Der Bayerische Landesbeauftragte für den Datenschutz informiert die Öffentlichkeit

26. Tätigkeitsbericht

Berichtszeitraum
2013/2014

26. Tätigkeitsbericht des Landesbeauftragten für den Datenschutz

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

Berichtszeitraum: 2013/2014
Veröffentlichungsdatum: 20.01.2015

Inhaltsverzeichnis

1 Überblick

Soweit in den nachfolgenden Ausführungen Bezeichnungen von Personen im Maskulinum verwendet werden, wird diese Form verallgemeinernd verwendet und bezieht sich auf beide Geschlechter.

1.1 Der Spiegel des Alexander – Zur NSA-Spähaffäre

Eine orientalische Sage berichtet, Alexander der Große habe nur in seinen Spiegel blicken müssen, um auf einen Blick alle Pläne des Perserkönigs Darius zu durchschauen. Dadurch gelang es Alexander mehrfach, die zahlenmäßig deutlich überlegenen Heere seines Gegners vernichtend zu schlagen.

Seit dem 06.06.2013 hat die Welt immer mehr Details über das Bündnis der „Five Eyes", einem Zusammenschluss von Nachrichtendiensten der Vereinigten Staaten von Amerika, des Vereinigten Königreichs, Kanadas, Australiens und Neuseelands erfahren. Durch die von Edward Snowden angestoßenen Enthüllungen wissen wir heute, dass die US-amerikanischen Nachrichtendienste mit ihren Bündnispartnern einen totalen Überwachungsansatz verfolgen. Bildlich gesprochen scheint das Bündnis der „Five Eyes" einen Spiegel entwickeln zu wollen, der Einblick in die Gedankenwelt eines jeden Menschen auf dem Erdball ermöglichen soll.

Diese umfassende Überwachung versuchen die betreffenden Nachrichtendienste vor Allem damit zu begründen, dass sie terroristische Anschläge verhindere. Beispielsweise behaupteten hochrangige Vertreter der US-Nachrichtendienste bereits Mitte 2013 sinngemäß, dass durch die Überwachung der NSA in mindestens 54 Fällen Terroranschläge verhindert worden seien. Diese Zahl hat sich als falsch, zumindest als grob irreführende Information herausgestellt. Der damalige NSA-Chef Keith Alexander musste im Rahmen einer Senatsanhörung vom 02.10.2013 einräumen, dass die NSA allenfalls 13 Beiträge zur Aufklärung von Fällen mit Terrorismusbezug geleistet habe. Von der Verhinderung terroristischer Anschläge war dabei keine Rede mehr. Wohl aus gutem Grund: Eine Expertenkommission der renommierten New America Foundation untersuchte später in Bezug auf 225 islamismusverdächtige Personen die für die USA relevanten Terrorismusfälle seit dem 11.09.2001. Sie konnte in keinem dieser Fälle erkennen, dass die Massenüberwachung der NSA zu Hinweisen geführt hätte, die zur Aufdeckung konkreter Anschläge in den USA relevant gewesen waren. Der Bericht kann unter www.newamerica.net/publications/policy/do_nsas_bulk_surveillance_programs_stop_terrorists abgerufen werden. Im Ergebnis haben die aus der Massenüberwachung der Nachrichtendienste stammenden, an andere Sicherheitsbehörden übermittelten Daten jedenfalls in den USA einen nur sehr begrenzten Wert für die Terrorismusbekämpfung erzielt. Unabhängig hiervon ist die Frage zu stellen, ob ein legitimes Ziel wie die Terrorismusbekämpfung in einem freiheitlichen Rechtsstaat wirklich jedes Mittel rechtfertigt.

Nach meiner Überzeugung hat die anlasslose, massenhafte Überwachung des weltweiten Telekommunikationsverkehrs durch das Bündnis der „Five Eyes" vielfach und grundlegend das international verbürgte Menschenrecht auf Privatheit

verletzt. Art. 17 des Internationalen Pakts über die bürgerlichen und politischen Rechte (IPbpR) verlangt, dass niemand willkürlichen oder rechtswidrigen Eingriffen in sein Privatleben, seine Familie, seine Wohnung oder seinen Schriftverkehr ausgesetzt werden darf.

Art. 17 IPbpR
(1) Niemand darf willkürlichen oder rechtswidrigen Eingriffen in sein Privatleben, seine Familie, seine Wohnung und seinen Schriftverkehr oder rechtswidrigen Beeinträchtigungen seiner Ehre und seines Rufes ausgesetzt werden.
(2) Jedermann hat Anspruch auf rechtlichen Schutz gegen solche Eingriffe oder Beeinträchtigungen.

Die Generalversammlung der Vereinten Nationen hat in einer Resolution am 18.12.2013 bekräftigt, dass dieses Menschenrecht auf Privatheit uneingeschränkt auch im digitalen Zeitalter gilt (Resolution 68/167. Das Recht auf Privatheit im digitalen Zeitalter). Art. 17 des Paktes verdeutlicht ebenso wie Art. 8 der Europäischen Menschenrechtskonvention: Die staatliche Überwachung von Menschen ist eine rechtfertigungsbedürftige Ausnahme. Wer wie das Bündnis der „Five Eyes" die Überwachung zur Regel macht, verkehrt also das in den Menschenrechten angelegte Regel-Ausnahme-Verhältnis. Dementsprechend dürfte der britische Geheimdienst Government Communications Headquarters (GCHQ) auch das Grundrecht aus Art. 8 der Europäischen Menschenrechtskonvention massiv verletzt haben. Seine Beteiligung an der weltumspannenden Massenüberwachung der Internet- und Telekommunikation ist Gegenstand eines Verfahrens, das gegenwärtig beim Europäischen Gerichtshof für Menschenrechte anhängig ist (App.No. 58170/13).

Bislang für die Öffentlichkeit völlig ungeklärt ist auch die Frage, inwieweit die deutschen Nachrichtendienste mit den „Five Eyes" kooperiert haben. Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat deshalb sich einerseits gegen eine umfassende und anlasslose Überwachung durch Nachrichtendienste gewandt und andererseits eine umfassende Aufklärung des Sachverhalts eingefordert.

Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 05.09.2013
Keine umfassende und anlasslose Überwachung durch Nachrichtendienste!

Zeit für Konsequenzen

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder stellt fest, dass noch immer nicht alles getan wurde, um das Ausmaß der nachrichtendienstlichen Ermittlungen mithilfe von Programmen wie PRISM, TEMPORA und XKEYSCORE für die Bundesrepublik Deutschland aufzuklären.

Schon die bisherigen Erkenntnisse lassen den Schluss zu, dass die Aktivitäten u.a. des US-amerikanischen und des britischen Geheimdienstes auf eine globale und tendenziell unbegrenzte Überwachung der Internetkommunikation hinauslaufen, zumal große Internet- und Telekommunikationsunternehmen in die Geheimdienstaktionen eingebunden sind.

Da zahlreiche Anbieter von Kommunikationsdienstleistungen, deren Server in den USA stehen, personenbezogene Daten der Menschen in der Bundesrepublik

Deutschland verarbeiten, betreffen die Berichte, dass US-amerikanische Geheimdienste auf dem Territorium der USA personenbezogene Daten umfassend und anlasslos überwachen, auch ihre Daten. Unklar ist daneben noch immer, ob bundesdeutsche Stellen anderen Staaten rechtswidrig personenbezogene Daten für deren Zwecke zur Verfügung gestellt und ob bundesdeutsche Stellen rechtswidrig erlangte Daten für eigene Zwecke genutzt haben.

Die staatliche Pflicht zum Schutz der Grundrechte erfordert es, sich nicht mit der gegenwärtigen Situation abzufinden. Die Regierungen und Parlamente des Bundes und der Länder sind dazu aufgerufen, das ihnen im Rahmen ihrer Zuständigkeiten Mögliche zu tun, um die Einhaltung des deutschen und des europäischen Rechts zu gewährleisten. Das Bundesverfassungsgericht hat festgestellt, dass es "zur verfassungsrechtlichen Identität der Bundesrepublik Deutschland gehört, für deren Wahrung sich die Bundesrepublik in europäischen und internationalen Zusammenhängen einsetzen muss", "dass die Freiheitswahrnehmung der Bürger nicht total erfasst und registriert werden darf". Es müssen daher alle Maßnahmen getroffen werden, die den Schutz der informationellen Selbstbestimmung der in Deutschland lebenden Menschen und ihr Grundrecht auf Vertraulichkeit und Integrität informationstechnischer Systeme für die Zukunft sicherstellen.

Für die Wahrung der Grundrechte der Menschen in der Bundesrepublik Deutschland kommt es nun darauf an, die notwendigen Konsequenzen zu ziehen.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder fordert deshalb:

- *Nationales, europäisches und internationales Recht so weiterzuentwickeln und umzusetzen, dass es einen umfassenden Schutz der Privatsphäre, der informationellen Selbstbestimmung, des Fernmeldegeheimnisses und des Grundrechts auf Vertraulichkeit und Integrität informationstechnischer Systeme garantiert.*

- *Sofern verfassungswidrige nachrichtendienstliche Kooperationen erfolgen, müssen diese abgestellt und unterbunden werden.*

- *Die Kontrolle der Nachrichtendienste muss durch eine Erweiterung der Befugnisse sowie eine gesetzlich festgelegte verbesserte Ausstattung der parlamentarischen Kontrollgremien intensiviert werden. Bestehende Kontrolllücken müssen unverzüglich geschlossen werden. In diesem Zusammenhang ist zu prüfen, ob die Datenschutzbeauftragten verstärkt in die Kontrolle der Nachrichtendienste eingebunden werden können.*

- *Es sind Initiativen zu ergreifen, die die informationelle Selbstbestimmung und das Grundrecht auf Vertraulichkeit und Integrität informationstechnischer Systeme sicherstellen.*

  Dazu gehört,

  - *zu prüfen, ob das Routing von Telekommunikationsverbindungen in Zukunft möglichst nur über Netze innerhalb der EU erfolgen kann.*

  - *sichere und anonyme Nutzungsmöglichkeiten von Telekommunikationsangeboten aller Art auszubauen und zu fördern. Dabei ist sicherzustellen, dass den Betroffenen keine Nachteile entstehen,*

wenn sie die ihnen zustehenden Rechte der Verschlüsselung und Nutzung von Anonymisierungsdiensten ausüben.

- *die Voraussetzungen für eine objektive Prüfung von Hard- und Software durch unabhängige Zertifizierungsstellen zu schaffen.*

- *Völkerrechtliche Abkommen wie das Datenschutz-Rahmenabkommen und das Freihandelsabkommen zwischen der EU und den USA dürfen nur abgeschlossen werden, wenn die europäischen Datenschutzgrundrechte ausreichend geschützt werden. Das bedeutet auch, dass jeder Mensch das Recht hat, bei vermutetem Datenmissbrauch den Rechtsweg zu beschreiten. Das Fluggastdatenabkommen und das Überwachungsprogramm des Zahlungsverkehres müssen auf den Prüfstand gestellt werden.*

- *Auch innerhalb der Europäischen Union ist sicherzustellen, dass die nachrichtendienstliche Überwachung durch einzelne Mitgliedstaaten nur unter Beachtung grundrechtlicher Mindeststandards erfolgt, die dem Schutzniveau des Art. 8 der Charta der Grundrechte der Europäischen Union entsprechen.*

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder fordert alle Verantwortlichen auf, die umfassende Aufklärung mit Nachdruck voranzutreiben und die notwendigen Konsequenzen zügig zu treffen. Es geht um nichts weniger als das Grundvertrauen der Bürgerinnen und Bürger in den Rechtsstaat.

Zur Aufklärung der nachrichtendienstlichen Internet- und Telekommunikationsüberwachung seit Jahresbeginn 2001 hat der Deutsche Bundestag einen Untersuchungsausschuss eingesetzt (Einsetzungsbeschluss vom 18.03.2014, Bundestags-Drucksache 18/843). Vor dem Hintergrund der Entschließung vom 05.09.2013 begrüße ich diesen Schritt.

Insbesondere hat sich auch der Bayerische Landtag mehrfach mit der NSA-Affäre auseinandergesetzt. Unter anderem hat der Ausschuss für Kommunale Fragen, Innere Sicherheit und Sport mich im November 2013 eingeladen, zur NSA-Spähaffäre Stellung zu nehmen. Im Rahmen dieser Anhörung kündigte ich an, etwaige Kooperationen des Bayerischen Landesamts für Verfassungsschutz mit ausländischen Sicherheitsbehörden näher zu überprüfen. Diese Überprüfung ist mittlerweile erfolgt (zum Ergebnis dieser Prüfung siehe Nr. 4.4.4).

Ebenfalls im November 2013 hat die Bayerische Staatsregierung intensiv mögliche Folgerungen aus der NSA-Affäre für die Datensicherheit erörtert (Bericht aus der Kabinettsitzung vom 06.11.2013, abrufbar unter www.bayern.de „Pressemitteilungen“). In diese Überlegungen der Bayerischen Staatsregierung wurde ich eingebunden und habe dabei insbesondere Verbesserungen in der vertraulichen Kommunikation empfohlen. Überdies habe ich darauf hingewiesen, dass es um die Möglichkeiten der Bürgerinnen und Bürgern zum technischen Selbstschutz gegen Überwachungsmaßnahmen allgemein schlecht bestellt ist. Für die digitale Kommunikation mit sensiblen Inhalten halte ich es daher für äußerst wünschenswert, wenn der Freistaat Bayern die Entwicklung einer nutzerfreundlichen Ende-zu-Ende-Verschlüsselung und ähnliche Mittel zum Selbstdatenschutz nachhaltig fördern würde.

Insgesamt möchte ich auf die Entschließung der 87. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 27./28.03.2014 aufmerksam machen, die auf notwendige technische und organisatorische Schutzmaßnahmen hingewiesen hat.

Entschließung der 87. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 27./28.03.2014
Gewährleistung der Menschenrechte bei der elektronischen Kommunikation

Die Enthüllungen des Whistleblowers Edward Snowden haben ein Ausmaß an geheimdienstlicher Überwachung aufgezeigt, das viele zuvor nicht für möglich gehalten hatten. Die tendenziell unbegrenzte und kaum kontrollierte Überwachung der elektronischen Kommunikation aller verletzt das auch im digitalen Zeitalter weltweit anerkannte Recht auf Privatheit in täglich wiederkehrender millionenfacher Weise. Dies beeinträchtigt zugleich die Wahrnehmung anderer Menschenrechte wie der Meinungs- und Versammlungsfreiheit. Es ist eine gesamtgesellschaftliche Aufgabe, berechtigtes Vertrauen in die prinzipielle Unverletzlichkeit der Kommunikation wieder herzustellen.

Die Datenschutzbeauftragten des Bundes und der Länder haben daher schon im September 2013 gefordert, auf diese neue Qualität der Überwachung rechtlich und politisch zu reagieren. Darüber hinaus sind aber auch technische und organisatorische Schutzmaßnahmen erforderlich. Der Schutz der informationellen Selbstbestimmung der in Deutschland lebenden Menschen sowie der Vertraulichkeit und Integrität informationstechnischer Systeme muss wieder hergestellt und dauerhaft gesichert werden.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder fordert daher die Prüfung und Umsetzung folgender Maßnahmen:

1. *Sichere Verschlüsselung beim Transport und bei der Speicherung von Daten,*

2. *Bereitstellung einer einfach bedienbaren Verschlüsselungs-Infrastruktur,*

3. *Einsatz von Ende-zu-Ende-Verschlüsselung in Kombination mit Verfahren zur Verbindungsverschlüsselung,*

4. *Sichere und vertrauenswürdige Bereitstellung von Internetangeboten,*

5. *Weiterentwicklung innovativer Vorkehrungen zum Schutz von Verkehrsdaten,*

6. *Ausbau der Angebote und Förderung anonymer Kommunikation,*

7. *Angebot für eine Kommunikation über kontrollierte Routen,*

8. *Sichere Verschlüsselung der Mobilkommunikation und Einschränkung der Möglichkeiten der Geolokalisierung,*

9. *Beschränkung des Cloud Computing mit personenbezogenen Daten auf vertrauenswürdige Anbieter mit zertifizierter Informationssicherheit,*

10. Förderung der Vertrauenswürdigkeit informationstechnischer Systeme durch Zertifizierung,

11. Sensibilisierung von Nutzerinnen und Nutzern moderner Technik,

12. Ausreichende Finanzierung von Maßnahmen der Informationssicherheit.

Der Arbeitskreis „Technische und organisatorische Datenschutzfragen" der Datenschutzkonferenz hat einen Anforderungskatalog formuliert, der die hier genannten Maßnahmen konkretisiert (siehe Anlage zu dieser Entschließung).

Die Datenschutzbeauftragten des Bundes und der Länder fordern die Anbieter elektronischer Kommunikationsdienste auf, entsprechende Technologien und Dienste zur Verfügung zu stellen. Die Verwaltungen in Bund und Ländern, insbesondere die zuständigen Regulierungsbehörden, sind aufgefordert, auf die Durchsetzung der o.g. Maßnahmen zu dringen. Der Gesetzgeber ist aufgerufen, die zu ihrer Durchsetzung ggf. nötigen Änderungen und Präzisierungen an dem bestehenden Rechtsrahmen vorzunehmen.

1.2 Europa

1.2.1 Reform des Datenschutzrechtsrahmens

Bereits in meinem 25. Tätigkeitsbericht 2012 unter Nr. 1.1 bin ich auf die Reform des Europäischen Datenschutzrechtsrahmens eingegangen. Die Europäische Kommission hat schon im Jahr 2012 den Entwurf einer Datenschutz-Grundverordnung (KOM 2012/0011 endg.) vorgelegt. Er zielt auf eine allgemeine und in den Mitgliedstaaten unmittelbar geltende Gesetzeslage ab. Diese Verordnung soll die geltende allgemeine Datenschutz-Richtlinie 95/46/EG ersetzen. Nunmehr hat das Europäische Parlament am 12.03.2014 mit großer Mehrheit eine Verhandlungsposition festgelegt (Legislative Entschließung des Europäischen Parlaments am 12.03.2014, P7_TA(2014)0212); 622 Ja-Stimmen und 10 Nein-Stimmen bei 22 Enthaltungen). Der Textentwurf lehnt sich stark an den Kommissionsentwurf an.

Parallel dazu ist ein Entwurf einer Datenschutz-Richtlinie für den Bereich der Strafjustiz (KOM 2012/0010) vorgelegt worden. Er soll den Datenschutz im Bereich der Strafjustiz von der vorbeugenden Bekämpfung der Kriminalität über die Strafverfolgung bis hin zum Strafvollzug abdecken. Nach dem Willen der Kommission soll damit der Anwendungsbereich der Richtlinie gegenüber dem Rahmenbeschluss 2008/977/JI deutlich weiter ausgestaltet sein. Er soll insbesondere auch die mitgliedsstaatlichen Datenverarbeitungen im Bereich der Strafjustiz betreffen. Das Europäische Parlament hat auch hier mehrheitlich eine Verhandlungsposition festgelegt, die nicht grundlegend vom Kommissionsentwurf abweicht (Legislative Entschließung des Europäischen Parlaments am 12.03.2014, P7_TA(2014)0219). Wie das Abstimmungsergebnis zeigt, ist der Entwurf jedoch deutlich umstrittener gewesen als der Schwesterentwurf einer Datenschutz-Grundverordnung (371 Ja-Stimmen und 276 Nein-Stimmen bei 30 Enthaltungen). Die Änderungsvorschläge des Parlaments zielen auf eine weitergehende Angleichung der Richtlinie an die Datenschutz-Grundverordnung, insbesondere auf eine effektivere Datenschutzkontrolle ab.

Für einen erfolgreichen Abschluss des Gesetzgebungsvorhabens wäre es allerdings erforderlich, dass sich auch der Rat der Europäischen Union eine Verhandlungsposition erarbeitet. Im Rat stocken jedoch die Verhandlungen. Dem Vernehmen nach behandelt der Rat der Europäischen Union dabei den Entwurf einer Datenschutz-Grundverordnung vorrangig gegenüber dem Richtlinienentwurf. Sowohl die Europäische Kommission als auch das Europäische Parlament haben sich auf ein Junktim festgelegt: Danach soll die Datenschutz-Grundverordnung nicht ohne die Richtlinie verabschiedet werden. Offiziellen Verlautbarungen zufolge soll die Datenschutz-Grundverordnung spätestens im Jahr 2015 verabschiedet werden.

Die Konferenz hat den Reformprozess erneut mit mehreren Entschließungen begleitet, die ich mitgetragen habe.

Entschließung der 87. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 27./28.03.2014
Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder zur Struktur der künftigen Datenschutzaufsicht in Europa

Ein zentrales Verhandlungsthema bei den Beratungen im Rat der EU betrifft die Frage, welche Aufgaben die Datenschutzbehörden künftig haben und wie sie in Fällen, die mehrere Mitgliedstaaten oder die gesamte EU betreffen, besser zusammenarbeiten können. Die Europäische Kommission hatte hierzu das Prinzip einer einheitlichen Anlaufstelle ("One-Stop-Shop") vorgeschlagen, wonach die Datenschutzbehörde am Sitz der Hauptniederlassung EU-weit zuständig ist für die Aufsicht über alle Niederlassungen eines Unternehmens innerhalb der EU. Daneben schlug sie die Einführung eines Kohärenzverfahrens vor, das es den Datenschutzbehörden ermöglichen soll, in grenzüberschreitenden Fällen zu einheitlichen Entscheidungen im Rahmen des europäischen Datenschutzausschusses zu gelangen.

Vor dem Hintergrund der aktuell im Rat erörterten unterschiedlichen Modelle plädieren die Datenschutzbeauftragten des Bundes und der Länder für einen effektiven und bürgernahen Kooperations- und Entscheidungsmechanismus, der folgende Kernelemente beinhalten sollte:

1. *Die Datenschutzbeauftragten des Bundes und der Länder bekräftigen den Grundsatz, dass jede Aufsichtsbehörde im Hoheitsgebiet ihres Mitgliedstaats die ihr mit der Verordnung übertragenen Aufgaben und Befugnisse über alle Datenverarbeitungen ausübt, durch welche Personen dieses Mitgliedstaates betroffen sind, unabhängig davon, ob die verantwortliche Stelle über eine Niederlassung innerhalb dieses Mitgliedstaates verfügt oder nicht.*

2. *Die Datenschutzbeauftragten des Bundes und der Länder die Einführung eines One-Stop-Shop-Mechanismus für Fälle, in denen der Datenverarbeiter über mehrere Niederlassungen in unterschiedlichen EU-Mitgliedstaaten verfügt. In diesem Fall fungiert die Aufsichtsbehörde am Orte der Hauptniederlassung als federführende Behörde, die mit den Aufsichtsbehörden der Mitgliedstaaten, in denen der Verantwortliche über weitere Niederlassungen verfügt oder in denen Personen betroffen sind, eng kooperiert. Es bleibt damit den betroffenen Personen unbenommen, sich an die Aufsichtsbehörden ihres Heimatlandes zu wenden.*

3. *Die federführende Behörde und die mit zuständigen nationalen Aufsichtsbehörden kooperieren mit dem Ziel einer einheitlichen Entscheidungsfindung. Im Falle der Einigkeit erlässt die federführende Behörde die erforderlichen Maßnahmen gegenüber der Hauptniederlassung des Verantwortlichen. Der Verantwortliche ist verpflichtet, die Maßnahmen in allen Niederlassungen innerhalb der EU umzusetzen.*

4. *Sofern eine nationale Behörde dem Maßnahmenentwurf der federführenden Behörde widerspricht, ist der Europäische Datenschutzausschuss mit dem Fall zu befassen, der hierzu verbindliche Leitlinien erlassen oder sonstige verbindliche Maßnahmen treffen kann.*

5. *Die Datenschutzbeauftragten des Bundes und der Länder befürworten die in dem Verordnungsentwurf enthaltenen Elemente zur Stärkung der Verantwortlichkeit der Unternehmen zur Einhaltung des Datenschutzrechts. Hierzu zählen die EU-weite Einführung betrieblicher Datenschutzbeauftragter, Datenschutz-Folgeabschätzungen, Privacy-by-Design und Privacy-by-Default, Zertifizierungen, Datenschutzsiegel und Verhaltensregeln. Fragen zur Rechtskonformität einer Datenverarbeitung können im Rahmen der vorherigen Zurate Ziehung mit den Aufsichtsbehörden geklärt werden.*

6. *Für die Einführung formeller, fristgebundener Verfahren zur Erlangung EU-weit gültiger Compliance-Entscheidungen besteht aus Sicht der Datenschutzbeauftragten des Bundes und der Länder daneben kein Bedarf. Insbesondere darf die Klärung von Compliance-Fragen nicht zu einer Verlagerung der Verantwortlichkeit auf die Aufsichtsbehörden und zur Einschränkung aufsichtsbehördlicher Maßnahmen im Falle von Datenschutzverstößen führen.*

7. *Ein originärer Schwerpunkt der Aufsichtstätigkeit in Bezug auf Zertifizierungsprozesse sollte darin liegen, im Rahmen der Norminterpretation Prüfstandards mitzugestalten, auf deren Grundlage die Vergabe von Zertifikaten geprüft wird.*

Nach wie vor halte ich eine Reform des Europäischen Datenschutzrechtrahmens für geboten. Das Gesetzgebungsverfahren werde ich dementsprechend konstruktiv-kritisch weiter begleiten. Mein besonderes Augenmerk werde ich weiterhin darauf legen, dass eine künftige europäische Regelung den Mitgliedstaaten Gestaltungsspielräume für einen weitergehenden Datenschutz bzw. für die Fortentwicklung des Datenschutzes eröffnet.

1.2.2 Ende der Vorratsdatenspeicherung?

Mit Urteil vom 08.04.2014 hat der Europäische Gerichtshof (EuGH) die aus datenschutzrechtlicher Sicht höchst problematische Richtlinie 2006/24/EG über die Vorratsspeicherung von Telekommunikationsdaten für ungültig erklärt. Zwar hat der Gerichtshof die Vorratsspeicherung als „nützliches Mittel“ angesehen, das zur Aufklärung schwerer Straftaten geeignet sein kann. Zugleich hat er jedoch darauf hingewiesen, dass schon die Pflicht zur anlasslosen Speicherung einen besonders schwerwiegenden Eingriff großen Ausmaßes in das Recht auf Privatleben und den Datenschutz der Betroffenen darstellt. Diese Feststellung steht im Einklang mit

der gefestigten Rechtsprechung des Europäischen Gerichtshofs für Menschenrechte (siehe beispielsweise Urteil vom 04.12.2008 – 30562/04, S. u. Marper/Vereinigtes Königreich).

Diese in Art. 7 und Art. 8 der Europäischen Grundrechte-Charta verbrieften Rechte dürfen nur eingeschränkt werden, soweit dies absolut notwendig ist. Die für ungültig erklärte Richtlinie entsprach diesen Vorgaben nicht, weil sie ohne jede Differenzierung, Einschränkung oder Ausnahme zur pauschalen Totalerfassung der Telekommunikations-Verkehrsdaten verpflichtete. Ausdrücklich hat der Gerichtshof festgestellt, dass das an sich legitime Ziel der Bekämpfung schwerer Straftaten für sich genommen die Erforderlichkeit der Pflicht zur Vorratsspeicherung nicht rechtfertigt. Dem genügte die Richtlinie offenkundig nicht. Insbesondere schrieb sie die Speicherung von Telekommunikations-Verkehrsdaten fast der gesamten europäischen Bevölkerung vor. Auch solche Personen mussten erfasst werden, deren Verhalten nicht einmal in einem mittelbaren oder entfernten Zusammenhang zu schweren Straftaten steht oder die einem Berufsgeheimnis unterliegen. Auch musste kein Zusammenhang zwischen den auf Vorrat gespeicherten Daten und einer Bedrohung der öffentlichen Sicherheit bestehen.

Bislang haben weder deutsche noch andere europäische Strafverfolgungsbehörden den konkreten Nachweis erbracht, dass ohne eine Vorratsdatenspeicherung typischerweise erfolgreiche Ermittlungsansätze fehlen. Insbesondere der Hinweis auf plakative Einzelfälle weist nicht nach, dass sich die Sicherheitslage ohne Vorratsdatenspeicherung wesentlich verschlechtert hat.

Auch in der mündlichen Verhandlung vor dem Europäischen Gerichtshof konnten die Verteidiger der Richtlinie nicht die zwingende Erforderlichkeit zur Bekämpfung schwerer Straftaten nachweisen. Vor diesem Hintergrund ist die Entscheidung des Europäischen Gerichtshofs nicht nur dogmatisch überzeugend, sondern auch folgerichtig.

Überdies stammt die der Vorratsdatenspeicherung zugrunde liegende Richtlinie bereits aus dem Jahr 2006. In dieser Zeit hinterließ der Einzelne weitaus weniger digitale Spuren, als dies heute der Fall ist. Heute erfassen Smartphones und zunehmend auch Gebrauchsgegenstände des täglichen Lebens wie z.B. Fahrzeuge mit eingebauten Speichertechniken enorm viele Daten.

Ungeachtet dessen hat das Vereinigte Königreich in Reaktion auf das Urteil ein eigenes Gesetz zur Vorratsdatenspeicherung verabschiedet (Data Retention and Investigatory Powers Act 2014, vom 17.07.2014). Demgegenüber hatte die bisherige EU-Innenkommissarin Cecilia Malmström in einem Interview angekündigt, nach dem EuGH-Urteil keinen Gesetzesentwurf mehr zur Vorratsdatenspeicherung vorzulegen (Die Welt: EU will keine neue Regeln für Vorratsdaten, Welt-Online vom 04.06.2014).

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat vor diesem Hintergrund die Absichtserklärung der Bundesregierung begrüßt, zunächst kein Gesetz zur Speicherung von Telekommunikations-Verkehrsdaten in die Wege zu leiten.

Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 25.04.2014
Ende der Vorratsdatenspeicherung in Europa!

Der Europäische Gerichtshof hat in seinem Urteil vom 8. April 2014 die Europäische Richtlinie zur Vorratsspeicherung von Telekommunikations-Verkehrsdaten (Richtlinie 2006/24/EG) für ungültig erklärt. Dieses Urteil hat weitreichende Folgen für den Datenschutz in Europa.

Die Datenschutzbeauftragten des Bundes und der Länder haben die anlasslose und massenhafte Speicherung von Verkehrsdaten der Telekommunikation stets abgelehnt. Sie begrüßen die Entscheidung des Europäischen Gerichtshofs als wichtigen Schritt zur Bekräftigung der informationellen Selbstbestimmung und des Telekommunikationsgeheimnisses.

Der Europäische Gerichtshof hat in seinem Urteil der undifferenzierten und automatischen Totalerfassung solcher Daten eine klare Absage erteilt. Er hat darauf hingewiesen, dass schon die Pflicht zur anlasslosen Speicherung einen besonders schwerwiegenden Eingriff großen Ausmaßes in das Recht auf Privatleben und den Datenschutz der Betroffenen darstellt. Diese in der Europäischen Grundrechte-Charta verbrieften Rechte dürften nur eingeschränkt werden, soweit dies absolut notwendig ist.

Die für ungültig erklärte Richtlinie entsprach diesen Vorgaben nicht, weil sie ohne jede Differenzierung, Einschränkung oder Ausnahme zur pauschalen Totalerfassung der Verkehrsdaten verpflichtete. Nach dem Urteil des Gerichtshofs kann eine undifferenzierte Pflicht zur anlasslosen und flächendeckenden Vorratsdatenspeicherung unionsrechtlich nicht mehr neu begründet werden. Die Absichtserklärung der Bundesregierung, zurzeit kein Gesetz zur Speicherung von Verkehrsdaten einzuführen, wird von der Konferenz der Datenschutzbeauftragten des Bundes und der Länder begrüßt. Etwaige Diskussionen auf europäischer Ebene sollten abgewartet werden.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder weist ausdrücklich darauf hin, dass der Maßstab des EuGH auch für das anlasslose exzessive Überwachen durch sämtliche Nachrichtendienste gelten muss.

Zudem hält der Gerichtshof die Pflicht zur großflächigen Speicherung von personenbezogenen Daten nur dann für zulässig, wenn die Daten in der Europäischen Union gespeichert werden und damit unter die Kontrolle unabhängiger Datenschutzbehörden fallen. Dies zwingt auch zu einer Neubewertung z.B. der Fluggastdaten-Übermittlung in die USA und des Safe-Harbor-Abkommens.

In einem Urteil vom 03.07.2014 hat der Bundesgerichtshof mittlerweile klargestellt, dass die Erwägungen des EuGH aus seiner Sicht allein die Datenspeicherung für die Zwecke der Strafverfolgungsbehörden betreffen. Sie seien auf die Speicherung von IP-Adressen nicht anwendbar, die Telekommunikationsanbieter zu den Zwecken der Störungserkennung und Störungsbeseitigung vornehmen würden (Bundesgerichtshof, Urteil vom 03.07.2014, Az.: III ZR 391/13, online abrufbar in der Entscheidungsdatenbank auf www.bundesgerichtshof.de).

1.2.3 Datenschutz im Internet

Zur datenschutzrechtlichen Beurteilung von Sozialen Netzwerken habe ich mich in meinem 25. Tätigkeitsbericht 2012 unter Nr. 1.3 ausführlich geäußert (zum aktuellen Stand siehe Nr. 12.4). Gegen die beiden größten Anbieter, Google und

Facebook sind allein in dem Berichtszeitraum zahlreiche Klagen anhängig gemacht worden, die sich auch auf Datenschutzverstöße beziehen.

1.2.3.1 Europäischer Gerichtshof: Ein Recht auf Vergessenwerden?

Europas Bürger haben einen Anspruch gegen Google, Verweise aus der Ergebnisliste von Suchanfragen zu entfernen, wenn dort enthaltene Informationen das Recht auf Privatleben und Datenschutz einer Person verletzen. Das hat der EuGH in einer Entscheidung vom 13.05.2014 (Az.: C -131/12) festgestellt. Der zu entscheidende Fall betraf einen spanischen Bürger. Im Jahr 1998 hatte eine große spanische Tageszeitung über die Versteigerung seines Grundstücks aufgrund einer Pfändung berichtet. Die Pfändung war seit Jahren erledigt, tauchte aber nach wie vor in dem Online-Archiv der Tageszeitung auf. Die Suchmaschine von Google verwies bei entsprechenden Anfragen auf Beiträge dieses Online-Archivs.

Der EuGH hat nun darauf hingewiesen, eine von einem Suchmaschinenbetreiber ausgeführte Verarbeitung personenbezogener Daten könne die Grundrechte auf Achtung des Privatlebens und Schutz personenbezogener Daten erheblich beeinträchtigen, wenn die Suche mit dieser Suchmaschine anhand des Namens einer natürlichen Person durchgeführt werde. Denn eine solche Verarbeitung ermögliche es jedem Internetnutzer, mit der Ergebnisliste einen strukturierten Überblick über die zu der betreffenden Person im Internet zu findenden Informationen zu erhalten, die potenziell zahlreiche Aspekte von deren Privatleben beträfen. Im Allgemeinen würden die aus Art. 7 und 8 der Grundrechtecharta geschützten Rechte der betroffenen Person das Interesse der Internetnutzer am Erhalt von Informationen überwiegen.

Das Urteil ist vielfach kritisiert worden. Kritiker beklagen eine neue Form der Zensur und bemängeln, das Gericht habe die Bedeutung der Informationsfreiheit nicht hinreichend gewürdigt. Darüber hinaus werde dem Recht auf Privatleben einseitig Vorrang gegenüber Wirtschaftsinteressen eingeräumt. Nach meinem Eindruck sind diese Angriffe überzogen. Sie berücksichtigen nicht hinreichend, dass die Entscheidung regelmäßig nur Fälle betrifft, in denen Suchanfragen mit dem Namen ausgeführt werden. Der EuGH stellt nur einen Anspruch von betroffenen Personen fest, dass Google Situationen korrigiert, in denen eine Suchanfrage mit dem Namen der betroffenen Person inadäquate, nicht (mehr) relevante, oder übermäßige Suchergebnisse erzeugt. Nicht Gegenstand der Entscheidung war die Veröffentlichung der Informationsseite, auf die eine Suchmaschine verweist.

Möglicherweise ist die Entscheidung also vielfach missinterpretiert worden. Auf der Grundlage US-amerikanischen Urheberrechts löscht Google jeden Monat viele Tausende von Suchergebnissen. Ohnehin ist die Reihung der Suchergebnisse bei Google wie bei den meisten anderen Betreibern von Suchmaschinen für die Internetnutzenden völlig intransparent. Eine nach objektiven Kriterien und für jede Person nachvollziehbare Vermittlung von Suchergebnissen findet nicht statt.

Die 88. Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat Hinweise zur Umsetzung des Urteils gegeben.

Entschließung der 88. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 08./09.10.2014
Zum Recht auf Sperrung von Suchergebnissen bei Anbietern von Suchmaschinen

Der Europäische Gerichtshof (EuGH) hat mit seinem Urteil vom 13. Mai 2014 – C-131/12 „Google Spain" einen fundamentalen Beitrag zum Schutz der Persönlichkeitsrechte im Internet geleistet. Die Namenssuche in Suchmaschinen kann erhebliche Auswirkungen auf die Persönlichkeitsrechte haben. Mit Suchmaschinen lassen sich weltweit in Sekundenschnelle detaillierte Profile von Personen erstellen. Oft sind Einträge über eine unbegrenzte Zeit hinweg abrufbar. Sie können dann zu sozialen und wirtschaftlichen Nachteilen für die Betroffenen führen, die ggf. ein Leben lang mit früheren oder vermeintlichen Verfehlungen konfrontiert bleiben. Das Urteil stellt nun klar, dass die Betreiber von Suchmaschinen ein Recht Betroffener auf Sperrung von Suchergebnissen bei Anbietern von Suchmaschinen umzusetzen haben. Künftig bleiben die Betroffenen daher nicht nur darauf angewiesen, ihre Ansprüche unmittelbar gegenüber den Informationsanbietern zu verfolgen, die häufig nur schwer oder auch gar nicht zu realisieren sind.

Betroffene können sich nun auch direkt an die Suchmaschinenbetreiber wenden und verlangen, dass bei der Suche einzelne Links zu ihrem Namen künftig nicht mehr angezeigt werden.

Das Urteil ordnet dabei allerdings nicht an, bestimmte Inhalte, wie Presseartikel oder Artikel aus der Wikipedia, zu löschen oder ihre Auffindbarkeit im Internet unmöglich zu machen. Vielmehr soll – nach einer erfolgreichen Beschwerde des Betroffenen – der entsprechende Link lediglich bei Eingabe eines bestimmten Personennamens nicht mehr angezeigt werden. Der betroffene Inhalt bleibt mit allen anderen Suchbegriffen weiterhin frei zugänglich (für Inhalte, die regelmäßig durch Eingabe des Namens einer Person in eine Suchmaschine gefunden werden, weil es sich um eine Person des öffentlichen Lebens handelt, hat der EuGH ausdrücklich eine Ausnahme vorgesehen).

Zu Recht wird in der Debatte auf die erhebliche Macht der Anbieter von Suchmaschinen hingewiesen, über die Veröffentlichung von Suchergebnissen zu entscheiden. Diese Macht besteht jedoch nicht erst seit der Entscheidung des EuGH. Tatsächlich haben Inhalteanbieter keinen Rechtsanspruch am Nachweis ihrer Inhalte durch Suchmaschinen. Anbieter von Suchmaschinen sind keine neutralen Sachwalter der Informationsgesellschaft, sondern kommerziell handelnde Wirtschaftsunternehmen. Welche Suchergebnisse den Nutzern angezeigt wurden, bestimmt sich damit jedenfalls auch nach den kommerziellen Interessen von Suchmaschinen und ihren Vertragspartnern. Darüber hinaus unterlagen Suchmaschinen auch bereits vor der Entscheidung des EuGH bei der Gestaltung der Suchergebnisse äußeren Beschränkungen (z.B. durch das Urheberrecht). Mit dem Urteil wird klargestellt, dass Suchmaschinen neben diesen Erwägungen jetzt auch die Grundrechte der Betroffenen zu berücksichtigen haben.

Das Urteil konkretisiert die Kriterien, unter welchen sich ausländische Unternehmen an europäisches bzw. nationales Datenschutzrecht halten müssen. Dieses für den Grundrechtsschutz maßgebliche Urteil muss nunmehr von den Suchmaschinenbetreibern umfassend umgesetzt werden.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder weist in diesem Zusammenhang auf folgende Punkte hin:

- *Die effektive Wahrung der Persönlichkeitsrechte des Betroffenen setzt voraus, dass Anbieter von Suchmaschinen die Suchergebnisse bei einem begründeten Widerspruch weltweit unterbinden. Angesichts der territorialen*

Unbeschränktheit des Internet muss der Schutz des Einzelnen vor einer unberechtigten Verbreitung personenbezogener Daten universell gelten.

— *Der verantwortliche Betreiber der Suchmaschine hat regelmäßig die Rechte der Betroffenen gegen die Interessen der Öffentlichkeit an einem freien und umfassenden Informationszugang im Einzelfall abzuwägen. Dabei ist insbesondere auf die Schwere der Persönlichkeitsrechtsbeeinträchtigung, die Stellung des Betroffenen im öffentlichen Leben sowie auf den zeitlichen Ablauf zwischen der Veröffentlichung und dem Antrag des Betroffenen beim Suchmaschinenbetreiber abzustellen.*

— *Die Entscheidung über die Verbreitung von Suchergebnissen, die Umsetzung von Widersprüchen und die Abwägungsentscheidung mit dem öffentlichen Interesse treffen zunächst die Suchmaschinenbetreiber. Die Kontrolle dieser Entscheidungen obliegt den jeweiligen Aufsichtsbehörden für den Datenschutz oder den staatlichen Gerichten. Alternative Streitbeilegungs- oder Streitschlichtungsverfahren dürfen das verfassungsmäßige Recht der Betroffenen auf eine unabhängige Kontrolle durch die dafür vorgesehenen staatlichen Institutionen nicht beschneiden.*

— *Eine Befugnis der Anbieter von Suchmaschinen, Inhaltsanbieter routinemäßig über die Sperrung von Suchergebnissen zu informieren, besteht nicht. Dies gilt auch dann, wenn die Benachrichtigung nicht ausdrücklich den Namen des Betroffenen enthält.*

Dem Vernehmen nach sollen weitere Verfahren gegen Google beim EuGH anhängig sein. Möglicherweise entwickelt der Gerichtshof die vorgestellte Rechtsprechung weiter.

1.2.3.2 Facebook

Der irische High Court hatte bereits eine Klage gegen die Richtlinie 2006/24/EG über die Vorratsdatenspeicherung dem Europäischen Gerichtshof zur Beurteilung vorgelegt (siehe Nr. 1.2.2). Im Juni 2014 soll dasselbe Gericht eine Klage der Studentengruppe „Europe versus Facebook“ an den Europäischen Gerichtshof verwiesen haben. Die Gruppe vertritt die Auffassung, dass Facebook in vielfältiger Hinsicht europäisches Datenschutzrecht verletzt.

Presseberichten zufolge hat das irische Gericht offenbar die Überzeugung, dass es Belege gibt, dass Facebook der NSA den massenhaften und undifferenzierten Zugriff auf personenbezogene Daten ermöglicht. Eine Übermittlung personenbezogener Daten in die USA sei aber nur zulässig, wenn sie dort nach den Maßstäben des europäischen Datenschutzrechts angemessen geschützt werden.

Die beispielhaft vorgestellten Verfahren verdeutlichen, wie dringlich es ist, klare rechtliche Rahmenbedingungen für Soziale Netzwerke zu schaffen. Die 85. Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat dementsprechende Regeln eingefordert (siehe Nr. 12.4.1).

1.3 Deutschland

1.3.1 Beschäftigtendatenschutz

Bereits in meinem 24. Tätigkeitsbericht 2010 habe ich mich mit dem aus dem Jahr 2010 stammenden Gesetzesentwurf der Bundesregierung zum Beschäftigtendatenschutz auseinandergesetzt (24. Tätigkeitsbericht 2010 Nr. 1.2.7). Vor dem Hintergrund kontroverser Diskussionen wurde der Entwurf im Ergebnis nicht weiterverfolgt.

Zur Regelung des Beschäftigtendatenschutzes trifft der Koalitionsvertrag 2013 zwischen CDU, CSU und SPD zur 18. Legislaturperiode auf Seite 70 nunmehr folgende Aussage:

„Beschäftigtendatenschutz gesetzlich regeln
Die Verhandlungen zur Europäischen Datenschutzgrundverordnung verfolgen wir mit dem Ziel, unser nationales Datenschutzniveau – auch bei der grenzüberschreitenden Datenverarbeitung – zu erhalten und über das Europäische Niveau hinausgehende Standards zu ermöglichen. Sollte mit einem Abschluss der Verhandlungen über die Europäische Datenschutzgrundverordnung nicht in angemessener Zeit gerechnet werden können, wollen wir hiernach eine nationale Regelung zum Beschäftigtendatenschutz schaffen."

Danach dürfte es auch in der 18. Legislaturperiode nicht zu einer Vollregelung des Beschäftigtendatenschutzes kommen. Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat deshalb eine Entschließung gefasst, die auf die Notwendigkeit einer zeitnahen Regelung hinweist.

Entschließung der 87. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 27./28.03.2014
Beschäftigtendatenschutzgesetz jetzt!

Trotz zahlreicher Aufforderungen durch die Konferenz der Datenschutzbeauftragten des Bundes und der Länder sowie des Deutschen Bundestages ist die Verabschiedung einer angemessenen Regelung des Beschäftigtendatenschutzes in der vergangenen Legislaturperiode erneut gescheitert. Der Koalitionsvertrag für die 18. Legislaturperiode sieht vor, das nationale Datenschutzniveau im Beschäftigtendatenschutz bei den Verhandlungen zur Europäischen Datenschutzgrundverordnung zu erhalten und darüber hinausgehende Standards zu ermöglichen. Falls mit einem Abschluss der Verhandlungen über die Europäische Datenschutzgrundverordnung nicht in angemessener Zeit gerechnet werden kann, soll eine nationale Regelung geschaffen werden.

Dies reicht nicht aus. Wann die Datenschutzgrundverordnung verabschiedet wird, ist derzeit völlig unklar. Ohnehin ist mit einem Inkrafttreten dieser europäischen Regelungen schon aufgrund der notwendigen Umsetzungsfrist erst in einigen Jahren zu rechnen. Aufgrund der voranschreitenden technischen Entwicklung, die eine immer weiter gehende Mitarbeiterüberwachung ermöglicht, besteht unmittelbarer Handlungsbedarf. Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder fordert die Bundesregierung deshalb auf, ein nationales Beschäftigtendatenschutzgesetzes umgehend auf den Weg zu bringen. Die Formulierung "in angemessener Zeit" lässt befürchten, dass das der Beschäftigtendatenschutz in dieser Legislaturperiode schon wieder auf die lange Bank geschoben wird.

Ein Beschäftigtendatenschutzgesetz muss ein hohes Datenschutzniveau gewährleisten und einen angemessenen Ausgleich zwischen den berechtigten Informationsinteressen des Arbeitgebers und dem Recht auf informationelle Selbstbestimmung des Arbeitnehmers schaffen.

Dies wird erkennbar in den vielfältigen Fragestellungen, für die es bislang keine klaren rechtlichen Vorgaben gibt. Zu nennen sind hier beispielsweise die immer umfassendere Videoüberwachung, Dokumentenmanagementsysteme, die die Leistung der Beschäftigten transparent werden lassen, die zunehmende Verquickung von Arbeit und Privatem verbunden mit der dienstlichen Nutzung von privaten Arbeitsmitteln wie Handy und Laptop; die Nutzung von dienstlich zur Verfügung gestellten Kfz mit oder ohne die Erlaubnis privater Nutzung oder die private Nutzung der vom Arbeitgeber zur Verfügung gestellten E-Mail- und Internetzugänge, der zunehmende Einsatz biometrischer Verfahren sowie die Erhebung und Verarbeitung von Bewerberdaten beispielweise aus sozialen Netzwerken.

Hierfür müssen künftig gesetzliche Standards geschaffen werden, um sowohl die Rechtssicherheit für die Arbeitgeber zu erhöhen als auch einen wirksamen Grundrechtsschutz für die Beschäftigten zu schaffen.

1.3.2 Polizeiarbeit in sozialen Netzwerken?

Die Konferenz hat sich auch mit dem Interesse der Strafverfolgungsbehörden auseinander gesetzt, soziale Netzwerke zur Öffentlichkeitsfahndung zu nutzen (zur Problematik siehe auch 25. Tätigkeitsbericht 2012 Nr. 3.1.4). Auf entsprechende Bitte der Justizministerkonferenz hin hat die Datenschutzkonferenz mit der nachfolgenden Entschließung einen einheitlichen Standpunkt entwickelt.

Entschließung der 87. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 27./28.03.2014
Öffentlichkeitsfahndung mit Hilfe sozialer Netzwerke – Strenge Regeln erforderlich!

Mit zunehmender Beliebtheit sozialer Netzwerke bei Bürgerinnen und Bürgern steigt das Interesse von Strafverfolgungsbehörden, diese sozialen Netzwerke auch zur Öffentlichkeitsfahndung zu nutzen. So gibt es in Deutschland bereits Polizeidienststellen, die mittels Facebook nach Straftätern suchen. Auch die 84. Konferenz der Justizministerinnen und Justizminister hat sich im November 2013 mit dem Thema befasst.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hält es erneut für notwendig darauf hinzuweisen, dass eine Nutzung sozialer Netzwerke privater Betreiber (wie z.B. Facebook) zur Öffentlichkeitsfahndung aus datenschutzrechtlicher Sicht sehr problematisch ist. Durch die weltweit recherchierbare Veröffentlichung von Fahndungsdaten wird in weitaus schwerwiegenderer Weise in die Grundrechte Betroffener (Tatverdächtiger oder auch Zeugen) eingegriffen, als dies bei der Nutzung klassischer Medien der Fall ist. Auch sind im Internet veröffentlichte Daten einer Fahndungsausschreibung nur sehr schwer bzw. gar nicht mehr zu löschen. Geben Nutzerinnen und Nutzer der Sozialen Netzwerke in Diskussionsforen und Nutzerkommentaren öffentlich Spekulationen, Behauptungen und Diskriminierungen ab, beeinträchtigt dies die Persönlichkeitsrechte der Betroffenen erheblich. Solche Funktionen sind in von den Ermittlungsbehörden be-

triebenen Angeboten weder geeignet noch erforderlich, um die behördlichen Aufgaben zu erfüllen. Die Konferenz weist darauf hin, dass Öffentlichkeitsfahndung nur auf Diensten von Anbietern erfolgen darf, die die datenschutzrechtlichen Vorgaben des Telemediengesetzes zur Nutzungsdatenverarbeitung, insbesondere der Regeln zur Reichweitenmessung gemäß §§ 13 Abs. 4 Nr. 6, 15 Abs. 3 TMG, und das Recht auf anonyme und pseudonyme Nutzung gemäß § 13 Abs. 6 TMG beachten.

Sofern es Strafverfolgungsbehörden gleichwohl gestattet werden soll, zu Zwecken der Öffentlichkeitsfahndung auf soziale Netzwerke mit deaktivierter Kommentierungsfunktion zurückzugreifen, so darf dies – ungeachtet der generellen Kritik an der Nutzung sozialer Netzwerke durch öffentliche Stellen – nur geschehen, wenn folgende Maßgaben beachtet werden:

- *Die Vorschriften der Strafprozessordnung (§ 131 Abs. 3, § 131a Abs. 3, § 131b StPO) zur Öffentlichkeitsfahndung kommen aufgrund der technikoffenen Formulierung als Rechtsgrundlage für die Öffentlichkeitsfahndung im Internet grundsätzlich in Betracht. Sie sind aber im Hinblick auf den Verhältnismäßigkeitsgrundsatz nur eingeschränkt anzuwenden. Eine entsprechende Klarstellung durch den Gesetzgeber wäre wünschenswert. Zumindest aber sind die besonderen Voraussetzungen der Fahndung im Internet, insbesondere in sozialen Netzwerken in Umsetzungsvorschriften zu konkretisieren. Änderungsbedarf besteht beispielsweise für die Anlage B der RiStBV.*

- *In materiell-rechtlicher Hinsicht haben die Strafverfolgungsbehörden den Verhältnismäßigkeitsgrundsatz strikt zu beachten. Die zu schaffenden Regelungen müssen den besonderen Gefahren der Öffentlichkeitsfahndung in sozialen Netzwerken gerecht werden. Insbesondere muss sichergestellt werden, dass eine solche Fahndung nur bei im Einzelfall schwerwiegenden Straftaten überhaupt in Betracht gezogen werden kann.*

- *In verfahrensrechtlicher Hinsicht müssen die Umsetzungsregelungen die Staatsanwaltschaft verpflichten, bereits im Antrag auf richterliche Anordnung der Maßnahme die Art, den Umfang und die Dauer der Öffentlichkeitsfahndung konkret anzugeben. Dies umfasst insbesondere die ausdrückliche Angabe, ob und warum die Anordnung auch die Öffentlichkeitsfahndung in sozialen Netzwerken umfassen soll.*

- *Es ist sicherzustellen, dass*

  - *die zur Öffentlichkeitsfahndung verwendeten personenbezogenen Daten von den Strafverfolgungsbehörden ausschließlich auf im eigenen Verantwortungsbereich stehenden Servern gespeichert und verarbeitet werden, nicht hingegen auf Servern der privaten Anbieter*

  - *die Weitergabe und der automatisierte Abruf der personenbezogenen Daten aus dem Internet durch Web-Crawler und ähnliche Dienste so weit als technisch möglich verhindert werden*

  - *die Kommunikation zwischen den Strafverfolgungsbehörden und den Nutzern nur außerhalb der sozialen Netzwerke erfolgt*

In Ansehung meiner grundsätzlichen Bedenken hat sich ein bayerisches Polizeipräsidium erst nach langem Zögern dazu entschlossen, eine Fanseite auf Facebook einzurichten. Dabei hat es meine Empfehlung teilweise berücksichtigt. Beispielsweise verzichtet die Polizei darauf, Öffentlichkeitsfahndungen auf der Fanpage zu veröffentlichen. An meinen grundsätzlichen Bedenken hinsichtlich der Einrichtung von Fanpages zum Zwecke der Öffentlichkeitsarbeit ändert dies freilich nichts (siehe Nr. 12.4.1).

1.3.3 Biometrische Gesichtserkennung durch Google, Facebook und Co.

Die Gesichtserkennung bei Online- und Mobilfunkdiensten ermöglicht in besonderem Maß die automatisierte Verfolgung und Aufspürung von Personen sowie die Profilerstellung. Es liegt auf der Hand, dass sie erhebliche Auswirkungen auf die Privatsphäre und auf das Recht des Einzelnen auf Datenschutz haben kann. Typischerweise werden dabei Bilder von Einzelpersonen erfasst (mit und ohne ihre Kenntnis) und dann für die Weiterverarbeitung an einen Remote-Server übermittelt. Online-Dienste, die sich häufig im Besitz von privaten Organisationen befinden und von diesen betrieben werden, haben immense Bildersammlungen angelegt, die von den betroffenen Personen selbst hochgeladen wurden. Kleine mobile Geräte mit hochauflösenden Kameras ermöglichen es den Nutzern, Bilder aufzunehmen und in Echtzeit über ständig bestehende Datenverbindungen eine Verbindung zu Online-Diensten herzustellen. Dadurch können die Nutzer diese Bilder mit anderen teilen oder eine Identifizierung, Authentifizierung/Verifizierung oder Kategorisierung durchführen, um zusätzliche Informationen über die bekannte oder unbekannte, vor ihnen stehende Person zu erhalten. Die Konferenz hat nun in einer Entschließung klargestellt, dass die Erstellung derartiger Profile wegen der hohen Sensibilität der Informationen nur zulässig sein kann, wenn sie auf einer gesetzlichen Grundlage oder auf einer informierten und freiwillig erteilten Zustimmung der Betroffenen beruht.

Entschließung der 87. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 27./28.03.2014
Biometrische Gesichtserkennung durch Internetdienste – Nur mit Wahrung des Selbstbestimmungsrechts Betroffener!

Die Nutzung biometrischer Daten wird zunehmend zu einem Phänomen des Alltags. Dies gilt in besonderer Weise für die biometrische Gesichtserkennung, die in sozialen Medien auf dem Vormarsch ist. Für den Zweck der Auswertung von Personenfotos werden die Gesichter der Nutzer biometrisch erfasst, so dass ein späterer Abgleich mit anderen Fotos die Identifizierung einzelner Personen ermöglicht. Dazu werden sogenannte Templates erstellt. Dies sind mathematische Modelle der wesentlichen Merkmale des Gesichts wie etwa dem Abstand von Augen, Mundwinkel und Nasenspitze. Es darf nicht verkannt werden, dass die Vermessung der Gesichtsphysiognomie in hohem Maße die schutzwürdigen Interessen Betroffener berührt, denn stets ist die dauerhafte Speicherung eines Referenz-Templates des eigenen Gesichts erforderlich.

Dass die Templates dann in den Datenbanken global agierender Internetunternehmen gespeichert werden, stellt nicht erst seit den Enthüllungen über das Überwachungs-Programm Prism, das den US-Geheimdiensten den Zugriff auf die Datenbanken der US-Anbieter erlaubt, ein erhebliches Risiko für das Persönlichkeitsrecht des Einzelnen dar.

Die biometrische Gesichtserkennung ist eine Technik, die sich zur Ausübung von sozialer Kontrolle eignet und der damit ein hohes Missbrauchspotential immanent ist. Mit ihrer Hilfe ist es möglich, aus der Flut digitaler Fotografien im Internet gezielt Aufnahmen von Zielpersonen herauszufiltern. Darüber hinaus könnten durch den Abgleich von Videoaufnahmen mit vorhandenen Templates in Echtzeit Teilnehmerinnen und Teilnehmer etwa von Massenveranstaltungen sowie von Demonstrationen oder einfach nur Passanten individualisiert und identifiziert werden. Der Schutz der Anonymität des Einzelnen in der Öffentlichkeit lässt sich damit zerstören, ohne dass die Betroffenen ihre biometrische Überwachung kontrollieren oder sich dieser entziehen können.

An die Erzeugung biometrischer Templates der Gesichter von Personen durch Internet-Dienste sind daher hohe rechtliche Anforderungen zu stellen, die das informationelle Selbstbestimmungsrecht von Betroffenen in höchst möglicher Weise berücksichtigen:

- *Die Erhebung, Verarbeitung und/oder Nutzung biometrischer Daten zur Gesichtserkennung zum Zweck der Erstellung eines dauerhaften biometrischen Templates kann nur bei Vorliegen einer wirksamen Einwilligung des Betroffenen i.S.d. § 4a BDSG rechtmäßig erfolgen.*

- *Die Einwilligung in die Erstellung biometrischer Templates zur Gesichtserkennung muss aktiv und ausdrücklich durch den Betroffenen erteilt werden. Die Betroffenen müssen vor der Erteilung der Einwilligung über die Funktionsweise der Erstellung und Nutzung der sie möglicherweise betreffenden Templates und die damit verfolgten Zwecke und Risiken in klarer und verständlicher Weise umfassend informiert werden. Eine Zweckänderung ist unzulässig. Sie bedarf einer Einwilligung, die dem Standard an die Einwilligungen bei der Verarbeitung besonderer personenbezogener Daten, § 4a Abs. 3 BDSG, entspricht.*

- *Die Einwilligung kann nicht durch den Verweis auf entsprechende Klauseln in allgemeinen Nutzungsbedingungen oder Datenschutzerklärungen ersetzt werden.*

- *Für eine logische Sekunde kann es nach § 28 Abs. 1 Satz 1 Nr. 2 bzw. Nr. 3 BDSG auch ohne Einwilligung zulässig sein, ein Template zu erstellen, mit dem ein Abgleich mit bereits vorhandenen, zulässigerweise gespeicherten Templates im Rahmen des von der Einwilligung abgedeckten Zwecks möglich ist. Betroffene sind über den Umstand, dass Bilder zum Abgleich mit bestehenden Templates verwendet werden, zu informieren.*

- *Derartige biometrische Templates zum automatischen Abgleich, bei denen eine Einwilligung fehlt, sind unverzüglich nach dem Abgleich zu löschen.*

- *Die Speicherung von biometrischen Templates von Dritten, die – anders als die Nutzer von sozialen Medien – regelmäßig nicht einwilligen können, ist ausgeschlossen.*

1.4 Bayern

1.4.1 Änderungen im Polizeiaufgabengesetz und Verfassungsschutzgesetz

Die Entscheidungen des Bundesverfassungsgerichts vom 24.01.2012 (Az.: 1 BvR 1299/05) hat zu Änderungen im Polizeiaufgabengesetz und im Verfassungsschutzgesetz geführt. Meine Forderungen und Empfehlungen wurden teilweise berücksichtigt (siehe Nrn. 3.1.1 und 4.1).

1.4.2 Videoüberwachung in Bayern

Die Videoüberwachung durch bayerische öffentliche Stellen führte bereits in der Vergangenheit zu zahlreichen Beschwerden. Sie bildet daher seit jeher einen Schwerpunkt meiner Prüftätigkeit. Im Berichtszeitraum bin ich durch die Beantwortung einer Parlamentarischen Anfrage („Videoüberwachung in Bayern", Landtags-Drucksache 16/15571) in die Lage versetzt worden, die Videoüberwachung systematischer zu kontrollieren. Der Antwort der Staatsregierung zufolge hat die Videoüberwachung durch bayerische öffentliche Stellen in den letzten Jahren deutlich zugenommen. Dies lässt sich an einer detailgenauen Auflistung der Kamerastandorte ablesen, die in einer Anlage der Antwort beigefügt ist.

Ich habe diese Liste von Kamerastandorten auf Auffälligkeiten untersucht und bin ebensolchen Auffälligkeiten nachgegangen. Insgesamt zeigten sich dabei erhebliche Unsicherheiten bei der Anwendung der für die Videoüberwachung maßgeblichen Vorschrift des Art. 21a BayDSG. In vielen der überprüften Fälle musste ich die öffentlichen Stellen davon überzeugen, bereits installierte Kameras wieder abzubauen. In zahlreichen Fällen der Videoaufzeichnung fehlten die gebotenen Freigaben, teilweise wurden Aufzeichnungen zu lange aufbewahrt, teilweise unterblieb die vorgeschriebene Kennzeichnung der Videoüberwachung.

Vor dem Hintergrund dieser Unsicherheiten im Umgang mit Art. 21a BayDSG habe ich einen Leitfaden zur Videoüberwachung durch bayerische Behörden entwickelt, der mit dem Staatsministerium des Innern, für Bau und Verkehr abgestimmt ist. Er ergänzt meine bisherigen Veröffentlichungen zur Videoüberwachung und soll vor Allem Kommunen bei der Prüfung unterstützen, ob eine Videoüberwachung im jeweiligen Einzelfall überhaupt zulässig ist und welche Vorgaben dann einzuhalten sind.

Der Leitfaden „Videoüberwachung – Leitfaden für bayerische Kommunen" ist auf meiner Homepage https://www.datenschutz-bayern.de unter „Veröffentlichungen" – „Broschüren und Orientierungshilfen" abrufbar.

Die Prüfergebnisse im Einzelnen und einzelfallbezogene Besonderheiten werden in den nachfolgenden Kapiteln dargestellt.

1.5 Öffentlichkeitsarbeit

Öffentlichkeitsarbeit hat eine zentrale Bedeutung für den Datenschutz. Daher will ich Informationen und datenschutzrechtliche Positionen – über den unmittelbaren Kontakt mit Politik, Presse, Behörden und im Einzelfall Betroffenen hinaus – allge-

mein bekannt machen. Auch so kann ich die Verwaltung dabei unterstützen, datenschutzkonform zu handeln. Bürgerinnen und Bürgern helfe ich damit, ihre Rechte sowie ihre Möglichkeiten, die eigenen Daten zu schützen, zu (er)kennen und wahrzunehmen.

Ein wesentlicher Baustein meiner Öffentlichkeitsarbeit ist der **Internetauftritt** meiner Dienststelle (https://www.datenschutz-bayern.de). Erfreulicherweise sind die Zugriffe gegenüber dem letzten Berichtszeitraum um ca. 50 % gestiegen. Die Webseite habe ich inhaltlich ausgebaut, Rubriken wie etwa „Häufige Fragen" aktualisiert und erweitert. Auch die Zahl der abrufbaren Materialien wächst stetig. Nur beispielhaft möchte ich die von meiner Dienststelle erarbeiteten Orientierungshilfen und Muster für die Verwaltung sowie die Orientierungshilfen und Entschließungen der Konferenz der Datenschutzbeauftragten des Bundes und der Länder nennen. Über neue Inhalte des Internetauftritts kann sich übrigens jeder per RSS Feed informieren lassen.

Allerdings will ich auch Bevölkerungsgruppen erreichen, die meine Webseite normalerweise nicht besuchen. Deshalb wandert meine **Ausstellung „Vom Eid des Hippokrates bis zu Edward Snowden – eine kleine Reise durch 2500 Jahre Datenschutz"** von Ort zu Ort. Die Ausstellung erklärt insbesondere gesetzliche Grundlagen, Datenschutzrechte, meine Aufgabenstellung sowie Möglichkeiten, die eigenen Daten zu schützen. Diese Informationen sind unterhaltsam in einer kleinen Zeitreise verpackt – von den Ursprüngen des Datenschutzes bis zu den anstehenden Herausforderungen des digitalen Zeitalters und der Globalisierung.

Es freut mich besonders, dass die Ausstellung zuerst im Bayerischen Landtag zu sehen war und dort im April 2014 mit Vorträgen und einem Live-Hacking eröffnet wurde. Anschließend war die Ausstellung bei der Bayerischen Verwaltungsschule in München, der Stadt Nürnberg, der Hochschule Ansbach, der Stadt Würzburg, der Stadt Bayreuth, der Stadt Aschaffenburg und der Fachhochschule für öffentliche Verwaltung und Rechtspflege in Hof zu Gast. Weitere Orte werden folgen. Die Ausstellung kann zudem virtuell auf meiner Webseite im Bereich „Aktuelles" besucht werden, dort sind außerdem die Stationen der Wanderausstellung aufgelistet.

Aufgrund der guten Erfahrungen werde ich auch meinen **Informationsstand** weiter nutzen, um Bürgerinnen und Bürger vor Ort zu informieren, sie darüber hinaus zu beraten und mit ihnen zu diskutieren. Im Berichtszeitraum war der Stand am 13.10.2013 beim Tag der offenen Tür der Stadt Nürnberg und am 08.11.2014 beim Tag der offenen Tür des Bayerischen Landtags.

Nicht nur dort war das Interesse an meinen **Broschüren** (siehe 25. Tätigkeitsbericht 2012 Nr. 1.5) groß. Sie wurden zudem rege bei mir bestellt und von meiner Webseite herunter geladen. Angesichts der anhaltenden Nachfrage sind bereits weitere Nachdrucke vorgesehen.

Anlässlich des **8. Europäischen Datenschutztags** habe ich im Januar 2014 zusammen mit dem Vorsitzenden der Datenschutzkommission beim Bayerischen Landtag, Herrn Eberhard Rotter, MdL, eine Podiumsdiskussion zum Thema „Social Media Guidelines" veranstaltet.

Außerdem haben Angehörige meiner Dienststelle und ich an zahlreichen **Informations- und Diskussionsveranstaltungen** als Referenten teilgenommen sowie vor Schulklassen **Vorträge** und an Hochschulen Vorlesungen oder Gastvorträge

gehalten. Bemühungen zur Stärkung der Medienkompetenz unterstütze ich nachhaltig.

Pressearbeit ist besonders wichtig, um die Öffentlichkeit zu informieren und datenschutzrechtliche Positionen darzustellen. Die Medien berichten inzwischen fast täglich zu Themen mit Bezug zum Datenschutz, auch hieran zeigt sich das stetig steigende Interesse. Dementsprechend hatte ich zahlreiche Presseanfragen zu beantworten und Interviews zu geben. Daneben habe ich eine Reihe von Pressemitteilungen herausgegeben und Hintergrundgespräche geführt.

Auf die gestiegenen Anforderungen habe ich auch organisatorisch reagiert und eine **Stabsstelle** eingerichtet. Der Stabsstelle ist neben anderen Aufgaben die Öffentlichkeits- und Pressearbeit zugeordnet.

1.6 Schlussbemerkung

Die nachfolgenden Kapitel geben einen Überblick über meine Beteiligung an wesentlichen, hier nicht erwähnten Gesetzesverfahren und meine Datenschutzkontrolle der bayerischen öffentlichen Stellen im Berichtszeitraum 2013/2014.

.

2 Informations- und Kommunikationstechnik und Organisation

2.1 Grundsatzthemen

2.1.1 Empfehlungen aus der Vergangenheit für Gefährdungen in der Gegenwart

Gerade in diesem Berichtszeitraum sind durch die Veröffentlichungen in den Medien über die Tätigkeiten und Möglichkeiten vor allem US-amerikanischer Nachrichtendienste die Gefahren bei der IuK-gestützten Übertragung und Verarbeitung von personenbezogenen Daten in den Fokus der öffentlichen Diskussion gerückt.

Unabhängig davon musste eine Übertragung von Daten über das Internet schon seit den Anfängen des Internets als unsicher gelten. Während zu den Anfangszeiten des Internets Daten inklusive Kennungen und Passwörtern in der Regel unverschlüsselt – beispielsweise mittels telnet – übertragen wurden, ersetzten mit dem zunehmenden Wachstum des Netzes in den 1990er Jahren vermehrt verschlüsselte Alternativen (ssh) diese Protokolle. Damals war es nicht unüblich, dass sich Dritte unberechtigt Zugriff auf Teile der Netzwerkinfrastruktur verschafften und dort versuchten, Kennungen und Passwörter abzugreifen. Lange vor der Entwicklung und Inbetriebnahme des World Wide Web (WWW) enthielt mein 5. Tätigkeitsbericht 1982 deshalb bereits folgenden Hinweis:

5. Tätigkeitsbericht des Landesbeauftragten für den Datenschutz 1982
Kapitel 5.1.1 Datensicherung und moderne Technologie
Eine Reihe von Problemen zeichnet sich schon jetzt bei der Gewährleistung des Zugriffsschutzes der in Konzentratoren und Zentralen gespeicherten Daten und der allgemeinen Datensicherheit auf dem Übertragungsweg ab. Im Zusammenhang damit tauchen die Fragen der Verschlüsselung und Authentifikation auf, die zwar allgemein bekannt sind, im öffentlichen Bereich jedoch bisher – wohl auch wegen der damit verbundenen Kosten – nur vereinzelt gelöst wurden.

Im Jahr 1988 wurde die Bedeutung der Sicherheit bei der Datenübertragung immer deutlicher:

10. Tätigkeitsbericht des Landesbeauftragten für den Datenschutz 1988
Kapitel 21.1.1 Fortentwicklung der Datensicherung
In der Datenkommunikation ist es weiter von großer Bedeutung, dass auf Leitungen übertragene Informationen nicht unbemerkt verfälscht oder von Lauschern interpretiert werden können.

Auch mein 12. Tätigkeitsbericht aus dem Jahre 1990 hat selbst 25 Jahre später immer noch eine erschreckende Aktualität:

12. Tätigkeitsbericht des Landesbeauftragten für den Datenschutz 1990
Kapitel 22.3.4 Datensicherheit bei der Datenübertragung

Was bleibt, ist aber vor allem das Risiko, dass die Datenübertragungsstrecken abgehört werden. Große Verunsicherung herrschte, als (…) in der Öffentlichkeit bekannt wurde, dass fremde Geheimdienste regelmäßig und in manchen Gebieten vollständig den Fernsprechverkehr abgehört haben. … Der Anwender kann sich nur insofern gegen das Abhören schützen, als er die auf die Leitung geschickten Daten verschlüsselt.

Dies zeigt, dass seit dem Beginn der elektronischen Datenübertragung deren Sicherung stets eine wichtige Aufgabe war oder zumindest hätte gewesen sein müssen. Meine Warnungen und Forderungen nach zu ergreifenden zusätzlichen Sicherungsmaßnahmen wie etwa einer Ende-zu-Ende-Verschlüsselung zur Wahrung der Vertraulichkeit werden nunmehr schon seit mehr als 30 Jahren oft dem Kosten- und Aufwand-Argument gegenübergestellt.

Allerdings darf bei Sicherheitsmaßnahmen nicht nur an die verschlüsselte Übertragung gedacht werden. Auch sollten ausländische Nachrichtendienste nicht als einzige Bedrohung angesehen werden. Ich warne davor, die anderen Gefahren (unberechtigtes Eindringen in Computernetzwerke etwa durch nicht-staatliche Hacker, Trojaner und andere Schadsoftware, Sicherheitslücken in Netzwerkdiensten usw.) zu vernachlässigen. Ein durchgehender IT-Grundschutz gegen die bekannten und weitverbreiteten Gefahren der Datenverarbeitung und -übertragung ist eine Grundvoraussetzung auch für die technische Abwehr von hochprofessionellen Angreifern.

Deshalb sind gerade bei neuen Projekten die Informationssicherheit und der Datenschutz bereits bei der Planung zu berücksichtigen („Security and Privacy by Design"). Hohe Kosten für die Abwehr von IT-Gefahren entstehen vor allem dann, wenn Sicherheitsmaßnahmen erst nachträglich eingeführt werden müssen. Neben den Anfangskosten sind aber auch für den fortlaufenden Betrieb Mittel und Personalressourcen einzuplanen, sodass das anfänglich erreichte Sicherheits- und Datenschutzniveau immer wieder geprüft und dauerhaft sichergestellt werden kann.

Auch die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat in der Anlage zur Entschließung „Gewährleistung der Menschenrechte bei der elektronischen Kommunikation" vom 27./28.03.2014 Maßnahmen aufgeführt, von denen ich folgende gerade auch für öffentliche Stellen herausheben möchte:

Entschließung der 87. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 27./28.03.2014
Gewährleistung der Menschenrechte bei der elektronischen Kommunikation (Auszug aus der Anlage zur Entschließung)

1. Sichere Verschlüsselung beim Transport und bei der Speicherung von Daten als wesentliches Element für den Schutz von Daten

Der verschlüsselte Transport und die verschlüsselte Speicherung von Daten müssen zu einem in Produkte und Verfahren integrierten Standard werden, der durch jedermann einfach zu nutzen ist. Sichere kryptographischen Algorithmen, die seit vielen Jahren zur Verfügung stehen, stellen auch für Geheimdienste eine erhebliche Hürde dar und erschweren die unberechtigte Kenntnisnahme der so geschützten Daten wesentlich.
Für die Sicherung der Übertragungswege sollen Verfahren zum Einsatz

kommen, die eine nachträgliche Entschlüsselung des abgeschöpften Datenverkehrs erschweren (perfect forward secrecy).

2. *Bereitstellung einer von jeder Person einfach bedienbaren Verschlüsselungsinfrastruktur*

   Für eine breite Anwendung von Verschlüsselung durch die Bürgerinnen und Bürger wird eine Infrastruktur benötigt, die es jeder Person weitgehend ohne Barrieren (in Form von Wissen, nötiger spezieller Software oder finanziellen Mitteln) ermöglicht, den von ihr verwendeten Kommunikationsadressen Schlüssel authentisch zuzuordnen und die anderer zu nutzen. Die Entstehung dieser Infrastruktur bedarf der Förderung durch den Staat unter Einbeziehung bestehender Instrumente bspw. durch Entwicklung kryptografischer Zusatzfunktionen des neuen Personalausweises.

   Es mangelt also nicht vorrangig an theoretischen Konzepten, sondern an einer ausreichenden Durchdringung in der Praxis. Der öffentliche wie der private Sektor müssen daher ihre Anstrengungen erhöhen, Verschlüsselungstechniken selbst einzusetzen und in ihre Produkte und Dienstleistungen einzubinden.

3. *Einsatz von Ende-zu-Ende-Verschlüsselung in Kombination mit Verbindungsverschlüsselung*

   Der Einsatz von Mechanismen für eine Ende-zu-Ende-Verschlüsselung muss gefördert werden. Die Enthüllungen von Edward Snowden haben gezeigt, dass der Zugriff auf Daten besonders einfach ist, wenn sie an Netzknoten unverschlüsselt vorliegen oder innerhalb interner Netze unverschlüsselt übertragen werden. Nur eine Ende-zu-Ende-Verschlüsselung ist in der Lage, die Inhaltsdaten auch an diesen Stellen zu schützen. Die zusätzliche Verschlüsselung der Verbindungen zwischen den an der Übertragung beteiligten Netzknoten (Verbindungsverschlüsselung) hingegen schützt die Metadaten der Kommunikation in allen Zwischenknoten der verschlüsselten Wegstrecke. Durch die Kombination beider Verfahren kann ein Optimum an Schutz zwischen den Endpunkten erreicht werden.

   Für beide Ansätze stehen etablierte Verfahren zur Verfügung, sowohl in Bezug auf kryptografische Verfahren und Datenformate, als auch in Bezug auf das Identitäts- und Schlüsselmanagement, von dessen Stringenz die Sicherheit wesentlich abhängt.

4. *Sichere und vertrauenswürdige Bereitstellung von Internetangeboten*

   Sämtliche Internetangebote öffentlicher Stellen sollten standardmäßig über TLS (Transport Layer Security)/SSL (Secure Socket Layer) unter Beachtung der Empfehlungen des Bundesamtes für Sicherheit in der Informationstechnik angeboten werden. Die Behörden sollten sich hierbei mit Zertifikaten ausweisen, die von vertrauenswürdigen Ausstellern herausgegeben wurden, die sich in europäischer, und vorzugsweise in öffentlicher Hand befinden. Nichtöffentliche Stellen stehen gleichermaßen in der Verpflichtung, die Nutzung von ihnen angebotener Telemedien einschließlich der von einem Nutzer abgerufenen URIs (Uniform Resource Identifier) gegen Kenntnisnahme Dritter im Rahmen der Verhältnismäßigkeit durch Verschlüsselung zu schützen.

8. Sichere Verschlüsselung der Mobilkommunikation und Einschränkung der Möglichkeiten der Geolokalisierung

(…) Wie für TK-Anbieter, so gilt auch für Anbieter von Telemedien für die mobile Nutzung, insbesondere in Form mobiler Anwendungen (Apps), dass sie die Erhebung von personenbezogenen Daten auf das für die jeweils erbrachte Dienstleistung erforderliche Minimum beschränken müssen und die Übertragung dieser Daten durch Verschlüsselung schützen sollten. Apps sollten künftig so durch Nutzerinnen und Nutzer konfigurierbar sein, dass diese selbst bestimmen können, wem welche Daten zu welchem Zweck übermittelt werden.

9. Beschränkung des Cloud Computings mit personenbezogenen Daten auf vertrauenswürdige Anbieter mit zertifizierter Informationssicherheitstechnik

Sollen personenbezogene Daten in einer Cloud-Anwendung verarbeitet werden, so dürfen nur Anbieter zum Zuge kommen, deren Vertrauenswürdigkeit sowohl in Bezug auf die Gewährleistung der Informationssicherheit, als auch in Bezug auf den Rechtsrahmen, innerhalb dessen sie operieren, gegeben ist.

Dazu gehören unter anderem ein (zertifiziertes) Informationssicherheitsmanagement, die sichere Verschlüsselung der zu verarbeitenden Daten sowohl bei ihrer Übertragung in und aus der Cloud als auch bei ihrer Speicherung und eine durch den Auftraggeber kontrollierte Vergabe von Unteraufträgen. Das Datenschutzniveau dieser Dienste sollte durch unabhängige und fachkundige Auditoren geprüft und zertifiziert werden.

10. Förderung der Vertrauenswürdigkeit informationstechnischer Systeme durch Zertifizierung

Hard- und Software sollten so entwickelt und hergestellt werden, dass Anwenderinnen und Anwender und unabhängige Dritte sich jederzeit von der Wirksamkeit der getroffenen Sicherheitsvorkehrungen überzeugen können. Open-Source-Produkte ermöglichen derartige Prüfungen besonders gut. Daher ist der Einsatz von Open-Source-Produkten zu fördern.

Darüber hinaus ist es erforderlich, die bereits bestehenden Zertifizierungsverfahren für informationstechnische Produkte und die Informationssicherheit von Verarbeitungsvorgängen breiter zur Anwendung zu bringen und um weitere Zertifizierungsverfahren zu ergänzen, um die Vertrauenswürdigkeit von informationstechnischen Produkten zu stärken. Voraussetzung dafür sind unabhängige und fachkundige Auditoren sowie transparente Kriterienkataloge und Zertifizierungsprozesse.

12. Ausreichende Finanzierung für Maßnahmen der Informationssicherheit

Die Ausgaben der öffentlichen Hand für Informationssicherheit müssen erhöht werden und in einem angemessenen Verhältnis zum gesamten IT-Budget stehen. Die Koalitionspartner auf Bundesebene haben die Bundesbehörden bereits verpflichtet, zehn Prozent des IT-Budgets für die Sicherheit zu verwenden. Dies muss in angemessener Weise auch für Landesbe-

hörden und andere öffentliche Stellen gelten. Die Ressourcen werden sowohl für die Planung und Absicherung neuer Vorhaben insbesondere des E-Governments als auch für die Revision und sicherheitstechnische Ergänzung der Verfahren und der Infrastruktur im Bestand benötigt.

Ein Großteil dieser Punkte dürfte allgemein bekannt sein. Ich halte es heutzutage für mehr als geboten, dass sie – auch trotz der damit verbundenen Kosten – im Gegensatz zu meinen Feststellungen im Jahre 1982 nicht nur vereinzelt, sondern grundsätzlich umgesetzt werden. Ein vertrauenswürdiger Einsatz von Informations- und Kommunikationstechnik und ein vertrauenswürdiges E-Government sind ohne Berücksichtigung und Umsetzung der vorgenannten Sicherheitsmaßnahmen nicht möglich.

2.1.2 Apps

Anwendungen für mobile Geräte – sogenannte „Apps" – werden Großteils im nicht-öffentlichen Bereich entwickelt und angeboten. Aber auch immer mehr öffentliche Stellen in Bayern bieten Bürgern oder eigenen Mitarbeitern speziell für Mobilgeräte angepasste Webseiten („Web-Apps") oder für mobile Geräte entwickelte Anwendungen („Native-Apps") an.

Lediglich in Ausnahmefällen („Offline-Apps"), in denen keine Verbindung mit den zur Verfügung stehenden Netzen aufgenommen wird, sind Apps wie normale Anwendungen auf Arbeitsplatzrechnern zu bewerten.

Im Regelfall sind aus Sicht des Datenschutzes Apps – auch Native-Apps mit Übertragung von Daten über öffentliche Netzwerke – weitgehend wie klassische Webseiten zu bewerten. Dabei stehen auf dem Gerät, auf dem die App genutzt wird, meist mehr personenbezogene Daten als auf einem üblichen PC (wie beispielsweise der aktuelle Standort oder Geräte- und Kartenkennungen) zur Verfügung, die unter Umständen an den Anbieter der App oder an Dritte gesendet werden. Darauf ist bei der datenschutzrechtlichen Prüfung und Freigabe von mobilen Verfahren besonders zu achten.

Der Anbieter der App ist in der Regel für die mit der App verbundene Verarbeitung von personenbezogenen Daten verantwortlich. Lediglich für Daten, die immer in der Verfügungsgewalt des Nutzers bleiben und auf die der Anbieter weder direkt noch indirekt Zugriff hat, kann die Verantwortung allein beim Nutzer liegen.

Betreibt ein Dritter die Infrastruktur, die die App nutzt, um personenbezogene Daten zu speichern oder zu verarbeiten, also etwa Web- oder Datenbankserver, so handelt es sich grundsätzlich um eine Speicherung oder Verarbeitung von Daten im Auftrag gemäß Art. 6 BayDSG. Auch hierbei bleibt der Anbieter für die Einhaltung der Vorschriften des Bayerischen Datenschutzgesetzes und anderer Vorschriften über den Datenschutz verantwortlich. Insbesondere bei Web-Apps, die über die (Weiterleitung von einer) Internet-Adresse (URL) einer öffentlichen Stelle nutzbar sind, ist davon auszugehen, dass die öffentliche Stelle – nicht ein eventuell vorhandener Dritter als Entwickler der App oder Betreiber der Netzdienste – die datenschutzrechtlich verantwortliche Stelle ist.

Auch Verfahren zur Reichweitemessung („Nutzungsstatistiken"), die innerhalb einer App eingesetzt werden, hat der Anbieter der App zu verantworten. Zur diesbezüglichen rechtlichen Unzulässigkeit von Reichweitemessungen habe ich mich

bereits in meinem 24. Tätigkeitsbericht 2010 unter Nr. 2.1.6 und im 25. Tätigkeitsbericht 2012 unter Nr. 2.3.2 geäußert.

Insbesondere muss jede App ein Impressum, das § 5 Telemediengesetz (TMG) genügt, verfügbar halten und der Diensteanbieter muss seinen Pflichten nach § 13 TMG, wie etwa der Unterrichtung des Nutzers mit einer Datenschutzerklärung, nachkommen:

§ 5 TMG Allgemeine Informationspflichten
(Auszug)
(1) Diensteanbieter haben für geschäftsmäßige, in der Regel gegen Entgelt angebotene Telemedien folgende Informationen leicht erkennbar, unmittelbar erreichbar und ständig verfügbar zu halten:

1. *den Namen und die Anschrift, unter der sie niedergelassen sind, bei juristischen Personen zusätzlich die Rechtsform, den Vertretungsberechtigten und, sofern Angaben über das Kapital der Gesellschaft gemacht werden, das Stamm- oder Grundkapital sowie, wenn nicht alle in Geld zu leistenden Einlagen eingezahlt sind, der Gesamtbetrag der ausstehenden Einlagen,*
2. *Angaben, die eine schnelle elektronische Kontaktaufnahme und unmittelbare Kommunikation mit ihnen ermöglichen, einschließlich der Adresse der elektronischen Post,*
3. *soweit der Dienst im Rahmen einer Tätigkeit angeboten oder erbracht wird, die der behördlichen Zulassung bedarf, Angaben zur zuständigen Aufsichtsbehörde,*

...

