausstellungsareal. Zwar blieb der angesichts des attraktiven Programms und der Lage im Zentrum Brandenburgs erwartete Ansturm auf die Veranstaltung aus. Die Landesbeauftragte, die während des gesamten Wochenendes mit mehreren Mitarbeitern in einem Informationszelt präsent war, hatte dennoch umfangreich Gelegenheit, auf alle Bürgeranfragen einzugehen. Reges Interesse bestand an Informationen zum Auskunftsrecht über die eigenen Daten, zum Datenschutz an Schulen, zum Personaldatenschutz und zum Adresshandel. Auch neue Technologien auf dem Gebiet der Near Field Communication, also der Einsatz von RFID in Kleidung oder die Auslesbarkeit von Chip- bzw. Geldkarten und Personalausweisen, waren Gegenstand von Beratungsgesprächen. Ein Preisrätsel zur Sicherheit am eigenen Rechner ermöglichte es, mit Besuchern zu diesem alle Generationen betreffenden Thema ins Gespräch zu kommen.

5.1.3 Festveranstaltung – 25 Jahre Datenschutz im Land Brandenburg

Mit einer Festveranstaltung im Plenarsaal des Landtags beging die Landesbeauftragte am 16. Mai 2017 das 25-jährige Jubiläum der Verabschiedung des Brandenburgischen Datenschutzgesetzes und der damit verbundenen Gründung der Dienststelle. Die Veranstaltung wurde mit einer Begrüßung der

Landesbeauftragten eingeleitet, in der sie die aktuellen Herausforderungen des Datenschutzes hervorhob. Daran schloss sich ein Grußwort der Präsidentin des Landtages Brandenburg, Frau Britta Stark, an, die die Arbeit und Bedeutung der Landesbeauftragten würdigte. Der erste brandenburgische Datenschutzbeauftragte Herr Dr. sc. med. vet. Dietmar Bleyl erinnerte in seiner Rede an die aufregende Gründungszeit der Behörde und schilderte die schwierigen Startbedingungen, unter denen die Dienststelle zunächst arbeiten musste. Der Gegenwart wandte sich die ehemalige Bundesjustizministerin Sabine Leutheusser-Schnarrenberger in ihrer Festrede zu. Sie mahnte insbesondere eine Weiterentwicklung des Grundrechts auf Datenschutz im digitalen Zeitalter an. Umrahmt wurde die Festveranstaltung von musikalischen Darbietungen der Combo #j.in des Evangelischen Gymnasiums Hermannswerder. Die Redebeiträge hat der Landtag Brandenburg dankenswerterweise in einer Festschrift veröffentlicht. Sie steht im Internetangebot der Landesbeauftragten zum Download zur Verfügung.

5.1.4 Tag der offenen Tür im Landtag Brandenburg

Am 1. Juli 2017 veranstaltete der Landtag Brandenburg einen Tag der offenen Tür. In diesem Rahmen hatte die Landesbeauftragte die Möglichkeit, ihre Arbeit bürgernah zu präsentieren. Neben allgemeinen Informationsmaterialien stand Interessierten ein anschauliches Modell zum Thema „Videoüberwachung in der Nachbarschaft“ zur Verfügung, anhand dessen gemeinsam mit Mitarbeitern der Landesbeauftragten die gesetzlichen Rahmenbedingungen erörtert werden konnten. Zudem hatten die Bürger die Möglichkeit, ihr (neu erworbenes) Wissen in einem sich thematisch anschließenden Quiz zu überprüfen. Insgesamt nutzten ca. 5.000 Besucher die Veranstaltung.

5.1.5 Internationales Symposium „Datenschutz und Informationsfreiheit – Widerspruch oder Ergänzung?“ am 28. September 2017

Das 10. Internationale Symposium der Landesbeauftragten fand am 28. September 2017 in Potsdam statt. Das Thema „Datenschutz und Informationsfreiheit – Widerspruch oder Ergänzung?“ wurde während der Konferenz aus verschiedenen Blickwinkeln erörtert.

Zunächst erläuterte eine Vertreterin des Europäischen Datenschutzbeauftragten die Balance zwischen beiden Grundrechten auf der Ebene der Europäischen Union sowie die Bedeutung der Rechtsprechung des Europäischen Gerichtshofs auf diesen Gebieten. Die Informationsfreiheitsbeauftragte Kroatiens stellte das in ihrem Land erst seit wenigen Jahren bestehende Modell zweier getrennter Aufsichtsbehörden vor, das für die Informationsfreiheitsbeauftragte, die gleichzeitig für die Informationsweiterverwendung zuständig ist, harte Sanktionsbefugnisse vorsieht. Aus der Ukraine berichtete Transparency

International über ein zum Zweck der Korruptionsprävention eingeführtes Verfahren zur verpflichtenden und im Ergebnis öffentlichen Vermögensdeklaration durch Beamte und Politiker – ein Verfahren, das nicht zuletzt von internationalen Geldgebern als Voraussetzung für weitere Unterstützungen gefordert wurde. Eine Präsentation aus Albanien stellte eine Plattform vor, die dort vom Beauftragten für Datenschutz und Informationsfreiheit betrieben wird und einem ähnlichen Modell folgt wie die in den meisten Ländern von zivilgesellschaftlichen Organisationen betriebenen Plattformen wie z. B. „Frag den Staat“, „AskTheEU“ oder „WhatDoTheyKnow?“. Anhand ausgewählter internationaler Beispiele zeigte die Stiftung Neue Verantwortung e. V. aus Berlin auf, wie leicht aus vermeintlich anonymisierten Daten, die im Rahmen von Open Data veröffentlicht wurden, durch eine Verknüpfung mit anderen Informationen Rückschlüsse auf die tatsächliche Identität von Personen gezogen werden können. Der Vortrag regte eine über den klassischen Datenschutz hinausgehende ethische, aber auch ganz praktische gesellschaftliche Verständigung über den Umgang mit Daten an. Am Beispiel des Großherzogtums Luxemburg stellte ein Vertreter der dortigen Datenschutzkommission das Thema des Whistleblowings im Spannungsfeld zwischen Datenschutz und Transparenz vor. Er ging dabei auch auf den rechtlichen Schutz von Whistleblowern sowohl auf internationaler und europäischer Ebene als auch durch das luxemburgische Whistleblowing-Gesetz ein und illustrierte die Problematik anhand der LuxLeaks-Affäre. Schließlich berichtete eine Teilnehmerin des Bundeskanzler-Stipendiums der Alexander von Humboldt-Stiftung über ihre Forschungsergebnisse zur Informationsfreiheit in Schweden. Unter der Überschrift „Zu viel Transparenz im digitalen Zeitalter?“ berichtete sie über ein erstaunliches Grundvertrauen der schwedischen Öffentlichkeit in die redliche Verwendung von weitgehend veröffentlichten personenbezogenen Daten der Bürger.

Das Symposium fand auf Deutsch und Englisch mit Simultanübersetzung statt und erfreute sich großen Zuspruchs; sowohl internationale Gäste als auch Teilnehmer aus Brandenburg und weiteren Ländern beteiligten sich an den Diskussionen. Die Plätze waren restlos belegt; bereits im Vorfeld der Veranstaltung konnten wir zahlreiche Anmeldungen nicht mehr entgegennehmen.

5.2 Neue Publikationen der Landesbeauftragten

Gesetzliche Änderungen, die im Berichtszeitraum in Kraft getreten sind, machten die Überarbeitung einiger Publikationen der Landesbeauftragten erforderlich. So wurde die Broschüre zum Verbraucherinformationsrecht in der vierten, aktualisierten Auflage herausgegeben. Die Druckschrift mit dem Text des Bundesdatenschutzgesetzes wurde in einer fünften Auflage aktualisiert. Angesichts der bevorstehenden Anpassung des Bundesrechts an die

Datenschutz-Grundverordnung wird dies die letzte Auflage in dieser Form gewesen sein.

Auf den neuesten Stand hat die Landesbeauftragte auch ihre Faltblätter zu speziellen Datenschutz-Themen gebracht: Tipps und Hinweise zu den Themen „Schulen, Internet und Datenschutz“, „Wissenschaftliche Untersuchungen an Schulen“, „Vom Fingerabdruck bis zur DNA-Analyse“, „RFID-Technologie“, „Digitale Angriffe“, „Ungeziefer aus dem Netz“, „Verräterische Spuren auf Festplatten“ sowie „Meine Datenschutzrechte als Telefonkunde“ sind somit wieder aktuell verfügbar. Angesichts der zunehmenden Fragen rund um das Thema Videoüberwachung hat die Landesbeauftragte ein neues Faltblatt mit dem Titel „Videoüberwachung in der Nachbarschaft – Was ist erlaubt?“ herausgegeben.

Schließlich hat die Landesbeauftragte die Präsentationen der Referenten ihres Internationalen Symposiums, das sie am 28. September 2017 zum Thema „Datenschutz und Informationsfreiheit – Widerspruch oder Ergänzung?“ in Potsdam durchgeführt hat, in Form einer Dokumentation veröffentlicht. Die Tagungsbeiträge sind als zehnter Band in der Reihe „Potsdamer Materialien zu Akteneinsicht und Informationszugang“ erschienen.

Sämtliche gedruckten Publikationen sind im Internetangebot der Landesbeauftragten auch in elektronischer Form verfügbar. Darüber hinaus werden dort weitere Veröffentlichungen angeboten, die wir nicht in Papierform vorhalten.

5.3 Internetangebot der Landesbeauftragten

5.3.1 Aktualisierung des bestehenden Internetangebots

Das gedruckte Datenscheckheft war für lange Zeit ein beliebter „Klassiker“ in der Öffentlichkeitsarbeit der Landesbeauftragten. Es enthielt Vordrucke zu ganz unterschiedlichen Lebenssachverhalten, mit denen Bürger bei Unternehmen oder öffentlichen Stellen ohne großen Aufwand Auskunft zu den über ihre Person gespeicherten Daten beantragen konnten. An das Auskunftsrecht knüpfen weitere Rechte an: In manchen Bereichen, vor allem in der Werbung, können Betroffene die Verarbeitung personenbezogener Daten gänzlich unterbinden. Außerdem besteht gegenüber Behörden und Unternehmen der Anspruch, Daten berichtigen, sperren oder löschen zu lassen, wenn diese falsch sind bzw. sich die Richtigkeit nicht feststellen lässt oder die Daten nicht hätten gespeichert werden dürfen. Auch haben Bürger in manchen Fällen das Recht, der Verarbeitung ihrer Daten zu widersprechen, wenn sie ein besonderes persönliches Interesse darlegen, das der Verarbeitung entgegensteht. All diese Rechte geltend zu machen, war mit den Vordrucken aus dem Datenscheckheft möglich. Nicht nur ist über das Scheckformat

dieser Broschüre die Zeit hinweggegangen. Auch hätten die vielen Änderungen der Rechtslage in einzelnen Lebenssachverhalten immer häufiger einen vollständigen Neudruck erfordert. Die begrenzten personellen Kapazitäten der Landesbeauftragten ließen dies nicht mehr zu; es wäre auch wirtschaftlich nicht mehr vertretbar gewesen. Im Berichtszeitraum hat die Landesbeauftragte daher das Datenscheckheft umfassend überarbeitet und stellt nunmehr in ihrem Internetangebot entsprechende Musterschreiben mit Hinweisen zur jeweiligen Rechtslage ausschließlich in elektronischer Form zur Verfügung.

Die Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder, deren Mitglied die brandenburgische Landesbeauftragte ist, hat im Berichtszeitraum verschiedene Orientierungshilfen herausgegeben:

Die Orientierungshilfe zur datenschutzgerechten Nutzung von E-Mail und anderen Internetdiensten am Arbeitsplatz zeigt den datenschutzrechtlichen Rahmen und Regelungsmöglichkeiten der Nutzung des betrieblichen Internet- und E-Mail-Dienstes durch Beschäftigte auf. Sie soll es Arbeitgebern und Beschäftigten erleichtern, eine klare Regelung im Unternehmen zu erreichen, soweit eine private Nutzung des Internets und/oder des E-Mail-Dienstes erlaubt sein soll. Zudem enthält diese Orientierungshilfe ein Muster für eine Betriebsvereinbarung, Richtlinie oder Anweisung für die private Nutzung von Internet und/oder des betrieblichen E-Mail-Postfachs.

Die Orientierungshilfe zur datenschutzrechtlichen Einwilligungserklärung in Formularen enthält Hinweise zur Formulierung und Gestaltung von schriftlichen Einwilligungserklärungen auf der Grundlage des Bundesdatenschutzgesetzes und elektronischen Texten nach dem Telemediengesetz. Damit sollen Unternehmen, wie beispielsweise Versicherungen oder Banken, in die Lage versetzt werden, in Antragsvordrucken die datenschutzrechtlichen Einwilligungserklärungen rechtssicher zu formulieren und von allgemein geltenden Geschäftsbedingungen erkennbar abzugrenzen.

Die Orientierungshilfe für Online-Lernplattformen im Schulunterricht richtet sich insbesondere an Schulen, die Online-Lernplattformen als Lernmittel einsetzen wollen. Sie sollen sich einen Überblick darüber verschaffen können, welche datenschutzrechtlichen Kriterien Online-Lernplattformen erfüllen müssen. Diese Orientierungshilfe gibt auch deren Anbietern die Möglichkeit, ihr jeweiliges Produkt so zu gestalten oder anzupassen, dass eine Nutzung durch Schulen zulässig ist.

Neben der regelmäßigen Aktualisierung des Internetangebots der Landesbeauftragten war es im Berichtszeitraum erforderlich, der Datenschutz-Grundverordnung auch dort eine ihrer Bedeutung angemessene Geltung zu verschaffen. Gerade in der Vorbereitungszeit zur Umsetzung des neuen Datenschutzrechts galt es, Daten verarbeitenden Stellen praktische Unter-

stützung anzubieten. Informationen zur Datenschutz-Grundverordnung sind nunmehr direkt von der Startseite aus abrufbar.

Hinzuweisen ist auch auf die Verknüpfung unseres Internetangebots mit der zum Redaktionsschluss dieses Tätigkeitsberichts noch in Überarbeitung befindlichen Netzseite der Artikel-29-Datenschutzgruppe. Dieses unabhängige Gremium setzt sich aus Vertretern der nationalen Datenschutzbehörden, dem Europäischen Datenschutzbeauftragten und der Europäischen Kommission zusammen. Seine Hauptaufgaben sind die Beratung der Europäischen Kommission in Datenschutzfragen und die Förderung einer einheitlichen Anwendung der Datenschutzrichtlinie in den Mitgliedstaaten der Europäischen Union sowie in Norwegen, Liechtenstein und Island. Sie veröffentlicht Leitlinien, Empfehlungen und Stellungnahmen, die einen wichtigen Beitrag zur einheitlichen Anwendung der europäischen Datenschutzbestimmungen darstellen.

Ebenfalls größere Aufmerksamkeit widmet das Internetangebot der Landesbeauftragten dem internationalen Datenverkehr. Hier ist vor allem der EU-US Privacy Shield zu nennen, der die frühere Safe-Harbor-Entscheidung der Europäischen Kommission ersetzt. Die Landesbeauftragte bietet hier zwei Formulare an. Betroffene können sich damit über die Verletzung des EU-US Privacy Shields durch ein amerikanisches Unternehmen oder über angenommene Datenzugriffe durch amerikanische Geheimdienste oder Sicherheitsbehörden beschweren.

Im Berichtszeitraum wurde zudem der Internetauftritt des Virtuellen Datenschutzbüros, zu deren Projektpartnern die Landesbeauftragte gehört, runderneuert. Das Virtuelle Datenschutzbüro ist ein Informationsangebot der öffentlichen Datenschutzinstanzen und soll als zentraler Einstiegspunkt für Informationen zum Thema Datenschutz dienen. Die Webseite wurde umfassend überarbeitet, nutzerfreundlicher gestaltet, aber auch konzeptionell neu aufgestellt. Der unübersichtliche Schlagwortkatalog mit zahlreichen Artikeln wurde deaktiviert und durch eine eigene Suchmaschine ersetzt, die Informationen zum Datenschutz in den Internetangeboten der Projektpartner gezielt erschließt. Insgesamt trägt die Umgestaltung dem geänderten Nutzerverhalten im Internet Rechnung und konzentriert sich auf die Bereitstellung eines schnellen und verständlichen Zugangs zu Datenschutzfragen.