§ 13 TMG Pflichten des Diensteanbieters
(1) Der Diensteanbieter hat den Nutzer zu Beginn des Nutzungsvorgangs über Art, Umfang und Zwecke der Erhebung und Verwendung personenbezogener Daten sowie über die Verarbeitung seiner Daten in Staaten außerhalb des Anwendungsbereichs der Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (ABl. EG Nr. L 281 Seite 31) in allgemein verständlicher Form zu unterrichten, sofern eine solche Unterrichtung nicht bereits erfolgt ist. Bei einem automatisierten Verfahren, das eine spätere Identifizierung des Nutzers ermöglicht und eine Erhebung oder Verwendung personenbezogener Daten vorbereitet, ist der Nutzer zu Beginn dieses Verfahrens zu unterrichten. Der Inhalt der Unterrichtung muss für den Nutzer jederzeit abrufbar sein.
(2) Die Einwilligung kann elektronisch erklärt werden, wenn der Diensteanbieter sicherstellt, dass

1. *der Nutzer seine Einwilligung bewusst und eindeutig erteilt hat,*
2. *die Einwilligung protokolliert wird,*
3. *der Nutzer den Inhalt der Einwilligung jederzeit abrufen kann und*
4. *der Nutzer die Einwilligung jederzeit mit Wirkung für die Zukunft widerrufen kann.*

(3) Der Diensteanbieter hat den Nutzer vor Erklärung der Einwilligung auf das Recht nach Abs. 2 Nr. 4 hinzuweisen. Abs. 1 Satz 3 gilt entsprechend.
(4) Der Diensteanbieter hat durch technische und organisatorische Vorkehrungen sicherzustellen, dass

1. *der Nutzer die Nutzung des Dienstes jederzeit beenden kann,*
2. *die anfallenden personenbezogenen Daten über den Ablauf des Zugriffs oder der sonstigen Nutzung unmittelbar nach deren Beendigung gelöscht oder in den Fällen des Satzes 2 gesperrt werden,*

3. der Nutzer Telemedien gegen Kenntnisnahme Dritter geschützt in Anspruch nehmen kann,
4. die personenbezogenen Daten über die Nutzung verschiedener Telemedien durch denselben Nutzer getrennt verwendet werden können,
5. Daten nach § 15 Abs. 2 nur für Abrechnungszwecke zusammengeführt werden können und
6. Nutzungsprofile nach § 15 Abs. 3 nicht mit Angaben zur Identifikation des Trägers des Pseudonyms zusammengeführt werden können.

An die Stelle der Löschung nach Satz 1 Nr. 2 tritt eine Sperrung, soweit einer Löschung gesetzliche, satzungsmäßige oder vertragliche Aufbewahrungsfristen entgegenstehen.

(5) Die Weitervermittlung zu einem anderen Diensteanbieter ist dem Nutzer anzuzeigen.

(6) Der Diensteanbieter hat die Nutzung von Telemedien und ihre Bezahlung anonym oder unter Pseudonym zu ermöglichen, soweit dies technisch möglich und zumutbar ist. Der Nutzer ist über diese Möglichkeit zu informieren.

(7) Der Diensteanbieter hat dem Nutzer nach Maßgabe von § 34 des Bundesdatenschutzgesetzes auf Verlangen Auskunft über die zu seiner Person oder zu seinem Pseudonym gespeicherten Daten zu erteilen. Die Auskunft kann auf Verlangen des Nutzers auch elektronisch erteilt werden.

Der Düsseldorfer Kreis als informeller Zusammenschluss der Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich hat eine Orientierungshilfe zu den Datenschutzanforderungen an App-Entwickler und App-Anbieter erstellt, die auf meiner Homepage unter https://www.datenschutz-bayern.de/technik/orient/OH_Apps.pdf abgerufen werden kann. Speziell die dortigen Ausführungen zum TMG sind auch auf öffentliche Stellen in Bayern übertragbar. Öffentliche Stellen sollten deshalb bei der Entwicklung und dem Betrieb von Apps diese Orientierungshilfe beachten. Dabei müssen sie allerdings berücksichtigen, dass neben dem TMG grundsätzlich nicht die dort genannten Vorschriften, sondern das Bayerische Datenschutzgesetz und andere vorrangig zu beachtende, bereichsspezifische Datenschutzvorschriften maßgeblich sind.

Im Berichtszeitraum habe ich begonnen, bei ausgewählten Apps aus unterschiedlichen Bereichen der bayerischen Staatsverwaltung verschiedene Kriterien in einem ersten Schritt mit einem ausführlichen Fragebogen zu prüfen. Davon abhängig werden gegebenenfalls weitere Prüfschritte folgen. Als Ausgangspunkt für meine Prüfungen dienen dabei die Inhalte oben genannter Orientierungshilfe.

2.1.3 Neue Vorschriften zur Datenträgervernichtung

Bei der Entsorgung von Datenträgern mit personenbezogenen Daten ist zu beachten, dass die Anforderungen an technische und organisatorische Maßnahmen bei der Vernichtung von Datenträgern umso höher sein müssen, je höher die Sensibilität der Daten ist. Als Orientierungshilfe kann hierfür die neu entwickelte DIN 66399 herangezogen werden. Eine DIN-Norm ist keine gesetzliche Vorgabe, sondern ein unter dem Dach des Deutschen Instituts für Normung erarbeiteter freiwilliger Standard, in dem materielle und immaterielle Gegenstände vereinheitlicht sind.

Zur Festlegung der für die einzelnen Daten erforderlichen Maßnahmen und Anforderungen an die Entsorgungsgeräte, wurde bereits im Jahre 1985 die

DIN 32757-1 entwickelt, die zwischen fünf verschiedenen Sicherheitsstufen (in Abhängigkeit von der Sensibilität der Daten) unterschied.

Im August 2009 wurde eine europäische Norm (EN 15713:2009 – „Secure destruction of confidential material") veröffentlicht, die in Deutschland unter der Bezeichnung DIN EN 15713 „Sichere Vernichtung von vertraulichen Unterlagen – Verfahrensregeln" Gültigkeit erlangt hat.

Da eine der europäischen Normung entgegenstehende nationale Normung nicht zulässig ist, konnte die bisherige DIN 32757 nicht unverändert aufrechterhalten bleiben. Mit der Überarbeitung der bisherigen DIN 32757 sollten daher die festgelegten Sicherheitsstufen und die in der EN 15713 empfohlenen Zerkleinerungsstufen aufeinander abgestimmt, neue gesetzliche Vorgaben zum Datenschutz berücksichtigt, mehr auf deutsche Gegebenheiten und Bedürfnisse eingegangen sowie der neueste Stand der Technik berücksichtigt werden.

Daher hat der zuständige Normenausschuss innerhalb von drei Jahren die DIN-Norm 66399 erstellt. Diese neue DIN-Norm besteht aus drei Teilen:

— DIN 66399-1 „Büro- und Datentechnik – Vernichten von Datenträgern – Teil 1: Grundlagen und Begriffe"
(definiert die Grundlagen und Begriffe, die bei der Datenträgervernichtung beachtet werden sollten)

— DIN 66399-2 „Büro- und Datentechnik – Vernichten von Datenträgern – Teil 2: Anforderungen an Maschinen zur Vernichtung von Datenträgern"
(beschreibt die Anforderungen an Maschinen zur Vernichtung von Datenträgern)

— DIN SPEC 66399-3 „Büro- und Datentechnik – Vernichten von Datenträgern – Teil 3: Prozess der Datenträgervernichtung"
(bildet den kompletten Prozess der Datenträgervernichtung durch entsprechende Spezifikation (SPEC) ab)

Während die ersten beiden Teile im Oktober 2012 in Kraft getreten sind, hat der dritte Teil erst zum Jahreswechsel 2012/13 seine Gültigkeit erlangt. Gleichzeitig sind die DIN 32757-1 und DIN 44300 außer Kraft getreten.

Nähere Einzelheiten zu den neuen DIN-Normen (insbesondere zur DIN 66399) enthält die Orientierungshilfe „Datenträgerentsorgung" – abrufbar auf meiner Homepage https://www.datenschutz-bayern.de unter „Veröffentlichungen" – „Broschüren und Orientierungshilfen".

2.1.4 Strategie bei der Auswahl geeigneter Datensicherheitsmaßnahmen

Viele öffentliche Stellen in Bayern wollen zwar einerseits die gesetzlichen Vorgaben der Datenschutzgesetze erfüllen, allerdings fehlt es ihnen häufig am notwendigen Know-how, mit welchen technisch-organisatorischen Maßnahmen sie die Datensicherheit gewährleisten können. Diesen Stellen teile ich auf ihre Anfragen regelmäßig Folgendes bezüglich der Auswahl von geeigneten Datensicherheitsmaßnahmen mit:

Zweck der Datenschutzgesetze ist es, den Einzelnen davor zu schützen, dass er durch den Umgang mit seinen personenbezogenen Daten in seinem Persönlichkeitsrecht beeinträchtigt wird. Beeinträchtigungen seiner Persönlichkeit können unter anderem zur Verletzung seiner Privatsphäre, zu Belästigungen, zu Ruf- oder Geschäftsschädigungen und zur Verletzung existenzieller Grundlagen führen.

Bei der Prüfung, ob eine Datensicherheitsmaßnahme zur Erreichung des erforderlichen Schutzzwecks notwendig ist, sollte daher stets von der Gefährdung ausgegangen werden, die eine missbräuchliche Verwendung von Daten für den Einzelnen verursachen kann. Je stärker das Persönlichkeitsrecht verletzt werden kann, desto umfassendere technische und organisatorische Maßnahmen sind zur Verhinderung missbräuchlicher Datenverarbeitung erforderlich.

Bei der Auswahl der Datensicherheitsmaßnahmen ist stets darauf zu achten, dass das Datensicherheitskonzept in sich geschlossen und abgestimmt ist. Daher sind alle im Art. 7 des BayDSG aufgeführten zehn Kontrollbereiche zu untersuchen und gegebenenfalls durch geeignete Maßnahmen auszufüllen. Es ergibt wenig Sinn, wenn bei einigen Kontrollbereichen starke, ja vielleicht sogar überzogene Maßnahmen vorgeschlagen, aber andere Kontrollbereiche außer Acht gelassen werden, sodass das Gesamtsystem lückenhaft wird und seinen Schutzzweck nicht erfüllen kann.

Zur Festlegung, welche Datensicherheitsmaßnahmen für welche Datenverarbeitung oder welche Datei zu ergreifen sind, empfiehlt sich folgendes Vorgehen:

- Untersuchung der zu verarbeitenden personenbezogenen Daten auf ihre Sensibilität und Zuordnung zu einer Schutzkategorie.

- Festlegung der Sicherheitsbereiche und der Zugangs- bzw. Zugriffsberechtigungen.

- Definition der erforderlichen Datensicherheitsmaßnahmen und Überprüfung auf ihre Brauchbarkeit.

- Realisierung der technischen und organisatorischen Maßnahmen; bei deren schrittweiser Einführung sind Freiräume zu vermeiden.

- Probeweises Einführen der Maßnahmen, um Akzeptanz bei den Beteiligten zu erzeugen und Erfolg und Effektivität der Maßnahmen sicherzustellen.

- Überprüfung und gegebenenfalls Nachbesserung des Sicherheitskonzepts, wenn sich eine Sicherheitsmaßnahme als nicht praktikabel erweist und den Arbeitsablauf zu stark behindert oder wenn beim Probebetrieb vorher nicht erkannte Lücken auftreten.

- Anordnung der Sicherheitsmaßnahmen nach Erreichen der Einsatzreife und Bekanntgabe an alle Beteiligte.

- Regelmäßige Überprüfung der Sicherheitsmaßnahmen auf deren Einhaltung und Ergreifen geeigneter Sanktionen bei deren Nichteinhaltung.

Insbesondere bei Heranziehung von Maßnahmenkatalogen ist im Rahmen der Definition von Sicherheitsmaßnahmen zu beachten, dass manche Maßnahmen

gleiche Sachverhalte regeln, sich gegenseitig behindern oder auch durch andere Maßnahmen bereits abgedeckt sein können.

Beziehen sich Maßnahmen beispielsweise auf ein Rechenzentrum als Ganzes, etwa baulichen Maßnahmen, so muss sich die Stärke der einzelnen Maßnahmen an dem Verfahren mit der höchsten Schutzklasse orientieren. Hingegen gibt es bei bestimmten Sicherheitsmaßnahmen, etwa bei der Transportkontrolle, durchaus auch verfahrensbezogene Unterschiede.

2.1.5 Anfertigen von Kopien des neuen Personalausweises (nPA)

Auch wenn der neue Personalausweis bereits seit dem Jahr 2010 ausgegeben wird, scheint es nach wie vor Unklarheiten zu geben, ob und zu welchem Zweck das Anfertigen einer Kopie beziehungsweise das Scannen des nPA zulässig ist. Aus technischer Sicht ist eine vollständige Kopie der Vorderseite des nPA unter anderem deshalb kritisch zu sehen, da auf der Vorderseite eine sechsstellige Zugangsnummer aufgedruckt ist. Mit Hilfe dieser Nummer und einem entsprechenden Zertifikat können die auf dem Chip gespeicherten elektronischen Daten kontaktlos ausgelesen werden. Ohne diese Nummer ist ein unbemerktes Auslesen, etwa solange sich der nPA in einer Geldbörse befindet, nicht möglich.

In diesem Zusammenhang maßgeblich zu beachten ist § 20 Abs. 2 Personalausweisgesetz (PAuswG).

§ 20 PAuswG Verwendung durch öffentliche und nichtöffentliche Stellen
(2) Außer zum elektronischen Identitätsnachweis darf der Ausweis durch öffentliche und nichtöffentliche Stellen weder zum automatisierten Abruf personenbezogener Daten noch zur automatisierten Speicherung personenbezogener Daten verwendet werden.

In der Gesetzesbegründung (Bundestags-Drucksache 16/10489, Seite 42) wird hierzu ausgeführt, dass alle Formen des automatischen Abrufs, insbesondere Scannen, Fotokopieren und Ablichten der Daten von der Vorschrift umfasst sind.

Trotzdem kann eine Kopie des nPA durch eine öffentliche Stelle etwa durch spezialgesetzliche Ausnahmeregelungen (wie etwa in der Fahrerlaubnis-Verordnung) zulässig sein.

Im Falle der Anfertigung einer Kopie sollten jedenfalls die nicht benötigten Daten (insbesondere Zugangs- und Seriennummern) auf der Kopie geschwärzt werden. Fordert eine öffentliche Stelle von Bürgern eine Kopie ihres Personalausweises an, so sind diese auf die Möglichkeit und Notwendigkeit einer Schwärzung der nicht benötigten Daten hinzuweisen.

2.1.6 Überwachung der ordnungsgemäßen Anwendung der Datenverarbeitungsprogramme

Grundsätzlich ist jede öffentliche Stelle in Bayern nach Art. 25 BayDSG dazu verpflichtet, einen behördlichen Datenschutzbeauftragten zu bestellen. Dieser Verpflichtung kommen die Behörden und Gemeinden in der Regel auch nach. Allerdings verfügen viele neu bestellte Datenschutzbeauftragte zu Beginn ihrer Tätig-

keit noch nicht über das hierfür speziell notwendige Wissen. So wendet sich jährlich eine ganze Reihe neu bestellter behördlicher Datenschutzbeauftragter mit der Frage an mich, wie sie am besten ihre Aufgaben erfüllen können. Insbesondere ist ihnen häufig unklar, wie sie die ordnungsgemäße Anwendung der Datenverarbeitung bei ihrer öffentlichen Stelle überwachen können. Diese Anfragen beantworte ich wie folgt:

Zu den wesentlichen Aufgaben eines behördlichen Datenschutzbeauftragten gehört die Überwachung der ordnungsgemäßen Anwendung der Datenverarbeitungsprogramme, mit denen personenbezogene Daten verarbeitet werden sollen.

Neben der Zuständigkeit zur Erteilung der datenschutzrechtlichen Freigabe ist der behördliche Datenschutzbeauftragte daher gehalten, die Einhaltung der Datenschutzvorschriften (insbesondere der nach Art. 7 BayDSG erforderlichen technisch-organisatorischen Datensicherheitsmaßnahmen) und der behördlichen Dienstanweisungen zu Datenschutz und Datensicherheit zu überwachen.

Während eine datenschutzrechtliche Freigabe bereits vorliegen muss, bevor das entsprechende Verfahren in den Echtbetrieb übernommen werden kann, muss der Datenschutzbeauftragte nach Produktionsaufnahme die Einhaltung der datenschutzrechtlichen Vorschriften (insbesondere der Sicherheitsmaßnahmen) beim Verfahren überprüfen. Diese Kontrolle ist jederzeit möglich und sollte möglichst unangekündigt vorgenommen werden. Der behördliche Datenschutzbeauftragte kann selbst entscheiden, wann und in welcher Form er Kontrollen durchführt.

Neben dem Nachgehen von Beschwerden, die Anlass zu einer gezielten Kontrolle in dem betroffenen Bereich geben (sogenannte Anlasskontrollen), sollten auch ohne einen speziellen Anlass regelmäßige Kontrollen stattfinden.

Für die Durchführung von Kontrollen gibt es verschiedene Ansätze. In Betracht kommt insbesondere eine gezielte Prüfung der technisch-organisatorischen Maßnahmen und ihrer Einhaltung. Denkbar ist auch, sich auf die Prüfung eines der in der Art. 7 BayDSG benannten Maßnahmenbereiche zu konzentrieren.

Die Kontrolle kann auch auf ein bestimmtes Verfahren oder einen Bearbeitungsvorgang einschließlich der materiell-rechtlichen Prüfung, Einhaltung der Zweckbindung, Beachtung der Rechtsgrundlage etc. oder auch auf eine Kombination der angesprochenen Vorgehensweisen ausgerichtet werden.

Ein weiteres Ziel der Überprüfung der getroffenen Datensicherheitsmaßnahmen besteht darin, bestehende Schwachstellen zu entdecken, damit durch die Ergreifung weiterer Sicherheitsmaßnahmen das Risiko eines Schadens auf ein möglichst geringes Maß verringert werden kann.

Zur Durchführung der Kontrollen muss dem Datenschutzbeauftragten Zutritt zum Serverraum und den entsprechenden Diensträumen ermöglicht werden. Ferner muss er alle Unterlagen einsehen können, die mit der Verarbeitung personenbezogener Daten im Zusammenhang stehen. Ihm steht auch ein generelles Einsichtsrecht in die gespeicherten personenbezogenen Daten zu. Eine Kontrollbefugnis gegenüber dem Personalrat besteht dagegen nicht.

2.2 Prüfungen, Beanstandungen und Beratungen

Im Berichtszeitraum 2013/2014 habe ich eine ganze Reihe öffentlicher Stellen unter technisch-organisatorischen Datenschutzaspekten geprüft. Großteils wurden diese Prüfungen von meinem Technikreferat gemeinsam mit dem jeweils zuständigen Rechtsreferat durchgeführt. Im Nachfolgenden gehe ich auf einige ausgewählte Beispiele ein (siehe Nrn. 2.2.1 mit 2.2.4).

Im Berichtszeitraum musste ich keine Beanstandungen aufgrund technisch-organisatorischer Mängel aussprechen.

Von einer Vielzahl öffentlicher Stellen aus dem staatlichen und dem kommunalen Bereich wurde ich auch um Beratung zu technisch-organisatorischen Datenschutzfragen im Zusammenhang mit dort laufenden oder geplanten Projekten gebeten. Auf einige größere Projekte gehe ich im Nachfolgenden ein (siehe Nrn. 2.2.5 mit 2.2.7).

2.2.1 Geprüfte Einrichtungen

Folgende Stellen wurden von mir im Berichtszeitraum geprüft:

- DONAUISAR Klinikum Deggendorf
- Gesundheitsamt Aschaffenburg
- Gesundheitsamt Bayreuth
- Gesundheitsamt Eichstätt
- Gesundheitsamt Memmingen
- Gesundheitsamt Regensburg
- Heim für blinde Frauen München
- Justizvollzugsanstalt Aichach
- Justizvollzugsanstalt Landshut – Jugendarrestanstalt
- Justizvollzugsanstalt München – Frauenanstalt
- Justizvollzugsanstalt Straubing – Einrichtung für Sicherungsverwahrte
- Justizvollzugsanstalt Würzburg
- Kliniken des Landkreises Neumarkt i.d.Opf.
- Klinikum Augsburg
- Sozialgericht München – Postbehandlung
- Stadt Ornbau
- Technische Universität München mit Leibnitz Rechenzentrum
- Universitätsklinikum Würzburg
- Diverse Webauftritte staatlicher Stellen

Im Bereich der Kliniken lag der thematische Prüfungsschwerpunkt in der praktischen Umsetzung der im Jahr 2011 erstmalig veröffentlichten Orientierungshilfe Krankenhausinformationssysteme (siehe Nrn. 2.4.2, 7.2.8 und 25. Tätigkeitsbericht 2012 Nr. 7.2) mit besonderem Augenmerk auf Protokollierung, Protokollauswertung und Möglichkeiten der Datenschutzkontrolle von Zugriffen (zu den hierbei gewonnenen Erkenntnissen siehe Nr. 2.2.3).

Die Verwendung von Videoüberwachungsanlagen und die zugehörigen Regelungen waren Hauptgegenstand der Prüfungen in den Einrichtungen des Justizvollzugs (zu den hierbei gewonnenen Erkenntnissen siehe Nr. 5.4.4).

Bei den Gesundheitsämtern waren der Umgang mit den dortigen Datenverarbeitungssystemen und die Anbindung an die Datenverarbeitungssysteme des jeweiligen Landratsamts beziehungsweise der jeweiligen Kommune von besonderem Interesse (siehe Nr. 2.2.2).

Die Webauftritte von 31 staatlichen Stellen habe ich hinsichtlich ihrer SSL-Sicherheit geprüft, nachdem das Bundesamt für Sicherheit in der Informationstechnik (BSI) im Herbst 2013 darauf hingewiesen hatte, dass der für die TLS/SSL-Verschlüsselung häufig verwendete Kryptoalgorithmus RC4 als nicht mehr ausreichend sicher eingestuft werde. Mit einer Ausnahme, die ich noch weiter verfolgen werde, haben alle Stellen meine Aufforderung, nun auf den Einsatz von RC4 zu verzichten, aufgegriffen und verwenden andere Verfahren (siehe Nr. 2.2.4).

2.2.2 Prüfung Gesundheitsämter, technisch-organisatorische Anforderungen

Im 19. Tätigkeitsbericht 2000 unter Nr. 17.3.6 wurden einige Forderungen zur technischen Realisierung der Eingliederung der Gesundheitsämter in die informationstechnische Infrastruktur der Landratsämter aufgestellt. Im Berichtszeitraum habe ich einige Gesundheitsämter diesbezüglich besucht. Aufgrund der Prüfungsergebnisse werden die vorgenannten Forderungen im Folgenden aktualisiert und präzisiert. Zu den rechtlichen Aspekten der Prüfungen siehe Nr. 7.1.1.

Werden die Fachanwendungen des Gesundheitsamts auf der **informationstechnischen Infrastruktur** des Landratsamts gemeinsam mit anderen Anwendungen betrieben, muss sichergestellt sein, dass die technisch-organisatorischen Sicherheitsmaßnahmen für die gesamte Infrastruktur dem hohen Schutzbedarf der medizinischen Daten entsprechen. Beispielsweise sind gemäß den Vorgaben der Grundschutzkataloge des Bundesamts für Sicherheit in der Informationstechnik (BSI) eine besondere Risikoanalyse und über die Grundschutzkataloge hinausgehende Maßnahmen erforderlich. Zudem müssen besondere Schutzmaßnahmen für die Vertraulichkeit von Daten umgesetzt werden, die der ärztlichen Schweigepflicht unterliegen. Dies gilt insbesondere auch gegenüber anderen Nutzergruppen des Landratsamts und den Administratoren. Insgesamt muss somit für den Betrieb der Fachanwendungen ein Datenschutz- und Sicherheitskonzept erstellt werden, aus dem die Risiken sowie die ergriffenen Schutzmaßnahmen hervorgehen.

Für den **Betrieb der Fachanwendungen** auf den allgemeinen Servern des Landratsamts ist eine logische Trennung der Systeme des Landratsamts von denen des Gesundheitsamts als Basismaßnahme erforderlich. Dies kann beispielsweise über eigene virtuelle Server oder getrennte Datenbankinstanzen erfolgen. Wo dies technisch bereits möglich ist, sollten zudem die dort vorhandenen Verschlüsselungsfunktionen verwendet werden, um die Gefahr einer unbefugten Kenntnisnahme zu verringern. Wo dies technisch derzeit nicht möglich ist, sollte auf eine Einführung von Verschlüsselungsmöglichkeiten von Seiten des Herstellers gedrängt werden. Der Schlüssel/Masterkey muss hierbei so abgelegt werden, dass er sich in der Hoheit des Gesundheitsamts befindet, damit weder die Administratoren noch der Systemhersteller die Daten entschlüsseln können. Auf die früher geforderte Weisungsbefugnis des Leiters des Gesundheitsamts gegenüber den Administratoren kann unter diesen Umständen verzichtet werden. Gleiches gilt, wenn die Tätigkeit der Administratoren so eng begrenzt ist, dass kein Zugriff auf personenbezogene medizinische Daten möglich ist.

Wird die **Administration der Fachanwendung** des Gesundheitsamts per Fernwartung durch den Systemhersteller übernommen, muss sichergestellt sein, dass die Möglichkeit zur Einsichtnahme in medizinische Daten gering und zudem kontrollierbar ist. Deshalb müssen die für die Fernwartung üblichen Maßnahmen umgesetzt (siehe 18. Tätigkeitsbericht 1998 Nr. 3.3.4) und ein Vertrag zur Auftragsdatenverarbeitung abgeschlossen werden. Ein Versand von Datenbankauszügen oder ähnlichem an den externen Dienstleister sollte nicht stattfinden, da hier sensible personenbezogene Daten physikalisch an eine externe Stelle übertragen werden.

Bei der **Mitnutzung des Dokumentenmanagementsystems** (DMS) des Landratsamts gelten die gleichen Anforderungen wie bei der Nutzung einer gemeinsamen informationstechnischen Infrastruktur. Es sollte somit ebenfalls eine logische Trennung erfolgen, zum Beispiel über verschiedene Mandanten. Andernfalls muss über das Berechtigungskonzept sichergestellt sein, dass nur die berechtigten Mitarbeiter des Gesundheitsamts Zugriffsmöglichkeiten haben. Ebenfalls müssen die Einsichtsmöglichkeiten für Administratoren soweit wie möglich unterbunden werden, indem zum Beispiel eine verschlüsselte Speicherung der Dokumente erfolgt.

In allen Fällen müssen **Administratortätigkeiten**, bei denen eine Möglichkeit zum Zugriff auf personenbezogene medizinische Daten besteht, einer aussagekräftigen Protokollierung unterliegen. Sie muss in Stichproben regelmäßig ausgewertet werden. Hierzu sind ein entsprechendes technisches Konzept sowie eine Vereinbarung mit der Personalvertretung zu treffen.

In den Fachverfahren sollten die vorhandenen Möglichkeiten zur Konfiguration von **Löschfristen** genutzt werden, so dass die zu löschenden Daten vom System zeitgerecht und automatisch vorgeschlagen werden. Sie müssen dann entsprechend gelöscht werden. Auch für auf den Fileservern abgelegte personenbezogene Daten muss sichergestellt werden, dass die Löschfristen umgesetzt werden. Des Weiteren müssen auch für die Stammdaten Löschfristen festgelegt werden, zum Beispiel in jedem Fall nach dem Tod des Patienten oder ansonsten nach einem gewissen vordefinierten und angemessenen Zeitraum.

Bei langen Aufbewahrungsfristen sollte geprüft werden, ob im elektronischen Fachverfahren Möglichkeiten zur Auslagerung beziehungsweise **Sperrung von Datenbeständen** bestehen, wenn diese nicht mehr im täglichen Zugriff benötigt werden. Ein Zugriff beziehungsweise die Möglichkeit zur Entsperrung darf dann nur noch für einen beschränkten Personenkreis für den Fall bestehen, dass der Patient zu einem späteren Zeitpunkt noch einmal vorstellig wird. Dies entspräche dem Vorgehen bei Papierakten, die in der Regel nach einer gewissen Zeit in das Archiv verlagert werden, so dass sie sich nicht mehr im allgemeinen Zugriff befinden. Soweit die aktuell eingesetzten Systeme eine derartige Funktion nicht anbieten, sollte diese beim Hersteller eingefordert werden.

2.2.3 Prüfung der Umsetzung der OH KIS

Nach der Überarbeitung der OH KIS (siehe Nr. 7.2.8) habe ich in einigen Krankenhäusern vor Ort die praktische Umsetzung geprüft. In einigen Bereichen konnte ich Verbesserungen feststellen. Sie betreffen sowohl KIS-Hersteller, die angefangen haben, die Anforderungen der OH KIS in ihren Systemen umzusetzen, als auch Krankenhäuser, die die neuen Möglichkeiten im täglichen Betrieb nutzen.

Positiv hervorzuheben ist beispielsweise, dass in allen besuchten Häusern mittlerweile eine Protokollierung der lesenden Zugriffe erfolgt, so dass überprüft werden kann, wer in welche Daten zu welchem Zeitpunkt Einsicht genommen hat. Dies ist ein wichtiger Baustein hinsichtlich der Umsetzbarkeit einer effektiven Datenschutzkontrolle sowie auch der Auskunftsansprüche von Bürgern. Zunehmend Verbreitung findet auch die Vergabe personenbezogener Benutzerkennungen, die eine sinnvolle Auswertung der Protokollierung überhaupt erst ermöglicht.

KIS-Hersteller bieten zunehmend Möglichkeiten, Patientendaten nach der Entlassung des Patienten zu sperren, so dass sie nicht mehr im regulären Zugriff stehen. Auch dies ist eine der Kernforderungen der OH KIS, die in einigen Häusern auch bereits genutzt wird. KIS, die diese Möglichkeit noch nicht bieten, sollten entsprechend ergänzt werden.

Zunehmend Verbreitung findet auch die Begrenzung von Zugriffsrechten von Ärzten und Pflegepersonal auf die Fachbereiche, für die sie originär zuständig sind, verbunden mit einer Notfall-/Sonderzugriffsfunktion, über die bei Bedarf in Verbindung mit der Eingabe einer Begründung auch auf Daten anderer Patienten zugriffen werden kann. Dies ist eine deutliche Verbesserung gegenüber dem Zustand, dass z.B. alle Ärzte auf alle Patienten ohne weiteres zugreifen können. Sie sollte schnellstmöglich in KIS und Krankenhäusern, die diese Möglichkeit noch nicht nutzen, umgesetzt werden.

Leider noch nicht realisiert worden ist die technische Umsetzung des Widerspruchs eines Patienten in die Hinzuziehung von Daten aus Vorbehandlungen. Nach der Rechtslage kann der Patient zwar im Rahmen der medizinischen Aufnahme der Hinzuziehung der Vorbehandlungsdaten widersprechen. Sein Widerspruch kann jedoch in den meisten Fällen nicht im KIS vermerkt werden und führt daher auch nicht zu einem Entzug der Zugriffsrechte o.ä.

Auch sind viele KIS nicht in der Lage, Daten physikalisch zu löschen. Selbst wenn man von einer Aufbewahrungszeit von 30 Jahren in Krankenhäusern ausgeht, müssen nunmehr hierzu Lösungen in Angriff genommen werden, da manche KIS schon seit 15 Jahren in Betrieb sind.

2.2.4 TLS/SSL als (Un-)Sicherheitsfaktor

Im Berichtszeitraum kam es mehr als einmal vor, dass die Sicherheit von Verschlüsselungsalgorithmen (z.B. RC4) und Verschlüsselungsimplementierungen (OpenSSL), die etwa zur Absicherung von Internetauftritten („https“) verwendet werden, nicht mehr gegeben war. Ich verweise hierzu auf die entsprechenden Medienberichte im Herbst 2013.

RC4 ist ein Algorithmus zur Erzeugung einer Stromchiffre. Er berechnet aus einem Schlüssel eine beliebig lange Folge von (im Idealfall Zufalls-) Zahlen, die dann zur Verschlüsselung der eigentlichen Nachricht verwendet werden. Bereits 2001 wurden erste Möglichkeiten aufgezeigt, RC4 anzugreifen (Scott Fluhrer, Itsik Mantin und Adi Shamir: Weaknesses in the Key Scheduling Algorithm of RC4). In der technischen Richtlinie TR-02102-2 des Bundesamts für Sicherheit in der Informationstechnik (BSI) ist RC4 daher zuletzt als nicht empfehlenswerter Algorithmus eingestuft worden.

Da RC4 auch zur Absicherung einer Reihe von Internetauftritten von öffentlichen Stellen in Bayern eingesetzt wurde, habe ich diesbezüglich automatisierte Prüfungen von 31 mir bekannten verschlüsselten Webseiten vorgenommen und den betroffenen Stellen empfohlen, auf einen sichereren Algorithmus zu wechseln.

Wohl unter anderem weil in 2013 neue Angriffsmöglichkeiten in Bezug auf RC4 untersucht wurden (Pouyan Sepehrdad, Serge Vaudenay, Martin Vuagnoux: Discovery and Exploitation of New Biases in RC4) weist das BSI in der aktuellen Version 2014-01 der Richtlinie (vom Februar 2014) in Kapitel 3.3.2 darauf hin, dass RC4 „erhebliche Sicherheitsschwächen" enthält und nicht mehr eingesetzt werden darf.

Die überwiegende Mehrzahl der Stellen, die in der oben genannten Prüfung RC4 eingesetzt hatten, hatte zwischenzeitlich den Algorithmus gewechselt. Mit einer Ausnahme, die ich noch weiter verfolgen werde, haben alle anderen Stellen meine Aufforderung, nun ebenfalls auf den Einsatz von RC4 zu verzichten, aufgegriffen und verwenden andere Verfahren.

Während sich die Sicherheitsproblematik bei RC4 schon seit langem angekündigt hatte, hat die als „Heartbleed" benannte Sicherheitslücke zwar seit ungefähr zwei Jahren bestanden, ist aber erst 2014 öffentlich bekannt geworden.

Bei Heartbleed handelt es sich um eine fehlerhafte Programmierung einer Funktionalität in der OpenSSL Bibliothek, die dazu führt, dass bei betroffenen Systemen unberechtigt Speicherinhalte mit Zertifikatsdaten, Passwörtern oder anderen sicherheitsrelevanten Daten ausgelesen werden können. Alle mir bekannten verschlüsselten Webseiten von öffentlichen Stellen in Bayern setzen jedoch die von Heartbleed betroffenen OpenSSL-Versionen nicht ein, so dass hier kein konkreter Prüfungsanlass gegeben war.

Beide Sicherheitsproblematiken zeigen erneut, dass Sicherheit kein statischer Zustand ist, den man einmal erreicht hat und der dann für immer gegeben ist. Sicherheit ist vielmehr ein Prozess, der immer wieder Korrekturen in den eingesetzten Systemen erfordert. Deshalb ist es wichtig, im Falle neu bekannt werdender Sicherheitslücken zeitnah zu reagieren und bereits bei der Entwicklung von Verfahren darauf zu achten, dass im späteren Betrieb eine Aktualisierung der Sicherheitsmaßnahmen vorgesehen und möglich ist.

Auch wenn bei der Verschlüsselung mittels TLS/SSL von Internetauftritten („https") wie bei jeder anderen Sicherheitstechnik auch immer wieder Sicherheitslücken auftreten können, so stellt die sichere und vertrauenswürdige Bereitstellung von Internetangeboten eine wichtige Voraussetzung für den Datenschutz dar.

Selbst wenn die aktuelle Diskussion um das Abhören von Internetkommunikation außer Acht gelassen wird, so kann eine https-Verschlüsselung auch verhindern, dass die Nutzung des Internets durch Unbefugte überwacht wird. Ohne https kann beispielsweise unberechtigt und unbemerkt die Protokollierung am Internetübergang einer Behörde eingeschaltet und dann beispielsweise überwacht werden, welche Inhalte genau etwa sich der behördliche Datenschutzbeauftragte oder der Personalrat beispielsweise auf der Webseite des Bayerischen Landesbeauftragten für den Datenschutz betrachtet hat. Mit einer intakten https-Verschlüsselung sieht ein unberechtigter Dritter, der Zugriff auf die Verbindung hat, lediglich dass Inhalte abgerufen wurden, aber nicht, um welche konkreten Inhalte es sich dabei

handelt. Schon aus diesem Grund bietet eine Verschlüsselung mittels https für jeden Besucher einer Webseite einen erhöhten Sicherheitsgewinn, so dass ich dringend empfehle, generell und auch bei Webseiten ohne personenbezogene Daten die https-Verschlüsselung einzusetzen.

Sobald jedoch personenbezogene Daten – und dazu zählt grundsätzlich auch schon ein Kontaktformular – übertragen werden, ist eine TLS/SSL-Verschlüsselung unumgänglich.

Auch wenn auf meiner Webseite keine personenbezogenen Daten erhoben oder verarbeitet werden, ist seit März 2014 meine Homepage unter https://www.datenschutz-bayern.de verschlüsselt erreichbar.

Auch die Datenschutzbeauftragten des Bundes und der Länder haben in ihrer Entschließung „Gewährleistung der Menschenrechte bei der elektronischen Kommunikation" vom 27./28.03.2014 die sichere und vertrauenswürdige Bereitstellung von Internetangeboten gefordert:

Entschließung der 87. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 27./28.03.2014
Gewährleistung der Menschenrechte bei der elektronischen Kommunikation

Die Enthüllungen des Whistleblowers Edward Snowden haben ein Ausmaß an geheimdienstlicher Überwachung aufgezeigt, das viele zuvor nicht für möglich gehalten hatten. Die tendenziell unbegrenzte und kaum kontrollierte Überwachung der elektronischen Kommunikation aller verletzt das auch im digitalen Zeitalter weltweit anerkannte Recht auf Privatheit in täglich wiederkehrender millionenfacher Weise. Dies beeinträchtigt zugleich die Wahrnehmung anderer Menschenrechte wie der Meinungs- und Versammlungsfreiheit. Es ist eine gesamtgesellschaftliche Aufgabe, berechtigtes Vertrauen in die prinzipielle Unverletzlichkeit der Kommunikation wieder herzustellen.

Die Datenschutzbeauftragten des Bundes und der Länder haben daher schon im September 2013 gefordert, auf diese neue Qualität der Überwachung rechtlich und politisch zu reagieren. Darüber hinaus sind aber auch technische und organisatorische Schutzmaßnahmen erforderlich. Der Schutz der informationellen Selbstbestimmung der in Deutschland lebenden Menschen sowie der Vertraulichkeit und Integrität informationstechnischer Systeme muss wieder hergestellt und dauerhaft gesichert werden.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder fordert daher die Prüfung und Umsetzung folgender Maßnahmen:

1. *Sichere Verschlüsselung beim Transport und bei der Speicherung von Daten,*

2. *Bereitstellung einer einfach bedienbaren Verschlüsselungs-Infrastruktur,*

3. *Einsatz von Ende-zu-Ende-Verschlüsselung in Kombination mit Verfahren zur Verbindungsverschlüsselung,*

4. *Sichere und vertrauenswürdige Bereitstellung von Internetangeboten,*

5. *Weiterentwicklung innovativer Vorkehrungen zum Schutz von Verkehrsdaten,*

6. *Ausbau der Angebote und Förderung anonymer Kommunikation,*

7. *Angebot für eine Kommunikation über kontrollierte Routen,*

8. *Sichere Verschlüsselung der Mobilkommunikation und Einschränkung der Möglichkeiten der Geolokalisierung,*

9. *Beschränkung des Cloud Computing mit personenbezogenen Daten auf vertrauenswürdige Anbieter mit zertifizierter Informationssicherheit,*

10. *Förderung der Vertrauenswürdigkeit informationstechnischer Systeme durch Zertifizierung,*

11. *Sensibilisierung von Nutzerinnen und Nutzern moderner Technik,*

12. *Ausreichende Finanzierung von Maßnahmen der Informationssicherheit.*

Der Arbeitskreis „Technische und organisatorische Datenschutzfragen" der Datenschutzkonferenz hat einen Anforderungskatalog formuliert, der die hier genannten Maßnahmen konkretisiert (siehe Anlage zu dieser Entschließung).

Die Datenschutzbeauftragten des Bundes und der Länder fordern die Anbieter elektronischer Kommunikationsdienste auf, entsprechende Technologien und Dienste zur Verfügung zu stellen. Die Verwaltungen in Bund und Ländern, insbesondere die zuständigen Regulierungsbehörden, sind aufgefordert, auf die Durchsetzung der o.g. Maßnahmen zu dringen. Der Gesetzgeber ist aufgerufen, die zu ihrer Durchsetzung ggf. nötigen Änderungen und Präzisierungen an dem bestehenden Rechtsrahmen vorzunehmen.

Ich rate allen öffentlichen Stellen in Bayern zu prüfen, ob eine Verschlüsselung mittels TLS/SSL für ihre Internetauftritte möglich oder sogar notwendig ist und, soweit noch nicht bereits geschehen, ihre Internetauftritte entsprechend umzustellen.

2.2.5 De-Mail-Pilotierungstest

Am 3. Mai 2011 ist das De-Mail-Gesetz des Bundes und am 1. August 2013 ist das Gesetz zur Förderung der elektronischen Verwaltung (E-Government-Gesetz) sowie zur Änderung weiterer Vorschriften des Bundes in Kraft getreten. Damit sind auf Bundesebene unter anderem der Behördenzugang mittels De-Mail und der Schriftformersatz festgeschrieben worden. Soweit Landes- und Kommunalbehörden Bundesgesetze vollziehen, also z.B. im Bereich des Sozialrechts, gelten einige Regelungen seit 1. Juli 2014 auch für sie.

De-Mail ist ein Kommunikationsdienst, der eine sichere, vertrauliche und nachweisbare Kommunikation im Internet gewährleisten soll. De-Mail ist insoweit eine besondere Form der aus dem Internet bekannten E-Mail, bei der Sicherheit, Vertraulichkeit und Nachweisbarkeit bekanntermaßen nicht ohne weiteres gegeben sind. Bereitgestellt wird De-Mail auf einer elektronischen Plattform, die von kommerziellen Unternehmen (De-Mail-Diensteanbieter – DMDA) für ihre Kunden/

Benutzer gebührenpflichtig betrieben wird. Diese Unternehmen bedürfen für den Betrieb der De-Mail-Dienste einer staatlichen Akkreditierung.

Vor der erstmaligen Nutzung der De-Mail-Dienste muss sich der Benutzer dem DMDA gegenüber eindeutig identifizieren – nur so kann der Absender einer De-Mail zweifelsfrei ermittelt werden. Absende- und Eingangsbestätigungen, die mit einer qualifizierten elektronischen Signatur des Diensteanbieters versehen sind, bieten den sicheren Nachweis über Versand und Eingang einer De-Mail. De-Mails werden durch den Diensteanbieter von und zu seinen Kunden transportverschlüsselt (SSL/TLS), von und zu anderen Diensteanbietern transport- und inhaltsverschlüsselt (SSL/TLS und S/MIME) sowie bei Durchlauf über die Server der Diensteanbieter automatisch auf Schadsoftware geprüft.

Im Januar 2013 wurde ich von der damaligen Stabsstelle des IT-Beauftragten der Bayerischen Staatsregierung (jetzt Staatsministerium der Finanzen, für Landesentwicklung und Heimat) über einen geplanten Testbetrieb von De-Mail im Freistaat Bayern unterrichtet.

Der Test begann im April 2013 und war auf sechs Monate begrenzt. Am Test beteiligt waren vier Staats- beziehungsweise Kommunalbehörden aus unterschiedlichen Verwaltungsebenen, ein DMDA und das IT-Dienstleistungszentrum des Freistaats Bayern (ehemals Rechenzentrum Süd). Gegenstand des Tests waren u.a. die Überprüfung der gewählten De-Mail-Zugangsmöglichkeit, nämlich einem Gateway zwischen der De-Mail-Kommunikationsplattform/dem DMDA und dem Bayerischen Behördennetz/dem Rechenzentrum Süd, die Handhabbarkeit und die Integrierbarkeit von De-Mails in die internen Abläufe der Verwaltung.

Im Rahmen einer den Test vorbereitenden Besprechung zwischen Vertretern der Stabsstelle des IT-Beauftragten und meiner Geschäftsstelle im Februar 2013 habe ich auf mögliche datenschutzrechtliche und technische Risiken und Probleme hingewiesen. Dazu gehören beispielsweise die Sicherung der Datenverbindung zwischen dem Bayerischen Behördennetz und dem DMDA, eine zusätzlich erforderliche Ende-zu-Ende-Verschlüsselung für Daten mit hohem und sehr hohem Schutzbedarf sowie zugehöriger weiterer Mechanismen, die rechtliche Einordnung des zentralen Gateways, die rechtliche Problematik zur Beibehaltung der gesetzlich garantierten De-Mail-Sicherheitseigenschaften (z.B. bei Zwischenspeicherung auf dem Gateway und weiterer Übertragung der De-Mail als „normale“ E-Mail im Bayerischen Behördennetz).

Die Stabsstelle des IT-Beauftragten hat meine Anregungen aufgegriffen und soweit möglich umgesetzt. So hat sie für den Testbetrieb festgelegt, dass mit De-Mail nur Nachrichten mit normalem Schutzbedarf ausgetauscht werden sollten – also nur solche Nachrichten, die bislang auch mit der klassischen E-Mail ohne weitere Sicherheitsmaßnahmen ausgetauscht werden dürfen, da eine für den Versand von Daten mit hohem und sehr hohem Schutzbedarf erforderliche Ende-zu-Ende-Verschlüsselung nicht möglich war. Mit dem DMDA wurden vertraglich dessen Verpflichtungen zu Datenschutz und Datensicherheit festgelegt. Ergänzend wurde mit dem DMDA ein Vertrag zur Datenverarbeitung im Auftrag gemäß Art. 6 BayDSG geschlossen.

Im Oktober 2013 wurde ich von Vertretern der Stabsstelle des IT-Beauftragten über den Abschluss des Testbetriebs unterrichtet. Als ein Ergebnis des Tests musste festgestellt werden, dass zum damaligen Zeitpunkt eine produktionsreife

und datenschutzrechtlich einwandfreie Lösung auf Landesebene nicht verfügbar war.

Für den zukünftigen De-Mail-Einsatz in Bayern entwickelt nun das Staatsministerium der Finanzen, für Landesentwicklung und Heimat gemeinsam mit dem Bundesministerium des Innern eine gegenüber dem durchgeführten Test modifizierte Konzeption, die in der bestehenden technischen Infrastruktur Bayerns umgesetzt und letztendlich auch datenschutzrechtlich freigegeben werden kann. Spezifische rechtliche Aspekte sollen über ein zukünftiges bayerisches E-Government-Gesetz adressiert werden.

Ich werde das Vorhaben De-Mail in Bayern weiterhin begleiten und zum gegebenen Zeitpunkt darüber berichten.

2.2.6 Plattform für sichere Kommunikation in Bayern – BayMail

Am 23.04.2013 fand auf Einladung des Staatsministeriums des Innern, für Bau und Verkehr eine erste Besprechung zu einem dort geplanten Projekt mit dem Arbeitstitel Erreichbarkeitsplattform (EPF) statt. Wie auch im vorgenannten Projekt zu De-Mail ist ein Ziel dieses Projektes, die elektronischen Kommunikationsmöglichkeiten zwischen Bürgern/Unternehmen und Behörden insbesondere hinsichtlich der Gewährleistung von Datenschutz und Datensicherheit deutlich zu verbessern. Die Kommunikation soll hierbei – im Unterschied zum vorgenannten De-Mail-Projekt – aber über ein sogenanntes Portal und ohne die gesetzlich garantierten De-Mail-Sicherheitseigenschaften abgewickelt werden.

Kern des Projektes ist, dass die elektronische Kommunikation zwischen Bürger/Unternehmen zukünftig verschlüsselt über ein internetbasiertes, von staatlicher Seite zentral betriebenes Portal abgewickelt werden soll. Für den Bürger/das Unternehmen soll dabei weder technischer noch finanzieller Aufwand entstehen und im Wesentlichen lediglich eine gültige E-Mail-Adresse, eine Registrierung am zentralen Portal und ein SSL-fähiger Browser erforderlich sein. Für die an das Portal angeschlossenen Behörden soll lediglich die Einbindung in die bayerische Verwaltungs-PKI erforderlich sein.

Die Erreichbarkeitsplattform soll zunächst im Zusammenhang mit dem bestehenden EG-Dienstleistungsportal erstellt und zukünftig auch mit dem Portal „Verwaltungsservice Bayern“ verknüpft werden. Über die Erreichbarkeitsplattform sollen – jedenfalls zunächst – vor allem Dokumente, die keiner Schriftform bedürfen, zwischen Bürgern und Behörden in beiden Richtungen ausgetauscht werden können. Eine formelle Zustellung soll über die Erreichbarkeitsplattform nicht durchgeführt werden. Mittelfristig soll die Erreichbarkeitsplattform auch mit einer Lösung zur Integration der eID-Funktion des elektronischen Personalausweises und Aufenthaltstitel verknüpft werden, um so u.a. eine zuverlässigere Benutzeridentifikation zu erreichen.

Aufgrund meiner frühzeitigen Beteiligung durch das Staatsministerium des Innern, für Bau und Verkehr konnte ich von Anfang an datenschutzrechtliche Problemstellungen ansprechen und entsprechende Vorgaben in die Projektentwicklung einbringen sowie konkrete Umsetzungsanregungen geben.

Schwerpunkt im Bereich der rechtlichen Fragestellungen waren z.B. die Anwendbarkeit des allgemeinen Datenschutzrechts mit vorrangigen fachspezifischen Datenschutzvorschriften, Konstruktion der Auftragsdatenverarbeitungen der teilnehmenden Behörden, verantwortliche speichernde Stellen, datenschutzrechtliche Verantwortlichkeiten, datenschutzrechtliche Freigaben und Einwilligungserklärungen.

In technisch-organisatorischer Hinsicht lagen die Schwerpunkte z.B. beim Anmelde- und Registrierungsprozess sowie der Identitätsprüfung, bei Ver- und Entschlüsselungstechniken und Virenprüfungen, der zeitlich begrenzten Speicherung von Dokumenten und Nachrichten, den Möglichkeiten zur Ende-zu-Ende-Verschlüsselung.

Im Juli 2014 erteilte das Staatsministerium des Innern, für Bau und Verkehr im Einvernehmen mit der Staatskanzlei, den Staatsministerien, dem Obersten Rechnungshof und dem Landtagsamt aufgrund der bis dahin erreichten Ergebnisse die datenschutzrechtlichen Freigabe für das nunmehr so genannte Verfahren BayMail.

Da bis zu dieser Produktivsetzung im Sommer 2014 leider noch nicht alle von mir thematisierten Gesichtspunkte – wie insbesondere die grundsätzlich zu ermöglichende Ende-zu-Ende-Verschlüsselung und die bessere Sicherstellung der Identität der Kommunikationspartner – zur Zufriedenheit gelöst werden konnten, wurde die Freigabe zeitlich zunächst bis zum 31.07.2018 befristet. Vor einer eventuellen Verlängerung der datenschutzrechtlichen Freigabe und damit einer Fortsetzung des Betriebs muss dann eine umfassende Evaluation des Verfahrens erfolgen.

Ich werde den Fortgang des Projektes weiterhin beobachten und zum gegebenen Zeitpunkt darüber berichten.

2.2.7 Digitales Bildungsnetz (DBB)

Im Dezember 2011 wurde ich von dem damaligen IT-Beauftragten der Bayerischen Staatsregierung über das Forschungs- und Entwicklungsprojekt „Digitales Bildungsnetz Bayern“ in Kenntnis gesetzt und um entsprechende Beratung gebeten.

Mit dem DBB soll eine Infrastruktur geschaffen werden, die es Schulen ermöglicht, Synergieeffekte im Betrieb der an Schulen notwendigen Systeme zu nutzen und dabei den Belangen des Datenschutzes in besonderer Weise Rechnung tragen. Durch eine gemeinsame technische Basis und Standards sollen so eine höhere Qualität des IT-Betriebs für pädagogische Systeme, eine Vereinfachung der Administration und niedrigere Betriebskosten sowie hohe Datensicherheit und verbesserter Datenschutz an den Schulen erreicht werden.

Dazu wurden mit einem Projektpartner aus der Industrie an einer Reihe von Schulen verschiedene Ansätze erprobt, wie digitales Lernen in den Klassenzimmern unterstützt und ein bewusster Umgang mit der Informationstechnik vermittelt werden kann. Das Projekt umfasste z.B. die sichere Anbindung und Einbindung mobiler Geräte in das DBB, die Nutzung von Kommunikationsplattformen zwischen Schülern und Lehrern und die Bereitstellung von Unterrichtsmaterialien.

Im Rahmen meiner Beratungsleistung habe ich an diversen Besprechungen teilgenommen und mir auch an einigen Pilotschulen die jeweiligen konkreten Umsetzungen zeigen lassen. Dabei habe ich Anregungen zu Datensicherheit und Datenschutz gegeben; insbesondere betraf dies die Aspekte der Benutzerverwaltung, des Identitätsmanagements und eines durchgängigen Sicherheitsmanagements.

Das Projekt „Digitales Bildungsnetz Bayern“ wurde Ende 2014 abgeschlossen. Dabei sollte unter den Projektdurchführenden abgestimmt werden, welche Basisdienste aus dem Projekt weiter betrieben und künftig allen bayerischen Schulen angeboten werden. Das für das Projekt zuständige Staatsministerium der Finanzen, für Landesentwicklung und Heimat hat zugesagt, nach Vorliegen des weiteren Konzeptes wieder auf mich zuzugehen.

Ich werde den Fortgang des Projektes weiterhin beobachten und zum gegebenen Zeitpunkt darüber berichten.

2.3 Technisch-organisatorische Einzelthemen

2.3.1 Dienstliche Nutzung von Online-Terminplanern

In letzter Zeit erreichen mich vermehrt Anfragen von bayerischen Behörden und Kommunen bezüglich des datenschutzgerechten Einsatzes von Online-Terminplanern, wie zum Beispiel des Produkts „Doodle“. Davon rate ich generell ab, außer die Nutzung erfolgt zumindest pseudonymisiert und ohne Registrierung.

Bei Doodle handelt es sich um einen werbefinanzierten, intelligenten Zeitplaner, der sowohl für private Zwecke als auch von Unternehmen und Behörden genutzt werden kann. Doodle eignet sich sowohl für die Online-Terminplanung als auch für die Vereinbarung von Terminen, der Durchführung von Umfragen und für die Urlaubsplanung (sowohl mit internen als auch mit externen Teilnehmern).

Bei der Nutzung von Doodle fallen in der Regel auch personenbezogene Daten (z.B. E-Mail-Adressen und personalisierte Nachrichten) an. Diese Daten werden aber nicht beim Nutzer der Online-Software, sondern vom Anbieter Doodle AG gespeichert und weiterverarbeitet. Die Doodle AG hat zwar ihren Sitz in Zürich, trotzdem erfolgt die Speicherung der Daten zumindest teilweise außerhalb von Europa – in keinem Fall jedoch in einem Land der Europäischen Union. So setzen beide Versionen von Doodle (sowohl die kostenlose als auch die Premiumversion) Google Analytics für statistische Zwecke ein. Nutzer von Doodle müssen also davon ausgehen, dass Informationen über sie ungefragt in die USA gesandt werden. Zwar deklariert Doodle die Nutzung von Google Analytics in der Datenschutzerklärung und setzt die von Google angebotene IP-Kürzung ein, dadurch wird aber nicht die Übertragung der IP Adresse verhindert, sondern nur die Speicherung der vollständigen IP Adresse. In meinem 25. Tätigkeitsbericht 2012 unter Nr. 2.3.2 habe ich mich zu dieser Problematik mit Google Analytics ausführlich geäußert.

Überdies bietet Doodle keinen effektiven Zugriffsschutz. So muss für den Zugriff auf die Terminanfrage kein Passwort eingegeben, sondern lediglich ein Link aufgerufen werden. Dadurch kann nicht zuverlässig ausgeschlossen werden, dass die in den Terminabsprachen und Umfragen eingetragenen (personenbezogenen)

Daten von Dritten unbefugt eingesehen und geändert werden können, z.B. durch Weitergabe des für den Zugriff erforderlichen Links.

Als datenschutzfreundliche Alternative stehen die Produkte „dudle“ der Technischen Universität Dresden (https://dudle.inf.tu-dresden.de/?lang =de) und der „DFN-Terminplaner“ (https://terminplaner.dfn.de/schedule. php) zur Verfügung, bei denen zumindest keine Speicherung von IP-Adressen und keine Datenweitergabe ins nicht-europäische Ausland, aber eine automatische Löschung der Einträge nach einer vorher definierten Zeit erfolgt.

Sollte eine öffentliche Stelle in Bayern trotz meiner Bedenken die dienstliche Nutzung von Doodle zulassen, so sind die Bediensteten wenigstens darauf hinzuweisen, dass im Rahmen der Nutzung keine personenbezogenen Daten eingegeben werden dürfen. Überdies hat der Terminkoordinator sicherzustellen, dass jede An- und Umfrage nach Beendigung bei Doodle zuverlässig gelöscht wird.

2.3.2 Schutz vor Backdoor-Programmen

Backdoor-Programme ermöglichen es einem Dritten, unter Umgehung der normalen Zugriffssicherung Zugang zum Computer oder einer sonst geschützten Funktion eines Computerprogramms zu erlangen. Anders als Viren, Trojaner und Würmer öffnen sie ohne Wissen und Wollen des Berechtigten Hintertüren (Backdoor) in Datenverarbeitungssystemen für weitere Zugriffe darauf. Über diese Hintertüren können dann heimlich Verbindungen zu fremden Rechnern gestartet werden, um so Informationen (z.B. Passwörter, Zugangskennungen, Kreditkartennummern, Bankverbindungen) auf den befallenen Datenverarbeitungssystemen auszuspähen, diese Daten zu stehlen oder sie zu manipulieren. Häufig übernehmen Backdoor-Programme auch die komplette Kontrolle und Steuerung des befallenen Datenverarbeitungssystems, nachdem sie zuvor eventuelle Schutzmechanismen (z.B. Firewalls oder Datenverschlüsselung) deaktiviert oder ausgehebelt haben. Sehr oft werden Backdoor-Programme auch zur Erstellung eines Botnetzes eingesetzt, indem sie befallene Datenverarbeitungssysteme miteinander verbinden.

Verbreitungswege

Bei Backdoors kann es sich auch um bewusst eingebaute Sicherheitslücken in Hard- oder Software handeln, die zu den erwähnten Angriffen ausgenutzt werden können. Ich verweise hierzu auf entsprechende Berichte in den Medien vom Dezember 2013 zu solchen Maßnahmen an Routern und Firewalls bestimmter Hersteller im Auftrag amerikanischer Geheimdienste.

Gelegentlich werden Backdoors von Herstellern eines Datenverarbeitungssystems oder seiner Komponenten eingebaut, um ihnen selbst ohne die sonst übliche Authentifizierung remote einen Zugriff auf das Datenverarbeitungssystem zu ermöglichen, z.B. für Wartungszwecke.

Backdoor-Programme werden auch oft heimlich von Trojanern eingeschleppt, die dabei als Trägersysteme dienen. Sie können anschließend vollkommen selbständig von dem Trojaner auf dem befallenen Rechnersystem agieren. Selbst eine Entdeckung und Beseitigung des Trojaners bedeutet also nicht, dass damit auch das Backdoor-Programm entdeckt und beseitigt ist. Gelegentlich werden Mischformen von Trojanern und Backdoor-Programmen entdeckt. Dabei handelt es

sich um scheinbar nützliche Programme, die jedoch heimlich einen Fernzugriff auf das befallene Rechnersystem ermöglichen.

Des Weitern können Backdoors dazu dienen, heimlich weitere Schadenssoftware (wie Viren, Trojaner oder Würmer) einzuschleppen oder ein befallenes Rechnersystem für unbefugte Operationen wie beispielsweise Distributed Denial of Services-Angriffe (DDoS) zu benutzen.

Schutzmaßnahmen

Verantwortliche Stellen können Backdoor-Programme wohl am ehesten erkennen und abwehren, wenn sie Open Source Produkte einsetzen. Solche Produkte werden von einer Vielzahl von unabhängigen Entwicklern erarbeitet, was den heimlichen Einbau von technischen Schwachstellen erschwert. Über das Internet können kostenlose Backdoor Scanner heruntergeladen werden, die einen Router auf einen Befall von bekannten Backdoor-Programmen überprüfen.

Desweiteren sollten verantwortliche Stellen zur Vorbeugung vor Backdoor-Programmen folgende Maßnahmen ergreifen:

— Es sollten redundante, sich gegenseitig überwachende Systeme verschiedener Hersteller beschafft werden.

— Alle Verbindungen ins Internet sollten über eine Firewall laufen, um unerlaubte Verbindungsversuche entdecken und verhindern zu können.

— Dabei sollten standardmäßig alle Ports gesperrt und nur diejenigen freigegeben werden, die für gestattete Dienste und Verbindungen benötigt werden.

— Das Betriebssystem und die eingesetzte Software sollten zur Behebung von Schwachstellen regelmäßig automatisch aktualisiert werden.

— Es müssen auf allen Rechnersystemen geeignete Antiviren-Programme zur Erkennung von Backdoor-Programmen installiert und auf dem neuesten Stand gehalten werden.

— Die Rechnersysteme sollten regelmäßig mit Hilfe dieser Schutzprogramme hinsichtlich des Vorhandenseins von Backdoor-Programmen gescannt werden.

— Es sollten Netzwerk-Monitoring-Programme zur Überwachung aller Ports und Statusanzeigen verwendet werden, um so verdächtige Aktivitäten aufzuspüren.

— Das Herunterladen von Programmen im Internet sollte nur aus zuverlässigen Quellen erfolgen, z.B. erst nach erfolgreicher Zertifikatsprüfung.

2.3.3 Gewährleistung eines sicheren Datenträgeraustausches

Beim Datenträgeraustausch sind gemäß Art. 7 Abs. 2 Nr. 2 BayDSG Maßnahmen zu treffen, die geeignet sind zu gewährleisten, dass personenbezogene Daten

(während ihres Transports) auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können (Datenträgerkontrolle). Somit muss verhindert werden, dass Datenträger jeglicher Art beim Transport

— verloren gehen,
— entwendet werden,
— gelesen oder manipuliert werden oder
— bei einem falschen Empfänger landen.

Gefahren und Risiken

Die öffentliche Stelle hat solche Maßnahmen für einen sicheren Datenträgeraustausch im Rahmen einer Risikoanalyse zu ermitteln. Sie hat zu berücksichtigen, dass bei einem Datenträgeraustausch vor allem die Vertraulichkeit, die Integrität (Unversehrtheit) und die Authentizität (Zurechenbarkeit der Daten) solange nicht sichergestellt sind, wie Manipulationen, unbefugte Kenntnisnahmen und Zustellfehler beim jeweiligen Transport nicht ausgeschlossen werden können.

Bei der Risikoanalyse des Transportwegs sind die Art und Beschaffenheit des zu transportierenden Mediums und die darauf aufgezeichneten Informationen natürlich von besonderer Bedeutung. Sind die gespeicherten Daten verschlüsselt, sind sie für einen Außenstehenden meist ohne Nutzen. Beim Papier- und Filmdatenträger scheidet die Verschlüsselung als Sicherheitsmaßnahme jedoch regelmäßig aus.

Bei maschinenlesbaren Datenträgern ist zusätzlich das Problem der Restdaten aus der letztmaligen Nutzung des Datenträgers zu beachten. Solche Datenträger sind deshalb vor einer Wiederverwendung durch vollständiges Überschreiben mit bedeutungslosen Zeichen datenschutzgerecht zu löschen.

Natürlich besteht bei einem Datenträgeraustausch auch die Gefahr, dass die verwendete Soft- und Hardware bei Absender und Empfänger nicht kompatibel sind, d.h. die übertragenen Informationen beim Empfänger nicht gelesen werden können. Daher muss auch die Kompatibilität überprüft werden. Ist eine Kompatibilität nicht gegeben, müssen Konvertierungsroutinen erstellt werden.

Wahl der Transportart

In Abhängigkeit von der Sensitivität des zu transportierenden Datenmaterials sind die Versandart und der Transportweg festzulegen. Oft sind die Eigenschaften des Transportweges dem Absender und dem Empfänger weder bekannt noch durch sie beeinflussbar. Je mehr Personen mit dem Transport befasst sind und je unbeaufsichtigter der Transport stattfindet, desto größer sind die Risiken für die Vertraulichkeit und Integrität der auf den Datenträgern gespeicherten Informationen. Auch die Verfügbarkeit ist bei der Auswahl der Versand- bzw. Transportart zu berücksichtigen, damit eine rechtzeitige Zustellung soweit wie möglich garantiert werden kann.

Die gängigsten Versand- und Transportarten sind:

— Postdienste (z.B. Deutsche Post AG, Hermes, UPS, GLS)
— Deutsche Bahn AG
— beauftragte Kurierdienste

- eigene Kuriere
- persönliche Übergabe

Sicherheitsmaßnahmen

Zur Sicherstellung eines ordnungsgemäßen Datenträgertransports beziehungsweise zur Nachvollziehbarkeit des Transportweges können nachfolgende Sicherheitsmaßnahmen beitragen:

- Festlegung der Verantwortlichkeiten und Befugnisse zur Auftragserteilung sowie zur Entgegennahme
- Eindeutige Kennzeichnung von Datenträgern bezüglich Absender und Empfänger
- Ausreichende und klare Beschriftung der Transportbehälter
- Auswahl vertrauenswürdiger Firmen
- Schriftliche Auftragserteilung oder sonstige vertragliche Vereinbarungen
- Festlegung der Transportart und des Transportdienstes in Abhängigkeit von der Sensitivität der Daten
- Vorgabe des Transportweges und Benutzung eines bestimmten Transportmittels
- Verwendung verschließbarer (verplombter, versiegelter) und stabiler Transportbehälter
- Physikalisches Löschen der Datenträger vor deren erstmaliger oder auch deren Wiederverwendung
- Verifizieren der Datenträger vor dem Transport bezüglich der Rekonstruierbarkeit der Datenbestände
- Vorhaltung von Sicherungskopien der Datenträger
- Verschlüsselung der Daten
- Einsatz von Checksummen-Verfahren und der elektronischen Signatur zur Erkennung von Datenmanipulationen
- Dokumentation des Datenträgertransportes
- Verwendung von Begleitpapieren
- Führung eines Datenträgereingangs- bzw. -ausgangsbuchs
- Quittierung des Empfangs

Der gesamte vorgesehene Ablauf des Datenträgeraustausches sollte in einer Dienstanweisung geregelt werden, die den Beschäftigten mitgeteilt wird und die sie zu ihrer Einhaltung verpflichtet.

2.3.4 Teleradiologie mit externem Dienstleister – TKmed

Im Bereich der Teleradiologie gewinnt bundesweit die Plattform „TKmed“ an Bedeutung. Sie ist ein Beispiel für die in meinem 25. Tätigkeitsbericht 2012 unter Nr. 2.2.4 bereits allgemein vorgestellte Teleradiologie mit Beteiligung eines externen Dienstleisters.

TKmed bietet eine bundesweite Plattform für den Austausch von Radiologiedaten/Teleradiologie, die im Auftrag der AUC (Akademie für Unfallchirurgie) geschaffen worden ist. Alle Kliniken können an dieser Plattform teilnehmen; Systemanbieter im Auftrag der AUC ist die Chili GmbH. Sie stellt dabei die Softwarekomponenten selbst zur Verfügung. Für die technische Infrastruktur ist die Pegasus GmbH als Auftragnehmer beteiligt. Die Pegasus GmbH stellt die benötigten Server und Netzwerkkomponenten in ihren Rechenzentren zur Verfügung.

Um zu verhindern, dass die beteiligten Dienstleister während der Übermittlung unbefugt Kenntnis von den personenbezogenen medizinischen Daten erhalten können, werden die Daten im jeweiligen Krankenhaus auf den TKmed-Komponenten (Client, Router, Gateway) verschlüsselt und erst beim Empfänger wieder entschlüsselt. Sie werden maximal 14 Tage in der Infrastruktur zwischengespeichert.

Allerdings werden die Verschlüsselungsschlüssel nicht dauerhaft in den Krankenhäusern gespeichert, sondern im ESZ (externen Sicherheitszentrum). Das ESZ wird von einer weiteren Firma als Auftragnehmer der AUC betrieben.

Aus rechtlicher Sicht ist zur Konzeption von TKmed zunächst festzuhalten, dass Patienten über das eingesetzte Verfahren aufzuklären sind und ihre personenbezogenen Daten nur mit ihrer Einwilligung verarbeitet und genutzt werden dürfen (siehe dazu mein 21. Tätigkeitsbericht 2004 Nr. 5.1). Die Einwilligung kann auch zusammen mit dem Behandlungsvertrag abgegeben werden. Sie ist jedoch dann im äußeren Erscheinungsbild der Erklärung hervorzuheben.

Hintergrund ist, dass das Telekonsil aus juristischer Sicht grundsätzlich nicht anders zu behandeln ist, als die Beteiligung eines Konsilararztes ohne telemedizinische Unterstützung. Befindet sich der Konsilararzt in einem anderen Krankenhaus, so müssen die datenschutzrechtlichen Vorschriften zur Übermittlung von Patientendaten eingehalten werden. Nach Art. 27 Abs. 5 Satz 1 Bayerisches Krankenhausgesetz ist eine Übermittlung von Patientendaten an Dritte insbesondere zulässig im Rahmen des Behandlungsverhältnisses oder wenn die betroffenen Personen eingewilligt haben.

Im Hinblick auf meine im 25. Tätigkeitsbericht 2012 unter Nr. 2.2.4 aufgestellten technischen Anforderungen ist festzustellen, dass die Nutzung von TKmed in bayerischen öffentlichen Krankenhäusern folgende Zusatzmaßnahmen erfordert:

Im Konzept von TKmed erfolgt tatsächlich eine Ver- und Entschlüsselung im Krankenhaus. Allerdings liegen die Klartextdaten sowie die Verschlüsselungsschlüssel temporär auf den TKmed-Komponenten im Krankenhaus. Da auf diesen Komponenten ein Fernwartungszugriff erfolgt, muss sichergestellt sein, dass hierbei für die beteiligten Dienstleister kein Zugriff auf diese Daten oder die Schlüssel möglich ist. Es sind daher vertraglich entsprechende Maßnahmen festzulegen, wie z.B. grundsätzliche Deaktivierung des Fernwartungszugangs und Anschalten nur durch das Klinikum, Möglichkeit zur Entfernung der Schlüssel und der Daten bzw. zur Unterbrechung von Datenübertragungen vor der Fernwartung, geschützte

Ablage der Schlüssel auf den TK-Komponenten, so dass diese für die Fernwartung nicht zugänglich sind. Zudem sollte in der Einwilligungserklärung (siehe oben) auf die Fernwartung hingewiesen werden.

Die gewählte Verschlüsselung stellt sicher, dass die Chili GmbH beziehungsweise die Pegasus GmbH während des Transports und der Zwischenspeicherung der Daten in der externen Infrastruktur keine Einsicht nehmen können. Allerdings ist das ESZ kein Klinikum oder eine mit einem Traumanetzwerk verbundene Einrichtung, sondern ebenfalls eine externe Firma, mit der das Klinikum nicht in einer direkten vertraglichen Beziehung steht und somit auch keine Weisungsbefugnisse oder ähnliches ausüben kann. Es muss jedoch sichergestellt werden, dass das ESZ als eine Art Treuhänder für die Kliniken fungiert und nicht etwa die AUC oder Chili GmbH als Gesamtauftraggeber eine Herausgabe des Schlüssels fordern können. Für die Nutzung von TKmed durch bayerische Kliniken sind vertragliche Regelungen zur Weisungsbefugnis und zu den erlaubten Tätigkeiten zu treffen. Zudem muss ein Sicherheitskonzept zum Umgang mit den Schlüsseln im ESZ vorhanden sein, da diese von kritischer Bedeutung für die Sicherheit des Gesamtsystems und aller übermittelten medizinischen Daten sind.

2.3.5 Weitere Entwicklungen bei der Verwendung von mobilen Geräten im Krankenhaus, BYOD

Im Vergleich zu meinem letzten Tätigkeitsbericht hat es im Bereich der mobilen Geräte (Smartphones, TabletPCs) einige technische Weiterentwicklungen gegeben. So bieten beispielsweise mittlerweile einige Hersteller Virtualisierungssoftware für diese Geräte an, so dass ein virtueller Arbeitsplatz eingerichtet werden kann, bei dem sensible Daten nicht mehr auf dem Gerät abgelegt werden. Auch die Trennung der Anwendungen in einen privaten und in einen dienstlichen Bereich hat Fortschritte gemacht.

Dennoch sehe ich die Nutzung von privaten Geräten für den Zugriff auf personenbezogene medizinische Daten aus den im 25. Tätigkeitsbericht 2012 unter Nrn. 2.1.3, 2.1.4, 2.2.5 und 7.3 aufgeführten Gründen weiterhin kritisch.

Werden mobile Geräte aus dienstlichen Gründen benötigt, sollten sie vom Dienstherrn mit den entsprechenden Sicherheitsmaßnahmen zur Verfügung gestellt werden. Die Nutzung von Privatgeräten kann nur nach einer Einzelfallprüfung der Erforderlichkeit unter Beteiligung des behördlichen Datenschutzbeauftragten sowie bei angemessenen Sicherheitsmaßnahmen in Betracht kommen.

Besonders erfreulich ist, dass sich auch die Taskforce IT-Sicherheit der bayerischen Universitätsklinika dieser Ansicht angeschlossen und einen entsprechenden Leitfaden erarbeitet hat, da gerade in den Universitätsklinika der Wunsch nach einer Nutzung von Privatgeräten aufgrund der Forschungstätigkeiten der Ärzte groß ist. Mit dem Leitfaden konnte eine für alle Beteiligten zufriedenstellende und datenschutzgerechte Lösung gefunden werden.

2.3.6 Backup von Radiologiedaten bei externen Dienstleistern

Im Rahmen von Prüfungen und Befragungen diverser bayerischer Krankenhäuser hat sich herausgestellt, dass einige das Backup ihrer Radiologiedaten in einem Re-

chenzentrum eines kommerziellen Unternehmens im europäischen Ausland halten, wobei die Daten dort zum Prüfungs- bzw. Befragungszeitpunkt unverschlüsselt abgespeichert waren.

Ich sehe eine unverschlüsselte Speicherung personenbezogener medizinischer Daten bei einem externen Dienstleister als nicht vereinbar mit Art. 27 Abs. 4 Satz 6 Bayerisches Krankenhausgesetz (BayKrG) an. Das Backup hat so zu erfolgen, dass es entweder nur innerhalb des/eines Krankenhauses oder eine Verschlüsselung der Daten in der Form erfolgt, dass der externe Dienstleister keine Einsicht in die Daten nehmen kann.

Bezüglich der verschlüsselten Datenspeicherung bei externen Dienstleistern sind die bereits in meinen früheren Tätigkeitsberichten aufgeführten Punkte zu beachten (siehe 17. Tätigkeitsbericht 1996 Nr. 3.4.1.5, 18. Tätigkeitsbericht 1998 Nr. 3.3.5.2, 21. Tätigkeitsbericht 2004 Nr. 22.2.3.2, 22. Tätigkeitsbericht 2006 Nr. 13.2.5). Kern dabei ist, dass nur das Krankenhaus selbst die Möglichkeit zur Entschlüsselung der Daten haben darf und die Daten während der gesamten Speicherdauer auf Servern des Dienstleisters verschlüsselt bleiben müssen.

Die Verschlüsselung der Daten hat somit vor ihrer Übertragung an das externe Rechenzentrum innerhalb des Krankenhauses zu erfolgen und nicht erst im Rechenzentrum des Dienstleisters. Die Verschlüsselungsschlüssel müssen auf Komponenten im Krankenhaus gespeichert werden. Eine Zugriffsmöglichkeit auf die Schlüssel darf nur für Mitarbeiter des Krankenhauses, nicht jedoch für den externen Dienstleister (z.B. per Fernwartung) bestehen. Das Schlüsselmanagement (Schlüsselerzeugung, Schlüsselwechsel etc.) muss von Mitarbeitern des Krankenhauses durchgeführt werden; ein vom Dienstleister eventuell angebotener entsprechender Service scheidet aus.

Eine Entschlüsselung der Daten darf ebenfalls nur im Krankenhaus erfolgen – bei Beachtung der vorgenannten Aspekte kann sie auch nur dort vorgenommen werden.

2.3.7 Bayerisches Rotes Kreuz Telematik II

Das Bayerische Rote Kreuz (BRK) hat mich um Beratung bezüglich des Projekts Telematik II gebeten. Bei diesem Projekt wurde das BRK von den Krankenkassen beauftragt, eine Lösung für die elektronische Dokumentation im Rettungswesen für alle in Bayern tätigen Rettungsdienste bereitzustellen, bei der das bisherige papierene Rettungseinsatzprotokoll (DIVI-Protokoll) durch eine elektronische Dokumentation ersetzt wird. Die nunmehr vom BRK verwirklichte Konzeption berücksichtigt die von mir gemachten Änderungs- und Ergänzungsvorschläge.

Für die Umsetzung des Projekts wird die Systemlösung eines Herstellers aus dem Medizinbereich verwendet. Die Erfassung des Einsatzes durch die Rettungsdienstmitarbeiter erfolgt hierbei auf speziellen Pads, die für den Einsatz im Rettungswagen konzipiert sind. Es handelt sich dabei nicht um aus dem Konsumentenbereich bekannte TabletPCs, sondern um speziell für derartige Einsatzzwecke entwickelte Geräte. Die Einsatzprotokolle werden nach Abschluss der Dateneingabe an einen Server übermittelt, der im Rechenzentrum des BRK steht. Dieser wiederum übermittelt die Daten elektronisch an die aufnehmende Klinik und die ZAST (Zentrale Abrechnungsstelle für den Rettungsdienst Bayern GmbH). Zusätzlich besteht für die BRK-Rettungswachen, die die Einsätze durchführen, die

Möglichkeit, die Daten der eigenen Einsätze über eine Client-Anwendung einzusehen. Nach einer vorangegangenen gegenseitigen Authentifizierung der Komponenten erfolgen alle Datenübermittlungen und -abrufe verschlüsselt.

Eine elektronische Übergabe der Einsatzprotokolle von dem zentralen Server des BRK an das jeweilige Krankenhausinformationssystem ist derzeit noch nicht möglich, da die entsprechenden Schnittstellen noch nicht vorhanden sind. Die Übergabe der Daten erfolgt daher derzeit durch Ausdruck aus dem Pad, per Telefax oder durch eine spezielle Software, über die das Krankenhaus per virtuellem privaten Netzwerk (VPN) für einen bestimmten Zeitraum Einsicht in die auf dem Server gespeicherten Daten nehmen kann. Dabei besteht die Möglichkeit, den Bericht als PDF-Datei herunterzuladen. Dabei kann das Krankenhaus Einsicht nur in die Berichte derjenigen Patienten nehmen, die auch dorthin eingewiesen werden.

Die Zugriffsmöglichkeiten innerhalb der BRK-Rettungswachen richten sich nach den Aufgaben der einzelnen Mitarbeiter. Es ist ein Berechtigungskonzept umgesetzt, das sicherstellt, dass jeder nur die Daten einsehen kann, die für seine Aufgabenerfüllung erforderlich sind. Hinsichtlich der Einsichtsrechte ergeben sich durch die elektronische Dokumentation keine Änderungen im Vergleich zur Papierdokumentation.

Auf den Pads ist immer nur das aktuell in Bearbeitung befindliche Einsatzprotokoll gespeichert. Nach der erfolgreichen Übertragung auf den zentralen Server beim BRK wird es automatisch vom Pad gelöscht. Es wird eine PIN zur Sperrung der Geräte verwendet, so dass nur die Mitarbeiter des Rettungsdienstes auf das Gerät zugreifen können. Die PINs werden auf allen Geräten regelmäßig ausgewechselt um zu verhindern, dass beispielsweise Personen, die aus dem Rettungsdienst ausgeschieden sind, weiterhin auf Geräte zugreifen können. Zudem wurden Maßnahmen gegen ein beliebiges Ausprobieren von PINs ergriffen.

Am Projekt sind externe Firmen beteiligt – sowohl für die Wartung der Geräte als auch für den Betrieb des Rechenzentrums des BRK. In beiden Fällen wurden Verträge zur Auftragsdatenverarbeitung gemäß Art. 6 BayDSG abgeschlossen. Um den externen Dienstleistern einen unberechtigten Zugriff auf und eine unberechtigte Kenntnisnahme der personenbezogenen Daten zu verwehren, erfolgt in der Datenbank des Servers eine Trennung der Einsatzprotokolle in verschiedene Datenbank-Tabellen und eine Verschlüsselung der identifizierenden Daten der Patienten.

2.3.8 Brennen und Versand von CDs durch Krankenhäuser

Aufgrund der großen Datenmengen z.B. bei Radiologiedaten wie CT-Bildern geben Krankenhäuser zunehmend CDs an Patienten oder auch an nachbehandelnde Ärzte heraus, die die Daten des jeweiligen Patienten enthalten. Im Berichtszeitraum erreichten mich zwei voneinander unabhängige Eingaben von Bürgern, dass auf von ihren behandelnden Krankenhäusern erstellten CDs neben oder teilweise anstelle der eigenen Daten (auch) Daten anderer Patienten enthalten seien. Meine Nachprüfungen ergaben, dass ursächlich für diese Vorkommnisse organisatorische Schwächen verbunden mit einer schlechten technischen Unterstützung der Abläufe waren. Da ich hier auch von einer gewissen Dunkelziffer an ähnlich gelagerten Vorfällen ausgehe, weise ich auf Folgendes hin:

Die Weitergabe von CT-Bildern eines Patienten an einen anderen Patienten stellt sowohl einen Verstoß gegen Datenschutzbestimmungen als auch eine Durchbrechung der ärztlichen Schweigepflicht dar.

§ 10 Abs. 5 Berufsordnung für die Ärzte Bayerns
Aufzeichnungen auf elektronischen Datenträgern oder anderen Speichermedien bedürfen besonderer Sicherungs- und Schutzmaßnahmen, um deren Veränderung, Vernichtung oder unrechtmäßige Verwendung zu verhindern. Ärztinnen und Ärzte haben hierbei die Empfehlungen der Ärztekammer zu beachten.

Sie muss daher durch technische wie organisatorische Maßnahmen verhindert werden. Hierzu gehört insbesondere eine Dienstanweisung, in der festgelegt wird, durch wen und nach welcher Vorgehensweise Patientendaten auf CD gebrannt werden dürfen. Insbesondere muss darin der Punkt „Ausgangskontrolle" enthalten sein: Vor Herausgabe einer CD muss durch Einsichtnahme in die CD geprüft werden, ob die gespeicherten Bilder mit den Daten des Empfängers (gemäß Personalausweis oder schriftlicher Anforderung) übereinstimmen, d.h. tatsächlich nur diesem zuzuordnen sind. Erst dann darf die CD an den Empfänger herausgegeben oder versandt werden. Alle Mitarbeiter müssen regelmäßig in diese Vorgehensweisen und in die Handhabung der Brennstation unterwiesen werden.

Zudem muss nachprüfbar sein, wer zu welchem Zeitpunkt welche Patientendaten auf CD gebrannt hat. Vorzugsweise sollte dies durch eine Protokollierung in der Brennstation erfolgen. Ist dies technisch nicht möglich, sollten alle Brennvorgänge über einen Leistungsauftrag oder ähnlichem stattfinden, in dem die CDs und Patientennamen schriftlich von dem Mitarbeiter, der die CD gebrannt hat, festgehalten werden.

Für einen Postversand der CDs muss ein zuverlässiger Postdienstleister ausgewählt werden. Zudem muss ein Verfahren festgelegt werden, wie der Postdienstleister nicht zustellbare CDs zu behandeln hat. Auch der Versand muss nachvollziehbar dokumentiert werden, in dem zum Beispiel festgehalten wird, warum (Anforderung des Nachbehandlers oder des Patienten) und wann eine CD mit welchen Inhalten an welche Adresse versandt wurde.

2.3.9 Webportale in der Sozialverwaltung

Im Bereich der Sozialverwaltung werden zunehmend Webportale entwickelt, um dem Bürger die Beantragung von Leistungen zu erleichtern. So gibt es beispielweise Webportale des ZBFS (Zentrum Bayern Familie und Soziales) für die Online-Beantragung von Elterngeld und Betreuungsgeld oder die Zusendung von Elternbriefen. Auch zur Erfüllung von Dokumentationspflichten durch beteiligte Stellen in Verbundverfahren werden Webportale verwendet, auf die über das Internet zugegriffen wird.

Bei Webportalen im Sozialbereich ist besonders zu beachten, dass es sich bei den übermittelten Daten häufig um Sozialdaten handelt, die einem besonderen Schutzbedarf unterliegen. Dementsprechend müssen Webportale im Sozialbereich mit erhöhten technischen Sicherheitsmaßnahmen geschützt werden:

Häufig erfolgt der technische Betrieb des Webportals und des Servers zur Speicherung der eingegebenen Daten nicht durch die einsetzende Stelle selbst, son-

dern durch ein Rechenzentrum. Es kann sich dabei um eine Auftragsdatenverarbeitung handeln, für die ein entsprechender Vertrag abgeschlossen werden muss. Dabei hat die sozialdatenschutzrechtlich verantwortliche Stelle den Auftragnehmer mit besonderer Sorgfalt auszuwählen. Es empfiehlt sich daher die Nutzung öffentlich-rechtlicher Rechenzentren, wobei der vorhandene Mustervertrag zur Auftragsdatenverarbeitung um Klauseln für den besonderen Schutzbedarf der Sozialdaten ergänzt werden muss. Bei privaten Rechenzentren muss der Auftraggeber zunächst sorgfältig prüfen, ob sie die Anforderungen an den Schutzbedarf überhaupt erfüllen können.

Das Webportal muss mit dem Stand der Technik entsprechender Verschlüsselung arbeiten (siehe Nr. 2.2.4), zudem muss eine zuverlässige Identifizierung und Authentifizierung der Benutzer erfolgen. Vor der Inbetriebnahme muss eine Prüfung des Webportals auf Sicherheitslücken durch das Bayern-CERT erfolgen, des Weiteren ist die Freigabe des behördlichen Datenschutzbeauftragten der einsetzenden Stelle (Auftraggeber) erforderlich. Da neue Sicherheitslücken typischerweise in sehr kurzen zeitlichen Abständen bekannt werden, müssen auch während des Betriebs des Webportals regelmäßig Sicherheitsüberprüfungen erfolgen.

Um das Anwachsen der Datenbestände zu verhindern, muss bereits bei der Konzeption des Webportals und der dahinter stehenden Anwendungen geprüft werden, wann Daten gelöscht werden können und wie dies technisch umgesetzt wird.

2.3.10 Meldungen nach § 42a BDSG im Krankenhaus

Krankenhäuser in öffentlicher Trägerschaft sind eigenständige öffentliche Stellen im Sinne von Art. 4 Abs. 2 Satz 1 in Verbindung mit Art. 2 Abs. 1 und 2 BayDSG. Es gilt für sie somit grundsätzlich das Bayerische Datenschutzgesetz, soweit nicht gemäß Art. 2 Abs. 7 BayDSG bereichsspezifische Datenschutzvorschriften vorgehen oder das Bayerische Datenschutzgesetz selbst die Anwendbarkeit des Bundesdatenschutzgesetzes (BDSG) bestimmt.

Gemäß Art. 3 Abs. 1 BayDSG ist für öffentliche Stellen das BDSG mit Ausnahme des zweiten Abschnitts anwendbar, soweit sie im Sinne von Art. 3 Abs. 1 BDSG am Wettbewerb teilnehmen, indem sie etwa Leistungen erbringen, die auch von anderen (privaten) Stellen erbracht werden können. Dies trifft grundsätzlich für Leistungen im Bereich der Krankenversorgung zu.

Ich gehe daher für die bayerischen öffentlichen Krankenhäuser inklusive der Universitätsklinika in der Regel davon aus, dass für sie die Sonderregelung für Wettbewerbsunternehmen des Art. 3 Abs. 1 BayDSG zur Anwendung kommt.

Die Krankenhäuser müssen daher interne Regelungen treffen, dass von allen Bereichen datenschutzrelevante Vorfälle gemeldet werden. Die Mitarbeiter sind entsprechend zu sensibilisieren und interne Stellen zu benennen, an die die Vorfälle zu melden sind. Im Rahmen einer krankenhausinternen Prüfung des Vorfalls unter Beteiligung des behördlichen Datenschutzbeauftragten muss festgestellt werden, ob der Vorfall den Anforderungen des § 42a BDSG genügt und damit eine entsprechende Meldepflicht einhergeht.

Wird ein Fall einer unrechtmäßigen Kenntniserlangung von personenbezogenen medizinischen Daten festgestellt, sind die Maßnahmen nach § 42a BDSG zu ergreifen. Im Rahmen der Meldung des Vorfalls an meine Behörde sind insbesondere folgende Punkte detailliert darzulegen:

— Schilderung des Sachverhalts

— Umfang der bekanntgewordenen Daten, Sensibilität

— Anzahl der betroffenen Personen

— Darlegung zu den möglichen nachteiligen Folgen für die Betroffenen

— Ergriffene Maßnahmen, um eine Wiederholung des Datenschutzverstoßes in Zukunft zu verhindern

— Mitteilung, ob bzw. wann die Betroffenen gemäß § 42a BDSG informiert wurden

Seit der Einführung dieses Paragraphen zum 01.09.2009 habe ich von den Krankenhäusern Meldungen im einstelligen Bereich erhalten, was möglicherweise auch auf Unklarheiten bei der Frage zurückzuführen ist, ob § 42a BDSG überhaupt für bayerische öffentliche Krankenhäuser anwendbar ist.

Die gemeldeten Fälle betrafen zumeist den Verlust von Papierunterlagen bzw. Datenträgern oder Nachlässigkeiten bei der Aufbewahrung sensibler Informationen, so dass eine unbefugte Kenntnisnahme erfolgen konnte. Hierbei war immer nur ein kleiner Teil der Gesamtzahl der Patienten betroffen, die entsprechend vom Krankenhaus informiert wurden. Des Weiteren habe ich mir von allen Häusern darlegen lassen, welche Maßnahmen sie ergriffen haben, um eine Wiederholung zu verhindern.

2.3.11 Bestellung eines Hauptamtsleiters zum behördlichen Datenschutzbeauftragten

Insbesondere bei kleineren Gemeinden stellt sich immer wieder die Frage, wer zum behördlichen Datenschutzbeauftragten bestellt werden kann. Wie ich aufgrund von Prüfungen und Anfragen erfahren habe, wird zunehmend dazu übergegangen, den Hauptamtsleiter zum behördlichen Datenschutzbeauftragten zu ernennen. Dazu ist Folgendes festzustellen:

Der behördliche Datenschutzbeauftragte kann innerhalb einer Gemeinde auch mit anderen Aufgaben beauftragt werden, da er nur bei großen Kommunen mit Datenschutzaufgaben voll ausgelastet sein wird. Er sollte jedoch nicht mit solchen Aufgaben beschäftigt sein, die mit seiner Funktion als Datenschutzbeauftragter inhaltlich nicht vereinbar sind. Nicht vereinbar sind weitere Aufgaben, wenn sie die Gefahr von Interessenskonflikten begründen. So sollte der Datenschutzbeauftragte nicht in der DV-Abteilung tätig sein (insbesondere nicht als deren Leiter oder Systemverwalter), auch wenn dies gesetzlich nicht ausdrücklich verboten ist.

Auch nicht zu Datenschutzbeauftragten können die datenschutzrechtlich Verantwortlichen (z.B. der Bürgermeister) bestellt werden, da sie sich selbst nicht wirksam kontrollieren können. Außerdem bestimmt Art. 25 Abs. 3 BayDSG, dass der

Datenschutzbeauftragte der Leitung der öffentlichen Stelle oder deren ständigen Vertretung unmittelbar zu unterstellen ist; in Gemeinden kann er auch einem berufsmäßigen Gemeinderatsmitglied unterstellt werden.

Ein Hauptamtsleiter ist zwar bereits in dieser Funktion dem Bürgermeister direkt unterstellt, allerdings ist auch er in der Regel Interessenkonflikten ausgesetzt, da er gleichzeitig in verantwortlicher Position Aufgaben in anderen Bereichen wahrnimmt – so entscheidet er im Regelfall über die Einstellung, Einstufung, Beförderung oder Entlassung von Bediensteten zumindest mit. Überdies dürfte der Hauptamtsleiter häufig nicht über genügend Zeit auch noch zur Ausübung der Tätigkeit eines Datenschutzbeauftragten verfügen. Ich rate daher davon ab, einen Hauptamtsleiter zum behördlichen Datenschutzbeauftragten zu bestellen.

2.3.12 Einsatz privater Laptops bei der Auszählung von Kommunalwahlen

Aufgrund leerer Kassen sind vereinzelt Gemeinden auf die Idee gekommen, private Laptops (z.B. der Wahlhelfer) bei der Auszählung von Kommunalwahlen einzusetzen. Dies habe ich aus datenschutzrechtlichen Gründen abgelehnt.

So könnten die Wahlergebnisse – falls sie auf dem Laptop gespeichert werden – manuell oder automatisch mittels einer präparierten Software verfälscht werden. Selbst wenn die Datenspeicherung lediglich auf externen, kommunalen Datenträgern (z.B. USB-Sticks) und nicht auf den eingesetzten privaten Rechnern erfolgen sollte – was eine Minimalforderung bezüglich der Verwendung privater PCs wäre – könnten diese Datenträger unbefugt gelesen, kopiert, verändert oder entfernt werden. Es ist zumindest nicht auszuschließen, dass die personenbezogenen Daten von dem Datenträger auf die Festplatte des eingesetzten privaten Rechners kopiert, dort (automatisch mit Hilfe eines abgespeicherten Programms) verändert und die veränderten Daten wieder auf den externen Datenträger übertragen werden.

Unter Umständen ist auch ein Kopieren der Daten gar nicht erforderlich, um sie zu verfälschen. Dieses Verfälschen könnte auch – zumindest bei einer fehlenden oder fehlerhaften Zugangs- und Zugriffskontrolle (Art. 7 Abs. 2 Nrn. 1 und 5 BayDSG) – direkt auf dem externen Datenträger vorgenommen werden. Für einen IT-Kenner dürfte die Erstellung eines entsprechenden Schadensprogramms und Abspeicherung auf seinem zur Wahlauszählung eingesetzten Rechner kein großes Problem sein, wodurch die erwähnte Manipulation unbemerkt im Hintergrund ablaufen könnte. Auch ein Austausch des gesamten USB-Sticks gegen einen vorher entsprechend präparierten eigenen USB-Stick ist sicherlich nicht ganz auszuschließen. In diesem Falle hätte die Gemeinde nicht nur ein Datenschutzproblem, sondern auch ein strafrechtliches Problem (Wahlfälschung).

Auch eine verschlüsselte Datenspeicherung bietet unter diesen Gegebenheiten keinen ausreichenden Schutz, da die Daten zumindest gelöscht werden könnten.

Das gleiche Problem und die gleichen Gefahren bestehen bei einem Anmieten von Laptops. Zusätzlich müsste auch noch eine datenschutzgerechte Entsorgung etwaig gespeicherter Daten auf diesen Rechnern gewährleistet sein.

Ich rate daher dringend, auch bei den nächsten Kommunalwahlen ausschließlich auf dienstliche Geräte zurückzugreifen und auf den – wenn auch gut gemeinten – Einsatz privater Geräte zu verzichten.

2.4 Orientierungshilfen

2.4.1 Aktualisierungen

Im 25. Tätigkeitsbericht 2012 unter Nr. 7.2 habe ich über die im Jahr 2011 erstmalig veröffentlichte „Orientierungshilfe Krankenhausinformationssysteme“ der Datenschutzbeauftragten des Bundes und der Länder berichtet.

Die im Rahmen von gezielten Prüfungen gewonnenen wesentlichen Erkenntnisse zur praktischen Umsetzung dieser Orientierungshilfe stelle ich in Nr. 2.2.3 vor.

Diese Orientierungshilfe wurde nun redaktionell zu einer 2. Fassung überarbeitet (siehe Nr. 7.2.8) und ist ebenso wie die 1. Fassung auf meiner Homepage https://www.datenschutz-bayern.de unter „Veröffentlichungen“ – „Broschüren und Orientierungshilfen“ auffindbar.

2.4.2 Neuerscheinungen

Orientierungshilfe „Datenträgerentsorgung“

Im Februar 2014 habe ich die Orientierungshilfe „Datenträgerentsorgung“ erstellt. Damit habe ich dem Umstand Rechnung getragen, dass die im Jahre 1985 erschienene DIN 32757 und die DIN 44300 im Oktober 2012 beziehungsweise zum Jahreswechsel 2012/2013 durch die neue DIN 66399 abgelöst wurden.

Für nähere Informationen verweise ich auf meine Ausführungen (siehe Nr. 2.1.3) und auf die Orientierungshilfe selbst, die auf meiner Homepage https://www.datenschutz-bayern.de unter „Veröffentlichungen“ – „Broschüren und Orientierungshilfen“ abgerufen werden kann.

Orientierungshilfe „Fanpages bayerischer öffentlicher Stellen in sozialen Netzwerken zum Zweck der Öffentlichkeitsarbeit“

Im März 2013 habe ich die Orientierungshilfe „Fanpages bayerischer öffentlicher Stellen in sozialen Netzwerken zum Zweck der Öffentlichkeitsarbeit“ erstellt. Sie kann auf meiner Homepage https://www.datenschutz-bayern.de unter „Veröffentlichungen“ – „Broschüren und Orientierungshilfen“ abgerufen werden.

Anlass für diese Orientierungshilfe war unter anderem der Umstand, dass viele bayerische öffentliche Stellen bereits seit Längerem auf ihrer eigenen Webseite Informationen veröffentlichen, aber auch zunehmend nach weiteren, erfolgversprechenden Kommunikationswegen suchen. Einer dieser neuen Kommunikationswege scheinen die sogenannten sozialen Netzwerke wie z.B. Facebook und Google+ zu sein.

In meiner Orientierungshilfe gehe ich auf die grundsätzlichen rechtlichen Fragestellungen bei Fanpages sowie die noch nicht endgültig geklärten Aspekte ein, gebe eine Empfehlung für bayerische öffentliche Stellen hierzu ab und beschreibe mögliche Ausgestaltungsvarianten.

In diesem Zusammenhang verweise ich auch auf die Entschließung „Soziale Netzwerke brauchen Leitplanken – Datenschutzbeauftragte legen Orientierungshilfe

vor“ der 85. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 13./14.03.2013.

Entschließung der 85. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 13./14.03.2013
„Soziale Netzwerke brauchen Leitplanken – Datenschutzbeauftragte legen Orientierungshilfe vor“

„Angesichts der zunehmenden Bedeutung sozialer Netzwerke erinnert die Datenschutzkonferenz deren Betreiber an ihre Verpflichtung, die Einhaltung datenschutzrechtlicher Anforderungen sicherzustellen. Auch Unternehmen und öffentliche Stellen, die soziale Netzwerke nutzen, müssen diesen Anforderungen Rechnung tragen. Die Erfahrung der Aufsichtsbehörden zeigt, dass der Schutz der Privatsphäre von den Betreibern sozialer Netzwerke nicht immer hinreichend beachtet wird.

Häufig vertrauen die Nutzenden den Betreibern dieser Dienste sehr persönliche Informationen an. Auch die Vielfalt der Informationen, die innerhalb eines Netzwerkes aktiv eingestellt oder über die Nutzerinnen und Nutzer erhoben werden, ermöglicht einen tiefen Einblick in deren persönliche Lebensgestaltung.

Es zeichnet sich ab, dass die angekündigte Selbstregulierung für soziale Netzwerke – insbesondere auf Grund der mangelnden Bereitschaft einiger großer Netzwerk-Betreiber – den erforderlichen Datenschutzstandard nicht gewährleisten kann. Deshalb haben die Datenschutzbeauftragten des Bundes und der Länder die Orientierungshilfe "Soziale Netzwerke" erarbeitet. Sie soll die Betreiber sozialer Netzwerke und die die Netzwerke nutzenden öffentlichen und privaten Stellen bei der datenschutzgerechten Gestaltung und Nutzung der Angebote unterstützen. Die Konferenz weist darauf hin, dass der vorhandene Rechtsrahmen zur Gewährleistung eines angemessenen Datenschutzes bei sozialen Netzwerken weiterentwickelt werden muss, insbesondere in Bezug auf konkrete und präzise Vorgaben zu datenschutzfreundlichen Voreinstellungen, zum Minderjährigenschutz, zur Löschungsverpflichtung bei Dritten und zum Verhältnis von Meinungsfreiheit und Persönlichkeitsrecht. Ferner wird die Verantwortlichkeit für den Umgang mit Nutzungsdaten in Bezug auf Social Plug-Ins, Fanpages sowie für den Einsatz von Cookies von vielen Unternehmen und Behörden in Abrede gestellt. Der europäische und nationale Gesetzgeber bleiben aufgefordert, für die notwendige Klarheit zu sorgen und damit einen ausreichenden Datenschutzstandard zu sichern. Darauf weist die Konferenz der Datenschutzbeauftragten erneut nachdrücklich hin.“

Der Text der Entschließung und die zugehörige Orientierungshilfe stehen auch auf meiner Homepage https://www.datenschutz-bayern.de unter „Konferenzen“ – „Entschließung der 85. DSK vom 13. - 14. März 2013“ zum Abruf bereit.

Orientierungshilfe „Apps“

Die Datenschutzaufsichtsbehörden des Bundes und der Länder für den nichtöffentlichen Bereich haben im Juni 2014 eine „Orientierungshilfe Apps“ erstellt, in der sie die Rahmenbedingungen für eine gesetzeskonforme Entwicklung und Nutzung von Apps dargestellt haben. Die Orientierungshilfe ist unter anderem abrufbar beim Landesamt für Datenschutzaufsicht unter http://www.lda.bayern.de/lda/datenschutzaufsicht/lda_daten/Orientierungshilfe_Apps_2014.pdf.

Die Datenschutzaufsichtsbehörden tragen damit den niederschmetternden Ergebnissen ihrer datenschutzrechtlichen Prüfungen von Apps im nicht-öffentlichen Bereich Rechnung. Bei diesen Prüfungen mussten sie feststellen, dass sehr viele Apps insbesondere im Hinblick auf die Information der Nutzer, wann welche Daten zu welchem Zweck erhoben und genutzt werden, unzureichend waren.

Auch bayerische öffentliche Stellen treten zunehmend selbst als App-Entwickler oder als App-Anbieter auf. Ich empfehle daher allen bayerischen öffentlichen Stellen, bei entsprechendem Vorhaben auch die vorgenannte Orientierungshilfe mit heranzuziehen. Im Übrigen verweise ich auf meine Ausführungen unter Nr. 2.1.2.

3 Polizei

3.1 Allgemeines

3.1.1 PAG-Änderungen bezüglich der Möglichkeit der Bestandsdatenauskunft

Das Bundesverfassungsgericht hat mit Beschluss vom 24.01.2012 (Az.: 1 BvR 1299/05) einzelne Regelungen des Telekommunikationsgesetzes zur Speicherung und Verwendung von Telekommunikationsdaten für verfassungswidrig erklärt. Diese Vorschriften durften nur noch übergangsweise bis längstens 30.06.2013 angewendet werden. Aufgrund dieser Entscheidung bedurfte der Bestandsdatenabruf durch eine Sicherheitsbehörde einer qualifizierten, fachrechtlichen Ermächtigungsgrundlage. Sie musste hinreichend klar regeln, gegenüber welchen Behörden die Telekommunikationsunternehmen konkret zur Datenübermittlung verpflichtet sein sollen. Zudem bedurfte es nach Ablauf der Übergangsfrist auch für die Zuordnung von sog. dynamischen IP-Adressen (Telekommunikationsnummern, die bei der Nutzung des Internets zeitweilig vom Provider an die Kunden vergeben werden können) klarer landesgesetzlicher Abrufbefugnisse.

Um die vom Bundesverfassungsgericht geforderten spezifischen Erhebungsbefugnisse zu schaffen, ist das Polizeiaufgabengesetz (PAG) mit Einfügen der Abs. 4 bis 7 in Art. 34b PAG geändert worden. Neue Befugnisse für die Polizei sollten damit nicht geschaffen werden.

Im Rahmen des Gesetzgebungsverfahrens habe ich verfahrensrechtliche Sicherungen für den Schutz des Persönlichkeitsrechts eingefordert. Der Gesetzgeber hat einen Teil meiner Forderungen aufgegriffen. So hat er die Auskunft über sog. Zugriffssicherungscodes, wie Passwörter, PIN und PUK, unter den Richtervorbehalt gestellt. Aus datenschutzrechtlicher Sicht sind allerdings die Ausnahmen vom Erfordernis der richterlichen Anordnung sehr weitgehend ausgestaltet und daher äußerst kritisch zu beurteilen. Positiv zu bewerten ist der Umstand, dass das Polizeiaufgabengesetz nunmehr eine Benachrichtigungspflicht sowohl für Auskünfte über Zugriffssicherungscodes als auch über dynamische IP-Adressen vorsieht.

Art. 34b PAG Mitwirkungspflichten der Diensteanbieter

...

(4) [1]Die Polizei kann Diensteanbieter verpflichten, Auskunft über die nach §§ 95 und 111 TKG erhobenen Bestandsdaten zu erteilen, soweit dies zur Abwehr einer Gefahr für die öffentliche Sicherheit oder Ordnung erforderlich ist (§ 113 Abs. 1 Satz 1 TKG). [2]Bezieht sich das Auskunftsverlangen nach Satz 1 auf Daten, mittels derer der Zugriff auf Endgeräte oder auf Speichereinrichtungen, die in diesen Endgeräten oder hiervon räumlich getrennt eingesetzt werden, geschützt wird (§ 113 Abs. 1 Satz 2 TKG), darf die Auskunft nur verlangt werden, wenn die gesetzlichen Voraussetzungen für die konkret beabsichtigte Nutzung der Daten im Zeitpunkt des Ersuchens vorliegen.

(5) Die Auskunft nach Abs. 4 darf auch anhand einer zu einem bestimmten Zeitpunkt zugewiesenen Internetprotokoll-Adresse verlangt werden (§ 113 Abs. 1 Satz 3 TKG).

(6) Die nach Abs. 2, 4 und 5 verlangten Daten sind der Polizei unverzüglich zu übermitteln.
(7) Für die Entschädigung der Diensteanbieter ist § 23 des Justizvergütungs- und -entschädigungsgesetzes entsprechend anzuwenden, soweit nicht eine Entschädigung nach dem Telekommunikationsgesetz zu gewähren ist.

3.1.2 PAG-Änderung bezüglich Wohnraumüberwachung und Online-Durchsuchung

Mit Gesetz zur Änderung des Polizeiaufgabengesetzes (PAG) und des Bayerischen Verfassungsschutzgesetzes vom 24. Juni 2013, in Kraft seit 1. Juli 2013, wurden in Art. 34 PAG (Aufzeichnungen im Rahmen einer Wohnraumüberwachung, sog. „Großer Lauschangriff"), in Art. 34c PAG (Verwendungsverbot bei Überwachung und Aufzeichnung der Telekommunikation und bei Bestandsdatenauskünften) und in Art. 34d PAG (verdeckter Zugriff auf informationstechnische Systeme, sog. „Online-Durchsuchung") Abgeordnete und Journalisten dem Kreis der besonders geschützten Berufsgeheimnisträger hinzugefügt. Die vorgenommene Erweiterung des Schutzbereiches begrüße ich. Jedoch bleibt der Gesetzgeber damit immer noch hinter dem von mir bereits in meinem 24. Tätigkeitsbericht 2010 gemachten Vorschlag zurück. Ich hatte empfohlen, alle im Strafprozessrecht geschützten Berufsgeheimnisträger auch im Bayerischen Polizeirecht zu schützen und damit in Zukunft nicht mehr zwischen den verschiedenen geschützten Berufsgruppen zu unterscheiden (siehe 24. Tätigkeitsbericht 2010 Nr. 3.1.1). Nach wie vor kann ich keinen sachlichen Grund für die konkret getroffene Differenzierung zwischen „mehr" oder „weniger" geschützten Berufsgeheimnisträgern erkennen.

3.1.3 Richtlinie zur Vorratsdatenspeicherung ungültig

Bereits in meinen beiden letzten Tätigkeitsberichten hatte ich ausführlich über die Ausgestaltung der Vorratsdatenspeicherung und den Stand der gerichtlichen Verfahren hinsichtlich der Richtlinie berichtet (siehe 24. Tätigkeitsbericht 2010 Nr. 3.3 und 25. Tätigkeitsbericht 2012 Nr. 3.1). Am 08.04.2014 hat der Europäische Gerichtshof nunmehr die Richtlinie 2006/24/EG über die Vorratsdatenspeicherung von Telekommunikationsverkehrsdaten für ungültig erklärt (siehe Nr. 1.2.2).

3.1.4 Automatisierte Kennzeichenerfassung

Zuletzt habe ich in meinem 23. Tätigkeitsbericht 2008 über die Regelung zur automatisierten Kennzeichenerfassung (AKE) in Art. 33 Abs. 2 Sätze 2 bis 5 des Bayerischen Polizeiaufgabengesetzes (PAG) berichtet (siehe 23. Tätigkeitsbericht 2008 Nr. 4.1.1).

Art 33 PAG Besondere Mittel der Datenerhebung
(2) [1]Die längerfristige Observation oder der verdeckte Einsatz technischer Mittel zur Anfertigung von Bildaufnahmen oder -aufzeichnungen ist zulässig, wenn die Erfüllung einer polizeilichen Aufgabe auf andere Weise gefährdet oder erheblich erschwert würde. [2]Darüber hinaus kann die Polizei unbeschadet des Art. 30 Abs. 3 Satz 2 durch den verdeckten Einsatz automatisierter Kennzeichenerkennungssysteme bei Vorliegen entsprechender Lageerkenntnisse in den Fällen des Art. 13 Abs. 1 Nrn. 1 bis 5 Kennzeichen von Kraftfahrzeugen sowie Ort, Datum, Uhrzeit

und Fahrtrichtung erfassen. [3]Zulässig ist der Abgleich der Kennzeichen mit polizeilichen Fahndungsbeständen, die erstellt wurden

1. *über Kraftfahrzeuge oder Kennzeichen, die durch Straftaten oder sonst abhandengekommen sind,*
2. *über Personen, die ausgeschrieben sind*
   a) *zur polizeilichen Beobachtung, gezielten Kontrolle oder verdeckten Registrierung,*
   b) *aus Gründen der Strafverfolgung, Strafvollstreckung, Auslieferung oder Überstellung,*
   c) *zum Zweck der Durchführung ausländerrechtlicher Maßnahmen,*
   d) *wegen gegen sie veranlasster polizeilicher Maßnahmen der Gefahrenabwehr.*

[4]Ein Abgleich mit polizeilichen Dateien, die zur Abwehr von im Einzelfall oder im Hinblick auf bestimmte Ereignisse allgemein bestehenden Gefahren errichtet wurden, ist nur zulässig, wenn dies zur Abwehr einer solchen Gefahr erforderlich ist und diese Gefahr Anlass für die Kennzeichenerfassung war. [5]Die Kennzeichenerfassung darf nicht flächendeckend eingesetzt werden.

Mittlerweile hat sich der Bayerische Verwaltungsgerichtshof mit der automatisierten Kennzeichenerfassung befasst. Er hat in seinem Urteil vom 17.12.2012 (Az.: 10 BV 09.2641) entschieden, dass die Vorschriften, die eine automatisierte Kennzeichenerfassung und den Abgleich mit polizeilichen Dateien ermöglichen, eine noch verfassungsgemäße Beschränkung des Grundrechts auf informationelle Selbstbestimmung darstellen.

Geklagt hatte ein Pendler, der regelmäßig eine bestimmte Autobahnstrecke befährt und mit seiner Klage erreichen wollte, dass der Freistaat Bayern nicht mehr automatisiert die Kennzeichen der auf ihn zugelassenen Fahrzeuge erfassen und mit polizeilichen Daten abgleichen darf.

Nach Auffassung des Bayerischen Verwaltungsgerichtshofs stellt allein die Erfassung der Autokennzeichen und ihr Abgleich mit den polizeilichen Fahndungsdaten noch keinen Eingriff in das Grundrecht auf informationelle Selbstbestimmung dar, soweit die Fahrzeugdaten danach sofort und folgenlos gelöscht werden (sog. „Nichttreffer"). Jedoch sei ein Eingriff in das Grundrecht auf informationelle Selbstbestimmung dann zu bejahen, wenn ein erfasstes Kennzeichen in einem Speicher festgehalten wird und gegebenenfalls Grundlage weiterer Maßnahmen werden kann. Dies sei nicht erst beim echten Treffer, also der tatsächlichen Übereinstimmung der abgeglichenen Kennzeichen, sondern bereits beim sogenannten „unechten Treffer" der Fall. Solche „unechten Treffer" können zum Beispiel durch eine falsche Ablesung des Kennzeichens wegen schlechter Bildqualität auftreten. Bei diesen „unechten Treffern" liege der Grundrechtseingriff allerdings wohl nicht bereits in einer Speicherung des Kennzeichens, sondern darin, dass eine Person, nämlich der bearbeitende Polizeibeamte, das Kennzeichen ablesen könne. Die gesetzlichen Regelungen der automatisierten Kennzeichenerfassung stellen aber nach Ansicht des Bayerischen Verwaltungsgerichtshofs eine verfassungsgemäße Beschränkung des Grundrechts auf informationelle Selbstbestimmung dar. Insbesondere werde der Grundsatz der Verhältnismäßigkeit noch gewahrt. Der Gesetzgeber habe schwerwiegende Eingriffe, die nur zu besonders gewichtigen Zwecken erfolgen dürften, von vornherein ausgeschlossen oder eng begrenzt. So sei es nur in besonderen Fällen zulässig, Einzelerfassungen zu einem Bewegungsbild zu verbinden. Der flächendeckende Einsatz der Kennzeichenerfassung sei grundsätzlich nicht erlaubt. Da die Kennzeichenerfassung und der Datenabgleich nicht anlasslos und darüber hinaus nur entsprechend den jeweiligen

Lageerkenntnissen erfolgten, werde auch nicht eine unbegrenzte Kontrolle aller Verkehrsteilnehmer ausgeübt. Auch liege ein Vollzugsdefizit derzeit nicht vor.

In der mündlichen Verhandlung am 10.12.2012 wurde ich als sachkundige Person befragt. Hierbei habe ich einerseits bestätigt, dass die mir auf meine Anforderung hin von der Polizei vorgelegten Lageerkenntnisse entsprechende Gefahrensituationen schlüssig bzw. nachvollziehbar umschreiben. Andererseits habe ich darauf hingewiesen, dass ich es rechtlich für problematisch halte, dass die bayerische Regelung (Art. 33 Abs. 2 Satz 2 PAG) vom Grundsatz der heimlichen Datenerfassung ausgeht. Meines Erachtens wäre es aus verfassungsrechtlicher Sicht geboten, zunächst eine offene Datenerhebung vorzusehen und nur bei entsprechender Erforderlichkeit verdeckte Maßnahmen zuzulassen.

Dieser Argumentation ist der Bayerische Verwaltungsgerichtshof nicht gefolgt.

Er führt diesbezüglich in seinem Urteil u.a. aus, dass sich zwar durchaus subjektiv das Gefühl des Überwachtwerdens einstellen könne, da die Erfassung für den Bürger nicht erkennbar, also heimlich, erfolge. Andererseits hielten sich die Einschüchterungseffekte dann in Grenzen, wenn die Erfassung weder flächendeckend noch routinemäßig erfolge und auch nicht dem Zweck der Erstellung von Bewegungsprofilen diene, sondern anlassbezogen nach den jeweiligen Lageerkenntnissen durchgeführt werde.

Aufgrund der grundsätzlichen Bedeutung wurde vom Bayerischen Verwaltungsgerichtshof das Rechtsmittel der Revision zugelassen. Das Bundesverwaltungsgericht (Az.: 6 C 7.13) hat die Revision am 22.10.2014 zurückgewiesen. Nach Ansicht des Bundesverwaltungsgerichts soll sogar im Fall des „unechten Treffers“ kein Eingriff in das Recht auf informationelle Selbstbestimmung vorliegen. Ein Eingriff wird nur für den „echten Treffer“ bejaht. Ein solcher drohe dem Kläger jedoch nicht mit hinreichender Wahrscheinlichkeit. Derzeit ist beim Bundesverfassungsgericht noch eine Verfassungsbeschwerde anhängig (Az.: 1 BvR 1782/09). Auch in diesem Verfahren habe ich eine Stellungnahme abgegeben und auf die Problematik der Verdecktheit hingewiesen. Zum Zeitpunkt des Redaktionsschlusses war dieses Verfahren noch nicht abgeschlossen.

3.1.5 Polizeilicher Informations- und Analyseverbund (PIAV)

Mit dem Polizeilichen Informations- und Analyseverbund (PIAV) planen die Polizeien der Länder und des Bundes ein neues Dateisystem, um einen bundesweiten Zugriff auf Personen-, Fall- und Sachdaten aus der Kriminalitätsbekämpfung zu erhalten. Im Zuge der Umstellung sollen teilweise alte Systeme wie INPOL-Fall Dateien oder auch der bisherige Kriminalpolizeiliche Meldedienst (KPMD) schrittweise ersetzt und mit neuer Analysetechnik ausgestattet werden. Die Teilnehmer des Informationsverbundes liefern dann die im System ausgetauschten Daten eigenverantwortlich und automatisiert an. Demzufolge wird auch die datenschutzrechtliche Verantwortung für die Speicherungen größtenteils auf die Landespolizei entfallen. Eine wesentliche Koordinierungsfunktion in Bayern wird hierbei das Bayerische Landeskriminalamt übernehmen.

Da bei solch umfangreichen und kostenaufwendigen Entwicklungen die Konkretisierung der datenschutzrechtlichen Anforderungen mit dem Fortgang der Planung einhergehen muss, habe ich mich sowohl auf Landes- als auch auf Bundesebene frühzeitig mit den zuständigen Gremien beraten. Auch wenn zahlreiche

maßgebliche Entscheidungen zum Dateibetrieb noch ausstehen, hat mir das Bayerische Landeskriminalamt bereits signalisiert, die von mir vorgetragenen Bedenken aufzugreifen und entsprechende Regelungen für die bayerischen Quelldateien des Systems zu treffen. So wird das Landeskriminalamt eine konkret formulierte Eingrenzung der zulässigen Speicherungen auf Fälle von Straftaten von erheblicher Bedeutung und anderer Straftaten von länderübergreifender oder internationaler Bedeutung vornehmen. Spätestens bis zum Betrieb der ersten Teildateien müssen allerdings noch weitere datenschutzrechtlich erhebliche Entscheidungen folgen.

3.2 Polizeiliche Tätigkeiten im Zusammenhang mit Versammlungen

3.2.1 Datei „Veranstaltungs-/Einsatzkalender“

Schon anlässlich früherer Prüfungen (siehe 24. Tätigkeitsbericht 2010 Nr. 3.4.1) musste ich bei Datenschutzkontrollen feststellen, dass verschiedentlich – auch bei störungsfreiem Versammlungsverlauf – die personenbezogenen Daten von Versammlungsanmeldern oder Versammlungsleitern im Vorgangsverwaltungs- und Dokumentationsverfahren (Integrationsverfahren – IGVP) der Polizei erfasst und über mehrere Jahre gespeichert wurden. Ich hatte die betreffenden Polizeipräsidien umgehend aufgefordert, diese Daten zu löschen und dafür Sorge zu tragen, dass die hier zutreffenden verbindlichen Speicherungsverbote auch eingehalten werden.

Wie mir das Staatsministerium des Innern, für Bau und Verkehr im vergangenen Jahr dann mitteilte, hat es einer neuen Datei zugestimmt, in der u.a. solche personenbezogenen Daten von Versammlungsanmeldern oder Versammlungsleitern gespeichert werden. Der Zugriff auf diese Daten sollte nahezu allen Mitarbeitern der Bayerischen Polizeipräsidien gewährt werden. Trotz allem Verständnis für das polizeiliche Informationsbedürfnis bei Einsatzvorbereitungen zur Gewährleistung der Sicherheit von Versammlungen habe ich deutlich meine datenschutzrechtlichen Bedenken an einer Datei in diesem Umfang zum Ausdruck gebracht. Eine Speicherung sensibler Daten, wie z.B. von Versammlungsanmeldern oder Versammlungsleitern und deren recherchierbare Vorhaltung bei der Polizei darf nur unter sehr engen Rahmenkriterien und nicht ohne eine einzelfallbezogene Prüfung der Erforderlichkeit erfolgen. Die zunächst vorgesehene Dateifassung war zudem geeignet, das durch polizeiliche Richtlinien vorgegebene Speicherungsverbot für solche Daten im Integrationsverfahren zu umgehen und diese sensiblen Daten weiten Teilen der Bayerischen Polizei über Jahre hinaus zur Verfügung zu stellen.

Derzeit stehe ich mit der Polizei in konstruktiven Gesprächen, um eine praxistaugliche Lösung für eine solche Veranstaltungsdatei zu finden. Dabei sollen sowohl das Persönlichkeitsrecht Einzelner, als auch das polizeiliche Informationsbedürfnis angemessen berücksichtigt werden. In einem ersten Schritt hat die Polizei nunmehr bereits den internen Kreis der Zugriffsberechtigten auf sensible personenbezogene Daten in ganz erheblichem Maße eingeschränkt.

3.2.2 Filmen wegen einer vermeintlichen erheblichen Störung einer Versammlung

Bei einer Versammlung hatten kurz nach Beginn der Kundgebung zwei sich aus dem Fenster eines Wohngebäudes lehnende Personen Lautsprecher in Position gebracht und Musik abgespielt. Sie wurden dabei von eingesetzten Polizeikräften gefilmt. Die Kundgebung war zu diesem Zeitpunkt vom betreffenden Wohngebäude noch deutlich entfernt. Ein Verfahren wegen Störung der Versammlung wurde von der zuständigen Staatsanwaltschaft nicht eingeleitet.

Die eingesetzten Polizeibeamten beurteilten das Abspielen der Musik als mögliche erhebliche Störung der Versammlung, so dass sich aus ihrer Sicht der Anfangsverdacht einer Straftat ergeben habe und damit ein offenes Filmen gemäß Strafprozessrecht möglich gewesen sei.

Nach Sichtung der Filmsequenzen und der mir vorliegenden Unterlagen war für mich diese Annahme nicht nachvollziehbar. Eine erhebliche Störung der Versammlung lag aus meiner Sicht nicht vor. Die Lautstärke, die von der sich nähernden Versammlung erzeugt wurde, war so groß, dass von der Musik aus den aufgestellten Lautsprechern auf der mir übersandten Filmsequenz nichts zu hören war. Da somit bereits keine Störung der Versammlung zu erkennen war, existierte erst recht keine Straftat der erheblichen Störung einer Versammlung oder auch nur ein Anfangsverdacht einer solchen Straftat. Damit lagen auch nicht die Voraussetzungen für das Filmen auf einer strafprozessualen Rechtsgrundlage vor; dieses war daher rechtswidrig.

Ich habe dem zuständigen Polizeipräsidium daher mitgeteilt, dass ich das Filmen durch die eingesetzten Beamten für rechtswidrig halte, da keine Störung der Versammlung vorlag und damit auch keine Rechtsgrundlage für das Filmen gegeben war. Die betreffenden Videoaufnahmen sind mittlerweile gelöscht.

3.3 Durchsuchungen von Personen

Im Berichtszeitraum kam es zu Presseberichterstattungen im Zusammenhang mit einer den Intimbereich des Betroffenen berührenden Betäubungsmittelkontrolle am Münchner Hauptbahnhof und einer ebenfalls den Intimbereich betreffenden Durchsuchung von Schülern an einer Schule durch Jugendbeamte wegen des Verdachts des Diebstahls eines Fünf-Euro-Scheins.

Diese Berichterstattung habe ich zum Anlass genommen, die polizeiliche Handhabung und Regelungslage in Bezug auf solche intensive Personenkontrollen im Grundsatz zu überprüfen und das betroffene Polizeipräsidium auf einen Verbesserungsbedarf in folgenden Punkten hinzuweisen:

Strafprozessuale Eingriffsmaßnahmen stehen immer unter dem Vorbehalt der Verhältnismäßigkeit. Durchsuchungen, die mit einer Entkleidung verbunden sind, stellen einen schwerwiegenden Eingriff in das allgemeine Persönlichkeitsrecht dar. Wegen des besonderen Gewichts von Eingriffen, die den Intimbereich und das Schamgefühl des Betroffenen berühren, hat dieser Anspruch auf besondere Rücksichtnahme (vgl. Bundesverfassungsgericht, Beschluss vom 10.07.2013, Az.: 2 BvR 2815/11).

Grundsätzlich kann es sich bei der Durchsuchung eines Tatverdächtigen einer Straftat zwar um eine erfolgversprechende und notwendige polizeiliche Erstmaßnahme gemäß § 102 Strafprozessordnung (StPO) handeln. Dabei ist jedoch zu beachten, dass strafunmündige Kinder keine „Verdächtigen" im Sinne des § 102 StPO sein können, d.h. eine Durchsuchung von Strafunmündigen ist allenfalls unter den strengeren Voraussetzungen des § 103 StPO zulässig, wenn beispielsweise das Kind als Zeuge in Betracht kommt. Sie stellt erhöhte Anforderungen an die Prüfung des Verhältnismäßigkeitsgrundsatzes (vgl. Meyer-Goßner, § 103 StPO, Rn. 1a).

Gemäß § 105 Abs. 1 StPO dürfen Durchsuchungen nur durch den Richter, bei Gefahr im Verzug auch durch die Staatsanwaltschaft und ihre Ermittlungspersonen angeordnet werden. Hierbei handelt es sich um ein Stufenverhältnis, d.h. in erster Linie zuständig ist der Richter, der die Eingriffsvoraussetzungen eigenverantwortlich zu prüfen hat. Eine Zuständigkeit der Staatsanwaltschaft und – sollte auch sie nicht erreichbar sein – ihrer Ermittlungspersonen besteht nur bei Gefahr im Verzug. Die richterliche Anordnung ist damit die Regel, so dass die handelnden Polizeibeamten grundsätzlich versuchen müssen, eine solche einzuholen. Mit anderen Worten muss zumindest der Versuch einer telefonischen Kontaktaufnahme mit dem Gericht unternommen werden. An einem regulären Arbeitstag ist damit zu rechnen, dass ein Richter telefonisch zu erreichen ist. Darüber hinaus ist die Staatsanwaltschaft über ihren Bereitschaftsdienst rund um die Uhr zu erreichen. Ein Abweichen von diesem Stufenverhältnis wäre nur möglich, wenn die dadurch bedingte zeitliche Verzögerung zu einem Beweismittelverlust führen könnte.

Ich habe das betroffene Polizeipräsidium gebeten, die genannten Punkte geeignet umzusetzen und seine Beamten diesbezüglich zu sensibilisieren.

3.4 Einsatz von Videotechnik

3.4.1 Videoüberwachung nach Art. 32 PAG

3.4.1.1 Polizei beendet Videoüberwachung in Grafenwöhr

Im Jahr 2012 informierte mich das Polizeipräsidium Oberpfalz über sein Vorhaben, an einem Gefahrenbrennpunkt mit Gaststättenbetrieben und einer hohen polizeilichen Einsatzbelastung im Nahbereich des Truppenübungsplatzes Grafenwöhr, eine zeitlich begrenzte Videoüberwachung einzurichten. Nach Überlegungen der zuständigen Sicherheitsbehörden sollte den ansteigenden Deliktszahlen mit einem umfangreichen Maßnahmenbündel, von einer Sperrzeitverlängerung bis hin zu einem stadtsatzungsrechtlichen Alkoholverbot, begegnet werden. Angesichts der von der Polizei dargelegten besonderen Einsatzsituation in den Jahren 2011/2012 erschien auch nach meiner Bewertung eine polizeiliche Videoüberwachung nach Art. 32. Abs. 2 Nr. 2 Polizeiaufgabengesetz (PAG) vertretbar.

Art. 32 PAG Datenerhebung bei öffentlichen Veranstaltungen und Ansammlungen sowie an besonders gefährdeten Objekten
(2) [1]Die Polizei kann
1. zur Abwehr einer im Einzelfall bestehenden Gefahr
2. an den in Art. 13 Abs. 1 Nr. 2 genannten Orten, wenn sie öffentlich zugänglich sind, oder

3. an Orten, bei denen tatsächliche Anhaltspunkte die Annahme rechtfertigen, dass dort Ordnungswidrigkeiten von erheblicher Bedeutung begangen werden, wenn diese Orte öffentlich zugänglich sind,

offen Bild- und Tonaufnahmen oder -aufzeichnungen von Personen anfertigen. [2]In den Fällen des Satzes 1 Nrn. 2 und 3 soll in geeigneter Weise auf die Bild- und Tonaufnahmen und -aufzeichnungen hingewiesen werden.

In Absprache mit dem Staatsministerium des Innern, für Bau und Verkehr wurde die Dauer der Maßnahme zunächst auf ein Jahr begrenzt. Im Zeitraum bis zum 11.11.2013 erfolgte die Überwachung in den festgelegten Nachtstunden an insgesamt 184 Tagen. Wohl auch unter dem Einfluss der reduzierten Belegungszahlen und einer veränderten Truppenstruktur am Truppenübungsplatz Grafenwöhr konnte die Polizei ab Jahresbeginn 2013 eine stark rückläufige Entwicklung der Deliktszahlen im überwachten Bereich feststellen. Das Polizeipräsidium Oberpfalz entschied daher, die Maßnahme nicht weiter fortzuführen und beendete die Videoüberwachung in Grafenwöhr zum 11. November 2013.

Ich begrüße den Rückbau der Videoüberwachung. Vor allem bewerte ich es als sehr positiv, dass die Polizei bereit ist, von sich aus auf eine bereits geschaffene Überwachungsstruktur zu verzichten, sobald dies durch den Rückgang der Kriminalitätsentwicklung vor Ort angezeigt erscheint.

3.4.1.2 Videoüberwachung einer Auslandsvertretung

Die polizeiliche Videoüberwachung einer Auslandsvertretung habe ich zum Anlass für eine datenschutzrechtliche Prüfung genommen.

Rechtsgrundlage dieser stationären Videoüberwachung ist Art. 32 Abs. 3 Polizeiaufgabengesetz (PAG).

Art. 32 PAG Datenerhebung bei öffentlichen Veranstaltungen und Ansammlungen sowie an besonders gefährdeten Objekten

(3) Die Polizei kann an oder in den in Art. 13 Abs. 1 Nr. 3 genannten Objekten Bild- und Tonaufnahmen oder -aufzeichnungen von Personen anfertigen, soweit tatsächliche Anhaltspunkte die Annahme rechtfertigen, dass an oder in Objekten dieser Art Straftaten begangen werden sollen, durch die Personen, diese Objekte oder andere darin befindliche Sachen gefährdet sind.

Im Rahmen meiner Prüfung hatte ich darum gebeten, die tatsächlichen Voraussetzungen für die polizeiliche Videoüberwachung, die im Einvernehmen mit der betroffenen Auslandsvertretung vorgenommen wird, insbesondere anhand einer konkreten polizeilichen Gefährdungseinschätzung, näher zu erläutern. Ferner habe ich das zuständige Polizeipräsidium darauf hingewiesen, dass in der Einsatzanordnung Löschroutinen, Zugriffsrechte, Protokollierungsfragen, Auswertungskriterien, sowie eine Regelungslage bei Versammlungen konkret anzuordnen sind. Besonderes Augenmerk habe ich bei meiner datenschutzrechtlichen Prüfung auf die Reichweite der Kameras hinsichtlich einer möglichen Einsichtnahme in private Wohn- oder Geschäftsräume gelegt. Auch hier habe ich das zuständige Polizeipräsidium darauf hingewiesen, eine Einsichtnahme in Privaträume in jedem Fall technisch, etwa durch Schwarzschaltungen, auszuschließen.

3.4.1.3 Einsatz von Body-Cams

Seit Mai 2013 wird die sog. Body-Cam in Hessen als Pilotversuch bei der Polizei getestet. Dabei wird eine Videokamera auf der Schulter der Uniformweste angebracht und soll dem Schutz der Beamten vor Übergriffen dienen. Die Polizeibeamten können dabei die Kameras selbständig ein- und ausschalten. Der Einsatz ist auf Personenkontrollen und Streitschlichtung begrenzt. Als Rechtsgrundlage dient § 14 Abs. 6 Hessisches Gesetz über die öffentliche Sicherheit und Ordnung (HSOG):

§ 14 HSOG Datenerhebung und sonstige Datenverarbeitung an öffentlichen Orten und besonders gefährdeten öffentlichen Einrichtungen
(6) Die Polizeibehörden können an öffentlich zugänglichen Orten eine Person, deren Identität nach diesem Gesetz oder anderen Rechtsvorschriften festgestellt werden soll, mittels Bildübertragung offen beobachten und dies aufzeichnen, wenn dies nach den Umständen zum Schutz von Polizeivollzugsbeamtinnen und Polizeivollzugsbeamten oder Dritten gegen eine Gefahr für Leib oder Leben erforderlich ist. Dabei können personenbezogene Daten auch über dritte Personen erhoben werden, soweit dies unerlässlich ist, um die Maßnahme nach Satz 1 durchführen zu können. Sind die Daten für Zwecke der Eigensicherung oder der Strafverfolgung nicht mehr erforderlich, so sind sie unverzüglich zu löschen.

Aktuell ist bei der Bayerischen Polizei kein Pilotversuch zur Einführung von Body-Cams geplant. Allerdings prüft die Bayerische Polizei derzeit einen möglichen Einsatz von Body-Cams unter rechtlichen und fachlichen Gesichtspunkten, was ich kritisch begleiten werde.

Der Einsatz von Body-Cams ist nur zulässig, sofern die jeweils geltenden gesetzlichen Voraussetzungen erfüllt sind. Für den Bereich der polizeilichen Gefahrenabwehr in Bayern ist dabei vor allem an Art. 32 Polizeiaufgabengesetz zu denken. Eine vergleichbare Regelung wie § 14 Abs. 6 HSOG existiert in Bayern jedoch nicht. Nach meiner Einschätzung würde eine flächendeckende Erfassung sämtlicher Polizeieinsätze gegen Verfassungsrecht verstoßen. Polizeiliche Videoüberwachung mag zwar auch dem Schutz des Betroffenen dienen, zugleich ist sie jedoch auch stets ein Grundrechtseingriff. Solche Grundrechtseingriffe bedürfen nach dem Grundgesetz einer Rechtfertigung. Dies bedeutet insbesondere, dass sie für ein legitimes Ziel erforderlich und angemessen sein müssen. Sollten Polizeieinsätze vollständig mittels Body-Cams erfasst werden, würde man nicht nur die Polizeibeamten übermäßig kontrollieren, sondern auch den öffentlichen Raum mit einer unverhältnismäßigen Vorratsdatenspeicherung überziehen.

3.4.2 Videoüberwachung von Dienstgebäuden nach Art. 21a BayDSG

Mit dem Thema Videoüberwachung im Bereich der Polizei habe ich mich bereits wiederholt ausführlich befasst. Auch in diesem Berichtszeitraum habe ich mich wiederum mit der Videoüberwachung von Gebäuden verschiedener Bayerischer Polizeidienststellen auseinandergesetzt.

Die Rechtsgrundlage für die Videoüberwachung einer Polizeidienststelle liegt in der Regel im Hausrecht der Behörde nach Art. 21a BayDSG. Art. 49 Polizeiaufgabengesetz (PAG) bestimmt, dass Art. 21a BayDSG in Ausübung des Hausrechts Anwendung findet. Diese spezielle Regelung verdrängt Art. 32 PAG. Sofern die Anlagen zur Videoüberwachung auch eine Aufzeichnung ermöglichen, ist nach

Art. 49 PAG und Art. 21a Abs. 6 in Verbindung mit Art. 26 und Art. 27 BayDSG eine datenschutzrechtliche Freigabe und die Aufnahme in das Verfahrensverzeichnis erforderlich. Gemäß Art. 21a Abs. 2 BayDSG sind die Videoüberwachung und die erhebende Stelle durch geeignete Maßnahmen erkennbar zu machen. Die Videoüberwachung ist grundsätzlich gemäß Art. 21a Abs. 1 BayDSG auf den Bereich der „unmittelbaren Nähe" zu beschränken.

Im Rahmen meiner Prüfungen habe ich festgestellt, dass insbesondere für den Fall, dass im Umfeld des videoüberwachten Gebäudes eine Versammlung stattfindet, sichergestellt werden muss, dass Aufzeichnungen nur nach dem Bayerischen Versammlungsgesetz zulässig sind. Liegen die Voraussetzungen des Bayerischen Versammlungsgesetzes nicht vor, müssen die betroffenen Kameras weggeschwenkt bzw. ausgeschaltet werden. Auf eine entsprechende Ergänzung der Dienstanweisung habe ich hingewirkt. Bei der Beschilderung habe ich darum gebeten sicherzustellen, dass diese bereits erkennbar sein muss, bevor der Bürger den überwachten Bereich betritt. Positiv habe ich festgestellt, dass der Sichtbereich der Kameras zum Teil durch Schwarzschaltungen abgedeckt wurde, soweit öffentliche Bereiche erfasst wurden, die über den Nahbereich des Gebäudes hinausgingen wie z.B. Fußgängerzonen. Auch im Fall eines Zoomes lässt sich die Schwarzschaltung nicht umgehen; der einsehbare Raum verkleinert sich im Gegenteil noch deutlich. Auch dies halte ich für eine sehr datenschutzkonforme Lösung.

3.5 Speicherungen in polizeilichen Dateien

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

3.5.1 Formulierungen in Kurzsachverhalten des Integrationsverfahrens der Bayerischen Polizei (IGVP)

Im Rahmen meiner Prüftätigkeit stieß ich auf einen IGVP-Kurzsachverhalt, der die Formulierung „der ehrenwerte Herr …" enthielt. Aufgrund der Gesamtumstände war davon auszugehen, dass diese Wortwahl eine herabsetzende Intention hatte. Da Eintragungen im IGVP in einer sprachlich neutralen Form abgefasst werden müssen und herablassende Äußerungen inakzeptabel sind, habe ich das zuständige Polizeipräsidium auf diese Eintragung aufmerksam gemacht. Das Polizeipräsidium war daraufhin sofort bereit, die zitierte Formulierung zu korrigieren.

3.5.2 Freitextrecherchen in Kurzsachverhalten des Integrationsverfahren der Bayerischen Polizei (IGVP)

Meiner Ankündigung im letzten Tätigkeitsbericht entsprechend (siehe 25. Tätigkeitsbericht 2012 Nr. 3.5.1) habe ich die Freitextrecherche in den Kurzsachverhalten im polizeilichen Integrationsverfahren (IGVP) bei zwei Polizeipräsidien überprüft. Hintergrund der Prüfung war die Ausdehnung der Freitextrecherche auf die im IGVP gespeicherten Kurzsachverhalte. Das Staatsministerium des Innern, für Bau und Verkehr hatte diesbezüglich die Anweisung erteilt, dass in den Kurzsachverhalten auf bestehende Daten – wie beispielsweise Namensangaben – in strukturierten Datenfeldern (z.B. „BES“ für „Beschuldigter“) verwiesen werden soll, in denen automatisiert gelöscht werden kann. Ich hatte dem Staatsministerium des Innern, für Bau und Verkehr gegenüber die Befürchtung geäußert, dass andernfalls Prüfungs- und Löschungstermine für die suchfähige Speicherung personenbezogener Daten (insbesondere von Kindern und Jugendlichen) nicht durchwegs eingehalten werden. Im Rahmen meiner Prüfung habe ich stichprobenartig neue Eintragungen im IGVP dahingehend kontrolliert, ob in den gespeicherten Kurzsachverhalten unzulässigerweise weiter Namensangaben gemacht werden oder stattdessen lediglich auf strukturierte Datenfelder verwiesen wird.

Meine Prüfung hat ergeben, dass Kurzsachverhalte in einigen Fällen vollständige Namen enthielten bzw. teilweise Namen nur unwesentlich abgekürzt waren. Diese Kürzel ließen einen Rückschluss auf den vollständigen Namen zu.

Ich habe dieses Prüfungsergebnis sowohl den betroffenen Polizeipräsidien als auch dem Staatsministerium des Innern, für Bau und Verkehr mitgeteilt. Die Polizeipräsidien haben mir daraufhin bestätigt, dass die konkreten Fälle im IGVP bereinigt wurden. Das Staatsministerium hat mir versichert, dass die Polizeiverbände angewiesen wurden, die Mitarbeiter im Rahmen der Aus- und Fortbildung sowie im Rahmen fortgesetzter Datenqualitätsmaßnahmen eingehend hinsichtlich der bestehenden Regelungslage zu sensibilisieren.

3.5.3 Prüfung der Speicherungsvoraussetzung „polizeilicher Restverdacht“

Mit der polizeilichen Speicherung von personenbezogenen Daten aus strafrechtlichen Ermittlungen zu präventiven Zwecken im Sinne von Art. 38 Abs. 2 Polizeiaufgabengesetz (PAG) (INPOL/KAN-Datei) beschäftige ich mich fortlaufend sehr intensiv. Die Polizei kann die erhobenen personenbezogenen Daten auch nach Abschluss des Strafverfahrens weiterhin in dieser Datei speichern, selbst wenn die Staatsanwaltschaft das Verfahren eingestellt hat oder der Angeklagte von einem Gericht freigesprochen wurde. Voraussetzung für die weitere Speicherung ist nach Auffassung des Bayerischen Verwaltungsgerichtshofs, dass nach Abschluss des Strafverfahrens ein Tatverdacht von ausreichender Substanz verbleibt und nicht auszuschließen ist, dass die Speicherung der Daten des vormals Beschuldigten auch künftig bei der vorbeugenden Straftatenbekämpfung von Nutzen sein könnte. Der für eine weitere polizeiliche Speicherung erforderliche sogenannte Restverdacht ist von dem hinreichenden Tatverdacht im Sinne der Strafprozessordnung zu unterscheiden. Auch wenn der strafprozessuale Tatnachweis hinsichtlich einer Straftat nicht geführt werden kann, können Zeugenaussagen oder sonstige konkrete Anhaltspunkte dafür sprechen, dass der polizeiliche Restverdacht fortbesteht (vgl. auch Bundesverfassungsgericht, Beschluss vom 16.05.2002, Az.: 1 BvR 2257/01, siehe auch Beschluss vom 01.06.2006,

Az.: 1 BvR 2293/03). Die Einstellung eines Verfahrens oder ein gerichtlicher Freispruch beseitigt daher für sich alleine den Tatverdacht grundsätzlich noch nicht.

Anders liegt der Fall, wenn in der Einstellungsverfügung oder dem freisprechenden Urteil ausdrücklich festgestellt wird, dass der Tatverdacht gegen den Beschuldigten vollständig entfallen ist – etwa weil keine Straftat vorliegt, der Beschuldigte nicht der Täter ist oder er nicht rechtswidrig gehandelt hat. Von einer solchen ausdrücklichen Bewertung der Staatsanwaltschaft oder des Gerichts darf die Polizei nicht von sich aus abweichen. So auch die Rechtsprechung des Bayerischen Verwaltungsgerichtshofs, wonach die Speicherungen im Fall der Feststellung der Staatsanwaltschaft oder des Gerichts über ein vollständiges Entfallen des Verdachts zu löschen sind (Art. 38 Abs. 2 Satz 2 PAG) und eine eigenständige Prüfung der Polizei zum verbleibenden Verdacht nur in Fällen erforderlich ist, in welchen keine derartige Feststellung erfolgte (Verwaltungsgerichtshof vom 01.08.2012, Az.: 10 ZB 11. 2438, Rn. 3).

Im Berichtszeitraum habe ich die Speicherungspraxis im Bereich zweier Polizeipräsidien in dieser Hinsicht überprüft. Dabei konzentrierte ich mich auf Ermittlungsverfahren, die mit der ausdrücklichen Feststellung der Staatsanwaltschaft eingestellt wurden, dass der Beschuldigte unschuldig ist bzw. ein begründeter Tatverdacht nicht mehr besteht. Überprüft habe ich also Fälle, die keine – abweichende – Bewertung der Polizei gestatten und bei der die polizeiliche präventive Speicherung (INPOL/KAN-Datei) unzulässig ist (vgl. oben). In der polizeilichen Vorgangsverwaltungsdatei IGVP hingegen darf der Vorgang zur Dokumentation polizeilichen Handelns zunächst weiterhin gespeichert werden, der Status des vormals Beschuldigten ist in diesen Fällen allerdings auf Zeuge zu ändern. Meine Prüfung zeigte in vielen Fällen, dass die Speicherung in der Vorgangsverwaltung der Polizei (IGVP) nicht dem Verfahrensausgang entsprechend angepasst wurde. In seltenen Fällen war der ehemalige Beschuldigte sogar trotz der Feststellung des restlos entfallenen Tatverdachts im INPOL/KAN weiterhin als Beschuldigter geführt. Stellenweise beruhten diese Umstände darauf, dass der Polizei die für eine Einzelprüfung erforderliche Mitteilung über den Verfahrensausgang entweder nicht oder nicht vollständig übermittelt wurde (siehe Nr. 5.3.5). Ich habe die geprüften Präsidien demgemäß zur Änderung bzw. Löschung der Speicherungen entsprechend den oben dargestellten Grundsätzen aufgefordert und auf die Bedeutung der Thematik für die betroffenen Bürger hingewiesen. Die Präsidien sind allen Forderungen nachgekommen. Bei meiner Prüfung hat sich zudem gezeigt, welche erhebliche Bedeutung die Mitteilung der Staatsanwaltschaft an die Polizei über den Ausgang des Verfahrens besitzt. Diese stellt meist die einzige Grundlage der Polizei für ihre Umsetzung der Feststellungen der Staatsanwaltschaft in ihren polizeilichen Dateien dar.

3.5.4 Prüfung erkennungsdienstlicher Maßnahmen

Sollen Beschuldigte im Rahmen von Ermittlungsverfahren erkennungsdienstlich behandelt werden, empfinden sie dies zumeist als einen weitaus drastischeren Eingriff in ihre Rechtssphäre, als andere gegen sie gerichtete Maßnahmen. Dies zeigt zumindest meine Erfahrung mit Bürgereingaben in diesem Bereich. Oft verstärkt sich dieser Eindruck beim Betroffenen noch, wenn die erhobenen Daten nicht der Aufklärung im gerade geführten Strafverfahren dienen sollen, sondern die Polizei die Unterlagen für die Zukunft bereithalten möchte, da sie erneute Strafverfahren gegen die Person erwartet. Der Gesetzgeber hat die Voraus-

setzungen für eine erkennungsdienstliche Maßnahme in § 81b Strafprozessordnung (StPO) eher knapp umschrieben.

§ 81b StPO Erkennungsdienstliche Maßnahmen bei dem Beschuldigten
Soweit es für die Zwecke der Durchführung des Strafverfahrens oder für die Zwecke des Erkennungsdienstes notwendig ist, dürfen Lichtbilder und Fingerabdrücke des Beschuldigten auch gegen seinen Willen aufgenommen und Messungen und ähnliche Maßnahmen an ihm vorgenommen werden.

Wann diese Voraussetzungen für eine erkennungsdienstliche Maßnahme zur vorbeugenden Bekämpfung von künftigen Straftaten tatsächlich erfüllt sind, lässt sich aber an Hand der Rechtsprechung zu § 81b StPO konkretisieren. So muss insbesondere eine auf Tatsachen basierende verlässliche Prognose getroffen werden, dass der Beschuldigte wieder in den Kreis der Verdächtigen einer noch aufzuklärenden strafbaren Handlung einbezogen werden könnte. Zusätzlich müssen die erkennungsdienstlichen Unterlagen die dann möglicherweise zu führenden Ermittlungen auch fördern können. Insgesamt kommt es bei der Frage der Zulässigkeit einer erkennungsdienstlichen Behandlung auf die Umstände des Einzelfalls an. Dabei sind bei der Gesamtbewertung die Art, Schwere und Begehungsweise der dem Betroffenen im strafrechtlichen Anlassverfahren zur Last gelegten Straftaten, seine Persönlichkeit sowie der Zeitraum zu berücksichtigen, währenddessen er strafrechtlich nicht mehr in Erscheinung getreten ist. Der polizeiliche Sachbearbeiter hat also eine ganze Reihe von Kriterien in seine Abwägung einzubeziehen, bevor er sich für eine so gravierende Maßnahme entscheidet. Er sollte stets vor Augen haben, dass eine **erkennungsdienstliche Behandlung typischerweise bei gewerbs- oder gewohnheitsmäßig handelnden Tätern in Betracht kommt.** Insbesondere hat er diese Entscheidung ohne eigenen Belastungseifer gegenüber dem Beschuldigten und ohne einen etwaigen Quotendruck zu treffen. Dies gilt umso mehr, als einmal vollzogene erkennungsdienstliche Maßnahmen, ohne eine regelmäßige Kontrolle durch eine weitere Instanz, über einen langen Zeitraum (Regelspeicherfrist bei Erwachsenen 10 Jahre) gespeichert bleiben – zumindest soweit nicht der Betroffene selbst dagegen Einwände erhebt.

Als Ergebnis meiner Prüfung kann ich zusammenfassen, dass zu viel und zu schnell erkennungsdienstlich behandelt wurde. Im Rahmen meiner Prüfung ließ ich mir zunächst 150 erkennungsdienstliche Maßnahmen von Personen, die im Kriminalaktennachweis mit höchstens drei Unterlagen gespeichert sind, vorlegen. Nach einer weiteren Vorauswahl konzentrierte ich mich bei meiner Vorortprüfung auf zwanzig Maßnahmen. In dreizehn von diesen zwanzig Fällen forderte ich das betroffene Präsidium zur Löschung der erkennungsdienstlichen Unterlagen oder gar der gesamten Speicherung im Kriminalaktennachweis auf.

Die Bandbreite der festgestellten Mängel stellte sich dabei wie folgt dar: Fehlen eines haltbaren Tatverdachts; keine ausreichenden Erkenntnisse für die geforderte Negativprognose (weil keine ausreichende Grundlage gegeben war, um eine erneute Verfehlung der Betroffenen zu erwarten oder weil der Abstand zwischen den in der Vergangenheit vorgefallenen Delikten als für eine Prognoseentscheidung zu lange angesehen werden musste); fehlende Notwendigkeit der Speicherung von erkennungsdienstlichen Unterlagen für die Aufklärung der begangenen und möglicherweise wieder zu erwartenden Delikte (weil es sich z.B. um einen Warenkreditbetrug handelte und über die Identität des Betroffenen zu keinem Zeitpunkt Zweifel bestand); Nichtbeachtung des Verhältnismäßigkeitsgrundsatzes (z.B. erkennungsdienstliche Behandlung wegen zweier Ladendiebstähle

geringwertiger Sachen – einmal eine Packung Brotzeiteier und dreieinhalb Jahre später eine DVD im Wert von 8,99 Euro).

Trotz dieser negativen Feststellungen ist diese Prüfung ein Beispiel für die erfreuliche Zusammenarbeit mit der Polizei in den vergangenen Jahren. So folgte das geprüfte Polizeipräsidium in allen Fällen meiner Aufforderung zur Löschung. Darüber hinaus hat es mir zugesichert, das Thema „erkennungsdienstliche Behandlungen" intern aufzubereiten und eine Verbesserung der Maßnahmenqualität anzustreben.

3.5.5 Prüfung retrograder DNA-Speicherungen

Bereits in meinem vorangegangenen Tätigkeitsbericht habe ich mich mit sogenannten retrograden DNA-Speicherungen beschäftigt (siehe 25. Tätigkeitsbericht 2012 Nr. 3.5.6). Auch hatte ich angekündigt, wegen der datenschutzrechtlichen Bedeutung des Themas noch weitere Präsidien zu prüfen. Dies ist in der Zwischenzeit geschehen und meine diesbezüglichen Prüfungen sind abgeschlossen.

§ 81g StPO Identifikationsfeststellung
(1) Ist der Beschuldigte einer Straftat von erheblicher Bedeutung oder einer Straftat gegen die sexuelle Selbstbestimmung verdächtig, dürfen ihm zur Identitätsfeststellung in künftigen Strafverfahren Körperzellen entnommen und zur Feststellung des DNA-Identifizierungsmusters sowie des Geschlechts molekulargenetisch untersucht werden, wenn wegen der Art oder Ausführung der Tat, der Persönlichkeit des Beschuldigten oder sonstiger Erkenntnisse Grund zu der Annahme besteht, dass gegen ihn künftig Strafverfahren wegen einer Straftat von erheblicher Bedeutung zu führen sind. Die wiederholte Begehung sonstiger Straftaten kann im Unrechtsgehalt einer Straftat von erheblicher Bedeutung gleichstehen.

Im Rahmen meiner Prüfungen konnte ich in einigen Fällen erreichen, dass die gespeicherten DNA-Muster wieder gelöscht wurden, da die Voraussetzungen des § 81g Strafprozessordnung (StPO) nicht erfüllt waren.

Mehrfach musste ich kritisieren, dass oftmals DNA-Speicherungen vorgenommen wurden, obwohl der Betroffene nur zu einer Bewährungsstrafe verurteilt und dieser Umstand bei der nach § 81g StPO zu treffenden Prognoseentscheidung nicht berücksichtigt wurde. Voraussetzung für eine DNA-Speicherung nach § 81g StPO ist eine **Prognose** dahingehend, dass **gegen den Beschuldigten erneut Strafverfahren wegen Straftaten von erheblicher Bedeutung zu führen sein werden.** Um eine solche Prognose treffen zu können, müssen alle Umstände in den Abwägungsvorgang eingestellt werden, die gleichermaßen bei einer Sozialprognose für die Strafaussetzung zur Bewährung bestimmend sein können. Dies bedeutet letztlich, dass in Fällen, in denen der Betroffene zu einer Bewährungsstrafe verurteilt wurde, eine DNA-Speicherung einem erhöhten Begründungsbedarf unterliegt (vgl. u.a. Bundesverfassungsgericht, Beschluss vom 29.09.2013, Az.: 2 BvR 939/13).

3.5.6 Herausragende Einzelfälle

3.5.6.1 Unzulässige Speicherung eines Rechtsanwalts wegen Geldwäscheverdachts

Im Rahmen einer Personenkontrolle erfuhr ein Rechtsanwalt zufälligerweise und für ihn völlig überraschend, dass er polizeilich gespeichert sei. Daraufhin wandte er sich an mich.

Bei meiner anschließenden datenschutzrechtlichen Prüfung stellte ich Folgendes fest: Der Rechtsanwalt war im Zusammenhang mit seiner Funktion als Geschäftsführer einer Leasingfirma in INPOL wegen Diebstahls in einem besonders schweren Fall (Kfz) und wegen Verdachts der Geldwäsche gespeichert.

Den Diebstahlsverdacht speicherte die Polizei, da im Jahr 2003 ein durch die Firma des Rechtsanwalts verleastes Fahrzeug entwendet wurde. Inwieweit der Rechtsanwalt damit zu tun hatte, konnte die Polizei nicht substantiiert erläutern. So stellte die Staatsanwaltschaft das Verfahren nach § 170 Abs. 2 Strafprozessordnung (StPO) ein. Die Polizei begründete die weitere Speicherung vor allem damit, dass der polizeiliche Restverdacht infolge der ihr in diesem Fall vorliegenden Verfahrenseinstellung nach § 170 Abs. 2 StPO nicht vollständig entfallen sei. Aus datenschutzrechtlicher Sicht problematisch war hierbei insbesondere die Argumentation, mit der die Polizei die weitere Speicherung zusätzlich zu begründen versuchte: Im Rahmen der Ermittlungen hätten auch keine entlastenden Beweise bzw. Erkenntnisse festgestellt werden können, so dass der Tatverdacht auch nicht ausgeräumt worden sei. Diese Argumentation verfängt nicht. Das Fortbestehen eines Restverdachts ist, wie aus Art. 38 Abs. 2 Satz 2 Personalaufgabengesetz folgt, zwingende Tatbestandsvoraussetzung für die Rechtmäßigkeit der weiteren Speicherung. **Beruft sich die speichernde Polizeibehörde auf einen fortbestehenden Restverdacht, obliegt ihr daher auch die entsprechende Darlegungs- und Beweislast.**

Der Speicherung wegen Geldwäsche lag ein Steuerstrafverfahren gegen einen Leasingnehmer der oben erwähnten Firma zugrunde. Aus Sicht der Ermittlungsbehörden lagen, insbesondere aufgrund des Verhaltens des Leasingnehmers, auch geldwäscherelevante Anhaltspunkte gegen die Leasingfirma des Rechtsanwalts vor. Als Ermittlungsansatz führte die Polizei zusätzlich belastend an, der Rechtsanwalt sei im Jahr 2003 wegen eines schweren Diebstahls polizeilich in Erscheinung getreten. Gleichwohl konnte ein Anfangsverdacht wegen Geldwäsche nicht verifiziert werden, weshalb 2009 von der Einleitung eines förmlichen Ermittlungsverfahrens gemäß § 152 Abs. 2 StPO abgesehen wurde. Da sich der ursprüngliche Anfangsverdacht im Laufe der Ermittlungen nicht erhärtet hatte und noch nicht einmal ein förmliches Ermittlungsverfahren eingeleitet wurde, hätte auch diese Speicherung nach Wegfall des zugrundeliegenden Verdachts gelöscht werden müssen.

Erst aufgrund meines Betreibens wurden beide Speicherungen gelöscht.

Insbesondere der Umstand, dass die eigentlich unzulässige Speicherung wegen schweren Diebstahls im zweiten Verfahren wegen Geldwäsche belastend herangezogen wurde, verdeutlicht, wie wichtig es für die Rechte des Einzelnen ist, dass solche polizeilichen Speicherungen nur vorgenommen werden dürfen, wenn auch tatsächlich ein polizeilicher Restverdacht vorliegt.

3.5.6.2 Unzulässige Speicherungen im Zusammenhang mit Verstößen gegen das Betäubungsmittelgesetz

Schon in meinen früheren Tätigkeitsberichten habe ich immer wieder gewarnt, welche negativen Konsequenzen für den Betroffenen unzulässige Speicherungen in polizeilichen Systemen haben können. Gerade bei mutmaßlichen Verstößen gegen das Betäubungsmittelgesetz ist daher eine gewissenhafte Speicherpraxis unerlässlich. Im Widerspruch hierzu stelle ich immer wieder fest, dass schon nach ersten Verdachtsmomenten – die sich später nicht erhärten – entsprechende Speicherungen im Kriminalaktennachweis angelegt bzw. nicht wieder gelöscht werden.

So im Fall einer jungen Frau, die bei einer Polizeidienststelle eigentlich eine Beschädigung ihres Autos anzeigen wollte. Aus ihrem aufgeregten und redseligen Verhalten schlossen die Beamten, sie sei unter Drogeneinfluss mit dem Auto zur Polizeiwache gefahren. Den bei der jungen Frau daraufhin durchgeführten Drogenschnelltest deuteten die Beamten als Beweis für ihre Einschätzung. Sie leiteten deshalb ein Strafverfahren wegen Trunkenheit im Verkehr ein und stellten auch noch eine Strafanzeige wegen einer Straftat nach dem Betäubungsmittelgesetz, da die Frau die vermeintlich eingenommenen Drogen ja auch einmal besessen haben musste. Diese Annahmen wurden sodann der zuständigen Fahrerlaubnisbehörde mitgeteilt und flossen auch – obwohl hierfür völlig unerheblich – in den Unfallbericht wegen der zurückliegenden Beschädigung ihres Fahrzeuges ein. All dies, obwohl sich laut polizeilicher Ermittlungsakte keine weiteren Ermittlungsansätze finden ließen und die chemisch-toxikologische Untersuchung einer Blutprobe durch ein Institut für Rechtsmedizin keinerlei Hinweise ergab, dass die junge Frau berauschende Mittel konsumiert habe. Der polizeiliche Vorbefund wurde durch die Untersuchung somit unmissverständlich widerlegt und die Staatsanwaltschaft stellte die anhängigen Ermittlungsverfahren umgehend ein.

Trotz dessen sollten aus polizeilicher Sicht die Verdachtsspeicherungen weiterhin aufrechterhalten werden. So wertete das Polizeipräsidium zunächst ein von den Beamten selbst ausgefülltes Protokoll, in dem die vermeintlichen „drogentypischen Auffälligkeiten“ durch den Sachbearbeiter angekreuzt wurden, als Indiz dafür, dass die Beamten mit ihren Vermutungen richtig lagen. Einer näheren Betrachtung hielt dieses Protokoll allerdings nicht Stand. Die darin angekreuzten Angaben widersprachen sich und deuteten eher auf eine fehlerhafte Verhaltensinterpretation durch die Beamten hin. Nach längerem Schriftwechsel löschte die Polizei schließlich die betreffenden Speicherungen und teilte die Verfahrenseinstellung auch der Führerscheinstelle beim Landratsamt mit. Insoweit dürften der jungen Frau nunmehr keine weiteren Unannehmlichkeiten drohen.

3.5.6.3 Unzulässige Speicherungen trotz Verfahrenseinstellung und Entfallen eines Restverdachts

Eine Fahrerlaubnisbehörde wollte die Eignung einer Petentin zum Führen von Kraftfahrzeugen überprüfen, da gegen diese polizeiliche Ermittlungen aufgrund des Verdachts eines Betäubungsmitteldelikts geführt wurden. Die Petentin, der diese Ermittlungen zum damaligen Zeitpunkt unbekannt waren, konnte sich dies zunächst nicht erklären und wandte sich an mich. Wie sich später herausstellte, wurden die Personalien der Petentin missbräuchlich verwendet. Sie wurde von dem unbekannten tatsächlichen Absender eines Briefes fälschlicherweise als Absenderin auf dem Briefumschlag genannt. Der Brief enthielt unter das Betäu-

bungsmittelgesetz fallende Amphetamine und wurde an eine Anschrift in München zugestellt. Der Adressat dieses Briefes, der ebenfalls nichts mit dem Versand der Betäubungsmittel zu tun zu hatte, ließ den Brief samt Inhalt bei der Polizei abgeben. Auch nach den polizeilichen Erkenntnissen hatten weder die als Absenderin genannte Petentin noch der Adressat des Briefes mit Betäubungsmitteldelikten jemals etwas zu tun.

Ganz offensichtlich wurde also die teils in der regionalen Öffentlichkeit stehende Petentin bewusst missbräuchlich als Absenderin des Briefes genannt, eventuell um sie in Misskredit zu bringen. Die Ermittlungsverfahren gegen die Petentin und den Empfänger wurden demgemäß auch gemäß § 170 Abs. 2 Strafprozessordnung mangels Tatverdacht eingestellt. Trotz der bereits von Anfang an schwachen Verdachtsgrundlage, teilte die Polizei den Vorwurf gegen die Petentin an die zuständige Fahrerlaubnisbehörde zur Überprüfung der Fahreignung mit. Eine solche Mitteilung kann zwar grundsätzlich nach § 2 Abs. 12 Straßenverkehrsgesetz (StVG) erfolgen.

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

Hier jedoch wurden die Umstände des Einzelfalls nicht berücksichtigt, die einer solchen Mitteilung der Polizei entgegengestanden hatten. Insbesondere erfolgte die Meldung verfrüht und auf einer nicht genügenden Verdachtsgrundlage.

Obwohl nach den geführten Ermittlungen und der Einstellung durch die Staatsanwaltschaft im vorliegenden Fall der für eine Speicherung in der polizeilichen Gefahrenabwehrdatei INPOL/KAN erforderliche Restverdacht weder bei der Petentin noch beim Empfänger des Briefes vorlag, blieben beide Personen als Beschuldigte eines Strafverfahrens im Zusammenhang mit einem Betäubungsmitteldelikt gespeichert. Weil der Restverdacht gegen beide Personen vollständig entfallen war, habe ich die Polizei um Löschung dieser Speicherungen in INPOL/KAN gebeten. Zudem habe ich eine entsprechende Klarstellung in der Vorgangsverwaltungsdatei IGVP gefordert, aus der sich das Entfallen des Tatverdachts gegen beide Personen ergibt. Die Polizei bedauerte den Vorfall und kam meinen sämtlichen Forderungen nach, die Speicherungen beider Personen zu löschen bzw. entsprechend zu ändern.

3.5.7 Speicherung von Fingerabdrücken von Zeugen zum Vergleich mit Tatortspuren

Sofern im Rahmen von strafrechtlichen Ermittlungen Fingerabdrücke am Tatort oder an tatrelevanten Gegenständen gesichert werden können, ersuchen die Strafverfolgungsbehörden nichtverdächtige Zeugen, die sich berechtigt am Tatort aufgehalten haben oder mit den betreffenden Gegenständen berechtigterweise in Berührung gekommen sind, um die Abgabe von Fingerabdrücken zum Vergleich. Diese Vergleichsfingerabdrücke dienen dazu, die von berechtigten Perso-

nen hinterlassenen Fingerabdrücke von denjenigen potentieller Täter unterscheiden zu können. Soweit kein Verdacht gegen diese Personen besteht, können derartige Vergleichsfingerabdrücke nur mit deren Einwilligung erhoben werden. Eine nichtverdächtige Zeugin beschwerte sich bei mir, dass die Polizei ihre Vergleichsfingerabdrücke zu lange gespeichert habe. Dies nahm ich zum Anlass, mich näher mit der freiwilligen Abgabe und Speicherung solcher Vergleichsfingerabdrücke zu befassen. Im Zuge meiner Überprüfung des konkreten Falles wurde die entsprechende bayernweite Datei für Vergleichsabdrücke bzw. deren Regelung überarbeitet und verbessert. Für die freiwillige Abgabe existiert nun ein einheitliches Formblatt zur Einwilligung. Gegenüber älteren Formblättern enthält das neue Formular zusätzliche Hinweise, wie etwa auf die jederzeit mögliche Rücknahme der Einwilligung. Die freiwillig abgegebenen Vergleichsfingerabdrücke werden ausschließlich in der **eigenständigen Datei „Tatortberechtigte/Vergleichsabdrücke“** gespeichert, um den Ausschluss berechtigt gesetzter Spuren im konkreten Ermittlungsverfahren durchzuführen. In die bundesweite Datei mit Fingerabdrücken verdächtiger Personen werden sie nicht übernommen. Die betroffenen Personen können ihre Einwilligung jederzeit zurücknehmen, die Vergleichsabdrücke sind dann unverzüglich zu löschen. Im Übrigen dürfen die Strafverfolgungsbehörden freiwillige Vergleichsabdrücke auch nur so lange speichern, als sie für den Abgleich erforderlich ist. Nach Abschluss des Abgleichs sind sie zu löschen, wobei diese Löschungspflicht nochmals durch eine automatisierte Löschroutine abgesichert wird. Unabhängig vom Stand der Bearbeitung und des Abgleichs werden die Vergleichsabdrücke spätestens nach Ablauf eines Jahres automatisch gelöscht.

Auch der Petentin des Ausgangsfalles konnte ich weiterhelfen, ihre Vergleichsfingerabdrücke wurden auf mein Betreiben hin gelöscht.

3.6 Datenübermittlungen

3.6.1 Datenübermittlung an privaten Sicherheitsdienst

Ein Bürger hatte sich an mich gewandt und folgenden Sachverhalt geschildert: An einem lauen Sommerabend feierte er mit Freunden in einem Erholungsgebiet an einem bekannten bayerischen See den Geburtstag seiner Tochter. Zu vorgerückter Stunde traten dann zwei Männer eines privaten Wach- und Sicherheitsdienstes an die Gruppe heran und forderten von den Anwesenden ihre Personalien. Auf Nachfrage erklärten die Wachmänner, vom zuständigen Landratsamt mit dieser Aufgabe betraut zu sein. Anhand der Personalien könnten später eventuell entstehende Verschmutzungen geahndet werden. Da offensichtlich aber weder eine Verschmutzung vorlag, noch übermäßig Lärm durch die Gruppe erzeugt worden war, wollten die Anwesenden ihre Personalien nicht grundlos den privaten Wachmännern überlassen. So kamen diese einige Zeit später mit zwei Polizeibeamten der dortigen Polizeiinspektion zurück. Als die Kontrolle dann durch die Polizeibeamten durchgeführt wurde, händigte der Petent widerwillig seinen Ausweis der Polizei aus. Die Beamten notierten sich die Personalien und gaben sie anschließend an den Sicherheitsdienst weiter.

Auf meine Anfrage hin bestätigte mir die Polizei den Sachverhalt einschließlich der Kontrolle und der Weitergabe der Daten an den Sicherheitsdienst. Da dieser vom Landratsamt beauftragt war, die Einhaltung der Nutzungsregelungen für das Naherholungsgebiet zu überwachen, gingen die Beamten irrtümlich davon aus, die Weitergabe der Personalien sei im Rahmen der Amtshilfe geboten und zulässig.

Das zuständige Polizeipräsidium bewertete diese Einschätzung der Beamten als falsch und versicherte mir gegenüber, diese Problematik im Rahmen von Dienstunterrichten bei den betreffenden Polizeidienststellen nochmals aufzugreifen, um mögliche rechtliche Unsicherheiten bei den Beamten abzubauen. Zudem erklärte der zuständige Landkreis in seiner Stellungnahme, dass der Sicherheitsdienst nicht dazu ermächtigt oder gar angewiesen ist, Personalien festzustellen. Soweit sich Anhaltspunkte für das Vorliegen von Ordnungswidrigkeiten oder Straftaten ergeben, solle dieser lediglich die Polizei informieren und diese dann im Rahmen ihrer Befugnisse eigene Maßnahmen treffen. Nachdem sich die zuständigen Behörden in diesem Fall einsichtig gezeigt haben, beließ ich es im Hinblick auf den datenschutzrechtlichen Verstoß im Rahmen der Datenübermittlung bei meinem Hinweis. Soweit mir ähnliche Fälle bekannt werden, beabsichtige ich das Thema jedoch erneut aufzugreifen.

3.6.2 Vorzeigen eines erkennungsdienstlichen Bildes

Aufgrund nachfolgenden Sachverhalts habe ich das zuständige Polizeipräsidium förmlich gemäß Art. 31 Abs. 1 BayDSG beanstandet, da es sich hierbei um einen schwerwiegenden Verstoß gegen datenschutzrechtliche Vorschriften handelte:

Ein Polizeibeamter überschritt seine Befugnisse im Rahmen der Verfolgung einer von ihm beobachteten Verkehrsordnungswidrigkeit (Nutzung eines Mobiltelefons während einer Autofahrt) deutlich. Im Zuge der Fahrerermittlung war bereits anhand eines Abgleichs mit dem polizeilichen Informationssystem und den darin gespeicherten (vier Jahre alten) Lichtbildern des Betroffenen aus einer früheren erkennungsdienstlichen Behandlung die Betroffeneneigenschaft sehr wahrscheinlich. Obwohl der ermittelnde Polizeibeamte den Betroffenen mittels der polizeilichen Lichtbilder wiedererkannt hatte, suchte er diesen zu Hause auf, um sich zweifelsfrei von seiner Identität zu überzeugen. Da der Betroffene unter der angegebenen Adresse jedoch nicht anzutreffen war, läutete der Beamte an der benachbarten Wohnung desselben Hauses. Dort öffnete ihm ein – nach seiner Einschätzung 10 bis 12 Jahre altes – Mädchen, dem er die gespeicherten Bilder des Betroffenen zeigte. Das Mädchen bestätigte ihm gegenüber, dass es sich bei diesen Bildern um ihren Nachbarn handele.

Damit übermittelte der Beamte zum einen äußerst sensible Daten, da er nicht irgendein Lichtbild, sondern zwei aus einer erkennungsdienstlichen Behandlung stammende Lichtbilder offenbarte. Zugleich machte er damit auch noch die äußerst sensibel anzusehende Tatsache bekannt, dass der Betroffene erkennungsdienstlich behandelt ist. Neben dieser unzulässigen Datenübermittlung an Dritte wurde darüber hinaus auch noch ein Kind als Zeuge vernommen, ohne vorherige Belehrung und Zustimmung der gesetzlichen Vertreter. Aufgrund dieser gravierenden datenschutzrechtlichen Verstöße sah ich mich veranlasst, das zuständige Polizeipräsidium förmlich zu beanstanden.

3.6.3 Information einer Schule über einen Tatverdacht gegen einen Schüler

Die polizeiliche Vorgehensweise nach Erlangung eines Tatverdachts gegen einen Schüler gab im folgenden Fall Anlass zu datenschutzrechtlicher Kritik. Die Jugendbeamten einer Polizeiinspektion wurden von Kollegen einer anderen Dienststelle gebeten, die Personalien eines Jugendlichen zu ermitteln, der bis dato nur über seinen Nutzernamen und ein Bild bei Facebook bekannt war. Die Jugendbeamten

wendeten sich an die Rektorin der Schule, die der Verdächtige besuchte. Ihm war von einem Schüler einer anderen Schule angelastet worden, vor kurzem Marihuana besessen zu haben. Die Rektorin konnte das gezeigte Bild einem ihrer Schüler zuordnen und ließ ihn sogleich aus dem Unterricht holen. Noch bevor die Eltern des Schülers eintrafen, begannen die Beamten dann – im Beisein mehrerer Mitarbeiter der Schulleitung – mit der Befragung des Jugendlichen. Dass der Tatvorwurf dabei den anwesenden Lehrern bekannt wurde, liegt auf der Hand.