5.3.2 Online-Beschwerdeformular

Ab 25. Mai 2018 gelten die Regelungen der Datenschutz-Grundverordnung (DS-GVO). Spätestens bis zu diesem Zeitpunkt muss unsere Dienststelle ein elektronisches Beschwerdeformular bereitstellen.

Jede Aufsichtsbehörde ist nach Art. 57 Abs. 1 Buchst. f DS-GVO verpflichtet, sich mit Beschwerden einer betroffenen Person oder Beschwerden einer Stelle, einer Organisation oder eines Verbandes zu befassen, den Gegenstand der Beschwerde in angemessenem Umfang zu untersuchen und den Beschwerdeführer innerhalb einer angemessenen Frist über den Fortgang und das Ergebnis der Untersuchung zu unterrichten. Gemäß Art. 57 Abs. 2 DS-GVO erleichtert die Behörde das Einreichen von Beschwerden durch Maßnahmen wie etwa die Bereitstellung eines Beschwerdeformulars, das auch elektronisch ausgefüllt werden kann, ohne dass andere Kommunikationsmittel ausgeschlossen werden.

Im Berichtszeitraum haben wir die Voraussetzungen für den Einsatz eines Online-Beschwerdeformulars geschaffen. Wesentlich hierbei ist die Sicherstellung einer Verschlüsselung der übertragenen personenbezogenen Daten. Aus diesem Grund bieten wir für unser Online-Beschwerdeformular eine Transportverschlüsselung sowie eine Ende-zu-Ende-Verschlüsselung an. Bei der Transportverschlüsselung werden die Daten per https-Protokoll zwischen dem Browser des Beschwerdeführers und dem Webserver bei unserem IT-Dienstleister verschlüsselt übertragen. Von dort erfolgt die Datenübermittlung zu uns per E-Mail über das verschlüsselte Landesverwaltungsnetz Brandenburg. Da die Daten vorübergehend entschlüsselt und dann neu verschlüsselt werden, kann ein unbefugter Zugriff auf diese nicht vollständig ausgeschlossen werden. Deshalb empfehlen wir auch dem Beschwerdeführer zusätzlich eine Ende-zu-Ende-Verschlüsselung. In diesem Fall werden die Daten noch vor der Übertragung auf seinem Client verschlüsselt und erst in unserer Dienststelle wieder entschlüsselt. Dieses Verfahren stellt somit die sicherste Methode dar.

Das Online-Beschwerdeformular wird spätestens mit Geltung der Datenschutz-Grundverordnung auf unserer Webseite zu finden sein. Abgefragt werden u. a. Name und Anschrift des Beschwerdeführers, wobei diese Angaben freiwillig sind, um auch anonyme Beschwerden zuzulassen. Dabei muss beachtet werden, dass eine Antwort an den Petenten nur erfolgen kann, wenn eine Kontaktmöglichkeit angegeben wurde. Pflichtangaben sind hingegen Name und Adresse des Beschwerdegegners sowie die Beschwerde selbst, da wir sonst nicht aktiv werden können.

Beschwerdeführer, die das elektronische Webformular nicht verwenden möchten, können sich weiterhin vertrauensvoll per Brief, (verschlüsselter) E-Mail, Telefon oder auch persönlich an uns wenden.

Anlagen

1 Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder – Datenschutzkontrolle öffentlicher Stellen

1.1 94. Konferenz vom 8. bis 9. November 2017 in Oldenburg

1.1.1 Keine anlasslose Vorratsspeicherung von Reisedaten

Der Gerichtshof der Europäischen Union (EuGH) hat in seinem Gutachten vom 26. Juli 2017 (Gutachten 1/15) zum Fluggastdaten-Abkommen der EU mit Kanada die langfristige Speicherung von Fluggastdaten (Passenger Name Records-PNR-Daten) sämtlicher Passagiere für nicht mit der Europäischen Grundrechtecharta vereinbar erklärt und seine Position zu anlasslosen Speicherungen personenbezogener Daten bekräftigt. Er erteilt damit einer anlasslosen Vorratsdatenspeicherung von personenbezogenen Daten erneut eine klare Absage. Die Aussagen des EuGH sind nicht nur auf alle geltenden PNR-Instrumente übertragbar und stellen Anforderungen an die Anpassung des Fluggastdatengesetzes, sie betreffen auch die auf europäischer Ebene angestrebte Einrichtung eines Entry-Exit-Systems (EES) sowie eines EU-weiten Reiseinformations- und -genehmigungssystems (ETIAS), die ebenfalls weitreichende anlasslose Speicherungen beabsichtigen.

Zwar hält der EuGH es grundsätzlich für zulässig, Fluggastdaten automatisiert zu übermitteln und auszuwerten, um Personen zu ermitteln, die eine potentielle Gefahr für die öffentliche Sicherheit darstellen und bei ihrer Einreise einer gewissenhaften Kontrolle unterzogen werden sollen. Das gilt jedoch nicht für sensible Daten, die Rückschlüsse etwa auf die rassische und ethnische Herkunft, religiöse Überzeugungen oder das Sexualleben ermöglichen. Der Übermittlungszweck rechtfertigt auch nicht automatisch die weitere Verwendung und Speicherung der Daten. Die übermittelten Daten haben vielmehr ihren Zweck erfüllt, wenn sich während des Aufenthaltes keine konkreten Anhaltspunkte für geplante terroristische oder andere schwere Straftaten ergeben haben. In diesem Fall sieht der EuGH keine Rechtfertigung für eine weitere Speicherung der Daten.

Das Fluggastdatengesetz, mit dem die Richtlinie (EU) 2016/681 des Europäischen Parlaments und des Rates vom 27. April 2016 über die Verwendung von PNR-Daten zur Verhütung, Aufdeckung, Ermittlung und Verfolgung von terroristischen Straftaten und schwerer Kriminalität umgesetzt wurde, geht

insbesondere durch die Einbeziehung der innereuropäischen Flüge, die im Widerspruch zu dem Grundsatz des freien Personenverkehrs im Schengen-Raum steht, noch über den verpflichtenden Teil der Richtlinie hinaus.

Die Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder (DSK) sieht in den vom EuGH ausgesprochenen Feststellungen zur Rechtslage einen unverzichtbaren Maßstab für die Verordnungsvorschläge zur Einrichtung eines neuen Entry-Exit-Systems (EES) sowie eines EU-weiten Reiseinformations- und -genehmigungssystems (ETIAS).

Mit dem EES sollen alle Ein- und Ausreisen sowie Einreiseverweigerungen von Drittstaatlern in die EU zentral erfasst und für mehrere Jahre gespeichert werden (einschließlich biometrischer Identifizierungsmerkmale). Im ETIAS sollen zum Zwecke der Erleichterung der Grenzkontrollen vorab Daten von einreisewilligen visa-befreiten Drittstaatlern erhoben und ebenfalls für mehrere Jahre zentral gespeichert werden. In beiden Datenbanken sollen also Daten, die im Rahmen der Einreise und Grenzkontrolle erhoben werden, ebenso wie nach dem PNR-Abkommen, ohne konkreten Anlass zentral für einen langen Zeitraum vorgehalten werden. Die Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder hält dies nicht für vertretbar.

Die Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder fordert die jeweils zuständigen Gesetzgeber auf, zeitnah und konsequent sämtliche PNR-Instrumente der EU im Sinne der EuGH-Rechtsprechung nachzubessern, insbesondere das deutsche Fluggastdatengesetz.

Sie fordert die Bundesregierung zudem auf, sich auf europäischer Ebene für eine den Anforderungen der EU-Grundrechtecharta und der Rechtsprechung des EuGH entsprechende Ausgestaltung der angestrebten Systeme EES und ETIAS einzusetzen.

1.1.2 Umsetzung der DSGVO im Medienrecht

Das Inkrafttreten der Datenschutzgrundverordnung (DSGVO) und deren Geltungsbeginn im Mai 2018 verlangt eine Anpassung der medienrechtlichen Datenschutzbestimmungen an die neuen Vorgaben. Dabei muss dem hohen Stellenwert der Meinungs- und Informationsfreiheit sowie der Presse-, Rundfunk- und Medienfreiheit gemäß Art. 5 Grundgesetz (GG) und Art. 11 EU-Grundrechtecharta (GRCh) für die freiheitliche demokratische Grundordnung ebenso Rechnung getragen werden wie dem Recht auf Informationelle Selbstbestimmung gemäß Art. 1 i.V.m. Art. 2 GG und dem Recht auf Schutz personenbezogener Daten gemäß Art. 8 GRCh. Kollisionen der Schutzbereiche der Grundrechte sind im Sinne einer praktischen Konkordanz aufzulösen.

Die Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder weist daher auf die Anpassungsklausel des Art. 85 DSGVO hin. Danach können die Mitgliedstaaten Ausnahmen und Abweichungen von bestimmten Vorgaben der DSGVO normieren, wenn „dies erforderlich ist, um das Recht auf Schutz der personenbezogenen Daten mit der Freiheit der Meinungsäußerung und der Informationsfreiheit in Einklang zu bringen". Das sich daraus ergebende Regel-Ausnahme-Verhältnis bedeutet, dass die Vorgaben der DSGVO grundsätzlich auch auf sämtliche Verarbeitungen personenbezogener Daten zu grundrechtlich besonders geschützten journalistischen, wissenschaftlichen, künstlerischen oder literarischen Zwecken angewendet werden sollen.

Bei der Umsetzung von Art. 85 DSGVO gilt es insbesondere folgende Anforderungen zu beachten:

- Ausnahmen oder Abweichungen von der Anwendung der DSGVO auf die Verarbeitung personenbezogener Daten im journalistischen Bereich müssen notwendig sein, um freie Meinungsäußerung und Informationsfreiheit gemäß Art. 11 GRCh sicherzustellen.

- Einen regelhaften Vorrang der Presse-, Rundfunk- und Medienfreiheit sieht die DSGVO nicht vor. Sie verlangt vielmehr, einen angemessenen Ausgleich zwischen den Grundrechten herzustellen, wenn diese in Widerstreit geraten (vgl. 153. Erwägungsgrund der DSGVO).

- Die Grundsätze des Datenschutzes (Art. 5 DSGVO) müssen hinreichend Beachtung finden. Jedenfalls steht es nicht im Einklang mit dem Recht auf Schutz personenbezogener Daten, wenn die Grundsätze des Datenschutzes im Journalismus in weitem Umfang ausgeschlossen werden. Eine Regelung kann keinesfalls als notwendig i. S. d. DSGVO angesehen werden, wenn sie zum Zwecke der Abwägung mit der Meinungs- und Informationsfreiheit die Transparenzrechte und Interventionsmöglichkeiten für betroffene Personen sowie Verfahrensgarantien über eine unabhängige Aufsicht missachtet.

- Über den eingeräumten Gestaltungsspielraum geht es hinaus, wenn die Verarbeitung personenbezogener Daten durch Hilfsunternehmen zu undifferenziert vom Geltungsbereich der DSGVO ausgenommen wird, ohne dass diese Aktivitäten unmittelbar der journalistischen Tätigkeit dienen. Die Reichweite der journalistischen Tätigkeit bedarf zudem einer Konkretisierung.

- Die künftige Aufsicht über den Datenschutz beim Rundfunk ist unabhängig auszugestalten. Sie bedarf wirksamer Abhilfebefugnisse bei Datenschutzverstößen.

Die Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder fordert daher für die Anpassung von Rundfunk-Staatsverträgen, Presse- und Mediengesetzen:

- Die gesetzlichen Anpassungen i. S. d. Art. 85 DSGVO müssen konkret und spezifisch - bezogen auf die jeweiligen Normen und Vorgaben der DSGVO - Ausnahmen und Abweichungen regeln und diese begründen.

- Bei der Ausübung der jeweiligen Regelungskompetenz ist das europäische Datenschutzrecht zwingend zu beachten. Eine faktische Beibehaltung der bisherigen nationalen Rechtslage würde dem nicht gerecht.

1.2 93. Konferenz vom 29. bis 30. März 2017 in Göttingen

1.2.1 Göttinger Erklärung – Vom Wert des Datenschutzes in der digitalen Gesellschaft

Datenschutz ist zurzeit in aller Munde: Mit der Europäischen Datenschutzreform werden ab Mai 2018 in der ganzen Europäischen Union neue einheitliche Regeln gelten. Gegenwärtig sind die Gesetzgeber in Bund und Ländern mit Hochdruck dabei, das nationale Recht an die Europäischen Vorgaben anzupassen. Zugleich schreitet die Digitalisierung der Gesellschaft mit großen Schritten voran, etwa mit dem Internet der Dinge, der Wirtschaft 4.0 und künstlicher Intelligenz, und fordert die Wahrung des Datenschutzes und die Gewährleistung der Persönlichkeitsrechte heraus. Auch der Staat erweitert fortwährend seine Befugnisse zur Verarbeitung personenbezogener Daten, sei es zur Bekämpfung des Terrorismus und zur Gewährleistung der öffentlichen Sicherheit, sei es bei der Digitalisierung staatlicher Dienstleistungen.

Dabei gerät aber leichtfertig eines aus dem Blick: Datenschutz ist ein Grundrecht, wie die Meinungsfreiheit oder die Eigentumsgarantie. Es bindet alle Staatsgewalten unmittelbar, schützt die Menschenwürde und die freie Entfaltung der Persönlichkeit und kann auch Aspekte der Teilhabe und Chancengleichheit betreffen. Alle gesetzlichen Regelungen, sowie die Geschäftsmodelle und Anwendungen auch im Bereich der Wirtschaft, haben dies zu berücksichtigen. Immer häufiger stellen aber Verantwortliche in Politik und Wirtschaft dieses grundrechtlich geschützte Recht auf informationelle Selbstbestimmung implizit oder sogar explizit in Frage. Datenschutz wird als Hindernis diskreditiert.

Dies betrachtet die Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder mit großer Sorge. Es befremdet sehr, wenn Mitglieder der Bundesregierung und andere Stimmen in der Politik in letzter Zeit immer wieder betonen, es dürfe kein Zuviel an Datenschutz geben und das Prinzip der Datensparsamkeit könne nicht die Richtschnur für die Entwicklung

neuer Produkte sein. Stattdessen wird für eine vermeintliche Datensouveränität geworben, deren Zielrichtung aber im Unklaren bleibt.

Die Konferenz betont, dass Informationen über Personen keine Ware sind wie jede andere und nicht allein auf ihren wirtschaftlichen Wert reduziert werden dürfen. Gerade in Zeiten von Big Data, Algorithmen und Profilbildung bieten die digitalen Informationen ein nahezu vollständiges Abbild der Persönlichkeit des Menschen. Mehr denn je muss daher die Menschenwürde auch im digitalen Zeitalter der zentrale Maßstab staatlichen und wirtschaftlichen Handelns sein. Zu einer menschenwürdigen und freien Entfaltung der Persönlichkeit gehört die freie Selbstbestimmung über das eigene Ich.

„Datensouveränität“ verstanden als eigentumsähnliche Verwertungshoheit kann daher nur zusätzlich zum Recht auf informationelle Selbstbestimmung greifen, dieses jedoch keinesfalls ersetzen.

Die Konferenz fordert daher alle Entscheidungsträger in Politik und Wirtschaft auf, den hohen Wert des Rechts auf informationelle Selbstbestimmung für eine freiheitliche Gesellschaft zu achten und sich nachdrücklich vertrauensbildend für die Persönlichkeitsrechte einzusetzen. Datenschutz stellt kein Hindernis für die Digitalisierung dar, sondern ist wesentliche Voraussetzung für deren Gelingen.

Die Entwicklung datenschutzkonformer IT-Produkte und -Verfahren muss nachhaltig gefördert werden, um den Datenschutz zu einem Qualitätsmerkmal der europäischen Digitalwirtschaft zu machen.