Die Polizei berief sich bei der insoweit erfolgten Datenübermittlung an die Anwesenden auf die Verpflichtung der Schule, einzugreifen, wenn von Schülern bekannt wird, dass diese Rauschmittel konsumieren, mit Rauschmitteln handeln, sie erwerben oder besitzen. Der Schulleitung solle so die Aufrechterhaltung der Ordnung innerhalb der Schule ermöglicht werden. Im Grundsatz kann eine zu diesem Zweck erfolgende Datenübermittlung von der Polizei an die Schulleitung nach den Bestimmungen des Polizeiaufgabengesetzes durchaus auch als vertretbar bewertet werden. Hierfür muss allerdings gegen den betroffenen Schüler ein hinreichender Tatverdacht bestehen und überdies ein konkreter Bezug zu der Schule vorhanden sein. Im vorliegenden Fall beruhte der Verdacht einzig auf der Äußerung eines Kindes, die sich letztlich nicht weiter erhärtete. Den Beamten hätte es daher oblegen, zunächst eine Abwägung der Verhältnismäßigkeit der Maßnahmen zu treffen. Insbesondere war dies in Anbetracht der zu erwartenden erheblichen schulischen Auswirkungen bei Bekanntgabe eines solchen Verdachts unverzichtbar. Nach meiner Bewertung lagen im vorliegenden Fall die Voraussetzungen für eine zulässige Weitergabe des Anfangsverdachts an die Schulleitung noch nicht vor, zumal hier nicht nur die Schulleiterin selbst, sondern auch mehrere andere Personen einbezogen wurden. Ich habe meine Auffassung dem zuständigen Polizeipräsidium mitgeteilt und darum gebeten, zukünftig gerade in solch sensiblen Fällen darauf zu achten, nicht vorschnell Verdachtsmomente gegen Schüler preiszugeben. Das eingeleitete Strafverfahren hat die Staatsanwaltschaft schließlich eingestellt.

Neben der Datenübermittlung für sich, gab der Sachverhalt zudem Anlass zur Kritik, da bei der Vernehmung des Schülers diverse Lehrer anwesend waren – aber nicht die Eltern. Die Mutter des Schülers bemängelte aus meiner Sicht zu Recht, hierdurch sei ein immenser psychischer Druck auf ihren Sohn ausgeübt worden. Gerade eine solche Situation hätte durch ein angemessenes Zuwarten der Polizei bis zum Eintreffen der Eltern vermieden werden können.

3.6.4 Weitergabe von Opferdaten

Eine Bürgerin, die zuvor einem Fahrraddieb zum Opfer gefallen war, schilderte mir folgenden Sachverhalt: Dank eines Zufalls konnte sie zu ihrer Diebstahlsanzeige noch einen wichtigen Hinweis auf den Täter nachreichen. Der wurde dann auch rasch gefasst und die junge Dame bekam ihr entwendetes Fahrrad zurück. Zu ihrem besonderen Ärgernis erhielt sie überdies aber auch einen ungewollten Anruf des Täters auf ihrem Privathandy. Der hatte die Nummer von der Polizei bekommen, um sich für seinen Diebstahl bei der Geschädigten entschuldigen zu können.

Ob diese Weitergabe der Privatnummer auch im Sinne der Bestohlenen war, hatte der Beamte zuvor nicht geprüft. Auch das zuständige Polizeipräsidium konnte für dieses Verhalten des Beamten kein Verständnis aufbringen. Es stellte im dienstrechtlichen Ermittlungsverfahren fest, dass in dem Fall offenkundig keine polizeiliche Befugnis für die Übermittlung der Handynummer an den Dieb vorgelegen

habe. Selbst wenn sich dieser tatsächlich habe entschuldigen wollen, wäre eine Weitergabe der Telefonnummer – sowohl nach meiner Bewertung als auch nach Einschätzung der Polizei – lediglich mit dem ausdrücklichen Einverständnis der Geschädigten zulässig gewesen. Da diese Zustimmung nicht vorlag und in dem betreffenden Fall auch nicht vorausgesetzt werden konnte, kamen hier sowohl ein datenschutzrechtlicher als auch ein dienstrechtlicher Verstoß zusammen, die von dem zuständigen Polizeipräsidium entsprechend geahndet wurden.

3.6.5 Öffentlichkeitsfahndung mit falschem Bild

Eine Überraschung erlebte eine Frau, als sie bei einem Blick in die Zeitung ihr eigenes Bild entdecken musste. Prekär wurde die Angelegenheit vor allem aber durch den Umstand, dass es sich dabei um ein Fahndungsfoto der Polizei handelte. So sei einer Rentnerin aus der Handtasche ihre Geldbörse entwendet worden und die mutmaßliche Diebin habe dann versucht, an einem Geldautomaten mit der gestohlenen EC-Karte Geld abzuheben. Nur – das Foto zeigte nicht den Dieb, sondern die unbescholtene Frau, wie sie an einem anderen Geldautomaten in der Bank von ihrem eigenen Konto Geld abhob.

Auf den Irrtum angesprochen musste die zuständige Polizeidienststelle eingestehen, dass eine Verwechselung der Geldautomaten bei der polizeilichen Auswertung zu dieser Panne geführt habe. Zwar entschuldigte sich die Polizei umgehend bei der unschuldig verdächtigten Frau, das bereits veröffentlichte Foto ließ sich allerdings nicht mehr zurückziehen. Nachdem mir die Polizei ausführlich geschildert hat, wie es zu der Verwechslung kommen konnte, habe ich den Vorfall zum Anlass genommen, von dem zuständigen Polizeipräsidium Maßnahmen einzufordern, die zukünftig die Gefahr der Veröffentlichung von unrichtigen Fahndungsbildern soweit wie möglich verringern. Zum einen sollten die für solche Ermittlungen in Frage kommenden Beamten regelmäßig sensibilisiert werden, zum anderen sollten Vorgesetzte gerade solche Maßnahmen ausreichend überprüfen.

3.6.6 Verwendung unverschlüsselter E-Mails

Von einer öffentlichen Stelle aus dem Bereich des Gesundheitswesens erhielt ich den Hinweis, dass Polizeidienststellen eines bestimmten Polizeipräsidiums ihre Auskunftsersuchen über bestimmte personenbezogene Daten für polizeiliche Ermittlungen vermehrt per unverschlüsselter E-Mail versenden. Gemäß den für die gesamte Bayerische Polizei geltenden EDV-Rahmenrichtlinien darf demgegenüber der gesamte polizeiliche Schriftverkehr, soweit er personenbezogene Daten enthält, nur per Post, Fax oder per E-Mail nur innerhalb des leitungsverschlüsselten Bayerischen Behördennetzes (und nur unter zusätzlichen technischen Bedingungen) übermittelt werden. Die öffentliche Stelle, von der ich den Hinweis erhielt, war jedoch nicht an das leitungsverschlüsselte Behördennetz angeschlossen. Das betreffende Polizeipräsidium habe ich daher auf die Gefahr unberechtigter Zugriffe Dritter auf derartige unverschlüsselte E-Mails der Polizei hingewiesen. Die Dienststellen im Bereich dieses Präsidiums wurden daraufhin auf diese Gefahr und die Einhaltung der geltenden Richtlinien der Polizei nochmals hingewiesen.

3.7 Ausweiskopien zum Identitätsnachweis bei Auskunftsersuchen

Das Auskunftsrecht in Art. 48 Polizeiaufgabengesetz (PAG) stellt eine spezialgesetzliche Regelung zu Art. 10 BayDSG dar. Es gewährleistet die erforderliche Transparenz, die der Betroffene einer polizeilichen Speicherung benötigt, um im Einzelfall seine Schutzrechte gegenüber der speichernden Stelle geltend machen zu können.

Art. 48 PAG Auskunftsrecht
(1) [1]Die Polizei erteilt dem Betroffenen auf Antrag über die zu seiner Person gespeicherten Daten Auskunft. [2]In dem Antrag sollen die Art der personenbezogenen Daten, über die Auskunft erteilt werden soll, und der Grund des Auskunftsverlangens näher bezeichnet werden. [3]Die Polizei bestimmt das Verfahren, insbesondere die Form der Auskunftserteilung, nach pflichtgemäßem Ermessen.
(2) Die Auskunft unterbleibt, soweit
1. eine Gefährdung der Aufgabenerfüllung durch die Auskunftserteilung, insbesondere eine Ausforschung der Polizei, zu besorgen ist,
2. die Auskunft die öffentliche Sicherheit oder Ordnung gefährden oder dem Wohle des Bundes oder eines Landes Nachteile bereiten würde, oder
3. die Daten oder die Tatsache ihrer Speicherung nach einer Rechtsvorschrift oder ihrem Wesen nach, insbesondere wegen der überwiegenden berechtigten Interessen eines Dritten, geheim gehalten werden müssen, und das Interesse des Betroffenen an der Auskunftserteilung nicht überwiegt.
(3) [1]Die Ablehnung der Auskunftserteilung bedarf keiner Begründung. [2]Wird die Auskunft verweigert, ist der Betroffene darauf hinzuweisen, dass er sich an den Landesbeauftragten für den Datenschutz wenden kann.
(4) [1]Wird dem Betroffenen keine Auskunft erteilt, so ist sie auf sein Verlangen dem Landesbeauftragten für den Datenschutz zu erteilen, soweit nicht das Staatsministerium des Innern im Einzelfall feststellt, dass dadurch die Sicherheit des Bundes oder eines Landes gefährdet würde. [2]Die Mitteilung des Landesbeauftragten an den Betroffenen darf keine Rückschlüsse auf den Erkenntnisstand der Polizei zulassen, sofern diese nicht einer weitergehenden Auskunft zustimmt.

Noch bevor die Polizei aber eine Ermessensentscheidung hinsichtlich der Auskunftserteilung im Sinne des Art. 48 PAG treffen kann, muss sie sich in ausreichender Weise davon überzeugen, dass der vorliegende Auskunftsantrag auch tatsächlich von dem genannten Betroffenen selbst oder einer berufenen Vertretung stammt. Allerdings beschwerten sich bei mir einige Bürger, dass die Polizei eine Auskunftserteilung von einer beglaubigten Ausweiskopie abhängig mache. Eine gesetzliche Festlegung, in welcher Form ein Nachweis zu erfolgen hat, sehen weder das Polizeiaufgabengesetz noch das Bayerische Datenschutzgesetz vor. In der Praxis muss also die Auskunft erteilende Stelle nach pflichtgemäßem Ermessen selbst darüber entscheiden, wie sie Auskunftserteilungen an unberechtigte Dritte vermeidet, die sich widerrechtlich im Namen des Betroffenen an die Polizei gewandt haben. Gleichzeitig soll diese Absicherung die Auskunftserteilung für den Antragsteller aber nicht in einer solchen Weise erschweren, dass er dies als Gängelung oder Schikane empfinden muss.

In der Vergangenheit hat sich für schriftliche Auskunftsersuchen an die Bayerische Polizei die Übersendung einer einfachen Ausweiskopie bewährt. In einem konstruktiven Dialog mit dem Landeskriminalamt wurde diese Auskunftspraxis nun nochmals erörtert und im Ergebnis daran festgehalten. Soweit nicht in Einzelfällen berechtigte Zweifel an der Identität des Antragstellers bestehen, wird das Landes-

kriminalamt von der Einforderung einer amtlich beglaubigten Ausweiskopie weiterhin absehen. Zum Anfertigen von Kopien des neuen Personalausweises im Allgemeinen verweise ich auf Nr. 2.1.5.

4 Verfassungsschutz

4.1 BayVSG-Änderungen bezüglich der Möglichkeit der Bestandsdatenauskunft

Der Bayerische Gesetzgeber hat in Ansehung der Entscheidung des Bundesverfassungsgerichts vom 24.01.2012 (siehe Nr. 3.1.1) auch das Bayerische Verfassungsschutzgesetz (BayVSG) geändert.

Die Bestandsdatenauskunft soll dem Landesamt für Verfassungsschutz insbesondere dazu dienen, Strukturermittlungen zu relevanten Personen und Gruppierungen sowie deren Vernetzungen untereinander zu ermöglichen.

Das BayVSG ist daher um einen neuen Art. 6g BayVSG ergänzt worden, der die Rechtsgrundlage für die Abfrage von Bestandsdaten durch das Landesamt für Verfassungsschutz darstellt. Neue Befugnisse für den Verfassungsschutz sollen damit nicht geschaffen werden.

Auch hier habe ich mich mit meiner Forderung durchsetzen können, dass zumindest für die Auskunft über sog. Zugriffssicherungscodes im Bereich des BayVSG die grundrechtssichernden Verfahrensvorschriften des Art. 6f Abs. 1 und Abs. 3 Satz 1 - 7 zur Anwendung kommen. Aus datenschutzrechtlicher Sicht kritisch bewerte ich nach wie vor die Tatsache, dass die grundrechtssichernden Verfahrensvorschriften nicht auch für eine Auskunft über sog. dynamische IP-Adressen eingeführt worden sind. Ferner ist meiner Forderung entsprechend eine Benachrichtigungspflicht für Auskünfte über Zugriffssicherungscodes und über dynamische IP-Adressen in das BayVSG aufgenommen worden

4.2 Antiterrordateigesetz

4.2.1 Folgen aus dem Urteil des Bundesverfassungsgerichts zum Antiterrordateigesetz (ATDG) vom 24.04.2013

In seinem Urteil zum Antiterrordateigesetz vom 24.04.2013 (Az.: 1 BvR 1215/ 07) hat sich das Bundesverfassungsgericht mit der Verfassungsmäßigkeit des Gesetzes über die Antiterrordatei befasst, einer Verbunddatei verschiedener Polizei- und Verfassungsschutzbehörden des Bundes und der Länder zur Bekämpfung des internationalen Terrorismus.

Darüber hinaus hat das Gericht in seinem Urteil allgemeine verfassungsrechtliche Anforderungen an die Datenübermittlung zwischen Polizei und Nachrichtendiensten aufgestellt, die von grundlegender Bedeutung sind. Diese allgemeinen Ausführungen des Bundesverfassungsgerichts legen Änderungen in den betreffenden bayerischen Fachgesetzen insbesondere im Bayerischen Verfassungsschutzgesetz nahe.

Polizei und Nachrichtendienste verfolgen unterschiedliche Aufgaben. Sie nehmen ihre Aufgaben auf unterschiedliche Art wahr und haben bei ihrer Datenerhebung

unterschiedliche Anforderungen zu beachten. Daraus folgert das Bundesverfassungsgericht, dass einer Zusammenführung von Daten und damit auch einer Datenübermittlung grundsätzlich enge Grenzen gesetzt sind. Aufgrund dieser Unterschiede zwischen Polizei und Nachrichtendiensten ergibt sich aus dem Grundrecht auf informationelle Selbstbestimmung und dem Grundsatz der Zweckbindung der erhobenen Daten ein **informationelles Trennungsprinzip** zwischen Polizeibehörden einerseits und Nachrichtendiensten andererseits. Ein Datenaustausch zwischen den Nachrichtendiensten und Polizeibehörden ist danach grundsätzlich nicht zulässig. Einschränkungen dieses Trennungsprinzips sind nur ausnahmsweise erlaubt. Soweit Einschränkungen des Trennungsprinzips zur operativen Aufgabenwahrnehmung erfolgen, liegt sogar ein besonders schwerer Eingriff vor.

Soweit der Datenaustausch zwischen Polizei und Nachrichtendienst daher „für ein mögliches operatives Tätigwerden" der Polizei erfolgt, sind somit folgende besondere verfassungsrechtliche Anforderungen zu stellen:

— der Datenaustausch hat einem herausragenden öffentlichen Interesse zu dienen, welches den Zugriff auf die unter erleichterten Bedingungen erhobenen Daten der Nachrichtendienste rechtfertigt; dies ist durch hinreichend konkrete und qualifizierte Eingriffsschwellen auf der Grundlage normenklarer gesetzlicher Regelung abzusichern

— die jeweiligen besonderen Eingriffsschwellen für die Erlangung der Daten dürfen durch den Datenaustausch nicht unterlaufen werden

Die einschlägigen Fachgesetze sind demzufolge dahingehend zu ändern, dass spezielle Datenübermittlungsregelungen für den Datenaustausch zwischen Polizei und Verfassungsschutz normiert werden müssen. Die bisherigen Regelungen genügen den im ATDG-Urteil insbesondere für eine Datenübermittlung von Nachrichtendiensten an die Polizeibehörden zur Wahrnehmung polizeilicher operativer Aufgaben aufgestellten Anforderungen nicht.

Für eine derartige Datenübermittlung an die Polizei ist in hinreichend konkreter und normenklarer Weise eine qualifizierte Einschränkung auf herausragende öffentliche Interessen als Zweck des Datenaustausches zu regeln. Zudem ist in den Normen sicherzustellen, dass die im Vergleich zu den Eingriffsbefugnissen des Verfassungsschutzes erhöhten Eingriffsschwellen, denen die Polizei bei der eigenen Datenerhebung unterliegt, nicht durch Datenübermittlungen des Verfassungsschutzes unterlaufen werden.

Ich habe gegenüber dem Staatsministerium des Innern, für Bau und Verkehr bereits zeitnah nach Verkündung des ATDG-Urteils auf den oben genannten Änderungsbedarf hingewiesen. Die dortigen Überlegungen zum Reformbedarf sind noch nicht abgeschlossen. Den weiteren Verlauf der Reformüberlegungen werde ich kritisch mitverfolgen.

4.2.2 Datenabrufe aus der Antiterrordatei (ATD)

Im Vorfeld der ATDG-Prüfung durch das Bundesverfassungsgericht (siehe Nr. 4.2.1) konnte ich mich erneut mit der Anwendung der ATD durch die Bayerischen Sicherheitsbehörden befassen. Mein besonderes Augenmerk legte ich

diesmal auf die Anwendungs- und Auswertungsmöglichkeiten der Datei im praktischen Einsatz. So zeigten unter meiner Anleitung durchgeführte Auswerteversuche beim Landesamt für Verfassungsschutz die technische Fähigkeit der ATD, Auswertungen auch mit wenigen merkmalbezogenen Grunddaten oder erweiterten Grunddaten vorzunehmen. Zum Teil ergaben sich dabei dreistellige Auswerteergebnisse. Wenngleich ich bei meiner Prüfung nicht feststellen konnte, dass die Polizei oder das Landesamt für Verfassungsschutz solche umfassenden Auswertungen vorgenommen hat, habe ich schon wegen der bestehenden technischen Möglichkeit solcher Datenabrufe Bedenken. Immerhin scheinen diese auch zu allgemeinen Rasterungen, übergreifenden Lageauswertungen oder zur reinen Verdachtsschöpfung geeignet. Die Unzulässigkeit einer solchen ATD-Anwendung hat das Bundesverfassungsgericht in seinem Urteil vom 24.04.2013, Az.: 1 BvR 1215/07, betont. Das Bundesverfassungsgericht unterstreicht damit, dass die Vorschrift stets einen konkreten Ermittlungsanlass für Abfragen voraussetzt.

Weiterhin bewertet das Bundesverfassungsgericht diese als „Inverssuche“ bezeichnete technische Auswertemöglichkeit schon grundsätzlich als unzulässig, wenn die merkmalbezogene Recherche in den erweiterten Grunddaten der abfragenden Behörde unmittelbar einen Zugang zu den einfachen Grunddaten im Trefferfall verschafft. Laut Bundesverfassungsgericht trägt eine solch weitgehende Nutzung der inhaltlichen Reichweite der erweiterten Grunddaten nicht hinreichend Rechnung. Schon die Möglichkeit der individuellen Erschließung des weitreichenden Informationsgehalts aller erweiterten Grunddaten im Rahmen von merkmalbezogenen Recherchen ist mit dem Übermaßverbot nicht vereinbar. Wenn der Gesetzgeber in diesem Umfang Daten in die Datei einzustellen anordnet, dürfen sie im Rahmen der Informationsanbahnung nur zur Ermöglichung eines Fundstellennachweises genutzt werden. Dementsprechend muss eine Nutzungsregelung so ausgestaltet sein, dass dann, wenn sich eine Recherche auch auf erweiterte Grunddaten erstreckt, nur das Aktenzeichen und die informationsführende Behörde angezeigt werden, nicht aber auch die korrespondierenden einfachen Grunddaten (Bundesverfassungsgericht, ATDG-Urteil vom 24.04.2013, Az.: 1 BvR 1215/07). Unmittelbar nach der Verkündung der Entscheidung des Bundesverfassungsgerichts wurden vom Bundesministerium des Innern bereits Sofortmaßnahmen ergriffen, die die Nutzung der ATD einschränken. Am 16.10.2014 hat der Bundestag einen Gesetzesentwurf zur Änderung des Antiterrordateigesetzes verabschiedet, der insbesondere die oben geschilderte „Inverssuche“ stark einschränkt. Bei einer Suche in den erweiterten Grunddaten ohne Angabe eines Namens wird demnach im Trefferfall nur Zugriff auf folgende Daten gewährt: Angabe der Behörde, die über die Erkenntnisse verfügt, sowie das zugehörige Aktenzeichen oder sonstige Geschäftszeichen und, soweit vorhanden, die jeweilige Einstufung als Verschlusssache.

Ein weiterer Schwerpunkt meiner diesmaligen ATD-Prüfung lag in der Kontrolle von Anfragen, die eine Freischaltung der erweiterten Grunddaten in der ATD zum Ziel hatten. Hierbei schien mir zunächst die sehr geringe Anzahl solcher Anfragen innerhalb der von mir festgelegten Kontrollgruppe überraschend. Letztendlich deckt sich diese Feststellung jedoch mit dem Bericht zur Evaluierung des Antiterrordateigesetzes der Bundesregierung (Bundestags-Drucksache 17/12665), wonach Gespräche mit den Behördenvertretern gezeigt haben, dass die erweiterten Grunddaten im Rahmen der ATD-Nutzung insgesamt keine herausragende Rolle spielen würden. Sowohl mir gegenüber bei meinen Prüfungen, als auch gegenüber den Erstellern des o.g. Evaluierungsberichts wurde als Grund hierfür genannt, dass nach einem Treffer in den Grunddaten eher eine direkte Kontaktauf-

nahme zwischen den beteiligten Behörden erfolge. Weitergehende personenbezogene Informationen – wie auch solche, die in den erweiterten Grunddaten enthalten sind – würden dann in der Regel außerhalb der ATD ausgetauscht.

Vor diesem Hintergrund beabsichtige ich bei meinen regelmäßigen Überprüfungen der ATD zukünftig auch den – nach einer ersten Kontaktanbahnung in der ATD – außerhalb der Datei erfolgenden Datenaustausch noch näher zu beleuchten. Von besonderem Interesse wird dabei sein, wie die Sicherheitsbehörden auf das vom Bundesverfassungsgericht in seinem ATD-Urteil besonders hervorgehobene informationelle Trennungsgebot zwischen Polizeibehörden und Nachrichtendiensten in der Praxis reagieren.

4.3 Dokumentenmanagementsystem (DMS)

In meinem letzten Tätigkeitsbericht (siehe 25. Tätigkeitsbericht 2012 Nr. 4.2) habe ich bereits über Prüfungsergebnisse zu dem neuen Dokumentenmanagementsystem des Landesamts für Verfassungsschutz berichtet. Eine meiner zentralen Forderungen aus Anlass der bei der Prüfung erkannten Mängel war dabei die Erstellung eines abgestuften Löschungskonzepts. Zudem sollten entsprechende technische Vorkehrungen die Mitarbeiter des Landesamts für Verfassungsschutz bei der Festsetzung der Löschungsfristen unterstützen. Nachdem diese Forderungen mit Umstellungen in der Systemsoftware verbunden sind, hat mir das Landesamt für Verfassungsschutz mittlerweile zugesichert, in der nächsten System-Version die entsprechenden Änderungen vornehmen zu lassen. Nach derzeitigem Sachstand könnten meine Forderungen dann ab Mitte des Jahres 2015 berücksichtigt werden.

Einer weiteren von mir gestellten datenschutzrechtlichen Forderung kommt das Landesamt für Verfassungsschutz bereits seit dem Jahr 2012 nach. Seither werden auch Akten, Vorgänge oder Dokumente aus dem DMS, die eine Personenrecherche im System hervorbringt, im Rahmen von Auskünften nach Art. 11 Bayerisches Verfassungsschutzgesetz mit in die Auskunftserteilung einbezogen. Bis dahin war dies nur der Fall, wenn die Person zugleich auch in IBA (Informationssystem des Landesamts für Verfassungsschutz für die Beschaffung und Auswertung) oder in NADIS (Nachrichtendienstliches Informationssystem) gespeichert war. Sonstige Speicherungen – beispielsweise nach einer nicht IBA-relevant eingestuften Mitteilung durch eine andere Behörde – die ausschließlich im DMS vorlagen, wurden in die Auskunft nicht aufgenommen.

4.4 Prüfungen

4.4.1 Datenerhebung im Zusammenhang mit dem Aussteigerprogramm Rechtsextremismus

Seit dem Jahr 2001 bietet das Landesamt für Verfassungsschutz mit der Informationsstelle gegen Extremismus ausstiegswilligen Personen Beratungs- und Unterstützungsmöglichkeiten, um sich von der rechtsextremen Szene zu lösen. Seit dem Jahr 2012 wird dieses Programm allein von der im Jahr 2009 gegründeten Bayerischen Informationsstelle gegen Extremismus (BIGE), einer beim Landesamt für Verfassungsschutz angesiedelten Stelle des Staatsministeriums des Innern, für Bau und Verkehr, verantwortet. In welchem Umfang die dabei erlangten

Erkenntnisse über Personen beim Landesamt für Verfassungsschutz gespeichert werden und ob die zu Ausstiegszwecken erlangten Daten auch zur sonstigen Aufgabenerfüllung des Landesamts für Verfassungsschutz herangezogen werden, habe ich hinterfragt.

Laut Auskunft des Landesamts für Verfassungsschutz werden die im Rahmen des Aussteigerprogramms erlangten personenbezogenen Daten lediglich im Dokumentenmanagementsystem des Landesamts für Verfassungsschutz gespeichert und nur zu Zwecken der Ausstiegshilfe verwendet. Eine Speicherung in der Amtsdatei (IBA – Informationssystem des Landesamts für Verfassungsschutz für die Beschaffung und Auswertung) oder in anderen Fachdateien findet demnach nicht statt. Zudem erfolgt die Speicherung der Daten mit der ausdrücklichen Einwilligung der Betroffenen. Die Ausstiegswilligen dokumentieren ihre Zustimmung mit ihrer Unterschrift auf einem Fragebogen, den sie zu Beginn des Programms ausfüllen.

Nach meiner Einsichtnahme in das Verfahren habe ich das Landesamt für Verfassungsschutz gebeten, diese schriftliche Einwilligung der Betroffenen an die Ausgestaltung der Einwilligungserklärung in Art. 15 BayDSG anzulehnen. Nachdem das Bayerische Verfassungsschutzgesetz (BayVSG) keine eigene Regelung für die Ausgestaltung einer Einwilligungserklärung enthält, erachte ich auch vor dem Hintergrund des Art. 10 BayVSG eine solche Handhabung aus datenschutzrechtlicher Sicht für sinnvoll. So ist laut Art. 10 BayVSG die Bestimmung aus Art. 15 BayDSG hier zwar nicht unmittelbar anwendbar, gleichwohl sollte der Betroffene jedoch unter Darlegung der Rechtsfolgen darauf hingewiesen werden, dass er die Einwilligung in die Datenerhebung – gänzlich oder teilweise – verweigern kann. Nachdem dieser Hinweis bis dahin im Fragebogen so nicht enthalten war, hat ihn das Landesamt für Verfassungsschutz nunmehr hinzugefügt.

4.4.2 Speicherung von Mandatsträgern

Das Bundesverfassungsgericht hat sich aufgrund einer Klage eines Abgeordneten der Partei Die Linke mit Beschluss vom 17.09.2013 zu den Voraussetzungen für die Beobachtung von Abgeordneten durch Behörden des Verfassungsschutzes geäußert. Die Beobachtung stellt demnach einen Eingriff in das freie Mandat dar und unterliegt strengen Anforderungen an die Verhältnismäßigkeit (Bundesverfassungsgericht, Beschluss vom 17.09.2013, Az.: 2 BvR 2436/10).

Aus diesem Anlass habe ich die Speicherungspraxis des Landesamts für Verfassungsschutz anhand der Kriterien der Entscheidung des Bundesverfassungsgerichts von Amts wegen überprüft.

Wie mir das Staatsministerium des Innern, für Bau und Verkehr mitgeteilt hat, habe das Landesamt für Verfassungsschutz im niedrigen zweistelligen Bereich Mandatsträger der Partei Die Linke gespeichert gehabt. Im Anschluss an die Entscheidung des Bundesverfassungsgerichts hat das Landesamt für Verfassungsschutz anhand der vom Gericht vorgegebenen Kriterien die Speicherungen überprüft und die Mehrzahl der Speicherungen gelöscht. Die Daten zu den verbleibenden Personen würden aufgrund ihres Bezugs zu Bayern, ihren offenen extremistischen Bestrebungen bzw. ihren Kontakten zu extremistischen Gruppen beim Landesamt für Verfassungsschutz weiterhin gespeichert werden.

In Bezug auf eine weiterhin gespeicherte Person habe ich erhebliche Zweifel an der Erforderlichkeit der weiteren Speicherung der personenbezogenen Daten geltend gemacht. Diesen Bedenken ist das Landesamt für Verfassungsschutz letztlich gefolgt und hat die Datenspeicherungen gelöscht.

4.4.3 Auskunftsverweigerungen

Zu meiner regelmäßigen Aufgabe gehört die Kontrolle von Auskunftserteilungen des Landesamts für Verfassungsschutz. So beispielsweise, wenn den Antragstellern mitgeteilt wird, über sie lägen keine Speicherungen beim Landesamt für Verfassungsschutz vor. Mehrfach habe ich mich dann bei persönlichen Besuchen davon überzeugt, dass sich in den Dateisystemen des Landesamts für Verfassungsschutz tatsächlich keine Speicherungen zu den Antragstellern recherchieren lassen. Bei keiner dieser Überprüfungen konnte ich Fehlauskünfte durch das Landesamt für Verfassungsschutz feststellen.

Ferner kommt dem Landesbeauftragten für den Datenschutz eine wesentliche Funktion zu, wenn sich das Landesamt für Verfassungsschutz gemäß Art. 11 Abs. 3 Bayerisches Verfassungsschutzgesetz (BayVSG) darauf beruft, die Auskunft an den Antragsteller aus den dort genannten Gründen zu versagen. Das Verfassungsschutzgesetz sieht in Art. 11 Abs. 4 BayVSG und das Sicherheitsüberprüfungsgesetz in Art. 28 Abs. 5 BaySÜG in solchen Fällen einer Ablehnung der Auskunft gegenüber dem Betroffenen vor, auf dessen Antrag die Auskunft zur Überprüfung an mich zu erteilen. Auch im vergangenen Berichtszeitraum habe ich auf Antrag von Betroffenen derartige Auskunftsüberprüfungen vorgenommen. Dabei konnte ich keine unzulässigen Speicherungen durch das Landesamt für Verfassungsschutz feststellen. Für die Gegebenheit, dass meine Antwort an die Betroffenen in diesen Fällen keinen Rückschluss auf den Kenntnisstand des Landesamts für Verfassungsschutz zulassen darf, sofern dieses nicht einer weitergehenden Auskunft zugestimmt hat, zeigten die Betroffenen Verständnis.

4.4.4 Datenaustausch mit ausländischen Nachrichtendiensten

Nicht zuletzt vor dem Hintergrund der öffentlichen Diskussion um die Datenausspähung durch ausländische Nachrichtendienste in Deutschland kommt der datenschutzrechtlichen Bewertung einer Zusammenarbeit zwischen deutschen und ausländischen Nachrichtendiensten besondere Bedeutung zu. Zwar fällt ein Großteil dieser Zusammenarbeit Bundesbehörden zu, gleichwohl besteht mit Art. 14 Abs. 3 Bayerisches Verfassungsschutzgesetz (BayVSG) auch für das Bayerische Landesamt für Verfassungsschutz eine Rechtsgrundlage für die Übermittlung personenbezogener Daten an ausländische Stellen.

Art. 14 BayVSG Personenbezogene Datenübermittlung durch das Landesamt für Verfassungsschutz
(3) [1]Das Landesamt für Verfassungsschutz darf personenbezogene Daten an öffentliche Stellen außerhalb des Geltungsbereichs des Grundgesetzes sowie an über- oder zwischenstaatliche öffentliche Stellen übermitteln, wenn die Übermittlung zur Erfüllung seiner Aufgaben nach diesem Gesetz oder zur Wahrung erheblicher Sicherheitsinteressen des Empfängers erforderlich ist; das Landesamt für Verfassungsschutz hat die Übermittlung aktenkundig zu machen. [2]Die Übermittlung unterbleibt, wenn auswärtige Belange der Bundesrepublik Deutschland oder überwiegende schutzwürdige Interessen der betroffenen Person entgegenstehen.

[3]Sie ist aktenkundig zu machen. [4]Der Empfänger ist darauf hinzuweisen, daß die übermittelten Daten nur zu dem Zweck verwendet werden dürfen, zu dem sie ihm übermittelt wurden.

In welchem Umfang zwischen dem Landesamt für Verfassungsschutz und ausländischen Nachrichtendiensten direkte Kontakte unterhalten werden und in welchen Fällen personenbezogene Daten – ohne vorherige Einbeziehung des Bundesamts für Verfassungsschutz – direkt mit ausländischen Nachrichtendiensten ausgetauscht werden, ließ ich mir nun vom Landesamt für Verfassungsschutz erläutern. Insgesamt vermittelte mir das Landesamt für Verfassungsschutz dabei den Eindruck, durch strikte interne administrative Regelungen der besonderen Bedeutung solcher Auslandskontakte Rechnung zu tragen. So sind in alle Vorgänge die jeweiligen Abteilungsleitungen sowie die Präsidialebene einzubinden. Soweit ich bei meiner Prüfung der Ausgestaltung der internen Regelungen Verbesserungsmöglichkeiten erkannt habe, hat mir das Landesamt für Verfassungsschutz bereits zugesichert, diese zeitnah umzusetzen.

Weiterhin habe ich für meine datenschutzrechtliche Prüfung einzelne Fallbereiche ausgewählt. Im Ergebnis kann dabei festgehalten werden, dass ich in keinem der geprüften Fälle Übermittlungen personenbezogener Daten feststellen konnte, die sich nicht im Rahmen der gesetzlichen Übermittlungsbestimmungen bewegten. Gleichwohl habe ich im Hinblick auf die erforderliche Hinweispflicht an den Datenempfänger in Art. 14 Abs. 3 Satz 4 BayVSG das Landesamt für Verfassungsschutz gebeten, den verwendeten standardisierten Hinweistext zu überarbeiten und enger an die gesetzlichen Vorgaben anzupassen. Zudem muss zur Klarstellung der Zweckbindung in den Datenübermittlungen auch der jeweils angestrebte Zweck noch deutlicher hervorgehoben werden. Das Landesamt für Verfassungsschutz hat mir zugesichert, auch diese beiden Anregungen zukünftig zu berücksichtigen.

5 Justiz

5.1 Gesetze, Rechtsverordnungen und Verwaltungsvereinbarungen

5.1.1 Allgemeines

Im Berichtszeitraum bin ich im Rahmen verschiedener Gesetzgebungsvorhaben beteiligt worden, insbesondere erneut zum neuen Bayerischen Sicherungsverwahrungsvollzugsgesetz sowie zur Änderung des Bayerischen Verwaltungszustellungs- und Vollstreckungsgesetzes. Ebenfalls habe ich mich mit Beiträgen an den Stellungnahmen des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit zum Gesetz zur Einführung der elektronischen Strafakte und zum Gesetz zur Förderung des elektronischen Rechtsverkehrs mit den Gerichten beteiligt. Im Rahmen meiner Stellungnahmen konnte ich zahlreiche Verbesserungen für den Datenschutz anregen, welche teilweise aufgegriffen wurden.

Bereits in den letzten Tätigkeitsberichten habe ich wiederholt eine normenklare Rechtsgrundlage für die Durchführung des Maßregelvollzugs in Bayern angemahnt. Das entsprechende Gesetzgebungsvorhaben, im Rahmen dessen ich bereits zu einem früheren Entwurf eines Maßregelvollzugsgesetzes Stellung bezogen habe, wurde nun mit einem neuen Gesetzesentwurf endlich wiederaufgenommen. Ich habe auch zum aktuellen Entwurf eines Bayerischen Maßregelvollzugsgesetzes (BayMRVG) Stellung genommen. Dabei habe ich zahlreiche Regelungen als datenschutzrechtlich unzureichend kritisiert und Nachbesserungen gefordert.

5.1.2 Gesetzliche Regelung des Auskunftsanspruchs über Einsichten Dritter in das Grundbuch

Zum 01.10.2014 wurde in § 12 Abs. 4 Grundbuchordnung (GBO) der Auskunftsanspruch des Eigentümers oder Inhabers eines grundstücksgleichen Rechts über Einsichten Dritter in das sein Grundstück betreffende Grundbuch oder die Erteilung von Abschriften aus diesem Grundbuch an Dritte erstmals gesetzlich geregelt. Damit ist der Gesetzgeber einer langjährigen Forderung insbesondere der Datenschutzbeauftragten des Bundes und der Länder nachgekommen. Bisher war ein solcher Auskunftsanspruch über Grundbucheinsichten lediglich für das automatisierte (elektronische) Abrufverfahren gesetzlich geregelt und damit ausdrücklich anerkannt, nicht jedoch für die herkömmliche und weit verbreitete Einsichtnahme in das Grundbuch. Dem Eigentümer wird durch diese Neuregelung ermöglicht, die Einsichtnahmen Dritter in die eigenen Daten des Grundbuchs besser kontrollieren zu können. Die Einsichtnahmen Dritter werden nunmehr mit der Bezeichnung des Datums, des Grundbuchblattes, der Einsicht nehmenden Person/Stelle, des Umfangs der Einsicht und des zugrundeliegenden berechtigten Interesses protokolliert. Der Eigentümer des betroffenen Grundstücks oder der Inhaber eines grundstücksgleichen Rechts kann grundsätzlich Auskunft aus diesen protokollierten Daten verlangen. Die Protokolldaten dürfen nur für eine solche Auskunft verwendet werden, eine andere Verwendung ist nicht zulässig. Sie wer-

den grundsätzlich nach Ablauf des zweiten auf ihre Erstellung folgenden Kalenderjahres gelöscht. Ansprechpartner für Anträge auf Auskunft aus diesen Protokolldaten ist das jeweilige Grundbuchamt. Die neuen Regelungen hierzu finden sich in § 12 Abs. 4 GBO sowie § 46a Grundbuchverfügung (GBV).

§ 12 GBO
(4) Über Einsichten in Grundbücher und Grundakten sowie über die Erteilung von Abschriften aus Grundbüchern und Grundakten ist ein Protokoll zu führen. Dem Eigentümer des betroffenen Grundstücks oder dem Inhaber eines grundstücksgleichen Rechts ist auf Verlangen Auskunft aus diesem Protokoll zu geben, es sei denn, die Bekanntgabe würde den Erfolg strafrechtlicher Ermittlungen gefährden. Das Protokoll kann nach Ablauf von zwei Jahren vernichtet werden. Einer Protokollierung bedarf es nicht, wenn die Einsicht oder Abschrift dem Auskunftsberechtigten nach Satz 2 gewährt wird.

§ 46a GBV
(1) Das Protokoll, das nach § 12 Abs. 4 der Grundbuchordnung über Einsichten in das Grundbuch zu führen ist, muss enthalten:
1. das Datum der Einsicht,
2. die Bezeichnung des Grundbuchblatts,
3. die Bezeichnung der Einsicht nehmenden Person und gegebenenfalls die Bezeichnung der von dieser vertretenen Person oder Stelle,
4. Angaben über den Umfang der Einsichtsgewährung sowie
5. eine Beschreibung des der Einsicht zugrunde liegenden berechtigten Interesses; dies gilt nicht in den Fällen des § 43.

Erfolgt die Einsicht durch einen Bevollmächtigten des Eigentümers oder des Inhabers eines grundstücksgleichen Rechts, sind nur die Angaben nach Satz 1 Nummer 1 bis 3 in das Protokoll aufzunehmen.
(2) Dem Eigentümer des jeweils betroffenen Grundstücks oder dem Inhaber des grundstücksgleichen Rechts wird die Auskunft darüber, wer Einsicht in das Grundbuch genommen hat, auf der Grundlage der Protokolldaten nach Abs. 1 erteilt. Eine darüber hinausgehende Verwendung der Daten ist nicht zulässig. Diese sind durch geeignete Vorkehrungen gegen zweckfremde Nutzung und gegen sonstigen Missbrauch zu schützen.
(3) Die Grundbucheinsicht durch eine Strafverfolgungsbehörde ist im Rahmen einer solchen Auskunft nicht mitzuteilen, wenn
1. die Einsicht zum Zeitpunkt der Auskunftserteilung weniger als sechs Monate zurückliegt und
2. die Strafverfolgungsbehörde erklärt hat, dass die Bekanntgabe der Einsicht den Erfolg strafrechtlicher Ermittlungen gefährden würde.

Durch die Abgabe einer erneuten Erklärung nach Satz 1 Nummer 2 verlängert sich die Sperrfrist um sechs Monate; mehrmalige Fristverlängerung ist zulässig. Wurde dem Grundstückseigentümer oder dem Inhaber eines grundstücksgleichen Rechts eine Grundbucheinsicht nicht mitgeteilt und wird die Einsicht nach Ablauf der Sperrfrist auf Grund eines neuerlichen Auskunftsbegehrens bekanntgegeben, so sind die Gründe für die abweichende Auskunft mitzuteilen.
(4) Nach Ablauf des zweiten auf die Erstellung der Protokolle folgenden Kalenderjahres werden die nach Abs. 1 gefertigten Protokolle gelöscht. Die Protokolldaten zu Grundbucheinsichten nach Abs. 3 Satz 1 werden für die Dauer von zwei Jahren nach Ablauf der Frist, in der eine Bekanntgabe nicht erfolgen darf, für Auskünfte an den Grundstückseigentümer oder den Inhaber eines grundstücksgleichen Rechts aufbewahrt; danach werden sie gelöscht.

(5) Zuständig für die Führung des Protokolls nach Abs. 1 und die Erteilung von Auskünften nach Abs. 2 ist der Urkundsbeamte der Geschäftsstelle des Grundbuchamts, das das betroffene Grundbuchblatt führt.
(6) Für die Erteilung von Grundbuchabschriften, die Einsicht in die Grundakte sowie die Erteilung von Abschriften aus der Grundakte gelten die Abs. 1 bis 5 entsprechend. Das Gleiche gilt für die Einsicht in ein Verzeichnis nach § 12a Abs. 1 der Grundbuchordnung und die Erteilung von Auskünften aus einem solchen Verzeichnis, wenn hierdurch personenbezogene Daten bekanntgegeben werden.

5.1.3 Vollstreckungsportal zum Online-Zugriff auf das elektronische Schuldnerverzeichnis und die Vermögensverzeichnisse

Im Berichtszeitraum wurden die gesetzlichen Regelungen zum Online-Zugriff auf das elektronische Schuldnerverzeichnis und die elektronischen Vermögensverzeichnisse in der Zwangsvollstreckung umgesetzt (siehe bereits mein 25. Tätigkeitsbericht 2012 Nr. 5.1.4). Für den gesetzlich geregelten Online-Zugriff wurde von den Ländern das bundesweite gemeinsame Vollstreckungsportal im Internet eingerichtet. Im Berichtszeitraum habe ich die Umsetzung dieses Vollstreckungsportals begleitet. So habe ich zur Dienstleistungsvereinbarung zur Errichtung und zum Betrieb des gemeinsamen Vollstreckungsportals, zur Vereinbarung über die Auftragsdatenverarbeitung mit dem Betreiber und zum entsprechenden IT-Sicherheitskonzept auf datenschutzrechtlichen Verbesserungsbedarf hingewiesen. Meine Hinweise wurden jeweils vom zuständigen Staatsministerium der Justiz aufgegriffen.

5.2 Aus der Justiz allgemein

5.2.1 Anonymisierung bei der Veröffentlichung von Gerichtsentscheidungen

Auch in diesem Berichtszeitraum habe ich mich, ausgehend von den im letzten Bericht dargelegten Grundsätzen (siehe 25. Tätigkeitsbericht 2012 Nr. 5.2.2), wieder mit der Frage der ausreichenden Anonymisierung von veröffentlichten Gerichtsentscheidungen befasst. Eine Eingabe betraf einen Rechtsstreit vor einem Verwaltungsgericht um die Besetzung des Postens als Dienststellenleiter einer Polizeiinspektion. Das Verwaltungsgericht hatte seine Entscheidung auf seiner Homepage veröffentlicht. Die Anonymisierung der Entscheidung an sich war zur Wahrung der Datenschutzrechte der darin genannten Personen ausreichend. Insbesondere wurde neben den Personalien der Betroffenen auch die konkrete Polizeiinspektion, deren Posten zu besetzen war, nicht genannt. Weitere Daten mit Gesundheitsbezug konnten hingegen nicht geschwärzt werden, ohne dass die Entscheidung ihre inhaltliche Verständlichkeit verloren hätte. Die daher erforderliche Abwägung des Gerichts ergab, dass in diesem Einzelfall das Interesse der Öffentlichkeit an der im übrigen – soweit inhaltlich ohne Defizite in der Verständlichkeit der Entscheidung möglich – anonymisierten Gerichtsentscheidung die schutzwürdigen Interessen der betroffenen Personen überwogen habe. Dieses Abwägungsergebnis habe ich nicht beanstandet. Eine Verletzung der Betroffenen in ihren Datenschutzrechten habe ich jedoch in der Verknüpfung der dargestellten veröffentlichten Entscheidung mit der Entscheidungsübersicht auf der Homepage des Gerichts gesehen. Die Entscheidungsübersicht enthielt neben dem Link auf den Wortlaut der geschwärzten Entscheidung bereits einen Kurzhinweis, in wel-

chem die Polizeiinspektion, um deren Dienstleiterposten gestritten wurde, eindeutig genannt wurde. Mit dieser zusätzlichen Information war einem außenstehenden Dritten ohne größeren Aufwand eine Identifizierbarkeit der betreffenden Person und damit letztlich auch eine Zuordnung der im Urteil enthaltenen Gesundheitsdaten möglich. Die betreffende Entscheidung wurde vom Verwaltungsgericht nach Bekanntwerden der Problematik unverzüglich von seiner Homepage entfernt. Ich habe daher von einer förmlichen Beanstandung abgesehen. Das Verwaltungsgericht habe ich jedoch auf diese Datenschutzverletzung hingewiesen und es im Hinblick auf eine Verknüpfung des anonymisierten Urteils mit einem nicht ausreichend anonymisierten Übersichtshinweis für die Zukunft um eine striktere Beachtung der Datenschutzrechte der Betroffenen angehalten.

5.2.2 Zugangskontrollen in Gerichten und Aufzeichnung der dabei erhobenen personenbezogenen Daten in Wachbüchern

In den Gerichten werden an den Eingängen regelmäßig allgemeine Zugangskontrollen durchgeführt. Diese Zugangskontrollen beruhen nach gefestigter Rechtsprechung auf dem Hausrecht des Gerichtspräsidenten bzw. des Direktors des Gerichts. Das Hausrecht gestattet zur Gewährleistung eines ordnungsgemäßen Dienstbetriebes verhältnismäßige Maßnahmen zur Aufrechterhaltung der Sicherheit und Ordnung im Gerichtsgebäude, wie z.B. das Passieren eines Metalldetektorrahmens mit den damit verbundenen Begleitanordnungen. Eine solche Maßnahme habe ich aufgrund einer Eingabe überprüft, welche die Zugangskontrolle bei einem bayerischen Sozialgericht betraf. Die Maßnahmen, die im Rahmen der Zugangskontrollen auf der Grundlage des Hausrechts getroffen wurden, waren in diesem konkreten Fall datenschutzrechtlich nicht zu beanstanden. Es stellte sich jedoch heraus, dass anlässlich der Vorkommnisse bei der konkreten Zugangskontrolle neben der Beschreibung des Sachverhalts und der getroffenen Maßnahmen auch die – zulässiger Weise – erhobenen Personalien des Petenten im Wachbuch des kontrollierenden Sicherheitsdienstes aufgezeichnet wurden. In diesem Zusammenhang habe ich es für kritisch erachtet, dass die Wachbücher zur Evaluierung des Sicherheitsdienstes über längere Zeit aufbewahrt werden, ohne dass es eine klare Regelung über die Dauer der Aufbewahrung sowie die Löschung der personenbezogenen Daten in den Wachbüchern gibt. Meine Bedenken habe ich dem betreffenden Sozialgericht mitgeteilt, worauf sich sämtliche Gerichte der bayerischen Sozialgerichtsbarkeit auf einer Dienstbesprechung mit diesem Thema beschäftigt haben. Die Gerichte der Sozialgerichtsbarkeit kamen dabei überein, die personenbezogenen Daten bei besonderen Vorkommnissen vorzugswürdig nur noch in die erforderlichen Meldungen an die Gerichtsverwaltung, hingegen nicht mehr zusätzlich in die Wachbücher aufzunehmen. Es gibt allerdings auch Fälle, in denen das Wachpersonal personenbezogene Daten aus anderen Anlässen in den Wachbüchern vermerken muss. Solche aus Zugangskontrollen gewonnene Daten sollen künftig nur noch vorübergehend, regelmäßig bis zum Ende des auf die Erhebung folgenden Jahres aufbewahrt und danach entnommen bzw. geschwärzt werden. Die neu gewonnene Haltung der Sozialgerichtsbarkeit begrüße ich ausdrücklich, weil sie den datenschutzrechtlichen Belangen der betroffenen Personen nunmehr in höherem Maße gerecht wird.

5.2.3 Übersendung von Telefaxen an falschen Empfänger

Eine Staatsanwaltschaft versandte ein Telefax mit teils äußerst sensiblen Daten über den Betroffenen (Prognose weiterer Straffälligkeit, Angaben zur Alkohol-

und Sexualproblematik) statt an die zuständige Dienststelle der Polizei, welche unter einem Kürzel bekannt ist, an eine mit dem üblichen Kürzel dieser Dienststelle namensähnliche Privatfirma. Nachdem ich davon erfahren habe, habe ich mich an die betreffenden Justizbehörden gewandt, um weitere Verwechslungen in Zukunft zu verhindern. Wie sich herausstellte, hatte im vorliegenden Fall der Staatsanwalt die Übermittlung der Unterlagen an die betreffende Polizeidienststelle per Telefax verfügt. Er hatte dabei jedoch die entsprechende Faxnummer nicht angegeben und die Dienststelle nur unter dem allgemein üblichen Kürzel genannt. Ein Mitarbeiter der Geschäftsstelle, der diese Verfügung ausführen wollte, ermittelte die erforderliche Faxnummer eigenmächtig durch eine Recherche über eine Suchmaschine im Internet. Im Rahmen seiner Recherche geriet der Mitarbeiter jedoch an die namensähnliche Privatfirma, die er fälschlicherweise mit dem verfügten Empfänger-Kürzel gleichsetzte. Auf diese Weise wurde das Telefax mit sensiblen Daten des Betroffenen an die Privatfirma übersandt, die mit dem Verfahren oder dem Betroffenen in keinerlei Zusammenhang stand. Anlässlich dieses Vorfalls wurden inzwischen diverse Vorkehrungen organisatorischer Art sowohl im Bereich der betreffenden Staatsanwaltschaft als auch darüber hinaus seitens des Staatsministeriums der Justiz für ganz Bayern getroffen, um eine solche Verwechslung für die Zukunft zu verhindern.

Der Fall zeigt jedoch allgemein über den konkreten Anlass hinaus, dass besondere Sorgfalt nicht nur bei der Eingabe der korrekten Faxnummer in das Faxgerät notwendig ist, sondern auch bereits bei der Ermittlung der zutreffenden Faxnummer. Besondere Vorsicht ist bei einer Recherche nach einem (unbekannten) Empfänger im Internet und einer allzu unkritischen Übernahme eines vermeintlich passenden Rechercheergebnisses geboten.

5.3 Strafverfolgung

5.3.1 Öffentlichkeitsfahndung mit Hilfe sozialer Netzwerke

Auf meine Bedenken gegen eine Öffentlichkeitsfahndung auch in sozialen Netzwerken habe ich bereits in der Vergangenheit hingewiesen (siehe 25. Tätigkeitsbericht 2012 Nr. 3.14). Die Thematik besitzt nach wie vor größte Aktualität. Seitens der Innen- und Justizministerkonferenz bestehen derzeit konkrete Bestrebungen, die Öffentlichkeitsfahndung auch in sozialen Netzwerken näher zu regeln. Hierzu soll die betreffende Regelung der Richtlinien für das Straf- und Bußgeldverfahren Anlage B Ziffer 3.2 geändert werden, die einer Öffentlichkeitsfahndung in sozialen Netzwerken bislang entgegenstand (siehe 25. Tätigkeitsbericht 2012 Nr. 3.14).

Die Datenschutzbeauftragten des Bundes und der Länder haben sich auf ihrer 87. Konferenz am 27./28.03.2014 mit der Thematik befasst und mit der nachstehenden Entschließung strenge Vorgaben für eine Öffentlichkeitsfahndung in sozialen Netzwerken aufgestellt.

Entschließung der 87. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 27./28.03.2014
Öffentlichkeitsfahndung mit Hilfe sozialer Netzwerke – Strenge Regeln erforderlich!

Mit zunehmender Beliebtheit sozialer Netzwerke bei Bürgerinnen und Bürgern steigt das Interesse von Strafverfolgungsbehörden, diese sozialen Netzwerke auch

zur Öffentlichkeitsfahndung zu nutzen. So gibt es in Deutschland bereits Polizeidienststellen, die mittels Facebook nach Straftätern suchen. Auch die 84. Konferenz der Justizministerinnen und Justizminister hat sich im November 2013 mit dem Thema befasst.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hält es erneut für notwendig darauf hinzuweisen, dass eine Nutzung sozialer Netzwerke privater Betreiber (wie z.B. Facebook) zur Öffentlichkeitsfahndung aus datenschutzrechtlicher Sicht sehr problematisch ist. Durch die weltweit recherchierbare Veröffentlichung von Fahndungsdaten wird in weitaus schwerwiegenderer Weise in die Grundrechte Betroffener (Tatverdächtiger oder auch Zeugen) eingegriffen, als dies bei der Nutzung klassischer Medien der Fall ist. Auch sind im Internet veröffentlichte Daten einer Fahndungsausschreibung nur sehr schwer bzw. gar nicht mehr zu löschen. Geben Nutzerinnen und Nutzer der Sozialen Netzwerke in Diskussionsforen und Nutzerkommentaren öffentlich Spekulationen, Behauptungen und Diskriminierungen ab, beeinträchtigt dies die Persönlichkeitsrechte der Betroffenen erheblich. Solche Funktionen sind in von den Ermittlungsbehörden betriebenen Angeboten weder geeignet noch erforderlich, um die behördlichen Aufgaben zu erfüllen. Die Konferenz weist darauf hin, dass Öffentlichkeitsfahndung nur auf Diensten von Anbietern erfolgen darf, die die datenschutzrechtlichen Vorgaben des Telemediengesetzes zur Nutzungsdatenverarbeitung, insbesondere der Regeln zur Reichweitenmessung gemäß §§ 13 Abs. 4 Nr. 6, 15 Abs. 3 TMG, und das Recht auf anonyme und pseudonyme Nutzung gemäß § 13 Abs. 6 TMG beachten.

Sofern es Strafverfolgungsbehörden gleichwohl gestattet werden soll, zu Zwecken der Öffentlichkeitsfahndung auf soziale Netzwerke mit deaktivierter Kommentierungsfunktion zurückzugreifen, so darf dies – ungeachtet der generellen Kritik an der Nutzung sozialer Netzwerke durch öffentliche Stellen – nur geschehen, wenn folgende Maßgaben beachtet werden:

- *Die Vorschriften der Strafprozessordnung (§ 131 Abs. 3, § 131a Abs. 3, § 131b StPO) zur Öffentlichkeitsfahndung kommen aufgrund der technikoffenen Formulierung als Rechtsgrundlage für die Öffentlichkeitsfahndung im Internet grundsätzlich in Betracht. Sie sind aber im Hinblick auf den Verhältnismäßigkeitsgrundsatz nur eingeschränkt anzuwenden. Eine entsprechende Klarstellung durch den Gesetzgeber wäre wünschenswert. Zumindest aber sind die besonderen Voraussetzungen der Fahndung im Internet, insbesondere in sozialen Netzwerken in Umsetzungsvorschriften zu konkretisieren. Änderungsbedarf besteht beispielsweise für die Anlage B der RiStBV.*

- *In materiell-rechtlicher Hinsicht haben die Strafverfolgungsbehörden den Verhältnismäßigkeitsgrundsatz strikt zu beachten. Die zu schaffenden Regelungen müssen den besonderen Gefahren der Öffentlichkeitsfahndung in sozialen Netzwerken gerecht werden. Insbesondere muss sichergestellt werden, dass eine solche Fahndung nur bei im Einzelfall schwerwiegenden Straftaten überhaupt in Betracht gezogen werden kann.*

- *In verfahrensrechtlicher Hinsicht müssen die Umsetzungsregelungen die Staatsanwaltschaft verpflichten, bereits im Antrag auf richterliche Anordnung der Maßnahme die Art, den Umfang und die Dauer der Öffentlich-*

keitsfahndung konkret anzugeben. Dies umfasst insbesondere die ausdrückliche Angabe, ob und warum die Anordnung auch die Öffentlichkeitsfahndung in sozialen Netzwerken umfassen soll.

- *Es ist sicherzustellen, dass*
  - *die zur Öffentlichkeitsfahndung verwendeten personenbezogenen Daten von den Strafverfolgungsbehörden ausschließlich auf im eigenen Verantwortungsbereich stehenden Servern gespeichert und verarbeitet werden, nicht hingegen auf Servern der privaten Anbieter*
  - *die Weitergabe und der automatisierte Abruf der personenbezogenen Daten aus dem Internet durch Web-Crawler und ähnliche Dienste so weit als technisch möglich verhindert werden*
  - *die Kommunikation zwischen den Strafverfolgungsbehörden und den Nutzern nur außerhalb der sozialen Netzwerke erfolgt*

5.3.2 Geldwäscheverdachtsmeldung

Das Geldwäschegesetz verpflichtet bestimmte Personen und Unternehmen (wie u.a. Kreditinstitute) bei tatsächlichen Anhaltspunkten, die darauf hindeuten, dass eine von ihnen auszuführende Transaktion mit einer Geldwäsche oder der Terrorismusfinanzierung im Zusammenhang steht, die Transaktion an das Bundeskriminalamt – Zentralstelle für Verdachtsmeldungen – und die zuständige Strafverfolgungsbehörde zu melden (§ 11 Geldwäschegesetz – GWG). Im Regelfall kommen die nach dieser Norm Verpflichteten mit dieser sogenannten Geldwäscheverdachtsmeldung lediglich ihrer gesetzlichen Pflicht zur Meldung nach. Sie betrachten sich dabei nicht notwendigerweise auch als Geschädigte einer Straftat oder als Anzeigeerstatter eines strafbaren Sachverhalts und besitzen demgemäß nicht ohne weiteres ein eigenes Strafverfolgungsinteresse. Dennoch wurden die Absender der Geldwäscheverdachtsmeldung von den für die Prüfung der Verdachtsmeldung zuständigen Generalstaatsanwaltschaften bislang in der Regel wie Anzeigeerstatter einer Strafanzeige behandelt. Aufgrund dessen wurden den meldenden Personen und Unternehmen vielfach neben einer Eingangsbestätigung im folgenden personenbezogene Daten über den weiteren Verfahrensgang betreffend die gemeldeten Personen mitgeteilt, die auch ein daraus hervorgehendes Strafverfahren einschließen konnten. Bei mehreren hiervon betroffenen Petenten, die als Absender einer Geldwäscheverdachtsmeldung als Anzeigeerstatter einer Strafanzeige behandelt wurden und solche weitergehenden Informationen zum Verfahrensfortgang gegen die von ihnen gemeldeten Personen und Transaktionen erhielten, führte diese Handhabung zu großer Verunsicherung.

Vor dem Hintergrund dieser Problematik habe ich dem Staatsministerium der Justiz gegenüber meine Einwände gegen eine regelmäßige Gleichstellung von Anzeigeerstattern einer Strafanzeige mit einem Interesse zur Strafverfolgung sowie zur Information über den Verfahrensfortgang einerseits und den gesetzlich hierzu verpflichteten Absendern einer bloßen Geldwäscheverdachtsmeldung andererseits dargelegt. Ich konnte erreichen, dass in der Praxis der Information über den Verfahrensfortgang nunmehr deutlicher zwischen einer bloßen Geldwäscheverdachtsmeldung und einer Strafanzeige unterschieden wird. Die jeweiligen bayernweit verwendeten Vordrucke und Hinweise wurden entsprechend angepasst. Nunmehr wird ausdrücklich hervorgehoben, dass über die einfache Bestätigung

des Eingangs einer Geldwäscheverdachtsmeldung hinaus Mitteilungen über den Verfahrensfortgang an die meldende Stelle nur in zwei Fallgestaltungen zu erfolgen habe: Zum einen, wenn die meldende Stelle ein berechtigtes Interesse daran zur Überprüfung ihres Meldeverhaltens kundgetan hat, wie es in § 11 Abs. 8 Satz 3 GWG vorgesehen ist. Zum anderen aufgrund der Regelung des § 171 Strafprozessordnung, wenn sich aus der Verdachtsmeldung der erkennbare Wille der meldenden Stelle ergibt, auch die strafrechtliche Verfolgung der gemeldeten Person veranlassen zu wollen. Auf diese beiden Fallkonstellationen wird zudem die meldende Stelle bereits in der Eingangsbestätigung hingewiesen.

Die Persönlichkeitsrechte der von der Meldung betroffenen Personen werden durch diese Änderung nun stärker gewahrt. Gleichzeitig wird berücksichtigt, dass die meldende Stelle mit ihrer Meldung im Regelfall nur ihren gesetzlichen Verpflichtungen nach dem Geldwäschegesetz nachkommen möchte, ohne ihrem Kunden gegenüber als Anzeigeerstatter einer Strafanzeige gelten zu wollen.

5.3.3 Übersendung von Akten der Staatsanwaltschaft an andere Behörde durch Mitarbeiter der Registratur

Eine Staatsanwaltschaft hat Teile der Akte (Anklageschrift und Urteil) eines abgeschlossenen Strafverfahrens an ein Jugendamt übersandt. Dem lag ein Ersuchen des Jugendamts auf Übermittlung dieser Aktenteile zugrunde. Anlässlich einer Eingabe des in diesem Verfahren damaligen Beschuldigten habe ich diese Datenübermittlung geprüft. Die Übersendung der Aktenteile an das Jugendamt auf deren Ersuchen war in diesem konkreten Fall von einer einschlägigen Übermittlungsvorschrift gedeckt. Bemängelt habe ich jedoch, dass die Übersendung in Fehlauslegung einer internen Regelung durch einen Justizangestellten der Registratur der Staatsanwaltschaft erfolgte, ohne dass hierüber zuvor eine Entscheidung etwa eines Staatsanwalts eingeholt wurde. Aufgrund der häufig sehr komplexen gesetzlichen Vorschriften zur Übermittlung von Akten/-teilen an private wie auch öffentliche Stellen und der in diesem Zusammenhang notwendigen rechtlichen Prüfungen sollte die Entscheidung über die Übermittlung grundsätzlich von einem entsprechend hierfür geschulten Mitarbeiter der Staatsanwaltschaft, im Idealfall einem Staatsanwalt, getroffen werden. Ausnahmen können allenfalls für eindeutige sich oft wiederholende Standardfälle von Übermittlungen an bestimmte Behörden zu bestimmten Zwecken gelten. Die Staatsanwaltschaft hat ihre Beschäftigten entsprechend angewiesen.

5.3.4 Einschaltung privater Stellen zur Vermittlung und Überwachung von gemeinnützigen Auflagen im Strafverfahren

Dem Beschuldigten eines Strafverfahrens kann seitens der Staatsanwaltschaft insbesondere im Rahmen einer Einstellung gemäß § 153a Strafprozessordnung zur Auflage gemacht werden, Arbeitsstunden in einer gemeinnützigen Einrichtung abzuleisten. Derartige gemeinnützige Arbeitsleistungen können auch von Gerichten einem Angeklagten im Rahmen von gerichtlichen Verfahrenseinstellungen oder Bewährungsauflagen zur Auflage gemacht werden. Dabei betrauen Gerichte und Staatsanwaltschaften teilweise spezielle private Stellen, wie Vereine aus dem sozialen Bereich, mit der Vermittlung der gemeinnützigen Arbeitsstelle und der Überwachung der Auflagenerfüllung. Zum Zwecke dieser Aufgaben werden den privaten Vermittlungsstellen Daten über den Betroffenen mitgeteilt.

Die Einschaltung der privaten Vermittlungsstelle und die Datenübermittlung an diese Stelle zur Vermittlung der gemeinnützigen Arbeitsstelle und Überwachung der Auflage halte ich an sich datenschutzrechtlich für zulässig. Eine spezielle Vermittlungsstelle kann die Zuweisung einer möglichen und für den Betroffenen geeigneten Arbeitsstelle sowie die Überwachung der Auflagenerfüllung in der Regel in besserem Maße gewährleisten als die Justizbehörden selbst. Jedoch ist bei solchen Datenübermittlungen sorgfältig darauf zu achten, dass nur diejenigen Daten an die private Vermittlungsstelle weitergegeben werden, welche die Stelle zur Vermittlung der gemeinnützigen Arbeit und zur Überwachung der Erfüllung benötigt. Die Gerichte und Staatsanwaltschaften in Bayern haben den Umfang der übermittelten Daten nach Auskunft des Staatsministeriums der Justiz bislang teilweise unterschiedlich gehandhabt, insbesondere was die Daten zum Tatvorwurf anbelangt. Ich habe gegenüber dem Staatsministerium dargelegt, dass ich eine regelmäßige Übermittlung des Tatvorwurfs im Gegensatz zu den zur Vermittlung einer geeigneten Arbeitsstelle notwendigen Daten – wie Name, Vorname, Geburtsdatum, Anschrift, Aktenzeichen, angeordnete Auflage, Frist für die Auflage – nicht für erforderlich und damit nicht für zulässig halte. Die Übermittlung bestimmter Tatvorwürfe bzw. bestimmter tat- oder täterbezogenen Besonderheiten kann hingegen zulässig sein, sofern sie sich auf den Zweck der Einschaltung privater Stellen, nämlich die Vermittlung einer geeigneten Stelle zur Auflagenerbringung, unmittelbar auswirken könnte. Gerade sofern aus dem Tatvorwurf die Gefahr eines Risikos für die vermittelte Einrichtung oder auch für den Beschuldigten/Angeklagten selbst folgt, kann die Mitteilung auch des Tatvorwurfs an die Vermittlungsstelle zur Bestimmung der geeigneten Arbeitsstelle erforderlich sein. Zu denjenigen Fällen, in denen die Übermittlung des bestehenden Tatvorwurfs häufig erforderlich sein kann, zählen insbesondere Straftaten gegen Kinder im Hinblick auf eine gemeinnützige Arbeit in Kinder- und Jugendeinrichtungen oder Betäubungsmittelstraftaten und Diebstahlsstraftaten im Hinblick auf eine Arbeit in Alten- und Pflegeheimen oder sonstigen medizinischen Einrichtungen. Auch in diesen Fällen halte ich jedoch die Übermittlung beispielsweise eines kompletten Strafurteils in den Fällen einer Bewährungsauflage in der Regel nicht für erforderlich. Eine solche Übermittlung an die private Vermittlungsstelle, die über die bloße Mitteilung des Tatvorwurfs weit hinaus geht und regelmäßig zahlreiche Informationen enthält, die für die Vermittlung einer geeigneten Stelle nicht erforderlich sind, kann allenfalls in Ausnahmefällen bei Hinzutreten besonderer Umstände erforderlich und damit datenschutzrechtlich zulässig sein.

Das Staatsministerium teilte mir mit, dass meine oben skizzierte Bewertung zum Umfang der Datenübermittlung mit den Behördenleitern der Staatsanwaltschaften und den Präsidenten der Gerichte erörtert wurde und man dabei übereinkam, künftig im Sinne meiner Bewertung zu verfahren.

5.3.5 Mitteilungen der Staatsanwaltschaft an die Polizei über den Verfahrensabschluss

Im Rahmen meiner Prüfung der Speicherungen in polizeilichen Dateien unter dem Gesichtspunkt des polizeilichen Restverdachts (siehe Nr. 3.5.3) habe ich auch die Mitteilungen der Staatsanwaltschaft über den Ausgang der betreffenden Strafverfahren im Bereich zweier Staatsanwaltschaften überprüft. Um der Polizei die datenschutzkonforme Verarbeitung der Verfahrensausgänge in den polizeilichen Dateien zu ermöglichen, ist es von großer Bedeutung, dass die Ausgangsmitteilungen stets an die ermittelnde Polizeidienststelle gelangen. Zudem ist inhaltlich insbesondere darauf zu achten, bei Einstellung mit der ausdrücklichen

Feststellung „unschuldig“ oder „kein begründeter Tatverdacht“ die Ausgangsmitteilung mit diesem Zusatz bzw. mit den Gründen der Einstellung zu versehen. Der Inhalt der Ausgangsmitteilung der Staatsanwaltschaft entscheidet darüber, ob die Polizei überhaupt in die Lage versetzt wird, ihre Entscheidung über die weitere Speicherung in ihren Dateien entsprechend den gesetzlichen Vorgaben und damit datenschutzgerecht treffen zu können.

Den geprüften Staatsanwaltschaften gegenüber habe ich die Wichtigkeit korrekter Ausgangsmitteilungen hervorgehoben, auf die von mir festgestellten, in Einzelfällen unvollständigen Ausgangsmitteilungen habe ich hingewiesen. Auch habe ich die Staatsanwaltschaften dafür sensibilisiert, dass bei Einstellungen mit der Feststellung „unschuldig“ oder „kein begründeter Tatverdacht“ zusätzlich in der Verfahrensdatei der Staatsanwaltschaft eine Datensperre zu verhängen ist.

5.3.6 Neue Informationen zu verschiedenen Datenschutzthemen auf meiner Homepage

Ausgehend von wiederholten Bürgeranfragen zu bestimmten Themen habe ich mein Informationsangebot auf meiner Homepage https://www.datenschutz-bayern.de für den Bereich der Justiz, insbesondere im Bereich der Strafverfolgung, wesentlich verbessert. So habe ich unter „Häufige Fragen“ – „Justiz“ die wichtigsten Register der Justiz zur Strafverfolgung näher dargestellt, wobei ich jeweils auch auf das Recht auf Selbstauskunft eingehe. An gleicher Stelle finden sich Hinweise zu den Geschäftsverteilungsplänen der Gerichte und der Frage, inwieweit diese von Bürgern eingesehen werden können.

Im Bereich der Strafverfolgung kann für eine Vielzahl von Bürgern gegebenenfalls eine Beteiligung an einem Reihengentest (auch Massengentest genannt) in Frage kommen. Nähere Informationen zum Ablauf eines solchen Reihengentests und zur Speicherung und Verarbeitung des entnommenen DNA-Materials und der dabei gewonnenen Daten habe ich daher auf meiner Homepage unter „Themen“ – „Polizei“ – „Reihengentest“ eingestellt.

5.4 Strafvollzug

5.4.1 Telefonate mit Verteidigern

Soweit Gefangenen erlaubt wird, in der Justizvollzugsanstalt ein Telefonat mit ihren Verteidigern zu führen, darf der Inhalt des Telefonats nicht überwacht werden. Für den Strafvollzug ist dies in Art. 35 Abs. 1 Satz 2 in Verbindung mit Art. 30 Abs. 5 Bayerisches Strafvollzugsgesetz geregelt, für den Vollzug von Untersuchungshaft folgt dies aus Art. 22 Abs. 1 Satz 1 Bayerisches Untersuchungshaftvollzugsgesetz. Meine Anfrage an das Staatsministerium der Justiz über die Handhabung von Telefonaten der Gefangenen mit ihren Verteidigern vor dem Hintergrund dieser Rechtslage hat ergeben, dass in einigen Justizvollzugsanstalten Telefonate mit den Verteidigern in der Vergangenheit dennoch inhaltlich überwacht wurden. In diesen Fällen fand das Telefonat in einem Dienstzimmer im Beisein eines Bediensteten statt, der jedenfalls den Gesprächsbeitrag des telefonierenden Gefangenen im Raum mithören konnte. Auch wenn die Gesprächsteilnehmer vor dem Gespräch auf diese Überwachung hingewiesen werden, so widerspricht eine sol-

che Überwachung von Verteidigertelefonaten eindeutig der gesetzlichen Regelungslage und missachtet das besonders schützenswerte Vertrauensverhältnis des Gefangenen zu seinem Verteidiger. Meine entsprechende Rechtsauffassung wird vom Staatsministerium geteilt. Wie mir mitgeteilt wurde, wurde zwischenzeitlich in allen bayerischen Justizvollzugsanstalten den Gefangenen die Möglichkeit geschaffen, genehmigte Telefonate mit ihren Verteidigern ohne inhaltliche Überwachung zu führen. Hierfür wurden die Justizvollzugsanstalten mit schnurlosen Telefonen ausgestattet, auf die im Bedarfsfall die Telefonate mit den Verteidigern nach Vermittlung der Gespräche durch die Justizvollzugsanstalt gelegt werden können. Entgegen der zuvor teilweise bestehenden Praxis können diese Telefonate somit unbeaufsichtigt, etwa in einem Besuchsraum o.ä. erfolgen. Meinem Anliegen, inhaltlich unüberwachte Telefonate mit den Verteidigern sicherzustellen, wurde damit in zufriedenstellender Weise Rechnung getragen.

Die Einhaltung der gesetzlichen Vorschriften sowie die gegenwärtige Handhabung zur Gewährleistung unüberwachter Verteidigertelefonate überprüfe ich laufend im Rahmen meiner regelmäßigen datenschutzrechtlichen Kontrollen der Justizvollzugsanstalten vor Ort. Soweit es im Einzelfall mitunter noch zu einer abweichenden Praxis kommen sollte, bestehe ich auf eine Änderung der Handhabung und auf die Beachtung der gesetzlichen Vorschriften.

5.4.2 Erhebung und Aufbewahrung von Daten in Mutter-Kind-Abteilungen

Wird gegen eine Mutter Strafhaft vollzogen, kann unter bestimmten Voraussetzungen auch deren Kind (im Säuglings- oder Kleinkindalter) zusammen mit ihr in der Justizvollzugsanstalt untergebracht werden, wenn dies dem Kindeswohl entspricht. Geregelt ist dies in Art. 86 des Bayerischen Strafvollzugsgesetzes (BayStVollzG). Dies geschieht in speziellen Mutter-Kind-Abteilungen, in denen auch die Versorgung und Betreuung der Kinder sichergestellt werden kann. In Bayern gibt es zwei derartige Abteilungen.

Art. 86 BayStVollzG Besondere Vorschriften für den Frauenstrafvollzug – Mütter mit Kindern
(1) Ist das Kind einer Gefangenen noch nicht schulpflichtig, so kann es mit Zustimmung der aufenthaltsbestimmungsberechtigten Person in der Anstalt untergebracht werden, in der sich seine Mutter befindet, wenn dies seinem Wohl entspricht. Vor der Unterbringung ist das Jugendamt zu hören.

Beide bayerischen Mutter-Kind-Abteilungen habe ich im Berichtszeitraum vor Ort geprüft. Dabei habe ich neben Themen, die allgemein alle Strafvollzugsanstalten betreffen, wie etwa die Videoüberwachung, mein Augenmerk vor allem auf die Besonderheiten der Mutter-Kind-Unterbringung gelegt. Im Gegensatz zu seiner Mutter ist das Kind kein Strafgefangener und lediglich aus sozialen Gründen wie aus Gründen des Kindeswohls für eine bestimmte Zeit dort mit seiner Mutter untergebracht. Dementsprechend darf das Kind auch nicht als Strafgefangener behandelt werden.

Vor diesem Hintergrund habe ich insbesondere die Erhebung und Übermittlung von Daten über das Kind durch die Anstalt überprüft, ebenso wie die Kontaktmöglichkeiten des Kindes zu Personen wie Verwandten außerhalb der Anstalt. Soweit Daten über das Kind erhoben werden, ist besonders streng darauf zu achten, stets nur diejenigen Daten zu erheben, die für die gemeinsame Unterbringung des Kindes mit seiner Mutter in der Anstalt auch erforderlich sind. Soweit Daten über das

Kind zulässigerweise erhoben wurden, ist strikt darauf zu achten, dass nur die berechtigten Personen in der Mutter-Kind-Abteilung auf diese Daten Zugriff nehmen können und ein Zugriff Unberechtigter ausgeschlossen wird. Ich konnte in diesem Zusammenhang anlässlich meiner Prüfung Verbesserungen in der Art der Aufbewahrung der Kinderakten erzielen.

Bei den Kinderunterlagen stellte sich zudem die Problematik der Aufbewahrungsdauer nach Haftentlassung der Mutter. Die Unterlagen über das Kind werden nicht in den Gefangenenpersonalakten aufbewahrt und unterfallen daher nicht ohne weiteres den Aufbewahrungs- und Vernichtungsregelungen, wie sie für die Gefangenenpersonalakten gelten. Eine verbindliche schriftliche Regelung über die Aufbewahrungsdauer- und Vernichtung der Kinderakten gab es in den von mir geprüften Mutter-Kind-Abteilungen bisher nicht. Die beteiligten Anstalten kamen meinem Wunsch nach einer verbindlich fixierten Regelung dieser Thematik nach. Dabei konnte ich mit den Anstalten eine datenschutzgerechte Lösung erzielen, die die einzelnen schutzwürdigen Belange der Beteiligten in einen angemessenen Ausgleich bringt. Danach werden die Akten mit den Unterlagen über das Kind nach der Haftentlassung der Mutter noch für ein Jahr aufbewahrt. Diese Aufbewahrungsdauer ist erforderlich, weil Jugendämter, Vollstreckungsbehörden oder andere beteiligte Stellen in diesem Zeitraum wiederholt Rückfragen nach der Situation und den Verhältnissen des Kindes während der Mutter-Kind-Unterbringung an die Anstalt richten, die sie ohne die Kinderakten nicht sachgerecht beantworten könnte. Nach Ablauf dieses Jahres nach Haftentlassung werden die Kinderakten vernichtet.

5.4.3 Schriftsätze an Gerichte

Soweit Schriftsätze an ein Gericht gehen, ist stets damit zu rechnen, dass diese aus prozessualen Gründen vom Gericht auch an den jeweiligen Prozessgegner übermittelt werden, damit dieser vom Inhalt des Schriftsatzes Kenntnis nehmen und gegebenenfalls darauf reagieren kann. Dies hat eine Justizvollzugsanstalt nicht beachtet, wie mir im Rahmen einer Eingabe eines Strafgefangenen bekannt wurde. Die betreffende Justizvollzugsanstalt wurde von zwei Strafgefangenen in unterschiedlichen Gerichtsverfahren unabhängig voneinander vor demselben Gericht verklagt. Um in den beiden Verfahren jeweils eine Fristverlängerung bei Gericht zu beantragen, versandte die Anstalt ein einziges gemeinsames Schreiben an das Gericht, obwohl es sich um unterschiedliche Verfahren und damit unterschiedliche Prozessgegner handelte. Die Anstalt erstellte den gemeinsamen Antrag aus verfahrensökonomischen Gründen. Es wurde dabei jedoch nicht bedacht, dass Schriftsätze an das Gericht (auch bloße Fristverlängerungsanträge) nach den Verfahrensordnungen von diesem grundsätzlich auch dem jeweiligen Prozessgegner übermittelt werden müssen. Der gemeinsame Schriftsatz wurde den beiden Klägern im Folgenden auch tatsächlich durch das Gericht übermittelt. Da darin die Personalien der jeweiligen Kläger aufgeführt waren, konnten somit beide jeweils erkennen, dass auch ein anderer namentlich genannter Strafgefangener Kläger in einem gerichtlichen Verfahren gegen die Justizvollzugsanstalt ist, ohne dass dies von den Verfahrensbeteiligten gewollt gewesen wäre. Ich habe die Anstalt darauf hingewiesen, dass in unterschiedlichen Verfahren auch jeweils getrennte Schriftsätze an das Gericht zu erstellen sind, um eine Vermischung der getrennten Verfahren und letztlich eine damit einhergehende, datenschutzrechtlich unzulässige Datenübermittlung zu vermeiden. Die betreffende Justizvollzugsanstalt versicherte mir, dies künftig zu beachten.

5.4.4 Videoüberwachung

Im Rahmen meiner regelmäßigen Prüfungen von Justizvollzugsanstalten kontrolliere ich auch stets die dortigen Videoüberwachungsmaßnahmen. Auch wenn die eingesetzte Videoüberwachung an sich jeweils datenschutzrechtlich zulässig war, konnte ich im Berichtszeitraum bei einigen Justizvollzugsanstalten noch Verbesserungen, insbesondere in der Art und Weise der Videoüberwachung, erzielen. Ein besonderes Augenmerk legte ich darauf, dass durch die Videoüberwachung außerhalb geschlossener Räume etwa mit Hilfe schwenkbarer Kameras mit Zoom-Funktion keine Einsicht in Privaträume außerhalb der Anstalt – wie etwa in umliegende Privathäuser – ermöglicht wird. Teilweise wurde auch nicht ausreichend auf die Videoüberwachung hingewiesen, dies betraf insbesondere die für Besucher zugänglichen videoüberwachten Freiflächen auf dem Anstaltsgelände wie z.B. Parkplätze. Großen Wert lege ich im Rahmen meiner Prüfungen auch auf die Einhaltung der nach dem Gesetz zulässigen Höchstspeicherfrist für Videoaufzeichnungen von grundsätzlich 3 Wochen (Art. 21a Abs. 5 BayDSG; im Falle der Aufzeichnung der Besuchsüberwachung nach Art. 30 Bayerisches Strafvollzugsgesetz – BayStVollzG 1 Monat). Mit den betroffenen Justizvollzugsanstalten konnte ich jeweils zufriedenstellende Lösungen erzielen.

In einem Fall habe ich die Justizvollzugsanstalt darauf hingewiesen, dass im sogenannten besonders gesicherten Haftraum (Besondere Sicherungsmaßnahme nach Art. 96 BayStVollzG) nach dem Gesetzeswortlaut zwar eine ständige Beobachtung auch mit technischen Mitteln (Art. 96 Abs. 2 Nr. 2 BayStVollzG) und damit eine reine Videobeobachtung zulässig ist, nicht jedoch eine Videoaufzeichnung. Die betreffende Anstalt hat daraufhin von der bisherigen Praxis einer Videoaufzeichnung im besonders gesicherten Haftraum Abstand genommen und führt dort nur mehr eine Videobeobachtung durch.

5.5 Ordnungswidrigkeitenrecht

5.5.1 Anhörungsbogen/Zeugenfragebogen bei Verkehrsordnungswidrigkeiten

Von Amts wegen habe ich zahlreiche öffentliche Stellen, die Verkehrsordnungswidrigkeiten in eigener Zuständigkeit verfolgen, in diesem Tätigkeitsfeld geprüft. Es handelte sich überwiegend um Kommunen bzw. kommunale Zweckverbände. Geprüft habe ich die Formulare für die Anhörung des Betroffenen, dem eine Verkehrsordnungswidrigkeit zur Last gelegt wird (Anhörungsbogen) wie auch die Formulare zur Befragung von Zeugen der Verkehrsordnungswidrigkeit (Zeugenfragebogen). Dabei musste ich bei zahlreichen Stellen feststellen, dass die jeweiligen Belehrungen auf den Formularen nicht durchgehend den gesetzlichen Vorgaben entsprachen oder zumindest für den juristischen Laien unklar oder missverständlich waren.

Der Betroffene, dem ein Verkehrsverstoß zur Last gelegt wird, ist darüber zu belehren, dass es ihm nach dem Gesetz freisteht, sich zur Beschuldigung zu äußern oder nicht zur Sache auszusagen (§ 46 Abs. 1 Ordnungswidrigkeitengesetz – OWiG in Verbindung mit § 136 Abs. 1 Satz 2 Strafprozessordnung – StPO). Lediglich zu den Angaben über seine Person ist der Betroffene verpflichtet (§ 111 OWiG). Hingegen sind Zeugen zu wahrheitsgemäßen Angaben auch zur Sache verpflichtet (§ 46 Abs. 1 OWiG in Verbindung mit § 161a Abs. 1 Satz 1 StPO). Sie sind jedoch insbesondere darüber zu belehren, dass sie die Antwort auf solche

Fragen verweigern dürfen, durch deren wahrheitsgemäße Beantwortung sie sich selbst oder einen in § 52 Abs. 1 StPO bezeichneten Angehörigen (Verlobte, Ehegatten, Lebenspartner, bestimmte verwandte und verschwägerte Personen) der Gefahr der Verfolgung wegen einer Straftat oder einer Ordnungswidrigkeit aussetzen würden (§ 46 Abs. 1 OWiG in Verbindung mit § 55 StPO).

Die betreffenden Stellen haben meine Kritikpunkte ausnahmslos aufgegriffen und ihre Formulare entsprechend meinen Wünschen geändert. Die darin enthaltenen Belehrungen entsprechen nun den gesetzlichen Vorgaben und sind verständlicher gefasst.

5.5.2 Veröffentlichung von „Blitzerfotos“

Zwei öffentliche Stellen (eine Stadt sowie ein Kommunaler Zweckverband) haben sogenannte „Blitzerfotos“, die sie im Rahmen der von ihnen durchgeführten kommunalen Verkehrsüberwachung angefertigt haben, als „Verkehrsverstoß des Monats“ veröffentlicht. Mit einer derartigen Veröffentlichung verfolgen die betroffenen Stellen das Ziel, die Öffentlichkeit über die erheblichen Gefahren von Verkehrsverstößen, insbesondere von Geschwindigkeitsverstößen, aufzuklären und damit die Verkehrssicherheit zu erhöhen. Während der Zweckverband die Fotos auf seiner Homepage einstellte, veröffentlichte die Stadt die Fotos sogar auf ihrem Facebook-Auftritt.

Das grundsätzliche Anliegen, Raser mit Mitteln der Verkehrserziehung zur Vernunft zu bringen, kann ich gut nachvollziehen. Allerdings ist nicht abschließend geklärt, ob die mit den Fotos korrespondierenden Bußgeldverfahren zum Zeitpunkt der Veröffentlichung bereits rechtskräftig abgeschlossen waren. Bis zum rechtskräftigen Verfahrensabschluss gilt jedoch zunächst die Unschuldsvermutung zugunsten der jeweiligen Fahrzeugführer. Vor Verfahrensbeendigung kann nicht ausgeschlossen werden, dass sich der Vorwurf eines Verkehrsverstoßes nicht bewahrheitet, insbesondere sind Messfehler der Überwachungsgeräte stets denkbar.

Vor diesem Hintergrund habe ich datenschutzrechtliche Bedenken gegen derartige Veröffentlichungen geäußert. Jedenfalls ist auf eine umfassende und sorgfältige Anonymisierung der Fotos zu achten, um die Gefahr der Zuordnung sicher auszuschließen. Insbesondere sind über Gesichter und Kennzeichen hinaus zusätzlich alle individuellen oder auffälligen Merkmale der abgebildeten Fahrzeuge oder Personen zu schwärzen. In Zweifelsfällen ist auf die Veröffentlichung des jeweiligen „Blitzerfotos“ zu verzichten.