1.2.2 Einsatz von Videokameras zur biometrischen Gesichtserkennung birgt erhebliche Risiken

In Pilotprojekten wird derzeit der Einsatz von Videoüberwachungssystemen erprobt, die erweiterte Möglichkeiten der Verhaltensauswertung und der Identifizierung von Beobachteten bieten. Neben der Mustererkennung steht besonders die biometrische Gesichtserkennung im Fokus dieser Projekte. Dies verschärft die ohnehin schon vorhandene Problematik derartiger neuer Überwachungsverfahren, mit denen „abweichendes Verhalten" erkannt werden soll.[1]

Der Einsatz von Videokameras mit biometrischer Gesichtserkennung kann die Freiheit, sich in der Öffentlichkeit anonym zu bewegen, gänzlich zerstören. Es ist kaum möglich, sich solcher Überwachung zu entziehen oder diese gar zu kontrollieren.

---

1 Siehe auch Entschließung der 83. Konferenz der Datenschutzbeauftragten des Bundes und der Länder „Öffentlich geförderte Forschungsprojekte zur Entdeckung abweichenden Verhaltens im öffentlichen Raum – nicht ohne Datenschutz“.

Anders als bei konventioneller Videoüberwachung könnten Passanten mit dieser Technik nicht nur beobachtet und anhand bestimmter Muster herausgefiltert werden, sondern während der Überwachung anhand von Referenzbildern (Templates) automatisiert identifiziert werden. Damit wird eine dauerhafte Kontrolle darüber möglich, wo sich konkrete Personen wann aufhalten oder bewegen und mit wem sie hierbei Kontakt haben. Ermöglicht wird so die Erstellung von umfassenden Bewegungsprofilen und die Verknüpfung mit anderen über die jeweilige Person verfügbaren Daten.

Neben den genannten massiven gesellschaftspolitischen Problemen bestehen auch erhebliche rechtliche und technische Bedenken gegen den Einsatz solcher Überwachungstechniken. Biometrische Identifizierung arbeitet mit Wahrscheinlichkeitsaussagen; bei dem Abgleich zwischen ermitteltem biometrischen Merkmal und gespeichertem Template sind falsche Identifizierungen keine Seltenheit. Beim Einsatz dieser Technik durch Strafverfolgungsbehörden kann eine falsche Zuordnung dazu führen, dass Bürgerinnen und Bürger unverschuldet zum Gegenstand von Ermittlungen und konkreten polizeilichen Maßnahmen werden. Dieselbe Gefahr besteht, falls sie sich zufällig im öffentlichen Raum in der Nähe von gesuchten Straftätern oder Störern aufhalten.

Es gibt keine Rechtsgrundlage für die Behörden von Bund und Ländern für den Einsatz dieser Technik zur Gefahrenabwehr und Strafverfolgung. Die bestehenden Normen zum Einsatz von Videoüberwachungstechnik erlauben nur den Einsatz technischer Mittel für reine Bildaufnahmen der -aufzeichnungen, nicht hingegen für darüber hinausgehende Datenverarbeitungsvorgänge. Aufgrund des deutlich intensiveren Grundrechtseingriffs, der durch Videotechnik mit erweiterter Auswertung einhergeht, können die bestehenden gesetzlichen Regelungen nicht analog als Rechtsgrundlage herangezogen werden, da sie für einen solchen Einsatz verfassungsrechtlich zu unbestimmt sind.

Nach der Rechtsprechung des Bundesverfassungsgerichts sind Maßnahmen mit großer Streubreite ein erheblicher Grundrechtseingriff. So verlangt das Bundesverfassungsgericht bereits für das automatisierte Erfassen von KFZ-Kennzeichen zwecks Abgleichs mit dem Fahndungsbestand eine normenklare und verhältnismäßige Rechtsgrundlage, die einen anlasslosen und flächendeckenden Einsatz ausschließt. Da bereits die allgemeine Regelung zur Videoüberwachung nicht zur Erfassung von KFZ-Kennzeichen ermächtigt, muss dies erst recht für die viel stärker in die Grundrechte Betroffener eingreifende Videoüberwachung zwecks Abgleichs biometrischer Gesichtsmerkmale einzelner Personen gelten. Ein Einsatz der Videoüberwachung mit Gesichtserkennung darf daher auf derzeitiger Grundlage auch im Rahmen eines Pilotbetriebs nicht erfolgen.

Der europäische Gesetzgeber hat die enormen Risiken dieser Technik für die Privatsphäre erkannt und die Verarbeitung biometrischer Daten zur Identifizierung sowohl in der ab Mai 2018 wirksamen Datenschutz-Grundverordnung als auch in der bis Mai 2018 umzusetzenden Datenschutz-Richtlinie im Bereich Justiz und Inneres nur unter entsprechend engen Voraussetzungen für zulässig erachtet. Wird über den Einsatz dieser Technik nachgedacht, muss der Wesensgehalt des Rechts auf informationelle Selbstbestimmung gewahrt bleiben und es müssen angemessene und spezifische Regelungen zum Schutz der Grundrechte und -freiheiten der Betroffenen vorgesehen werden. Hierzu gehören u. a. eine normenklare Regelung für die Verwendung von Templates, z. B. von Personen im Fahndungsbestand, für den Anlass zum Abgleich des Templates mit den aufgenommenen Gesichtern sowie zum Verfahren zur Zulassung von technischen Systemen für den Einsatz.

Etwaige gesetzliche Regelungen müssten die vorgenannten verfassungs- und europarechtlichen Bedingungen beinhalten und den mit dieser Technik verbundenen erheblichen Risiken für die Freiheitsrechte der Bürgerinnen und Bürger angemessen Rechnung tragen!

1.3 Entschließungen zwischen der 92. und 93. Konferenz

1.3.1 Entschließung vom 16. März 2017: Neues Bundeskriminalamtgesetz – Informationspool beschneidet Grundrechte!

Der „Entwurf eines Gesetzes zur Neustrukturierung des Bundeskriminalamtgesetzes“ (BT-Drs. 18/11326 und 18/11163; BR-Drs. 109/17) ändert das polizeiliche Datenschutzrecht grundlegend und betrifft Polizeibehörden in Bund und Ländern gleichermaßen. Er beschränkt sich nicht darauf, die Vorgaben des Bundesverfassungsgerichts aus dem Urteil vom 20. April 2016 zum Bundeskriminalamtgesetz und aus der neuen EU-Richtlinie zum Datenschutz im Bereich Justiz und Inneres umzusetzen. Tatsächlich nimmt er sogar wichtige Datenschutzregeln und Verfahrenssicherungen zurück, die der Gesetzgeber nach dem Volkszählungsurteil des Bundesverfassungsgerichts geschaffen hatte.

Der Entwurf ändert den bisherigen Informationsverbund für alle Polizeibehörden grundlegend. Dieser ist nicht mehr nach Dateien untergliedert und führt zu unverhältnismäßig weitreichenden Speicherungen. In dieser Form ist dies weder durch das Urteil des Bundesverfassungsgerichts zum BKAG noch durch die EU-Richtlinie zum Datenschutz im Bereich Justiz und Inneres veranlasst. Das Urteil des Bundesverfassungsgerichts fordert, den Zweck der jeweiligen Ermittlungsmaßnahmen bei allen weiteren Schritten zu berücksichtigen, bei denen die ermittelten Daten verwendet werden. Nicht im Einklang damit steht es, Verfahrenssicherungen und datenschutzrechtliche Rahmenbedingungen aufzugeben.

Abzulehnen ist insbesondere der vorgesehene Verzicht auf Errichtungsanordnungen. Diese sind bislang Ausgangspunkt sowohl für datenschutzrechtliche Kontrollen als auch die Selbstkontrolle der Polizeibehörden. In ihnen wird festgelegt, zu welchen Zwecken personenbezogene Daten gespeichert sind. Dies ist eine wesentliche verfassungsrechtliche Vorgabe. Die neuen Regeln führen zu umfassenden themenübergreifenden Verknüpfungen und Abgleichen aller gespeicherten Personen. Sie verkürzen die Kontrollmöglichkeiten der Datenschutzaufsichtsbehörden von Bund und Ländern.

Ebenso sind die künftig durch die geplante „Mitziehautomatik“ erheblich längeren Speicherfristen abzulehnen. Die geplante Neuregelung hat zur Folge, dass alte Speicherungen – auch zu Personen, die lediglich im Verdacht standen, eine Straftat begangen zu haben und die nicht verurteilt wurden – bei jedem neuen Speicheranlass ungeprüft weiter fortgeschrieben werden. Dafür soll es schon genügen, wenn die betroffene Person als Zeuge oder Kontaktperson erneut in Erscheinung tritt. Auch dies verstößt gegen das durch die ständige Rechtsprechung des Bundesverfassungsgerichtes bekräftigte Übermaßverbot.

Die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder fordert daher, den Gesetzentwurf in der parlamentarischen Beratung datenschutzkonform zu überarbeiten!

1.3.2 Entschließung vom 16. März 2017: Gesetzesentwurf zur Aufzeichnung von Fahrdaten ist völlig unzureichend!

Die Bundesregierung hat im Januar 2017 einen Entwurf zur Novellierung des Straßenverkehrsgesetzes (BT-Drs. 18/11300) vorgelegt, um die Nutzung automatisierter Fahrfunktionen auf Deutschlands Straßen zu erlauben. Dabei sollen Fahrdaten aufgezeichnet werden, anhand derer bewertet werden kann, zu welchem Zeitpunkt das Auto jeweils durch den Fahrer oder durch eine „automatisierte Fahrfunktion“ gesteuert wurde und wann ein Fahrer die Aufforderung zur Übernahme der Steuerung erhalten hat. Ebenfalls aufgezeichnet werden sollen Daten zu technischen Störungen automatisierter Fahrfunktionen. Mit den Daten soll sich nach einem Unfall klären lassen, ob die Technik und damit der Hersteller oder der Fahrer für einen Unfall verantwortlich war. Welche Daten dies sind und wie das Speichermedium ausgestaltet werden soll, regelt der Gesetzentwurf nicht.

Auf Verlangen der nach Landesrecht für Verkehrskontrollen zuständigen Behörden müssen die Fahrdaten diesen Behörden übermittelt werden. Die Fahrdaten sind auch Dritten zu übermitteln, wenn diese glaubhaft machen können, dass sie die Fahrdaten zur Geltendmachung, Abwehr oder Befriedigung von Rechtsansprüchen aus Unfällen benötigen. Unklar ist, wer die

Daten übermitteln muss. Es bleibt ebenfalls unbestimmt, ob ggf. auch die Behörden Fahrdaten übermitteln dürfen.

Im Gesetzesentwurf sind außerdem weder die Zwecke noch die zu übermittelnden Daten hinreichend konkretisiert. Weiterhin geht nicht hervor, wie die Integrität, Vertraulichkeit und Verfügbarkeit bei der Aufzeichnung und Übermittlung der Fahrdaten sichergestellt werden soll.

Sollte der Entwurf in der vorgelegten Form in Kraft treten, besteht in Kraftfahrzeugen mit hoch- oder vollautomatisierter Fahrfunktion die Gefahr elektronischer Fahrtenschreiber, die personenbezogene Profile bilden.

Die Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder fordert den Gesetzgeber zu einer dem datenschutzrechtlichen Bestimmtheitsgebot genügenden Novellierung des Straßenverkehrsgesetzes und zur Stärkung der Datenschutzrechte der Fahrer auf.

Sofern man eine Datenverarbeitung überhaupt für erforderlich hält, ist folgendes zu regeln:

- die abschließende Aufzählung derjenigen Daten, die aufgezeichnet und gespeichert werden dürfen,
- die Bestimmung des für die Verarbeitung Verantwortlichen,
- die Ergänzung einer Übermittlungs-/Zugriffsregelung für den Fahrer/Halter,
- die Konkretisierung der Daten, die den nach Landesrecht zuständigen Behörden zu übermitteln sind,
- die datenschutzgerechte Ausgestaltung des Speichermediums, insbesondere die Festlegung einer angemessenen Speicherdauer anhand der Erforderlichkeit und des Zwecks der Beweisführung für die Haftung,
- eindeutige Festlegungen für die Trennung der Daten von den in den Fahrzeugdatenspeichern der Fahrzeuge gespeicherten Daten,
- die Konkretisierung der Zwecke für die Übermittlung der gespeicherten Daten,
- die Nennung des Adressaten für das Übermittlungsverlangen,

- die abschließende Nennung berechtigter Übermittlungsempfänger und ihrer jeweiligen Verarbeitungsbefugnisse mit im Übrigen strikter Zweckbindung und

- die Konkretisierung des Löschzeitpunkts der übermittelten Daten.

1.3.3 Entschließung vom 15. März 2017: Einsatz externer Dienstleister durch Berufsgeheimnisträger rechtssicher und datenschutzkonform gestalten!

Die Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder fordert den Bundesgesetzgeber auf, mit dem derzeit vorliegenden Gesetzentwurf der Bundesregierung „zur Neuregelung des Schutzes von Geheimnissen bei der Mitwirkung Dritter an der Berufsausübung schweigepflichtiger Personen“ (BR-Drs. 163/17) den Einsatz externer Dienstleister durch Berufsgeheimnisträger rechtssicher und datenschutzkonform zu gestalten.

Die Schweigepflicht ist Grundlage des für die Berufsausübung notwendigen Vertrauensverhältnisses. Aber auch Berufsgeheimnisträger können heute nicht mehr wirtschaftlich agieren, ohne die moderne Informations- und Kommunikationstechnik zu nutzen. Kaum ein Anwalt oder Arzt verfügt über das notwendige Spezialwissen, um diese Technik selbst zu warten und vor ständig neuen Bedrohungen abzusichern. Der vorliegende Gesetzentwurf will deshalb eine Praxis legalisieren, die aus Gründen der Praktikabilität längst etabliert ist. Der strafrechtliche Schutz von Privatgeheimnissen soll die Beauftragung externer Dienstleister durch Berufsgeheimnisträger nicht länger erschweren. Im Gegenzug sollen diese Auftragnehmer künftig einer strafrechtlich sanktionierten Verschwiegenheitspflicht unterliegen. Dennoch versäumt es der Gesetzentwurf, insbesondere mit der vorgeschlagenen Formulierung zu § 203 StGB, klare Verhältnisse zu schaffen. Bisher sorgte unter Ärzten – und mitunter sogar Anwälten – der Umstand für Verwirrung, dass das, was datenschutzrechtlich legitim war, noch längst nicht strafrechtlich erlaubt sein musste. Was nach dem Gesetzentwurf nunmehr strafrechtlich erlaubt sein soll, könnte wiederum nach der neuen Europäischen Datenschutz-Grundverordnung mit empfindlichen Bußgeldern in Millionenhöhe sanktioniert werden. Denn es ist weder mit dem Schutzzweck von § 203 StGB vereinbar, noch datenschutzrechtlich zulässig, dass Berufsgeheimnisträger, wie im neuen § 203 StGB vorgesehen, die Verantwortung für die Datenverarbeitung ohne Einwilligung der Betroffenen an externe Dienstleister übertragen. Nicht absehbar ist zudem, ob die Zeugnisverweigerungsrechte und das Beschlagnahmeverbot in einem weiteren Gesetzgebungsverfahren entsprechend weitgehend auf alle denkbaren Dienstleister ausgeweitet werden, die an der Berufsausübung durch Berufsgeheimnisträger mitwirken.

Die Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder dringt daher darauf, den Gesetzentwurf nachzubessern und die geplanten straf- und berufsrechtlichen Regelungen mit den datenschutzrechtlichen Vorschriften zu synchronisieren. Es muss Berufsgeheimnisträgern möglich sein, externe Dienstleister zu Rate zu ziehen. Im Sinne der ungestörten Berufsausübung der Berufsgeheimnisträger und des Rechts auf informationelle Selbstbestimmung der Betroffenen sollten die Pflichten, die den Berufsgeheimnisträger dabei aus unterschiedlichen Rechtsgebieten treffen, aber soweit als möglich gleichlaufend ausgestaltet werden.

1.3.4 Entschließung vom 24. Januar 2017: Novellierung des Personalausweisgesetzes – Änderungen müssen bürger- und datenschutzfreundlich realisiert werden!

Sonderkonferenz am 24.01.2017 in Hannover

Die Bundesregierung plant grundlegende Änderungen des Personalausweisrechts. Nach dem vom Bundeskabinett beschlossenen Gesetzentwurf (BR-Drs. 787/16) werden das Recht auf informationelle Selbstbestimmung der Bürgerinnen und Bürger übergangen und Datenschutz sichernde Standards unterlaufen. Die Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder fordert daher insbesondere folgende datenschutzrechtliche Anforderungen zu berücksichtigen:

- Die obligatorische Aktivierung der eID-Funktion ist dann hinnehmbar, wenn dauerhaft sichergestellt ist, dass daraus keine verpflichtende Nutzung der eID-Funktion des Personalausweises resultiert. Die Entscheidung über die Nutzung der eID-Funktion muss allein bei den Bürgerinnen und Bürgern liegen. Deren Selbstbestimmungsrecht muss gewahrt bleiben.

- An der bisherigen Verpflichtung der Ausweisbehörden, Bürgerinnen und Bürger über die eID-Funktion des Personalausweises schriftlich zu unterrichten, sollte festgehalten werden. Nur durch eine bundesweit einheitliche Vorgabe zu einer solchen Information wird sichergestellt, dass alle Bürgerinnen und Bürger in hinreichend verständlicher Form aufgeklärt werden.

- Vor einer Datenübermittlung aus dem Personalausweis müssen die Bürgerinnen und Bürger Kenntnis über den Zweck der Übermittlung erhalten; zur Wahrnehmung des Rechts auf informationelle Selbstbestimmung müssen die Betroffenen stets - wie bislang - nachvollziehen können, in welchem konkreten Kontext ihre Identitätsdaten übermittelt werden. Zudem sollte die bisherige Möglichkeit, die Übermittlung einzelner Datenkategorien auszuschließen, beibehalten werden.

- Die Einführung von organisationsbezogenen Berechtigungszertifikaten bei Diensteanbietern wird abgelehnt. Um sicherzustellen, dass Diensteanbieter nur die für den jeweiligen Geschäftsprozess erforderlichen Angaben übermittelt bekommen, sollte an der aktuellen Rechtslage festgehalten werden, nach der der antragstellende Diensteanbieter die Erforderlichkeit der aus der eID-Funktion des Personalausweises zu übermittelnden Angaben nachweisen muss und an den jeweils festgelegten Zweck gebunden ist.

- Berechtigungszertifikate dürfen nur an Diensteanbieter erteilt werden, die Datenschutz und Datensicherheit gewährleisten. Daher sollten antragstellende Diensteanbieter nach wie vor durch eine Selbstverpflichtung die Erfüllung dieser Anforderungen schriftlich bestätigen und nachweisen müssen.

- Die maßgeblichen Regelungen für die mit der Anlegung und Nutzung von Servicekonten einhergehende Erhebung und Verarbeitung von Identitätsdaten aus dem Personalausweis sowie die sicherheitstechnischen Rahmenbedingungen sollten im Personalausweisgesetz getroffen werden.

- Die Voraussetzungen für die Erstellung und Weitergabe von Personalausweisablichtungen sollten gesetzlich konkreter normiert werden. Insbesondere das Prinzip der Erforderlichkeit ist durch eine verpflichtende Prüfung der Notwendigkeit der Anfertigung einer Ablichtung sowie durch eine Positivliste von Erlaubnisgründen zu stärken. Die Einwilligung der Betroffenen als alleinige Voraussetzung birgt die Gefahr, dass in der Praxis Ablichtungen angefertigt werden, obwohl sie nicht erforderlich sind. Zudem dürfte fraglich sein, ob betroffene Personen in eine solche Maßnahme stets informiert und freiwillig einwilligen können.

- Die zum 1. Mai 2021 vorgesehene Einführung eines nahezu voraussetzungslosen Abrufs des Lichtbildes im automatisierten Verfahren durch die Polizeibehörden des Bundes und der Länder sowie die Verfassungsschutzbehörden und Nachrichtendienste wird abgelehnt. Bisher dürfen zur Verfolgung von Straftaten und Verkehrsordnungswidrigkeiten insbesondere die Polizei- und Ordnungsbehörden Lichtbilder automatisiert abrufen, wenn die Personalausweisbehörde nicht erreichbar ist und ein weiteres Abwarten den Ermittlungszweck gefährdet. Diese gesetzlichen Einschränkungen für das Abrufverfahren sollen nun entfallen. Zudem sollen alle Nachrichtendienste künftig voraussetzungslos Lichtbilddaten abrufen können. Die bisherige Rechtslage ist völlig ausreichend.

1.4 92. Konferenz vom 9. bis 10. November 2016 in Kühlungsborn

1.4.1 „Videoüberwachungsverbesserungsgesetz“ zurückziehen!

Das Vorhaben des Bundesministeriums des Innern (BMI), durch ein „Videoüberwachungsverbesserungsgesetz“ Änderungen des Bundesdatenschutzgesetzes (BDSG) einzuführen, die künftig privaten Stellen den Betrieb von Videokameras zur Verhinderung von Anschlägen wie in Ansbach und Amokläufen wie in München erleichtern sollen, wird von den unabhängigen Datenschutzbehörden des Bundes und der Länder[1] abgelehnt. Der Gesetzentwurf vermag nicht zu begründen, dass die angestrebte Erleichterung der Videoüberwachung die öffentliche Sicherheit besser gewährleisten kann, als dies gegenwärtig der Fall ist. Auch die Verlagerung der Verantwortung für diese Aufgabe auf die privaten Betreiber von Einkaufszentren und öffentlichem Personennahverkehr lehnen die unabhängigen Datenschutzbehörden des Bundes und der Länder ab. Nach der nicht abschließenden Aufzählung zielt der Gesetzentwurf überwiegend auf Orte, an denen Betroffene ihre Freizeit verbringen. Gerade in diesen Bereichen, in denen sich Menschen typischerweise zur ungezwungenen Kommunikation, Erholung und Entspannung für längere Dauer aufhalten, gilt es das Persönlichkeitsrecht in besonderem Maße zu schützen.

Gleichwohl lässt es die einschlägige Bestimmung des § 6b BDSG bereits gegenwärtig zu, die Sicherheitsbelange von Personen, die sich in öffentlich zugänglichen Bereichen aufhalten, bei der Abwägung zwischen den Rechten Betroffener und den Betreiberinteressen zu berücksichtigen. Im Rahmen der Hausrechtsausübung können auch heute Kameras installiert werden, um Personen von Straftaten an den Objekten abzuhalten. Darüber hinaus kann Videotechnik zur Beweissicherung eingesetzt werden und nach § 6 Abs. 3 Satz 2 BDSG können Videobilder an Polizei-, Ordnungs- und Strafverfolgungs- und Ordnungsbehörden weitergegeben werden, wenn dies zur Abwehr von Gefahren für die staatliche und öffentliche Sicherheit sowie zur Verfolgung von Straftaten erforderlich ist. Die Begründung des BMI suggeriert, die Datenschutzaufsichtsbehörden verhinderten angesichts der angespannten Sicherheitslage die Durchführung von Videoüberwachung. Dies trifft nicht zu. Tatsächlich werden gerade im Bereich der großen Einkaufszentren, aber auch an Bahnhöfen und in Fahrzeugen des Personennahverkehrs bereits heute zahlreiche Kameras mit ausdrücklicher Billigung der Aufsichtsbehörden betrieben.

Terroristen wie auch irrational handelnde Einzeltäter, vor denen die gesetzliche Regelung schützen soll, nehmen ihren eigenen Tod bei derartigen An-

[1] Bei Enthaltung der Bundesbeauftragten für Datenschutz und Informationsfreiheit.

schlägen bewusst in Kauf. Sie werden sich daher von ihren Taten auch nicht durch Videokameras abschrecken lassen.

Hinzu kommt, dass die Betreiber von Videoüberwachungsanlagen bereits heute meistens nicht in der Lage sind, ein Live-Monitoring durchzuführen und die Bilder der vielen Kameras durch ihr eigenes Personal so auszuwerten, dass bei Gefahren direkt und schnell eingegriffen werden kann. In der Praxis bleibt die Bedeutung der Kameras daher auf eine Speicherung auf Vorrat und für die spätere Strafverfolgung beschränkt. Auch die mögliche Erhöhung eines faktisch ungerechtfertigten subjektiven Sicherheitsgefühls könnte Grundrechtseingriffe nicht rechtfertigen. Insoweit ist die Regelung, die von den privaten Betreibern eine stärkere Gewichtung des Schutzes von Leben, Gesundheit oder Freiheit der Betroffenen bei der rechtlichen Abwägung fordert, letztlich gar nicht geeignet, das Ziel der gesetzlichen Regelung zu erreichen.

Die unabhängigen Datenschutzbehörden des Bundes und der Länder betonen mit Nachdruck, dass es nicht die Aufgabe privater Stellen ist, die Sicherheit der Bevölkerung zu gewährleisten. Dies obliegt allein den Sicherheitsbehörden, die über ausreichende landes- und bundesgesetzliche Grundlagen sowohl für die Gefahrenabwehr als auch für die Strafverfolgung verfügen.

Die Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder fordert den Bundesinnenminister auf, den Gesetzentwurf zurückzuziehen.

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

Die Datenschutzbeauftragten des Bundes und der Länder[1] Baden-Württemberg, Bayern, Berlin, Brandenburg, Bremen, Hessen, Niedersachsen, Nordrhein-Westfalen, Rheinland-Pfalz, Sachsen-Anhalt, Schleswig-Holstein und Thüringen haben parallel die bundesweit geführte „Falldatei Rauschgift“ (FDR) datenschutzrechtlich geprüft.

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

[1] Bei Enthaltung Hamburg.

ihrer Kontrollen sowohl die Struktur der Datei als auch Einzelspeicherungen überprüft.

Die Prüfung hat im Wesentlichen folgende Mängel aufgedeckt:

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

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

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

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

Die Ergebnisse machen deutlich:

1. Es ist wichtig, die konkrete Zwecksetzung jeder Datei in einer Errichtungsanordnung festzulegen. Die Voraussetzungen, wann welche Daten für den jeweiligen Zweck erforderlich sind und welcher Personenkreis erfasst werden darf, müssen genau definiert werden.

2. Bagatellfälle in Verbunddateien zu speichern, ist auch im Hinblick auf die bundesweite Abrufbarkeit der Daten unverhältnismäßig.

3. In der Praxis ist sicherzustellen, dass in Verbunddateien alle Speichervoraussetzungen, vor allem die Negativprognose, durchgehend und gründlich bezogen auf den jeweiligen Einzelfall dokumentiert werden.

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

1.5 Entschließungen zwischen der 91. und 92. Konferenz

1.5.1 Entschließung[1] vom 25. Mai 2016: EU-Datenschutz-Grundverordnung erfordert zusätzliche Ressourcen für Datenschutzbehörden

Am 14. April 2016 hat das Europäische Parlament dem neuen Rechtsrahmen für den Datenschutz in Europa zugestimmt. Wesentlicher Teil des Rechtsrahmens ist die EU-Datenschutz-Grundverordnung, deren Text am 4. Mai 2016 im Amtsblatt der Europäischen Union veröffentlicht wurde. Die Verordnung ist am 25. Mai 2016 in Kraft getreten und zwei Jahre später verbindlich in allen Mitgliedstaaten der Europäischen Union anzuwenden.

Die Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder weist darauf hin, dass mit der EU-Datenschutz-Grundverordnung eine Reihe neuer bzw. erweiterter Aufgaben auf sie zukommen. Hierzu gehören insbesondere:

- Bearbeitung von Beschwerden und Beratung Betroffener sowie datenschutzrechtliche Beratung und Kontrolle von Unternehmen nunmehr unter Beachtung des erweiterten räumlichen Anwendungsbereichs der Verordnung (Marktortprinzip),

- verpflichtende Beratung von Behörden und Unternehmen bei der Datenschutz-Folgenabschätzung, insbesondere im Rahmen der vorherigen Konsultation der Aufsichtsbehörde, sowie Beratung bei der Umsetzung neuer Anforderungen wie Datenschutz durch Technikgestaltung und datenschutzfreundliche Voreinstellungen (Privacy By Design, Privacy By Default),

- Aufbau und Anwendung eines Kooperationsverfahrens zwischen Datenschutzbehörden in Europa bei grenzüberschreitenden Datenverarbeitungen (One-Stop-Shop), Verpflichtung zur gegenseitigen Amtshilfe und umfassender Austausch von Informationen zwischen federführenden und betroffenen Aufsichtsbehörden jeweils mit kurzen Bearbeitungsfristen,

- Etablierung eines Kohärenzverfahrens zwischen den Datenschutzbehörden in Europa zur Gewährleistung der europaweit einheitlichen Anwendung der Verordnung, Mitwirkung im Europäischen Datenschutzausschuss,

[1] Bei Enthaltung Bayerns (Bayerischer Landesbeauftragter für den Datenschutz und Bayerisches Landesamt für Datenschutzaufsicht).

- europaweit einheitliche Auslegung der Grundverordnung in Bezug auf fehlende Regelungen (z. B. zur Videoüberwachung oder zum Scoring) und neue Anforderungen (z. B. Recht auf transparente Information oder Recht auf Datenübertragbarkeit),

- Erarbeitung von Stellungnahmen und Billigung von branchenspezifischen Verhaltensregeln zur ordnungsgemäßen Anwendung der Verordnung, Erarbeitung von Zertifizierungskriterien, ggf. Durchführung von Zertifizierungen, Erarbeitung von Kriterien für die Akkreditierung von Zertifizierungsstellen, ggf. Durchführung der Akkreditierung,

- Bearbeitung von gerichtlichen Rechtsbehelfen Betroffener gegen Entscheidungen von Aufsichtsbehörden,

- Ausübung neuer bzw. erweiterter Befugnisse der Datenschutzbehörden zur Erteilung von Anordnungen gegenüber den Verantwortlichen nunmehr auch im öffentlichen Bereich sowie Berücksichtigung zusätzlicher Tatbestände für Ordnungswidrigkeiten und eines erweiterten Bußgeldrahmens.

Die Europäische Datenschutz-Grundverordnung verpflichtet die Mitgliedstaaten, die Aufsichtsbehörden zur Gewährleistung ihrer Unabhängigkeit mit den erforderlichen personellen, finanziellen und technischen Ressourcen auszustatten (Art. 52 Abs. 4 DSGVO). Aus Sicht der Datenschutzkonferenz ist es für die Bewältigung der neuen Aufgaben zwingend erforderlich, für die Datenschutzbehörden in Deutschland erweiterte personelle und finanzielle Ressourcen vorzusehen. Dies gilt bereits für die jetzt laufende Vorbereitungsphase, in der die Weichen für eine funktionierende Umsetzung der Datenschutz-Grundverordnung gestellt werden. Die Konferenz appelliert deshalb an die Gesetzgeber in Bund und Ländern, rechtzeitig die haushaltsrechtlichen Vorkehrungen für eine jeweils angemessene, erweiterte Ausstattung der Datenschutzbehörden zu treffen. Nur so lassen sich die zusätzlichen Aufgaben der Datenschutz-Grundverordnung von den Datenschutzbehörden in Deutschland effektiv wahrnehmen.

1.5.2 Entschließung vom 20. April 2016: Klagerecht für Datenschutzbehörden – EU-Kommissionentscheidungen müssen gerichtlich überprüfbar sein

Die Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder (Datenschutzkonferenz) fordert den Gesetzgeber auf, umgehend ein eigenständiges Klagerecht für die unabhängigen Datenschutzbehörden vorzusehen. Wenn die unabhängigen Datenschutzbehörden der Auffassung sein sollten, dass eine Entscheidung der EU-Kommission rechtswidrig ist, wären sie gleichwohl an diese gebunden. Sie müssten daher ggf. gegen den

rechtsstaatlichen Grundsatz der Gesetzmäßigkeit der Verwaltung verstoßen. Um dies zu verhindern, sind die prozessualen Voraussetzungen dafür zu schaffen, dass die Datenschutzbehörden selbst bestehende Zweifel an der Rechtmäßigkeit einer Kommissionsentscheidung gerichtlich klären lassen können.

Anlass für die obige Aufforderung der Datenschutzkonferenz ist die zwischenzeitliche Vorlage einer Reihe von Dokumenten unterschiedlicher Repräsentanten der US-Administration durch die EU-Kommission am 29. Februar 2016, die für Unternehmen und Behörden Zusagen für den Umgang mit aus der EU übermittelten personenbezogenen Daten enthalten. Im Rahmen eines so genannten EU-US Privacy Shield sollen diese Dokumente Grundlage für eine künftige EU-Kommissionsentscheidung zur Angemessenheit des Datenschutzniveaus in den USA sein und damit als Nachfolgeregelung für die Safe Harbor-Entscheidung dienen. Letztere wurde bekanntlich am 6. Oktober 2015 durch den Europäischen Gerichtshof aufgehoben.