Soweit die Fotos nicht auf der Homepage der Behörde, sondern in sozialen Netzwerken wie Facebook veröffentlicht werden, sehe ich dies aufgrund der Problematik der Verarbeitung der Nutzungsdaten durch die sozialen Netzwerke ohne Wissen der Betroffenen (siehe 25. Tätigkeitsbericht 2012 Nr. 1.3) sowie der verstärkten Prangerwirkung durch Kommentierungsmöglichkeiten besonders kritisch. Ich empfehle daher, von der Veröffentlichung von „Blitzerfotos“ auf sozialen Netzwerken generell Abstand zu nehmen.

Die betroffenen Stellen habe ich auf meine Bedenken hingewiesen. Diese haben mir insbesondere zugesagt, künftig noch strenger auf die ausreichende Anonymisierung der Fotos zu achten und zusätzlich auch auffällige individuelle Merkmale der abgebildeten Fahrzeuge und Personen zu schwärzen.

5.5.3 Lichtbildübermittlungen im Rahmen von Verkehrsordnungswidrigkeitenverfahren

Auch in diesem Prüfzeitraum musste ich wieder vereinzelt datenschutzrechtliche Defizite bei Lichtbildübermittlungen im Rahmen von Verkehrsordnungswidrigkeiten feststellen.

Ich habe daher bei den betroffenen Behörden auf die Einhaltung des Datenschutzrechts hingewirkt und sie bei der Bearbeitung von Verkehrsordnungswidrigkeiten auf Folgendes hingewiesen:

Eine Lichtbildübermittlung aus dem Pass-/Personalausweisregister darf nur nach Maßgabe des § 22 Abs. 2 Passgesetz (PassG) bzw. § 24 Abs. 2 Personalausweisgesetz (PAuswG) erfolgen. Die Verantwortung für derartige Ersuchen trägt die ersuchende Behörde (vgl. § 22 Abs. 3 Satz 1 PassG bzw. § 24 Abs. 3 Satz 1 PAuswG). Die ersuchende Behörde hat den Anlass des Ersuchens und die Herkunft der übermittelten Daten und Unterlagen aktenkundig zu machen (vgl. § 22 Abs. 3 Satz 3 PassG bzw. § 24 Abs. 3 Satz 3 PAuswG).

§ 22 PassG Verarbeitung und Nutzung der Daten im Paßregister
(3) Die ersuchende Behörde trägt die Verantwortung dafür, daß die Voraussetzungen des Abs. 2 vorliegen. Ein Ersuchen nach Abs. 2 darf nur von Bediensteten gestellt werden, die vom Behördenleiter dafür besonders ermächtigt sind. Die ersuchende Behörde hat den Anlaß des Ersuchens und die Herkunft der übermittelten Daten und Unterlagen aktenkundig zu machen. Wird die Passbehörde von dem Bundesamt für Verfassungsschutz, den Landesbehörden für Verfassungsschutz, dem Militärischen Abschirmdienst, dem Bundesnachrichtendienst, dem Bundeskriminalamt oder dem Generalbundesanwalt oder der Generalbundesanwältin um die Übermittlung von Daten ersucht, so hat die ersuchende Behörde den Familiennamen, die Vornamen und die Anschrift des Betroffenen unter Hinweis auf den Anlass der Übermittlung aufzuzeichnen. Die Aufzeichnungen sind gesondert aufzubewahren, durch technische und organisatorische Maßnahmen zu sichern und am Ende des Kalenderjahres, das dem Jahr der Übermittlung folgt, zu vernichten.

§ 24 PAuswG Verwendung im Personalausweisregister gespeicherter Daten
(3) Die ersuchende Behörde trägt die Verantwortung dafür, dass die Voraussetzungen des Abs. 2 vorliegen. Ein Ersuchen nach Abs. 2 darf nur von Bediensteten gestellt werden, die vom Behördenleiter dazu besonders ermächtigt sind. Die ersuchende Behörde hat den Anlass des Ersuchens und die Herkunft der übermittelten Daten und Unterlagen zu dokumentieren. Wird die Personalausweisbehörde vom Bundesamt für Verfassungsschutz, den Landesbehörden für Verfassungsschutz, dem Militärischen Abschirmdienst, dem Bundesnachrichtendienst, dem Bundeskriminalamt oder dem Generalbundesanwalt oder der Generalbundesanwältin um die Übermittlung von Daten ersucht, so hat die ersuchende Behörde den Familiennamen, die Vornamen und die Anschrift des Betroffenen unter Hinweis auf den Anlass der Übermittlung aufzuzeichnen. Die Aufzeichnungen sind gesondert aufzubewahren, durch technische und organisatorische Maßnahmen zu sichern und am Ende des Kalenderjahres, das dem Jahr der Übermittlung folgt, zu vernichten.

Aus datenschutzrechtlicher Sicht ist es daher erforderlich, dass ein entsprechender kurzer Aktenvermerk vom zuständigen Sachbearbeiter angefertigt wird, der die Voraussetzungen für eine Lichtbildübermittlung dokumentiert.

Auch ist eine Lichtbildübermittlung aus dem Pass- bzw. Personalausweisregister per E-Mail ohne die Anwendung entsprechender Verschlüsselungsverfahren datenschutzrechtlich nicht zulässig.

§ 6a PassG Form und Verfahren der Paßdatenerfassung, -prüfung und -übermittlung
(1) Die Datenübermittlung von den Passbehörden an den Passhersteller zum Zweck der Passherstellung, insbesondere die Übermittlung sämtlicher Passantragsdaten, erfolgt durch Datenübertragung. Die Datenübertragung kann auch über Vermittlungsstellen erfolgen. Die beteiligten Stellen haben dem jeweiligen Stand der Technik entsprechende Maßnahmen zur Sicherstellung von Datenschutz und Datensicherheit zu treffen, die insbesondere die Vertraulichkeit und Unversehrtheit der Daten sowie die Feststellbarkeit der übermittelnden Stelle gewährleisten; im Fall der Nutzung allgemein zugänglicher Netze sind dem jeweiligen Stand der Technik entsprechende Verschlüsselungsverfahren anzuwenden.

§ 12 PAuswG Form und Verfahren der Datenerfassung, -prüfung und -übermittlung
(1) Die Datenübermittlung von den Personalausweisbehörden an den Ausweishersteller zum Zweck der Ausweisherstellung, insbesondere die Übermittlung sämtlicher Ausweisantragsdaten, erfolgt durch Datenübertragung. Die Datenübertragung kann auch über Vermittlungsstellen erfolgen. Die beteiligten Stellen haben dem jeweiligen Stand der Technik entsprechende Maßnahmen zur Sicherstellung von Datenschutz und Datensicherheit zu treffen, die insbesondere die Vertraulichkeit und Unversehrtheit der Daten sowie die Feststellbarkeit der übermittelnden Stelle gewährleisten; im Falle der Nutzung allgemein zugänglicher Netze sind Verschlüsselungsverfahren anzuwenden, die dem jeweiligen Stand der Technik entsprechen.

Zwar kann eine Lichtbildübermittlung gemäß § 22 Abs. 2 PassG bzw. § 24 Abs. 2 PAuswG nach den gesetzlichen Bestimmung des § 22a Abs. 1 PassG und § 25 Abs. 1 PAuswG auch durch Datenübertragung erfolgen. Es gelten aber § 6a Abs. 1 Satz 3 PassG bzw. § 12 Abs. 1 Satz 3 PAuswG entsprechend. Danach haben die beteiligten Stellen dem jeweiligen Stand der Technik entsprechende Maßnahmen zur Sicherstellung von Datenschutz und Datensicherheit zu treffen, die insbesondere die Vertraulichkeit und Unversehrtheit der Daten sowie die Feststellbarkeit der übermittelnden Stelle gewährleisten. Im Falle der Nutzung allgemein zugänglicher Netze sind Verschlüsselungsverfahren anzuwenden, die dem jeweiligen Stand der Technik entsprechen.

6 Kommunales

6.1 Erlass eines Bundesmeldegesetzes und Novellierung des Bayerischen Meldegesetzes

Im Zuge der Föderalismusreform wurde das Meldewesen in die ausschließliche Gesetzgebungskompetenz des Bundes überführt. Am 28. Juni 2012 hatte der Bundestag mit dem Gesetz zur Fortentwicklung des Meldewesens (MeldFortG) ein Bundesmeldegesetz beschlossen, welches das geltende Melderechtsrahmengesetz sowie die bisherigen Landesmeldegesetze ersetzt (siehe 25. Tätigkeitsbericht 2012 Nr. 1.4.2 sowie 23. Tätigkeitsbericht 2008 Nr. 10.1). Das MeldFortG war nach einer Beschlussempfehlung des Vermittlungsausschusses vom 26. Februar 2013 nochmals in wesentlichen Punkten geändert und am 28. Februar 2013 verabschiedet worden. Der Bundesrat hat dazu am 1. März 2013 seine Zustimmung erteilt.

Die Bemühungen der Datenschutzbeauftragten des Bundes und der Länder, eine datenschutzkonforme Ausgestaltung des neuen Melderechts zu erreichen, waren nur zum Teil erfolgreich (siehe hierzu auch die unten abgedruckte Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 22. August 2012). Die wichtigsten Ergebnisse im Einzelnen:

- Erfreulicherweise stärkt die Neuregelung die Rechte der Meldepflichtigen **bei einfachen Melderegisterauskünften für Zwecke der Werbung oder des Adresshandels**. Entsprechende Auskünfte dürfen danach nur noch erteilt werden, wenn die betreffende Person in die Übermittlung für jeweils diesen Zweck **eingewilligt hat**. Leider nicht aufgegriffen wurde hingegen die datenschutzrechtliche Forderung, den Meldepflichtigen ein generelles Widerspruchsrecht in Bezug auf sonstige einfache Melderegisterauskünfte einzuräumen, sofern der Auskunftssuchende kein rechtliches Interesse glaubhaft gemacht hat.

- Künftig unterliegen auch Melderegisterauskünfte zu gewerblichen Zwecken ausdrücklich der **Zweckbindung**. Empfänger dürfen die erhaltenen Daten nur für die Zwecke verwenden, zu deren Erfüllung sie übermittelt wurden. Das neue **Wiederverwendungsverbot** für Daten, die zum Zwecke der geschäftsmäßigen Anschriftenermittlung für Dritte erhoben werden, soll das ungerechtfertigte Sammeln von Adressen („Adressen-Pooling“) verhindern.

- Bei den **Melderegisterauskünften in besonderen Fällen** (Auskünfte an Parteien zu Wahlwerbezwecken, an Presse oder Rundfunk über Alters- und Ehejubiläen und an Adressbuchverlage) hat das Bundesmeldegesetz das Recht auf informationelle Selbstbestimmung bedauerlicherweise nicht gestärkt. Es bestehen insoweit nach wie vor lediglich Widerspruchsregelungen. Einwilligungslösungen wurden nicht aufgenommen. Außerdem erlaubt das Bundesmeldegesetz **erweiterte Melderegisterauskünfte** bereits bei Glaubhaftmachung eines jedweden berechtigten Interesses.

– Für die Betroffenen besteht weiterhin kein umfassender **Auskunftsanspruch**, z.B. in Bezug auf erweiterte Melderegisterauskünfte, Gruppenauskünfte und einfache Melderegisterauskünfte auf herkömmlichem Weg. Immerhin können jetzt neben regelmäßigen Datenübermittlungen auch Datenübermittlungen durch ein automatisiertes Abrufverfahren im Einzelfall oder eine automatisierte Melderegisterauskunft nach § 49 Abs. 1 Bundesmeldegesetz beauskunftet werden.

– Nach der gesetzlichen Neuregelung soll für die öffentlichen Stellen länderübergreifend ein **Online-Zugang** zu bestehenden Meldedatenbeständen eröffnet werden. Von der Schaffung eines – aus datenschutzrechtlicher Sicht abzulehnenden – zentralen Bundesmelderegisters hat der Gesetzgeber Abstand genommen.

– Die **Hotelmeldepflicht** für inländische Gäste, deren Abschaffung von den Datenschutzbeauftragten über Jahre hinweg immer wieder gefordert worden war, bleibt bestehen. Trotz datenschutzrechtlicher Kritik wurde außerdem die **Mitwirkungspflicht des Wohnungsgebers** bei der An- und Abmeldung von Mietern wieder eingeführt, obwohl diese durch das Gesetz zur Änderung des Melderechtsrahmengesetzes und anderer Gesetze vom 25. März 2002 gestrichen worden war.

Bis zum voraussichtlichen Inkrafttreten des Bundesmeldegesetzes am 1. November 2015 gilt das Bayerische Meldegesetz (MeldeG) weiter. Im Hinblick darauf hat der Bayerische Gesetzgeber Art. 31 MeldeG erfreulicherweise bereits dahin gehend geändert, dass die Erteilung einer einfachen Melderegisterauskunft für Zwecke der Werbung oder des Adresshandels nur mit Einwilligung des Betroffenen zulässig ist. Das entsprechende Gesetz zur Änderung des Meldegesetzes vom 22. Mai 2013 ist am 1. Juli 2013 in Kraft getreten.

Art. 31 MeldeG Melderegisterauskunft
(1) [1]Personen, die nicht Betroffene sind, und andere als die in Art. 28 Abs. 1 bezeichneten Stellen können von den Meldebehörden Auskunft über
1. Vor- und Familiennamen,
2. Doktorgrad und
3. Anschriften
einzelner bestimmter Einwohner verlangen (einfache Melderegisterauskunft). […] [3]Die Erteilung einer Auskunft ist nur zulässig, wenn der Antragsteller erklärt, die Daten nicht zu verwenden für Zwecke
1. der Werbung oder
2. des Adresshandels,
es sei denn, der Betroffene hat ihm gegenüber in die Übermittlung für jeweils diesen Zweck eingewilligt.

Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 22.08.2012
Melderecht datenschutzkonform gestalten!

Das vom Deutschen Bundestag am 28.06.2012 beschlossene neue Melderecht weist erhebliche datenschutzrechtliche Defizite auf. Schon die im Regierungsentwurf enthaltenen Datenschutzbestimmungen blieben zum Teil hinter dem bereits geltenden Recht zurück. Darüber hinaus wurde der Regierungsentwurf durch das Ergebnis der Ausschussberatungen des Bundestages noch einmal deutlich verschlechtert.

Bei den Meldedaten handelt es sich um Pflichtangaben, die die Bürgerinnen und Bürger gegenüber dem Staat machen müssen. Dies verpflichtet zu besonderer Sorgfalt bei der Verwendung, insbesondere wenn die Daten an Dritte weitergegeben werden sollen.

Die Datenschutzbeauftragten des Bundes und der Länder fordern daher den Bundesrat auf, dem Gesetzentwurf nicht zuzustimmen, damit im Vermittlungsverfahren die erforderlichen datenschutzgerechten Verbesserungen erfolgen können. Dabei geht es nicht nur darum, die im Deutschen Bundestag vorgenommenen Verschlechterungen des Gesetzentwurfs der Bundesregierung rückgängig zu machen, vielmehr muss das Melderecht insgesamt datenschutzkonform ausgestaltet werden. Hierfür müssen auch die Punkte aufgegriffen werden, die von den Datenschutzbeauftragten im Gesetzgebungsverfahren gefordert worden sind, aber unberücksichtigt blieben.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hält insbesondere in den folgenden Punkten Korrekturen und Ergänzungen für erforderlich:

- *Einfache Melderegisterauskünfte für Zwecke der Werbung und des Adresshandels bedürfen ausnahmslos der Einwilligung des Meldepflichtigen. Dies gilt auch für die Aktualisierung solcher Daten, über die die anfragenden Stellen bereits verfügen und die Weitergabe der Daten an Adressbuchverlage.*

  Melderegisterauskünfte in besonderen Fällen, wie Auskünfte an Parteien zu Wahlwerbungszwecken und an Presse oder Rundfunk über Alters- und Ehejubiläen sollten im Interesse der Betroffenen ebenfalls nur mit Einwilligung der Meldepflichtigen zulässig sein.

- *Der Meldepflichtige muss sonstigen einfachen Melderegisterauskünften widersprechen können. Die Übermittlung hat bei Vorliegen eines Widerspruchs zu unterbleiben, sofern der Anfragende kein rechtliches Interesse geltend machen kann.*

- *Die Zweckbindung der bei Melderegisterauskünften übermittelten Daten ist zu verstärken. Die im Gesetzentwurf nur für Zwecke der Werbung und des Adresshandels vorgesehene Zweckbindung muss auch auf die Verwendung für sonstige gewerbliche Zwecke erstreckt werden.*

- *Angesichts der Sensibilität der Daten, die im Rahmen einer erweiterten Melderegisterauskunft mitgeteilt werden, und der relativ niedrigen Voraussetzungen, die an die Glaubhaftmachung des berechtigten Interesses gestellt werden, sollte anstelle des berechtigten Interesses ein rechtliches Interesse an der Kenntnis der einzelnen Daten vom potentiellen Datenempfänger glaubhaft gemacht werden müssen.*

- *Die Erteilung einfacher Melderegisterauskünfte im Wege des Abrufs über das Internet oder des sonstigen automatisierten Datenabrufs sollte wie bisher nur zulässig sein, wenn die betroffene Person ihr nicht widerspricht.*

– *Die Hotelmeldepflicht sollte entfallen, weil es sich dabei um eine sachlich nicht zu rechtfertigende Vorratsdatenspeicherung handelt. Hotelgäste dürfen nicht schlechthin als Gefahrenquellen oder (potentielle) Straftäter angesehen und damit in ihrem Persönlichkeitsrecht verletzt werden.*

– *Die erst vor wenigen Jahren abgeschaffte Mitwirkungspflicht des Wohnungsgebers bei der Anmeldung des Mieters darf nicht wieder eingeführt werden. Die Verpflichtung des Meldepflichtigen, den Vermieter zu beteiligen, basiert auf einer Misstrauensvermutung gegenüber der Person des Meldepflichtigen. Der Gesetzgeber hat die damalige Abschaffung der Vermietermeldepflicht unter anderem damit begründet, dass die Erfahrungen der meldebehördlichen Praxis zeigen, dass die Zahl der Scheinmeldungen zu vernachlässigen ist. Es liegen keine Anhaltspunkte dafür vor, dass sich dies zwischenzeitlich geändert hat. Ferner steht der Aufwand hierfür – wie auch bei der Hotelmeldepflicht – außer Verhältnis zum Nutzen.*

6.2 Leitfaden zur kommunalen Videoüberwachung veröffentlicht

Die Videoüberwachung ist – abgesehen von einzelnen Sondervorschriften etwa für die Polizei – in Art. 21a BayDSG geregelt. Hintergrund für den Erlass der Vorschrift war ein Hinweis des Bundesverfassungsgerichts (Az.: 1 BvR 2368/06). Danach bedarf es einer klaren gesetzlichen Regelung, unter welchen konkreten Voraussetzungen eine Videoüberwachung öffentlicher Räume zulässig ist. In der Begründung zu Art. 21a BayDSG wurde ausdrücklich darauf hingewiesen, dass eine Ausweitung der Videoüberwachung nicht beabsichtigt ist (Landtags-Drucksache 15/9799).

Laut Statistiken (Landtags-Drucksache 16/15571) hat die Videoüberwachung in Bayern über die letzten Jahre jedoch deutlich zugenommen. Bürger und Behörden haben sich zuletzt vermehrt mit Beschwerden bzw. mit der Bitte um Beratung an mich gewandt. Hierbei musste ich immer wieder feststellen, dass gerade auf Seiten der Kommunen erhebliche Unsicherheiten hinsichtlich der datenschutzrechtlichen Zulässigkeit und insbesondere der Grenzen kommunaler Videoüberwachungen bestehen.

Ich habe daher einen Leitfaden entwickelt, welcher kurz und prägnant die gerade bei kommunalen Videoüberwachungen zu beachtenden Datenschutzgesichtspunkte erläutert. Dieser mit dem Staatsministerium des Innern, für Bau und Verkehr abgestimmte Leitfaden wurde den Kommunen über die Regierungen und Landratsämter mit IMS vom 9. April 2014 (Az.: IA7-1083-1-28-1) zur Beachtung übermittelt. Parallel dazu wurde der Leitfaden Videoüberwachung auf meiner Homepage https://www.datenschutz-bayern.de u.a. unter „Themen“ – „Kommunales“ veröffentlicht. Der Leitfaden ergänzt das insoweit den Kommunen bereits bisher schon als Hilfestellung an die Hand gegebene **„Prüfungsschema zur Videobeobachtung und Videoaufzeichnung (Videoüberwachung)“** sowie das **„Muster zur Beschreibung der technischen und organisatorischen Maßnahmen beim Einsatz einer Videoaufzeichnungsanlage“,** welche beide ebenfalls von meiner Homepage unter „Veröffentlichungen“ – „Broschüren“ – „Mustervordrucke“ abgerufen werden können.

Vor dem Hintergrund des starken Anstiegs der gemeldeten Kameras im öffentlichen Raum werde ich auch kommunale Videoüberwachungen zukünftig noch stärker als bisher schon überprüfen, da eine Videoüberwachung öffentlicher

Plätze oder Einrichtungen ganz überwiegend Personen betrifft, die keinerlei Anlass für eine solche Beobachtung ihres Verhaltens gegeben haben und deshalb besonders intensiv in grundrechtliche Freiheiten eingreift. Bei derartigen Vor-Ort-Überprüfungen kommunaler Videoüberwachungen gab es aus datenschutzrechtlicher Sicht in der Vergangenheit immer wieder Grund zur Beanstandung, da beispielsweise bloße Bagatellschäden nicht den Einsatz von Überwachungskameras rechtfertigen oder eine kommunale Videoüberwachung nicht ausschließlich der nachträglichen Strafverfolgung von Tätern dienen darf. Besondere Bedeutung wird daher zukünftig der Beachtung des neuen Leitfadens Videoüberwachung zukommen, welcher folgenden Wortlaut hat:

„Seit dem 1. Juli 2008 sind Zulässigkeit und Grenzen der Videoüberwachung durch bayerische öffentliche Stellen, wozu gerade auch Kommunen zählen, in Art. 21a Bayerisches Datenschutzgesetz (BayDSG) geregelt. Für die Polizei gelten Sonderregelungen wie Art. 32 Abs. 2 Polizeiaufgabengesetz und Art. 9 Bayerisches Versammlungsgesetz.

Führen bayerische Kommunen Videobeobachtungen (Erhebung personenbezogener Daten mit Hilfe optisch-elektronischer Einrichtungen) oder gar noch eingriffsintensivere Videoaufzeichnungen (Speicherung personenbezogener Daten mit Hilfe optisch-elektronischer Einrichtungen) durch, müssen diese im Einklang mit Art. 21a BayDSG stehen. Dies gilt auch für solche kommunalen Eigenbetriebe bzw. sonstige dem BayDSG unterfallende kommunale öffentliche Stellen, die gemäß Art. 3 Abs. 1 Satz 1 BayDSG als Unternehmen am Wettbewerb teilnehmen, denn eine **Videoüberwachung** *stellt* **keine Wettbewerbsteilnahme** *dar, so dass es insoweit nicht zur Anwendung des Bundesdatenschutzgesetzes kommt. Da auch nicht funktionsfähige Kameras (***Kameraattrappen***) eine Verhaltensbeeinflussung bezwecken und daher in ähnlicher Weise wie „echte" Videoüberwachungen in die Persönlichkeitsrechte Betroffener eingreifen, beurteilt sich deren Zulässigkeit ebenfalls nach Art. 21a BayDSG.*

Art. 21a Abs. 1 und 2 BayDSG stellen für die Zulässigkeit von Videoüberwachungen strenge materielle Datenschutzvoraussetzungen auf. Im Ergebnis darf eine Videoüberwachung nur durchgeführt werden, wenn sie zur Erfüllung öffentlicher Aufgaben oder in Ausübung des Hausrechts **für Zwecke des Personen- oder Objektschutzes** *erforderlich ist,* **keine überwiegenden schutzwürdigen Interessen der Betroffenen beeinträchtigt werden** *und sie* **transparent** *gestaltet ist. Im Einzelnen:*

(1) Da die Ermöglichung einer repressiven Strafverfolgung – beispielsweise hinsichtlich Vandalismus – keine kommunale Aufgabe, sondern eine solche von Polizei und Staatsanwaltschaft ist, kann dies allenfalls Nebenzweck einer der Gefahrenabwehr dienenden kommunalen Videoüberwachung sein. Soweit die Videoüberwachung zur Erfüllung der den Gemeinden gesetzlich zugewiesenen Aufgabe der Gefahrenabwehr erfolgt, ist plausibel darzulegen, dass sie hierzu geeignet und erforderlich ist und andere weniger eingreifende Maßnahmen nicht in Betracht kommen. Vor einer Entscheidung über die Zulässigkeit einer Videoüberwachung ist daher eine Gefahrenanalyse durchzuführen. Es müssen Erfahrungswerte vorliegen, die den Schluss zulassen, dass bei dem betreffenden Objekt, z.B. einem Dienstgebäude oder Schule, eine Verletzung der in Art. 21a Abs. 1 Satz 1 BayDSG genannten Rechtsgüter in Zukunft wahrscheinlich ist. Die Videoüberwachung muss dazu dienen, dieser prognostizierten Gefahr entgegenzuwirken. Ein Mittel des präventiven Entgegenwirkens ist auch die Steigerung der Wahrscheinlichkeit

einer repressiven Straf- oder zivilrechtlichen Verfolgung. Denn es kann davon ausgegangen werden, dass Täter oder Störer, die (aufgrund der Videoüberwachung) gesteigert eine repressive Ahndung befürchten müssen, im Sinne einer Verhaltenssteuerung zumindest zum Teil auch präventiv abgeschreckt werden.

(2) Auch bei einer Videoüberwachung in Wahrnehmung des Hausrechts ist plausibel darzulegen, dass sie hierzu geeignet und erforderlich ist und andere weniger eingreifende Maßnahmen nicht in Betracht kommen. Dabei ist zu Gunsten öffentlicher Hausrechtsinhaber und der Verantwortlichen für eine öffentliche Einrichtung zu berücksichtigen, dass sie ein auch durch das Gesetz geschütztes Interesse daran geltend machen können, bei Sachbeschädigungen an der durch das Hausrecht geschützten Einrichtung zivilrechtlich Schadensersatzforderungen durchzusetzen.

(3) Bei einer alleine auf die Erfüllung der den Gemeinden gesetzlich zugewiesenen Aufgabe der Gefahrenabwehr gestützten Maßnahme muss die ***generelle Erforderlichkeit*** *einer Videoüberwachung in einem* ***ersten Schritt*** *– grundsätzlich anhand einer detaillierten und regelmäßig aktualisierten* ***Vorfallsdokumentation*** *– geprüft und bejaht werden können. Hierfür wird regelmäßig die durch entsprechende Zahlen (ggf. auch von vergleichbaren Objekten) belegte signifikante Häufung von Gefahren erforderlich sein. Ein rein subjektives Empfinden der Bevölkerung bzw. eine rein subjektive Überwachungsbedürftigkeit genügen gerade nicht.*

In einem ***zweiten Schritt*** *ist der Standort* ***jeder einzelnen Kamera*** *sowie deren Erfassungswinkel entsprechend zu begründen. Die Videoüberwachung ist dabei zum einen* ***räumlich*** *auf die „gefährdeten" Bereiche zu begrenzen, insbesondere also auf „Tote Winkel" und auf Bereiche, bei denen aufgrund von Schadensfällen in der Vergangenheit auch künftig mit vergleichbaren Vorkommnissen zu rechnen ist. Der jeweilige Kameraerfassungsbereich ist dort, wo er über die gefährdeten Bereiche hinausgeht, durch geeignete technische Maßnahmen (z.B. Schwarzschaltungen, mechanische Sperren, Umsetzen der Kameras, softwaretechnische Sperren bestimmter möglicher Beobachtungsbereiche) einzuschränken. Zum anderen ist die Videoüberwachung aber auch in* ***zeitlicher Hinsicht*** *auf das erforderliche Maß – also in der Regel auf die Zeiten, in denen mit Schadensfällen zu rechnen ist – zu beschränken.*

Sollten sich bei den danach notwendigen Erforderlichkeitsprüfungen alternative, weniger in die Persönlichkeitsrechte von Betroffenen einschneidende Maßnahmen (z.B. verstärkte Überwachung durch Aufsichtspersonal oder Alarmanlagen) bei einem aus Sicht der verantwortlichen Stelle vertretbarem Aufwand als ebenso geeignet erweisen, sind solche Maßnahmen zunächst auszuschöpfen. ***Videoüberwachungen werden daher regelmäßig Teil eines Gesamtkonzeptes sein müssen.***

(4) Um eine Beeinträchtigung überwiegender schutzwürdiger Interessen von Betroffenen zu vermeiden, dürfen ***höchstpersönliche Bereiche,*** *wie z.B. (der Zugang zu) Toilettenanlagen, Umkleidekabinen oder Aufenthaltsräume* ***grundsätzlich nicht videoüberwacht*** *werden.*

Sollten auch Mitarbeiter von der Videoüberwachung betroffen sein, so ist zusätzlich der Mitbestimmungstatbestand des Art. 75a Abs. 1 Nr. 1 Bayerisches Personalvertretungsgesetz (BayPVG) zu beachten. Insoweit sollten schon aus Transparenzgründen Dienstvereinbarungen gemäß Art. 73 BayPVG abgeschlossen wer-

den, in welchen insbesondere geregelt werden sollte, welche Mitarbeiterdaten aufgezeichnet werden, wie lange die aufgezeichneten Daten gespeichert werden, welche Personen Zugriff auf diese Daten haben, sowie dass die Videoüberwachung nicht zu Zwecken der Verhaltens- und/oder Leistungskontrolle von Mitarbeitern eingesetzt werden darf.

(5) Gemäß Art. 21a Abs. 2 BayDSG sind die Videoüberwachung und die erhebende Stelle durch geeignete Maßnahmen erkennbar zu machen, wobei die Information regelmäßig durch deutlich sichtbare Anbringung von Piktogrammen (vgl. z.B. DIN 33450, weißes Kamerasymbol auf blauem Hintergrund) vor Betreten des videoüberwachten Bereichs zu geben sein wird. Sollte die Videoüberwachung nur zu bestimmten Zeiten erfolgen, ist grundsätzlich auch auf diese Zeiten hinzuweisen.

(6) Nach Art. 26 Abs. 1 Sätze 1 und 3 BayDSG bedürfen erstmaliger Einsatz/wesentliche Änderung von automatisierten Verfahren zur Verarbeitung personenbezogener Daten einer vorherigen schriftlichen Freigabe durch die das Verfahren einsetzende öffentliche Stelle. Erteilt wird die datenschutzrechtliche Freigabe gemäß Art. 26 Abs. 3 Satz 2 BayDSG grundsätzlich durch den behördlichen Datenschutzbeauftragten. Dieser hat gemäß Art. 27 BayDSG ein Verzeichnis der bei der Kommune eingesetzten und datenschutzrechtlich freigegebenen automatisierten Verfahren zu führen, in welches jeder Bürger kostenlos Einsicht nehmen kann. Die Beschreibung der technischen und organisatorischen Maßnahmen nach Art. 26 Abs. 3 Satz 1 BayDSG sowie die zusätzlichen Angaben nach Art. 21a Abs. 6 Satz 2 BayDSG sind dabei auch aus Sicherheitsgründen nicht in das öffentlich zugängliche Verfahrensverzeichnis nach Art. 27 BayDSG aufzunehmen. Aufgrund der Rechtsfolgenverweisung des Art. 21a Abs. 6 Satz 1 BayDSG unterfällt den letztgenannten gesetzlichen Bestimmungen auch der Betrieb einer Videoaufzeichnungsanlage. In diesem Zusammenhang weise ich insbesondere auf das „Prüfungsschema zur Videobeobachtung und Videoaufzeichnung (Videoüberwachung)“ und das „Muster zur Beschreibung der technischen und organisatorischen Maßnahmen beim Einsatz einer Videoaufzeichnungsanlage“ hin, welche von meiner Homepage https://www.datenschutz-bayern.de unter der Rubrik „Veröffentlichungen“, Unterrubrik „Mustervordrucke“ abgerufen werden können.“

6.3 Videoüberwachung in kommunalen Schwimmbädern

Mehrere Bürger wandten sich an mich und erkundigten sich nach der Zulässigkeit einer Videoüberwachung in kommunalen Schwimmbädern. Ich habe die Eingaben zum Anlass genommen, verschiedene Schwimmbäder auch vor Ort zu überprüfen. Wiederholt musste ich dabei feststellen, dass kommunale Betreiber von Schwimmbädern datenschutzrechtliche Vorschriften verletzten. Bei einer Videoüberwachung in kommunalen Schwimmbädern ist zusammengefasst insbesondere Folgendes zu beachten:

– Kommunale Schwimmbäder haben als öffentliche Einrichtungen die Vorgaben des Art. 21a BayDSG zu beachten. Der Personen- und Objektschutz gehört im Bereich der eigenen Liegenschaften zu den Aufgaben der Gemeinde. Eine Videoüberwachung kommt deshalb auch in Schwimmbädern in Betracht. Allerdings ist die Videoüberwachung **nicht bereits eine allgemein zulässige Maßnahme im normalen Betriebsablauf.**

– Die Videoüberwachung kann vielmehr **allein mit präventiver Gefahrenabwehr** bezüglich der in Art. 21a Abs. 1 BayDSG genannten Rechtsgüter begründet werden, so z.B. zum Schutz des Eigentums der Badegäste. Hierfür muss aber dokumentiert sein, dass es (z.B. an Umkleideschränken) bereits **zu wiederholten Aufbrüchen und Diebstählen kam**. Lediglich kleinere Sachbeschädigungen oder Eigentumsdelikte rechtfertigen eine derartige Eingriffsmaßnahme regelmäßig nicht. Allerdings können insofern unter Umständen auch Erfahrungen aus umliegenden, im Wesentlichen vergleichbaren Bädern herangezogen werden, um eine **konkrete Wiederholungsgefahr** zu begründen. Gerade im Bereich von Umkleideschränken kommt aber der Prüfung schutzwürdiger Interessen der von der Überwachung betroffenen Badegäste besondere Bedeutung zu. Da diese sich dort überwiegend „nur" in Badekleidung bewegen bzw. sich erfahrungsgemäß oft auch im Bereich der Umkleideschränke umziehen, ist ggf. der Erfassungsbereich der Kamera(s) auf die Umkleideschränke in „Kopfhöhe" zu begrenzen. In jedem Fall ist aber vorrangig zu prüfen, ob nicht andere, weniger belastende Maßnahmen (wie z.B. die Einrichtung separater Wertschließfächer, anderes Schließsystem oder Ähnliches) ergriffen werden können.

– Für zulässig erachtet habe ich eine Videoüberwachung der Beckenanlagen in schwer einsehbaren, besonderen Gefahrenbereichen im Rahmen der Bäderaufsicht. Dabei kann auch bereits eine abstrakte Gefahr genügen, soweit es um den **Schutz hochwertiger Rechtsgüter (Leben und Gesundheit der Badegäste)** geht. Dazu reicht aber eine räumlich versetzte Beobachtung der in Frage kommenden Badebereiche aus, um die Möglichkeit eines sofortigen Eingreifens zu sichern. Die Abwägung mit den schutzwürdigen Interessen der betroffenen Badegäste kann hier dazu führen, dass nur personenunscharfe Bilder erzeugt werden dürfen.

– Allein der **Schutz des Vermögens eines Bades rechtfertigt eine Videoüberwachung nicht**, da es sich dabei nicht um ein in Art. 21a Abs. 1 Satz 1 Nrn. 1 und 2 BayDSG geschütztes Rechtsgut handelt. **Unzulässig** wäre damit eine **Videoüberwachung an Drehkreuzanlagen**, die ausschließlich dazu dienen soll, ein unberechtigtes „Überspringen" und damit eine Leistungserschleichung zu verhindern. Eine solche Videoüberwachung würde überdies automatisch alle Badegäste beim Betreten bzw. Verlassen des Bades erfassen, obwohl sie überwiegend keinen Anlass für die Maßnahme geben. Damit würden überwiegende schutzwürdige Interessen der Badegäste beeinträchtigt, die sich vertragstreu verhalten und die in Anspruch genommene Leistung bezahlen. Auch **haftungs- und/oder versicherungsrechtliche Gründe** (z.B. bei Badeunfällen) **rechtfertigen eine Videoaufzeichnung regelmäßig nicht**.

Die Videoüberwachung muss grundsätzlich Teil eines **Gesamtkonzepts** sein, welches in erster Linie dazu dient, die Bäderaufsicht **zu unterstützen**. Eine pauschale Videoaufzeichnung allein ist dabei kein geeignetes Mittel, um z.B. Aufbrüche an Umkleideschränken und Diebstahl zu verhindern. Erfahrungsgemäß führt außerdem auch eine Videoaufzeichnung häufig nicht zur Täterermittlung. Einem relativ geringen Nutzen der Videoüberwachung steht dann ein unverhältnismäßiger Eingriff in die Persönlichkeitsrechte der Bürger gegenüber. Dem Badegast wird dadurch oftmals gar eine trügerische Sicherheit vermittelt, die in Schadensfällen nicht eingelöst werden kann.

6.4 Energienutzungspläne

Energienutzungspläne sind informelle gemeindliche Planungsinstrumente und sollen einen Beitrag zur Sicherstellung einer umweltfreundlichen und zukunftsweisenden Energieversorgung leisten. Vergleichbar mit dem Flächennutzungsplan in der räumlichen Planung und anderen städtebaulichen Fachplanungskonzepten sollen Energienutzungspläne ganzheitliche Konzepte und Planungsziele aufzeigen, um diese weiteren förmlichen Planungsentscheidungen der Gemeinde zu Grunde zu legen.

Die im Zusammenhang mit Energienutzungsplänen zu beachtenden Datenschutzanforderungen sind in dem mit mir abgestimmten ausführlichen und klaren Leitfaden Energienutzungsplan vom 21. Februar 2011 der (damaligen) Staatsministerien für Umwelt und Gesundheit, für Wirtschaft, Infrastruktur, Verkehr und Technologie sowie der Obersten Baubehörde im Staatsministerium des Innern, für Bau und Verkehr (im Internet abrufbar unter der Adresse www.energieatlas.bayern.de/kommunen/energienutzungsplan.html) enthalten. Hinweisen möchte ich an dieser Stelle insbesondere auf Folgendes:

– Angaben über die Art der Feuerstätte bzw. Brennstoff, Nennleistung und Baujahr sind personenbezogene Daten gemäß Art. 4 Abs. 1 BayDSG, wenn die Angaben einer bestimmten oder bestimmbaren natürlichen Person zugeordnet werden können. Eine den Personenbezug aufhebende Anonymisierung gemäß Art. 4 Abs. 8 BayDSG erfordert, **„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."** Ob durch eine Zusammenfassung der obigen Angaben zu Summendaten (sogenannte Aggregierung) eine – zumindest faktische – Anonymisierung erreicht wird, lässt sich nicht abstrakt beantworten; maßgeblich sind vielmehr stets die konkreten Umstände des Einzelfalles.

– Nach dem Grundsatz der Direkterhebung gemäß Art. 16 Abs. 2 BayDSG sind personenbezogene Daten primär beim Betroffenen mit dessen Kenntnis zu erheben. Vor diesem Hintergrund sieht der Leitfaden Energienutzungsplan insbesondere auf den Seiten 28 und 81 ff. vielfältige Methoden der Bürgerbeteiligung vor.

– Personenbezogene Daten, die sich bei Dritten befinden, unterliegen einer strengen Zweckbindung und dürfen grundsätzlich nur für die Zwecke genutzt werden, für die sie ursprünglich erhoben wurden. Für die Erstellung von Energienutzungsplänen dürfen Daten bei Dritten daher nur mit Einwilligung des Betroffenen bzw. anonymisiert verwendet werden. Ausnahmen hiervon sind nur in den engen Grenzen des Art. 17 Abs. 2 BayDSG zulässig, was der Leitfaden auf den Seiten 28 ff. einzelfallbezogen erläutert. Diese Grenzen sind gemäß § 19 Abs. 5 Sätze 2 und 3 Schornsteinfegerhandwerksgesetz auch im Hinblick auf Kehrbuchdaten zu beachten (siehe Nr. 13.4.2). Insbesondere kann ich nicht erkennen, dass eine Zweckänderung insoweit gemäß Art. 17 Abs. 2 Nr. 3 BayDSG im Interesse der Betroffenen liegt. Erforderlich hierzu wäre der Eintritt von Nachteilen, sollte die Zweckänderung nicht erfolgen (vgl. insoweit Wilde/Ehmann/Niese/Knoblauch, Art. 17 BayDSG Rn. 21). Welche konkreten Nachteile aber ein

Grundstückseigentümer erleiden sollte, wenn der zuständige Schornsteinfegermeister die Kehrbuchdaten nicht zur Erstellung von Energienutzungsplänen an die Kommune weiterleitet, kann ich derzeit nicht erkennen.

— Die zur Erstellung eines Energienutzungsplans verwendeten personenbezogenen Daten dürfen nach dem auf Seite 8 des Leitfadens erläuterten Anonymisierungsgebot nicht personenbezogen dargestellt bzw. veröffentlich werden.

— Auch wenn der Leitfaden Energienutzungsplan auf den Seiten 7 und 8 von der grundsätzlichen Möglichkeit einer Einbindung privater Fachplaner in die Erstellung von Energienutzungsplänen ausgeht, müssen hierbei doch die datenschutzrechtlichen Anforderungen gewahrt werden. Vor diesem Hintergrund mache ich insbesondere auf die Anforderungen des Art. 6 BayDSG für Auftragsdatenverarbeitungen aufmerksam. Als weitere Hilfestellung weise ich insoweit auf den auf meiner Homepage https://www.datenschutz-bayern.de unter „Veröffentlichungen" – „Mustervordrucke" veröffentlichten Mustervertrag zur Auftragsdatenverarbeitung hin.

Bei der konkreten Erstellung von Energienutzungsplänen vor Ort sind jedoch nach meinem Eindruck trotzdem datenschutzrechtliche Unklarheiten entstanden, worauf ich durch Bürgereingaben und Anfragen – insbesondere von Kaminkehrermeistern – aufmerksam wurde. Ich habe mich daher an die nunmehr innerhalb der Bayerischen Staatsregierung für Energienutzungspläne bzw. Kommunalaufsicht und Kaminkehrerwesen zuständigen Ministerien für Wirtschaft und Medien, Energie und Technologie bzw. des Innern, für Bau und Verkehr gewandt und diese unter Hinweis auf Art. 25 Abs. 1 BayDSG gebeten, im jeweiligen Geschäftsbereich verstärkt auf die Einhaltung der eingangs dargestellten datenschutzrechtlichen Anforderungen zu achten.

Meiner Bitte entsprechend hat das Staatsministerium für Wirtschaft und Medien, Energie und Technologie zugesichert, konkrete Maßnahmen zu ergreifen, damit die maßgeblichen Datenschutzanforderungen vor Ort berücksichtigt werden. Es hat das Merkblatt zum entsprechenden Förderschwerpunkt um einen eigenen – mit mir abgestimmten – Abschnitt Datenschutz ergänzt. In zukünftigen Zuwendungsbescheiden wird eine Verpflichtung zur Einhaltung datenschutzrechtlicher Vorschriften aufgenommen. Ergänzend hat das Staatsministerium des Innern, für Bau und Verkehr den Bayerischen Landesinnungsverband für das Kaminkehrerwesen sowie die Bezirksregierungen als Bestellungsbehörden der bevollmächtigten Bezirksschornsteinfeger in Gesprächen beziehungsweise Dienstbesprechungen für die Thematik sensibilisiert und Unklarheiten ausgeräumt.

Bei der Erstellung von Energienutzungsplänen werde ich auch in Zukunft weiterhin auf die Einhaltung der maßgeblichen Datenschutzanforderungen achten.

6.5 Veröffentlichung personenbezogener Daten im Internet im Zusammenhang mit Gemeinde- und Landkreiswahlen

Vielfach werden personenbezogene Daten im Zusammenhang mit Gemeinde- und Landkreiswahlen über die vorgeschriebene ortsübliche Bekanntmachung hinaus auch ins Internet eingestellt. Nach Auffassung des Staatsministeriums des Innern, für Bau und Verkehr sind Veröffentlichungen im Internet zwar nicht ausdrücklich vorgesehen, aber auch nicht ausgeschlossen. Soweit eine öffentliche

Stelle Informationen zu Wahlen, insbesondere auch zu Bewerberinnen und Bewerbern in ihren Internetangeboten veröffentliche, wolle sie eine breite Öffentlichkeit unterrichten. Sie verfolge damit ein öffentliches Anliegen von hohem Gewicht. Die Veröffentlichungen dürften auch regelmäßig im Interesse der Bewerberinnen und Bewerber selbst liegen, zumal entsprechende Informationen in vielen Fällen auch durch die Parteien selbst veranlasst würden. Aus datenschutzrechtlicher Sicht habe ich gegen die Veröffentlichung personenbezogener Daten im Internet im Zusammenhang mit allgemeinen Wahlen keine grundsätzlichen Einwände, sofern diese Daten der Allgemeinheit bereits bekannt sind, etwa aufgrund einer zeitlich vorangegangenen oder zumindest zeitgleich stattfindenden öffentlichen Bekanntmachung (z.B. durch öffentlichen Aushang, Veröffentlichung im Amtsblatt oder der Tageszeitung) gemäß den einschlägigen gesetzlichen Vorschriften (siehe dazu insbesondere §§ 45 und 51 Gemeinde- und Landkreiswahlordnung (GLKrWO) in Verbindung mit den Anlagen 13, 14 und 15 zur GLKrWO).

Allerdings habe ich eine sehr unterschiedliche Veröffentlichungspraxis und Unsicherheiten festgestellt, welche personenbezogenen Daten wie lange im Internetauftritt von Behörden eingestellt werden dürfen. Deshalb habe ich mich an das Staatsministerium gewandt, um eine einheitliche datenschutzgerechte Handhabung zu erreichen. Das Staatsministerium hat daraufhin die nachgeordneten Behörden unter Berücksichtigung meiner Anregungen in einem Rundschreiben über die Anforderungen informiert, die bei der Veröffentlichung personenbezogener Daten im Internet im Zusammenhang mit Gemeinde- und Landkreiswahlen beachtet werden müssen. Es hat weiterhin darauf hingewiesen, dass die Ausführungen unabhängig von der Form der Bekanntmachung gelten, d.h. auch dann, wenn die entsprechenden Bekanntmachungen im Amtsblatt erfolgen und dieses ins Internet eingestellt wird (siehe auch 25. Tätigkeitsbericht 2012 Nr. 6.1).

Gleichwohl weise ich auf die Risiken hin, die mit einer Veröffentlichung personenbezogener Daten im Internet verbunden sind (insbesondere weltweite Veröffentlichung und zeitlich praktisch unbegrenzte Speicherung durch die Übernahme in Suchmaschinen, Möglichkeit einer automatisierten Auswertung der Daten nach verschiedenen Suchkriterien). Diese Risiken sind bei der Entscheidung, ob die Daten im Internet veröffentlicht werden, zu berücksichtigen. Eine gesetzliche Regelung der Veröffentlichung von Wahl(bewerber)-Daten im Internet, wie sie zwischenzeitlich in § 86 Abs. 3 Bundeswahlordnung erfolgt ist, würde ich begrüßen.

6.6 Übermittlung personenbezogener Daten von Behördenbediensteten zum Zweck ihrer Berufung als Mitglieder von Wahl- und Briefwahlvorständen

Im Vorfeld der Gemeinde- und Landkreiswahlen am 16.03.2014 haben sich mehrere Beschäftigte des öffentlichen Dienstes mit der Frage an mich gewandt, ob ihr Dienstherr Daten zu ihrer Person an ihre Heimatgemeinde übermitteln darf. Die Rechtslage stellt sich wie folgt dar:

Die Erhebung und Verwendung personenbezogener Daten von Wahlberechtigten zum Zwecke der Besetzung von Wahlvorständen ist in den Wahlgesetzen bereichsspezifisch geregelt. Rechtsgrundlage für die Übermittlung personenbezogener Daten der Bediensteten von Behörden und sonstiger bayerischer öffentlicher Stellen an die für die Besetzung der Wahlvorstände zuständigen Gemeinden im Zusammenhang mit den allgemeinen Gemeinde- und Landkreiswahlen ist Art. 6 Abs. 5 Gemeinde- und Landkreiswahlgesetz (GLKrWG). Um Wahlvorstände

und Briefwahlvorstände bilden zu können, dürfen die Gemeinden bayerische Behörden und öffentliche Stellen ersuchen, ihnen wahlberechtigte Bedienstete zu benennen, die im Gebiet der ersuchenden Gemeinde wohnen. Die ersuchte Stelle ist zur Datenübermittlung verpflichtet. Sie hat die Betroffenen über die übermittelten Daten und den Empfänger zu benachrichtigen. Die Regelung entspricht dem für Landtagswahlen und Volksentscheide geltenden Art. 7 Abs. 5 Landeswahlgesetz (LWG), der im Übrigen auch für Bezirkswahlen Anwendung findet (Art. 4 Abs. 1 Nr. 2 Bezirkswahlgesetz in Verbindung mit Art. 7 Abs. 5 LWG). Eine weitgehend entsprechende Regelung enthält § 9 Abs. 5 Bundeswahlgesetz (BWG), der auch für Europawahlen gilt (§ 4 Europawahlgesetz in Verbindung mit § 9 Abs. 5 BWG). Für Bürgerentscheide nach Art. 18a Gemeindeordnung bzw. Art. 12a Landkreisordnung hingegen fehlt eine entsprechende bereichsspezifische Regelung, eine Übermittlung personenbezogener Daten von Behördenbediensteten wäre hier demnach nur mit Einwilligung der Beschäftigten gemäß Art. 15 Abs. 1 Nr. 2 BayDSG möglich.

Die übermittelten Daten dürfen von den Gemeinden für die aktuellen Wahlen verarbeitet und genutzt werden (Art. 6 Abs. 4 GLKrWG). Der Verarbeitung und Nutzung der Daten auch für **künftige Wahlen** können die Betroffenen nach Art. 6 Abs. 4 GLKrWG widersprechen (ebenso § 9 Abs. 4 BWG, Art. 7 Abs. 4 LWG). Sie sind über das Widerspruchsrecht zu unterrichten. Soweit Betroffene widersprochen haben, müssen dadurch entstehende Lücken in der „Wahlhelferdatei“ durch erneute Datenübermittlung bzw. Datenweitergabe gefüllt werden (vgl. Wilde/Ehmann/Niese/Knoblauch, BayDSG, Art. 17 Rnrn. 45b und 45d). Dies steht auch nicht im Widerspruch zu einer – zeitlich befristeten – Verarbeitung und Nutzung der Daten für die jeweils aktuelle Wahl nach einer erneuten Meldung des Dienstherrn.

Art. 6 GLKrWG Wahlvorsteher, Wahlvorstand, Briefwahlvorsteher, Briefwahlvorstand
(4) [1]Die Gemeinden sind befugt, personenbezogene Daten von Wahlberechtigten zum Zweck ihrer Berufung zu Mitgliedern von Wahlvorständen und Briefwahlvorständen zu erheben, zu verarbeiten und zu nutzen. [2]Zu diesem Zweck dürfen personenbezogene Daten von Wahlberechtigten, die zur Tätigkeit in Wahlvorständen und Briefwahlvorständen geeignet sind, auch für künftige Abstimmungen verarbeitet und genutzt werden, sofern die betroffene Person der Verarbeitung oder Nutzung nicht widersprochen hat. [3]Die betroffene Person ist über das Widerspruchsrecht zu unterrichten. [4]Im Einzelnen dürfen folgende Daten erhoben, verarbeitet und genutzt werden: Familienname, Vorname, akademische Grade, Tag der Geburt, Anschriften, Telefonnummern, Zahl der Berufungen zu einem Mitglied der Wahlvorstände und der Briefwahlvorstände und die dabei ausgeübte Funktion.
(5) [1]Auf Ersuchen der Gemeinde sind zur Sicherstellung der Durchführung der Wahl die Behörden des Freistaates Bayern, der Gemeinden, der Landkreise und der Bezirke sowie der sonstigen der Aufsicht des Freistaates Bayern unterstehenden juristischen Personen des öffentlichen Rechts verpflichtet, aus dem Kreis ihrer Bediensteten unter Angabe von Familienname, Vorname, akademischen Graden, Tag der Geburt, Anschriften und Telefonnummern zum Zweck der Berufung als Mitglieder der Wahlvorstände und der Briefwahlvorstände wahlberechtigte Personen zu benennen, die im Gebiet der ersuchenden Gemeinde wohnen. [2]Die ersuchte Stelle hat die Betroffenen über die übermittelten Daten und den Empfänger zu benachrichtigen.

6.7 Hotel-Stammtisch in Kurorten – Kein Platz für Indiskretionen!

Aufgrund einer Beschwerde wurde ich mit folgender langjähriger Praxis der Tourist-Information einer als Luftkurort staatlich anerkannten Gemeinde befasst:

Der Leiter der betreffenden Tourist-Information hatte im Rahmen regelmäßig stattfindender sog. Hotel-Stammtische Listen mit den Ankunfts- und Übernachtungszahlen der größeren ortsansässigen Betriebe an die beim Hotel-Stammtisch anwesenden Hoteliers verteilt. Einer Gegenüberstellung der Jahre 2010/2011 und 2011/2012 1. Halbjahr sowie einer Übersicht der Entwicklung der Ankunfts- und Übernachtungszahlen der vorangegangenen Jahre waren dabei die entsprechenden Betriebszahlen zu entnehmen. Hierfür wurden die in der Gemeinde vorliegenden Meldescheine für Beherbergungsstätten ausgewertet. Die Gemeinde legte dar, sie wolle die Hoteliers damit über die aktuelle Tourismusentwicklung informieren. Dies sei auch immer als wertvolle Serviceleistung geschätzt worden. In den Listen waren neben den Hotels auch andere Betriebe wie Gästehäuser und Pensionen aufgeführt, deren Inhaber jedoch nicht zu den Teilnehmern der Hotel-Stammtische zählten. Einwilligungen der betreffenden Betriebsinhaber lagen nicht vor.

Das Vorgehen der Gemeinde war datenschutzrechtswidrig:

Bei den Ankunfts- und Übernachtungszahlen der einzelnen Betriebe handelt es sich – soweit deren Inhaber natürliche Personen sind – um personenbezogene Daten im Sinne des Art. 4 Abs. 1 BayDSG. Diese Angaben sind ausdrücklich den jeweiligen Betrieben zugeordnet und ermöglichen damit Rückschlüsse auf die wirtschaftlichen Verhältnisse der Betriebsinhaber. Die Herausgabe der Ankunfts- und Übernachtungszahlen der jeweils anderen Betriebe an die Hoteliers stellt gemäß Art. 4 Abs. 6 Satz 2 Nr. 3a BayDSG eine Übermittlung personenbezogener Daten an Dritte dar. Eine Übermittlung personenbezogener Daten an Dritte ist datenschutzrechtlich eine Datenverarbeitung (Art. 4 Abs. 6 Satz 1 BayDSG). Sie ist nach Art. 15 Abs. 1 Nrn. 1 und 2 BayDSG nur zulässig, wenn das Bayerische Datenschutzgesetz oder eine andere Rechtsvorschrift sie erlaubt oder anordnet oder die betroffene Person eingewilligt hat. Mangels einer Einwilligung der betroffenen Betriebsstätteninhaber ist die Datenübermittlung nur auf der Grundlage einer Rechtsvorschrift zulässig (Art. 15 Abs. 1 Nr. 1 BayDSG). Dabei gehen besondere Rechtsvorschriften über den Datenschutz den allgemeinen Vorschriften des Bayerischen Datenschutzgesetzes vor (Art. 2 Abs. 7 BayDSG):

Die Erhebung, Verarbeitung und Nutzung der in den Beherbergungsstätten erhobenen Meldedaten ist in den Art. 23, 24 und 26 Bayerisches Meldegesetz (MeldeG) bereichsspezifisch abschließend geregelt. Nach Art. 26 Abs. 1 Satz 2 MeldeG dürfen diese Daten von den Gemeinden nur zur Erhebung des Fremdenverkehrsbeitrags und des Kurbeitrags, von staatlichen Kurverwaltungen zur Erhebung der Kurtaxe und im Übrigen für Zwecke der Beherbergungs- und Fremdenverkehrsstatistiken ausgewertet und verarbeitet werden. Eine darüber hinaus gehende Verarbeitung von Daten aus Gästemeldescheinen durch öffentliche Stellen, zu der auch die Datenübermittlung an private Dritte gehört, sieht Art. 26 MeldeG nicht vor.

Die Bekanntgabe aufbereiteter Daten aus den Meldescheinen in Form der Ankunfts- und Übernachtungszahlen einzelner Betriebe an die Teilnehmer der Hotel-Stammtische unterfiel damit nicht den Nutzungsbeschränkungen des Art. 26

MeldeG. Im Übrigen wäre eine Darstellung der Ankunfts- und Übernachtungszahlen getrennt nach einzelnen Betrieben von vornherein nicht erforderlich gewesen, um über die Tourismusentwicklung in der Gemeinde zu informieren. Zu diesem Zweck dienen regelmäßig gerade die Fremdenverkehrsstatistiken.

Die unzulässige Datenübermittlung habe ich beanstandet.

Art. 24 MeldeG Besondere Meldescheine für Beherbergungsstätten
(1) [1]Die Leiter von Beherbergungsstätten oder ihre Beauftragten haben auf die Erfüllung der Meldepflichten ihrer Gäste hinzuwirken und besondere Meldescheine nach Abs. 2 bereitzuhalten. . . .
(2) [1]Die besonderen Meldescheine müssen Angaben enthalten über
1. den Tag der Ankunft und den der voraussichtlichen Abreise,
2. den Familiennamen,
. . .
(3) [1]Soweit es zur Erhebung des Fremdenverkehrs- oder Kurbeitrags gemäß Art. 6 und 7 des Kommunalabgabengesetzes oder der Kurtaxe gemäß Art. 24 des Kostengesetzes erforderlich ist, haben die Leiter der Beherbergungsstätten oder ihre Beauftragten auf dem Meldeschein den Tag der tatsächlichen Abreise zu vermerken. [2]Sie können ferner die für Zwecke der Beherbergungs- und Fremdenverkehrsstatistiken erforderlichen Angaben auf dem Meldeschein vermerken.

Art. 26 MeldeG Nutzungsbeschränkungen
(1) [1]Die nach Art. 23 Abs. 2 erhobenen und die gemäß Art. 24 Abs. 2 Satz 3 und Abs. 3 vermerkten Angaben dürfen nur von den in Art. 28 Abs. 4 genannten Behörden für Zwecke der Gefahrenabwehr oder der Strafverfolgung sowie zur Aufklärung der Schicksale von Vermissten und Unfallopfern ausgewertet und verarbeitet werden. [2]Die Daten dürfen darüber hinaus zur Erhebung des Fremdenverkehrs- und Kurbeitrags gemäß Art. 6 und 7 des Kommunalabgabengesetzes, der Kurtaxe gemäß Art. 24 des Kostengesetzes und für Zwecke der Beherbergungs- und Fremdenverkehrsstatistiken ausgewertet und verarbeitet werden. [3]Beherbergungsbetriebe dürfen die Daten nach Maßgabe des Bundesdatenschutzgesetzes auch für eigene Zwecke verwenden.

6.8 Übermittlung von Hundesteuerdaten an die Polizei

Erneut hat sich eine Gemeinde an mich gewandt, weil die zuständige Polizeiinspektion sie um die Übermittlung einer aktuellen Liste der im Bereich der Gemeinde registrierten Hundehalter ersucht habe. Die Polizei habe diese Bitte damit begründet, sie könne damit in konkreten Einzelfällen unnötige Anfragen bei der Kommune vermeiden. Ich vertrete dazu folgende Auffassung:

Nach Art. 13 Abs. 6 Satz 1 Kommunalabgabengesetz (KAG) findet bei der Hundesteuer auf die Erhebung, Verarbeitung oder Nutzung personenbezogener Daten das Bayerische Datenschutzgesetz Anwendung. Datenübermittlungen an Behörden sind dabei insbesondere in den Fällen des Art. 13 Abs. 6 Sätze 2 und 3 KAG zulässig.

Im vorliegenden Fall richtete sich die Zulässigkeit der von der Polizei erbetenen Datenübermittlung nach der Spezialvorschrift des Art. 42 Abs. 2 Polizeiaufgabengesetz (PAG). Danach kann die Polizei an öffentliche Stellen Ersuchen um Übermittlung personenbezogener Daten stellen, soweit diese zur Erfüllung ihrer Aufgaben erforderlich sind. Die ersuchte öffentliche Stelle prüft dabei grundsätzlich

nur, ob das Ersuchen im Rahmen der Aufgaben der Polizei liegt, es sei denn im Einzelfall besteht Anlass zur Prüfung der Rechtmäßigkeit des Ersuchens.

Im vorliegenden Fall bestand Anlass zur Prüfung der Rechtmäßigkeit des Ersuchens. Die Gesamtheit der angeforderten Daten ist offenkundig nicht zur Erfüllung der Aufgaben der Polizei erforderlich. Der Begriff der Erforderlichkeit beinhaltet auch eine gewisse Gegenwartsbezogenheit. Die Datenerhebung muss sich in der Regel auf konkret und aktuell zur Bewältigung anstehende Aufgaben beziehen: Daten dürfen nicht nur rein vorsorglich für den Fall erhoben werden, dass sie später einmal möglicherweise erforderlich werden. Eine andere Beurteilung ist nur in jenen Fällen denkbar, in denen die gegenwärtige Aufgabe gerade darin besteht, Daten zu sammeln bzw. für den Fall des Eintritts eines bestimmten Ereignisses vorrätig zu halten. Dies mag z.B. im Bereich des Katastrophenschutzes oder bei der Führung bestimmter polizeilicher Spezialdateien der Fall sein. Im vorliegenden Fall bestand ein derartiger Ausnahmetatbestand allerdings nicht. Die Übermittlung einer Liste der im Bereich der Gemeinde registrierten Hundehalter an die Polizei wäre deshalb unzulässig.

Art. 13 KAG Anwendung von Vorschriften der Abgabenordnung (AO 1977)
(6) [1]Bei der Hundesteuer findet auf die Erhebung, Verarbeitung oder Nutzung personenbezogener Daten das Bayerische Datenschutzgesetz Anwendung. [2]In Schadensfällen darf Auskunft über Namen und Anschrift des Hundehalters an Behörden und Schadensbeteiligte gegeben werden. [3]Bei Kampfhunden im Sinn des Art. 37 Abs. 1 Satz 2 des Landesstraf- und Verordnungsgesetzes dürfen die Gemeinden Namen und Anschrift der Halter sowie die Hunderasse auch zum Vollzug der Vorschriften über Kampfhunde speichern, verändern, nutzen und an andere zum Vollzug dieser Vorschriften zuständige Behörden übermitteln. [4]Weitergehende Befugnisse bleiben unberührt.

Art. 42 PAG Datenübermittlung an die Polizei
(2) [1]Die Polizei kann an öffentliche Stellen Ersuchen um Übermittlung personenbezogener Daten stellen, soweit diese zur Erfüllung ihrer Aufgaben erforderlich sind. [2]Die ersuchte öffentliche Stelle prüft die Zulässigkeit der Datenübermittlung. [3]Wenn gesetzlich nichts anderes bestimmt ist, prüft sie nur, ob das Ersuchen im Rahmen der Aufgaben der Polizei liegt, es sei denn im Einzelfall besteht Anlaß zur Prüfung der Rechtmäßigkeit des Ersuchens. [4]Die Polizei hat die zur Prüfung erforderlichen Angaben zu machen. [5]Die ersuchte öffentliche Stelle hat die Daten an die Polizei zu übermitteln, soweit gesetzlich nichts anderes bestimmt ist.

6.9 Speicherung von Angaben zur ethnischen Herkunft durch Standesämter

Aufgrund einer Eingabe war ich mit der Frage befasst, ob bestimmte Angaben auf beglaubigten Kopien von ausländischen Personenstandsurkunden geschwärzt bzw. gesperrt werden dürfen. Der Eingabeführer hatte im Rahmen der Anmeldung einer Eheschließung beim zuständigen Standesamt eine Original-Geburtsurkunde der ehemaligen UdSSR aus dem Jahr 1974 vorgelegt, worin auch Angaben zur ethnischen Zugehörigkeit enthalten waren. Das Standesamt verweigerte dem Petenten die gewünschte Unkenntlichmachung dieser Angaben auf der im Sammelakt befindlichen beglaubigten Kopie der eingereichten Geburtsurkunde mit der Begründung, dass das Personenstandsrecht eine Entfernung oder Schwärzung von Inhalten der Sammelakten nicht vorsehe.

Bei der Angabe zur ethnischen Herkunft handelt es sich um ein besonders sensibles personenbezogenes Datum, das nach Art. 15 Abs. 7 Satz 1 Nr. 1 BayDSG in der Regel nur dann verarbeitet werden darf, wenn eine Rechtsvorschrift dies ausdrücklich vorsieht. Eine solche Rechtsvorschrift ist aber vorliegend nicht erkennbar, weshalb eine Datenverarbeitung, hier das Speichern eines solchen Datums, regelmäßig nur mit ausdrücklicher Einwilligung des Betroffenen im Sinne des Art. 15 Abs. 7 Satz 1 Nr. 2 BayDSG in Betracht kommen dürfte.

Ich habe dazu das fachlich zuständige Staatsministerium des Innern, für Bau und Verkehr um Stellungnahme gebeten. Das Staatsministerium teilte mir mit, dass nachträgliche Streichungen auf der beglaubigten Kopie einer Personenstandsurkunde durch das Standesamt zur Wahrung der urkundlichen Beweisfunktion nicht möglich seien. Die zudem vom Staatsministerium vertretene Auffassung, das Standesamt erhalte aufgrund von § 4 Abs. 2 Personenstandsverordnung (PStV) auch die Befugnis nach Art. 15 Abs. 7 Satz 1 Nr. 1 BayDSG zur Verarbeitung der in den vorgelegten für die Beurkundung erforderlichen Unterlagen enthaltenen besonderen Arten personenbezogener Daten, habe ich jedoch im Hinblick auf die eindeutige Bestimmung des Art. 15 Abs. 7 Satz 1 Nr. 1 BayDSG für nicht überzeugend gehalten.

Zumindest sollte es für die Betroffenen möglich sein, sich beim Ausstellungsstandesamt zu erkundigen, ob nicht eine „neue“ Urkunde ohne die entsprechenden Angaben ausgestellt werden kann. Das Staatsministerium hat meine Anregung aufgegriffen und die Standesämter entsprechend informiert. Andernfalls ist bei der Entgegennahme der Urkunde die entsprechende (schriftliche) Einwilligung des Betroffenen notwendig.

§ 4 PStV Rückgabe von Urkunden
(2) Bei in fremder Sprache abgefassten Urkunden, denen eine Übersetzung beigefügt ist, soll eine beglaubigte Abschrift oder Ablichtung der Urkunde und der Übersetzung beim Standesamt verbleiben.

6.10 Informantenschutz bei Datenübermittlung an die Staatsanwaltschaft

Die Ausländerbehörde einer bayerischen Kommune hat einen ausländischen Publizisten auf Grund zahlreicher rechtsradikaler Publikationen aus der Bundesrepublik Deutschland ausgewiesen und ihm zugleich die Wiedereinreise verboten. Der Publizist veröffentlichte in der Folge den Ausweisungsbescheid auf seiner Internetseite. Dabei ließ er erkennen, dass er sich entgegen der Ausweisungsverfügung rechtswidrig auf dem Gebiet der Bundesrepublik Deutschland aufhielt. Von diesen Internetveröffentlichungen nahm ein Bürger Kenntnis und verständigte die Ausländerbehörde per E-Mail. Eine irgendwie geartete Rückmeldung seitens der Ausländerbehörde erhielt der Bürger nicht. Einige Zeit später wurde jedoch sein Name auf der Internetseite des ausländischen Publizisten genannt, verbunden mit dem Hinweis, dass der Publizist aufgrund der „Denunziation“ zu einer Geldstrafe verurteilt worden war. Mit der Frage, wie der Publizist seinen Namen habe erfahren können, hat sich der Bürger an mich gewandt.

Meine Nachforschungen ergaben insoweit, dass die Ausländerbehörde aufgrund der E-Mail des Bürgers den Sachverhalt überprüft und anschließend eine Strafanzeige bei der Staatsanwaltschaft gestellt hatte. Die Ausländerbehörde fügte die E-Mail des Bürgers mit dessen Namen der Strafanzeige als Anlage bei. Wohl über

eine Akteneinsicht bei der zuständigen Staatsanwaltschaft gelangte der Publizist an die E-Mail und damit auch an den Namen des Bürgers.

Offenkundig lag hier ein datenschutzrechtlich sensibler Fall vor. Dies hätte die Ausländerbehörde von sich aus berücksichtigen müssen – unabhängig davon, ob sie vom Betroffenen um Vertraulichkeit gebeten wurde. Im Einzelnen:

Mit dem datenschutzrechtlichen Erforderlichkeitsgrundsatz ist es kaum vereinbar, wenn öffentliche Stellen ohne Anlass gezielt personenbezogene Daten im Internet erheben. Daher ist es folgerichtig, wenn Behörden – auch bei einer Anzeigeerstattung gegenüber der Staatsanwaltschaft – dokumentieren, dass keine derartige anlasslose Recherche vorliegt. Allerdings ist es hierfür **grundsätzlich nicht erforderlich, der Staatsanwaltschaft den Namen des Informanten zu nennen**, dessen Informationen der Anlass für die eigenen behördlichen Recherchen waren. Auch müssen zwar **erforderliche Beweismittel** vollständig und von Anfang an der Staatsanwaltschaft übermittelt werden. Ein solches erforderliches Beweismittel lag im konkreten Fall aber **nur** dann vor, **wenn zum Zeitpunkt der behördlichen Recherche der rechtswidrige Aufenthalt des Publizisten in Deutschland nicht mehr aus dem Internet ersichtlich** und der Bürger mit seiner Wahrnehmung daher als Zeuge erforderlich gewesen wäre.

Somit hätte die Ausländerbehörde aufgrund der E-Mail des Bürgers eigene Recherchen anstellen und diese Vorgehensweise sowie das Ergebnis der Recherchen der Staatsanwaltschaft grundsätzlich **zunächst ohne Namensnennung** mitteilen müssen. Zumindest aber hätte sich die Ausländerbehörde **vor der Preisgabe des Namens** gegenüber der Staatsanwaltschaft mit dem Bürger **ins Benehmen setzen** müssen.

Gleichwohl habe ich jedoch im Rahmen des mir gemäß Art. 31 Abs. 3 BayDSG zustehenden Ermessens von einer Beanstandung abgesehen. Auch bei dem von mir empfohlenen datenschutzfreundlicheren Vorgehen wäre eine Preisgabe der Identität des Bürgers nicht völlig ausgeschlossen gewesen. Falls sie dies für notwendig erachtet hätte, hätte die Staatsanwaltschaft eine entsprechende Auskunft bei der Ausländerbehörde anfordern bzw. die zuständigen Beamten vernehmen können. In diesem Fall hätte die Ausländerbehörde die Preisgabe des Namens gegenüber der Staatsanwaltschaft nur über eine Verweigerung der Aussagegenehmigung oder eine Sperrerklärung für Aktenteile bzw. Auskünfte nach § 96 Strafprozessordnung verhindern können. Dessen enge Tatbestandsvoraussetzungen dürften nicht vorgelegen haben. Auch wird der Anzeigenerstatter oder Zeuge im Rahmen einer Akteneinsicht des Beschuldigten bei der Staatsanwaltschaft grundsätzlich nicht geschützt. Der Beschuldigte erhält vielmehr grundsätzlich vollständige Akteneinsicht und erfährt so auch den Namen des Zeugen. Allenfalls bei tatsachengestützten Gefahren konkreter schwerwiegender Nachteile für den Zeugen können im seltenen Ausnahmefall bestimmte Personalien des Zeugen geschwärzt werden. Für das Vorliegen dieser strengen Anforderungen gab es zum damaligen Zeitpunkt jedoch wohl keine hinreichenden Anhaltspunkte.

6.11 Nochmals: Bekanntgabe des Namens des Anzeigeerstatters durch die Behörde an den Angezeigten

Zu der Frage, unter welchen Voraussetzungen eine Behörde dem Angezeigten den Namen des Behördeninformanten mitteilen darf, habe ich mich wiederholt in meinen Tätigkeitsberichten geäußert, zuletzt im 24. Tätigkeitsbericht 2010 unter

Nr. 6.10. Gleichwohl musste ich auch in diesem Berichtszeitraum wieder öffentliche Stellen beanstanden, die die Namen der Anzeigeerstatter in unzulässiger Weise weitergegeben hatten. Dies geschah entweder auf Nachfrage des Angezeigten oder durch die Weiterleitung des Beschwerdeschreibens an diesen mit dem Namen und der Anschrift des Anzeigeerstatters. Ich weise deshalb nochmals auf Folgendes hin:

Dem Bürger, der eine Behörde auf tatsächliche oder vermeintliche Missstände und Verstöße gegen Rechtsvorschriften hinweist, sollen dadurch keine Nachteile entstehen. Er vertraut darauf, dass seine Hinweise im Bereich der Verwaltung verbleiben. Dies gilt unabhängig davon, ob der Informant ausdrücklich um vertrauliche Behandlung gebeten hat. Die vertrauliche Behandlung solcher Hinweise ist auch im Interesse von Behörden, die zur ordnungsgemäßen Erfüllung ihrer Aufgaben auf derartige Informationen angewiesen sind. Der Informant ist nur dann nicht schutzwürdig, wenn es sich um haltlose, grob unwahre oder gar verleumderische Angaben handelt. Die Weitergabe des Namens und der Anschrift des Informanten an den Angezeigten ist in diesem Fall zulässig, wenn sich dieser mit erlaubten Mitteln gegen derartige Angaben zur Wehr setzen will (siehe dazu auch Wilde/Ehmann/Niese/Knoblauch, BayDSG, Art. 10 Rn. 49a - k m.w.N.).

6.12 Datenerhebung bei Dritten vor Ablauf einer der Betroffenen eingeräumten Frist zur Stellungnahme

Eine Petentin wandte sich an mich, weil sie aufgrund ihrer Beschäftigung bei einem Arbeitgeber in der Stadt X im dortigen Bürgerbüro vorgesprochen habe, um einen Nebenwohnsitz anzumelden. Lebensmittelpunkt sei ihr Hauptwohnsitz in Berlin, wo sie auch in einem Home Office arbeite. Die Stadt X sei jedoch davon ausgegangen, dass es sich bei der Wohnung in X um den Hauptwohnsitz handle. Denn die Entfernung zur (bisherigen) Hauptwohnung in Berlin betrage mehrere hundert Kilometer. Bei einer Beschäftigung in X sei es deshalb unwahrscheinlich, dass die Berliner Wohnung den Lebensmittelpunkt bilde. Die Stadt X habe sie daraufhin zur beabsichtigten Festsetzung der Hauptwohnung angehört und ihr die Möglichkeit zur Äußerung sowie zur Vorlage von Nachweisen, etwa des Arbeitsvertrages, innerhalb einer Frist von zwei Wochen gegeben. Ohne diese Frist abzuwarten, sei ihr Arbeitgeber (telefonisch und schriftlich) kontaktiert und nach Absprachen zu einem Home Office in Berlin sowie einer Kopie des Arbeitsvertrages gefragt worden. Daraufhin habe sie sich schriftlich bei der Stadt über die Kontaktaufnahme mit ihrem Arbeitgeber beschwert und gebeten, evtl. Anfragen an sie zu richten und die Anhörungsfrist abzuwarten.

In ihrer Stellungnahme verwies die Stadt darauf, sie sei nach Art. 26 Bayerisches Verwaltungsverfahrensgesetz (BayVwVfG) zur Sachverhaltsaufklärung berechtigt und verpflichtet. Hierzu dürfe sie sich aller erforderlichen Beweismittel bedienen, insbesondere auch Auskünfte einholen.

In datenschutzrechtlicher Hinsicht habe ich das Vorgehen der Stadt wie folgt bewertet:

Gemäß Art. 2 Abs. 8 BayDSG gehen die Vorschriften des Bayerischen Datenschutzgesetzes denen des Bayerischen Verwaltungsverfahrensgesetzes (BayVwVfG) vor, soweit bei der Ermittlung des Sachverhalts personenbezogene Daten erhoben, verarbeitet oder genutzt werden. Bei der Sachverhaltsermitt-

lung verdrängt wird insbesondere Art. 26 BayVwVfG. Von der „Sachverhaltsermittlung“ umfasst sind z.B. auch Datenübermittlungen im Zuge einer Erhebung (vgl. Wilde/Ehmann/Niese/Knoblauch, BayDSG, Art. 2 Rn. 84).

Die Erhebung personenbezogener Daten ist in Art. 16 BayDSG geregelt. Sie ist zulässig, wenn ihre Kenntnis zur Erfüllung der in der Zuständigkeit der erhebenden Stelle liegenden Aufgaben erforderlich ist (Art. 16 Abs. 1 BayDSG). Art. 16 Abs. 2 Satz 1 BayDSG normiert dabei den Grundsatz der Datenerhebung beim Betroffenen mit dessen Kenntnis. Bei Dritten dürfen personenbezogene Daten nur ausnahmsweise erhoben werden, etwa dann, wenn eine Rechtsvorschrift eine solche Erhebung vorsieht oder zwingend voraussetzt (Art. 16 Abs. 2 Satz 2 Nr. 1 BayDSG). Zulässig ist eine Datenerhebung bei Dritten auch, wenn

1. die zu erfüllende Verwaltungsaufgabe ihrer Art nach oder im Einzelfall eine solche Erhebung erforderlich macht oder

2. die Erhebung beim Betroffenen einen unverhältnismäßigen Aufwand (Alt. 1) erfordern würde oder keinen Erfolg (Alt. 2) verspricht

und keine Anhaltspunkte dafür bestehen, dass überwiegende schutzwürdige Interessen des Betroffenen beeinträchtigt werden (Art. 16 Abs. 2 Satz 2 Nr. 2 BayDSG).

Es gab keine Rechtsgrundlage, die den Arbeitgeber der Petentin zur Auskunft verpflichtet hätte. Jedenfalls innerhalb der Anhörungsfrist hatte die Stadt auch nach Art. 16 Abs. 2 Satz 2 Nr. 2 Buchst. b) Alt. 2 BayDSG keine Datenerhebungsbefugnis bei Dritten:

Soweit die Kontaktaufnahme mit dem Arbeitgeber noch während der Anhörungsfrist erfolgte, durfte die Stadt nicht unterstellen, dass eine Datenerhebung bei der Petentin generell nicht erfolgversprechend gewesen wäre. Das wäre jedoch nach Art. 16 Abs. 2 Satz 2 Nr. 2 Buchst. b) Alt. 2 BayDSG die Voraussetzung für eine Datenerhebung bei Dritten gewesen. Auch nachdem sich die Petentin schriftlich gegenüber der Stadt geäußert und sogar ausdrücklich darum gebeten hatte, evtl. Anfragen an sie zu richten, wurde dennoch innerhalb der Anhörungsfrist erneut der Arbeitgeber angeschrieben und mitgeteilt, die Petentin käme trotz Aufforderung ihrer Auskunftspflicht nicht nach. Tatsächlich unternahm die Stadt auf das Schreiben der Petentin hin keine weiteren Versuche, die benötigten Unterlagen von ihr selbst zu erhalten. Dabei hätte die Auskunftspflicht der Petentin nach Art. 18 Bayerisches Meldegesetz sogar mit Mitteln des Verwaltungszwangs durchgesetzt werden können. Zumindest wäre es ohne Weiteres möglich gewesen, die Petentin vorab darauf hinzuweisen, dass bei fehlender Mitwirkung ggf. eine Anfrage bei ihrem Arbeitgeber in Betracht kommt. Gründe, weshalb ein weiteres Zuwarten unzumutbar gewesen wäre, waren weder ersichtlich und wurden von der Stadt auch nicht angeführt.

Durch das vorzeitige Herantreten an den Arbeitgeber wurden überwiegende schutzwürdige Interessen der Petentin verletzt. Eine Beeinträchtigung überwiegender schutzwürdiger Interessen war bereits deshalb anzunehmen, weil entgegen der der Betroffenen eingeräumten Anhörungsfrist (unter Verstoß gegen Treu und Glauben) und ohne deren Wissen ihr Arbeitgeber um Auskunft ersucht wurde.

Den Datenschutzverstoß habe ich beanstandet.

6.13 Datenübermittlung an Wohnungseigentümer im Rahmen der Erteilung eines Wohnberechtigungsscheins

Aufgrund einer Eingabe überprüfte ich den nachfolgenden Sachverhalt:

Die Eingabeführerin hatte bei einer Stadt den Antrag auf Erteilung eines Wohnberechtigungsscheins für eine bestimmte, öffentlich geförderte Wohnung der dortigen Baugenossenschaft gestellt. Auf eine telefonische Nachfrage der Baugenossenschaft hin wurde seitens der Stadt die Auskunft erteilt, dass die Antragstellerin die Voraussetzungen für die Erteilung des Wohnberechtigungsscheins erfüllt. Der Wohnberechtigungsschein selbst wurde erst nach erfolgter Vergabeentscheidung ausgestellt und an die Petentin versandt.

Die betreffende Stadt hat mir gegenüber darauf hingewiesen, dass ihr Vorgehen der gängigen Praxis bei der Vergabe öffentlich geförderter Wohnungen entsprechen würde. Eine bereichsspezifische Vorschrift, die die Stadt zur Datenübermittlung an die Baugenossenschaft berechtigt hätte, nannte sie nicht. Aus datenschutzrechtlicher Sicht habe ich Bedenken geäußert, ob derartige Datenübermittlungen generell auf Art. 19 Abs. 1 Nr. 2 BayDSG gestützt werden können. Nach dieser Vorschrift ist eine Datenübermittlung an nicht-öffentliche Stellen (hier: die Baugenossenschaft) zulässig, wenn die nicht-öffentliche Stelle ein berechtigtes Interesse an der Kenntnis der zu übermittelnden Daten glaubhaft darlegt und der Betroffene kein schutzwürdiges Interesse an dem Ausschluss der Übermittlung hat.

Vorliegend hatte sich die Baugenossenschaft bei der Stadt telefonisch danach erkundigt, ob die Antragstellerin die Voraussetzungen für die Erteilung eines Wohnberechtigungsscheins erfüllt, um diese in die Vorschlagsliste für die Wohnungsvergabe aufnehmen zu können. Ein berechtigtes Interesse der Baugenossenschaft kann damit grundsätzlich bejaht werden, da nur berechtigte Personen bei der Wohnungsvergabe berücksichtigt werden sollen.

Ob die betroffene Person ein schutzwürdiges Interesse an dem Ausschluss der Übermittlung hat, beurteilt sich maßgeblich anhand der Sensibilität der Daten (vgl. Wilde/Ehmann/Niese/Knoblauch, BayDSG, Art. 19 Rn. 20). Hier ist zu berücksichtigen, dass der Baugenossenschaft die Tatsache, dass ein Antrag auf Feststellung der Wohnberechtigung gestellt wurde und das Ergebnis der Prüfung dieses Antrags mitgeteilt wurde. Zwar kann die Datenübermittlung möglicherweise auch im Interesse der Betroffenen liegen (Beschleunigung des Auswahl- und Vergabeverfahrens), zumal sie sich im Vorfeld bereits beim Wohnungseigentümer um die betreffende Sozialwohnung beworben hat. Gleichwohl lässt die Auskunftserteilung bezüglich des Ergebnisses der Antragsprüfung immer auch Rückschlüsse auf die tatsächliche soziale Situation der Betroffenen zu. Deshalb kann letztlich ein schutzwürdiges Interesse an dem Ausschluss der Übermittlung nicht ausgeschlossen werden.

Vor diesem Hintergrund habe ich – vor einer evtl. Auskunftserteilung gegenüber dem Verfügungsberechtigten – die Einholung einer Einwilligung des Wohnungssuchenden gemäß Art. 15 Abs. 1 Nr. 2 BayDSG angeraten.

In der Angelegenheit habe ich das fachlich zuständige Staatsministerium des Innern, für Bau und Verkehr um Stellungnahme gebeten. Es hat ergänzend darauf hingewiesen, dass nach Art. 14 Abs. 1 Satz 1 Bayerisches Wohnraumförderungsgesetz (BayWoFG) geförderter Wohnraum – wenn kein Benennungsverfahren

durchzuführen ist – nur aufgrund eines vom Wohnungssuchenden vorgelegten Wohnberechtigungsscheins überlassen werden darf. Damit hat es der Wohnungsuchende selbst in der Hand, wem die darin enthaltenen Daten zugänglich gemacht werden. Eine unmittelbare Auskunftserteilung durch die zuständige Stelle an den Verfügungsberechtigten kann nach dieser eindeutigen gesetzlichen Regelung die Ausstellung und Übergabe eines Wohnberechtigungsscheins nicht ersetzen. Das Staatsministerium hat die nachgeordneten Behörden durch Rundschreiben entsprechend informiert und dabei auch auf die datenschutzrechtliche Problematik hingewiesen.

Art. 14 BayWoFG Überlassung von Mietwohnraum
(1) [1]Der Vermieter darf Wohnraum nach Maßgabe der Förderentscheidung nur einem Wohnungssuchenden überlassen, dessen Wohnberechtigung sich aus einem vom Wohnungssuchenden vorgelegten Wohnberechtigungsschein oder einer Benennung durch die zuständige Stelle ergibt. [2]In der Förderentscheidung kann die Benennung eines oder mehrerer Wohnungssuchender bestimmt werden.

6.14 Datenwiederherstellung nach Bürgermeisterwechsel

Ein neu gewählter Bürgermeister musste beim Amtsantritt feststellen, dass sein langjähriger Vorgänger keinerlei Akten im Bürgermeisterbüro hinterlassen hatte und es anscheinend auch zu größeren Datenlöschungen auf dem Laufwerk „Bürgermeister“ des gemeindlichen Servers gekommen war. Der neue Bürgermeister hat mich daraufhin um Beratung gebeten, was bei einer Datenwiederherstellung – durch einen von der Gemeinde beauftragten EDV-Dienstleister – zu beachten ist. Hierzu habe ich aus datenschutzrechtlicher Sicht vor allem auf Folgendes hingewiesen:

— Datenschutzrechtliche Fragen im Sinne des Bayerischen Datenschutzgesetzes stellen sich nur insoweit, als personenbezogene Daten nach Art. 4 Abs. 1 BayDSG betroffen sind. Hierbei handelt es sich um **„Einzelangaben über persönliche oder sachliche Verhältnisse bestimmter oder bestimmbarer natürlicher Personen (Betroffene)“.** Reine Sachdaten wie beispielsweise Angaben über Art, Umfang und Kostenvolumen eines gemeindlichen Bauvorhabens werden nicht schon dadurch zu personenbezogenen Daten gemäß Art. 4 Abs. 1 BayDSG, dass diese Daten auf dem Laufwerk des vormaligen Bürgermeisters gespeichert waren. Sowohl eine Löschung als auch die Wiederherstellung derartiger Daten ist unter dem Blickwinkel des Bayerischen Datenschutzgesetzes daher von vornherein irrelevant.