Gegen den „EU-US Privacy Shield“ bestehen jedoch nach Auffassung der Artikel-29-Datenschutzgruppe, dem Zusammenschluss der Datenschutzbehörden der EU-Mitgliedstaaten und des Europäischen Datenschutzbeauftragten, erhebliche Bedenken. Die Artikel-29-Dateschutzgruppe hat zum „EU-US Privacy Shield“ zuletzt am 13. April 2016 detailliert Stellung genommen. Die Datenschutzkonferenz teilt diese umfassende Analyse und unterstützt die darin enthaltene Forderung an die EU-Kommission, vor einer Beschlussfassung substantielle Nachbesserungen vorzunehmen. Die Datenschutzkonferenz ist der Auffassung, dass auch der „EU-US Privacy Shield“ in seiner derzeitigen Form nicht ausreichend ist, das für die Übermittlung personenbezogener Daten in die USA erforderliche „angemessene Datenschutzniveau“ in den USA zu gewährleisten.

Der EuGH stellt in seiner o. g. Entscheidung zur Ungültigkeit von Safe Harbor ausdrücklich klar, dass nach Maßgabe der Datenschutz-Richtlinie der nationale Gesetzgeber für die Datenschutzbehörden Rechtsbehelfe vorzusehen hat, die ihnen bei rechtlichen Zweifeln über eine Angemessenheitsentscheidung die Anrufung nationaler Gerichte ermöglichen, so dass diese den EuGH um eine Entscheidung über die Vereinbarkeit mit den europäischen Grundrechten ersuchen können.

Die Datenschutzkonferenz begrüßt und unterstützt daher ausdrücklich die Bundesratsinitiative der Freien und Hansestadt Hamburg zur zeitnahen Einräumung eines Klagerechts für die Datenschutzaufsichtsbehörden von Bund und Ländern (BR-Drs. 171/16), in der nochmals deutlich gemacht wird, „dass das vom Europäischen Gerichtshof (EuGH) in seinem Urteil vom 6.10.2015 (Rechtssache C-362/14) statuierte Klagerecht für Datenschutzaufsichtsbe-

hörden für die Gewährleistung einer effektiven Datenschutzkontrolle von besonderer Bedeutung ist“.

1.6 91. Konferenz vom 6. bis 7. April 2016 in Schwerin

1.6.1 Stärkung des Datenschutzes in Europa – nationale Spielräume nutzen

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

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

Nach der Einschätzung der Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder ist es allerdings zur Erhaltung und Verstärkung des bestehenden Datenschutzniveaus auch im Lichte der jüngeren Entscheidungen des Europäischen Gerichtshofs geboten, die in der Grundverordnung enthaltenen Öffnungs- und Konkretisierungsklauseln zu Gunsten des Rechts auf informationelle Selbstbestimmung zu nutzen. Auch die von der Grundverordnung getroffenen Weiterentwicklungen des Datenschutzes wie beispielsweise die Grundsätze des Datenschutzes durch Technik und durch datenschutzfreundliche Voreinstellungen sowie das Erfordernis von Datenschutz-Folgeabschätzungen müssen wirksam ausgestaltet werden. Die Konferenz fordert deshalb Bundes- und Landesgesetzgeber auf, in allen gesetzgeberischen Bereichen die nationalen Spielräume im Sinne des Grundrechts auf informationelle Selbstbestimmung zu nutzen.

Insbesondere folgenden Regelungen kommt in diesem Zusammenhang hohe Bedeutung zu:

- Schaffung eines Beschäftigtendatenschutzgesetzes, mindestens jedoch Beibehaltung der §§ 3 Abs. 11, 32 BDSG (Art. 88 i.V.m. Erwägungsgrund [EG] 155),

- Beschränkungen für die Verarbeitung von genetischen, biometrischen oder Gesundheitsdaten (Art. 9 Abs. 4 i.V.m. EG 53, letzte beide Sätze),

- Stärkung der Befugnisse der Aufsichtsbehörden, insbesondere Schaffung von Klagebefugnissen und effektiven Sanktionen auch gegenüber Behörden (Art. 58 und 83 Abs. 7 i.V.m. EG 150, vorletzter Satz),

- jedenfalls im öffentlichen Bereich durch die Nennung der Schutzziele Datensparsamkeit, Vertraulichkeit, Integrität, Verfügbarkeit, Nichtverkettbarkeit, Transparenz und Intervenierbarkeit, um einen einfachen, flexiblen und praxistauglichen technischen und organisatorischen Datenschutz zu konkretisieren (Art. 6 Abs. 2, 25, 32),

- Begrenzung der Zweckänderung bei Videoüberwachung öffentlich zugänglicher Räume durch Private, soweit dies zur Abwehr von Gefahren für die staatliche und öffentliche Sicherheit sowie zur Verfolgung von Straftaten erforderlich ist (Art. 6 Abs. 4),

- Beibehaltung der Verpflichtung in § 4f Abs. 1 BDSG einen betrieblichen Datenschutzbeauftragten zu bestellen(Art. 37 Abs. 4).

1.6.2 Wearables und Gesundheits-Apps – Sensible Gesundheitsdaten effektiv schützen!

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

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

Allerdings stehen diesen Chancen auch Risiken, insbesondere für das Persönlichkeitsrecht, gegenüber. Zahlreiche Wearables und Gesundheits-Apps geben die aufgezeichneten Daten an andere Personen oder Stellen weiter, ohne dass die betroffenen Personen hiervon wissen oder dazu eine bewusste Entscheidung treffen. Darüber hinaus können Bedienungsfehler oder unzu-

reichende technische Funktionalitäten dazu führen, dass Gesundheitsinformationen ungewollt preisgegeben werden. Einige Angebote weisen erhebliche Sicherheitsdefizite auf, so dass auch Unbefugte sich Zugriff auf die Gesundheitsdaten verschaffen können. Für bestimmte Situationen besteht überdies das Risiko, dass Einzelne aufgrund massiver gesellschaftlicher, sozialer oder ökonomischer Zwänge nicht frei über die Nutzung derartiger Technologien entscheiden können. Zum notwendigen Schutz von Gesundheitsdaten bei Wearables und Gesundheits-Apps weist die Datenschutzkonferenz auf folgende Gesichtspunkte hin:

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

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

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

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

- Wer aus eigenen Geschäftsinteressen gezielt bestimmte Wearables und Gesundheits-Apps in den Umlauf bringt oder ihren Vertrieb systematisch unterstützt, trägt eine Mitverantwortlichkeit für die rechtmäßige Ausgestaltung solcher Angebote. In diesem Sinne Mitverantwortliche haben sich zu vergewissern, dass die Produkte verbindlichen Qualitätsstan-

dards an IT-Sicherheit, Funktionsfähigkeit sowie an Transparenz der Datenverarbeitung genügen.

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

1.6.3 Datenschutz bei Servicekonten

Der IT-Planungsrat hat sich in einem Beschluss in seiner 17. Sitzung im Juni 2015 für eine flächendeckende Verbreitung so genannter Servicekonten für Bürgerinnen, Bürger und Unternehmen ausgesprochen. Über diese Konten soll es künftig möglich sein, sich einfach für die Inanspruchnahme von Verwaltungsdienstleistungen auf kommunaler, Länder- und Bundesebene zu identifizieren. Dabei soll der neue Personalausweis mit seiner eID-Funktion eine wichtige Rolle spielen. Eine Projektgruppe des IT-Planungsrates erarbeitet zurzeit die rechtlichen und technischen Rahmenbedingungen für Servicekonten.

Die Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder nimmt die Aktivitäten des IT-Planungsrates zur Kenntnis, den Zugang zu elektronischen Verwaltungsdienstleistungen zu erleichtern und möglichst medienbruchfrei auszugestalten. Sie weist darauf hin, dass insbesondere die Einrichtung von länderübergreifenden Servicekonten gewichtige verfassungsrechtliche Fragen etwa zum Bund-Länder-Verhältnis und zum Persönlichkeitsrecht aufwerfen. So ist dabei das Verbot einer Vorratsdatenspeicherung zu unbestimmten Zwecken sowie das grundrechtliche Prinzip der informationellen Gewaltenteilung zu beachten. Servicekonten dürfen die gesetzliche Zuständigkeits- und Aufgabenverteilung der öffentlichen Verwaltung nicht unterlaufen.

Hiervon abgesehen müssen jedenfalls die Datenschutzprinzipien der Datensparsamkeit, der Nichtverkettbarkeit und der Transparenz berücksichtigt werden. Für die Integration von Verwaltungsdienstleistungen heißt insbesondere, dass auch die Schnittstellen zwischen den Systemen so definiert sein müssen, dass nur die für den vorgesehenen Zweck erforderlichen Daten übertragen werden. Dazu sind folgende Rahmenbedingungen einzuhalten:

- Auch künftig muss es möglich sein, ohne Servicekonto Verwaltungsdienstleistungen in Anspruch zu nehmen.

- Die einmalige Inanspruchnahme von Verwaltungsdienstleistungen muss auch ohne dauerhafte Speicherung identifizierender Daten möglich sein. Für diese Zwecke sollten temporäre Servicekonten eingerichtet werden.

- Bürgerinnen und Bürgern muss die Möglichkeit eingeräumt werden, sowohl einzelne im permanenten Servicekonto dauerhaft gespeicherte, personenbezogenen Daten als auch das Konto selbst löschen zu lassen.

- Soweit Daten aus dem Servicekonto übermittelt werden, müssen diese Übermittlungen durch die Bürger im Servicekonto selbst nachvollzogen werden können.

- Für die Erhebung personenbezogener Daten in behördenübergreifenden Servicekonten ist eine Rechtsgrundlage erforderlich, da sie als Aufgabe verwaltungsorganisationsrechtlich einer Stelle zugewiesen werden muss. Der Staat darf personenbezogene Daten zur Erfüllung seiner gesetzlichen Aufgaben grundsätzlich nur auf der Basis einer klaren Rechtsgrundlage verarbeiten. Da zudem die Bedeutung dieser Servicekonten zunehmen wird und absehbar ist, dass den Betroffenen durch die Nutzung dieser Konten erhebliche Vorteile im Sinne von „Digital by Default“ eingeräumt werden sollen, reicht die Einwilligung als Rechtsgrundlage für die Datenerhebung nicht aus.

- Vorbehaltlich weiterer verfassungsrechtlicher Prüfungen ist für die Länder übergreifende Nutzung von Servicekonten eine Rechtsgrundlage erforderlich. Durch die dauerhafte Speicherung identifizierender Daten werden bundesweit nutzbare Servicekonten zu einer digitalen Meldestelle bzw. zu einer zweiten, zentralen Identifizierungsstelle neben den Meldebehörden aufgewertet. Die Rechtsgrundlage muss eindeutige Vorgaben zum Datenumfang, zu Zweckbindungsregelungen, zur Löschung und zur Transparenz der Datenverarbeitung enthalten. Daten der Betroffenen sind alleine zum Betrieb des Serviceportals und zur Erledigung der Verfahren der Nutzer zu verarbeiten. Eine Nutzung dritter Stellen zu anderen Zwecken ist gesetzlich ausdrücklich auszuschließen.

- Bevor Unternehmen verpflichtet werden sollen, die eID-Funktion für Verwaltungsangelegenheiten zu nutzen, ist zu prüfen, ob und unter welchen Voraussetzungen der Einsatz privater digitaler Identifikationsnachweise zu nichtprivaten Zwecken bzw. zur Erfüllung arbeitsvertraglicher Pflichten zulässig ist und inwieweit Arbeitnehmerinnen und Arbeitnehmer hierzu verpflichtet werden können.

- Angesichts des Abhängigkeitsverhältnisses der Arbeitnehmerinnen und Arbeitnehmer im Beschäftigungsverhältnis kann die Nutzung von Servicekonten auf der Basis der privaten eID-Funktion keinesfalls auf der

Einwilligungsbasis erfolgen. Auch hierfür ist eine Rechtsgrundlage erforderlich, die die Datenverarbeitung in Servicekonten vollständig erfasst. Bei der Identifizierung eines bevollmächtigten Beschäftigten dürfen nur die für diese Identifizierung erforderlichen Daten erfasst werden.

Sichere, elektronische Identifizierungsmöglichkeiten können zur Datenschutzkonformität von E‑Government- und von E-Commerce-Verfahren beitragen. Die unabhängigen Datenschutzaufsichtsbehörden begrüßen daher Maßnahmen, die zur verstärkten Nutzung der eID-Funktion des neuen Personalausweises beitragen. Dennoch muss den Betroffenen die Möglichkeit gelassen werden, selbst zu entscheiden, ob sie die eID-Funktion freischalten und nutzen wollen. Die Datenschutzkonferenz lehnt daher die angedachte Änderung des Personalausweisgesetzes ab, wonach die eID-Funktion des neuen Personalausweises dauerhaft eingeschaltet wäre und nicht mehr deaktiviert werden könnte. Eine standardmäßige Aktivierung der eID-Funktion wäre allenfalls dann hinnehmbar, wenn den Bürgerinnen und Bürgern ein Opt-In mit Widerrufsmöglichkeit angeboten wird, um die eID-Funktion jederzeit gebührenfrei aktivieren und deaktivieren zu können.

1.6.4 Wahrung der Freiheits- und Persönlichkeitsrechte bei der Bekämpfung des internationalen Terrorismus

Rechtsstaat und Grundrechtsschutz – damit auch Datenschutz – stehen einer effektiven Bekämpfung des Terrorismus nicht entgegen.

Auch nach Brüssel gilt: Datenschutz verhindert nicht, Terroristen und ihre Helfernetzwerke zu erfassen und zu bekämpfen. Das geltende Datenschutzrecht erlaubt deren Daten zu speichern und Informationen wechselseitig auszutauschen. Der Datenschutz kann jedenfalls nicht für etwaige Defizite bei der Nutzung vorhandener Eingriffsbefugnisse sowie für möglicherweise ineffiziente sicherheitsbehördliche Strukturen verantwortlich gemacht werden.

Die häufig reflexartig erhobene Forderung nach weiteren Eingriffsbefugnissen und flächendeckenden Überwachungsmaßnahmen trägt zur Bekämpfung des internationalen Terrorismus nicht bei.

Es kennzeichnet den Rechtsstaat, dass sich jeder in einem fairen Verfahren gegen unberechtigte Verdachtsbehauptungen wehren, Schutz bei Gerichten suchen und auf die Kontrolle der Datenschutzbeauftragten vertrauen darf. Die massenhafte, verdachtsunabhängige Erhebung und Speicherung von Daten widerspricht dem Grundrecht auf Datenschutz.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder bekräftigt ihren mehrfach formulierten Appell*), dass alle neu erwogenen Maßnahmen zur Bekämpfung des internationalen Terrorismus sich daran

messen lassen müssen, ob sie für dessen wirkungsvolle Bekämpfung wirklich geeignet, erforderlich und angemessen sind und damit dem Verfassungsgrundsatz der Verhältnismäßigkeit entsprechen.

*) - Entschließung der 62. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 25./26. Oktober 2001 in Münster

- Entschließung der 72. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 26./27. Oktober 2006 in Naumburg

- Entschließung der 82. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 28./29. September 2011 in München

- Entschließung der 89. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 18./19. März 2015 in Wiesbaden

1.7 Grundsatzpositionen und Forderungen der Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder für die neue Legislaturperiode vom 16. Oktober 2017

Die fortschreitende Digitalisierung eröffnet wirtschaftliche und gesellschaftspolitische Chancen. Mit ihr einher gehen jedoch erhebliche Risiken für die Persönlichkeitsrechte der Menschen. Ein an diese Entwicklungen angepasster und damit starker Datenschutz ist das Gebot der Stunde.

Die Datenschutzkonferenz formuliert zu Beginn der Legislatur elf handlungsorientierte Grundforderungen, deren Ziel es ist, das Datenschutzrecht weiter zu entwickeln und seine Durchsetzung und Akzeptanz zu fördern. Ein wirksamer Datenschutz ist Grundrechtsschutz und darf nicht als Hindernis betrachtet werden. Er muss vielmehr als integraler und förderlicher Bestandteil politischer, wirtschaftlicher und gesellschaftlicher Fortentwicklung verstanden und gelebt werden.