— Soweit personenbezogene Daten im Sinne des Art. 4 Abs. 1 BayDSG betroffen sind, ist zu beachten, dass nach den das Datenschutzrecht durchziehenden Grundsätzen der informationellen Gewaltenteilung sowie der Erforderlichkeit des jeweiligen Datenumgangs nicht jeder Mitarbeiter im Rathaus auf alle dort über die Bürgerinnen und Bürger gespeicherten Daten zugreifen darf. Vielmehr gilt das Prinzip: Jeder darf nur auf solche Daten zugreifen können, die er für seine Aufgaben benötigt. Dies gilt grundsätzlich auch für den Bürgermeister. **Zur Wahrnehmung seiner Aufgaben ist es nicht erforderlich, jederzeit und umfassend auf die Datenbestände der Gemeinde zuzugreifen.** Als verantwortlicher Leiter der örtlichen Verwaltung kann sich der Bürgermeister aber anlassbezogen im konkreten Einzel-

fall – soweit erforderlich – informieren und die einschlägigen Akten vorlegen lassen beziehungsweise auf die Daten des konkreten Vorgangs zugreifen.

– Vor diesem Hintergrund ist das oftmals festzustellende Anlegen umfangreicher (elektronischer) Handaktenbestände aus datenschutzrechtlicher Sicht kritisch zu sehen. Denn diese Praxis führt zu parallelen – und noch dazu regelmäßig gegen unberechtigte Zugriffe nur unzureichend geschützten – Datenbeständen. Soweit es sich in dem eingangs geschilderten Sachverhalt also um die Löschung (elektronischer) Handaktenbestände gehandelt haben sollte, ist deren (sachgerechte) Löschung vom Grundsatz her datenschutzfreundlich und eine Wiederherstellung folglich kritisch zu hinterfragen. Ausreichend für die Aufgabenerfüllung des neuen Bürgermeisters ist es insoweit nämlich regelmäßig, dass sich der entsprechende Vorgang in der beim jeweils zuständigen Sachbearbeiter geführten Sachakte findet. **Eine Wiederherstellung (elektronischer) Handaktenbestände erscheint daher nicht erforderlich und nur schwerlich datenschutzkonform.**

– **Soweit es sich dagegen um die Wiederherstellung originär beim vormaligen Bürgermeister in dessen eigener Zuständigkeit geführter Aktenbestände handelt, darf mit diesen Daten insoweit umgegangen werden, als es für die Amtsführung des neuen Bürgermeisters erforderlich ist.**

– **Offensichtlich private oder persönliche Daten des vormaligen Bürgermeisters** wie beispielsweise Arztrechnungen oder private Anschreiben **dürfen dagegen nicht eingesehen werden beziehungsweise sind zu löschen, sobald deren private/persönliche Natur erkannt wird**. Zu diesem Bereich wird man regelmäßig auch Parteiangelegenheiten zählen müssen.

– Bei der Beauftragung einer externen Firma zur Wiederherstellung personenbezogener Daten handelt es sich um eine Auftragsdatenverarbeitung im Sinne des Art. 6 BayDSG, wobei der Auftraggeber für die Einhaltung der Vorschriften des Bayerischen Datenschutzgesetzes und anderer Vorschriften über den Datenschutz verantwortlich bleibt (Art. 6 Abs. 1 BayDSG). Insofern hat der Auftraggeber dafür Sorge zu tragen, dass der Auftragnehmer die gleichen datenschutzrechtlichen Vorgaben einhält, wie er selbst.

6.15 Widerspruchsrechte der Eltern beachtet – Rechte des Kindes missachtet

Melderegisterauskünfte zu Wahlwerbezwecken waren bereits in der Vergangenheit immer wieder Thema in meinen Tätigkeitsberichten (siehe 23. Tätigkeitsbericht 2008 Nr. 10.3, 20. Tätigkeitsbericht 2002 Nr. 10.3) Obwohl die melderechtlichen Bestimmungen den Meldebehörden hinlänglich bekannt sein dürften, muss ich dennoch immer wieder Verstöße feststellen, wie der folgende Fall zeigt:

Ein Vater hatte sich an mich gewandt und sich darüber beschwert, dass sein zweijähriger Sohn im Zusammenhang mit den Kommunalwahlen ein an ihn persönlich andressiertes Wahlwerbeschreiben erhalten habe. Für ihn selbst und seine Ehefrau hingegen seien Übermittlungssperren im Melderegister eingetragen.

In ihrer Stellungnahme teilte mir die betreffende Gemeinde mit, dem Vorsitzenden des Ortsverbandes einer Partei sei auf dessen Wunsch hin gemäß Art. 32 Meldegesetz (MeldeG) eine Liste aller Haushalte (Einwohner- und Geburtsdaten) übermittelt worden. Dabei seien in zehn Fällen auch Daten von nicht wahlberechtigten Personen übermittelt worden. Die zum Zeitpunkt der Auskunftserteilung eingetragenen Übermittlungssperren seien jedoch beachtet worden.

Diesen Sachverhalt habe ich wie folgt beurteilt:

Nach Art. 32 Abs. 1 Sätze 1 bis 3 MeldeG darf die Meldebehörde Parteien, Wählergruppen und anderen Trägern von Wahlvorschlägen im Zusammenhang mit allgemeinen Wahlen und Abstimmungen auf staatlicher oder kommunaler Ebene in den sechs der Stimmabgabe vorangehenden Monaten Auskunft aus dem Melderegister über Vor- und Familiennamen, Doktorgrad und Anschriften von Gruppen von Wahlberechtigten erteilen, für deren Zusammensetzung das Lebensalter der Betroffenen bestimmend ist, es sei denn, der Bürger hat dieser Weitergabe seiner Daten widersprochen. Die Geburtstage der Wahlberechtigten dürfen dabei nicht mitgeteilt werden.

Eine nach Art. 32 Abs. 1 Satz 1 MeldeG zulässige Gruppenauskunft muss sich demnach auf eine Gruppe von Wahlberechtigten beschränken, für deren Zusammensetzung ausschließlich das Lebensalter der Betroffenen maßgeblich ist. Danach ist es grundsätzlich nicht zulässig, die Daten aller Wahl- oder Stimmberechtigten mitzuteilen. Aus dem Gesetzeswortlaut „Gruppe“ wird deutlich, dass sich die Auskunft immer nur auf einen Teil der Wahl- oder Stimmberechtigten beziehen darf. Geburtsdaten dürfen ausdrücklich nicht mitgeteilt werden, ebensowenig die Daten nicht wahlberechtigter Personen.

Eine Auskunft über alle Haushalte, wie sie vorliegend erteilt wurde und die zudem die Geburtsdaten sowie auch die Daten von nicht wahlberechtigten Personen umfasst, stellt in mehrfacher Hinsicht einen Verstoß gegen Art. 32 Abs. 1 MeldeG dar. Die unzulässige Datenübermittlung habe ich beanstandet, da in erheblichem Maße gegen datenschutzrechtliche Bestimmungen verstoßen wurde und zumindest im Fall des Petenten die für die Eltern eingetragenen Übermittlungssperren gleichsam ausgehebelt wurden, indem die Daten des minderjährigen Kindes übermittelt wurden.

Art. 32 MeldeG Melderegisterauskünfte in besonderen Fällen
(1) [1]Die Meldebehörde darf Parteien, Wählergruppen und anderen Trägern von Wahlvorschlägen im Zusammenhang mit allgemeinen Wahlen und Abstimmungen auf staatlicher oder kommunaler Ebene in den sechs der Stimmabgabe vorangehenden Monaten Auskunft aus dem Melderegister über die in Art. 31 Abs. 1 Satz 1 bezeichneten Daten von Gruppen von Wahlberechtigten erteilen, für deren Zusammensetzung das Lebensalter der Betroffenen bestimmend ist. [2]Die Geburtstage der Wahlberechtigten dürfen dabei nicht mitgeteilt werden. [3]Die Betroffenen haben das Recht, der Weitergabe ihrer Daten nach Satz 1 zu widersprechen.

7 Gesundheitswesen

7.1 Gesundheitsamt

7.1.1 Prüfungen in den Gesundheitsämtern

Im Berichtszeitraum habe ich im Bereich Gesundheit den Schwerpunkt meiner Prüfungen darauf gelegt, mir einen aktuellen Überblick über die Einhaltung datenschutzrechtlicher Bestimmungen bei den Gesundheitsämtern zu verschaffen.

Im Wesentlichen ging ich der Frage nach, in welcher Weise die Gesundheitsämter die Geheimhaltungspflichten und Verwertungsverbote des Art. 30 Abs. 1 Gesundheitsdienst- und Verbraucherschutzgesetz (GDVG) sicherstellen. Die Vorschrift trägt dem Umstand Rechnung, dass der öffentliche Gesundheitsdienst neben seinen hoheitlichen Aufgaben in vielfältiger Weise auch beratende und aufklärende Funktionen übernimmt. Im Rahmen freiwilliger Inanspruchnahme entstehen Vertrauensverhältnisse zum Probanden, in denen der Arzt oder das nichtärztliche Fachpersonal gemäß § 203 Strafgesetzbuch zur Geheimhaltung verpflichtet ist.

Art. 30 GDVG Datenschutz, Geheimhaltungspflichten
(1) [1]Die Behörden für Gesundheit, Veterinärwesen, Ernährung und Verbraucherschutz dürfen Geheimnisse, die Amtsangehörigen in der Eigenschaft als Arzt, Tierarzt oder als andere gemäß § 203 Abs. 1 oder 3 des Strafgesetzbuchs (StGB) zur Wahrung des Berufsgeheimnisses verpflichtete Person

1. *in Wahrnehmung der in Art. 13 und 14 genannten Aufgaben,*
2. *im Zusammenhang mit einer Untersuchung oder Begutachtung, der sich der Betroffene freiwillig unterzogen hat oder*
3. *bei einer Beratung von Tierhaltern im Rahmen des Art. 19 Abs. 1 Nr. 3 anvertraut oder sonst bekannt geworden sind, bei der Erfüllung einer anderen Aufgabe als der, bei deren Wahrnehmung die Erkenntnisse gewonnen wurden, nicht verarbeiten oder nutzen. … [5] Die Wahrung der Geheimhaltungspflichten und Verwertungsverbote ist von den Behörden für Gesundheit, Veterinärwesen, Ernährung und Verbraucherschutz durch angemessene Maßnahmen auch organisatorisch sicherzustellen.*

– Schon die Organisation der Zuständigkeiten innerhalb des Gesundheitsamts muss eine datenschutzgerechte Trennung der Aufgabenbereiche ermöglichen. Nach Möglichkeit sollte einem Sachgebiet bzw. nur bestimmten Sachbearbeitern der Bereich der freiwilligen gesundheitlichen Aufklärung und Beratung zur weitgehend eigenverantwortlichen Aufgabenerfüllung übertragen sein. Hoheitliche Aufgaben, auch solche, die im fachlichen Zusammenhang mit freiwillig in Anspruch zu nehmenden Angeboten stehen, sollten dagegen von den anderen Sachgebieten bzw. von anderen Sachbearbeitern wahrgenommen werden. Ich empfehle im Rahmen der personellen und strukturellen Vorgaben eine sachgebietsbezogene Aufteilung in die übergeordneten Bereiche Medizinisches Gutachterwesen, Infektionsschutz und Hygiene sowie Gesundheitsförderung.

Meine Prüfungen ergaben, dass die Umsetzung der gesetzlichen Vorgaben des Art. 30 GDVG ganz erheblich von der Behördengröße und von der personellen Ausstattung des jeweiligen Gesundheitsamts abhängt. Kleinere Gesundheitsämter nehmen oft eine organisatorische Aufgabentrennung nach den verschiedenen im Gesundheitsamt tätigen Berufsgruppen vor (Ärzte, Sozialpädagogen o.ä., Sozialmedizinische Assistenten, Hygienekontrolleure). Die **berufsbezogene Aufgabenzuordnung** ist eine effektive Möglichkeit, den datenschutzrechtlichen Organisationsanforderungen weitgehend gerecht zu werden. Das gilt erst recht, wenn eine datenschutzgerechte Sachgebietsaufteilung aufgrund der geringen Größe bzw. der geringen Zahl der Mitarbeiter und Verantwortungsträger nicht sinnvoll zu realisieren ist. Allerdings können hierbei problematische Doppelzuständigkeiten für hoheitliche Aufgaben und Aufgaben der Gesundheitsförderung und Beratung nur dann vermieden werden, wenn zusätzliche Maßnahmen ergriffen werden (z.B. Aufgabenzuweisung an unterschiedliche Sachbearbeiter, Vertretungsregelungen, getrennte Aktenverwaltung und -aufbewahrung).

— In Bezug auf die Frage, wie sich Art. 30 Abs. 1 GDVG auf die Aktenverwaltung der Gesundheitsämter auswirkt, habe ich – wie auch schon bei vorangegangenen Prüfungen – leider erneut feststellen müssen, dass sich die geprüften Gesundheitsämter in der Regel nicht auf speziell für den Gesundheitsamtsbereich gültige **Dienstanweisungen** stützen können. Dabei liegt es auf der Hand, dass die vorhandenen allgemeinen Geschäftsanweisungen der Landratsämter und Städte die besonderen datenschutzrechtlichen Anforderungen nicht ausreichend abbilden. Dementsprechend habe ich bei meinen aktuellen Prüfungen wieder sehr unterschiedliche, zum Teil auch problematische Verfahrensweisen festgestellt, wenn es um die Frage ging, ob und wie die gesetzlich gebotene Trennung personenbezogener Unterlagen aus der Beratung, Untersuchung und Begutachtung auf freiwilliger Basis von den sonstigen im Gesundheitsamt vorhandenen personenbezogenen Aktenbeständen umgesetzt ist.

  So haben sich etwa in Bezug auf die Führung der **Registratur** Beispielsfälle dafür ergeben, dass dort, wo die Zentraldatei oder -kartei Hinweise auf Vorgänge zu freiwillig in Anspruch genommenen Angeboten des Gesundheitsamts enthält, diese auch den Anlass zum Informationsaustausch bis hin zur Zusammenführung der vorhandenen Unterlagen geben. Beides ist mit Art. 30 Abs. 1 GDVG grundsätzlich nicht vereinbar. Es darf nicht offen lesbar sein, aus welchen Gründen sich jemand zur freiwilligen Beratung oder Begutachtung ins Gesundheitsamt begeben hat. Nur formale Hinweise, in welchen Sachgebieten oder bei welchen Sachbearbeitern Vorgänge zu bestimmten Personen vorhanden sind, dürfen angezeigt werden, soweit sie notwendig sind, um Eingänge oder Anfragen in einer Zentrale zuordnen oder weitervermitteln zu können. Aus der Angabe eines bestimmten Sachgebiets oder Sachbearbeiters dürfen jedoch keine Rückschlüsse auf bestimmte Erkrankungen gezogen werden können (z.B. Sucht, psychische Erkrankungen, Beratung zu ansteckenden Krankheiten). Ist dies nicht vermeidbar, empfiehlt es sich in den relevanten Bereichen sowohl die Aktenverwaltung als auch die Aktenaufbewahrung sachgebiets- bzw. sachbearbeiterbezogen zu organisieren. Dies wird in einigen der geprüften Gesundheitsämter auch so praktiziert. Registraturen werden bei den Gesundheitsämtern im Übrigen heutzutage meist elektronisch verwaltet. Die verwendeten Software-Produkte zur Aktenverwaltung ermöglichen es, diese nur als

Suchdatei ohne Informationen über den Speicheranlass zu nutzen und weitergehende Informationen nur dann anzuzeigen, wenn entsprechende Berechtigungen bestehen.

Ich habe mir zudem die Aktenführung genauer angesehen. Auch wenn es in den Gesundheitsämtern schon Bestrebungen gibt, Akten ausschließlich elektronisch zu führen, dominiert noch die **papiergebundene Aktenführung**. Soweit es erforderlich ist, personenbezogene Akten anzulegen, werden in der Regel keine Einheitsakten in dem Sinne geführt, dass Unterlagen des Gesundheitsamts über ein und dieselbe Person aus freiwilliger Beratung oder freiwilliger Begutachtung einerseits und hoheitlicher Tätigkeit andererseits in einer Akte zusammengefasst werden. Mir fiel allerdings auf, dass insbesondere beim ärztlichen Dienst häufig Personenakten entstehen, die sämtliche Vorgänge enthalten, wegen denen der Betreffende untersucht oder begutachtet wurde. Es ist hier jedoch zu beachten, dass sich der Betroffene den jeweiligen Untersuchungen beim ärztlichen Dienst in vielen Fällen freiwillig unterzieht (z.B. im Auftrag des Dienstherrn, des Arbeitgebers, des Sozialamts). Folglich gelten die Geheimhaltungspflichten des Art. 30 Abs. 1 Satz 1 Nr. 2 GDVG. Für unterschiedliche Aufgaben, also insbesondere in Bezug auf verschiedene Auftraggeber bzw. nicht im Zusammenhang stehende Fragestellungen darf daher eine Zusammenfassung der Daten in einer Akte nur dann erfolgen, wenn Art. 30 Abs. 1 GDVG dem nicht entgegensteht (siehe Art. 30 Abs. 2 GDVG) und beispielsweise hinsichtlich der Heranziehung bereits vorhandener Dokumentationen die Einwilligung des Betroffenen vorliegt.

Zur räumlichen Aufbewahrung der Papierakten stellte ich fest, dass diese meist dezentral im jeweiligen Sachgebiet bzw. beim zuständigen Sachbearbeiter erfolgt, soweit die jeweiligen Vorgänge noch nicht abgeschlossen oder jüngeren Datums sind (je nach Raumkapazität). Ältere Akten befinden sich oft in speziellen Archivräumen. Hier werden die Grundsätze der Aktentrennung und -abschottung allerdings häufig nicht ausreichend gewahrt. Insbesondere werden die Akten unabhängig von ihren Inhalten in den gleichen Räumlichkeiten aufbewahrt und bestehen keine nennenswerten Zugangsbeschränkungen. Auch diesbezüglich gilt, dass die datenschutzgerechte Aufbewahrung der Aktenbestände durch geeignete organisatorische Maßnahmen sicherzustellen ist (siehe Art. 30 Abs. 1 Satz 5 GDVG). Insbesondere Akten über freiwillig in Anspruch genommene Leistungen des Gesundheitsamts sind abzuschotten. Daneben sind Zugangsbeschränkungen zu regeln und umzusetzen, indem nur bestimmten, für die Registratur und Archivierung zuständigen Mitarbeitern oder – bei getrennten Räumen – nur den berechtigten Sachbearbeitern der Zugriff bzw. die Entnahme von Akten ermöglicht wird.

– Auf meine ergänzenden Fragen zur Dauer der Aufbewahrung von Gesundheitsamtsdaten bzw. den Zeitpunkt der Aussonderung, Löschung oder Vernichtung ergab die Prüfung vielfältige Vorgehensweisen und einige Mängel. Im Rahmen geführter Prüfungsgespräche ließ sich ein großes Bedürfnis nach Information und Beratung feststellen. So musste zum Teil grundsätzlich darüber aufgeklärt werden, dass dann, wenn es sich nicht um ärztliche Aufzeichnungen handelt und auch keine sonstigen spezialgesetzlichen Aufbewahrungsvorschriften existieren, die notwendige Aufbewahrungsfrist nach dem Erforderlichkeitsgrundsatz zu bestimmen ist. Personenbezogene Daten in Dateien bzw. in Akten sind zu löschen, wenn ihre Kenntnis

für die speichernde Stelle zur Erfüllung der in ihrer Zuständigkeit liegenden Aufgaben nicht mehr **erforderlich** ist (Art. 12 Abs. 1 Nr. 2, Abs. 4 Satz 2 BayDSG). Zu beachten sind hierbei – was nicht bei allen geprüften Ämtern der Fall war – Anbietungspflichten gegenüber Archiven (siehe Art. 6 Abs. 1 Satz 1, Art. 13 Abs. 1 Bayerisches Archivgesetz). Soweit öffentliche Stellen verpflichtet sind, Unterlagen einem öffentlichen Archiv anzubieten, ist eine Löschung zur Aufgabenerfüllung nicht mehr erforderlicher Unterlagen erst dann zulässig, nachdem die Unterlagen dem öffentlichen Archiv angeboten wurden (siehe Art. 12 Abs. 8 BayDSG).

In Anbetracht der Vielzahl der zu verwaltenden Dateien und Akten sollte auf der Basis eines vom jeweiligen Gesundheitsamt zu erstellenden **Aussonderungs- bzw. Löschkonzepts** vorgegangen werden. Damit kann sichergestellt werden, dass in regelmäßigen Abständen geprüft wird, ob Dateien oder Akten auszusondern bzw. nach dem Angebot an das öffentliche Archiv zu löschen sind.

— Ich bin auch noch der Frage nachgegangen, wie im Zusammenhang mit der Aufgabe, gesundheitliche Beratung für Menschen anzubieten, die an einer Sucht oder an einer psychischen Krankheit leiden, von ihr bedroht oder dadurch gefährdet sind (siehe Art. 13 Abs. 1 Satz 2 Nr. 2 GDVG), gewährleistet wird, dass die Geheimhaltungspflichten und Verwertungsverbote des Art. 30 Abs. 1 GDVG gewahrt werden. Zugleich obliegt den Gesundheitsämtern nämlich auch die Aufgabe der Mitwirkung als fachkundige Stelle im Hinblick auf psychisch kranke Personen, die von einer Unterbringung bedroht sind (siehe Art. 13 Abs. 2 Nr. 2 GDVG). Mich interessierte besonders, wie verhindert wird, dass Erkenntnisse aus der freiwilligen Inanspruchnahme bei Begutachtungen in Unterbringungsverfahren Verwendung finden.

  Hierzu ergab sich ein differenziertes Bild. Grundsätzlich war die erforderliche Aufgaben- und Aktentrennung bzw. -abschottung zwar organisatorisch gut bewältigt. In einzelnen Ämtern führten besondere Verfahrensweisen dann aber doch dazu, dass die bestehenden Verwertungsverbote nicht in der gebotenen Weise Beachtung fanden. Nach meinen Prüfungsfeststellungen erhält der medizinische Dienst, der u.a. die Aufträge zur medizinischen Begutachtung im Zusammenhang mit einem Unterbringungsverfahren nach Art. 7 Unterbringungsgesetz bearbeitet, bei manchen Gesundheitsämtern Kenntnis von bereits existierenden Vorgängen zu der betreffenden Person aus dem Bereich des Sozialdienstes. Dies geschieht etwa dadurch, dass durch die Registratur auf solche aus dem Registratursystem ersichtlichen Vorgänge ausdrücklich hingewiesen wird oder dass beim Sozialdienst gezielt nachgefragt wird, ob die betreffende Person bekannt ist. Ist dies der Fall, findet ein Informationsaustausch zumeist in beide Richtungen statt, wenn auch in der Regel, ohne die jeweils fremde Akte zugänglich zu machen. Um eine Geheimnisoffenbarung handelt es sich gleichwohl, so dass es im Einzelfall entsprechender Offenbarungsbefugnisse bedarf (siehe etwa Art. 30 Abs. 2 Satz 2 bzw. Art. 31 Abs. 2 GDVG).

— Ein weiteres Schwerpunktthema meiner Prüfungen betraf die Anlässe und die Art und Weise der Verwendung formularmäßiger Einwilligungserklärungen in die Erhebung, Verarbeitung oder Nutzung personenbezogener Daten bzw. Erklärungen zur Schweigepflichtentbindung bei den Gesundheitsämtern. Ich stellte fest, dass entsprechende Formulare sehr vielfältig

zum Einsatz kommen. Sehr häufig sind die Formulare von den jeweiligen Gesundheitsämtern selbst entworfen worden und unterscheiden sich entsprechend weitreichend. Sie finden zum Teil auch dann Verwendung, wenn gesetzliche Grundlagen für die Erhebung bzw. Übermittlung von Probandendaten bestehen bzw. aufgrund der Gesamtsituation auch von einer wirksamen stillschweigenden Einwilligung des Probanden ausgegangen werden könnte (siehe Art. 30 Abs. 2 GDVG). Ich habe die geprüften Ämter darauf hingewiesen, dass sie Einwilligungserklärungen und insbesondere Erklärungen zur Entbindung von der ärztlichen Schweigepflicht nur dann einsetzen sollten, wenn die angestrebte Erhebung bzw. Übermittlung von personenbezogenen Daten tatsächlich erforderlich ist und keine gesetzliche Befugnisnorm existiert. Liegt eine Befugnis aufgrund von Rechtsvorschriften vor, führt eine zusätzlich eingeholte Einwilligungserklärung nicht unbedingt zur Rechtsklarheit, sondern u.U. zu Folgeproblemen, insbesondere dann, wenn der Proband die Einwilligung verweigert oder widerruft.

– Bei den gesichteten Schweigepflichtentbindungserklärungen war durch die Formulargestaltung nicht immer gewährleistet, dass die Erklärung sämtliche Wirksamkeitsvoraussetzungen erfüllt. Die mir zur Kenntnis gelangten formularmäßigen Entbindungserklärungen waren sehr häufig in Bezug auf die Person oder Institution (z.B. Sachgebiet) innerhalb des Gesundheitsamts sowie in Bezug auf die Person oder Stelle, die entbunden werden soll, zu allgemein gefasst. Die Formulare sind jedoch so zu gestalten, dass die betreffenden Personen und Stellen in dafür vorgesehenen Textfeldern ausdrücklich benannt werden können. In der Regel war den vorgelegten Formularerklärungen auch nicht die konkrete Zielsetzung der Entbindung zu entnehmen. Je nach Gutachterauftrag wird es jedoch häufig ausreichend sein, nur in Bezug auf konkrete medizinische Fragestellungen, jedenfalls aber nur hinsichtlich der aktuellen Begutachtungsthematik von der Schweigepflicht zu entbinden.

– Soweit sich datenschutzrechtliche Mängel in Bezug auf Formulare ergaben, die von zentraler Stelle den Gesundheitsämtern vorgegeben sind, bin ich mit dem zuständigen Staatsministerium in einen Dialog getreten. Die Formulare wurden daraufhin geändert. Dies betraf die beim ärztlichen Dienst Verwendung findende „Beurteilungsgrundlage“, ein Formular im Bereich der Schulgesundheitspflege („Mitteilungsbogen zur Vorlage bei der Schule“) und Musteranschreiben zu Impfbuchkontrollen an Schulen (siehe Nr. 7.1.2).

Die Verbesserung der datenschutzrechtlichen Standards bei den Gesundheitsämtern wird auch weiterhin zu meinen Schwerpunktthemen gehören (zu den technisch-organisatorischen Fragestellungen der Prüfungen siehe Nr. 2.2.2).

7.1.2 Impfberatung in Schulen

Wiederholt habe ich von den Bestrebungen des zuständigen Staatsministeriums berichtet, die Personensorgeberechtigten gesetzlich zu verpflichten, bei Schuleingangsuntersuchungen und weiteren schulischen Impfberatungen den Impfausweis ihres Kindes vorzulegen (siehe hierzu 25. Tätigkeitsbericht 2012 Nr. 7.8 sowie 24. Tätigkeitsbericht 2010 Nr. 7.2). Gemäß Art. 14 Abs. 5 Satz 8 des Gesundheitsdienst- und Verbraucherschutzgesetzes (GDVG) besteht nun seit dem

01.01.2013 eine solche gesetzliche Verpflichtung zur Vorlage von Impfdokumenten im Rahmen schulischer Impfberatungen. Sie gilt zunächst nur für die Dauer von drei Jahren und wird zum 01.01.2016 wieder aufgehoben, wenn sich nicht im Rahmen einer durchzuführenden Evaluation deren Nutzen für eine flächendeckende Impfaufklärung bzw. eine Erhöhung der Durchimpfungsrate feststellen lässt.

Art. 14 GDVG Schutz der Gesundheit von Kindern und Jugendlichen
(5) … [8]Bei der Schuleingangsuntersuchung nach Satz 4 und bei weiteren schulischen Impfberatungen sind vorhandene Impfausweise und Impfbescheinigungen (§ 22 IfSG) der Kinder durch die Personensorgeberechtigten vorzulegen …

Die datenschutzgerechte Umsetzung der schulischen Impfberatung war auch unabhängig von der neu eingeführten Vorlagepflicht für Impfausweise Gegenstand einiger Eingaben und meiner anlassunabhängigen Prüfungen von Gesundheitsämtern. Ich bin insbesondere der Frage nachgegangen, ob die Ämter ihre Verfahrensweise bei schulischen Impfberatungen, speziell in den 6. Jahrgangsstufen (siehe Art. 14 Abs. 5 Satz 8 GDVG, § 10 Abs. 1 Nr. 2 Verordnung zur Schulgesundheitspflege), datenschutzgerecht gestalten, um zu verhindern, dass Lehr- und Verwaltungskräfte, ggf. sogar andere Schüler, Verfügungsmöglichkeiten über die Impfdokumente erlangen und unbefugt Einsicht in diese nehmen können.

Die festgestellten Vorgehensweisen ähnelten sich. Mittels formularmäßigem Informationsblatt, welches in den betroffenen Schulklassen von den Klassenlehrern ausgeteilt wird, werden die Eltern um die Übergabe der Impfausweise gebeten. Diese werden dann entsprechend den Darstellungen im Informationsblatt von den Kindern in die Schule mitgebracht, von den Klassenleitern eingesammelt und meist bis zu dem Tag, an dem die Kontrolle durch Mitarbeiter des Gesundheitsamts stattfindet bzw. die Dokumente vom Gesundheitsamt abgeholt werden, in der Schule verwahrt. Danach werden die Impfausweise mit eingelegten Hinweisblättern zum Impfstatus wiederum über die Schule an die Schulkinder zurückgegeben.

Ich habe den geprüften Gesundheitsämtern und dem zuständigen Staatsministerium für Gesundheit und Pflege mitgeteilt, dass schulisches Personal künftig nur dann bei der Organisation der Impfausweiskontrolle mitwirken könne, wenn die Vertraulichkeit der Impfdokumente gewahrt bleibt. Beispielsweise kann ein Verfahren festgelegt werden, in dem die Impfdokumente in verschlossenen Umschlägen, adressiert an das Gesundheitsamt, in der Schule abgegeben und nach der Durchsicht durch Mitarbeiter des Gesundheitsamts wiederum nur in verschlossenen Umschlägen, mit dem Namen des jeweiligen Schülers versehen, an das Schulpersonal übergeben sowie in dieser Form an die Schüler weitergereicht werden. Die an die Eltern bzw. die Schule und die Klassenleiter gerichteten Informationsblätter, die die Gesundheitsämter vor der Impfausweiskontrolle austeilen, müssen entsprechende Hinweise enthalten.

Das Staatsministerium veranlasste im Rahmen der Verwaltungsvorschrift zum Vollzug des § 20 Abs. 5 des Infektionsschutzgesetzes (IfSG) Regelungen im Sinne der von mir vorgeschlagenen Vorgehensweise und änderte zugleich die Vorlagen für zu verwendende Formblätter (Elternanschreiben, Informationsschreiben an die Schulen). Die Musterformblätter enthalten nun auch einen deutlichen Hinweis auf die neu eingeführte Vorlagepflicht hinsichtlich der Impfdokumente.

7.1.3 Videoüberwachung im Gesundheitsamt (Türklingelanlage)

Ein staatliches Gesundheitsamt fragte bei mir an, ob es aus datenschutzrechtlicher Sicht bedenklich ist, eine Klingelanlage zu installieren, die eine Videoüberwachung ermöglicht. Die Kamera solle nur außerhalb der Öffnungszeiten durch Klingeln und jeweils nur für einen bestimmten Zeitraum aktiviert werden können. Die Überwachung finde am Bildschirm eines Mitarbeiters statt. Eine Aufzeichnung erfolge nicht.

Anhand der übermittelten Informationen konnte ich zwar keine abschließende rechtliche Beurteilung der Zulässigkeit der vorgesehenen Videoüberwachung vornehmen. Ich konnte das anfragende Amt jedoch darauf hinweisen, dass es sich in Bezug auf die vorgetragene datenschutzrechtliche Fragestellung an Art. 21a BayDSG zu orientieren hat. Danach ist die Videobeobachtung (Erhebung) personenbezogener Daten mit Hilfe von optisch-elektronischen Einrichtungen u.a. dann zulässig, wenn dies im Rahmen der Erfüllung öffentlicher Aufgaben oder in Ausübung des Hausrechts erforderlich ist, um öffentliche Einrichtungen oder sonstige bauliche Anlagen öffentlicher Stellen sowie die dort oder in deren unmittelbarer Nähe befindlichen Sachen zu schützen. Gemäß Art. 21a Abs. 1 Satz 2 BayDSG dürfen zudem keine Anhaltspunkte dafür bestehen, dass überwiegende schutzwürdige Interessen der Betroffenen beeinträchtigt werden. In diesem Zusammenhang sind insbesondere die Interessen besonders schutzbedürftiger Personen(gruppen) in den Blick zu nehmen (z.B. Besucher der Schwangerenberatung), für die aller Voraussicht nach nicht ausgeschlossen werden kann, dass sie Gesprächstermine oder Beratungsangebote auch außerhalb der üblichen Öffnungszeiten wahrnehmen bzw. nachfragen (siehe auch meine Ausführungen zur Videoüberwachung in einer Schwangerenberatungsstelle im 25. Tätigkeitsbericht 2012 Nr. 7.9).

Auf meiner Homepage ist ein Prüfungsschema zur Videobeobachtung und Videoaufzeichnung (Videoüberwachung) gemäß Art. 21a BayDSG über „Veröffentlichungen" – „Mustervordrucke" sowie ein Leitfaden für bayerische Kommunen zur Videoüberwachung unter „Themen" – „Kommunales" – „Videoüberwachung – Leitfaden für bayerische Kommunen" abrufbar.

7.2 Krankenhaus

7.2.1 De-Mail im Krankenhaus

Ich bin angefragt worden, ob für die Kommunikation zwischen Patienten und (kommunalen) Kliniken per De-Mail Rechtssicherheit angenommen werden könne. Dazu habe ich folgende Auffassung vertreten:

Gemäß Art. 27 Abs. 6 Bayerisches Krankenhausgesetz (BayKrG) sind insbesondere Schutzmaßnahmen technischer und organisatorischer Art zu treffen, dass Patientendaten nicht unberechtigt verwendet oder übermittelt werden können.

Art. 27 BayKrG Datenschutz
(6) Es sind besondere Schutzmaßnahmen technischer und organisatorischer Art zu treffen, dass Patientendaten nicht unberechtigt verwendet oder übermittelt werden können.

De-Mail garantiert die Authentizität von Sender und Empfänger sowie die gesicherte Zustellung von Nachrichten. Allerdings stellt nur eine Ende-zu-Ende-Verschlüsselung eine durchgängige Verschlüsselung zwischen Versender und Empfänger dar, die für eine Versendung besonders schutzbedürftiger Daten die notwendige Rechtssicherheit bieten kann. Eine Ende-zu-Ende-Verschlüsselung wird vom insoweit einschlägigen De-Mail-Gesetz jedoch nicht gefordert. Für den De-Mail-Diensteanbieter ergeben sich dementsprechend keine Pflichten, eine solche Verschlüsselung vorzusehen. Für den Versand von Daten mit dem Schutzbedarf „sehr hoch" ist eine Ende-zu-Ende-Verschlüsselung jedoch zwingend notwendig. Gesundheitsdaten, insbesondere Patientendaten, die der ärztlichen Schweigepflicht (§ 203 Strafgesetzbuch) unterliegen, sind als besonders schutzbedürftige Daten in aller Regel dem Schutzbedarf „sehr hoch" zuzurechnen. Beim Schutzbedarf „sehr hoch" können die Schadensauswirkungen bei unberechtigtem Zugriff ein existentiell bedrohliches Ausmaß erreichen. Insoweit müssen sich die Nutzer von De-Mail dann selbst um die Installation und Nutzung einer entsprechenden Verschlüsselungssoftware kümmern.

Weitere Informationen enthält die „Handreichung zum datenschutzgerechten Umgang mit besonders schützenswerten Daten beim Versand mittels De-Mail" der Bundesbeauftragten für den Datenschutz und die Informationsfreiheit vom 1. März 2013.

7.2.2 Patientendatenübermittlung an einen Nachlasspfleger

Der behördliche Datenschutzbeauftragte eines meiner Zuständigkeit unterliegenden Krankenhauses richtete an mich die Frage, ob es einem Nachlasspfleger Auskünfte über einen verstorbenen Patienten erteilen dürfe. Er stelle sich insbesondere die Frage, ob der Nachlasspfleger sich selbst von der ärztlichen Schweigepflicht entbinden könne. Ich wies auf Folgendes hin:

Der Nachlasspfleger im Sinne des § 1960 des Bürgerlichen Gesetzbuches (BGB) ist gesetzlicher Vertreter der (noch unbekannten) Erben. Eine Rechtsbeziehung zum verstorbenen Patienten hatte bzw. hat der Nachlasspfleger nicht inne. Nach dem Tod des Patienten, der zugleich Erblasser ist, kann weder der Erbe noch ein naher Angehöriger von der über den Tod des Patienten hinauswirkenden ärztlichen Schweigepflicht entbinden. Eine Vertretung ist insoweit unzulässig (siehe auch 24. Tätigkeitsbericht 2010 Nr. 7.4). Erst recht kann daher der Nachlasspfleger nicht wirksam und zu seinen Gunsten von der Schweigepflicht entbinden. Der Nachlasspfleger ist eine außen stehende Person, die Auskunftserteilung an ihn ist als Datenübermittlung einzustufen (siehe Art. 27 Abs. 5 Satz 1 des Bayerischen Krankenhausgesetzes – BayKrG).

Grundsätzlich gilt, dass sämtliche Patientendaten auch über den Tod des Behandelten hinaus geheim zu halten sind. Allerdings kann sich aus der Erforschung des Willens des verstorbenen Patienten ergeben, dass sein Interesse an der weiteren Geheimhaltung erloschen wäre. Insoweit ist der Wille des Erblassers zu Lebzeiten im Hinblick auf die Schweigepflicht zu ermitteln. Kann dieser nicht festgestellt werden, ist der mutmaßliche Wille des Erblassers zu erforschen, ob er die konkrete Offenlegung durch seinen Arzt billigen oder missbilligen würde (vgl. BGH NJW 1984, Seite 2893). Zu prüfen ist insoweit das wohlverstandene Interesse des Verstorbenen an der weiteren Geheimhaltung der dem Arzt anvertrauten Tatsachen (siehe z.B. Oberlandesgericht Sachsen-Anhalt, Beschluss vom 09.12.2004,

Az.: 4 W 43/04; siehe zum Einsichtsrecht eines Angehörigen in Patientenakten eines Verstorbenen auch 24. Tätigkeitsbericht 2010 Nr. 7.4).

Im Ergebnis kann also die Weitergabe von Patientendaten eines verstorbenen Patienten an den Nachlasspfleger im Einzelfall nach eingehender und gewissenhafter Prüfung der konkreten Umstände und bei hinreichenden Anhaltspunkten für einen entsprechenden (mutmaßlichen) Willen des Verstorbenen gerechtfertigt sein. Die Hauptverantwortung für die Einhaltung der Schweigepflicht vor dem Hintergrund einer ggf. eigenen Strafbarkeit nach § 203 Abs. 1 des Strafgesetzbuches (StGB) obliegt demnach dem Arzt. Ihm kann die Erforschung des mutmaßlichen Willens des Verstorbenen nicht abgenommen werden. Eine Offenlegung kann allerdings nicht einfach „aus grundsätzlichen Erwägungen" verweigert werden (siehe BGH, a.a.O.).

7.2.3 Übersendung eines Krankenhaus-Arztbriefes an namensgleiche Patientin

Aufgrund einer Eingabe erfuhr ich von einem Vorfall, bei dem ein Krankenhaus einen den stationären Aufenthalt einer Patientin betreffenden Arztbrief datenschutzrechtswidrig an die Anschrift einer anderen, bereits verstorbenen Frau verschickt hat. Der Witwer öffnete den dem Anschein nach an seine verstorbene Frau adressierten Brief. Erst nach Kenntnisnahme vom enthaltenen Arztbrief erkannte er, dass dieser eine ihm fremde Frau mit gleichem Namen betraf.

Den Angaben des Krankenhauses zu Folge geschah die falsche Adressierung versehentlich. Dieses Versehen war auch verständlich: Die Verstorbene war zu Lebzeiten ebenfalls Patientin des betreffenden Krankenhauses gewesen; Vor- und Nachnamen der beiden Frauen waren identisch. Hinzu kam sogar noch die Ähnlichkeit des Geburtsdatums, welches nur in einer Ziffer voneinander abwich. Dennoch handelte es sich bei der fehlerhaften Übersendung des Arztbriefes an die falsche Adresse aus datenschutzrechtlicher Sicht um eine unbefugte Übermittlung von Patientendaten. Gemäß Art. 27 Abs. 5 Satz 1 Bayerisches Krankenhausgesetz (BayKrG) ist die Übermittlung von Patientendaten an Dritte zulässig im Rahmen des Behandlungsverhältnisses oder dessen verwaltungsmäßiger Abwicklung oder wenn eine Rechtsvorschrift die Übermittlung erlaubt oder wenn die betroffene Person eingewilligt hat. Keine der genannten Voraussetzungen lag vor. Es handelt sich auch um einen erheblichen Verstoß, da als besonders sensibel einzustufende Patientendaten, die zugleich der ärztlichen Schweigepflicht unterliegen (siehe § 203 Strafgesetzbuch – StGB), unberechtigt weitergegeben wurden.

Von einer förmlichen Beanstandung habe ich in Anbetracht der außergewöhnlichen Umstände abgesehen (Art. 31 Abs. 3 BayDSG). Hierfür sprach auch, dass das Krankenhaus umgehend Maßnahmen ergriff, um vergleichbare Vorfälle zukünftig zu verhindern. Die Mitarbeiter des Krankenhauses wurden abteilungsübergreifend auf die Notwendigkeit der Kontrolle der Richtigkeit der Patientendaten vor jedem Postausgang hingewiesen. Die gegenständliche Personenverwechslung soll außerdem exemplarisch zum Gegenstand künftiger Datenschutzschulungen gemacht werden.

Da insbesondere Namensidentitäten jedoch nicht derart unwahrscheinlich sind, dass sie für die Zukunft völlig ausgeschlossen werden können, habe ich neben der Sensibilisierung der Mitarbeiter noch zusätzliche Schritte gefordert. Vor allem halte ich es in einem solchen Fall für notwendig, die Abläufe für die Herausgabe

von Arztbriefen und die Prüfung der Adressen einer eingehenden Prüfung zu unterziehen, um ggf. datenschutzgerechtere Verfahrensweisen vorzusehen. Erfolgt etwa die Arztbriefschreibung elektronisch und sind die Arztbriefe in das Krankenhausinformationssystem eingebunden, sollte der Aufruf und Ausdruck auch immer nur über das Krankenhausinformationssystem erfolgen, das automatisch die richtigen Adressdaten zur Verfügung stellt.

Außerdem sollten die in der Orientierungshilfe Krankenhausinformationssysteme (abrufbar unter https://www.datenschutz-bayern.de, „Themen" – „Gesundheitswesen" – „Orientierungshilfe Krankenhausinformationssysteme (2. Fassung))" im Teil 1 unter den Punkten 21 - 25 geforderten Maßnahmen umgesetzt sein, so dass spätestens ein Jahr nach Abschluss der Behandlung die Daten entlassener Patienten nicht mehr regulär im Zugriff stehen. Damit hätten die Daten der verstorbenen Patientin nicht mehr zur Auswahl gestanden und die Verwechslung hätte nicht stattfinden können.

7.2.4 Hygieneverordnung und Krankentransport

Eine Änderung des § 23 Infektionsschutzgesetz (IfSG) hat die Landesregierungen verpflichtet, für bestimmte Gesundheitseinrichtungen die Maßnahmen zum Infektionsschutz zu regeln. Bayern hat dazu eine Verordnung zur Hygiene und Infektionsprävention in medizinischen Einrichtungen erlassen (MedHygV). Insbesondere die Vorschrift des § 13 MedHygV hat dabei zu datenschutzrechtlichen Zweifelsfragen geführt, um deren Beantwortung ich wiederholt gebeten wurde. Meist ging es hierbei um die Informationsbedürfnisse und -befugnisse des Rettungsdienstes. Zum Rettungsdienst sind gemäß Art. 1 Bayerisches Rettungsdienstgesetz (BayRDG) u.a. die Notfallrettung, der arztbegleitete Patiententransport und der Krankentransport im Sinne des Art. 2 Abs. 5 BayRDG zu zählen, nicht jedoch Krankenfahrten (siehe Art. 3 Nr. 6 BayRDG).

Nach Art. 13 MedHygV, der sich am Wortlaut des § 23 Abs. 8 Nr. 10 IfSG orientiert, haben die in § 1 Abs. 2 Nrn. 1 bis 5 der Verordnung genannten medizinischen Einrichtungen bei Verlegung, Überweisung oder Entlassung von Patienten Informationen über Maßnahmen, die zur Verhütung und Bekämpfung von nosokomialen Infektionen und von Krankheitserregern mit speziellen Resistenzen und Multiresistenzen erforderlich sind, an den Rettungsdienst, die aufnehmende Einrichtung oder die niedergelassene Ärztin oder den niedergelassenen Arzt weiterzugeben.

Für Bayern entwickelte die Arbeitsgemeinschaft Multiresistente Erreger (LARE) für diesen sektorenübergreifenden Informationsaustausch spezielle Informationsweitergabebögen. Die zugehörigen vier Ausdrucke sind entweder für den ausstellenden Arzt, den weiterbehandelnden Arzt, den Krankentransport oder die aufnehmende Einrichtung bestimmt. Die Formulargestaltung ist jeweils an die unterschiedlichen Informationsbedürfnisse angepasst und wurde mit mir abgestimmt. Für den Krankentransport wurde allerdings in der Folge angezweifelt, dass die dem Ausdruck nach mitzuteilenden Informationen ausreichend sind. Insbesondere wurde diskutiert, welche Informationen zur konkret bestehenden Infektion oder Besiedelung des Patienten an den Krankentransport weitergegeben werden dürfen bzw. müssen.

Zur Reichweite der Informationsweitergabebefugnis des ausstellenden Arztes bzw. der abgebenden Einrichtung gegenüber dem Krankentransport habe ich wiederholt darauf hingewiesen, dass sowohl dem Wortlaut des § 13 MedHygV als

auch der Begründung zum Verordnungsentwurf zu entnehmen ist, dass beim Informationsaustausch zwischen den Einrichtungen die Information über die notwendigen Schutzmaßnahmen im Vordergrund steht. Die Zulässigkeit näherer Informationen über die konkrete Infektion oder Kolonisation hängt davon ab, ob deren Kenntnis für die Festlegung der Verhütungs- oder Bekämpfungsmaßnahmen erforderlich ist.

§ 13 MedHygV Sektorübergreifender Informationsaustausch
Die Einrichtungen nach § 1 Abs. 2 Nrn. 1 bis 5 haben bei Verlegung, Überweisung oder Entlassung von Patientinnen und Patienten Informationen über Maßnahmen, die zur Verhütung und Bekämpfung von nosokomialen Infektionen und von Krankheitserregern mit speziellen Resistenzen und mit Multiresistenzen erforderlich sind, an den Rettungsdienst, die aufnehmende Einrichtung oder die niedergelassene Ärztin oder den niedergelassenen Arzt weiterzugeben.

Die Frage, inwieweit das Vorliegen von Infektionskrankheiten oder die Besiedelung mit multiresistenten Erregern bzw. ein entsprechender Verdacht an den Rettungsdienst mitgeteilt werden darf, ist in Bayern bereits durch Art. 40 Abs. 2 des BayRDG geregelt. Art. 13 MedHygV kommt in Bezug auf den Rettungsdienst daher nur deklaratorische Bedeutung zu. Nach der genannten rettungsdienstgesetzlichen Spezialnorm ist der Besteller rettungsdienstlicher Leistungen verpflichtet, der Integrierten Leitstelle oder dem Unternehmer bei der Bestellung das Vorliegen oder den Verdacht einer Infektionskrankheit oder einer Besiedelung mit multiresistenten Erregern mitzuteilen. Wie bei Art. 13 MedHygV geht es auch bei dieser Rechtsvorschrift in erster Linie darum, den Rettungsdienst in die Lage zu versetzen, die im Einzelfall erforderlichen Hygienemaßnahmen zu treffen. Die Pflicht nach Art. 40 Abs. 2 BayRDG bezieht sich daher nur auf die insoweit erforderlichen Informationen. Die Reichweite oder der Umfang der Information ist nach dem Sinn und Zweck der Norm danach zu bestimmen, ob es zu Gefährdungen des Transportpersonals, des Patienten und/oder nachfolgend transportierter Patienten kommen kann und sich hieraus die Notwendigkeit der Einhaltung bestimmter Schutzvorkehrungen ergibt (vgl. auch die Begründung zu Art. 40 des Gesetzentwurfs, Landtags-Drucksache 15/10391). Es genügt daher in der Regel die Mitteilung, dass beim zu transportierenden Patienten eine Infektionskrankheit oder eine Besiedelung mit multiresistenten Erregern vorliegt bzw. ein diesbezüglicher Verdacht besteht und welche Hygienemaßnahmen erforderlich sind.

Die mit mir zuletzt abgestimmte Fassung des Informationsweitergabebogens, die in Bezug auf den Ausdruck für den Krankentransport Änderungen erfahren hat, berücksichtigt diese datenschutzrechtlichen Anforderungen. Ist ein Patient mit multiresistenten Erregern zu transportieren, sind dem Ausdruck für den Krankentransport allgemeine Informationen über das in einem solchen Fall erforderliche Hygienemanagement zu entnehmen. Lediglich dann, wenn beim Patienten eine Besiedelung von Nase oder Rachen vorliegt, wird eine entsprechende patientenbezogene Information an den Krankentransport aus fachlicher Sicht für erforderlich gehalten. In diesem Fall sei es zum Schutz des Personals und nachfolgend zu transportierender Patienten dringend notwendig, dem Patienten einen Mund-Nasenschutz anzulegen. Diese Begründung halte ich für nachvollziehbar.

7.2.5 Videoüberwachung im Patientenzimmer der Psychiatrie

Ein Universitätsklinikum bat mich um meine datenschutzrechtliche Einschätzung zur Frage der Rechtmäßigkeit der Videoüberwachung in speziellen Patientenzimmern der Psychiatrie (und zugehörigen Toilettenräumen). Den Angaben zu Folge liege der Videoüberwachung im Einzelfall eine Einwilligungserklärung des betreffenden Patienten zugrunde.

Soweit Videoüberwachung auf der Grundlage von Einwilligungserklärungen der Patienten durchgeführt wird, stellt sich für die Notwendigkeit der Videoüberwachung die naheliegende Frage, ob die betroffenen Patienten in ihrer besonderen Situation überhaupt in der Lage sind, wirksam einzuwilligen. Hierzu bedürfte es der Einwilligungsfähigkeit der Patienten. Die Erklärung müsste zudem freiwillig abgegeben worden sein (siehe § 4a Abs. 1 Satz 1 Bundesdatenschutzgesetz). Bei einem Patienten, der aufgrund seines akuten Krankheitszustandes in die geschlossene Abteilung eines psychiatrischen Krankenhauses aufgenommen wurde, kann schon nicht ohne weiteres angenommen werden, dass er einwilligungsfähig ist. Sollte der konkret betroffene Patient im Einzelfall als einwilligungsfähig eingestuft werden können, wird er im Fall einer zwangsweisen Unterbringung jedenfalls nicht freiwillig in eine Videoüberwachung einwilligen. Selbst dann, wenn der Patient sich aufgrund einer freien Entscheidung zur Behandlung in die geschlossene Abteilung begeben hat, entsteht in gewisser Weise ein Abhängigkeitsverhältnis zwischen ihm und der behandelnden Einrichtung, aufgrund dessen die Freiwilligkeit der Patientenerklärung grundsätzlich fraglich ist. Die Einwilligung des Patienten ist daher regelmäßig kein taugliches Instrument, um für den besonders sensiblen Bereich der Überwachung suizidgefährdeter Psychiatriepatienten eine datenschutzrechtliche Grundlage zu schaffen.

Insofern bedarf die Videoüberwachung einer gesetzlichen Grundlage. Dabei ist zu klären, welche Rechtsgrundlage für die Videobeobachtung der Patientenzimmer nebst Toilettenräumen in Betracht kommt. Universitätskliniken sind rechtsfähige Anstalten des öffentlichen Rechts des Freistaats Bayern (Art. 1 des Bayerischen Universitätsklinikagesetzes – BayUniKlinG) und damit öffentliche Stellen (siehe Art. 2 Abs. 1 BayDSG). Es gilt somit grundsätzlich das Bayerische Datenschutzgesetz, soweit nicht gemäß Art. 2 Abs. 7 BayDSG bereichsspezifische Datenschutzvorschriften vorgehen oder das Bayerische Datenschutzgesetz selbst die Anwendbarkeit des Bundesdatenschutzgesetzes bestimmt. **Auch für Universitätskliniken vertrete ich mittlerweile die Auffassung, dass für sie die Sonderregelung für Wettbewerbsunternehmen des Art. 3 Abs. 1 BayDSG gilt, wonach öffentliche Stellen, soweit sie als Unternehmen am Wettbewerb teilnehmen, dem Bundesdatenschutzgesetz mit Ausnahme dessen zweiten Abschnitts unterfallen.** Da Universitätskliniken Aufgaben der Krankenversorgung wahrzunehmen haben, die auch von privaten oder gemeinnützigen Krankenhäusern erbracht werden können, nehmen sie insoweit am Wettbewerb teil, auch wenn die Unikliniken die Krankenversorgung an den Aufgaben ihrer Universität in Forschung und Lehre auszurichten haben und diese hierdurch eine spezielle Prägung erfahren (siehe Art. 2 Abs. 1 Satz 1 BayUniKlinG und Wilde/Ehmann/Niese/Knoblauch, BayDSG, Art. 3, Rn 22 ff.). Bei der vorliegend thematisierten Videobeobachtung handelt es sich um die Erhebung von personenbezogenen Daten mittels optisch-elektronischer Einrichtungen, die der Krankenversorgung und damit der Erbringung der Wettbewerbsleistung dient (siehe hierzu Wilde/Ehmann/Niese/Knoblauch, BayDSG, Art. 3, Rn 4 f.).

In Bayern ist für Universitätskliniken allerdings auch die bereichsspezifische Datenschutzvorschrift des Art. 27 Bayerisches Krankenhausgesetz (BayKrG) entsprechend anwendbar (siehe Art. 2 Abs. 3 BayUniKlinG). Soweit Art. 27 BayKrG den Datenschutz im Krankenhaus regelt (siehe Art. 27 Abs. 1 Satz 2 BayKrG), kommt gemäß Art. 3 Abs. 1 Satz 2, Art. 2 Abs. 7 BayDSG die Verweisung auf das BDSG nicht zum Tragen. Insoweit ist von Bedeutung, dass das BDSG für die hier im Raum stehende Videobeobachtung keine spezielle Vorschrift bereithält. § 6b BDSG gilt nur für die Videoüberwachung öffentlich zugänglicher Räume. Um solche handelt es sich bei den (überwachten) Patientenzimmern nicht.

Gemäß Art. 27 Abs. 2 BayKrG dürfen Patientendaten erhoben werden, soweit dies zur Erfüllung der Aufgaben des Krankenhauses oder im Rahmen des krankenhausärztlichen Behandlungsverhältnisses erforderlich ist oder die betroffene Person eingewilligt hat. Die Beobachtung mittels optisch-elektronischer Einrichtungen stellt eine Form der Erhebung von Patientendaten dar (siehe Art. 27 Abs. 1 BayKrG). Der Schutz krankheitsbedingt suizidaler Patienten vor Selbstgefährdung ist Aufgabe des Krankenhauses. Sie resultiert aus Fürsorgepflichten gegenüber aufgenommenen Patienten und gehört zur Krankenversorgung. Soweit bestimmte Patienten wegen der akuten Gefahr, sich selbst zu verletzen, in besonderer Weise überwachungsbedürftig sind, ist bei der Wahl und Ausgestaltung der im konkreten Fall vorzusehenden Überwachungsmaßnahme allerdings dem Grundsatz der Verhältnismäßigkeit Rechnung zu tragen.

Die Maßnahme muss geeignet und erforderlich sowie im engeren Sinne verhältnismäßig sein. Bei der Prüfung der Geeignetheit ist zu fragen, ob sich die Videoüberwachung des konkret überwachungsbedürftigen Patienten im Hinblick auf seinen Krankheitszustand und seine Gefährdungssituation überhaupt eignet. Erforderlich ist die Videoüberwachung nur dann, wenn sie das mildeste Mittel zur Erreichung des angestrebten Zwecks darstellt, indem sie unter den zur Verfügung stehenden Maßnahmen (z.B. Sitzwache, bauliche oder sonstige organisatorische Maßnahmen) diejenige ist, die die schützenswerten Rechte des Betroffenen am wenigsten beeinträchtigt und daher angemessen ist. Der Schwerpunkt der Verhältnismäßigkeitsprüfung liegt folglich bei der Abwägung der Interessen des Einrichtungsträgers an der Videoüberwachung und den (verfassungs-) rechtlich geschützten Positionen des Betroffenen unter Würdigung aller Umstände des Einzelfalls.

Videoüberwachung ist generell mit einem erheblichen Kontroll- und Einschüchterungspotenzial verbunden und kann verhaltenslenkende Wirkungen entfalten. Der empfundene Überwachungsdruck, den die Kameras selbst dann auslösen, wenn sie nicht eingeschaltet sind, ist – je nach Krankheitsbild – bei Menschen, die stationärer psychiatrischer Behandlung bedürfen, u.U. sogar noch deutlich gesteigert. Erst recht gilt dies, wenn der betreffende Patient den Raum nicht verlassen und er sich der Videobeobachtung nicht einmal vorübergehend entziehen kann.

Die Videobeobachtung von Patientenzimmern ist daher immer als schwerwiegender Eingriff in das informationelle Selbstbestimmungsrecht (Art. 2 Abs. 1 in Verbindung mit Art 1 Abs. 1 Grundgesetz – GG) des betroffenen Patienten zu werten. Die Patientenzimmer stellen für die Patienten für die Dauer ihres Aufenthalts auf der geschlossenen Station auch Rückzugs- und Ruheraum dar. Die Beobachtung mittels Videokamera erfasst den höchstpersönlichen Lebensbereich des Patienten (siehe § 201a Strafgesetzbuch).

Erst recht gilt dies, soweit sogar die Toilettenräume videotechnisch überwacht werden sollen, in denen in intimster Weise der Körperhygiene nachgegangen wird. In diesem Zusammenhang kann sich im Einzelfall u.U. sogar die Frage stellen, ob eine solche Vorgehensweise noch als menschenwürdige Behandlung angesehen werden kann (siehe Art. 1 Abs. 1 GG). Die Menschenwürdegarantie verbietet eine Herabwürdigung zum Objekt und gebietet die Wahrung menschlicher Identität und Integrität (vgl. BVerfGE 96, 375, 399 f., m.w.N.).

Im Ergebnis halte ich die Videoüberwachung von Patientenzimmern psychiatrischer Patienten nur in Ausnahmefällen für zulässig, wenn sich in der konkreten Situation und bezogen auf den konkreten Patienten kein weniger einschneidendes Mittel anbietet, um Leib und Leben des Betreffenden zu schützen. Ihr Einsatz muss auf einer ärztlichen Gefahreneinschätzung beruhen und sich auf ganz bestimmte, als solche kenntlich gemachte Wachräume sowie auf das zeitlich Erforderliche beschränken. Die betroffenen Patienten sowie ihre gesetzlichen Vertreter sind über die Videoüberwachung und ihre Zwecke zu informieren. Anlass, Anordnung, Umfang und Dauer der Maßnahmen sind zu dokumentieren.

Noch strengere Anforderungen sind an die Überwachung der Toilettenräume mittels Videokamera zu stellen. In der Regel wird sie nicht verhältnismäßig sein. Insoweit ist zu berücksichtigen, dass die Videoüberwachung von Patientenzimmern nur dann zur Erhöhung der Sicherheit beiträgt, wenn Personal zur Verfügung steht, das die übertragenen Aufnahmen zeitgleich am Bildschirm überwacht. Das Aufsuchen der Toilette, die Verweildauer sowie sonstige Auffälligkeiten könnten daher nachvollzogen werden, ohne den Raum von innen zu überwachen. Daneben sind zunächst weniger belastende Möglichkeiten (bauliche und gestalterische Maßnahmen sowie Maßnahmen des Personaleinsatzes) zur Verbesserung der Sicherheit zu ergreifen.

7.2.6 Videoüberwachung auf dem Klinikparkplatz

Ein Klinikum wollte von mir wissen, ob es datenschutzrechtlich für die Videoüberwachung von Anlagen, Einfahrtsschranken und Parkautomaten auf dem Klinikparkplatz verantwortlich ist, obwohl die Betreuung der gesamten Parkflächen einschließlich Tiefgarage vertraglich an eine externe Firma vergeben wurde.

Grundsätzlich sind Videoüberwachung und -aufzeichnung im Krankenhaus und auf dem zugehörigen Gelände nach § 6b Bundesdatenschutzgesetz (BDSG) zu beurteilen, wenn es sich – wie bei der anfragenden Einrichtung – um ein Wettbewerbsunternehmen im Sinne des Art. 3 Abs. 1 BayDSG handelt. Soweit im Rahmen der Videoüberwachung auch Patientendaten erhoben oder gespeichert werden, ist Art. 27 Abs. 2 des Bayerischen Krankenhausgesetzes (BayKrG) zu beachten. Die Verantwortung für die Einhaltung der genannten datenschutzrechtlichen Vorschriften trägt das Krankenhaus. Das gilt grundsätzlich auch dann, wenn es den Bereich der Parkplatzüberwachung mittels optisch-elektronischer Einrichtungen im Wege der Auftragsdatenverarbeitung einem externen privaten Unternehmen übertragen hat. Im Rahmen der Auftragsdatenverarbeitung hat der Auftraggeber die datenschutzrechtliche Freigabe, die Erstellung und Führung einer entsprechenden Verfahrensbeschreibung sowie die Aufnahme des Verfahrens in sein öffentliches Verfahrensverzeichnis durchzuführen, soweit personenbezogene Daten in einem automatisierten Verfahren verarbeitet werden.

Mit den Voraussetzungen einer zulässigen Auftragsdatenverarbeitung im Sinne des § 11 BDSG (siehe auch Art. 27 Abs. 4 Satz 5 BayKrG) ist es nicht vereinbar, dass die externe Firma den Betrieb der Parkflächen einschließlich der Parkraumüberwachung und der Entscheidung über den Einsatz von optisch-elektronischen Einrichtungen in eigener Verantwortung wahrnimmt. Geschieht dies, spricht viel für das Vorliegen einer Funktionsübertragung, zu der die öffentliche Stelle Krankenhaus berechtigt sein müsste. Im Fall einer rechtmäßigen Funktionsübertragung wäre die private Betreiberfirma selbst verantwortliche Stelle nach § 3 Abs. 7 BDSG und für die Einhaltung der Voraussetzungen des § 6b BDSG zuständig.

7.2.7 Videoüberwachung eines OP-Zugangs

Ein Krankenhaus wandte sich an mich, um die datenschutzrechtliche Zulässigkeit der Videoüberwachung eines irregulären OP-Zugangs zu klären. Der spezielle Zugang bestehe neben den üblichen OP-Schleusen aus brandtechnischen Gründen. Er ermögliche es einzelnen Ärzten der nahegelegenen Anästhesieabteilung den OP-Bereich in Notfällen besonders schnell zu erreichen. Dies erfolge dann allerdings unter Umgehung der üblichen Hygienemaßnahmen in den OP-Schleusen. Hiergegen habe das zuständige Gesundheitsamt aufgrund der hygienischen Risiken Bedenken geäußert. Es habe überdies befürchtet, dass die Tür nicht nur im Notfall benutzt werde. Mit Hilfe der Videoüberwachung wolle man daher sicherstellen, dass der irreguläre Zugang tatsächlich nur in Notsituationen genutzt wird und dies auch kontrolliert werden kann. Die hierfür bereits eingeführten Maßnahmen, nämlich die Versiegelung der Tür, die tägliche Kontrolle des Siegels und die Anweisung an das Klinikpersonal, jede Nutzung schriftlich zu dokumentieren, um im Fall des Siegelbruchs die Berechtigung nachvollziehen zu können, seien nicht ausreichend gewesen. Die Kamera solle durch das Öffnen der Tür aktiviert werden. Die Videoaufzeichnungen würden nur bei Diskrepanzen zwischen gebrochenem Türsiegel und ärztlichen Aufzeichnungen ausgewertet.

Ich habe dem Krankenhaus mitgeteilt, dass zunächst durch die für den Datenschutz verantwortliche Stelle zu klären ist, welche Rechtsgrundlage für die geplante Maßnahme in Betracht kommt. Bei dem Klinikum handelt es sich um eine bayerische öffentliche Stelle, für die grundsätzlich das Bayerische Datenschutzgesetz anwendbar ist (Art. 4 Abs. 2 in Verbindung mit Art. 2 Abs. 1 und 2 BayDSG).

In Art. 3 Abs. 1 BayDSG ist zwar geregelt, dass auf öffentliche Stellen, „soweit“ sie als Unternehmen am Wettbewerb teilnehmen, die Vorschriften des Bundesdatenschutzgesetzes mit Ausnahme des Zweiten Abschnitts Anwendung finden. Der Begriff „soweit“ deutet jedoch daraufhin, dass es erforderlich ist, innerhalb einer öffentlichen Stelle, die als Wettbewerbsunternehmen agiert, zu differenzieren. Nach Art. 3 Abs. 1 BayDSG ist das Bundesdatenschutzgesetz nur bei der Erhebung, Verarbeitung und Nutzung personenbezogener Daten anzuwenden, die der Erbringung der Wettbewerbsleistung dienen und soweit keine besonderen Rechtsvorschriften über den Datenschutz anzuwenden sind (z.B. Art. 27 Bayerisches Krankenhausgesetz).

Wird also von der öffentlichen Stelle Videoüberwachung im Rahmen der Erfüllung (nicht bereichsspezifischer) öffentlicher Aufgaben oder in Ausübung des Hausrechts durchgeführt, bleibt es bei der Anwendbarkeit des Bayerischen Datenschutzgesetzes (siehe hierzu Wilde/Ehmann/Niese/Knoblauch, BayDSG, Art. 3, Rn. 4f.). Die Zulässigkeit der geplanten Videoüberwachungsmaßnahme (Videobeobachtung und Speicherung) beurteilte sich im konkreten Fall daher nach

Art. 21a BayDSG. Für die insoweit anzustellende Prüfung habe ich dem Klinikum empfohlen, das auf meiner Homepage https://www.datenschutz-bayern.de unter „Themen" – „Allgemeines" abrufbare Prüfungsschema Videoüberwachung heranzuziehen. Unter „Themen" – „Kommunales" ist nun auch ein Leitfaden zu finden („Videoüberwachung – Leitfaden für bayerische Kommunen"), der sich mit der Videoüberwachung auf der Grundlage des Art. 21a BayDSG befasst. Gegenüber dem Krankenhaus habe ich insbesondere auf Folgendes hingewiesen:

— Gemäß Art. 21a Abs. 1 BayDSG wäre die Erhebung (Videobeobachtung) und Speicherung (Videoaufzeichnung) personenbezogener Daten u.a. dann zulässig, wenn dies im Rahmen der Erfüllung öffentlicher Aufgaben oder in Ausübung des Hausrechts erforderlich ist, um Leben, Gesundheit, Freiheit oder Eigentum von Personen, die sich im Bereich der öffentlichen Einrichtung aufhalten, zu schützen. Die Videoüberwachung soll vorliegend der Nutzungsbeschränkung auf den Notfall und hiermit verbunden der Sicherstellung der Einhaltung der Hygienevorschriften im Zusammenhang mit dem Zugang zum OP-Bereich sowie dem Schutz der Patienten vor gesundheitlichen Nachteilen dienen.

  Unter den Gesichtspunkten der Geeignetheit und Erforderlichkeit wäre zunächst zu untersuchen, ob der betreffende Zugang – außer im Brandfall – überhaupt ermöglicht werden muss. Normalerweise sollte auch beim Zutritt medizinischen Personals über die regulär zu nutzenden OP-Schleusen notfallgerechtes Verhalten möglich sein. Immerhin diente der Zugang, der videoüberwacht werden soll, ausschließlich brandtechnischen Zwecken. Er wurde nicht errichtet, um die OP-Schleusen für Mitarbeiter (im Notfall) zu umgehen. Käme man zu dem Ergebnis, dass ein Notfallzugang zum OP-Trakt nicht ermöglicht werden muss, wäre der Zugang zwar vor missbräuchlicher Benutzung u.U. ebenfalls zu sichern (Siegel, Plombe, Alarm; ggf. auch unterstützend Videoüberwachung, soweit notwendig). Die Anforderungen, die an eine erforderliche und im engeren Sinne verhältnismäßige Überwachung zu stellen wären, wären dann aber in Anbetracht der Zielrichtung und der Gewichtung der schutzwürdigen Interessen des betroffenen Personenkreises voraussichtlich andere.

— Die schutzwürdigen Interessen der von einer Videoüberwachung betroffenen Personen sind bei der Prüfung der Angemessenheit der Maßnahme mit zu berücksichtigen (siehe Wilde/Ehmann/Niese/ Knoblauch, BayDSG, Art. 21a, Rn. 26). So kann eine Videoüberwachung am Arbeitsplatz aufgrund des damit verbundenen erheblichen Eingriffs in das Persönlichkeitsrecht der Beschäftigten nur durch besondere Sicherheitsinteressen des Dienstherrn ausnahmsweise gerechtfertigt sein.

  Sollten die Voraussetzungen für die geplante Videoüberwachung vorliegen, wäre zu bedenken, dass die Heranziehung der Videoaufnahmen zu Zwecken der personenbezogenen Dienstaufsicht nach der – eng auszulegenden – datenschutzrechtlichen Zweckidentitätsvorschrift des Art. 17 Abs. 3 Satz 1 Fall 1 BayDSG gesetzlich nicht von vornherein ausgeschlossen ist. Zur Sicherstellung der Persönlichkeitsrechte der Beschäftigten hat der Personalrat jedoch nach Art. 75a Abs. 1 Nr. 1 Bayerisches Personalvertretungsgesetz (BayPVG) ein Mitbestimmungsrecht bei der Einführung und Anwendung von technischen Einrichtungen, die – so die Auslegung der Rechtsprechung – an sich dazu geeignet sind, das Verhalten oder die

Leistung der Beschäftigten zu überwachen. Aus meiner Sicht empfehlenswert wäre in diesem Fall der Abschluss einer Dienstvereinbarung (siehe Art. 73, 70 BayPVG), die den Umfang und das Verfahren der Heranziehung der Videoaufzeichnungen zur Dienstaufsicht im Einzelnen festgelegt. Aus datenschutzrechtlicher Sicht sollte dabei der Zugriff auf die Aufzeichnungen nur in schwerwiegenden Fällen gestattet sein. Weiterhin ist unter dem Gesichtspunkt des Verfahrensrechts zu empfehlen, den Zugriff nur unter Beteiligung eines Mitglieds des Personalrats und des behördlichen Datenschutzbeauftragten zu gestatten. Aus Transparenzgründen wäre die Dienstvereinbarung den Beschäftigten zur Kenntnis zu geben.

7.2.8 Neufassung der „Orientierungshilfe Krankenhausinformationssysteme“ (OH KIS)

In meinem 25. Tätigkeitsbericht 2012 unter Nr. 7.2 habe ich über die im Jahr 2011 veröffentlichte „Orientierungshilfe Krankenhausinformationssysteme“ berichtet. Nun liegt eine 2. Fassung der Orientierungshilfe vor. Sie soll den Herstellern und Betreibern von Krankenhausinformationssystemen eine praxisgerechte und noch besser handhabbare Handreichung für die datenschutzgerechte Gestaltung und Nutzung von Krankenhausinformationssystemen bieten.

Im Rahmen der Neufassung der Orientierungshilfe tauschte sich eine Arbeitsgruppe der Datenschutzkonferenz intensiv mit der Deutschen Krankenhausgesellschaft (DKG) und einigen Landeskrankenhausgesellschaften aus. Die in diesem Rahmen gewonnenen Erkenntnisse sind in die überarbeitete Fassung der Orientierungshilfe eingeflossen.

Um Verständnisschwierigkeiten zu begegnen, die im Rahmen der vorausgegangenen Prüftätigkeiten einiger Datenschutzbeauftragten aufgefallen waren, ist ihr Teil I (Rechtliche Rahmenbedingungen) präzisiert worden. In Teil II (Technische Anforderungen) wird nun der durchgehende Bezug zu den rechtlichen Rahmenbedingungen verdeutlicht. Insgesamt wird jetzt auch klarer, dass den rechtlichen Anforderungen durch verschiedenartige System- und Prozessgestaltung entsprochen werden kann.

Die 2. Fassung der „Orientierungshilfe Krankenhausinformationssysteme“ ist auf meiner Homepage https://www.datenschutz-bayern.de unter „Veröffentlichungen“ – „Broschüren und Orientierungshilfen“ auffindbar.

7.3 Klinische Krebsregister

In meinem 19. Tätigkeitsbericht 2000 unter Nr. 3.3, meinem 24. Tätigkeitsbericht 2010 unter Nr. 7.1 und meinem 25. Tätigkeitsbericht 2012 unter Nr. 7.1 habe ich mich bereits eingehend mit der bayerischen Krebsregistrierung befasst. Zwischenzeitlich hat der Bundesgesetzgeber mit Einfügung des § 65c Sozialgesetzbuch Fünftes Buch – Gesetzliche Krankenversicherung (SGB V) beschlossen, dass alle Länder zur Verbesserung der Qualität der onkologischen Versorgung klinische Krebsregister einrichten. Die für die Einrichtung und den Betrieb der klinischen Krebsregister notwendigen Bestimmungen einschließlich datenschutzrechtlicher Regelungen bleiben dem Landesrecht vorbehalten (§ 65c Abs. 1 Satz 6 SGB V). Nun wird bundesweit in den Ländern und bei den Datenschutzbehörden darüber diskutiert, wie die klinischen Krebsregister ausgestaltet werden

sollen. Auf die derzeitigen Unstimmigkeiten zwischen den Anforderungen des Bayerischen Krebsregistergesetzes (BayKRG) und der Praxis in den klinischen Krebsregistern in Bayern habe ich insbesondere in meinem 24. Tätigkeitsbericht 2010 unter Nr. 7.1 bereits hingewiesen. Bis zu einer eventuellen gesetzlichen Neuregelung in Bayern habe ich zusammen mit den von mir geprüften klinischen Krebsregistern an der Erarbeitung einer schriftlichen Einwilligungserklärung und eines Informationsblatts für Patienten mitgewirkt, um den klinischen Krebsregistern im Rahmen des derzeit geltenden Bayerischen Krebsregistergesetzes zu ermöglichen, auch die Identitätsdaten mit Einwilligung der Betroffenen zu verarbeiten und zu nutzen (Art. 6 Abs. 1 Sätze 4 und 5 BayKRG). Inwieweit der bayerische Gesetzgeber die klinische und die epidemiologische Krebsregistrierung neu strukturieren wird, ist derzeit noch nicht absehbar. Die derzeitige Rechtslage in Bayern sieht jedenfalls nicht vor, dass alle in § 65c SGB V für die klinischen Krebsregister vorgesehenen Aufgaben ausgefüllt werden können. Dazu bedürfte es einer gesetzlichen Anpassung des BayKRG. Ich wäre selbstverständlich bereit, auch weiterhin meine datenschutzrechtliche Expertise einzubringen.

7.4 App „Gesundheitsservice Bayern“

Das Staatsministerium für Gesundheit und Pflege bat mich, an der datenschutzgerechten Gestaltung einer geplanten mobilen Applikation mit der Bezeichnung „Gesundheitsservice Bayern“ beratend mitzuwirken. Mir wurde mitgeteilt, dass die Applikation (App) für mobile Endgeräte den Zugriff auf Bayerns medizinisches Angebot von Krankenhäusern, Ärzten, Psychotherapeuten, Bereitschaftsdiensten, Apotheken, Notdiensten, Kur- und Heilbädern ermöglichen sowie zusätzlich allgemeine medizinische Beratungsleistungen bzw. Gesundheitsinformationen bieten soll. Nachdem das Staatsministerium selbst nicht über alle notwendigen Informationen zu den in Bayern erreichbaren medizinischen Dienstleistungen verfügt, werde eine Kooperation mit den bayerischen Kammern und Verbänden im Gesundheitswesen angestrebt. Daten der Ärzte, Zahnärzte, Psychotherapeuten, Apotheken, Krankenhäuser, Not- und Bereitschaftsdienste, die in eigenen Internetauftritten der kooperierenden Kammern und Verbände bereits veröffentlicht seien, sollten so in die App eingebettet werden, dass der Nutzer der App die Daten dem jeweiligen Verband bzw. der jeweiligen Kammer zuordnen könne. Man bewerte die beabsichtigte Kooperation hinsichtlich im Internet erreichbarer personenbezogener Daten als Auftragsdatenverarbeitung, bei der die Kammern und Verbände als Auftraggeber und das Staatsministerium als Auftragnehmer agieren.

Im Rahmen einer Besprechung sowie des sich daran anschließenden Schriftwechsels habe ich das Staatsministerium auf die folgenden datenschutzrechtlichen Problemstellungen aufmerksam gemacht.

— Sowohl nach den Vorschriften zum Sozialdatenschutz als auch nach dem in Bayern gültigen allgemeinen Datenschutzrecht ist als Auftragsdatenverarbeitung die Weitergabe personenbezogener Daten an einen Auftragnehmer zur Durchführung untergeordneter Hilfs- und Unterstützungsleistungen für den Auftraggeber zu verstehen. Ein Auftragsdatenverarbeitungsverhältnis ist dadurch gekennzeichnet, dass in Bezug auf die in Auftrag gegebene Datenverarbeitung der Auftraggeber „Herr der Daten“ und verantwortlich bleibt. Der Auftragnehmer darf die erhaltenen Daten nicht zu eigenen Zwecken nutzen und muss sich strikt an die schriftlichen Weisungen des Auftraggebers halten. Insoweit äußerte ich zunächst Zweifel, dass diese

Voraussetzungen vorliegen, da nach der mir vorgelegten Kooperationsvereinbarung von einer Zusammenarbeit und der Veröffentlichung einer gemeinsamen App die Rede war. Das Staatsministerium tritt als Mitherausgeber der App in Bezug auf bestimmte Inhalte (Patienten- bzw. Gesundheitsberatung) deutlich in Erscheinung. Später stellte sich heraus, dass das Staatsministerium im Rahmen der Kooperation eine Art Doppelrolle ausfüllt: Einerseits handelt es als Auftragnehmer in Bezug auf die Veröffentlichung von medizinischen Angeboten der weiteren Vertragspartner. Unabhängig hiervon platziert es andererseits mit der App auch eigene Inhalte (allgemeine Patientenberatung). Danach bestehen meine Bedenken hinsichtlich des Vorliegens der allgemeinen Voraussetzungen eines Auftragsdatenverarbeitungsverhältnisses nicht fort.

– Ausgehend hiervon habe ich darauf hingewiesen, dass der Auftraggeber gemäß § 80 Abs. 1 Sozialgesetzbuch Zehntes Buch – Sozialverwaltungsverfahren und Sozialdatenschutz (SGB X) bzw. Art. 6 Abs. 1 BayDSG für die Einhaltung der Vorschriften des Bayerischen Datenschutzgesetzes und anderer Vorschriften über den Datenschutz verantwortlich bleibt. Dies betrifft insbesondere die Vorschriften über die Zulässigkeit der Erhebung, Verarbeitung und Nutzung personenbezogener Daten. Es bedarf hinsichtlich der zusätzlichen bzw. weiteren Nutzung der personenbezogenen Daten im Rahmen der App einer Erweiterung der Einwilligungserklärung und vorausgehend einer entsprechenden Information.

– Mobile Applikationen sind als Telemediendienst zu qualifizieren. Entwickler und Anbieter haben daher die datenschutzrechtlichen Regelungen der §§ 11 ff. Telemediengesetz (TMG) sicherzustellen.

– Aus technisch-organisatorischer Sicht war zu diesem frühen Stadium u.a. zu prüfen, ob das vorgesehene Cache-Konzept dazu führt, dass ein zentraler Datenbestand geschaffen wird. Die App wäre dann als Verbundverfahren zu betrachten, für das eine rechtliche Grundlage erforderlich wäre. Nachdem die Speicherdauer im Cache nach dem mir übersandten Schnittstellen- und Cachekonzept auf maximal 1 Stunde reduziert wurde, ging ich davon aus, dass es sich bei der kurzfristigen Speicherung um eine rein technische Maßnahme zur Verbesserung der Performance handelt. Ich verwies zudem auf den vom Bayerischen Landesamt für Datenschutzaufsicht erstellten App-Prüfkatalog und bat, diesen bei der App-Entwicklung zugrunde zu legen (siehe Nr. 2.1.2).

Ich gehe davon aus, dass ich hinsichtlich der konkreten Umsetzung auf dem Laufenden gehalten werde, um auch weiterhin beratend tätig zu werden.

7.5 Datenschutz in medizinischen Forschungsprojekten

Soweit im Rahmen von medizinischen Forschungsprojekten personenbezogene Daten von Patienten bzw. Probanden erhoben, verarbeitet oder genutzt werden, hat dies in Einklang mit den datenschutzrechtlichen Vorschriften zu erfolgen. Die medizinische Forschung arbeitet zunehmend vernetzt in größeren Forschungsverbünden. Die Vernetzung schafft überregionale, meist auf die Erforschung bestimmter Krankheiten ausgerichtete Kooperationen von Grundlagenforschern

und Ärzten. Ein wichtiges Element dieser Kooperation ist die überregionale Zusammenführung und Bereitstellung aller forschungsrelevanten Daten in zentralen Datenbanken bzw. Registern und von Proben in zentralen Biobanken.

Im 21. Tätigkeitsbericht 2004 unter Nr. 22.2.3.4 habe ich bereits darüber berichtet, dass die TMF, die Technologie- und Methodenplattform für die vernetzte medizinische Forschung e.V., unter Einbeziehung der Datenschutzbeauftragten des Bundes und der Länder im Jahr 2003 ein Datenschutzkonzept „Generische Lösungen zum Datenschutz für die Forschungsnetze in der Medizin" entwickelt hat. Dieses Datenschutzkonzept enthielt modifizierbare Musterlösungen für verschiedene Varianten von medizinischen Forschungsnetzen. Dabei wurde zwischen dem Modell A für Forschungsnetze mit „klinischem Fokus" und dem Modell B für eher „wissenschaftlich orientierte" Netze unterschieden. Zudem wurde im Jahr 2006, ebenfalls unter Einbeziehung der Datenschutzbeauftragten des Bundes und der Länder, „ein generisches Datenschutzkonzept für Biomaterialbanken" von der TMF entwickelt. Mit der Bereitstellung dieser Modelllösungen der TMF sollten Wege aufgezeigt werden, wie datenschutzkonform mit Patientendaten umgegangen und gleichzeitig ein für die Forschung relevanter Datensatz verfügbar gemacht werden kann.

Aufgrund der mit den generischen Datenschutzkonzepten gemachten Erfahrungen wurden diese von der TMF überarbeitet, als „Leitfaden zum Datenschutz in medizinischen Forschungsprojekten – Generische Lösungen der TMF – 2.0" zusammengefasst und im Sommer 2013 den Datenschutzbeauftragten des Bundes und der Länder vorgestellt.

In diesem Leitfaden wird nunmehr zwischen vier Modulen unterschieden, die – je nach Zielrichtung des jeweiligen Forschungsverbundes – einzeln oder kombiniert verwendet werden können:

— dem Klinischen Modul, das der Gewinnung von Forschungsdaten aus dem direkten Behandlungszusammenhang dient und in dem auch einfache oder informelle Forschungsprojekte wie Beobachtungsstudien oder Benchmarking-Projekte durchgeführt werden können,

— dem Studienmodul, in dem klinische Studien durchgeführt werden, die auch den besonderen Regularien des Arzneimittelgesetzes oder Medizinproduktegesetzes unterliegen können,

— dem Forschungsmodul, in dem besonders qualitätsgesicherte Daten für langfristige Forschungsprojekte zusammengeführt und vorgehalten werden, die für die Behandlung des einzelnen Patienten keine direkte Relevanz haben und daher aus dem Behandlungskontext nicht zugänglich sein müssen (z.B. epidemiologische Register), und

— dem Biobankenmodul, das der Sammlung und Verwaltung von Biomaterialien (Proben und daraus gewonnenen Materialien) für Forschungszwecke dient.

Die Datenschutzbeauftragten des Bundes und der Länder haben diesen Leitfaden intensiv diskutiert und in ihrer 87. Konferenz am 27./28.03.2014 beschlossen, den medizinischen Forschungseinrichtungen und Forschungsverbünden zu empfehlen, den von der TMF entwickelten „Leitfaden zum Datenschutz in medizinischen Forschungsprojekten – Generische Lösungen der TMF – 2.0" als Basis für die

konkrete Ausgestaltung ihrer Datenschutzkonzepte zu verwenden. Der Leitfaden selbst ist unter www.tmf-ev.de zu beziehen.

8 Sozialwesen

8.1 Gesetzliche Krankenversicherung

8.1.1 Untergesetzliches Recht als datenschutzrechtliche Befugnis?

Das Recht der gesetzlichen Krankenversicherung ist überaus umfangreich und kompliziert. Rahmengesetz ist das Sozialgesetzbuch Fünftes Buch (SGB V). Darin hat der Gesetzgeber es den verschiedenen Beteiligten in der gesetzlichen Krankenversicherung aber auch ermöglicht, dieses Rahmenrecht durch unterschiedliche Vereinbarungen zu konkretisieren. Im Berichtszeitraum hatte ich dabei vielfach die Frage zu entscheiden, ob diese Verträge, Richtlinien etc. eine datenschutzrechtliche Befugnis sein können. Dies hatte ich noch in meinem 17. Tätigkeitsbericht 1996 unter Nr. 4.4.4 abgelehnt. Inzwischen hat sich jedoch die Rechtsprechung weiterentwickelt. Danach liegen hier Normsetzungsverträge vor, die Rechte und Pflichten der Beteiligten, aber auch der gesetzlich Krankenversicherten begründen. Damit liegt ein „Gesetz" vor, das als datenschutzrechtliche Befugnis herangezogen werden kann. Voraussetzung dafür ist allerdings, dass im SGB V entsprechende Aufgaben angelegt sind.

In einem konkreten Einzelfall hatte ich zu prüfen, ob das Verfahren bei der Begutachtung im Rahmen der vertragszahnärztlichen Versorgung datenschutzrechtlich zulässig ist. Ich habe nach eingehenden Erörterungen hierbei erstmals die Auffassung anerkannt, dass sich die Beteiligten in der Regel auf datenschutzrechtliche Befugnisse im zugrundeliegenden Bundesmantelvertrag-Zahnärzte (BMV-Z) berufen können.

Unabhängig hiervon musste ich auch datenschutzrechtliche Verstöße feststellen. So können Krankenkassen ihre datenschutzrechtlichen Befugnisse nicht durch den Einsatz von Beratungszahnärzten erweitern.

Außerdem musste ich eine Beanstandung aussprechen. So hat die Kassenzahnärztliche Vereinigung Bayerns über mehrere Jahre Gutachten für die Ersatzkassen vermittelt. Jedoch konnte sie sich nicht auf eine datenschutzrechtliche Befugnis im BMV-Z berufen. Des Weiteren war ein derartiges Vorgehen auch nicht erforderlich. Schließlich war bei anderen Krankenkassen ein sehr viel datenschutzfreundlicheres Vorgehen vorgesehen. Diese Vermittlung hatte ich daher bereits im Jahre 2005 kritisiert. Daraufhin hatte mir die Kassenzahnärztliche Vereinigung Bayerns zugesichert, dieses Verfahren einzustellen. Entgegen dieser Zusicherung beendete die Kassenzahnärztliche Vereinigung Bayerns diese datenschutzrechtlichen Verstöße erst kürzlich und nur deshalb, weil eine Ersatzkasse angekündigt hat, an der zentralen Gutachtensvergabe nicht weiter teilnehmen zu wollen. Angesichts dieser Umstände war eine Beanstandung logische Folge und unvermeidlich.

8.1.2 Hilfsmittelversorgung der Krankenkassen

Die datenschutzrechtlichen Befugnisse einer Krankenkasse sind nicht nur beim Krankengeldfallmanagement gegenüber dem Medizinischen Dienst der Krankenversicherung (MDK) abzugrenzen (siehe Nr. 8.1.4). Dies betrifft vielmehr grundsätzlich alle Leistungsbereiche einer Krankenkasse. Im Rahmen verschiedener Eingaben sowie einer Prüfung einer Krankenkasse vor Ort musste ich jedoch feststellen, dass dies bei der Versorgung mit Hilfsmitteln häufig nicht beachtet wurde.

Auch hier gilt der von der Rechtsprechung bestätigte Grundsatz, dass eine Krankenkasse grundsätzlich nicht befugt ist, sensible medizinische Daten zur Kenntnis zu nehmen. Erst recht darf eine Krankenkasse nicht in einem größeren Umfang sensible medizinische Daten erheben, wenn sie den MDK nicht einschaltet. Soll der MDK im Auftrag einer Krankenkasse prüfen, akzeptiere ich nach wie vor die „Kuvertlösung". Es soll auch zukünftig die Möglichkeit bestehen, sensible medizinische Daten datenschutzkonform in einem Kuvert mit der Aufschrift „Nur vom MDK zu öffnen" über die Krankenkasse an diesen zu schicken (siehe 17. Tätigkeitsbericht 1996 Nr. 4.4.2).

Eine Krankenkasse kann zwar eine vorherige Bewilligung eines Hilfsmittels vorsehen. Dadurch kann sie aber nicht den Umfang ihrer datenschutzrechtlichen Befugnisse erweitern. Es ergibt also datenschutzrechtlich keinen Unterschied, ob bei einem Hilfsmittel eine vorherigen Bewilligung oder eine nachträgliche Abrechnung vorgesehen ist.

Der Umfang der Erhebungsbefugnis einer Krankenkasse richtet sich dabei nach der Übermittlungsbefugnis der Leistungserbringer. Bei Ärzten ist grundsätzlich § 36 Bundesmantelvertrag-Ärzte (BMV-Ä) einschlägig, eine untergesetzliche Norm (siehe Nr. 8.1.1).

§ 36 BMV-Ä Schriftliche Informationen
(1) Der Vertragsarzt ist befugt und verpflichtet, die zur Durchführung der Aufgaben der Krankenkassen erforderlichen schriftlichen Informationen (Auskünfte, Bescheinigungen, Zeugnisse, Berichte und Gutachten) auf Verlangen an die Krankenkasse zu übermitteln. Wird kein vereinbarter Vordruck verwendet, gibt die Krankenkasse an, gemäß welcher Bestimmungen des Sozialgesetzbuches oder anderer Rechtsvorschriften die Übermittlung der Information zulässig ist. Eine patientenbezogene mündliche Auskunft des Vertragsarztes ist nur zulässig, wenn der Arzt sich vergewissert hat, dass der Gesprächspartner berechtigt ist, die Information zu erhalten …
(3) Für schriftliche Informationen werden Vordrucke vereinbart …
(5) Für formlose Anfragen, die auf die Erteilung von Auskünften, Bescheinigungen, Gutachten oder Bescheinigungen mit gutachterlicher Fragestellung gerichtet sind, für deren Zweck jedoch kein gesonderter Vordruck vereinbart worden ist, wird ein vereinbartes Rahmenformular verwendet. In diesem Rahmenformular sind Angaben vorzusehen, aus denen dem Arzt der Grund und die Berechtigung für die Beantwortung der Anfrage ersichtlich wird …

Grundsätzlich haben Ärzte daher nur vereinbarte Vordrucke auszustellen. Derzeit liegt ein Rahmenformular noch nicht vor und wird wohl in absehbarer Zeit auch nicht vorliegen. Ärzte sind daher grundsätzlich nicht befugt bzw. verpflichtet, formlose Anfragen von Krankenkassen zu beantworten.

Im Hilfsmittelbereich sind Ärzte daher derzeit grundsätzlich lediglich dazu verpflichtet, ein Rezept (Muster 16 der Vordruckvereinbarung) auszufüllen. In vielen Fällen haben Krankenkassen bei „Nachfragen" zwar dahingehend argumentiert, diese Angaben hätte der Arzt schon in der Verordnung angeben müssen. Dadurch dürfen sie aber keinesfalls die gesetzliche Regelung umgehen (siehe Nr. 8.1.6).

Einschlägige Übermittlungsbefugnis für Hilfsmittelerbringer ist hingegen die abschließende Regelung des § 302 Sozialgesetzbuch Fünftes Buch – Gesetzliche Krankenversicherung (SGB V).

§ 302 SGB V Abrechnung der sonstigen Leistungserbringer
(1) Die Leistungserbringer im Bereich der Heil- und Hilfsmittel und die weiteren Leistungserbringer sind verpflichtet, den Krankenkassen im Wege elektronischer Datenübertragung oder maschinell verwertbar auf Datenträgern die von ihnen erbrachten Leistungen nach Art, Menge und Preis zu bezeichnen und den Tag der Leistungserbringung sowie die Arztnummer des verordnenden Arztes, die Verordnung des Arztes mit der Diagnose und den erforderlichen Angaben über den Befund und die Angaben … (der Krankenversicherungskarte) anzugeben; bei der Abrechnung über die Abgabe von Hilfsmitteln sind dabei die Bezeichnungen des Hilfsmittelverzeichnisses … zu verwenden …

Darüber hinausgehende Befugnisse (z.B. durch weitere Gesetze bzw. Hilfsmittelverträge) bestehen nicht.

In einem konkreten Einzelfall musste ich sogar eine Beanstandung gegen eine Krankenkasse aussprechen. Diese Beanstandung betraf deren Erhebungsbogen zu Hilfsmitteln bei Dekubitus. Problematisch war dabei zum einem die potentielle Fotodokumentation des Falls. Zum anderen habe ich die Fragen zur Prophylaxe, Behandlung, Entstehungsort und Art der Wundversorgung des Dekubitus im Erhebungsbogen kritisiert. Derartige Fragen sind schließlich nicht zur Bewilligung des Hilfsmittels erforderlich. Ausschlaggebend für die Beanstandung war insbesondere, dass mir die Krankenkasse bereits im Jahre 2002 zugesichert hatte, die von mir problematisierten Punkte zu streichen und sich auf Einwilligungserklärungen des Betroffenen zu stützen. Der Erhebungsbogen wurde aber erst kürzlich – nach meiner nochmaligen eindrücklichen Erinnerung – geändert.

Zwar sicherte die Krankenkasse mir inzwischen zu, sich in Bezug auf die erörterten Fragen an die datenschutzrechtlichen Vorgaben zu halten. Ich gehe aber davon aus, dass ich mich im künftigen Berichtszeitraum mit vielen Einzelfragen zu beschäftigen habe. Angesichts meiner Erfahrungen in der Vergangenheit werde ich zudem das vereinbarte Verfahren überprüfen.

8.1.3 Unterstützung durch Krankenkasse bei Behandlungsfehlern

In den datenschutzrechtlichen Fokus geraten auch immer mehr die Fragestellungen rund um Behandlungsfehler. Hier kann sich der Betroffene an viele Stellen wenden, u.a. an seine Krankenkasse. Diese hat auch selbst ein Interesse, ihren Versicherten zur Seite zu stehen. Schließlich besteht ihrerseits eventuell die Möglichkeit, einen Erstattungs- bzw. Ersatzanspruch gegen den Schädiger geltend zu machen.

Zwar besteht auch hier der sozialdatenschutzrechtliche Grundsatz, dass die Krankenkasse grundsätzlich keine sensiblen medizinischen Daten zur Kenntnis nehmen darf (siehe Nrn. 8.1.4 und 8.1.2). Zivilrechtlich hat jedoch der Bundesgerichtshof anders entschieden: Danach geht der Anspruch des Betroffenen auf Einsicht in seine Unterlagen auf den Sozialversicherungsträger über, wenn und soweit dadurch das Bestehen von Schadensersatzansprüchen geklärt werden soll. Voraussetzung dafür ist jedoch eine Einwilligung des Betroffenen in die Einsichtnahme seiner Unterlagen durch den Sozialversicherungsträger. Bei einem derartigen zivilrechtlichen Anspruch kommen sozialdatenschutzrechtliche Regelungen nicht zur Anwendung.

Zukünftig wird die von mir kontrollierte Krankenkasse bei potentiellen Behandlungsfehlern ausschließlich zivilrechtliche Ansprüche geltend machen. Ich habe mich zudem bereit erklärt, eine entsprechende Einwilligungserklärung mitzugestalten. Bei deren Vorliegen kann die Krankenkasse ausnahmsweise Einblick in die Behandlungsunterlagen nehmen. Außerdem kann der Medizinische Dienst der Krankenversicherung (MDK) dann vollständige Gutachten an die Krankenkasse übermitteln (siehe Nr. 8.1.7).

8.1.4 Krankengeldfallmanagement der Krankenkassen bei Arbeitsunfähigkeit

Mit dem Krankengeldfallmanagement bei Arbeitsunfähigkeit versuchen die Krankenkassen, zur Überwindung von Arbeitsunfähigkeit und zur Reintegration kranker Versicherter in das Arbeitsleben beizutragen. Nicht zuletzt sollen auf diese Weise Kosten vermieden werden. Unter Krankengeldfallmanagement ist eine systematische und zielgerichtete Fallsteuerung durch die Krankenkasse zu verstehen. Dazu gehört die persönliche Beratung der Versicherten ebenso wie die Koordination zwischen den medizinischen Dienstleistungsangeboten und den verschiedenen Kostenträgern.

Auch im Berichtszeitraum habe ich mich mit unterschiedlichen datenschutzrechtlichen Problematiken (siehe 25. Tätigkeitsbericht 2012 Nr. 8.11) befasst. Besonders relevant war die Frage, inwiefern die Krankenkasse bei medizinischen Daten eine eigene Erhebungsbefugnis besitzt bzw. diese zur Kenntnis nehmen kann oder aber eine Kenntnisnahme derartiger Daten grundsätzlich ausschließlich dem Medizinischen Dienst der Krankenversicherung (MDK) zugewiesen ist. Nach wie vor meine ich, dass die für den MDK bestimmten Daten zwar auch über die Krankenkassen zugeleitet werden können. Dabei muss aber ausgeschlossen sein, dass die Krankenkasse vom Inhalt der Daten für den MDK Kenntnis nimmt (siehe Nr. 8.1.2 und bereits 17. Tätigkeitsbericht 1996 Nr. 4.4.2).

Auch im Berichtszeitraum erreichten mich Anfragen zu diesem bei den Versicherten oft angstbesetzten Thema. In meine Beratungs- und Kontrolltätigkeit konnte ich Erkenntnisse einfließen lassen, die ich im Rahmen einer überregional durchgeführten Prüfungsreihe gewonnen habe.

Insbesondere zu Beginn der Prüfungsreihe musste ich eine Vielzahl von Datenschutzverstößen feststellen. Gemeinsam mit einer großen bayerischen Krankenkasse konnte ich aber Änderungen in der Gestaltung des Krankengeldfallmanagements erreichen, die in Summe zu einem höheren Datenschutzniveau geführt haben.

— Durch Verwendung so genannter **Selbstauskunftsbögen**, die auch in den Räumlichkeiten der Krankenkasse gemeinsam mit der oder dem Betroffenen ausgefüllt wurden, wurden Versicherte dazu angehalten, gegenüber der Krankenkasse – ohne Hinzuziehung des MDK – u.a. Informationen zum Krankheitszustand zu offenbaren. Nach meiner Intervention sehen die Formulare zwischenzeitlich medizinische Fragen nicht weiter vor.

— Noch im 25. Tätigkeitsbericht 2012 unter Nr. 8.11 hatte ich festgestellt, dass die **Datenschutzhinweise**, die in Formularen, mit denen die Krankenkasse Auskünfte von Leistungserbringern (z.B. Ärzte oder Krankenhäuser) anfordert, vielfach fehlerhaft waren. Diese Situation hat sich erfreulicherweise deutlich gebessert.

— In den bei der Krankenkasse geführten Akten fanden sich oftmals – ohne Schutz vor unbefugten Zugriffen – ausführliche Arztberichte, Krankenhaus- und Rehaentlassungsberichte, vollständige Gutachten des MDK sowie umfangreiche Selbstauskunftsbögen, die die Krankenkasse von Versicherten eingeholt hatte. Ich habe deshalb darauf gedrungen, dass die Krankenkasse sensible medizinische Daten grundsätzlich nur noch mittels eines **verschlossenen Umschlags** erhebt und speichert, der mit dem Zusatz „nur durch den MDK zu öffnen" versehen ist. Kenntnis von diesen medizinischen Daten erlangt dann nicht (mehr) die Krankenkasse, sondern nur noch der MDK. Wie eine Nachprüfung ergeben hat, wird diese „Kuvertlösung" zwischenzeitlich weitgehend umgesetzt.

— Weiterhin musste ich feststellen, dass Auskünfte von Leistungserbringern in einer nicht unerheblichen Zahl von Fällen – zum Teil auf ausdrückliche Anforderung der Krankenkasse – per **Telefax** übermittelt wurden. Dies betraf auch Informationen, die ausschließlich für den MDK bestimmt waren. Bei einem solchen Vorgehen kann allerdings nicht ausgeschlossen werden, dass die Krankenkasse vom Inhalt von Daten für den MDK Kenntnis nimmt. Hier habe ich die Krankenkasse darauf hingewiesen, dass die Verwendung des Telefaxgeräts zumindest auf **absolute Ausnahmefälle** zu beschränken ist. In jedem Fall sind Faxsendungen mit Daten für den MDK – ebenso wie nicht mit einem besonderen Kuvert vor unberechtigter Einsichtnahme geschützte Briefsendungen für den MDK – bei der Krankenkasse mit einem Umschlag zu versehen und zu verschließen, um unberechtigte Kenntnisnahmen durch Mitarbeiter der Krankenkasse zu vermeiden.

8.1.5 Datenschutzrechtliche Befugnisse der Krankenkassen bei Krankenhausbehandlungen

Im Berichtszeitraum habe ich die datenschutzrechtlichen Befugnisse einer Krankenkasse bei Krankenhausbehandlungen geprüft. Auch hier musste ich feststellen, dass häufig vergleichbar zu anderen Leistungsbereichen oft nicht zwischen Daten „für die Krankenkasse" und „für den Medizinischen Dienst der Krankenversicherung (MDK)" unterschieden wird (siehe Nrn. 8.1.4 und 8.1.2).

Nach ständiger Rechtsprechung bestehen im Verhältnis zwischen Krankenhäusern, Krankenkassen und den Medizinischen Diensten Auskunfts- und Prüfpflichten auf drei Ebenen. Auf der ersten Stufe hat das Krankenhaus zunächst zwingend die Angaben nach § 301 Abs. 1 Sozialgesetzbuch Fünftes Buch – Gesetzliche

Krankenversicherung (SGB V) zu machen. Umfassende Entlass- bzw. Befundberichte gehören – entgegen häufiger Praxis – nicht dazu:

§ 301 SGB V Krankenhäuser
(1) Die … Krankenhäuser sind verpflichtet, den Krankenkassen bei Krankenhausbehandlung folgende Angaben im Wege elektronischer Datenübertragung oder maschinell verwertbar auf Datenträgern zu übermitteln:

1. *die Angaben … (der Krankenversichertenkarte) sowie das krankenhausinterne Kennzeichen des Versicherten,*
2. *das Institutionskennzeichen des Krankenhauses und der Krankenkasse,*
3. *den Tag, die Uhrzeit und den Grund der Aufnahme sowie die Einweisungsdiagnose, die Aufnahmediagnose, bei einer Änderung der Aufnahmediagnose die nachfolgenden Diagnosen, die voraussichtliche Dauer der Krankenhausbehandlung sowie, falls diese überschritten wird, auf Verlangen der Krankenkasse die medizinische Begründung, bei Kleinkindern bis zu einem Jahr das Aufnahmegewicht,*
4. *bei ärztlicher Verordnung von Krankenhausbehandlung die Arztnummer des einweisenden Arztes, bei Verlegung das Institutionskennzeichen des veranlassenden Krankenhauses, bei Notfallaufnahme die die Aufnahme veranlassende Stelle,*
5. *die Bezeichnung der aufnehmenden Fachabteilung, bei Verlegung die der weiterbehandelnden Fachabteilungen,*
6. *Datum und Art der im jeweiligen Krankenhaus durchgeführten Operationen und sonstigen Prozeduren,*
7. *den Tag, die Uhrzeit und den Grund der Entlassung oder der Verlegung, bei externer Verlegung das Institutionskennzeichen der aufnehmenden Institution, bei Entlassung oder Verlegung die für die Krankenhausbehandlung maßgebliche Hauptdiagnose und die Nebendiagnosen,*
8. *Angaben über die im jeweiligen Krankenhaus durchgeführten Leistungen zur medizinischen Rehabilitation und ergänzende Leistungen sowie Aussagen zur Arbeitsfähigkeit und Vorschläge für die Art der weiteren Behandlung mit Angabe geeigneter Einrichtungen,*
9. *die … berechneten Entgelte.*

Im Einzelfall kommt als datenschutzrechtliche Rechtsgrundlage ausnahmsweise auch ein Vertrag zwischen der Krankenhausgesellschaft und den zuständigen Verbänden der Krankenkassen in Betracht. Schließlich handelt es sich hier um einen Normsetzungsvertrag (siehe Nr. 8.1.1).

Kann die Krankenkasse den Sachverhalt aufgrund der Angaben der ersten Stufe nicht abschließend prüfen, ist auf der zweiten Stufe ein Prüfverfahren durch den MDK einzuleiten. Nach ständiger Rechtsprechung steht den Krankenkassen aber kein Recht zu, selbst in die ärztlichen Behandlungsunterlagen Einsicht zu nehmen bzw. diese „zur Vorprüfung“ anzufordern. Im Rahmen einer dritten Stufe hat das Krankenhaus dann ggf. dem MDK über die bisherigen Angaben hinaus alle weiteren Angaben zu erteilen und Unterlagen vorzulegen, die im Einzelfall zur Beantwortung der Prüfanfrage der Krankenkasse benötigt werden.

Auch hier hat die überprüfte Krankenkasse mir inzwischen zugesichert, sie werde sich im Grundsatz an diese datenschutzrechtlichen Vorgaben halten. Ich gehe aber auch hier davon aus, dass ich mich im künftigen Berichtszeitraum mit vielen Einzelfragen zu beschäftigen habe.

8.1.6 Datenschutzrechtliche Befugnisse im Rahmen des Risikostrukturausgleichs

Auf Grund einiger Eingaben und der Presseberichterstattung habe ich mich mit der folgenden datenschutzrechtlichen Problematik befasst. Danach nehmen Krankenkassen teilweise Kontakt mit Leistungserbringern auf, um über deren Abrechnungen zu sprechen. Zum einen sollen dabei Unklarheiten bzw. Unplausibilitäten geklärt werden. Zum anderen versuchen Krankenkassen aber zum Teil unmittelbar bzw. mittelbar Einfluss auf die konkrete Diagnose bzw. die entsprechende Codierung zu nehmen. Schließlich hängt es davon ab, wieviel Geld die Krankenkasse aus dem sog. Risikostrukturausgleich zwischen den Krankenkassen bekommt.

Wie bereits dargelegt, reicht eine Datenerhebungsbefugnis der Krankenkasse grundsätzlich nur soweit wie die entsprechende Übermittlungsbefugnis des Leistungserbringers (siehe Nrn. 8.1.2 und 8.1.5). Nach der Rechtsprechung haben die Krankenkassen zwar die entsprechenden Daten nachzuerfassen, sofern die Leistungserbringer (vermeintlich) ihren Übermittlungspflichten nicht nachkommen. Die Krankenkassen dürfen bei Zweifeln oder Unklarheiten in Bezug auf die übermittelten Daten aber grundsätzlich lediglich durch nicht-medizinische Nachfragen beim Leistungserbringer klären, ob die jeweiligen Voraussetzungen der Zahlungspflicht im Einzelfall gegeben sind. Die anschließende Prüfung, ob die genannten Gründe tatsächlich vorliegen und medizinisch stichhaltig sind, bleibt jedoch allein dem Medizinischen Dienst der Krankenversicherung vorbehalten (siehe Nrn. 8.1.4, 8.1.2, 8.1.5). Die künftige Einhaltung dieser Vorgaben wurde mir zugesichert.

8.1.7 Übermittlung von Gutachten an Krankenkassen durch den MDK Bayern

Zur Frage, in welchem Umfang der Medizinische Dienst der Krankenversicherung in Bayern (MDK Bayern) sozialmedizinische Gutachten an die Krankenkasse weitergeben kann, habe ich den Austausch mit dem MDK Bayern im Berichtszeitraum fortgeführt. Begleitend habe ich mir im Rahmen meiner Prüftätigkeit vor Ort ein Bild über den Inhalt von und den Umgang mit Gutachten des MDK Bayern in der Praxis gemacht.

Ausgangspunkt der – aufgrund erheblicher Fallzahlen besonders praxisrelevanten – datenschutzrechtlichen Bewertung ist die Regelung des § 277 Abs. 1 Sozialgesetzbuch Fünftes Buch – Gesetzliche Krankenversicherung (SGB V) über Mitteilungspflichten des MDK. Diese schafft die gesetzliche Grundlage für eine Übermittlung von bestimmten Sozialdaten durch den MDK an die Krankenkassen, **begrenzt** aber zugleich den **Umfang dieser Datenübermittlungen**. So dürfen durch den MDK lediglich das Ergebnis der Begutachtungen sowie die erforderlichen Angaben über den jeweiligen Befund an die Krankenkassen mitgeteilt werden, nicht aber weitere Informationen, die in den sozialmedizinischen Gutachten enthalten sind.

§ 277 SGB V Mitteilungspflichten
(1) Der Medizinische Dienst hat dem an der vertragsärztlichen Versorgung teilnehmenden Arzt, sonstigen Leistungserbringern, über deren Leistungen er eine gutachtliche Stellungnahme abgegeben hat, und der Krankenkasse das Ergebnis der Begutachtung und der Krankenkasse die erforderlichen Angaben über den

Befund mitzuteilen. Er ist befugt, den an der vertragsärztlichen Versorgung teilnehmenden Ärzten und den sonstigen Leistungserbringern, über deren Leistungen er eine gutachtliche Stellungnahme abgegeben hat, die erforderlichen Angaben über den Befund mitzuteilen. Der Versicherte kann der Mitteilung über den Befund an die Leistungserbringer widersprechen.

Über die auf meinen Anstoß hin erfolgte Überarbeitung des beim MDK Bayern zum Einsatz kommenden EDV-Verfahrens (ISmed 3) mit dem Ziel eines datenschutzkonformen Vorgehens beim Umgang mit medizinischen Daten durch den MDK Bayern habe ich bereits in meinem 25. Tätigkeitsbericht 2012 unter Nr. 8.13 berichtet. Zum Umgang mit dem Teilaspekt der Zusammenarbeit des MDK Bayern mit den Krankenkassen bei **drittverursachten Gesundheitsschäden** (hierzu gehören insbesondere die Behandlungsfehler) verweise ich auf meine obigen Ausführungen (siehe Nr. 8.1.3).

Unabhängig von der im Wesentlichen positiven Entwicklung konnte ich allerdings nicht davon absehen, den MDK Bayern **förmlich** zu **beanstanden**. Ursächlich war neben der Tatsache, dass es in der Vergangenheit in einer erheblichen Vielzahl von Fällen zur Übermittlung des **gesamten** sozialmedizinischen Gutachtens an die Krankenkasse gekommen war, der Aspekt, dass die datenschutzrechtlichen Verstöße auch **besonders sensible Sozialdaten** betrafen.

Zwischenzeitlich hat der bundesweit tätige Medizinische Dienst des Spitzenverbandes Bund der Krankenkassen e.V. (MDS) eine **„Gemeinsame Empfehlung zur Umsetzung des § 277 SGB V“** formuliert. Die Empfehlung enthält neben Hinweisen zu einer rechtskonformen Umsetzung der gesetzlichen Vorgabe die – auch von mir wiederholt geforderte – Anregung, die MDK-Gutachter hinsichtlich der Thematik, welche Sozialdaten an die Krankenkasse übermittelt werden, zu **sensibilisieren**.

Der Bund-Länder-Arbeitskreis „Gesundheit und Soziales“ der Datenschutzbeauftragten nahm die Empfehlung als **Mindeststandard** zustimmend zur Kenntnis und stellte zugleich fest, dass angesichts der deutschlandweit unterschiedlichen Situationen ein differenziertes Vorgehen notwendig sei.

8.1.8 Gewinnspiele von Krankenkassen

Mit der datenschutzrechtlichen Problematik von Gewinnspielen bei Krankenkassen war ich bereits in der Vergangenheit befasst (siehe 22. Tätigkeitsbericht 2006 Nr. 14.1.4). Zwar ist es angesichts des Wettbewerbs zwischen den gesetzlichen Krankenkassen nachvollziehbar, dass diese versuchen, neue Mitglieder zu werben bzw. an die personenbezogenen Daten potenzieller Neumitglieder zu gelangen. Dabei müssen sie jedoch die datenschutzrechtlichen Vorschriften einhalten. Der Gesetzgeber hat dazu im Jahr 2004 eine Regelung vorgesehen:

§ 284 Sozialgesetzbuch Fünftes Buch – Gesetzliche Krankenversicherung (SGB V) Sozialdaten bei den Krankenkassen
(1) Die Krankenkassen dürfen Sozialdaten für Zwecke der Krankenversicherung nur erheben und speichern, soweit diese für
1. die Feststellung des Versicherungsverhältnisses und der Mitgliedschaft, einschließlich der für die Anbahnung eines Versicherungsverhältnisses erforderlichen Daten … erforderlich sind.

(4) Zur Gewinnung von Mitgliedern dürfen die Krankenkassen Daten erheben, verarbeiten und nutzen, wenn die Daten allgemein zugänglich sind, es sei denn, dass das schutzwürdige Interesse des Betroffenen an dem Ausschluss der Verarbeitung oder Nutzung überwiegt … Widerspricht der Betroffene bei der verantwortlichen Stelle der Nutzung oder Übermittlung seiner Daten, ist sie unzulässig. Die Daten sind zu löschen, sobald sie für die Zwecke nach Satz 1 nicht mehr benötigt werden …

Im konkreten Einzelfall hat die Krankenkasse jedoch keine allgemein zugänglichen Daten verwendet. Vielmehr hat sie im Rahmen eines öffentlichen Festes Passanten angesprochen, ob sie an einem Gewinnspiel teilnehmen wollen. Dabei wurden u.a. auch 14jährige Jugendliche angesprochen. Lediglich bei unter 14jährigen hat die jeweilige Krankenkasse eine Einwilligungserklärung der Eltern verlangt.

Ich habe deutlich gemacht, dass ein derartiges Vorgehen nicht mit datenschutzrechtlichen Vorschriften vereinbar ist. Nach längeren Gesprächen mit der Krankenkasse konnte ich einige Verbesserungen erreichen: So wird die Krankenkasse zukünftig auf dem jeweiligen Handzettel darauf hinweisen, dass sie die Daten u.a. zum Zweck der Mitgliedergewinnung (Anbahnung eines Versicherungsverhältnisses) erhebt. Sie wird die entsprechende Einwilligungserklärung des Betroffenen umgestalten. Im Übrigen wird die Krankenkasse angesichts einer höchstrichterlichen Rechtsprechung zukünftig davon absehen, Daten von Minderjährigen zum Zwecke der Mitgliedergewinnung zu erheben. Ich werde auch weiterhin kontrollieren, ob diese Vorschriften eingehalten werden.

8.1.9 Callcenter im Auftrag von Krankenkassen

Bereits im 25. Tätigkeitsbericht 2012 unter Nr. 8.10 habe ich mich mit Telefonaktionen befasst, die Callcenter im Auftrag von Krankenkassen bei Krankenversicherten durchgeführt haben. Dabei konnte ich die datenschutzrechtliche Situation verbessern: Zum einen hat die Krankenkasse die Einwilligungserklärung modifiziert, die sie ihren Kunden vorlegt. Damit steht nun die Verarbeitung und Nutzung der Kundendaten auf einer datenschutzrechtlichen Grundlage. Zum anderen hat sie ihren Gesprächsleitfaden verändert. Danach erhebt sie Daten im Rahmen der Telefoninterviews nur dann, wenn dies zur Erfüllung bestimmter Aufgaben der Krankenkasse erforderlich ist.

Im Berichtszeitraum musste ich mich mit weiteren Telefonaktionen auseinandersetzen. Aus diesem Grund möchte ich nochmals darauf hinweisen, dass eine Krankenkasse nur dann Kontakt mit (potentiellen) Versicherten aufnehmen darf, wenn eine ausdrückliche Einwilligung hierzu vorliegt. Diese Auffassung teilen auch Rechtsprechung und das Staatsministerium für Gesundheit und Pflege.

§ 7 Gesetz gegen den unlauteren Wettbewerb (UWG) Unzumutbare Belästigungen
(1) Eine geschäftliche Handlung, durch die ein Marktteilnehmer in unzumutbarer Weise belästigt wird, ist unzulässig. Dies gilt insbesondere für Werbung, obwohl erkennbar ist, dass der angesprochene Marktteilnehmer diese Werbung nicht wünscht.
(2) Eine unzumutbare Belästigung ist stets anzunehmen …

[2]bei Werbung mit einem Telefonanruf gegenüber einem Verbraucher ohne dessen vorherige ausdrückliche Einwilligung oder gegenüber einem sonstigen Marktteilnehmer ohne dessen zumindest mutmaßliche Einwilligung …

8.1.10 Sonstige externe Gesundheitsdienstleister im Auftrag von Krankenkassen

Verschiedene Gesundheitsreformen versuchen über die Einführung von Wettbewerbsmechanismen, die Qualität und die Effizienz der gesetzlichen Krankenkassen zu verbessern. Die Kassen sind daher bemüht und vom Gesetzgeber angehalten, ihre Versicherten durch verschiedene Programme zu „steuern". Diese Steuerungsprogramme habe ich bereits in meinem 23. Tätigkeitsbericht 2008 Anlage 24 thematisiert. Dort habe ich auf die Entschließung der 76. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 06./07.11.2008 verwiesen. Die dort festgehaltenen datenschutzrechtlichen Grundsätze sind nach wie vor gültig.

Im Berichtszeitraum war ich insbesondere mit verschiedenen Programmen zur integrierten Versorgung nach § 140a Sozialgesetzbuch Fünftes Buch – Gesetzliche Krankenversicherung (SGB V) befasst. Dabei habe ich insbesondere auf weitere datenschutzrechtliche Vorgaben Wert gelegt:

§ 140a SGB V Integrierte Versorgung
(2) Die Teilnahme der Versicherten an den integrierten Versorgungsformen ist freiwillig … Ein behandelnder Leistungserbringer darf aus der gemeinsamen Dokumentation … die den Versicherten betreffenden Behandlungsdaten und Befunde nur dann abrufen, wenn der Versicherte ihm gegenüber seine Einwilligung erteilt hat, die Information für den konkret anstehenden Behandlungsfall genutzt werden soll und der Leistungserbringer zu dem Personenkreis gehört, der … zur Geheimhaltung verpflichtet ist. (Managementgesellschaften) … dürfen die für die Durchführung der zum Versorgungsmanagement notwendigen Steuerungsaufgaben im Rahmen der integrierten Versorgung erforderlichen personenbezogenen Daten aus der gemeinsamen Dokumentation … nur mit Einwilligung und nach vorheriger Information des Versicherten erheben, verarbeiten und nutzen …

Zum einen dürfen Krankenkassen auch bei Steuerungsprogrammen keine sensiblen medizinischen Daten zur Kenntnis nehmen. Dies ist ausschließlich dem Medizinischen Dienst der Krankenversicherung vorbehalten (siehe Nrn. 8.1.2 - 8.1.6).

Außerdem habe ich Zweifel an der Berechtigung einer Managementgesellschaft, sensible medizinische Daten zu erheben, zu verarbeiten und zu nutzen. Insbesondere ist eine Analyse dieser Daten (z.B. für eine Krankenkasse) grundsätzlich nur dann zulässig, sofern kein Personenbezug mehr vorliegt.

Zum anderen ist eine pauschale Information und Abstimmung von Ärzten und sonstigen Leistungserbringern untereinander datenschutzrechtlich nicht zulässig.

8.2 Pflege

8.2.1 Gesetz zur Änderung des Pflege- und Wohnqualitätsgesetzes

Die Zahl der Eingaben zu datenschutzrechtlichen Fragen bei der Pflege hat im Berichtszeitraum erheblich zugenommen. Daher war es sehr bedauerlich, dass ich bei der kürzlich erfolgten Änderung des Pflege- und Wohnqualitätsgesetzes (PfleWoqG) erst im Rahmen der Verbändeanhörung Gelegenheit hatte, mich zu äußern. Die Staatsregierung hat meine Ausführungen in meinem 23. Tätigkeitsbericht 2008 unter Nr. 17.7.1 berücksichtigt. Zukünftig dürfen Pflege-Prüfberichte keine personenbezogenen Daten enthalten. Meine weiteren Anregungen hat die Staatsregierung jedoch leider nicht aufgegriffen. Nicht zuletzt deshalb sind die derzeitigen datenschutzrechtlichen Regelungen, insbesondere Art. 11 Abs. 2 PfleWoqG nicht geeignet, die Erhebung, Verarbeitung und Nutzung von Daten in diesem Bereich rechtsklar zu regeln.

Art. 11 PfleWoqG Qualitätssicherung
(2) Die von der zuständigen Behörde mit der Überwachung der stationären Einrichtung beauftragten Personen sind befugt,

1. *die für die stationäre Einrichtung genutzten Grundstücke und Räume zu betreten; soweit diese einem Hausrecht der Bewohnerinnen und Bewohner unterliegen, nur mit deren Zustimmung,*
2. *Prüfungen und Besichtigungen vorzunehmen,*
3. *Einsicht in die Aufzeichnungen … der auskunftspflichtigen Person in der jeweiligen stationären Einrichtung zu nehmen,*
4. *sich mit den Bewohnerinnen und Bewohnern sowie der Bewohnervertretung oder dem Bewohnerfürsprecher in Verbindung zu setzen,*
5. *bei pflegebedürftigen Bewohnerinnen und Bewohnern mit deren Zustimmung den Pflegezustand zu begutachten,*
6. *die Beschäftigten zu befragen.*

Die Erhebung, Verarbeitung und Nutzung der durch Tätigkeiten nach Satz 1 gewonnenen personenbezogenen Daten bedarf der Zustimmung durch die Bewohnerin oder den Bewohner. Die Mitwirkung der Bewohnerinnen und Bewohner ist freiwillig; durch die Ablehnung dürfen keine Nachteile entstehen. Die Betroffenen sind darauf hinzuweisen, dass die Zustimmung verweigert werden kann. Die Zustimmung muss in Textform … abgegeben werden. Der Träger und die Leitung haben die Maßnahmen … zu dulden …

Diese Befugnis ist bei der Verarbeitung und Nutzung von Beschäftigtendaten wohl nicht einschlägig. Schließlich sieht sie immer eine Zustimmung der Bewohner vor. Der Gesetzgeber hatte bei Schaffung dieser Regelung also wohl nur die Daten der Bewohner im Auge. Ich gehe daher davon aus, dass bei Beschäftigtendaten der Anwendungsbereich dieser Vorschrift entsprechend ihrem Sinn und Zweck zu reduzieren ist und das Bayerische Datenschutzgesetz bzw. in entsprechender Anwendung das für die bayerischen Beamtinnen und Beamten geltende Personalaktenrecht Anwendung findet. Unabhängig vom Wortlaut der jeweiligen Regelung müsste überdies der verfassungsrechtlich garantierte Grundsatz der Erforderlichkeit Anwendung finden.

Der ursprüngliche Gesetzentwurf der Staatsregierung sah zunächst sogar nur eine mündliche Einwilligung vor. Es wurde befürchtet, dass andernfalls keine unangemeldeten Prüfungen mehr durchgeführt werden könnten. Damit hätten sich die datenschutzrechtlichen Regelungen des PfleWoqG und des Sozialgesetzbuches

Elftes Buch – Soziale Pflegeversicherung (SGB XI) (siehe Nr. 8.2.2) aber noch weiter voneinander entfernt, obwohl Heimaufsichten bzw. der Medizinische Dienst der Krankenversicherung (MDK) die Prüfungen an sich gemeinsam durchführen sollen.

Aus diesem Grund habe ich bereits in der Verbändeanhörung die Textform für diese Einwilligungserklärungen vorgeschlagen. Sie ermöglicht gewisse Erleichterungen; so könnte die Einwilligung nicht nur schriftlich, sondern auch per E-Mail oder Fax abgegeben werden. Daher hat es mich sehr gefreut, dass der Bayerische Landtag mein Anliegen aufgegriffen hat.

Trotz intensiver Gespräche vertrat das damals zuständige Staatsministerium nach Inkrafttreten dieser Vorschrift aber eine andere rechtliche Auffassung als ich: So sollten die Heimaufsichten (wie auch der MDK) grundsätzlich lediglich im Namen der Bewohner bzw. deren Betreuer deren mündlich erteilte Einwilligungserklärung vermerken. Ich habe darauf hingewiesen, dass eine solche rechtliche Auffassung den gesetzgeberischen Willen umgeht. Dieses Vorgehen wurde auch in vielen Eingaben an mich kritisiert.

Daher erachte ich es als besonders positiv, dass das Staatsministerium für Gesundheit und Pflege letztlich auf meine Anregung hin bereit war, die bisherige Rechtsauffassung des bisher zuständigen Staatsministeriums weiterzuentwickeln. Ich erlaube mir, die erarbeiteten Vorschläge wie folgt zusammenzufassen:

1. Im absoluten Regelfall hat die Zustimmung des Bewohners bzw. seines Betreuers vor der Prüfung in Textform zu erfolgen.

2. Sofern dies dokumentiert ausnahmsweise nicht möglich sein sollte, kann die Zustimmung des Bewohners bzw. seines Betreuers vor der Prüfung auch in mündlicher Form erfolgen. Diese mündliche Einwilligung ist aber sofort durch eine dritte Person – die jedoch nicht die Prüfinstitution selbst sein kann – in Textform zu dokumentieren.

Ich habe mich daraufhin bereit erklärt, von einer Beanstandung der Prüfinstitutionen abzusehen, sofern sie diese Auffassung berücksichtigen. Das Staatsministerium hat die Prüfinstitutionen in einem mit mir abgestimmten Schreiben über die weiterentwickelte Verfahrensweise informiert. Ich werde die Einhaltung der vereinbarten Verfahren überprüfen (siehe Nr. 8.2.2).

8.2.2 Einwilligung der Betroffenen bei der Durchführung von Qualitätsprüfungen

Das Pflege- und Wohnqualitätsgesetz (siehe Nr. 8.2.1) ist nicht das einzige Gesetz, das sich mit den Anforderungen in der Pflege auseinandersetzt. Die medizinischen Fragestellungen der Pflege sind im Sozialgesetzbuch Elftes Buch – Soziale Pflegeversicherung (SGB XI) geregelt. Danach führt der Medizinische Dienst der Krankenversicherung (MDK) regelmäßig Qualitätsprüfungen nach § 114a SGB XI durch.

§ 114a SGB XI Durchführung der Qualitätsprüfungen
(1) Der Medizinische Dienst der Krankenversicherung … (ist) berechtigt und verpflichtet, an Ort und Stelle zu überprüfen, ob die zugelassenen Pflegeeinrichtungen die Leistungs- und Qualitätsanforderungen nach diesem Buch erfüllen …

(2) Sowohl bei teil- als auch bei vollstationärer Pflege … (ist) der Medizinische Dienst der Krankenversicherung … berechtigt, zum Zwecke der Qualitätssicherung die für das Pflegeheim benutzten Grundstücke und Räume jederzeit zu betreten, dort Prüfungen und Besichtigungen vorzunehmen, sich mit den Pflegebedürftigen, ihren Angehörigen, vertretungsberechtigten Personen und Betreuern in Verbindung zu setzen sowie die Beschäftigten und die Interessenvertretung der Bewohnerinnen und Bewohner zu befragen … Bei der ambulanten Pflege … (ist) der Medizinische Dienst der Krankenversicherung … berechtigt, die Qualität der Leistungen des Pflegedienstes mit Einwilligung des Pflegebedürftigen auch in dessen Wohnung zu überprüfen. Der Medizinische Dienst der Krankenversicherung … (soll) die nach heimrechtlichen Vorschriften zuständige Aufsichtsbehörde an Prüfungen beteiligen, soweit dadurch die Prüfung nicht verzögert wird.
(3) Die Prüfungen beinhalten auch Inaugenscheinnahmen des gesundheitlichen und pflegerischen Zustands von Pflegebedürftigen. Sowohl Pflegebedürftige als auch Beschäftigte der Pflegeeinrichtungen, Betreuer und Angehörige sowie Mitglieder der heimrechtlichen Interessenvertretungen der Bewohnerinnen und Bewohner können dazu befragt werden … Die Teilnahme an Inaugenscheinnahmen und Befragungen ist freiwillig; durch die Ablehnung dürfen keine Nachteile entstehen. Einsichtnahmen in Pflegedokumentationen, Inaugenscheinnahmen von Pflegebedürftigen und Befragungen von Personen … sowie die damit jeweils zusammenhängende Erhebung, Verarbeitung und Nutzung personenbezogener Daten von Pflegebedürftigen zum Zwecke der Erstellung eines Prüfberichts bedürfen der Einwilligung der betroffenen Pflegebedürftigen.
(3a) Die Einwilligung nach Abs. 2 oder 3 muss in einer Urkunde oder auf andere zur dauerhaften Wiedergabe in Schriftzeichen geeignete Weise abgegeben werden, die Person des Erklärenden benennen und den Abschluss der Erklärung durch Nachbildung der Namensunterschrift oder anders erkennbar machen (Textform). Ist der Pflegebedürftige einwilligungsunfähig, ist die Einwilligung eines hierzu Berechtigten einzuholen …

Auch hier muss die Einwilligung der Betroffenen in Textform erfolgen. Einwilligungen können also z.B. auch per E-Mail oder Fax abgegeben werden.

Das damals zuständige Staatsministerium vertrat zunächst eine andere rechtliche Auffassung als ich. Letztendlich konnte aber – vergleichbar zum Pflege- und Wohnqualitätsgesetz – eine Lösung gefunden werden, die sowohl dem Grundgedanken des Gesetzes, als auch den Anforderungen in der Praxis Rechnung trägt (siehe Nr. 8.2.1).

8.2.3 Zusätzliche Leistungen für Pflegebedürftige in ambulant betreuten Wohngruppen

Mit dem Gesetz zur Neuausrichtung der Pflegeversicherung (Pflege-Neuausrichtungs-Gesetz – PNG), das am 30.10.2012 in Kraft getreten ist, hat der Bundesgesetzgeber in § 38a Sozialgesetzbuch Elftes Buch – Soziale Pflegeversicherung (SGB XI) eine neue Leistung für Pflegebedürftige in ambulant betreuten Wohngruppen geschaffen (eingefügt durch Art. 1 Nr. 13 Gesetz vom 23.10.2012, BGBl. I Seite 2246).

§ 38a SGB XI Zusätzliche Leistungen für Pflegebedürftige in ambulant betreuten Wohngruppen
(1) Pflegebedürftige haben Anspruch auf einen pauschalen Zuschlag in Höhe von 200 Euro monatlich, wenn

1. sie in ambulant betreuten Wohngruppen in einer gemeinsamen Wohnung mit häuslicher pflegerischer Versorgung leben,
2. sie Leistungen nach § 36, § 37 oder § 38 beziehen,
3. in der ambulant betreuten Wohngruppe eine Pflegekraft tätig ist, die organisatorische, verwaltende oder pflegerische Tätigkeiten verrichtet, und
4. es sich um ein gemeinschaftliches Wohnen von regelmäßig mindestens drei Pflegebedürftigen handelt mit dem Zweck der gemeinschaftlich organisierten pflegerischen Versorgung, dem die jeweils maßgeblichen heimrechtlichen Vorschriften oder ihre Anforderungen an Leistungserbringer nicht entgegenstehen.

(2) Keine ambulante Versorgungsform im Sinne von Abs. 1 liegt vor, wenn die freie Wählbarkeit der Pflege- und Betreuungsleistungen rechtlich oder tatsächlich eingeschränkt ist. Die von der Gemeinschaft unabhängig getroffenen Regelungen und Absprachen sind keine tatsächlichen Einschränkungen in diesem Sinne.

Die diese Leistung auf Antrag gewährenden gesetzlichen Pflegekassen haben für ihre Versicherten in der Regel unterschiedlich ausgestaltete Formulare zum „Antrag auf einen pauschalen Wohngruppenzuschlag für Pflegebedürftige in ambulant betreuten Wohngruppen“ entwickelt. Zur möglichst bundesweit einheitlichen Gestaltung der Antragsformulare haben sich die Bundes- und Landesdatenschutzbeauftragten weitgehend untereinander abgestimmt.

Auch ich hatte mich mit einem Antragsformular einer großen bayerischen gesetzlichen Pflegekasse zu befassen. Es ist gelungen, in dem Antragsformular alle wesentlichen Forderungen der Datenschutzbeauftragten des Bundes und der Länder umzusetzen und somit die Angaben im Antrag auf das zur Aufgabenerfüllung der Pflegekasse erforderliche Maß zu beschränken. Insbesondere wurde der Hinweis auf die Freiwilligkeit von Angaben in die Überschrift des Antragsformulars integriert und die freiwilligen Angaben (z.B. Angabe der Telefonnummer) mit dem Symbol (*) versehen. Wichtig war mir auch, dass die Rentenversicherungsnummer nicht abgefragt wird, genauso wie der Zeitpunkt des Einzugs in die Wohngemeinschaft, weil dies für die Antragsbearbeitung nicht erforderlich ist. Die Unterschrift der Pflege- bzw. Präsenzkraft ist nicht mehr verpflichtend und der Umfang der Datenerhebung bezüglich der anderen pflegebedürftigen Mitbewohner wurde auf die Angabe von zwei weiteren Pflegebedürftigen (mindestens Pflegestufe 1) reduziert; die Angaben wurden auf Name, Vorname, Geburtsdatum, Pflegekasse sowie die Frage, ob der Mitbewohner mindestens in Pflegestufe 1 eingestuft ist, beschränkt. Außerdem wurde die Unterschrift der Mitbewohner nur mehr als freiwillig gekennzeichnet.

Das zeitgerechte Abstimmungsverfahren hat nach meiner Überzeugung dazu beigetragen, dass zumindest in meiner Dienststelle keine nennenswerte Anzahl an Nachfragen oder gar Beschwerden zu den auszufüllenden Anträgen der Pflegekassen eingegangen sind.

Zwischenzeitlich hat der Bundesrat angeregt, mit der Aufnahme des neuen § 38a Abs. 2 SGB XI eine gesetzliche Ermächtigung zu schaffen, die es den Pflegekassen ermöglichen werde, zur Überprüfung der leistungsrechtlichen Tatbestandsmerkmale erforderliche Daten bei dem Antragsteller abzufragen (siehe Bundestags-Drucksache 18/1798 und Bundesrats-Drucksache 223/1/14 – Entwurf eines Fünften Gesetzes zur Änderung des Elften Buches Sozialgesetzbuch – Leistungsausweitung für Pflegebedürftige, Pflegevorsorgefonds (Fünftes SGB XI-Änderungsgesetz – 5. SGB XI-ÄndG)). Das Gesetzgebungsverfahren war bei Redaktionsschluss für diesen Tätigkeitsbericht noch nicht abgeschlossen.

8.3 Kindergarten

8.3.1 Veröffentlichung von personenbezogenen Daten durch Kindertageseinrichtungen

Viele Kindertageseinrichtungen wollen ihre Einrichtung und ihre pädagogische Arbeit der Öffentlichkeit, insbesondere interessierten Familien vorstellen.

Soweit sie dabei personenbezogene Daten der Kinder und Familien veröffentlichen, bedarf es hierfür aus datenschutzrechtlicher Sicht grundsätzlich einer freiwilligen, informierten und schriftlichen Einwilligung der betroffenen Eltern (zur Veröffentlichung von personenbezogenen Daten durch Schulen siehe auch meine Ausführungen im 25. Tätigkeitsbericht 2012 Nr. 10.3). Insbesondere wenn Fotografien gefertigt und veröffentlicht werden, handelt es sich um eine Erhebung bzw. Übermittlung personenbezogener Daten der abgebildeten Person. Solche Bildnisse dürfen nach dem Kunsturhebergesetz (KunstUrhG) nur mit Einwilligung des Abgebildeten verbreitet oder öffentlich zur Schau gestellt werden.

§ 22 KunstUrhG
(1) Bildnisse dürfen nur mit Einwilligung des Abgebildeten verbreitet oder öffentlich zur Schau gestellt werden …

In vielen Kindertageseinrichtungen ist es mittlerweile üblich, Aktivitäten der Kinder durch digitale Fotografien festzuhalten, diese auf eine CD zu brennen und diese dann den Eltern zu überlassen. Auch für diese Vorgehensweise muss eine datenschutzkonforme Einwilligung der Eltern vorliegen, die insbesondere schriftlich zu erfolgen hat und sich unter Darlegung des Sachverhaltes speziell auf diese Form der Datenspeicherung und Datenübermittlung beziehen muss. Fotografien der Kinder, deren Eltern keine entsprechende Einwilligung erteilt haben, dürfen nicht auf den an andere Eltern weitergebenen CDs enthalten sein.

8.3.2 Anmeldung für Kindertageseinrichtungen

Im Rahmen des Anmeldeverfahrens für Kindertageseinrichtungen ist es im Allgemeinen üblich, dass Eltern ihre Kinder bei verschiedenen Einrichtungen anmelden, um sicher zu gehen, auf jeden Fall einen der begehrten Plätze zu erhalten.

In diesem Zusammenhang stellt sich die Frage, ob die Einrichtungen untereinander personenbezogene Daten der angemeldeten Kinder austauschen dürfen bzw. ob die zuständige Gemeinde über eine zentrale Anmeldestelle alle angemeldeten Kinder erfassen darf.

Bereits im 17. Tätigkeitsbericht 1996 unter Nr. 4.8.1 habe ich dargelegt, dass ich eine Übermittlung und Nutzung von personenbezogenen Daten angemeldeter bzw. abgelehnter Kindergartenkinder durch benachbarte Kindergärten für zulässig erachte, soweit dies erforderlich ist, damit die Kindergärten ihre Aufgaben der Bedarfsplanung, der Kapazitätsberechnung, der Erkennung von Mehrfachanmeldungen und der Vermeidung von Doppelbelegungen erfüllen können und soweit hierzu kein weniger einschneidender Weg zur Verfügung steht. Die Eltern sollten allerdings bereits im Anmeldeformular bei der Kindergarten-Anmeldung darauf hingewiesen werden, dass ein Abgleich mit Anmeldungen bei benachbarten Kindergärten vorgesehen ist.

An dieser Auffassung habe ich auch im Berichtszeitraum festgehalten. Mit dem im Rahmen der Novellierung des Bayerischen Kinderbildungs- und -betreuungsgesetzes neu eingefügten Art. 28a BayKiBiG existiert hierfür nunmehr auch eine spezielle Rechtsgrundlage:

Art. 28a BayKiBiG Erhebung, Verarbeitung und Nutzung von Daten
(1) Die Erhebung, Verarbeitung und Nutzung von personenbezogenen Daten ist zulässig, wenn dies zur Erfüllung einer Aufgabe oder für eine Förderung nach diesem Gesetz erforderlich ist oder der Betroffene eingewilligt hat.
(2) Datenschutzrechtliche Regelungen in anderen Rechtsvorschriften bleiben unberührt.

Die Entscheidung der Gemeinden, welchen örtlichen Bedarf sie unter Berücksichtigung der Bedürfnisse der Eltern und ihrer Kinder für eine kindgerechte Bildung, Erziehung und Betreuung sowie sonstiger bestehender schulischer Angebote anerkennen (örtliche Bedarfsplanung), stellt eine Aufgabe nach Art. 7 BayKiBiG dar. Deshalb halte ich auch die **Einrichtung einer zentralen Anmeldestelle** bei der Gemeinde zur Erfüllung der Aufgabe der örtlichen Bedarfsplanung grundsätzlich für erforderlich und damit zulässig.

Im Zusammenhang mit dem zum 01.08.2013 in § 24 Abs. 2 Satz 1 Sozialgesetzbuch Achtes Buch – Kinder- und Jugendhilfe (SGB VIII) in Kraft getretenen Rechtsanspruch auf frühkindliche Förderung in einer Tageseinrichtung oder in Kindertagespflege für jedes Kind von Vollendung des ersten bis zur Vollendung des dritten Lebensjahres habe ich auch eine **Datenübermittlung** der bei den Gemeinden vorliegenden Anmeldelisten mit Name, Wohnort und Geburtsdatum der Kinder **an die örtlichen Träger der öffentlichen Jugendhilfe**, also die Landkreise und kreisfreien Städte, zur Erfüllung ihrer Aufgabe der Jugendhilfeplanung nach § 80 SGB VIII für erforderlich und damit zulässig gehalten.

Allerdings habe ich darauf hingewiesen, dass sowohl die Gemeinden als auch die Landkreise und kreisfreien Städte die Daten dann zu anonymisieren haben, wenn der jeweilige Planungszweck erfüllt ist.

8.4 Sonstige Jugendhilfe

8.4.1 Erweitertes Führungszeugnis für Ehrenamtliche

In meinem vorherigen 25. Tätigkeitsbericht 2012 unter Nr. 8.8 habe ich mich bereits grundsätzlich dazu geäußert, unter welchen Voraussetzungen es datenschutzrechtlich zulässig ist, dass Träger der Kinder- und Jugendhilfe und Stellen außerhalb der Kinder- und Jugendhilfe bestimmte Beschäftigtengruppen mit beruflichem Kontakt zu Minderjähren auffordern können, ein erweitertes Führungszeugnis zu beantragen und vorzulegen.

Im aktuellen Berichtszeitraum hatte ich mich mit folgenden Fragen zur Vorlage eines erweiterten Führungszeugnisses für ehrenamtliche Tätigkeiten im Rahmen der Jugendhilfe (§ 72a Sozialgesetzbuch Achtes Buch – Kinder- und Jugendhilfe – SGB VIII) zu befassen:

1. Können Mitglieder von Vereinen mit Name, Adresse, Personalausweisnummer und Unterschrift in einer Liste erfasst werden, die der Vereinsvorsitzende der zuständigen Gemeinde zur Beantragung der erweiterten Führungszeugnisse beim Bundeszentralregister übermittelt?

2. Kann die Einsichtnahme in die erweiterten Führungszeugnisse und die Erstellung einer „Unbedenklichkeitsbescheinigung" an Stelle des Vereinsvertreters durch Gemeindebedienstete erfolgen?

3. Verstößt die Einsichtnahme in erweiterte Führungszeugnisse ehrenamtlicher Helfer durch den Vereinsvorsitzenden gegen das Recht auf informationelle Selbstbestimmung?

4. Welche Vereine müssen nach § 72a SGB VIII Einsicht in die erweiterten Führungszeugnisse ihrer ehrenamtlichen Helfer nehmen? Gilt dies auch für Vereine außerhalb der Kinder- und Jugendhilfe, z.B. für ehrenamtliche Tätigkeiten der Freiwilligen Feuerwehr, der Kirchenchöre oder der „klassischen" Sportvereine?

Dazu habe ich folgende Auffassung vertreten:

1. Hinsichtlich der Eintragung der persönlichen Daten in eine offene Liste habe ich Bedenken. Schließlich ist eine derartige Übermittlung von Daten nicht erforderlich.

2. Rechtsgrundlage für eine Erhebung, Verarbeitung und Nutzung von Daten bei der Vorlage von erweiterten Führungszeugnissen im Rahmen der Kinder- und Jugendhilfe ist § 72a Abs. 5 SGB VIII. Der Wortlaut dieser Vorschrift berechtigt ausschließlich Träger der öffentlichen und freien Jugendhilfe. Daher sind Gemeinden datenschutzrechtlich nicht befugt, entsprechende Daten zu erheben, verarbeiten und zu nutzen.

3. Mit § 72a SGB VIII gibt es eine gesetzliche Regelung, die eine Einsichtnahme in erweiterte Führungszeugnisse ehrenamtlicher Helfer zulässt. Aus datenschutzrechtlicher Sicht sollte ausschließlich eine einzige vertrauenswürdige Person bei dem jeweiligen freien Träger für die Erhebung, Verarbeitung und Nutzung der entsprechenden Daten zuständig sein. Damit wäre am ehesten gewährleistet, dass möglichst wenige Personen Kenntnis von den betroffenen Daten erlangen.

4. Die Gesetzesbegründung zu § 72a SGB VIII (Bundestags-Drucksache 17/6256 Seite 26) führt ausdrücklich aus, dass sich diese Vorschrift nur auf die Erbringung von Leistungen der Kinder- und Jugendhilfe oder auf die Beteiligung der Erfüllung anderer Aufgaben seitens des Trägers der öffentlichen Jugendhilfe bezieht. Erfasst werden hierbei nur diejenigen Leistungen, die auch von der öffentlichen Jugendhilfe finanziert werden. Das Gesetz erfasst ferner nur diejenigen Tätigkeiten, die in einem pädagogischen Zusammenhang erbracht werden und wegen der Art, Dauer und Intensität des Kontaktes den Aufbau eines besonderen Vertrauensverhältnisses ermöglichen. Nicht bei allen ehrenamtlich tätigen Personen, die in unmittelbarem Kontakt mit Kindern und Jugendlichen stehen, darf Einsicht in das erweiterte Führungszeugnis genommen werden. Vielmehr ist nach dem eindeutigen Gesetzeswortlaut nach der Art, Intensität und Dauer des Kontaktes dieser Personen mit Kindern und Jugendlichen zu differenzieren.

8.4.2 Datenaustausch innerhalb der Jugendhilfe

„Es braucht ein ganzes Dorf, um ein Kind großzuziehen“ – dieses afrikanische Sprichwort wird vielfach bemüht, wenn es darum geht, Familien bei der Erziehung zu unterstützen. Natürlich ist Zusammenarbeit in der Jugendhilfe richtig und sinnvoll – kann allerdings nur im Rahmen der datenschutzrechtlichen Vorgaben erfolgen (siehe zuletzt 25. Tätigkeitsbericht 2012 Nr. 8.6). Dazu möchte ich auf einige Fragen eingehen, die immer wieder an mich herangetragen werden:

Zunächst möchte ich einen Irrtum aufklären, dem viele Eingabeführer unterliegen. Bei einer Datenerhebung in der Jugendhilfe ist grundsätzlich keine Einwilligung notwendig:

§ 62 Sozialgesetzbuch Achtes Buch – Kinder- und Jugendhilfe (SGB VIII) Datenerhebung
(1) Sozialdaten dürfen nur erhoben werden, soweit ihre Kenntnis zur Erfüllung der jeweiligen Aufgabe erforderlich ist.

Auch die Zusammenarbeit mit den Familiengerichten wird immer wieder kritisiert. Auch hier ist nach der gesetzlichen Konzeption grundsätzlich keine Einwilligung vorgesehen.

§ 50 SGB VIII Mitwirkung in Verfahren vor den Familiengerichten
(1) Das Jugendamt unterstützt das Familiengericht bei allen Maßnahmen, die die Sorge für die Person von Kindern und Jugendlichen betreffen. …
(2) Das Jugendamt unterrichtet insbesondere über angebotene und erbrachte Leistungen, bringt erzieherische und soziale Gesichtspunkte zur Entwicklung des Kindes oder des Jugendlichen ein und weist auf weitere Möglichkeiten der Hilfe hin. In Kindschaftssachen informiert das Jugendamt das Familiengericht … über den Stand des Beratungsprozesses.

Zusätzliche Anforderungen bestehen jedoch dann, sofern tatsächlich ein besonderes Vertrauensverhältnis zu einem Vertreter der Jugendhilfe vorlag:

§ 65 SGB VIII Besonderer Vertrauensschutz in der persönlichen und erzieherischen Hilfe
(1) Sozialdaten, die dem Mitarbeiter eines Trägers der öffentlichen Jugendhilfe zum Zwecke persönlicher und erzieherischer Hilfe anvertraut worden sind, dürfen von diesem nur weitergegeben werden
1. mit der Einwilligung dessen, der die Daten anvertraut hat, oder
2. dem Familiengericht …, wenn angesichts einer Gefährdung des Wohls eines Kindes oder eines Jugendlichen ohne diese Mitteilung eine für die Gewährung von Leistungen notwendige gerichtliche Entscheidung nicht ermöglicht werden könnte, oder …
3. an die Fachkräfte, die zum Zwecke der Abschätzung des Gefährdungsrisikos … hinzugezogen werden; …

Diese Vorschrift muss auch in der Aktenführung mit Leben gefüllt werden. Schließlich sind die technisch-organisatorischen Maßnahmen einschließlich der Dienstanweisungen zu treffen, die erforderlich sind, um die Einhaltung der datenschutzrechtlichen Vorschriften sicherzustellen. Ich gehe daher davon aus, dass für derartige anvertraute Daten ein eigenständiger Bereich in den jeweiligen Jugendhilfeakten vorgesehen ist.

Im Berichtszeitraum war ich aber leider auch mit Eingaben befasst, in denen das sprichwörtliche „Dorf“ leider etwas zu groß geworden ist.

Zwar mögen Fallkonferenzen, Supervisionen bzw. institutionsübergreifende Kooperationen durchaus geeignete pädagogische Mittel darstellen. Allerdings ist jeder Vertreter dieser Gespräche verpflichtet, die für ihn einschlägigen datenschutzrechtlichen Vorschriften einzuhalten. Aus diesem Grunde rege ich an, grundsätzlich möglichst abstrakt-generell über bestimmte Fallgestaltungen (und nicht Personen) zu diskutieren. Schließlich sind die datenschutzrechtlichen Vorschriften dann nicht anwendbar, sofern es sich nicht um personenbezogene Daten handelt. Es darf allerdings kein Rückschluss auf eine konkrete Person möglich sein. Eine Alternative wäre auch, eine Einwilligungserklärung der Betroffenen bzw. zu besprechenden Personen einzuholen.

Auch die Jugendhilfeplanung sollte grundsätzlich mit anonymisierten Daten arbeiten:

§ 64 SGB VIII Datenübermittlung und -nutzung
(3) Sozialdaten dürfen beim Träger der öffentlichen Jugendhilfe zum Zwecke der Planung … gespeichert oder genutzt werden; sie sind unverzüglich zu anonymisieren.

Auch die wirtschaftliche Jugendhilfe, die den Fall kostenmäßig abrechnet, will manchmal mehr wissen, als ihr zusteht (siehe auch 22. Tätigkeitsbericht 2006 Nr. 14.2.1). Hier ist meiner Einschätzung nach grundsätzlich lediglich die Übermittlung eines Datenblattes erforderlich, die die wirtschaftliche Jugendhilfe zur weiteren Bearbeitung braucht (z.B. Geltendmachung von Kostenerstattungsbeiträgen, Ersatzansprüche bzw. die fortdauernde Zuständigkeit). Der Inhalt von Hilfeplänen bzw. medizinischer Gutachten etc. ist grundsätzlich nicht erforderlich. Eine weitere Beteiligung der wirtschaftlichen Jugendhilfe ist meiner Einschätzung nach lediglich in Ausnahmefällen (z.B. sehr komplexe bzw. kostenintensive Maßnahmen) denkbar.

8.4.3 Erhebung von Gesundheitsdaten im Rahmen der Vollzeitpflege

Der tragische Tod des elfjährigen Pflegekinds Chantal in Hamburg im Jahr 2012 sorgte bundesweit für große Anteilnahme. In der Folge sahen sich zahlreiche Jugendämter veranlasst, ihre Praxis der Auswahl und Kontrolle von Pflegeeltern zu überprüfen und fortzuentwickeln.

Mit dem Fall eines Kreisjugendamts konfrontiert, das mittels eines Fragebogens die gesundheitliche Eignung von Pflegeeltern ermitteln wollte, habe ich geprüft, inwieweit im Rahmen der Vollzeitpflege Gesundheitsdaten von Pflegeeltern durch Jugendämter erhoben werden können. Der Fragebogen sah u.a. vor, dass die Pflegeeltern ihre Ärzte gegenüber dem Jugendamt von der Schweigepflicht entbinden.

Bei meiner datenschutzrechtlichen Bewertung war ich mir darüber im Klaren, dass meine für die Tagespflege entwickelte Rechtsauffassung (siehe 24.Tätigkeitsbericht 2010 Nr. 8.2) nicht auf die betreuungsintensivere Vollzeitpflege übertragen werden kann.

8.4.3.1 Datenerhebung vor Erteilung einer Pflegeerlaubnis

Um sich im Bereich der Vollzeitpflege engagieren zu können, müssen Interessenten eine Pflegeerlaubnis beim Jugendamt beantragen. Im Zuge des Verfahrens über die Erteilung einer Erlaubnis zur Vollzeitpflege dürfen Sozialdaten erhoben werden, soweit ihre Kenntnis zur Erfüllung der Aufgaben des Jugendamts erforderlich ist (§ 62 Abs. 1 Sozialgesetzbuch Achtes Buch – Kinder- und Jugendhilfe – SGB VIII).

§ 62 SGB VIII Datenerhebung
(1) Sozialdaten dürfen nur erhoben werden, soweit ihre Kenntnis zur Erfüllung der jeweiligen Aufgabe erforderlich ist.

Die Erlaubnis zur Vollzeitpflege ist durch das Jugendamt zu versagen, wenn die Pflegeperson oder in ihrem Haushalt lebende Personen an einer Krankheit leiden, die das Wohl des Kindes bzw. Jugendlichen nicht nur unerheblich gefährdet (§ 44 Abs. 1 SGB VIII in Verbindung mit Art. 35 Satz 2 Nr. 6 Gesetz zur Ausführung der Sozialgesetze – AGSG).

§ 44 SGB VIII Erlaubnis zur Vollzeitpflege
(1) [1]Wer ein Kind oder einen Jugendlichen über Tag und Nacht in seinem Haushalt aufnehmen will (Pflegeperson), bedarf der Erlaubnis.

Art. 35 AGSG Versagungsgründe
[1]Die Pflegeerlaubnis nach § 44 Abs. 1 SGB VIII ist zu versagen, wenn das Wohl des Kindes oder des bzw. der Jugendlichen in der Pflegestelle nicht gewährleistet ist.
[2]Sie ist insbesondere zu versagen, wenn
6. eine Pflegeperson oder die in ihrem Haushalt lebenden Personen an einer Krankheit leiden, die das Wohl des Kindes oder des bzw. der Jugendlichen nicht nur unerheblich gefährdet,

Vor diesem Hintergrund dürfen Sozialdaten, die zur Prüfung der gesundheitlichen Tauglichkeit der in Betracht kommenden Pflegeperson erforderlich sind, erhoben werden.

Dabei ist aufgrund des datenschutzrechtlichen Grundsatzes der Direkterhebung grundsätzlich zunächst eine Selbstauskunft der oder des Betroffenen in Betracht zu ziehen. Um eine fachlich fundierte Einschätzung zum Gesundheitszustand vornehmen zu können, kann sich aber auch die Vorlage einer ärztlichen Bescheinigung als notwendig erweisen.

Aus einer solchen ärztlichen Bescheinigung sollte hervorgehen, ob die Bewerberin oder der Bewerber nicht an einer Krankheit leidet, die das Wohl des Kindes bzw. Jugendlichen nicht nur unerheblich gefährdet. Auch eine Konkretisierung, etwa danach, ob es sich um eine akut lebensbedrohliche bzw. lebensverkürzende Erkrankung, eine Suchterkrankung, eine psychiatrische oder eine ansteckende Erkrankung handelt, halte ich für vertretbar. Als zu weitgehend und daher nicht zulässig erachte ich indes das Verlangen nach Auskünften, die Aufschluss über den Unterfall einer Krankheit oder die Diagnose geben.

8.4.3.2 Datenerhebung im laufenden Kontaktverhältnis

Von der Datenerhebung vor Erteilung einer Pflegeerlaubnis zu unterscheiden ist die Datenerhebung im laufenden Kontaktverhältnis, d.h. nach Erteilung der Pflegeerlaubnis.

In diesem Zusammenhang möchte ich daran erinnern, dass Pflegepersonen verpflichtet sind, das zuständige Jugendamt hinsichtlich wichtiger Ereignisse zu **unterrichten**, die das Wohl des Kindes oder Jugendlichen betreffen (§ 37 Abs. 3 Satz 2 Sozialgesetzbuch Achtes Buch – Kinder- und Jugendhilfe – SGB VIII).

§ 37 SGB VIII Zusammenarbeit bei Hilfen außerhalb der eigenen Familie
(3) [2]Die Pflegeperson hat das Jugendamt über wichtige Ereignisse zu unterrichten, die das Wohl des Kindes oder des Jugendlichen betreffen.

Die Pflegepersonen müssen dem Jugendamt insbesondere das Auftreten ansteckender oder sonstiger Krankheiten, die das Wohl des Kindes oder Jugendlichen nicht nur unerheblich gefährden können, **unverzüglich mitteilen** (Art. 37 Abs. 1 Gesetz zur Ausführung der Sozialgesetze – AGSG).

Art. 37 AGSG Versagungsgründe
(1) Eine Pflegeperson, die der Erlaubnis nach § 44b Abs. 1 SGB VIII bedarf, ist insbesondere verpflichtet, dem für den gewöhnlichen Aufenthalt der Pflegeperson zuständigen Jugendamt jeden Wohnungswechsel sowie das Auftreten ansteckender oder sonstiger Krankheiten, die das Wohl des Kindes oder des bzw. der Jugendlichen nicht nur unerheblich gefährden können, unverzüglich mitzuteilen.

Werden Pflegepersonen daneben im laufenden Kontaktverhältnis **einmalig** aufgefordert, eine ärztliche Bescheinigung vorzulegen, so ist dies nach § 62 Abs. 1 SGB VIII nur zulässig, wenn Anhaltspunkte für eine **konkrete Gefährdung** des Kindes oder des Jugendlichen bestehen oder die Erhebung anderweitig **eingehend begründet** werden kann.

Eine **wiederholte** und in **regelmäßigen zeitlichen Abständen** erfolgende Einholung ärztlicher Bescheinigungen im Rahmen eines laufenden Kontaktverhältnisses, die nicht vor dem Hintergrund eines konkreten Verdachts einer Gefährdung des Kindes oder des Jugendlichen stattfindet, halte ich dagegen für **nicht zulässig**. Eine solche Kontrollpraxis würde einer **lückenlosen Dauerkontrolle** der Pflegeperson nahekommen.

Im Übrigen halte ich es sowohl in der Zeit vor als auch in der Zeit nach Erteilung der Pflegeerlaubnis für **unzulässig**, **obligatorische Drogentests** für Pflegepersonen ohne konkreten Anlass vorzusehen. Angesichts der aufgezeigten Möglichkeiten, auf ärztliche Bescheinigungen zurückzugreifen, dürfte ein solches Verlangen ebenso an der Erforderlichkeit **scheitern** wie das Begehren nach einer **Entbindung** der Ärzte der Pflegepersonen **von der Schweigepflicht** gegenüber dem Jugendamt.

8.4.4 Verbundverfahren im Rahmen der Jugendhilfe

Bereits in früheren Tätigkeitsberichten hatte ich die Problematik von „Verbundverfahren“ thematisiert (siehe hierzu 23. Tätigkeitsbericht 2008 Nrn. 3.14 und 14.1 bzw. 24. Tätigkeitsbericht 2010 Nr. 7.7). Im 25. Tätigkeitsbericht 2012 unter

Nr. 8.5 war ich konkret mit zwei Programmen im Bereich der Kindertageseinrichtungen bzw. der Jugendsozialarbeit an Schulen befasst. Dadurch sollten unterschiedliche Stellen verschiedene Informationen zu verschiedenen Zwecken (Dokumentation, Abwicklung des Bewilligungsverfahrens, Ermöglichung von Statistik bzw. Evaluation, Planung) erhalten. Im Berichtszeitraum konnte ich hier datenschutzrechtliche Verbesserungen erreichen:

Auf meine Anregung hin hat das Staatsministerium für Arbeit und Soziales, Familie und Integration inzwischen die Kindertageseinrichtungen darauf hingewiesen, dass keine personenbezogenen Daten bei der Eingabe in KiBiG.web zu erfassen sind. Ebenso sollen in der Vergangenheit verwendete personenbezogene Daten in KiBiG.web anonymisiert bzw. gelöscht werden.

Auch bei dem betroffenen Programm für den Bereich der Jugendsozialarbeit an Schulen konnte ich Verbesserungen erzielen: So wird dieses Programm nun ausschließlich bei dem betroffenen Rechenzentrum eingesetzt; Auftraggeber sind die jeweiligen Regierungen. Die mit der Jugendsozialarbeit an Schulen befassten freien Träger haben lediglich die Möglichkeit, sich in das Programm einzuloggen. Des Weiteren verständigte ich mich mit dem Staatsministerium grundsätzlich darüber, dass neben dem Musterrahmenvertrag zur Auftragsdatenverarbeitung mit dem Rechenzentrum auch ein spezifischer Vertrag notwendig ist. Allerdings entsprechen die bisherigen Vereinbarungen noch nicht den gesetzlichen Anforderungen. Außerdem wurde mir zugesichert, dass alle Daten, die sich im System befinden und über die endgültige Verfahrensbeschreibung hinausgehen, nach einer kurzen Übergangsphase gelöscht werden.

8.5 Betreuungsgeld

In den letzten Jahren war und ist das Betreuungsgeld ein politischer Zankapfel. Leider war die datenschutzrechtliche Situation im Berichtszeitraum nicht anders. Insbesondere die Kommunalen Spitzenverbände befürchteten neue datenschutzrechtliche Probleme beim Vollzug des Elterngelds (siehe zuletzt 23. Tätigkeitsbericht 2008 Nr. 17.2.1). Insbesondere klärungsbedürftig war die Frage der Kontrollmöglichkeiten, ob Eltern für ihr Kind tatsächlich keine geförderte Kinderbetreuung in Anspruch nehmen.

Die für den Vollzug des Betreuungsgelds zuständige Behörde hat mir gegenüber erklärt, es würden lediglich personenbezogene Daten bei den Berechtigten erhoben. Für die Inanspruchnahme solle lediglich das Erklärungsprinzip gelten und auf die Angaben der Berechtigten im Antrag abgestellt werden. Regelhafte oder stichprobenartige Kontrollen etwa seitens der Kommunen seien nicht angedacht. Diese Aussage habe ich erfreut zur Kenntnis genommen. Außerdem habe ich das zuständige Staatsministerium und die Vollzugsbehörde bereits ein Jahr vor Inkrafttreten des Betreuungsgelds gebeten, mir die Entwürfe der Antragsunterlagen, der datenschutzrechtlichen Freigabe sowie der Verfahrensbeschreibung zur Prüfung zu Verfügung zu stellen.

Leider war meine Freude nur kurz: Trotz verschiedener Erinnerungen musste ich kurz vor Inkrafttreten des Betreuungsgelds der Zeitung entnehmen, dass die Vollzugsbehörde die Unterlagen bereits ausgefüllt an alle betroffenen Eltern verschickt hatte, ohne dass ich diese Unterlagen prüfen konnte. Auch eine datenschutzrechtliche Freigabe sowie eine Verfahrensbeschreibung lagen noch nicht

vor. Aus diesem Grund habe ich nochmals eindringlich auf Art. 26, 30 und 32 BayDSG hingewiesen.

Art. 26 BayDSG Datenschutzrechtliche Freigabe automatisierter Verfahren
(1) Der erstmalige Einsatz von automatisierten Verfahren, mit denen personenbezogene Daten verarbeitet werden, bedarf der vorherigen schriftlichen Freigabe durch die das Verfahren einsetzende öffentliche Stelle … Für wesentliche Änderungen von Verfahren gelten die Sätze 1 … entsprechend …
(3) Öffentliche Stellen haben ihren behördlichen Datenschutzbeauftragten rechtzeitig vor dem Einsatz oder der wesentlichen Änderung eines automatisierten Verfahrens eine Verfahrensbeschreibung mit den … Angaben zur Verfügung zu stellen; zugleich ist eine allgemeine Beschreibung der Art der für das Verfahren eingesetzten Datenverarbeitungsanlagen und der technischen und organisatorischen Maßnahmen … beizugeben. Die behördlichen Datenschutzbeauftragten erteilen die datenschutzrechtliche Freigabe …

Art. 30 BayDSG Aufgaben
(1) Der Landesbeauftragte für den Datenschutz kontrolliert bei den öffentlichen Stellen die Einhaltung dieses Gesetzes und anderer Vorschriften über den Datenschutz …

Art. 32 BayDSG Unterstützung durch die öffentlichen Stellen
(1) Der Landesbeauftragte für den Datenschutz ist von allen öffentlichen Stellen in der Erfüllung seiner Aufgaben zu unterstützen. Ihm sind alle zur Erfüllung seiner Aufgaben notwendigen Auskünfte zu geben und auf Anforderung alle Unterlagen über die Erhebung, Verarbeitung oder Nutzung personenbezogener Daten zur Einsicht vorzulegen. Er hat ungehinderten Zutritt zu allen Diensträumen, in denen öffentliche Stellen Daten erheben, verarbeiten oder nutzen. …
(3) Die Staatskanzlei und die Staatsministerien unterrichten den Landesbeauftragten für den Datenschutz rechtzeitig über Entwürfe von Rechts- und Verwaltungsvorschriften des Freistaates Bayern sowie über Planungen bedeutender Automationsvorhaben, sofern sie die Erhebung, Verarbeitung oder Nutzung personenbezogener Daten betreffen. …

Bei diesen Vorschriften handelt es sich nicht um lästige Formalia. Vielmehr sollen sie die verantwortliche Stelle dazu anhalten, sich bereits im Vorfeld über datenschutzrechtliche Fragen Gedanken zu machen. Schließlich ist eine Änderung im laufenden Verfahren in der Regel nur mit sehr großem Aufwand möglich.

Aber auch in der Sache bestand datenschutzrechtlicher Optimierungsbedarf: So waren das zuständige Staatsministerium sowie die Vollzugsbehörde u.a. zunächst nicht bereit, meine Anmerkungen in meinem 25. Tätigkeitsbericht 2012 unter Nr. 8.9 (Personalausweiskopie) umzusetzen. Sicherlich ist es zutreffend, dass sich die dortigen Erläuterungen primär auf den deutschen Personalausweis beziehen. Grundsätzlich gelten sie aber auch bei Ausweispapieren anderer Länder. Selbst wenn man hier ausnahmsweise auf Grund erhöhter Missbrauchsmöglichkeiten eine Ausweiskopie zulässt, so muss der Betroffene nicht erforderliche Daten schwärzen können. Nach der Rechtsprechung muss die verantwortliche Behörde sogar auf diese Möglichkeit hinweisen. Nach einer neueren Entscheidung ist dann sogar die Speicherung dieser (geschwärzten) Ausweiskopie zulässig. Letztendlich konnte ich die zuständigen Behörden nach umfangreicher Korrespondenz mit meinen Hinweisen auf die Rechtsprechung überzeugen.

8.6 Datenabgleich in der Sozialverwaltung

Bereits im 18. Tätigkeitsbericht 1998 unter Nr. 4.4 habe ich mich mit dem Thema des Datenabgleichs in der Sozialverwaltung befasst. Bei einem **Datenabgleich** werden bestimmte Informationen zu einer Person, die Sozialleistungen beantragt hat oder erhält, mit anderen zu dieser Person vorliegenden Datenbeständen abgeglichen. Abgesehen von spezialgesetzlichen Ausnahmefällen kann er nur zur Aufgabenerfüllung mindestens der den Abgleich initiierenden Stelle und bei einem **konkreten Anlass zulässig** sein. Ein solcher Anlass kann sich beispielsweise daraus ergeben, dass der Leistungsträger die Angaben des Antragstellers auf ihre Richtigkeit und Vollständigkeit hin überprüft, etwa weil er konkrete Anhaltspunkte für unrichtige bzw. unvollständige Angaben hat. Dabei muss sich die Behörde immer vor Augen führen, dass (Sozial)Daten grundsätzlich beim Betroffenen zu erheben sind und deren Erhebung ohne seine Mitwirkung bei anderen Personen oder Stellen nur in Ausnahmefällen zulässig ist.

Ein Datenabgleich kann zudem in automatisierter Form als sogenanntes **automatisiertes Abrufverfahren** zugelassen werden. Hierfür muss die Einrichtung eines automatisierten Abrufverfahrens gesetzlich vorgesehen sein. Daneben muss auch der einzelne tatsächlich vorgenommene Abruf im jeweiligen Einzelfall den gesetzlichen Datenerhebungs- und Datenübermittlungsvorschriften entsprechen.

Die wesentlichen Vorhaben in diesem Berichtszeitraum stelle ich im Folgenden dar.

8.6.1 Datenabgleich im Bereich der Sozialhilfe

In meinem 25. Tätigkeitsbericht 2012 unter Nr. 8.7 hatte ich mich mit Formularen einer Sozialbehörde befasst. In einem dieser Formblätter wurden Antragstellerinnen und Antragsteller von Sozialhilfe darauf hingewiesen, dass das Sozialamt Einsicht in die Daten der Wohngeldempfängerdatei, Ausländerdatei, Kfz-Zulassungsdatei und der Einwohnermeldedatei nimmt. Zur Begründung führte die Sozialbehörde hierzu aus, sie wolle hierdurch die rechtswidrige Inanspruchnahme von Sozialhilfe verhindern. Aufgrund der zahlreichen Sozialhilfefälle sei die Einsichtnahme für die Aufgabenerfüllung der Leistungssachbearbeiter zwingend erforderlich.

Die von der Behörde vorgenommenen Datenabgleiche hielt ich in vielen Punkten für zu weitgehend. Nach ausgiebigem Schriftwechsel und nach einer gemeinsamen Besprechung konnte ich erreichen, dass die Sozialbehörde auf Datenabgleiche mit der **Wohngeldempfängerdatei** und der **Ausländerdatei** zukünftig verzichten wird. Die Einsichtnahme in die **Kfz-Zulassungsdatei** ist auf die Haltereigenschaft beschränkt worden. Die Suche des Halters über das Kennzeichen und die Abfrage der Anzahl der Kraftfahrzeuge sind daraufhin nicht mehr vorgenommen worden.

Soweit die Sozialbehörde auf Datenabgleiche verzichtet hat, habe ich darum gebeten, die bestehenden Zugriffsmöglichkeiten auch technisch zu beschränken bzw. zu unterbinden und die zugrundeliegenden Verfahrensbeschreibungen entsprechend zu ändern.

8.6.2 Automatisiertes Abrufverfahren DIWO (Dialogorientiertes Wohngeldverfahren) für ein Jobcenter

Vom Wohnungsamt einer Stadt wurde ich darüber unterrichtet, dass für einzelne Mitarbeiterinnen und Mitarbeitern des Jobcenters dieser Stadt ein automatisiertes Abrufverfahren auf DIWO eingerichtet wurde. Danach konnten die Beschäftigten des Jobcenters als datenabrufende Stelle nach Eingabe von Namen und/oder Geburtsdatum des betreffenden Hilfesuchenden ersehen, ob ein Wohngeldantrag gestellt oder zurzeit Wohngeld gewährt wurde. Nicht ersichtlich war, dass beispielsweise ein Wohngeldbezug laufend erfolgte, oder die Höhe des ausbezahlten Wohngeldes. Der Zugriff ermöglichte nur eine Auskunft über den tagesaktuellen Stand. Die Einrichtung des automatisierten Abrufverfahrens war von der zuständigen Aufsichtsbehörde genehmigt worden.

Da im Hinblick auf das die Daten abrufende Jobcenter der Bundesbeauftragten für den Datenschutz und die Informationsfreiheit die datenschutzrechtliche Kontrollkompetenz zusteht, habe ich sie hiervon unterrichtet. Nach mehrmaligem Schriftwechsel und einem vor Ort vorgenommenen Beratungs- und Kontrollbesuch durch die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit hat sich das betreffende Jobcenter bereit erklärt, die bestehende Möglichkeit zum Datenabgleich nicht mehr zu nutzen. Vom Wohnungsamt der Stadt wurde mir bestätigt, dass die bestehenden Zugriffsmöglichkeiten der Beschäftigten des Jobcenters gelöscht wurden und auch in technischer Hinsicht nicht mehr möglich sind.

8.6.3 Automatisierter bundesweiter Wohngelddatenabgleich

Um die rechtswidrige Inanspruchnahme von Wohngeld zu vermeiden, ist zum 01.01.2013 ein bundesweit einheitliches automatisiertes Datenabgleichverfahren beim Wohngeld durch eine Änderung des § 33 Wohngeldgesetz (WoGG) und der §§ 16 ff Wohngeldverordnung eingeführt worden.