Digitale Souveränität – Datensouveränität

Die DSK fordert, das Verbotsprinzip nach der DSGVO nicht durch den Anspruch auf „Datensouveränität“ aufzuweichen.

„Datensouveränität“ ist ein Schlagwort in der politischen Auseinandersetzung um die zeitgemäße Positionierung des Datenschutzes, das in unterschiedlichen Zusammenhängen gebraucht wird. Aus der Alltagssprache entnommen, wird der aus dem Staatsrecht stammende Begriff „Souveränität“ mit selbstbe-

stimmtem Handeln assoziiert, der einen Anspruch auf (absolute) Herrschaft über die eigenen persönlichen Daten beinhaltet. Dies allerdings kommt nach gegenwärtigem Rechtsverständnis allenfalls im Kernbereich privater Lebensgestaltung in Betracht. Zudem trifft er datenschutzrechtliche Anforderungen ebenso wenig wie das mit dem neuen Begriff angestrebte Ziel, Daten zu einer rein wirtschaftlichen Größe zu machen und damit Einschränkungen des Datenschutzes zu verschleiern. Die DSK spricht sich daher dafür aus, auch künftig das aus der Menschenwürde abgeleitete Recht auf informationelle Selbstbestimmung in den Mittelpunkt zu stellen und bei dem funktionalen Begriff des datenschutz-rechtlichen Verbotsprinzips zu bleiben.

Grundsatz der Datenminimierung

Die DSK fordert, der Datenminimierung die ihr gemäß DSGVO gebührende Überholspur auf dem Weg der Digitalisierung frei zu räumen.

Datenminimierung heißt, dass personenbezogene Daten auf das für die Zwecke der Verarbeitung erforderliche Maß beschränkt sein müssen. Dies ist notwendig, um die mit der Datenverarbeitung einhergehenden Risiken für die betroffenen Personen einzudämmen. Der Grundsatz der Datenminimierung lässt sich aus dem Verfassungsrecht der EU und Deutschlands ableiten und wurde zu einem der Hauptprinzipien der DSGVO erhoben (Art. 5 Abs. 1 lit. c DSGVO). Damit ist Datenminimierung Rahmenbedingung jeder Datenverarbeitung in Europa und steht nicht zur Disposition des deutschen Gesetzgebers.

Hierdurch werden Innovationen nicht verhindert: Clevere Datenminimierungslösungen können das Bedürfnis zur Auswertung von Informationen und die Notwendigkeit des Datenschutzes vereinen, z. B. indem auf den Personenbezug von Daten verzichtet wird. Technologische Projekte, die Datenminimierung innovativ und intelligent umsetzen und damit erst rechtskonforme Geschäftsmodelle im Zusammenhang mit Big Data-Anwendungen und „smarten“ Lösungen ermöglichen, sollten gefördert werden.

Rahmenbedingungen für datenschutzfreundliche und sichere Systemgestaltung

Die DSK fordert, datenschutzfreundliche und sichere Systemgestaltung stärker öffentlich zu fördern.

Nach der DSGVO sollen nicht nur die erforderlichen technisch-organisatorischen Maßnahmen für Datensicherheit getroffen werden, sondern Datenschutz soll von Anfang an und über den gesamten Lebenszyklus hinweg in Produkte, Dienste und Anwendungen eingebaut sein.

Daher sollten Initiativen und Projekte verstärkt gefördert werden, die Datenschutz „by Design“ und „by Default“ gewährleisten und die Qualität der Datensicherheit verbessern. Die DSK fordert die Bundesregierung auf, sich für technologische Innovationen mit eingebautem Datenschutz einzusetzen und diese auch im Austausch mit Vertretern aus Wirtschaft, Forschung und Entwicklung voranzubringen. Auch sollten alle von der Bundesregierung geförderten Vorhaben mit Personenbezug zukünftig belegen, wie sie die Datenschutzanforderungen erfüllen, damit die Resultate rechtskonform sind. Datenschutzfreundliche und sichere Systemgestaltung ist im Sinne der Vorbildfunktion des öffentlichen Sektors in den öffentlichen Stellen des Bundes sowie in bestehenden oder aufzubauenden IT-Infrastrukturen nachzuweisen. Im Bereich der nationalen, europäischen und internationalen Standardisierung soll die Bundesregierung darauf hinwirken, dass Datenschutzanforderungen eine entsprechende Berücksichtigung finden. Dies betrifft auch einheitliche Vorgaben und Schnittstellen für den Selbstdatenschutz und ein angemessenes Niveau bei Zertifizierungen.

Klare gesetzliche Regelungen für automatisierte Entscheidungen durch Algorithmen

Die DSK fordert, für den Einsatz von Algorithmen im Hinblick auf Transparenz, Kontrolle und Begrenzung klare gesetzliche Regelungen zu schaffen.

Die digitale Informationsgesellschaft ist von Verfahren geprägt, die in unterschiedlichster Art und Weise automatisierte Entscheidungen treffen. Hinter ihnen verbergen sich Algorithmen, bei denen oft nicht ersichtlich ist, welche Daten als Grundlage für Entscheidungen herangezogen werden bzw. wie diese der Entscheidungsfindung dienen. Die Komplexität von Algorithmen macht es häufig unmöglich, ihre Funktionsweise analytisch zu bewerten. Sie entscheiden bspw. über Fahrzeugreaktionen, ob ein Kredit gewährt oder welcher Versicherungstarif angeboten wird und das meist ohne Berücksichtigung der individuellen Situation betroffener Personen. Es besteht die Gefahr von Diskriminierungen und Stigmatisierungen, eingeschränkten Auswahlmöglichkeiten bis hin zu Fehlentscheidungen. Menschen dürfen algorithmischen Entscheidungen nicht bedingungslos ausgeliefert werden. Es bedarf daher Regelungen zu Einsatzvoraussetzungen, Entwicklung, Prüfung und Verwendung von Algorithmen, deren Einsatzzweck in automatisierten Entscheidungen liegt.

Nachbesserungen beim Bundesdatenschutzgesetz

Die DSK fordert, die Einschränkung von Aufsichtsbefugnissen und Betroffenenrechten zurückzunehmen sowie die Regelungen zur Videoüberwachung europarechtskonform auszugestalten.

Den Untersuchungsbefugnissen der Aufsichtsbehörden sind Datenverarbeitungen entzogen, die dem Steuergeheimnis, der ärztlichen Schweigepflicht oder anderen Geheimhaltungspflichten unterliegen. Diese Beschneidung der Befugnisse gegenüber Berufsgeheimnisträgern geht weit über die Öffnungsklausel des Art. 90 DSGVO hinaus. Es sollte die bisherige Regelung des § 38 Abs. 3, 4 i. V. m. § 24 Abs. 2 und Abs. 6 BDSG-alt beibehalten werden. Die Aufsicht durch unabhängige Datenschutzbehörden dient den Interessen der betroffenen Personen. Geheimhaltungspflichten sind durch § 29 Abs. 3 S. 2 BDSG hinreichend geschützt.

Übermäßige Einschnitte in die Betroffenenrechte widersprechen dem Schutzcharakter der DSGVO. Beschränkungen dürfen nicht den Wesensgehalt der Grundrechte und Grundfreiheiten tangieren, müssen in einer demokratischen Gesellschaft notwendige und verhältnismäßige Maßnahmen darstellen sowie die in Art. 23 Abs. 1 DSGVO aufgezählten Ziele sicherstellen.

Die Vorschrift zur Videoüberwachung ist, soweit sie nicht-öffentliche Stellen betrifft, zu streichen. Sie lässt sich nicht auf den herangezogenen Art. 6 Abs. 1 S. 1 lit. e) i.V.m. Art. 6 Abs. 3 S. 1 DSGVO stützen. Zudem erlaubt die ohnehin unmittelbar geltende DSGVO einen angemessenen Ausgleich zwischen den berechtigten Interessen der Verantwortlichen an einer Videoüberwachung und dem Schutz der Persönlichkeitsrechte der Betroffenen.

Innere Sicherheit unter Wahrung des Datenschutzes

Die DSK fordert, bei der Bekämpfung von Terrorismus und Kriminalität das Vertrauen unbescholtener Menschen in die Vertraulichkeit ihrer Kommunikation und die Unberührtheit ihrer Privatheit zu wahren.

Datenschutz steht nicht im Widerspruch zu Sicherheit. Datenschutz schafft Sicherheit, denn das Grundrecht auf Schutz personenbezogener Daten verlangt klare gesetzliche Regelungen, die transparent für den Einzelnen die Leitplanken für die Ausübung seiner Rechte und deren Grenzen festlegen. Datenschutz bringt Rechtsklarheit und Rechtsklarheit trägt zur Steigerung des Gefühls der Sicherheit bei. Nur Sicherheit in Freiheit ist wirkliche Sicherheit für alle.

Auch das Verhalten im öffentlichen Raum muss grundsätzlich von Beobachtung, Aufzeichnung, biometrischer Erfassung und automatisierter Auswertung frei bleiben. Eine massenhafte, verdachtsunabhängige Erhebung und Speicherung von Daten widerspricht den Grundrechten. Die Vorratsdatenspeicherung ist daher in all ihren Ausprägungen auf den Prüfstand zu stellen. Befugnisse zu Überwachungsmaßnahmen müssen einem gestuften System folgen, wonach sich die Rechtfertigung für einen Grundrechtseingriff an der Eingriffsintensität bemisst.

Betroffene sind über sicherheitsbehördliche Maßnahmen zu informieren. Sollte dies nicht möglich sein, ist umso mehr eine unabhängige Kontrolle zu gewährleisten: Eine effektive Datenschutzkontrolle muss Sanktions- und Anordnungsbefugnisse und auch die Kontrolle der Nachrichtendienste umfassen. Auch grenzüberschreitende Datenübermittlungen dürfen davon nicht ausgeschlossen sein. Diese Prinzipien sind bei einer Änderung oder Neufassung von Sicherheitsgesetzen auch aus Anlass der Anpassung an Vorgaben der EU zu beachten.

Arbeiten 4.0 – ein Beschäftigtendatenschutzgesetz für die neue Arbeitswelt

Die DSK fordert, den Beschäftigtendatenschutz durch ein eigenständiges Gesetz zu regeln.

§ 26 BDSG-neu übernimmt weitgehend die bisher geltenden Regelungen des BDSG-alt. Diese sind jedoch unzureichend. Die Arbeitswelt 4.0 erweitert z. B. die Möglichkeiten der offenen und verdeckten technischen Überwachung erheblich. Ein angemessener Ausgleich zwischen Informationsinteressen des Arbeitgebers und Schutz der Rechte und Freiheiten des Arbeitnehmers ist nur durch eine differenzierte, umfassende gesetzliche Regelung zu erreichen.

Big Data im Gesundheitswesen

Die DSK fordert, für die Auswertung von Gesundheitsdaten strikte gesetzliche Vorgaben zu machen.

Gesundheitsdaten unterliegen dem strengeren Regelungsregime für besondere Kategorien personenbezogener Daten. Zunehmend werden sehr große Mengen von Gesundheitsdaten aus den unterschiedlichsten Lebensbereichen zusammengeführt und mit sog. Big Data-Anwendungen systematisch ausgewertet.

Verknüpfungen zwischen verschiedenen Datenbeständen, die Gesundheitsdaten enthalten, dürfen nur auf der Grundlage spezieller rechtlicher Regelungen zugelassen werden. Die Re-Identifizierung und unerlaubte Zusammenführung von Daten, das Anlegen von Datenprofilen zu einer Person sowie der Handel mit Gesundheitsdaten sind zu verbieten und unter Strafe zu stellen. Es muss zudem gesetzlich festgelegt werden, dass mit anonymisierten bzw. hinreichend pseudonymisierten Daten gearbeitet wird, in welchen Zusammenhängen ausnahmsweise auf die Einwilligung als Legitimation für eine Verarbeitung von Gesundheitsdaten in Big Data-Anwendungen zurückgegriffen werden darf und unter welchen Voraussetzungen eine wirksame Einwilligung gegeben werden kann. Zudem sind Transparenzvorgaben z. B. hinsichtlich der Analysemethoden, der Verarbeitungszwecke und der genutzten

Datenbestände bei geplanten Big Data-Projekten zu machen. Es sollte gesetzlich vorgesehen werden, dass für jedes Big Data-Projekt im Gesundheitswesen das Votum der zuständigen Datenschutzaufsichtsbehörde eingeholt wird.

E-Health

Die DSK fordert, bei der Digitalisierung des Gesundheitswesens („E-Health“) das Recht auf Schutz personenbezogener Daten der Patienten und Versicherten gesetzlich wirksam zu sichern.

Auch künftig muss das Vertrauensverhältnis zwischen Patienten und ihren Behandlern effektiv geschützt werden. Vor einer Nutzung neuer technischer Anwendungen ist deshalb ein den Anforderungen der DSGVO genügender Datenschutz- und Datensicherheitsstandard sicherzustellen. Bei einer Integration mobiler oder anderer neuer Technologien in die Regelversorgung sowie in das E-Health-System ist deren datenschutz- und datensicherheitsgerechte Ausgestaltung zu garantieren. Ebenso ist Transparenz für die Nutzer herzustellen.

Zu verhindern ist, dass Gesundheitsdaten zur Bemessung von Versicherungstarifen laufend erhoben und vertragsbegleitend genutzt werden. Im Bereich der Krankenversicherung drohen mit der Erhebung von Gesundheitsdaten mittels sog. Wearables und Fitness-Apps Diskriminierungen von Versicherten durch das Angebot gesundheitsbezogener Tarife. Bei der Bemessung von Versicherungstarifen dürfen nicht die Patienten und Versicherten benachteiligt werden, die einer umfassenden Erfassung und Übertragung von Gesundheitsdaten nicht zustimmen.

Mit Datenschutz E-Government gestalten

Die DSK fordert, für die verwaltungsebenenübergreifende Umsetzung von E-Government Verwaltungsdienstleistungen sicher und datenschutzgerecht anzubieten.

Das Onlinezugangsgesetz schafft zwar durch einen Portalverbund zwischen allen Verwaltungsangeboten des Bundes, der Länder und der Kommunen sowie ein Nutzerkonto für jedermann die rechtlichen Voraussetzungen. Die DSK weist aber darauf hin, dass E-Government Akzeptanz in der Verwaltung wie bei den Bürgern bedingt.

Die DSK fordert deshalb Bund und Länder auf, mit Datenschutz E-Government konsequent vertrauenswürdig zu gestalten, im Sinne eines Datenschutzes „by Design“ und „by Default“. Die Ende-zu-Ende-Verschlüsselung der Kommunikation, Konzepte mit Datenschutzgarantien

(z. B. datenschutzkonforme Bezahlsysteme und deutsche oder europäische „Trusted-Cloud“-Lösungen) und ein umfassendes Datenschutz- und Informationssicherheitsmanagement bilden dafür wesentliche Grundlagen. Rechtskonform müssen auch neue Entwicklungen wie „Data Driven Government“ – Verwaltungsentscheidungen auf Basis von Daten und Analysen – umgesetzt werden: mit Techniken zur Anonymisierung und Aggregation statt zentralisierter Anhäufung und Auswertung personenbezogener Daten.

Stärkung des internationalen Datenschutzes

Die DSK fordert die Bundesregierung auf, sich bei Entscheidungen der Europäischen Kommission über die Zulässigkeit von Datentransfers in Drittstaaten für ein hohes Datenschutzniveau einzusetzen. Zudem sind Versuche abzuwehren, den Datenschutz durch internationale Handelsverträge einzuschränken.

Das Bestreben der Europäischen Kommission, Drittstaatentransfer auf der Basis von Angemessenheitsbeschlüssen zu vereinfachen, darf nicht zu einer Erosion des Grundrechts auf informationelle Selbstbestimmung führen.

Die Bundesregierung sollte sich daher dafür einsetzen, dass die vom EuGH (C-362/14) aufgestellten Grundsätze Maßstab für Angemessenheitsentscheidungen bleiben. Künftige Handelsverträge dürfen den Datenschutz nicht aushöhlen, indem datenschutzrechtliche Regelungen als Handelshemmnis angesehen oder zum Gegenstand etwaiger Investor-Staat-Streitverfahren werden. Auch datenschutzrechtliche Standards im Europarat, in der OECD und den Vereinten Nationen müssen ein vergleichbar hohes Datenschutzniveau aufweisen.

2 Beschlüsse der Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich (Düsseldorfer Kreis)

Beschluss vom 13./14. September 2016: Fortgeltung bisher erteilter Einwilligungen unter der Datenschutz-Grundverordnung

Bisher erteilte Einwilligungen gelten fort, sofern sie der Art nach den Bedingungen der Datenschutz-Grundverordnung entsprechen (Erwägungsgrund 171, Satz 3 Datenschutz-Grundverordnung).

Bisher rechtswirksame Einwilligungen erfüllen grundsätzlich diese Bedingungen.

Informationspflichten nach Artikel 13 Datenschutz-Grundverordnung müssen dafür nicht erfüllt sein, da sie keine Bedingungen im Sinne des genannten Erwägungsgrundes sind.

Besondere Beachtung verdienen allerdings die folgenden Bedingungen der Datenschutz-Grundverordnung; sind diese Bedingungen nicht erfüllt, gelten bisher erteilte Einwilligungen nicht fort:

Freiwilligkeit („Kopplungsverbot“, Artikel 7 Absatz 4 in Verbindung mit Erwägungsgrund 43 Datenschutz-Grundverordnung),

Altersgrenze: 16 Jahre (soweit im nationalen Recht nichts anderes bestimmt wird; Schutz des Kindeswohls, Artikel 8 Absatz 1 in Verbindung mit Erwägungsgrund 38 Datenschutz-Grundverordnung).

3 Entschließungen der Konferenz der Informationsfreiheitsbeauftragten in Deutschland

3.1 33. Konferenz der Informationsfreiheitsbeauftragten am 13. Juni 2017 in Mainz

Mit Transparenz gegen „Fake-News“

Internet und soziale Medien eröffnen zunehmend auch Möglichkeiten für die gezielte Verbreitung von Falschmeldungen zur Beeinflussung der politischen Meinungs- und Willensbildung. Eine informierte und kritische Gesellschaft benötigt jedoch vielfältige, freie und qualitativ aussagekräftige Informationen für eine umfassende gesellschaftliche und politische Teilhabe. Da die öffentlichen Stellen der Länder und des Bundes über solche Informationen verfügen, kommt ihnen insoweit eine Schlüsselrolle zu. Deshalb ist es von zentraler Bedeutung, dass staatliche Institutionen transparent agieren, um das Vertrauen in die Demokratie und in deren Akteure zu stärken. Für den Prozess der politischen Meinungs- und Willensbildung sind verlässliche und solide Informationen eine unverzichtbare Voraussetzung.

Die Konferenz der Informationsfreiheitsbeauftragten in Deutschland appelliert an alle öffentlichen Stellen in Deutschland, sich ihrer Verantwortung für die Informationsfreiheit bewusst zu sein und durch größtmögliche Transparenz – sowohl auf Antrag als auch proaktiv – die Bürgerinnen und Bürger in ihrer politischen Willensbildung zu unterstützen. Sie wirbt dafür, dass sich öffentliche Stellen in Deutschland noch stärker öffnen, auf die Informationswünsche der Bürgerinnen und Bürger eingehen, mit behördlichen Dokumenten valide und qualitätsvolle Informationen aus vertrauenswürdiger Quelle bereitstellen und die Kontrolle durch die Bürgerinnen und Bürger ermöglichen.

Damit kann auch bewusst gestreuten Fehlinformationen, mit denen die Manipulation des Meinungsbildes und die Schwächung demokratischer Institutionen verfolgt wird, aktiv und aufgeklärt im öffentlichen Diskurs entgegengetreten werden.

3.2 32. Konferenz der Informationsfreiheitsbeauftragten am 2. Dezember 2016 in Düsseldorf

„Nicht bei Open Data stehenbleiben: Jetzt auch Transparenzgesetze in Bund und Ländern schaffen!“

Entschließung der Informationsfreiheitsbeauftragten[1]

Die Konferenz der Informationsfreiheitsbeauftragten fordert die Gesetzgeber in Bund und Ländern auf, jetzt flächendeckend Transparenzgesetze zu schaffen. Solche Gesetze verbinden den individuellen, antragsgebundenen Informationszugangsanspruch mit der Verpflichtung öffentlicher Stellen, bestimmte Informationen aktiv auf Informationsplattformen im Internet zu veröffentlichen.

Anlass für die Forderung ist ein Beschluss der Regierungschefs von Bund und Ländern vom 14. Oktober 2016. Nach dieser Vereinbarung werden Bund und Länder Open-Data-Gesetze erlassen und das Ziel verfolgen, bundesweit vergleichbare Standards für den Zugang zu öffentlichen Datenpools zu erreichen.

Die Informationsfreiheitsbeauftragten befürworten zwar die Zielrichtung des Beschlusses; dieser greift jedoch zu kurz. Neben der Bereitstellung von Rohdaten in standardisierten und offenen Formaten für eine Weiterverwendung gebietet die Transparenz öffentlichen Handelns, zusammenhängende, aus sich heraus nachvollziehbare Unterlagen zur Verfügung zu stellen. Hierfür kommen beispielsweise Verträge, Gutachten, Studien, umweltrelevante Konzepte, Pläne, Programme oder Zulassungsentscheidungen, Berichte, Protokolle, Beschlüsse, Organisationserlasse, Statistiken, öffentliche Planungen, Haushalts-, Stellen-, Organisations-, Geschäftsverteilungs- und Aktenpläne, Drucksachen, Verwaltungsvorschriften oder wesentliche Bestandteile von Subventions- und Zuwendungsvergaben und Baugenehmigungen sowie die wesentlichen Unternehmensdaten öffentlicher Beteiligungen einschließlich der Vergütung der Leitungsebenen infrage.

Daher fordert die Konferenz, dass Bund und Länder ihre Behörden verpflichten, derartige Dokumente grundsätzlich im Internet zu veröffentlichen. Der bekannt gewordene Entwurf des Eckpunktepapiers des Bundes vom 18.10.2016[2] genügt diesen Anforderungen nicht. Anstatt separate Gesetze zu schaffen oder die Regelungen den eher informationstechnisch orientierten E-Government-Gesetzen zu überlassen, sollte der Beschluss der Regierungschefs von Bund und Ländern so umgesetzt werden, dass Open-Data-

1 Bei Enthaltung des Bundes.

2 Siehe netzpolitik.org.

Regelungen in Transparenzgesetze aufgenommen werden. Länder, die noch nicht über solche Gesetze verfügen, sollten nach Auffassung der Informationsfreiheitsbeauftragten vorhandene Informationsfreiheitsgesetze entsprechend fortentwickeln. Auch fordert die Konferenz jene Länder auf, die keinen allgemeinen Anspruch auf Informationszugang gewähren, endlich ein modernes Informationsrecht einzuführen.

3.3 31. Konferenz der Informationsfreiheitsbeauftragten am 15. Juni 2016 in Düsseldorf

GovData: Alle Länder sollen der Verwaltungsvereinbarung beitreten und Daten auf dem Portal bereitstellen!

„GovData – das Datenportal für Deutschland“ ist eine Anwendung des IT-Planungsrats, die auf der Grundlage einer Verwaltungsvereinbarung vom Bund und mehreren Ländern betrieben wird. Das Portal bietet einen einheitlichen zentralen Zugang zu offenen Verwaltungsdaten aus Bund, Ländern und Kommunen. Ziel ist es, diese Daten möglichst flächendeckend zur Verfügung zu stellen und sie an einer zentralen Stelle auffindbar und so einfacher nutzbar zu machen. GovData dient damit nicht nur der Information der Bürgerinnen und Bürger, sondern fördert zugleich auch die Transparenz und Akzeptanz des Verwaltungshandelns. Es stellt der Wirtschaft darüber hinaus Verwaltungsdaten zur Entwicklung neuer Geschäftsmodelle zur Verfügung.

Bislang beteiligen sich jedoch an dem Bund-Länder-Online-Portal noch nicht alle Länder. Viele Daten, an deren Veröffentlichung ein großes öffentliches Interesse besteht, sind noch nicht abrufbar. Das immense wirtschaftliche Potential von Open Data bleibt ungenutzt.

Sowohl für die Wirtschaft als auch für die Zivilgesellschaft ergeben sich erhebliche Vorteile durch einen freien Zugang zu den öffentlichen Daten der Verwaltung. Der Umfang und die Qualität der in GovData zur Verfügung gestellten Daten müssen verbessert und der Nutzwert des Portals weiter erhöht werden.

Daher appelliert die Konferenz der Informationsfreiheitsbeauftragten in Deutschland an die verbleibenden Länder, der Verwaltungsvereinbarung beizutreten, und fordert alle Vereinbarungspartner zur verstärkten Bereitstellung von Daten auf.

3.4 Entschließung zwischen der 30. und 31. Konferenz

Entschließung vom 28. April 2016: Auch die Verwaltungen der Landesparlamente sollen Gutachten der Wissenschaftlichen Dienste proaktiv veröffentlichen!

Nach der aktuellen Rechtsprechung des Bundesverwaltungsgerichts (Urteil vom 25. Juni 2015, Az.: 7 C 1/14) muss die Bundestagsverwaltung auf Antrag Zugang zu den Ausarbeitungen der Wissenschaftlichen Dienste gewähren.

Wie der Deutsche Bundestag inzwischen bekannt gab, bedarf es derartiger individueller Anträge seit dem 18. Februar 2016 nicht mehr, denn die Bundestagsverwaltung veröffentlicht generell die Ausarbeitungen der Wissenschaftlichen Dienste nunmehr vier Wochen nach Auslieferung an die auftraggebenden Abgeordneten, damit diese zunächst die Möglichkeit haben, die Gutachten exklusiv nutzen zu können, proaktiv im Internet. Dabei werden die Namen der Auftraggeber nicht bekannt gegeben.

Die Entscheidung zur proaktiven Veröffentlichung ist im Sinne von Open Data und Transparenz nachdrücklich zu unterstützen, da es ein großes öffentliches Interesse an den Ausarbeitungen der Wissenschaftlichen Dienste gibt. So lagen infolge der neuen Rechtsprechung des Bundesverwaltungsgerichts der Bundestagsverwaltung in kürzester Zeit weit über 2000 Informationszugangsanträge vor. Die individuelle Bearbeitung dieser Anträge hätte in aller Regel viel Zeit gebunden und unnötig hohe Personal- und Sachkosten verursacht. Durch die Entscheidung werden die Kosten sowohl für die Verwaltung als auch für die Bürgerinnen und Bürger deutlich gesenkt. Die Ausarbeitungen stehen der interessierten Öffentlichkeit zukünftig schnell und einfach zur Verfügung.

Vor diesem Hintergrund fordert die Konferenz der Informationsfreiheitsbeauftragten in Deutschland die Verwaltungen der Landesparlamente auf, dem Beispiel der Bundestagsverwaltung in Sachen Transparenz und Open Data zu folgen. Dabei sind etwaige Ausschlussgründe (insbesondere durch Schwärzung der Namen der Auftraggeber) sowie landesrechtliche Vorgaben zu berücksichtigen. Auch die Verwaltungen der Landesparlamente sollten Ausarbeitungen der jeweiligen Wissenschaftlichen Dienste bzw. der Gesetzgebungs- und Beratungsdienste unabhängig von individuellen Zugangsanträgen im Internet veröffentlichen, soweit dies nicht bereits geschieht.

4 Forderungen der Informationsfreiheitsbeauftragten der Länder

4.1 Grundsatzpositionen der Landesbeauftragten für die Informationsfreiheit vom 6. Oktober 2017

Informationen sind die Basis einer Demokratie. Sie sind Grund- und Treibstoff des Prozesses der öffentlichen Meinungsbildung. Transparenz schafft Vertrauen zwischen Politik, Verwaltung und Bevölkerung. Das Recht auf Zugang zu Informationen stellt ein zentrales Element zur Regelung des Informationsflusses von staatlichen Stellen zu Bürgerinnen und Bürgern in Deutschland dar. Die Informationsfreiheitsbeauftragten der Länder wenden sich mit den folgenden Forderungen zunächst an die Bundespolitik mit dem Ziel, dass sie im Rahmen ihrer Kompetenzen diesen Grundaussagen zur Geltung verhilft. Auch gegenüber der Landespolitik sollen diese Forderungen als grundsätzliche Anregungen zur Weiterentwicklung und zum Ausbau der informatorischen Rechtsstellung des Einzelnen auch gegenüber der Landespolitik dienen.

I. Informationsfreiheit in die Verfassungen!

Der Anspruch auf freien Zugang zu amtlichen Informationen soll in das Grundgesetz und in die Landesverfassungen aufgenommen werden

In dem Beschluss vom 20. Juni 2017 (1 BvR 1978/13) stellt das Bundesverfassungsgericht fest, dass sich der Verfassungsrang der Informationszugangsfreiheit aus Art. 5 Abs. 1 Satz 1 Grundgesetz herleitet, jedenfalls soweit der Gesetzgeber eine einfachgesetzliche Regelung getroffen hat. Wer die Informationsfreiheit ernst nimmt, kann sie nicht in das Belieben des Gesetzgebers stellen. Deshalb ist die explizite Normierung im Grundgesetz erforderlich. Damit wäre für die Länder, die immer noch kein Recht auf voraussetzungslosen Zugang haben, die Pflicht verbunden, ein solches Recht einfachgesetzlich zu verankern. Auch im Jahr 2017 verfügt ein Viertel der Länder immer noch nicht über ein Informationsfreiheitsgesetz.

II. Ein Gesetz für den Informationszugang! Hin zu Transparenzgesetzen!

Zusammenfassung der verschiedenen Informationsfreiheitsgesetze in einem Gesetz und Weiterentwicklung zu Transparenzgesetzen mit umfassenden Veröffentlichungspflichten

Bestehende Informationszugangsansprüche in unterschiedlichen Informationsfreiheits- bzw. Transparenz- und Fachgesetzen sollten verstärkt zusammengefasst werden. Die Ansprüche auf Einsicht in Verwaltungsakten und auf Zugang zu sonstigen Informationen öffentlicher Stellen sind derzeit auf eine

Vielzahl von Einzelvorschriften verteilt: Sie finden sich in den Informationsfreiheitsgesetzen, in den Umweltinformationsgesetzen, im Verbraucherinformationsgesetz und in diversen weiteren Gesetzen. Dabei werden vergleichbare Sachverhalte unterschiedlich geregelt, etwa die Voraussetzungen für den Informationszugang, die Fristen zur Beantwortung von Anfragen, die Gebühren, welche für den Informationszugang zu entrichten sind, und die Rechte auf Anrufung der Informationsfreiheitsbeauftragten. Diese Zersplitterung erschwert die Wahrnehmung der Informationsrechte und trägt zu Unsicherheiten bei der Rechtsanwendung durch die Behörden bei. Zukünftig sollten die Vorschriften so gestaltet werden, dass ein Höchstmaß an Transparenz und Bürgerfreundlichkeit erreicht wird.

Neben diesen anzustrebenden Erleichterungen für die Bürgerinnen und Bürger bei der Durchsetzung ihrer Informationszugangsansprüche ist die Weiterentwicklung der jeweiligen Informationsfreiheitsgesetze zu Transparenzgesetzen ein wichtiges Anliegen. Solche Gesetze verbinden den individuellen, antragsgebundenen Informationszugangsanspruch mit der Verpflichtung öffentlicher Stellen, bestimmte Informationen von sich aus und antragsunabhängig auf Informationsplattformen im Internet zu veröffentlichen. Derartige gesetzliche Veröffentlichungspflichten erhöhen die Verwaltungstransparenz, die Nachvollziehbarkeit, Akzeptanz und Kontrolle behördlicher Entscheidungsprozesse.

Die Verwaltung soll zukünftig ihre Daten automatisch zur Verfügung stellen. Ausnahmen für die Nichtzurverfügungstellung müssen begründet werden. Das wirtschaftliche Potential von offenen Verwaltungsdaten wird bisher nicht ausreichend genutzt.

III. Nachrichtendienste ins IFG!

Erweiterung des Anwendungsbereichs der Informationsfreiheitsgesetze durch Abschaffung der Bereichsausnahme für die Nachrichtendienste

Die Informationsfreiheitsbeauftragten der Länder halten die in § 3 Nr. 8 IFG normierte Bereichsausnahme für die Nachrichtendienste für nicht erforderlich. Es läuft dem Transparenzgedanken zuwider, dass ein kompletter Verwaltungsbereich vom Informationsfreiheitsgesetz ausgenommen wird. Die Regelung führt dazu, dass die Nachrichtendienste im Fall eines Antrages nicht begründen müssen, warum eine Information nicht herauszugeben ist. Das bedeutet zudem, dass auch nicht-geheimhaltungsbedürftige Informationen zurückbehalten werden können.

Die Informationsfreiheitsbeauftragten stellen mit ihrer Forderung nicht den Geheimnisschutz an sich in Frage. Sie sind vielmehr der Ansicht, dass es ausreicht, wenn sich die Nachrichtendienste hinsichtlich der Herausgabe

bzw. Nichtherausgabe von Informationen auf die Ausschlusstatbestände des Informationsfreiheitsgesetzes berufen können. Somit wären die Nachrichtendienste dazu verpflichtet, ihre Entscheidungen zu begründen.

Vergleiche mit Bundesländern wie beispielsweise Schleswig-Holstein, Rheinland-Pfalz und Mecklenburg-Vorpommern zeigen, dass die Verfassungsschutzbehörden auch ohne Bereichsausnahme nicht auf Geheimnisschutz verzichten müssen.

IV. Abschaffung unnötiger Ausnahmen!

Beschränkungen der Ausnahmeregelungen auf das verfassungsrechtlich zwingend gebotene Maß auf der Grundlage der Evaluierung des IFG Bund

Bei der Regelung ihrer Informationsfreiheitsgesetze haben sich zahlreiche Länder in der Vergangenheit am Informationsfreiheitsgesetz des Bundes orientiert, das für sie eine Vorbildfunktion hatte. Nach dessen Evaluierung im Jahr 2012 ergibt sich für den Bund und damit inzident auch für diejenigen Bundesländer, die mit ihrem Landesrecht dem Bund gefolgt waren, erheblicher Reformbedarf. So ist etwa eine Reduzierung und Harmonisierung der Ausschlussgründe, die einem Informationszugang entgegenstehen können, angezeigt. Zu viele, teilweise redundante und sich überschneidende Ausschlussgründe konterkarieren Open Data, Open Government und damit Bürgerbeteiligung und Demokratie. Eine allgemeine Güterabwägung zwischen Informations- und Geheimhaltungsinteresse (public interest test) ist daher als Korrektiv erforderlich.

V. Mehr Transparenz in der Drittmittelforschung!

Sicherstellung von Transparenz der Kooperationen zwischen privaten und wissenschaftlichen Einrichtungen

Unternehmensfinanzierte Forschung gewinnt zunehmende Bedeutung für die Hochschulen in der Bundesrepublik Deutschland. Deutschlandweit ist eine große Anzahl von Lehrstühlen direkt oder indirekt von Unternehmen finanziert. Oft sind Ziele und Umfang der Förderung für Außenstehende nicht erkennbar. Für eine Einordnung der Forschungsergebnisse und deren Bewertung ist die Kenntnis dieser Hintergründe jedoch bedeutsam. Die Freiheit von Forschung und Wissenschaft lebt von einer offenen Diskussion; die Geheimhaltung von Zusammenhängen kann diese Freiheiten einengen.

Einer verborgenen Einflussnahme auf Forschungsgegenstände, Forschungsergebnisse und auf deren Veröffentlichung kann durch eine konsequente Politik der Offenheit begegnet werden. Deshalb sollten Kooperationsverträge

zwischen Wissenschaft und Unternehmen grundsätzlich offengelegt werden. Die Pflicht zur Veröffentlichung der Verträge darf nur zurücktreten, soweit und solange die Bekanntgabe geschützte Interessen beeinträchtigt.

Die regelmäßige Offenlegung der Finanzierung von Forschungsprojekten ist nach Auffassung der Informationsfreiheitsbeauftragten ein geeignetes Instrument, um die Freiheit der Forschung zu schützen, indem einseitige Abhängigkeiten oder auch nur deren Anschein vermieden werden. Eine bloße Selbstverpflichtung der Universitäten und Forschungseinrichtungen ist hierfür nicht ausreichend. Die Informationsfreiheitsbeauftragten der Länder fordern konsequente gesetzliche Regelungen zugunsten der Transparenz von drittmittelgeförderter Forschung in Bund und Ländern.

4.2 Beschluss der Informationsfreiheitsbeauftragten der Länder vom 13. Juni 2017: Grundsatzforderungen zu Informationsfreiheit und Transparenz

Die Landesbeauftragten für die Informationsfreiheit stellen Forderungen auf, um Fortschritte und Weiterentwicklungen zu mehr und besserer Wahrung von Informationsfreiheit und Transparenz zu erreichen. Diese Forderungen richten sich an die künftige Bundesregierung, aber auch an Bund und Länder insgesamt im Rahmen ihrer jeweiligen Zuständigkeiten.

Die Forderungen sind:

I. Verankerung des Anspruchs auf freien Zugang zu amtlichen Informationen im Grundgesetz und in den Landesverfassungen!

II. Weiterentwicklung der Informationsfreiheitsgesetze zu Transparenzgesetzen mit umfassenden Veröffentlichungspflichten!

III. Schaffung eines einheitlichen und umfassenden Informationsrechts: Zusammenfassung der Rechte auf amtliche Informationen, Umweltinformationen und auf Verbraucherinformationen!

IV. Abschaffung der Bereichsausnahme für die Nachrichtendienste und neuer Umgang mit Verschlusssachen!

V. Beschränkungen der Ausnahmeregelungen auf das verfassungsrechtlich zwingend gebotene Maß!

VI. Sicherstellung der Transparenz von Kooperationen zwischen Privaten und wissenschaftlichen Einrichtungen!

VII. Harmonisierung der europäischen Informationsfreiheitsrechte!

4.3 Entschließung der Informationsfreiheitsbeauftragten der Länder vom 24. April 2017: Open Data: Gesetzentwurf der Bundesregierung greift zu kurz!

Die Informationsfreiheitsbeauftragten der Länder fordern den Deutschen Bundestag auf, statt des von der Bundesregierung vorgelegten Entwurfs eines Open-Data-Gesetzes (Erstes Gesetz zur Änderung des E-Government-Gesetzes) das Informationsfreiheitsgesetz des Bundes zu einem umfassenden Transparenzgesetz zu entwickeln. Bereits im Dezember letzten Jahres hat die Konferenz der Informationsfreiheitsbeauftragten in Deutschland ihre Bedenken angesichts des geplanten Open-Data-Gesetzes in einer Entschließung zum Ausdruck gebracht. Das mittlerweile fortgeschrittene Gesetzgebungsverfahren bietet Anlass, noch einmal ausdrücklich auf folgende Bedenken hinzuweisen:

Der Deutsche Bundestag hat sich am 31. März 2017 in erster Lesung mit dem Entwurf der Bundesregierung für ein Erstes Gesetz zur Änderung des E-Government-Gesetzes (BT-Drucksache 18/11614) befasst. Bund und Länder hatten am 14. Oktober 2016 vereinbart, Open Data zu stärken. Dabei verpflichteten sich die Länder, Open-Data-Gesetze nach dem Beispiel der Bundesregelung zu erlassen. Die Ergebnisse im aktuellen Gesetzgebungsverfahren auf Bundesebene werden daher erhebliche Auswirkungen auf die Landesgesetzgebung haben.

Neben Rohdaten auch Dokumente aktiv veröffentlichen

Der Entwurf richtet sich ausschließlich auf die Bereitstellung von Rohdaten. Informationen, die aus sich heraus verständlich sind, zum Beispiel Verträge, Gutachten, Stellungnahmen und ähnliche Dokumente, sind davon nicht umfasst. Für das von der Bundesregierung angestrebte Ziel der Stärkung zivilgesellschaftlicher Teilhabe ist dies aber ein entscheidender Gehalt des Gesetzes.

Transparenzregelungen gehören in Transparenzgesetze

Die Informationsfreiheitsbeauftragten der Länder sind der Ansicht, dass das Informationsfreiheitsgesetz des Bundes der richtige Standort für eine Open-Data-Regelung wäre. Die Aufnahme von Open-Data-Regelungen in das E-Government-Gesetz des Bundes fördert zwar den Open-Data-Gedanken. Dabei darf jedoch nicht übersehen werden, dass die Behörden des Bundes nach wie vor verpflichtet bleiben, amtliche Informationen nach Maßgabe des Informationsfreiheitsgesetzes des Bundes zur Verfügung zu stellen. Eine zusätzliche Einzelregelung für offene Daten passt nicht in das bislang informationstechnisch orientierte E-Government-Gesetz. Statt die Regelung dort einzufügen, sollten die vorgesehenen Regelungen im Informationsfreiheits-

gesetz verankert werden. Dieses würde so zu einem modernen Transparenzgesetz, das erforderlichenfalls als weiteres Vorbild für die Landesgesetzgebung dienen könnte. Jede weitere Zersplitterung der ohnehin bereits unübersichtlichen Regelungen zum Informationszugang sollte vermieden werden.

Keine zusätzlichen Ausnahmen

Der Gesetzentwurf verweist zwar auf die Ausnahmetatbestände des Informationsfreiheitsgesetzes, enthält aber noch weitere Ausnahmen. Beispielsweise sollen nur Daten veröffentlicht werden, die außerhalb der Behörde liegende Verhältnisse betreffen. Das mit dem Gesetzentwurf verfolgte Ziel nach „mehr Teilhabe interessierter Bürgerinnen und Bürger und eine intensivere Zusammenarbeit der Behörde mit diesen“ dürfte damit nicht erreicht werden. Es erscheint insgesamt inkonsequent, Open Data durch Ausnahmen zu beschränken, die über die Regelung des Informationsfreiheitsgesetzes hinausgehen. Hiervon ist abzusehen. Die Weiterentwicklung der Informationsfreiheit kann nur im Abbau von Ausnahmen bestehen, nicht in deren Ausweitung.

Individueller Anspruch auf Veröffentlichung

Der Regierungsentwurf gewährt keinen individuellen Anspruch auf die Veröffentlichung von Daten. Ein solcher Anspruch, der von jedermann einklagbar wäre, ist als effektives Korrektiv zu einer reinen Selbstverpflichtung der öffentlichen Stellen jedoch unverzichtbar.

Für die Länder, die amtliche Informationen auf der Grundlage von Informationsfreiheitsgesetzen bereits in Informationsregistern zur Verfügung stellen, wie auch für die anderen Länder kann das geplante Open-Data-Gesetz in dieser Form keine Vorbildfunktion entfalten. Die Weiterentwicklung des Informationsfreiheitsgesetzes des Bundes zu einem Transparenzgesetz mit den dazugehörigen Open-Data-Regelungen könnte dagegen eine entsprechende Signalwirkung für die Länder haben.

Die Informationsfreiheitsbeauftragten der Länder fordern den Bundestag eindringlich auf, den eingeschlagenen Sonderweg zu überdenken.

5 Abkürzungsverzeichnis

ABl.	=	Amtsblatt
Abs.	=	Absatz
AIG	=	Akteneinsichts- und Informationszugangsgesetz
AOK	=	Allgemeine Ortskrankenkasse
App	=	Applikation (Anwendungssoftware) für mobile Endgeräte
Art.	=	Artikel
BbgDSG	=	Brandenburgisches Datenschutzgesetz
BbgKVerf	=	Kommunalverfassung des Landes Brandenburg
BbgPolG	=	Brandenburgisches Polizeigesetz
BbgSchulG	=	Brandenburgisches Schulgesetz
BbgVerfSchG	=	Brandenburgisches Verfassungsschutzgesetz
BbgVermG	=	Brandenburgisches Vermessungsgesetz
BCC	=	Blind Carbon Copy
BCR	=	Binding Corporate Rules
BDSG	=	Bundesdatenschutzgesetz
BGB	=	Bürgerliches Gesetzbuch
BIC	=	Bank Identifier Code
BKAG	=	Bundeskriminalamtsgesetz
BLB	=	Brandenburgischer Landesbetrieb für Liegenschaften und Bauen
BMG	=	Bundesmeldegesetz
BMI	=	Bundesministerium des Innern
BR	=	Bundesrat
BSI	=	Bundesamt für Sicherheit in der Informationstechnik
BT	=	Bundestag
Buchst.	=	Buchstabe
B. V.	=	Besloten vennootschap met beperkte aansprakelijkheid (niederländische Gesellschaft mit beschränkter Haftung)
BVerwGE	=	Entscheidungen des Bundesverwaltungsgerichts
bzw.	=	beziehungsweise

CAFM	=	Computer Aided Facility Management
CAM	=	Cooperative Awareness Message
CC	=	Carbon Copy
C-IST	=	Cooperative Intelligent Transport Systems
DENM	=	Decentralized Environmental Notification Message
d. h.	=	das heißt
DIN	=	Deutsches Institut für Normung
DNA	=	Deoxyribonucleic Acid (Desoxyribonukleinsäure)
Drs.	=	Drucksache
DS-GVO	=	Datenschutz-Grundverordnung
DSK	=	Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder
DSV	=	Datenschutzverordnung Schulwesen
EEG	=	Erneuerbare-Energien-Gesetz
EES	=	Entry-Exit-System
eID	=	elektronische Identität
ErwGr.	=	Erwägungsgrund
ETIAS	=	European Travel Information and Authorization System (EU-weites Reiseinformations- und -genehmigungs-system)
EU	=	Europäische Union
EuGH	=	Europäischer Gerichtshof
e. V.	=	eingetragener Verein
FDR	=	Falldatei Rauschgift
ff.	=	folgende (Seiten)
GG	=	Grundgesetz
ggf.	=	gegebenenfalls
GmbH	=	Gesellschaft mit beschränkter Haftung
GRCh	=	EU-Grundrechtecharta
IBAN	=	International Bank Account Number (Internationale Bankkontonummer)
ID	=	Identifier (Identitätskennung)
IFG	=	Informationsfreiheitsgesetz

ILITA	=	The Israel Law, Information and Technology Authority (Israelische Datenschutzaufsichtsbehörde)
insbes.	=	insbesondere
ISMT	=	Informationssicherheitsmanagementteam
IT	=	Informationstechnik
i. V. m.	=	in Verbindung mit
JI-Richtlinie	=	Datenschutz-Richtlinie im Bereich von Justiz und Inneres
Kfz.	=	Kraftfahrzeug
KitaG	=	Kindertagesstättengesetz
MDM	=	Mobile Device Management
MeldDÜV	=	Verordnung über regelmäßige Datenübermittlungen der Meldebehörden
NFM	=	Neues Finanzmanagement
Nr.	=	Nummer
o. g.	=	oben genannt
OECD	=	Organisation for Economic Co-operation and Development (Organisation für wirtschaftliche Zusammenarbeit und Entwicklung)
ÖPNV	=	Öffentlicher Personennahverkehr
OTA	=	Over The Air
PassG	=	Passgesetz
PAuswG	=	Personalausweisgesetz
PC	=	Personal Computer
PDCA	=	Plan, Do, Check, Act
PIAV	=	Polizeilicher Informations- und Analyseverbund
PNR	=	Passenger Name Record (Fluggastdatensatz)
RFID	=	Radio Frequency Identification
RKI	=	Robert-Koch-Institut
S.	=	Satz
SDM	=	Standard-Datenschutzmodell
SGB II	=	Zweites Buch Sozialgesetzbuch
SGB V	=	Fünftes Buch Sozialgesetzbuch
SGB VIII	=	Achtes Buch Sozialgesetzbuch

SGB X	=	Zehntes Buch Sozialgesetzbuch
SGB XI	=	Elftes Buch Sozialgesetzbuch
sog.	=	sogenannt
StPO	=	Strafprozessordnung
TLS	=	Transport Layer Security
TMG	=	Telemediengesetz
TÜV	=	Technischer Überwachungsverein
u. a	=	unter anderem
u. Ä.	=	und Ähnliches
UN	=	United Nationes
US	=	United States
USA	=	United States of America
usw.	=	und so weiter
vgl.	=	vergleiche
z. B.	=	zum Beispiel
ZIT-BB	=	Brandenburgischer IT-Dienstleister
z. T.	=	zum Teil