Bei der Durchführung des automatisierten Datenabgleichs nimmt die Datenstelle des Trägers der Deutschen Rentenversicherung (Datenstelle) die Funktion einer Vermittlungsstelle wahr. Ihr werden entweder direkt von den Wohngeldbehörden oder mittelbar durch eine zu bestimmende zentrale Landesstelle die in § 33 Abs. 2 WoGG genannten erforderlichen Daten übermittelt. Diese übermittelten Daten gleicht die Datenstelle mit den bei ihr gespeicherten Daten ab bzw. übermittelt diese an das Bundeszentralamt für Steuern, die Deutsche Post AG und die Deutsche Rentenversicherung Knappschaft-Bahn-See zum dortigen Datenabgleich weiter. Die Ergebnisse der vorgenommenen Datenabgleiche werden auf dem gleichen Weg über die zentrale Landesstelle an die Wohngeldbehörden zurück übermittelt.

Die Aufgabe der zentralen Landesstelle wurde in Bayern durch eine Ergänzung der Verordnung über die Zuständigkeit zum Vollzug des Wohngeldgesetzes auf die Regierung von Unterfranken übertragen, die die abzugleichenden Daten sammelt, auf Vollständigkeit überprüft und an die Datenstelle übermittelt.

Aufgrund der klaren gesetzlichen Regelungen sowie des auf meine Anregung hin überarbeiteten IT-Konzepts der zentralen Landesstelle habe ich grundsätzlich keine Bedenken gegen die datenschutzrechtliche Zulässigkeit dieses Vorgehens.

9 Steuer- und Finanzverwaltung

9.1 Datenschutzrechte der Arbeitnehmer beim Abruf der elektronischen Lohnsteuerabzugsmerkmale (ELStAM)

Über den langen Weg zur **Ablösung der herkömmlichen (Papier-)Lohnsteuerkarte durch ein elektronisches Abrufverfahren** hatte ich in meinen Tätigkeitsberichten immer wieder ausführlich berichtet (siehe nur zuletzt im 25. Tätigkeitsbericht 2012 Nr. 9.1 und im 24. Tätigkeitsbericht 2010 Nr. 9.1.3). Gesetzliche Grundlage dieses umfangreichen E-Government-Projekts ist der bereits durch das Jahressteuergesetz 2008 in das Einkommensteuergesetz (EStG) eingefügte § 39e EStG „Verfahren zur Bildung und Anwendung der elektronischen Lohnsteuerabzugsmerkmale". Danach werden die zur Abführung der Lohnsteuer benötigten Daten der Arbeitnehmer für den automatisierten Abruf durch den Arbeitgeber in einer beim Bundeszentralamt für Steuern errichteten, bundesweit zentralen Datenbank bereitgestellt. Zu den **E**lektronischen **L**ohn**St**euer**A**bzugs**M**erkmalen (ELStAM) gehören insbesondere die Steuerklasse, die Zahl der Kinderfreibeträge, die Freibeträge und die Kirchensteuerabzugsmerkmale. **Seit Ende des Jahres 2013** ist – nach mehrfachen Verzögerungen – die **Nutzung des elektronischen Abrufs für alle Arbeitgeber nunmehr grundsätzlich verpflichtend** (vgl. § 52b Abs. 5 EStG).

Zum elektronischen Abruf der ELStAM benötigt der Arbeitgeber unter anderem die steuerliche Identifikationsnummer, das Geburtsdatum und die Angabe des Arbeitnehmers, ob es sich um das Haupt- oder um ein Nebenarbeitsverhältnis handelt (§ 39e Abs. 4 EStG). Aus Datenschutzsicht möchte ich dabei hervorheben, dass **nur der jeweilige Arbeitgeber zum Abruf der ELStAM seiner Arbeitnehmer berechtigt** ist; diese Berechtigung endet mit Beendigung des Arbeitsverhältnisses. Der vorsätzliche oder leichtfertige Abruf für andere Zwecke als für die Durchführung des Steuerabzugs – also etwa eine „Neugierabfrage" – stellt zudem eine bußgeldbewehrte Ordnungswidrigkeit dar (§ 39e Abs. 4 Satz 7 in Verbindung mit § 39 Abs. 8 und 9 EStG).

Eine ausdrückliche Zustimmung des Arbeitnehmers zu diesem automatisierten Abruf durch den Arbeitgeber ist gesetzlich nicht vorgesehen. Zur Überprüfung der Abrufberechtigung wird allerdings **jeder Abruf protokolliert**. Um zusätzliche Maßnahmen zum Schutz vor – systembedingt nie ganz auszuschließenden – unberechtigten Abrufen ergreifen zu können, stehen dem Arbeitnehmer zudem verschiedene Datenschutzrechte zu.

Nach meiner Einschätzung haben Arbeitnehmer jedoch oftmals (noch) keine genaue Kenntnis darüber, welche Maßnahmen sie selbst zum Schutz ihres Grundrechts auf informationelle Selbstbestimmung vor unberechtigten Steuerdatenabrufen ergreifen können. Mit ausführlichen Hinweisen zum **„Selbstdatenschutz bei der Lohnsteuer – Datenschutzrechte der Arbeitnehmer beim Abruf der elektronischen Lohnsteuerabzugsmerkmale (ELStAM)"** habe ich mich daher bereits am 08.11.2013 mit einer Pressemitteilung an die Öffentlichkeit gewandt. Diese Pressemitteilung steht selbstverständlich auch jetzt noch auf meiner Homepage https://www.datenschutz-bayern.de unter „Presse" – „Pressemitteilungen"

zum Abruf bereit; nähere Informationen sind in diesem Zusammenhang zudem unter „Themen“ – „Steuer- und Finanzverwaltung“ abrufbar.

Auch an dieser Stelle möchte ich noch einmal darauf aufmerksam machen, welche **Maßnahmen der Arbeitnehmer** selbst **zum Schutz seines Grundrechts auf informationelle Selbstbestimmung vor unberechtigten Steuerdatenabrufen** ergreifen kann:

- Der Arbeitnehmer kann **von seinem Finanzamt Auskunft über die zu seiner Person gespeicherten ELStAM sowie über die in den letzten 24 Monaten erfolgten Abrufe der Arbeitgeber verlangen** (§ 39e Abs. 6 Satz 4 EStG in Verbindung mit BMF-Schreiben vom 07.08.2013, BStBl I Seite 943, Rn. 81). Über das ElsterOnline-Portal https://www.elsteronline.de/eportal kann der Arbeitnehmer auch online seine ELStAM einsehen; dazu ist eine – kostenfreie – Registrierung notwendig.

Der Arbeitnehmer kann darüber hinaus nach § 39e Abs. 6 Satz 6 EStG **bei seinem Finanzamt**

- einen oder mehrere **Arbeitgeber benennen, die zum Abruf der ELStAM berechtigt sein sollen** (Positivliste),

- einen oder mehrere – beispielsweise ehemalige – **Arbeitgeber benennen, die zum Abruf der ELStAM nicht berechtigt sein sollen** (Negativliste, Teilsperrung),

- den **Abruf der ELStAM allgemein für alle Arbeitgeber sperren lassen** (Vollsperrung),

- nach einer Voll-/Teilsperrung den **Abruf der ELStAM wieder allgemein für alle Arbeitgeber freischalten lassen.**

Damit der Arbeitnehmer den Arbeitgeber für die Positivliste wie für die Negativliste benennen kann, hat der Arbeitgeber dem Arbeitnehmer seine Wirtschafts-Identifikationsnummer (vgl. § 139c Abgabenordnung) mitzuteilen.

Kann der Arbeitgeber wegen einer vom Arbeitnehmer veranlassten Sperrung keine ELStAM abrufen, hat er die Lohnsteuer allerdings nach der – meist ungünstigen – Steuerklasse VI zu ermitteln (§ 39e Abs. 6 Satz 8 EStG).

§ 39e EStG Verfahren zur Bildung und Anwendung der elektronischen Lohnsteuerabzugsmerkmale
(6) … [4]Die elektronischen Lohnsteuerabzugsmerkmale sind dem Steuerpflichtigen auf Antrag vom zuständigen Finanzamt mitzuteilen oder elektronisch bereitzustellen. [5]Wird dem Arbeitnehmer bekannt, dass die elektronischen Lohnsteuerabzugsmerkmale zu seinen Gunsten von den nach § 39 zu bildenden Lohnsteuerabzugsmerkmalen abweichen, ist er verpflichtet, dies dem Finanzamt unverzüglich mitzuteilen. [6]Der Steuerpflichtige kann beim zuständigen Finanzamt

1. den Arbeitgeber benennen, der zum Abruf von elektronischen Lohnsteuerabzugsmerkmalen berechtigt ist (Positivliste) oder nicht berechtigt ist (Negativliste). [2]Hierfür hat der Arbeitgeber dem Arbeitnehmer seine Wirtschafts-Identifikationsnummer mitzuteilen. [3]Für die Verwendung der Wirtschafts-Identifikationsnummer gelten die Schutzvorschriften des § 39 Absatz 8 und 9 sinngemäß; oder

2. die Bildung oder die Bereitstellung der elektronischen Lohnsteuerabzugsmerkmale allgemein sperren oder allgemein freischalten lassen.

[7]Macht der Steuerpflichtige von seinem Recht nach Satz 6 Gebrauch, hat er die Positivliste, die Negativliste, die allgemeine Sperrung oder die allgemeine Freischaltung in einem bereitgestellten elektronischen Verfahren oder nach amtlich vorgeschriebenem Vordruck dem Finanzamt zu übermitteln. [8]Werden wegen einer Sperrung nach Satz 6 einem Arbeitgeber, der Daten abrufen möchte, keine elektronischen Lohnsteuerabzugsmerkmale bereitgestellt, wird dem Arbeitgeber die Sperrung mitgeteilt und dieser hat die Lohnsteuer nach Steuerklasse VI zu ermitteln.

Der **amtliche Vordruck zur Beantragung der Auskunft, Sperrung oder Freischaltung der ELStAM** ist bei den Finanzämtern erhältlich; er steht darüber hinaus auf der Homepage des Landesamts für Steuern www.lfst.bayern.de unter „Formulare" – „Lohnsteuer/ELStAM" – „Arbeitnehmer" zum Abruf zur Verfügung.

9.2 Staatliche Mitwirkung bei der Erhebung der Kirchensteuer

Die Religionsfreiheit wird in Art. 107 Verfassung des Freistaates Bayern (BV) sowie in Art. 4 Abs. 1 und 2 Grundgesetz für die Bundesrepublik Deutschland (GG) gewährleistet. Dieses Grundrecht umfasst insbesondere das Recht, frei über die Zugehörigkeit zu einer Religions- oder Weltanschauungsgemeinschaft zu entscheiden (positive Religionsfreiheit), aber auch das Recht, einer solchen Gemeinschaft fernzubleiben oder aus ihr jederzeit auszuscheiden (negative Religionsfreiheit). Das **Grundrecht auf negative Religionsfreiheit enthält** überdies das **Recht, über Glaubens- und Bekenntnisfragen grundsätzlich die Auskunft zu verweigern.**

Art. 107 BV
(5) [1]Niemand ist verpflichtet, seine religiöse Überzeugung zu offenbaren. [2]Die Behörden haben nur soweit das Recht, nach der Zugehörigkeit zu einer Religionsgemeinschaft zu fragen, als davon Rechte und Pflichten abhängen oder eine gesetzlich angeordnete statistische Erhebung dies erfordert.

Vor diesem verfassungsrechtlichen Hintergrund bringen immer wieder **Bürgerinnen und Bürger datenschutzrechtliche Bedenken** gegen die staatliche Mitwirkung bei der Erhebung der Kirchensteuer bei mir vor. Insbesondere wenden sie sich mit ihren Eingaben **gegen die Erhebung von weltanschaulichen und religionsbezogenen Angaben durch staatliche und private Stellen im Rahmen des Kirchensteuerverfahrens**.

Aus datenschutzrechtlicher Sicht nehme ich zu diesem Problemkreis wie folgt Stellung:

Zunächst beschränkt sich meine datenschutzrechtliche Kontrollkompetenz auf die Einhaltung der datenschutzrechtlichen Vorschriften durch bayerische öffentliche Stellen (Art. 33a Abs. 2 BV, Art. 30 Abs. 1 BayDSG). Zu den bayerischen öffentlichen Stellen zählen aufgrund Art. 140 GG in Verbindung mit Art. 137 Weimarer Reichsverfassung (WRV) nicht die als öffentlich-rechtliche Religionsgesellschaften anerkannten Kirchen. Die in der Verfassung angelegte Trennung von Kirche und Staat hat zur Folge, dass die Kirche von Staatsaufsicht frei zu bleiben hat. Eine Kontrolle kirchlicher Datenverarbeitung durch staatliche Aufsichtsinstanzen wäre hiermit nicht vereinbar. Im Bereich der Kirchensteuer **unterfällt meiner**

Kontrollkompetenz somit nur das Handeln der bayerischen Finanzämter, nicht jedoch die Tätigkeit der bayerischen Kirchensteuerämter.

Das vom Bundesverfassungsgericht auf Grundlage von Art. 1 Abs. 1 in Verbindung mit Art. 2 Abs. 1 GG entwickelte Grundrecht auf informationelle Selbstbestimmung besagt, dass jeder Einzelne grundsätzlich selbst über die Preisgabe und Verwendung seiner personenbezogenen Daten zu bestimmen hat (so genanntes „Volkszählungsurteil" vom 15.12.1983, Az.: 1 BvR 209/83 u.a.). Allerdings hat das Bundesverfassungsgericht klargestellt, dass dieses Grundrecht nicht schrankenlos gewährleistet ist. Der Einzelne muss vielmehr Einschränkungen im überwiegenden Allgemeininteresse hinnehmen, wenn hierfür eine normenklare gesetzliche Rechtsgrundlage besteht und der Grundsatz der Verhältnismäßigkeit beachtet ist.

Bei Angaben zur Religionszugehörigkeit handelt es sich um besonders sensible Daten. Die Freiheit, religiöse Überzeugungen zu verschweigen, ist als sog. negative Religionsfreiheit verfassungsrechtlich geschützt (Art. 4 Abs. 1 und 2 GG sowie ausdrücklich Art. 107 Abs. 5 Satz 1 BV und Art. 140 GG in Verbindung mit Art. 136 Abs. 3 Satz 1 WRV). Behörden dürfen somit grundsätzlich nicht nach dem religiösen Bekenntnis fragen. Ein Fragerecht nach der Zugehörigkeit zu einer Religionsgesellschaft ist jedoch dann vorgesehen, wenn davon Rechte und Pflichten abhängen oder eine gesetzlich angeordnete statistische Erhebung dies erfordert (Art. 107 Abs. 5 Satz 2 BV; Art. 140 GG in Verbindung mit Art. 136 Abs. 3 Satz 2 WRV). Derartige Rechte und Pflichten können sich aus dem Recht der Steuererhebung ergeben, das den Religionsgesellschaften des öffentlichen Rechts verfassungsrechtlich eingeräumt ist (Art. 143 Abs. 3 BV; Art. 140 GG in Verbindung mit Art. 137 Abs. 6 WRV). Die hiermit gewährleistete Mitwirkung des Staates bei der Erhebung der Kirchensteuern bezieht sich nach der Rechtsprechung des Bundesverfassungsgerichts konkret darauf, dass der Staat den Religionsgesellschaften des öffentlichen Rechts das Besteuerungsrecht verleiht, die Erhebung gesetzlich regelt (siehe Art. 140 GG in Verbindung mit Art. 137 Abs. 6 WRV: „nach Maßgabe der landesrechtlichen Bestimmungen"), sich in dem durch diese Regelungen bestimmten Umfang an deren Vollzug beteiligt und dabei auch den Verwaltungszwang zur Verfügung stellt. Hierduch ist der Staat von Verfassungs wegen auch verpflichtet, in Rechtsetzung und Vollzug die Möglichkeit geordneter Verwaltung der Kirchensteuern sicherzustellen (siehe hierzu Bundesverfassungsgericht, Beschluss vom 08.02.1977, Az.: 1 BvR 329/71 u.a.). Soweit diese verfassungsrechtliche Verpflichtung es notwendig macht, kann sie somit zu einer Einschränkung der Glaubens- und Bekenntnisfreiheit führen (Bundesverfassungsgericht, Beschluss vom 08.02.1977, Az.: 1 BvR 329/71 u.a.). Diese Garantie einer geordneten Besteuerung rechtfertigt nach der – soweit ersichtlich – einhelligen verfassungsgerichtlichen Rechtsprechung auch die gesetzlich vorgesehene Erhebung der Mitgliedschaft zu einer Religionsgemeinschaft im Rahmen des Lohnsteuerverfahrens (vgl. nur Bundesverfassungsgericht, Beschluss vom 23.10.1978, Az.: 1 BvR 439/75; Bayerischer Verfassungsgerichtshof, Entscheidung vom 12.10.2010, Az.: Vf. 19-VII-09).

Art. 143 BV
(3) Kirchen und Religionsgemeinschaften sowie weltanschauliche Gemeinschaften, die Körperschaften des öffentlichen Rechts sind, dürfen auf Grund der öffentlichen Steuerlisten Steuern erheben.

In Anbetracht dieser gefestigten höchstrichterlichen Rechtsprechung kann ich – auch vor dem Hintergrund meiner in Art. 33a Abs. 2 BV, Art. 30 Abs. 1 BayDSG

eng umrissenen Aufgabenstellung – nicht von einer unverhältnismäßigen Einschränkung des Grundrechts auf informationelle Selbstbestimmung durch das bayerische Kirchenlohnsteuerverfahren ausgehen. In diesem Zusammenhang möchte ich auch darauf aufmerksam machen, dass der **Arbeitgeber die Lohnsteuerabzugsmerkmale nach der ausdrücklichen gesetzlichen Verwendungsbeschränkung** des Art. 13 Abs. 1 Satz 2 Kirchensteuergesetz in Verbindung mit § 39 Abs. 8 Satz 1 Einkommensteuergesetz (EStG) **nur für die Einbehaltung der (Kirchen-)Lohnsteuer verwenden darf.** Die Kirchenlohnsteuer ist im Übrigen in den anderen Ländern entsprechend geregelt.

§ 39 EStG Lohnsteuerabzugsmerkmale
(8) [1]Der Arbeitgeber darf die Lohnsteuerabzugsmerkmale nur für die Einbehaltung der Lohn- und Kirchensteuer verwenden. [2]Er darf sie ohne Zustimmung des Arbeitnehmers nur offenbaren, soweit dies gesetzlich zugelassen ist.

Im Hinblick auf die Entrichtung der Kirchenkapitalertragsteuer konnten die Datenschutzbeauftragten des Bundes und der Länder in langdauernden und intensiven Verhandlungen erreichen, dass es in Zukunft weiterhin möglich ist, eine Kenntnisnahme des jeweils betroffenen Kreditinstituts von der Religionszugehörigkeit des Steuerbürgers bzw. von der Nichtzugehörigkeit zu einer Religionsgemeinschaft zu vermeiden. So **können Steuerbürger**, die das Bekanntwerden ihrer Religionszugehörigkeit bei ihrer Bank nicht wünschen, **der elektronischen Übermittlung ihrer Religionszugehörigkeit durch das Bundeszentralamt für Steuern an ihre Bank widersprechen („Sperrvermerk").** Die Kirchenkapitalertragsteuer wird in diesem Fall im Wege einer Veranlagung auf Basis einer Steuererklärung – und damit ohne Kenntnis der ansonsten abzugsverpflichteten Bank – erhoben (siehe § 51a Abs. 2c Satz 1 Nr. 3 und Abs. 2e EStG). Im Einzelnen möchte ich insoweit auf meine Ausführungen im 25. Tätigkeitsbericht 2012 unter Nr. 9.4 verweisen.

Aus meiner Sicht ist damit das aus der Religionsfreiheit folgende **Recht, sich zu seiner religiösen Überzeugung grundsätzlich nicht äußern zu müssen,** im Lichte der verfassungsrechtlichen Regelungen **gewahrt.**

10 Schulen und Hochschulen

10.1 Datenschutz in der Schule – Erneute Änderungen der Durchführungsverordnung zu Art. 28 Abs. 2 BayDSG

Meinen langjährigen Forderungen entsprechend werden seit dem Schuljahr 2011/2012 an den staatlichen Schulen bzw. Schulämtern sukzessive behördliche Datenschutzbeauftragte bestellt (siehe hierzu ausführlich meinen 25. Tätigkeitsbericht 2012 Nr. 10.1). Unabhängig davon hält das Staatsministerium für Bildung und Kultus, Wissenschaft und Kunst zumindest vorerst an der „Verordnung zur Durchführung des Art. 28 Abs. 2 des Bayerischen Datenschutzgesetzes“ (im Folgenden: Durchführungsverordnung) fest. Die **Schulen sollen** damit auch **weiterhin automatisierte Verfahren in dem in den Anlagen 1 bis 11 der Durchführungsverordnung aufgeführten Umfang** (Verfahren der Lehrerdatei, der Schülerdatei, der Oberstufendatei, Stundenplanprogramm, Vertretungsplanprogramm, Notenverwaltungsprogramm, Buchausleiheprogramm, Videoaufzeichnung an Schulen, Internetauftritt von Schulen, Passwortgeschützte Lernplattform, Schulinterner passwortgeschützter Bereich) ohne weitere Voraussetzungen **einsetzen dürfen** (siehe hierzu ausführlich bereits meinen 23. Tätigkeitsbericht 2008 Nr. 12.2). Insbesondere müssen die Schulen für die genannten Verfahren kein gesondertes datenschutzrechtliches Freigabeverfahren durchführen.

Im Berichtszeitraum hat das Staatsministerium die Durchführungsverordnung sukzessive in einigen Punkten ergänzt und um eine zusätzliche Anlage erweitert. In die Verfahren zur **Änderung der Durchführungsverordnung** war ich jeweils eingebunden; dabei konnte ich **einige datenschutzrechtliche Verbesserungen** erreichen. Folgende Punkte erscheinen mir aus Datenschutzsicht von besonderer Relevanz:

10.1.1 Anlage 6 „Verfahren Notenverwaltungsprogramm“

Bei Schülernoten handelt es sich um sensible personenbezogene Daten, auf die Lehrkräfte nur in dem sachlichen und zeitlichen Umfang zugreifen dürfen, der für die Erfüllung ihrer jeweiligen Aufgabe tatsächlich erforderlich ist (siehe hierzu ausführlich bereits meinen 23. Tätigkeitsbericht 2008 Nr. 12.2.1). Im Rahmen dieser Erforderlichkeitsprüfung ist abzuwägen zwischen dem Informationsinteresse der Lehrkräfte einerseits und dem Persönlichkeitsrecht der Schülerinnen und Schüler andererseits. Die Schülerinnen und Schüler haben einen Anspruch darauf, nicht befürchten zu müssen, dass schlechte Zensuren einer Lehrkraft in einem Fach bei den übrigen Lehrkräften – wenn auch nur unbewusst – zu einem negativen Eindruck oder gar zu einer Voreingenommenheit führen. Somit muss das Informationsinteresse der Lehrkräfte zumindest teilweise hinter dem Persönlichkeitsrecht der Schülerinnen und Schüler zurücktreten. Aus datenschutzrechtlicher Sicht ist es daher **nicht zulässig, allen Lehrkräften jederzeit und anlasslos einen fächerübergreifenden Einblick in die Leistungsdaten ihrer Schülerinnen und Schüler einzuräumen.**

Aus diesen Gründen habe ich im Verordnungsänderungsverfahren darauf geachtet, dass ein fächerübergreifendes elektronisches Einsichtsrecht in Schülerleistungsdaten auch zukünftig **nur für bestimmte, abschließend aufgeführte Lehrkräfte in eng begrenzten Fällen und unter detailliert geregelten Voraussetzungen zugelassen** wird. Dabei habe ich mich der eingehend begründeten schulrechtlichen Einschätzung des fachlich federführenden Staatsministeriums für Bildung und Kultus, Wissenschaft und Kunst nicht verschlossen, dass für die Aufgabenerfüllung der **Schulleitungen** wie auch der **Beratungslehrkräfte und Schulpsychologen** ein auf eine bestimmte Schülerin oder einen bestimmten Schüler bezogenes, zeitlich beschränktes automatisiertes Zugriffsrecht auf Leistungsdaten im konkreten Einzelfall erforderlich sein kann. Ein anlassloses, zeitlich unbeschränktes, umfassendes elektronisches Einsichtsrecht in alle Einzelnoten aller Schülerinnen und Schüler ist dagegen zur Aufgabenerfüllung weder der Schulleitungen noch der Beratungslehrkräfte und Schulpsychologen notwendig und damit nach wie vor datenschutzrechtlich unzulässig.

Anlage 6 Verordnung zur Durchführung des Art. 28 Abs. 2 des Bayerischen Datenschutzgesetzes (DVBayDSG-KM) Verfahren Notenverwaltungsprogramm
6. Personengruppen, die innerhalb der speichernden Stelle automatisiert nutzen und verarbeiten:
Lehrkräfte der Schule jeweils nur hinsichtlich der Daten von Schülerinnen und Schülern, die die jeweilige Lehrkraft unterrichtet bzw. deren Klassleitung sie wahrnimmt.
Fächerübergreifenden Zugriff auf Leistungsdaten (Nr. 3.3) dürfen erhalten

- *die Schulleitung nur im konkreten Einzelfall, soweit dies zur Erfüllung ihrer pädagogischen, organisatorischen und rechtlichen Aufgaben erforderlich ist,*
- *Beratungslehrkräfte und Schulpsychologen nur im konkreten Einzelfall, soweit dies zur Erfüllung ihrer pädagogisch-psychologischen und rechtlichen Aufgaben im Rahmen der Schulberatung erforderlich ist,*
- *die Lehrkräfte für die jeweils von ihnen unterrichteten Schülerinnen und Schüler nur im konkreten Einzelfall, insbesondere für den Zeitraum, für den dies zur Erfüllung ihrer Aufgaben als Mitglied der Klassenkonferenz (insbesondere Zeugniserstellung, Entscheidung über das Vorrücken, Empfehlung an die Lehrerkonferenz im Fall des Vorrückens auf Probe) erforderlich ist,*
- *die Klassenleitungen darüber hinaus für die Schülerinnen und Schüler ihrer Klasse, um schulische oder häusliche Probleme erkennen zu können, die sich durch einen plötzlichen Leistungsabfall in mehreren Fächern gleichzeitig bemerkbar machen, sowie für die Zeugnisvorbereitung und -erstellung,*
- *die Lehrkräfte an Berufsschulen darüber hinaus wegen der dort bestehenden schulorganisatorischen und didaktischen Besonderheiten für die jeweils von ihnen unterrichteten Schülerinnen und Schüler während des gesamten Schuljahres;*

im Übrigen ist der Zugriff auf Leistungsdaten auf die von der jeweiligen Lehrkraft unterrichteten Fächer beschränkt; soweit Lehrkräfte insbesondere an Förderschulen gemeinsam ein Fach unterrichten, haben sie wechselseitigen Zugriff auf diese Leistungsdaten.

10.1.2 Anlage 10 „Passwortgeschützte Lernplattform“

Mit der wachsenden Verbreitung des sog. E-Learning – also des Lehrens und Lernens unter Einsatz elektronischer Medien – hat in den letzten Jahren auch an den öffentlichen Schulen die **Nutzung von elektronischen Lernplattformen stark**

zugenommen. Im Rahmen dieser Unterrichtsform werden den Schülerinnen und Schülern von der Lehrkraft in „virtuellen Klassenzimmern“ Arbeitsmaterialien zur Verfügung gestellt, welche dann in der Schule oder zu Hause bearbeitet werden können. Durch Lernplattformen können aber auch darüber hinaus vielfältige elektronische Kommunikationsmöglichkeiten unter den Nutzern eröffnet werden.

Datenschutzrechtlich sind derartige Lernplattformen nicht unproblematisch. Aufgrund der regelmäßig personalisierten Anmeldung und der regelmäßigen Protokollierung aller Nutzungsbewegungen besteht die Möglichkeit, detaillierte Verhaltensprofile der einzelnen Nutzer anzufertigen. Deswegen hat das Staatsministerium für Bildung und Kultus, Wissenschaft und Kunst in Abstimmung mit mir bereits im Jahre 2008 in Anlage 10 „Passwortgeschützte Lernplattform“ der Durchführungsverordnung detailliert festgelegt, welche rechtlichen Rahmenbedingungen für den Einsatz elektronischer Lernplattformen an öffentlichen Schulen gelten (siehe hierzu zuletzt ausführlich meinen 24. Tätigkeitsbericht 2010 Nr. 10.3).

Seither ist die technische Entwicklung jedoch weiter fortgeschritten. Zudem treibt die Staatsregierung die Förderung des IT-gestützten Unterrichts an bayerischen Schulen – insbesondere im Wege des umfangreichen E-Government-Projekts „Digitales Lernen Bayern“ – stark voran. In diesem Zusammenhang hat mir das Staatsministerium nachvollziehbar dargelegt, dass der bisherige Umfang der Anlage 10 der Durchführungsverordnung alle nunmehr pädagogisch notwendigen Funktionalitäten passwortgeschützter Lernplattformen nicht mehr abdeckt. Diese eingehend begründete Einschätzung des fachlich federführenden Staatsministeriums habe ich akzeptiert. Bei der erforderlichen Verordnungsänderung habe ich jedoch aus datenschutzrechtlicher Sicht insbesondere darauf geachtet, dass

- personenbezogene Daten von Schülerinnen, Schülern und Lehrkräften weiterhin grundsätzlich nur auf der Basis wirksamer Einwilligungen gespeichert werden dürfen,

- in virtuellen Kursräumen weiterhin nur mit den insoweit erforderlichen personenbezogenen Daten der Betroffenen – wozu im Rahmen von Audiobeiträgen auch die Stimme zählen kann – umgegangen werden darf,

- die Zugriffsrechte – gerade auch bei Schulkooperationen – dem datenschutzrechtlichen Erforderlichkeitsgrundsatz entsprechend restriktiv ausgestaltet wurden,

- die Löschungsfristen kurz gehalten wurden.

Flankierend dazu habe ich im Rahmen meiner parallelen Einbindung in die Weiterentwicklung der Bekanntmachung „Medienbildung. Medienerziehung und informationstechnische Bildung in der Schule“ darauf Wert gelegt, dass ein Einsatz passwortgeschützter Lernplattformen nur unter sehr engen Maßgaben – dezentral von der jeweiligen Schule vor Ort – zum verpflichtenden Bestandteil des Unterrichts erklärt werden kann (siehe Nr. 10.3 dieses Tätigkeitsberichts). Insbesondere darf hierbei der von Anlage 10 der Durchführungsverordnung gesteckte Rahmen zulässiger Datenumgänge nicht – auch nicht im Wege einer datenschutzrechtlichen Freigabe vor Ort – überschritten werden. Aus Datenschutzsicht sollte jedoch ein verpflichtender Einsatz passwortgeschützter Lernplattformen im Unterricht generell nur zurückhaltend erfolgen. Regelfall ist und bleibt

nach Anlage 10 der Durchführungsverordnung eine schulische Nutzung passwortgeschützter Lernplattformen **auf freiwilliger Basis**. Zur Einholung der danach erforderlichen Einwilligungen der Betroffenen – Lehrkräfte, volljährige Schülerinnen und Schüler, Erziehungsberechtigte bei minderjährigen Schülerinnen und Schülern, diese zusätzlich ab Vollendung des 14. Lebensjahres – hat das Staatsministerium den Schulen verbindliche Muster vorgegeben (siehe die Anlagen 5.1 und 5.2 der von der Homepage des Staatsministeriums www.km.bayern.de unter „Ministerium" – „Recht" – „Datenschutz" abrufbaren „Handreichung für Datenschutzbeauftragte an bayerischen staatlichen Schulen").

Schließlich möchte ich darauf hinweisen, dass die Schule – je nach Ausgestaltung der passwortgeschützten Lernplattform – insbesondere auch die ggf. einschlägigen **personalvertretungsrechtlichen Vorschriften (vor allem Art. 75a Abs. 1 Bayerisches Personalvertretungsgesetz) zu beachten** hat.

10.1.3 Anlage 11 „Schulinterner passwortgeschützter Bereich"

Des Weiteren wurde die Durchführungsverordnung im Berichtszeitraum um eine detaillierte Regelung des schulinternen passwortgeschützten Bereichs erweitert. Hiermit soll nicht zuletzt einem praktischen Bedürfnis der Schulen entsprochen werden.

Nach der Neuregelung sollen **schulinterne passwortgeschützte Bereiche** den Schulen in erster Linie die Möglichkeit eröffnen, **allen Schulangehörigen (Schulleitung, Lehrkräfte, Verwaltungspersonal, Erziehungsberechtigte, Schülerinnen und Schüler) schnell und ohne größeren Aufwand schulbezogene Informationen – beispielsweise auf der Schulhomepage – zur Verfügung zu stellen.** In der schulischen Praxis wird es sich dabei nach derzeitiger Einschätzung hauptsächlich um **Stundenpläne, Vertretungspläne, Sprechstunden(buchungs)listen und Elternbriefe** handeln.

Durch die Aufnahme der neuen Anlage 11 in die Durchführungsverordnung setzt die Einrichtung eines schulinternen passwortgeschützten Bereichs **keine gesonderte datenschutzrechtliche Freigabe vor Ort** mehr voraus; sie steht damit insbesondere auch allen staatlichen Schulen problemlos offen. Bislang kam die Einrichtung eines schulinternen passwortgeschützten Bereichs dagegen vor allem für kommunale Schulen in Betracht, da hier der behördliche Datenschutzbeauftragte der Kommune entsprechend tätig werden konnte (siehe hierzu ausführlich meinen 24. Tätigkeitsbericht 2010 Nr. 10.2.4).

Bei der nunmehr in Anlage 11 der Durchführungsverordnung erfolgten generellen Freigabe schulinterner passwortgeschützter Bereiche habe ich **aus datenschutzrechtlicher Sicht insbesondere darauf geachtet, dass**

- **personenbezogene Daten von Schülerinnen, Schülern und Erziehungsberechtigten** durchweg **nur auf der Basis wirksamer Einwilligungen gespeichert** werden dürfen,

- das **Einwilligungserfordernis** auch für die Speicherung **privater E-Mail-Adressen von Lehrkräften und Verwaltungspersonal** sowie für die Speicherung sonstiger personenbezogener Daten dieser Personenkreise gilt, deren Bekanntgabe an die übrigen Schulangehörigen nicht gemäß Art. 85 Bayerisches Gesetz über das Erziehungs- und Unterrichtswesen aus

dienstlichen Gründen zulässig ist.
Daran gemessen können beispielsweise **Stundenpläne, Vertretungspläne und Sprechstundenlisten** ohne gesonderte Einwilligungen der Lehrkräfte in einen schulinternen passwortgeschützten Bereich eingestellt werden, während es bei **Elternbriefen und sonstigen klassen- und fachbezogenen Informationen** auf den jeweiligen Inhalt ankommt. Hier kann beispielsweise ohne gesonderte Einwilligung mitgeteilt werden, dass der Unterricht einer Lehrkraft bis auf weiteres ausfällt; eine Einwilligung der Lehrkraft ist hingegen erforderlich, wenn darüber hinaus mitgeteilt werden soll, dass der Unterricht wegen Eintritts in den Mutterschutz, wegen Krankheit oder wegen Unfalls etc. ausfällt,

— die **Zugriffsrechte** nach dem datenschutzrechtlichen Erforderlichkeitsgrundsatz **restriktiv ausgestaltet** wurden,

— die **Löschungsfristen kurz gehalten** wurden.

Im Übrigen weise ich darauf hin, dass die Schule – je nach Ausgestaltung des schulinternen passwortgeschützten Bereichs – insbesondere auch die ggf. einschlägigen **personalvertretungsrechtlichen Vorschriften (vor allem Art. 75a Abs. 1 Bayerisches Personalvertretungsgesetz) zu beachten** hat.

10.2 Neufassung der „Erläuternden Hinweise“

Im Berichtszeitraum hat das Staatsministerium für Bildung und Kultus, Wissenschaft und Kunst seine Bekanntmachung vom 19.04.2001 über „Erläuternde Hinweise für die Schulen zum Vollzug des Bayerischen Datenschutzgesetzes“ (Az.: III/4-III/1-L 0572-1/38 570, KWMBl I Seite 112, geändert durch Bekanntmachung vom 10.10.2002, Az.: III/4-III/1-L 0572-1/101 407, KWMBl Seite 354) grundlegend überarbeitet und als **„Bekanntmachung über erläuternde Hinweise zum Vollzug der datenschutzrechtlichen Bestimmungen für die Schulen“** am 11.01.2013 (Az.: I.5-5 L 0572.2-1a.54 865, KWMBl Seite 27, berichtigt am 18.02.2013, KWMBl Seite 72) **vollständig neu erlassen** (im Folgenden: „Erläuternde Hinweise“).

Das Staatsministerium hat mich in dieses umfangreiche Normsetzungsverfahren von Beginn an eng eingebunden. Im Laufe einer mehrmonatigen und intensiven Diskussion habe ich dabei **aus Datenschutzsicht zahlreiche Verbesserungsvorschläge** eingebracht, denen das Staatsministerium erfreulicherweise **im Wesentlichen Rechnung getragen** hat. **Nicht** gefolgt ist das Staatsministerium **allerdings** meiner Anregung, sich mit dem Ziel einer größeren Anwenderfreundlichkeit und Adressatenorientierung von dem bisherigen, meiner Erfahrung nach nicht immer glücklichen Aufbau völlig zu lösen und – ähnlich wie bei der „Handreichung für Datenschutzbeauftragte an bayerischen staatlichen Schulen“ (siehe dazu meinen 25. Tätigkeitsbericht 2012 Nr. 10.1) – eine **primär themenbezogene Neustrukturierung** vorzunehmen. Auch meinen Vorschlag, die „Erläuternden Hinweise“ und die „Handreichung“ **zusammenzulegen**, um so fehleranfällige Doppelungen und die Schulen vor Ort möglicherweise verwirrende Formulierungsunterschiede schon im Ansatz zu vermeiden, hat das Staatsministerium leider nicht aufgegriffen.

Einige, für die tägliche schulische Praxis meines Erachtens **besonders wertvolle datenschutzrechtliche Hinweise und Hilfestellungen** möchte ich im Folgenden, orientiert am Aufbau der „Erläuternden Hinweise", besonders erwähnen:

– **Erläuterung wesentlicher datenschutzrechtlicher Begriffe**

  Als grundlegende Hilfestellung wird in Nr. 2 der „Erläuternden Hinweise" zunächst der Begriff der **personenbezogenen Daten** vor einem spezifisch schuldatenschutzrechtlichen Hintergrund näher erläutert. Sodann werden insbesondere die verschiedenen Formen von **Datenumgängen** (nämlich: Erhebung, Verarbeitung und Nutzung) sowie die unterschiedlichen rechtlichen Folgen von **Anonymisierung und Pseudonymisierung** im Einzelnen dargelegt.

– **Geltungsbereich des Bayerischen Datenschutzgesetzes**

  In Nr. 3 der „Erläuternden Hinweise" erfolgt zum einen die Klarstellung, dass **bereichsspezifische Regelungen** über den Schuldatenschutz mit materieller Rechtsnormqualität gegenüber dem Bayerischen Datenschutzgesetz **vorrangig** sind.

  Zum anderen findet sich hier der Hinweis, dass die Regelungen des bereichsspezifischen und des allgemeinen Datenschutzrechts **unabhängig von Speichermedium und Verarbeitungsart** gelten.

– **Zulässigkeit der Datenerhebung, -verarbeitung und -nutzung**

  Aus den umfangreichen Ausführungen unter Nr. 4 der „Erläuternden Hinweise" möchte ich folgende, meines Erachtens besonders bedeutsame Punkte herausgreifen:

  Unter „Allgemeines" wird zunächst dargestellt, dass auch im Schulbereich **Eingriffe in das Grundrecht auf informationelle Selbstbestimmung** gemäß Art. 1 Abs. 1 in Verbindung mit Art. 2 Abs. 1 Grundgesetz **nur auf einer rechtlichen Grundlage zulässig** sind. Die Erhebung, Verarbeitung und Nutzung personenbezogener Daten sind nur zulässig, wenn eine Rechtsvorschrift sie erlaubt oder anordnet oder der Betroffene wirksam – also insbesondere freiwillig, informiert und in der Regel schriftlich – eingewilligt hat (siehe die für das Verständnis des Datenschutzrechts grundlegende Bestimmung des Art. 15 BayDSG).

  Der für das Datenschutzrecht maßgebliche **Erforderlichkeitsgrundsatz** wird in Nr. 4.1 der „Erläuternden Hinweise" vor einem spezifisch schuldatenschutzrechtlichen Hintergrund anhand der Datenerhebung erläutert.

  Für die Schulen vor Ort wichtige Einzelfragen zur Zulässigkeit von Datenverarbeitungen und -nutzungen – etwa im Hinblick auf eine **Datenweitergabe an außerschulische Stellen**, die Herausgabe eines **Jahresberichts**, die schulische **Öffentlichkeitsarbeit** oder einen **schulinternen passwortgeschützten Bereich** – werden in Nr. 4.2 der „Erläuternden Hinweise" eingehend beantwortet.

Die bei der **Datenverarbeitung auf privaten Rechnern der Lehrkräfte** zu beachtenden Vorgaben werden in Nr. 4.3 der „Erläuternden Hinweise“ im Einzelnen dargelegt.

Praxisrelevante Hinweise zu **schulischen Auftragsdatenvereinbarungen** finden sich in Nr. 4.5 der „Erläuternden Hinweise“.
Antworten auf an Schulen häufig auftretende Datenschutzfragen hinsichtlich **Videoüberwachung, Erhebungen an Schulen, Evaluationen an Schulen** sowie **digitaler Whiteboards im Unterricht** werden schließlich in Nr. 4.6 der „Erläuternden Hinweise“ gegeben.

– Berichtigung, Löschung, Sperrung, Speicherungsdauer

Aufmerksam machen möchte ich hier insbesondere auf die detaillierten Ausführungen zur Speicherungsdauer in Nr. 5.3 der „Erläuternden Hinweise“.

– Datensicherung, Datengeheimnis, Verpflichtung der Bediensteten

In Nr. 6.1 der „Erläuternden Hinweise“ werden insbesondere die technischen und organisatorischen Maßnahmen im Einzelnen dargelegt, die von der Schule zum Schutz der gespeicherten personenbezogenen (Schüler- und Lehrer-)Daten vor Verlust und Missbrauch zu treffen sind.

– Anspruch auf Auskunft

Nr. 7 der „Erläuternden Hinweise“ enthält sowohl Ausführungen zum allgemeinen **datenschutzrechtlichen** Auskunftsanspruch als auch zu den speziellen **schulrechtlichen** Auskunftsansprüchen der Schülerinnen und Schüler und ihrer Erziehungsberechtigten sowie zu den **beamtenrechtlichen Auskunftsansprüchen** des Schulpersonals.

– Institutionen des Datenschutzes

In Nr. 8 der „Erläuternden Hinweise“ wird zunächst erläutert, welche Institutionen im Einzelnen zur Sicherstellung des Datenschutzes an den Schulen berufen sind; sodann wird auch die Kontrollaufgabe des Landesbeauftragten für den Datenschutz erklärt.

Schließlich legt das Staatsministerium die **Reihenfolge** fest, in welcher Datenschutzfragen von den Schulen an die Beratungsstellen herangetragen werden sollen.

– Freigabe eines automatisierten Verfahrens / Verfahrensverzeichnis

Nähere Ausführungen zur datenschutzrechtlichen Freigabe und zum Verfahrensverzeichnis finden sich in Nrn. 9 und 10 der „Erläuternden Hinweise“.

– Wichtige Datenschutzbestimmungen für Schulen

Wichtige Datenschutzbestimmungen für Schulen werden schließlich in Nr. 11 der „Erläuternden Hinweise“ im Einzelnen aufgeführt.

– Anlagenverzeichnis: Musterformulare

  Das Anlagenverzeichnis der „Erläuternden Hinweise“ umfasst nunmehr die in Abstimmung mit mir für alle Gruppen von Schulangehörigen entwickelten vier Musterformulare für die Einholung der Einwilligung in die **Veröffentlichung von personenbezogenen Daten (einschließlich Fotos) durch Schulen**. In diesem Zusammenhang möchte ich auch auf meine Ausführungen im 25. Tätigkeitsbericht 2012 unter Nr. 10.3 hinweisen.

  Grundlegende datenschutzrechtliche Erläuterungen zur praxisbedeutsamen Problematik der Erstellung und Verwendung von Schülerfotos finden sich überdies in Nr. 10.4 dieses Tätigkeitsberichts.

Auch wenn die „Erläuternden Hinweise“ rechtliche Bindungswirkung nur für die dem Staatsministerium unmittelbar nachgeordneten bayerischen staatlichen Schulen entfalten, rufe ich alle **bayerischen kommunalen Schulen** dazu auf, **entsprechend diesen** – mit mir abgestimmten – **Hinweisen zu verfahren.**

In diesem Zusammenhang möchte ich darauf aufmerksam machen, dass die „Erläuternden Hinweise“ auch von meiner Homepage https://www.datenschutz-bayern.de unter „Recht & Normen“ – „Schul- und Hochschulrecht“ abrufbar sind.

10.3 Medienbildung, insbesondere Einsatz von passwortgeschützten Lernplattformen im Unterricht

Die **pädagogische Zielrichtung der schulischen Medienbildung** hat das Staatsministerium für Bildung und Kultus, Wissenschaft und Kunst bereits in der Bekanntmachung „Medienbildung. Medienerziehung und informationstechnische Bildung in der Schule“ vom 15.10.2009 (Az.: III.4 - 5 S 1356-5.625) fest verankert. Danach soll die Medienbildung die Schülerinnen und Schüler dazu befähigen, Medien zu privaten und beruflichen Zwecken verantwortungsvoll und effizient einzusetzen, sich insbesondere **sicher und kompetent in den virtuellen Kommunikations- und Sozialräumen zu bewegen und mit den persönlichen Daten verantwortungsbewusst umzugehen.** Dieses Ziel begrüße ich aus Datenschutzsicht ausdrücklich.

Seit 2009 ist der technische Fortschritt jedoch nicht stehen geblieben. Im schulischen Bereich haben vor allem die Entwicklung und Verwendung von **E-Learning-Angeboten – also das Lehren und Lernen unter Einsatz elektronischer Medien – in den vergangenen Jahren stetig zugenommen**. Dadurch wurden auch neue und schwierige Datenschutzfragen aufgeworfen. Im Vordergrund stehen hier **insbesondere die sog. Lernplattformen**. Bei diesen **„virtuellen Klassenzimmern“** besteht technisch die Möglichkeit, detaillierte Verhaltensprofile der einzelnen Nutzer – Schülerinnen und Schüler wie auch Lehrkräfte – zu erstellen: Die Nutzer müssen sich regelmäßig personalisiert anmelden, alle Nutzungsbewegungen können protokolliert werden und zudem oftmals auch von anderen Nutzern eingesehen werden (siehe dazu zuletzt meine Ausführungen im 24. Tätigkeitsbericht 2010 Nr. 10.3).

Dem durch die schulische Verwendung von elektronischen Lernplattformen ausgelösten datenschutzrechtlichen Regelungsbedarf hat das Staatsministerium erstmals durch Erlass der **Anlage 10 „Passwortgeschützte Lernplattform“ der Verordnung zur Durchführung des Art. 28 Abs. 2 des BayDSG** (im Folgenden:

Durchführungsverordnung) im Jahr 2008 Rechnung getragen (siehe dazu meinen 23. Tätigkeitsbericht 2008 Nr. 12.2.4). Im Berichtszeitraum hat das Staatsministerium die Anlage 10 der Durchführungsverordnung sodann den neueren technischen und pädagogischen Entwicklungen entsprechend **aktualisiert** (siehe Nr. 10.1.2 dieses Tätigkeitsberichts).

Im Hinblick auf den zunehmenden Einsatz elektronischer Medien im Unterricht hat das Staatsministerium darüber hinaus die eingangs erwähnte **Bekanntmachung „Medienbildung. Medienerziehung und informationstechnische Bildung in der Schule“** (im Folgenden: Bekanntmachung) unter meiner Einbindung weiterentwickelt und am 24.10.2012 (Az.: III.4-5 S 1356-3.18 725) **neu erlassen**.

Zum Schutz der Persönlichkeitsrechte der Schülerinnen und Schüler ebenso wie der Lehrkräfte ist es mir hierbei im Wege einer eingehenden und intensiven Diskussion mit dem Staatsministerium insbesondere gelungen, in der Bekanntmachung festzulegen, dass ein **Einsatz passwortgeschützter Lernplattformen nur unter sehr engen Maßgaben** – dezentral von der jeweiligen Schule vor Ort – zum **verpflichtenden Bestandteil des Unterrichts** erklärt werden kann. Im Einzelnen stellt Nr. 4.3 Abs. 3 der Bekanntmachung hierfür nunmehr folgende, von der jeweiligen Schule kumulativ zu erfüllende Voraussetzungen auf:

– Zunächst muss ein entsprechender **Beschluss der Lehrerkonferenz** in Abstimmung mit den maßgeblichen Schulgremien (insbesondere dem Schulforum) sowie dem Schulaufwandsträger vorliegen.

– Sodann muss sichergestellt sein, dass betroffenen **Schülerinnen und Schülern ohne häuslichen Internetanschluss kein Nachteil** erwächst. Dies kann beispielsweise dadurch erreicht werden, dass alternative Zugangsmöglichkeiten in der Schule auch außerhalb des Unterrichts zur Verfügung gestellt werden.

– Schließlich darf der **von Anlage 10 „Passwortgeschützte Lernplattform“ der Durchführungsverordnung gesteckte Rahmen nicht überschritten** werden. Insbesondere muss der Kreis der in den Nrn. 3.2.1, 3.2.2, 3.3.1 und 3.3.2 der Anlage 10 der Durchführungsverordnung abschließend aufgezählten Lehrer- und Schülerdaten eingehalten werden.

  Damit ist es den **Schulen** auch **untersagt**, die von der Anlage 10 der Durchführungsverordnung gezogenen **Grenzen im Wege einer datenschutzrechtlichen Freigabe vor Ort zu überschreiten.**

Unabhängig davon möchte ich ausdrücklich betonen, dass aus Datenschutzsicht von der durch die Bekanntmachung eröffneten Möglichkeit des **verpflichtenden Einsatzes** passwortgeschützter Lernplattformen im Unterricht **generell nur zurückhaltend Gebrauch gemacht werden** sollte. Als **Regelfall** sieht die Anlage 10 der Durchführungsverordnung **weiterhin** – unverändert – die **schulische Nutzung passwortgeschützter Lernplattformen auf freiwilliger Basis** vor (vgl. auch Nr. 4.3 Abs. 2 der Bekanntmachung). Zur Einholung der danach erforderlichen Einwilligungen der Betroffenen – Lehrkräfte, volljährige Schülerinnen und Schüler, Erziehungsberechtigte bei minderjährigen Schülerinnen und Schülern, diese zusätzlich ab Vollendung des 14. Lebensjahres – hat das Staatsministerium den Schulen verbindliche Muster vorgegeben (siehe die Anlagen 5.1 und 5.2 der

von der Homepage des Staatsministeriums www.km.bayern.de unter „Ministerium“ – „Recht“ – „Datenschutz“ abrufbaren „Handreichung für Datenschutzbeauftragte an bayerischen staatlichen Schulen“).

Schließlich mache ich darauf aufmerksam, dass das Staatsministerium den Schulen in Nr. 4.1 der Bekanntmachung den **Einsatz sozialer Netzwerke im Unterricht** mit Blick auf die besondere Schutzbedürftigkeit der Schülerinnen und Schüler **ausdrücklich untersagt** hat. Diese Vorgabe ist aus datenschutzrechtlicher Sicht zu begrüßen.

Auch wenn die Bekanntmachung „Medienbildung. Medienerziehung und informationstechnische Bildung in der Schule“ rechtliche Bindungswirkung nur für die dem Staatsministerium unmittelbar nachgeordneten bayerischen staatlichen Schulen entfaltet, rufe ich daher alle **bayerischen kommunalen Schulen** dazu auf, **entsprechend dieser** – mit mir abgestimmten – **Vorschrift zu verfahren.**

10.4 Erstellung und Verwendung von Schülerfotos

Im Berichtszeitraum konnte ich zwar erfreulicherweise feststellen, dass die bayerischen öffentlichen – staatlichen wie kommunalen – Schulen zunehmend ein stärkeres Bewusstsein für die datenschutzrechtliche Problematik von Schülerfotos entwickeln. Eine große Anzahl von schriftlichen und telefonischen Eingaben und Anfragen hat mir aber gezeigt, dass hier bei allen Gruppen von Schulangehörigen – von Schulleitungen, Lehrkräften und Verwaltungspersonal bis hin zu Erziehungsberechtigten sowie Schülerinnen und Schülern – immer noch große Unsicherheiten bestehen.

Aus diesem Grund möchte ich zu dem – im Zeitalter der digitalen Fotografie auch in der Schule allgegenwärtigen – Problemkreis der Erstellung und Verwendung von Schülerfotos aus Datenschutzsicht folgende Hinweise geben:

10.4.1 Allgemeines

Fotoaufnahmen stellen **personenbezogene Daten** im Sinne von Art. 4 Abs. 1 BayDSG dar. Nach Art. 15 Abs. 1 BayDSG sind die Erhebung, Verarbeitung und Nutzung personenbezogener Daten nur zulässig, wenn eine Rechtsvorschrift sie erlaubt oder anordnet (Nr. 1) oder der Betroffene eingewilligt hat (Nr. 2).

Eine gesetzliche Verpflichtung der Schülerinnen und Schüler, sich in der Schule fotografieren zu lassen, besteht nicht. Dies gilt unabhängig davon, ob die Aufnahmen von einem Schulangehörigen – etwa aus den Reihen des Lehr- und Verwaltungspersonals oder der Schüler- und Elternschaft – oder gar von einem externen Fotografen angefertigt werden. Auch kommt es nicht darauf an, ob die Schülerinnen und Schüler eigens für die Aufnahmen zusammenkommen oder ob die Fotografien im Rahmen des Unterrichts oder im Zusammenhang mit Schulprojekten angefertigt werden. Vielmehr existiert im Sinne von Art. 15 Abs. 1 Nr. 1 BayDSG **keine Rechtsgrundlage**, aus der sich die Befugnis **zur fotografischen Aufnahme von Schülerinnen und Schülern** – etwa in Form von Einzelaufnahmen, aber auch im Rahmen eines Gruppen- oder Klassenfotos – ableiten ließe. So sind die Schulen nach der schuldatenschutzrechtlichen Erlaubnisnorm des Art. 85 Abs. 1 Satz 1 Bayerisches Gesetz über das Erziehungs- und Unterrichtswesen zwar berechtigt, die Daten zu erheben, zu verarbeiten und zu nutzen, die zur Erfüllung der ihnen

durch Rechtsvorschriften zugewiesenen Aufgaben erforderlich sind. Dies bedeutet aber, dass die Datenerhebung, -verarbeitung und -nutzung nicht nur die Aufgabenerfüllung der Schule objektiv unterstützen, fördern und beschleunigen muss, sondern auch zu den schutzwürdigen Interessen der Betroffenen in einem angemessenen Verhältnis stehen muss. Bei Fotografien fehlt es an dieser Angemessenheit. Das Anfertigen und Verwenden von Fotografien stellt einen besonders schwerwiegenden Eingriff in das in Art. 1 Abs. 1 in Verbindung mit Art. 2 Abs. 1 Grundgesetz (GG) gewährleistete „Recht am eigenen Bild" dar, das als Ausprägung des Allgemeinen Persönlichkeitsrechts nicht nur in §§ 22 ff. Kunsturheberrechtsgesetz einfachgesetzlich, sondern auch als Grundrecht verfassungsrechtlich besonders geschützt ist. Ein Grundrechtseingriff liegt dabei schon dann vor, wenn die Fotos nur für schulinterne Zwecke angefertigt und verwendet werden.

Ohne eine ausdrückliche gesetzliche Ermächtigung ist die Anfertigung und Verwendung von Fotografien **nur mit datenschutzkonformer Einwilligung der Betroffenen** im Sinne des Art. 15 Abs. 1 Nr. 2 BayDSG zulässig. Bei minderjährigen Schülerinnen und Schülern müssen dabei die Erziehungsberechtigten einwilligen, ab Vollendung des 14. Lebensjahres zusätzlich auch die Minderjährigen selbst. Nach den gesetzlichen Vorgaben des Art. 15 Abs. 2 bis 4 und 7 BayDSG muss die Einwilligung insbesondere freiwillig, informiert und grundsätzlich **schriftlich** erteilt werden. An der **Freiwilligkeit** fehlt es beispielsweise, wenn die Betroffenen einem starken Gruppendruck ausgesetzt sind. Im Rahmen der **vollständigen Aufklärung** müssen die Betroffenen insbesondere darüber informiert werden, zu welchem konkreten Zweck die Fotos gemacht werden, in welcher Form und wie lange die Fotos gespeichert werden, wer darauf Zugriff hat und an wen sie unter Umständen weitergegeben werden. Die Betroffenen müssen somit eine konkrete Vorstellung über Ziel, Inhalt, Ablauf und Umfang der Datenerhebung und -verwendung erhalten können. Auch müssen die Betroffenen darauf hingewiesen werden, dass die Einwilligung ohne Angabe von Gründen und **ohne nachteilige Folgen verweigert sowie jederzeit widerrufen** werden kann.

Vor diesem rechtlichen Hintergrund ist es **nicht ausreichend**, wenn die Schule – beispielsweise auf der Schulhomepage, in Elternbriefen und/oder per Aushang – nur auf eine Fotoaktion hinweist, selbst wenn hierbei die Möglichkeit zum **Widerspruch** eingeräumt wird.

10.4.2 Beauftragung externer Fotografen

Mit der Anfertigung von Schülerfotos kann die Schule selbstverständlich einen privaten Dienstleister, insbesondere einen externen Fotografen, beauftragen. In diesem Falle sind allerdings die **gesetzlichen Vorgaben des Art. 6 BayDSG über die Auftragsdatenverarbeitung** zu beachten. Für die Einhaltung der datenschutzrechtlichen Vorschriften bleibt danach der Auftraggeber, also die Schule, verantwortlich. Der Auftragnehmer ist unter besonderer Berücksichtigung der Eignung der von ihm getroffenen technischen und organisatorischen Maßnahmen sorgfältig auszuwählen. Der Auftrag ist schriftlich zu erteilen, wobei Datenerhebung, -verarbeitung oder -nutzung, die technischen und organisatorischen Maßnahmen und etwaige Unterauftragsverhältnisse festzulegen sind. Der Auftragnehmer darf die Daten zudem nicht für andere Zwecke verwenden. Weitere Hinweise enthält in diesem Zusammenhang die jedenfalls für die bayerischen staatlichen Schulen verbindliche Bestimmung der Nr. 4.5 Buchst. a) der vom Staatsministerium für Bildung und Kultus, Wissenschaft und Kunst am 11.01.2013 erlassenen

„Bekanntmachung über erläuternde Hinweise zum Vollzug der datenschutzrechtlichen Bestimmungen für die Schulen“ (KWMBl Seite 27, berichtigt KWMBl Seite 72 – im Folgenden: „Erläuternde Hinweise“). Ein Mustervertrag zur Auftragsdatenverarbeitung ist zudem von meiner Homepage https://www.datenschutz-bayern.de unter „Themen“ – „Allgemeines“ abrufbar.

Rechtsgrundlage für die Anfertigung der Schülerfotos durch den von der Schule beauftragten privaten Dienstleister ist stets die von den Betroffenen gegenüber der Schule erteilte **datenschutzkonforme Einwilligung** gemäß Art. 15 Abs. 1 Nr. 2, Abs. 2 bis 4 und 7 BayDSG. Auch ist die Weitergabe von personenbezogenen Daten der Schülerinnen und Schüler – wie etwa Namen, Geburtsdatum und Klasse – an den beauftragten Fotografen zur Ermöglichung der Zuordnung der Aufnahmen nur mit entsprechender datenschutzkonformer Einwilligung der Betroffenen zulässig. Werden Klassenlisten an den Fotografen übergeben, ist darauf zu achten, dass nur die Daten der Schülerinnen und Schüler enthalten sind, für die eine schriftliche Einwilligung vorliegt. Sollen allen Mitschüler(elter)n die Fotoaufnahmen – etwa auf Datenträgern wie CDs oder USB-Sticks – zur Verfügung gestellt werden, ist auch hierfür eine entsprechende datenschutzkonforme Einwilligung notwendig. Zu den Anforderungen an eine datenschutzkonforme Einwilligung verweise ich im Einzelnen auf meine Ausführungen unter Nr. 10.4.1.

10.4.3 Schülerfotos im Jahresbericht, insbesondere Klassenfotos

Gibt eine Schule für die Schülerinnen und Schüler und Erziehungsberechtigten einen papiergebundenen Jahresbericht heraus, so dürfen – nicht müssen – darin gemäß der schuldatenschutzrechtlichen Erlaubnisnorm des Art. 85 Abs. 3 Bayerisches Gesetz über das Erziehungs- und Unterrichtswesen von den Schülerinnen und Schülern Name, Geburtsdatum, Jahrgangsstufe und Klasse sowie Angaben über besondere schulische Tätigkeiten und Funktionen enthalten sein. Sollen darüber hinaus Schülerfotos, insbesondere Klassenfotos in den Jahresbericht aufgenommen werden, so ist dies **nur auf der Grundlage einer datenschutzkonformen Einwilligung** gemäß Art. 15 Abs. 1 Nr. 2, Abs. 2 bis 4 und 7 BayDSG zulässig; zu den diesbezüglichen Anforderungen verweise ich im Einzelnen auf die Ausführungen unter Nr. 10.4.1.

Die jedenfalls für die bayerischen staatlichen Schulen verbindliche Bestimmung der Nr. 4.2 Buchst. d) der vom Staatsministerium für Bildung und Kultus, Wissenschaft und Kunst erlassenen „Erläuternden Hinweise“ verweist in diesem Zusammenhang ausdrücklich auf die mit mir abgestimmten **Muster-Einwilligungserklärungen**. Diese sind den „Erläuternden Hinweisen“ als Anlage beigefügt, aber auch auf meiner Homepage https://www.datenschutz-bayern.de unter „Themen“ – „Schulen“ abrufbar. Diesbezüglich möchte ich zudem auf meine Ausführungen im 25. Tätigkeitsbericht 2012 unter Nr. 10.3 hinweisen.

10.4.4 Schülerfotos auf der Schulhomepage

Im Rahmen der schulischen Öffentlichkeitsarbeit verzichtet kaum noch eine Schule darauf, eine Schulhomepage zu betreiben. Nach Anlage 9 „Internetauftritt von Schulen“ der Verordnung des Staatsministeriums für Bildung und Kultus, Wissenschaft und Kunst zur Durchführung des Art. 28 Abs. 2 des Bayerischen Datenschutzgesetzes dürfen personenbezogene Daten von Schülerinnen und Schülern – und damit auch Schülerfotos mit oder ohne Namensangabe – allerdings **nur auf**

der Grundlage einer datenschutzkonformen Einwilligung der Betroffenen gemäß Art. 15 Abs. 1 Nr. 2, Abs. 2 bis 4 und 7 BayDSG im Internet veröffentlicht werden; zu den diesbezüglichen Anforderungen verweise ich im Einzelnen auf meine Ausführungen unter Nr. 10.4.1.

Die jedenfalls für die bayerischen staatlichen Schulen verbindliche Bestimmung der Nr. 4.2 Buchst. e) der vom Staatsministerium erlassenen „Erläuternden Hinweise" verweist in diesem Zusammenhang ausdrücklich auf die mit mir abgestimmten **Muster-Einwilligungserklärungen**. Diese sind den „Erläuternden Hinweisen" als Anlage beigefügt, aber auch auf meiner Homepage https://www.datenschutz-bayern.de unter „Themen" – „Schulen" abrufbar. Auch diesbezüglich möchte ich auf meine eingehenden Ausführungen im 25. Tätigkeitsbericht 2012 unter Nr. 10.3 hinweisen.

10.4.5 Schülerfotos in Schülerausweisen

Um Schülerinnen und Schülern einen – oftmals zu Preisermäßigungen und anderen Vorteilen verhelfenden – Nachweis der Schülereigenschaft sowie des Alters zu ermöglichen, stellen Schulen ab der Jahrgangsstufe 5 auf Antrag Schülerausweise aus. Nach der jedenfalls für die bayerischen staatlichen Schulen verbindlichen, vom Staatsministerium für Bildung und Kultus, Wissenschaft und Kunst am 27.08.1996 erlassenen **Bekanntmachung „Ausstellung von Schülerausweisen"** (KWMBl I Seite 339) hat der Schülerausweis unter anderem ein Lichtbild zum Inhalt.

Bedient sich die Schule bei der Ausstellung der Schülerausweise eines privaten Dienstleisters, beispielsweise eines externen Fotografen, sind nach der genannten Bekanntmachung die **gesetzlichen Vorgaben des Art. 6 BayDSG über die Auftragsdatenverarbeitung** zu beachten. Für die Einhaltung der datenschutzrechtlichen Vorschriften bleibt damit der Auftraggeber, also die Schule, verantwortlich. Der Auftragnehmer ist unter besonderer Berücksichtigung der Eignung der getroffenen technischen und organisatorischen Maßnahmen sorgfältig auszuwählen. Der Auftrag ist schriftlich zu erteilen, wobei Datenerhebung, -verarbeitung oder -nutzung, die technischen und organisatorischen Maßnahmen und etwaige Unterauftragsverhältnisse festzulegen sind. Der Auftragnehmer darf die Daten zudem nicht für andere Zwecke verwenden. Weitere Hinweise enthalten in diesem Zusammenhang die jedenfalls für die bayerischen staatlichen Schulen verbindlichen Bestimmungen der Nr. 4.5 Buchst. a) und b) der vom Staatsministerium erlassenen „Erläuternden Hinweise". Ein Mustervertrag zur Auftragsdatenverarbeitung ist überdies von meiner Homepage https://www.datenschutz-bayern.de unter „Themen" – „Allgemeines" abrufbar.

Selbstverständlich sind die Schülerinnen und Schüler nicht dazu verpflichtet, die Ausstellung eines Schülerausweises zu beantragen. Im Ergebnis ist daher auch die hierzu notwendige Anfertigung und Verwendung von Schülerfotos **nur auf der Grundlage einer datenschutzkonformen Einwilligung** der Betroffenen gemäß Art. 15 Abs. 1 Nr. 2, Abs. 2 bis 4 und 7 BayDSG zulässig; zu den diesbezüglichen Anforderungen verweise ich im Einzelnen auf meine Ausführungen unter Nr. 10.4.1.

10.4.6 Schülerfotos im Schulunterricht

Teilweise wollen Lehrkräfte im Schulunterricht – etwa im Rahmen von Kunst- oder Sport-Projekten – Schülerfotos anfertigen und verwenden. Unabhängig von der – von mir nicht zu beurteilenden – Frage der pädagogischen Notwendigkeit kann ein solches Vorhaben schuldatenschutzrechtlich **allenfalls auf der Grundlage einer datenschutzkonformen Einwilligung** aller Betroffenen im Sinne des Art. 15 Abs. 1 Nr. 2, Abs. 2 bis 4 und 7 BayDSG zulässig sein (siehe dazu im Einzelnen oben unter Nr. 10.4.1).

Allerdings habe ich bereits erhebliche **Zweifel** daran, **ob im Unterrichtsverhältnis** überhaupt die für eine rechtlich tragfähige Einwilligung **notwendige Freiwilligkeit** gegeben sein kann. Vor diesem Hintergrund rate ich mit Blick auf das verfassungsrechtlich in Art. 1 Abs. 1 in Verbindung mit Art. 2 Abs. 1 Grundgesetz besonders geschützte „Recht am eigenen Bild" der Schülerinnen und Schüler von derartigen Unterrichtsvorhaben – und damit auch von der Einholung entsprechender Einwilligungen – grundsätzlich ab.

10.4.7 Schülerfotos für Fotositzpläne

Gerade zu Schuljahresbeginn stehen Lehrkräfte vor der Herausforderung, sich die Gesichter und Namen oftmals zahlreicher neuer Schülerinnen und Schüler einprägen zu müssen. Ein unkonventioneller Weg hierzu ist es, Einzelfotos von allen Schülerinnen und Schülern anzufertigen, nach dem „Sitzort" in der Klasse zusammenzustellen und mit den Schülernamen zu versehen (sog. „Fotositzpläne").

In Übereinstimmung mit dem Staatsministerium für Bildung und Kultus, Wissenschaft und Kunst stehe ich solchen „Fotositzplänen" **grundsätzlich ablehnend** gegenüber. Der damit verfolgte Hauptzweck – die Ermöglichung eines schnelleren Kennenlernens der Schülerinnen und Schüler – kann regelmäßig auch mit anderen Mitteln erreicht werden, die weniger stark in das verfassungsrechtlich in Art. 1 Abs. 1 in Verbindung mit Art. 2 Abs. 1 Grundgesetz garantierte „Recht am eigenen Bild" der Schülerinnen und Schüler eingreifen. In der Praxis bewährt hat sich dabei insbesondere das Aufstellen von Namensschildern vor den Schülerinnen und Schülern.

Allenfalls **im Bereich der beruflichen Schulen**, insbesondere der Berufsschulen mit dem dortigen Teilzeit- und Blockunterricht, möchte ich die Erstellung von „Fotositzplänen" – allerdings **nur auf der Grundlage datenschutzkonformer Einwilligungen** der Betroffenen gemäß Art. 15 Abs. 1 Nr. 2, Abs. 2 bis 4 und 7 BayDSG – nicht generell ausschließen. Hier sieht die Lehrkraft ihre Schülerinnen und Schüler teilweise nur in sehr großen Zeitabständen, während die Klassenstärken hoch sind. Zu den rechtlichen Anforderungen an eine datenschutzkonforme Einwilligung verweise ich im Einzelnen auf meine Ausführungen unter Nr. 10.4.1.

10.5 Datenerhebung bei Erkrankung von Schülerinnen und Schülern

Immer wieder wenden sich Schulleitungen, Lehrkräfte und Erziehungsberechtigte ebenso wie Schülerinnen und Schüler mit der Frage an mich, ob eine bayerische öffentliche Schule bei einer Erkrankung einer Schülerin oder eines Schülers die **Angabe der Art der Erkrankung** – also die Nennung der Krankheitsbezeichnung

oder der medizinischen Diagnose – verlangen darf. Bei der Beantwortung dieser Frage ist **wie folgt zu unterscheiden:**

10.5.1 Grundsatz: Keine Angabe der Art der Erkrankung

Die **Schulordnungen für die bayerischen öffentlichen Schulen** enthalten dazu im Wesentlichen gleichlautende Regelungen: Danach ist die Schule, wenn eine Schülerin oder ein Schüler aus zwingenden Gründen verhindert ist, am Unterricht oder an einer sonstigen verbindlichen Schulveranstaltung teilzunehmen, unverzüglich unter Angabe des Grundes schriftlich zu verständigen. Nur beispielhaft möchte ich hier den unten abgedruckten § 30 Abs. 1 Grundschulordnung (GrSO) nennen, u.a. aber auch auf § 39 Abs. 1 Mittelschulordnung, § 39 Abs. 1 Realschulordnung, § 37 Abs. 1 Gymnasialschulordnung, § 32 Abs. 1 Berufsschulordnung und § 36 Abs. 1 Wirtschaftsschulordnung hinweisen.

§ 30 GrSO Teilnahme
(1) [1]Ist eine Schülerin oder ein Schüler aus zwingenden Gründen verhindert, am Unterricht oder an einer sonstigen verbindlichen Schulveranstaltung teilzunehmen, so ist die Schule unverzüglich unter Angabe des Grundes zu verständigen. [2]Im Fall fernmündlicher Verständigung ist die schriftliche Mitteilung innerhalb von zwei Tagen nachzureichen.

Übereinstimmend fordern alle diese Schulordnungsbestimmungen lediglich die **Angabe des Verhinderungsgrundes.** Ein Grund für die Verhinderung, am Unterricht oder an einer sonstigen verbindlichen Schulveranstaltung teilzunehmen, kann beispielsweise eine Erkrankung sein. Im Falle einer Erkrankung muss der Schule somit **nur** der Grund der Verhinderung – also der **Umstand der Erkrankung** – mitgeteilt werden; die Angabe der Art der Erkrankung wird dagegen von den Schulordnungen nicht verlangt.

Auf Grundlage der Schulordnungen sind die bayerischen öffentlichen Schulen daher **nicht** berechtigt, die Angabe der **Art der Erkrankung** zu fordern. Auch in ärztlichen Attesten, deren Vorlage die Schule nach den Schulordnungen unter bestimmten Voraussetzungen – insbesondere bei Erkrankung von mehr als zwei oder drei Unterrichtstagen – verlangen kann, muss die Art der Erkrankung nicht angegeben werden.

Unabhängig davon kann in Einzelfällen eine **freiwillige Mitteilung** über die Art der Erkrankung an die Schule nützlich sein und die Fürsorge der Schule erleichtern. Diese Entscheidung bleibt aber den erkrankten Schülerinnen und Schülern bzw. ihren Erziehungsberechtigten vorbehalten.

10.5.2 Ausnahme: Meldepflichtige Erkrankungen

Um übertragbaren Krankheiten beim Menschen vorzubeugen, Infektionen frühzeitig zu erkennen und ihre Weiterverbreitung zu verhindern, hat der Bundesgesetzgeber in bestimmten Krankheitsfällen **gesetzliche Mitteilungspflichten nach dem Infektionsschutzgesetz** (IfSG) begründet. Diese Pflichten greifen jedoch nur bei den in § 34 Abs. 1 bis 3 IfSG abschließend aufgezählten, **meldepflichtigen Erkrankungen**; dazu gehören u.a. Keuchhusten, Masern, Scharlach und Windpocken.

Sind Schülerinnen oder Schüler von einer solchen Krankheit betroffen, haben sie bzw. ihre Sorgeberechtigten gemäß § 34 Abs. 5 Satz 1 IfSG die Schule unverzüglich hierüber zu informieren. Nach § 34 Abs. 6 Satz 1 IfSG hat die Schulleitung sodann unverzüglich das zuständige Gesundheitsamt zu benachrichtigen und krankheits- und personenbezogene Angaben zu machen. In diesem Zusammenhang darf ich beispielhaft auf meinen Beitrag im 24. Tätigkeitsbericht 2010 unter Nr. 10.5 hinweisen, in dem ich mich eingehend zum Umfang der Meldepflicht bei der Neuen Grippe (sog. „Schweine-Grippe“) geäußert habe.

Eine **generelle Pflicht,** der Schule in jedem Fall über die Art der Erkrankung Auskunft zu geben, begründet das Infektionsschutzgesetz damit gerade **nicht.**

§ 34 IfSG Gesundheitliche Anforderungen, Mitwirkungspflichten, Aufgaben des Gesundheitsamtes.
(5) [1]Wenn einer der in den Absätzen 1, 2 oder 3 genannten Tatbestände bei den in Absatz 1 genannten Personen auftritt, so haben diese Personen oder in den Fällen des Absatzes 4 der Sorgeinhaber der Gemeinschaftseinrichtung hiervon unverzüglich Mitteilung zu machen. [2]Die Leitung der Gemeinschaftseinrichtung hat jede Person, die in der Gemeinschaftseinrichtung neu betreut wird, oder deren Sorgeberechtigte über die Pflichten nach Satz 1 zu belehren.
(6) [1]Werden Tatsachen bekannt, die das Vorliegen einer der in den Absätzen 1, 2 oder 3 aufgeführten Tatbestände annehmen lassen, so hat die Leitung der Gemeinschaftseinrichtung das zuständige Gesundheitsamt unverzüglich zu benachrichtigen und krankheits- und personenbezogene Angaben zu machen. [2]Dies gilt auch beim Auftreten von zwei oder mehr gleichartigen, schwerwiegenden Erkrankungen, wenn als deren Ursache Krankheitserreger anzunehmen sind. [3]Eine Benachrichtigungspflicht besteht nicht, wenn der Leitung ein Nachweis darüber vorliegt, dass die Meldung des Sachverhalts durch eine andere in § 8 genannte Person bereits erfolgt ist.

10.6 Fahrtkostenerstattung im Rahmen der Schulwegkostenfreiheit

Nach Art. 3 Abs. 2 Satz 1 Gesetz über die Kostenfreiheit des Schulwegs (Schulwegkostenfreiheitsgesetz – SchKfrG) **erstattet der Aufgabenträger den Schülerinnen und Schülern bestimmter Schularten** bei Vorliegen der gesetzlichen Voraussetzungen **die Kosten der notwendigen Beförderung auf dem Schulweg.** Aufgabenträger ist gemäß Art. 1 Abs. 1 Satz 1 SchKfrG die kreisfreie Gemeinde oder der Landkreis des gewöhnlichen Aufenthalts der Schülerin oder des Schülers. Die Kostenerstattung erfolgt gemäß Art. 3 Abs. 2 Satz 8 Halbsatz 1 SchKfrG „auf Antrag gegen Vorlage insbesondere der entsprechenden Fahrausweise“.

§ 3 SchKfrG Kostenregelung
(2) [1]Für Schülerinnen und Schüler an öffentlichen und staatlich anerkannten privaten Gymnasien, Berufsfachschulen (ohne Berufsfachschulen in Teilzeitform) und Wirtschaftsschulen ab Jahrgangsstufe 11, für Schülerinnen und Schüler an öffentlichen und staatlich anerkannten privaten Fachoberschulen und Berufsoberschulen sowie für Schülerinnen und Schüler im Teilzeitunterricht an öffentlichen und staatlich anerkannten privaten Berufsschulen erstattet der Aufgabenträger die Kosten der notwendigen Beförderung (Art. 2 Abs. 1), soweit die nachgewiesenen vom Unterhaltsleistenden aufgewendeten Gesamtkosten der Beförderung eine Familienbelastungsgrenze von 370,- € je Schuljahr übersteigen. … [8]Die Kostenerstattung erfolgt auf Antrag gegen Vorlage insbesondere der entsprechenden

Fahrausweise; der Antrag ist bis spätestens 31. Oktober für das vorangegangene Schuljahr zu stellen.

Im Berichtszeitraum habe ich aus dem Bereich der von dieser Regelung betroffenen bayerischen öffentlichen Schulen erfahren, dass die Aufgabenträger als **Voraussetzung** für die Kostenerstattung in ihren Antragsformularen regelmäßig eine **Bestätigung der Schule über den Unterrichtsbesuch** der Antragstellerin oder des Antragstellers verlangen. Die Anforderungen variieren dabei von Aufgabenträger zu Aufgabenträger. So verlangt ein Großteil der Aufgabenträger eine bloße Bestätigung der Anzahl der Tage, an denen die Schule von der Schülerin oder von dem Schüler tatsächlich besucht wurde. Allerdings fordern einige Aufgabenträger von den Schulen darüber hinaus auch eine genaue Aufzählung der Fehl- bzw. Krankheitstage der Schülerin oder des Schülers mit exakter Datumsnennung.

Eine ausdrückliche Rechtsgrundlage für die Vorlage der von den Aufgabenträgern geforderten Bestätigungen der Schule findet sich im Schulwegkostenfreiheitsgesetz jedoch nicht.

Die Aufgabenträger sind zwar – nicht zuletzt auf Grund des Verweises in Art. 3 Abs. 2 Satz 1 SchKfrG auf Art. 2 Abs. 1 (Satz 3) SchKfrG – an die Grundsätze der Wirtschaftlichkeit gebunden. Sie haben daher ein berechtigtes Interesse daran zu prüfen, ob die von den Schülerinnen und Schülern zur Erstattung vorgelegten Fahrausweise tatsächlich zum Zweck des Schulbesuchs verwendet wurden. **Aus Datenschutzsicht** ist es für die Überprüfung aber **ausreichend, wenn** die **Schule** die **Anzahl der Tage bestätigt**, an denen die Schülerin oder der Schüler den Unterricht besucht hat, und gegebenenfalls darüber hinaus zusätzliche Angaben zum Unterrichtsturnus macht; bei Blockunterricht ist hier beispielsweise eine Benennung der Unterrichtszeiträume denkbar, bei regelmäßigem Unterricht eine Benennung der jeweiligen Unterrichtswochentage (beispielsweise montags in geraden Kalenderwochen). Die teilweise zusätzlich geforderte **datumsgenaue Aufzählung von Fehl- und sogar Krankheitstagen** erscheint dagegen im Hinblick auf das Grundrecht der Schülerinnen und Schüler auf informationelle Selbstbestimmung gemäß Art. 1 Abs. 1 in Verbindung mit Art. 2 Abs. 1 Grundgesetz **unverhältnismäßig**. Daraus könnten nämlich **Rückschlüsse auf** den **Gesundheitszustand**, aber auch auf die **Leistungsfähigkeit und Leistungsbereitschaft** der Schülerin oder des Schülers gezogen werden. Gerade aus diesem Grund wird etwa auf eine Ausweisung von Fehltagen in den Abschlusszeugnissen der bayerischen öffentlichen Schulen bewusst verzichtet. Für die ausdrückliche Ausweisung von Krankheitstagen ist ein sachlicher Grund ohnehin – auch mit Blick auf die besondere Schutzvorschrift des Art. 15 Abs. 7 BayDSG – nicht erkennbar.

Vor diesem Hintergrund habe ich das Staatsministerium für Bildung und Kultus, Wissenschaft und Kunst gebeten zu prüfen, wie ein bayernweit einheitlicher und **datenschutzgerechter Vollzug der Fahrtkostenerstattung** im Rahmen der Schülerbeförderung erreicht werden könnte. Dabei habe ich auch darauf hingewiesen, dass durch eine datenschutzkonforme pauschalierende Lösung der Verwaltungsaufwand bei den Aufgabenträgern, aber auch bei den Schulen deutlich verringert werden könnte.

In seiner Antwort hat mir das **Staatsministerium** mitgeteilt, dass der Staat hinsichtlich der Schülerbeförderung – einer Aufgabe der Kommunen im eigenen Wirkungskreis – **nur** die **Mindeststandards** vorgebe. Da über die Vorschrift des Art. 3 Abs. 2 Satz 8 SchKfrG hinaus keine weiteren staatlichen Vorgaben für die Gestaltung der Anträge auf Fahrtkostenerstattung bestünden, liege es im Ermessen der

Aufgabenträger, in welchem Maße sie in den Antragsformularen von den jeweiligen Schulen Nachweise über die Anwesenheit der Schülerinnen und Schüler anforderten. Diese Handlungsspielräume der Kommunen wolle das Staatsministerium nicht einschränken.

Immerhin hat das Staatsministerium aber die **Aufgabenträger der Schülerbeförderung** mit KMS vom 23.01.2014 (Az.: II.3-5 S 4365-7b.4 083) **um Beachtung meiner Ausführungen zu den Fehl- und Krankheitstagen** sowie insgesamt um **Überprüfung gebeten**, ob die in den jeweiligen Antragsformularen **konkret geforderten Angaben** der Schulen **aus Wirtschaftlichkeitsgründen tatsächlich benötigt** werden.

Auch ich möchte die Aufgabenträger der Schülerbeförderung an dieser Stelle dazu auffordern, **bei der Gestaltung der Antragsformulare** für die Fahrtkostenerstattung die aufgezeigten **datenschutzrechtlichen Anforderungen zu beachten**.

10.7 Informationsaustausch über Schülerinnen und Schüler zwischen Schule und Mittagsbetreuung

Viele Erziehungsberechtigte stehen heutzutage vor dem Problem, Kindererziehung und Berufstätigkeit in Einklang bringen zu müssen. Eine wertvolle Hilfe bei der Lösung dieses Problems ist die **Mittagsbetreuung**, die vor allem an immer mehr Grund- und Förderschulen in Bayern nach Maßgabe des Art. 31 Abs. 3 Bayerisches Gesetz über das Erziehungs- und Unterrichtswesen (BayEUG) angeboten wird. Die Mittagsbetreuung bietet den Erziehungsberechtigten in Zusammenarbeit mit der Schule eine **verlässliche Betreuung der Schülerinnen und Schüler für die Zeiten, die über das Unterrichtsende hinausgehen.**

Art. 31 BayEUG Mittagsbetreuung
(3) [1]Mittagsbetreuung wird bei Bedarf auf Antrag des jeweiligen Trägers an der Grundschule, in geeigneten Fällen auch an anderen Schularten nach Maßgabe der im Staatshaushalt ausgebrachten Mittel im Zusammenwirken mit den Kommunen und den Erziehungsberechtigten angeboten. [2]Diese bietet den Erziehungsberechtigten in Zusammenarbeit mit der Schule eine verlässliche Betreuung für die Zeiten, die über das Unterrichtsende hinausgehen. [3]Die Mittagsbetreuung untersteht der Schulaufsicht. [4]Für die Untersagung von Errichtung und Betrieb einer Mittagsbetreuung gilt Art. 110 entsprechend.

Die näheren Einzelheiten hat das Staatsministerium für Bildung und Kultus, Wissenschaft und Kunst in der **Bekanntmachung „Mittagsbetreuung und verlängerte Mittagsbetreuung an Grund- und Förderschulen“** vom 07.05.2012 (Az.: III.5-5 S 7369.1-4b.13 566) geregelt. Diese Bekanntmachung ist im Internet von der Homepage des Staatsministeriums unter www.km.bayern.de/lehrer/unterricht-und-schulleben/mittagsbetreuung.html abrufbar.

Im Berichtszeitraum wurde die Frage an mich herangetragen, ob und inwieweit ein **Informationsaustausch über Schülerinnen und Schüler** zwischen einer staatlichen Grundschule und dem kommunalen Träger der Mittagsbetreuung stattfinden darf.

In diesem Zusammenhang ist zu beachten, dass die **Mittagsbetreuung** – auch wenn sie im Regelfall in den Räumen der Schule stattfindet – **keine schulische,**

sondern eine eigenständige Einrichtung des jeweiligen Trägers ist. Träger der Mittagsbetreuung kann dabei entweder der **Schulaufwandsträger** (z.B. eine Kommune) oder ein **privatrechtlicher Träger** (z.B. ein Verein) sein. Der Träger ist auch Dienstherr bzw. Arbeitgeber des Personals der Mittagsbetreuung. In datenschutzrechtlicher Hinsicht stehen sich somit das Mittagsbetreuungspersonal und das schulische Lehrpersonal als Dritte im Sinne des Art. 4 Abs. 10 BayDSG gegenüber.

Der Austausch von Schülerdaten zwischen einer staatlichen Grundschule und dem kommunalen Träger der Mittagsbetreuung stellt in beiderlei Richtung eine **Datenübermittlung** an Dritte dar. Eine solche Datenübermittlung ist nach Art. 15 Abs. 1 BayDSG nur zulässig, wenn eine Rechtsvorschrift sie erlaubt oder anordnet (Nr. 1) oder der Betroffene eingewilligt hat (Nr. 2). Eine spezielle gesetzliche Erlaubnis für den Informationsaustausch über Schülerinnen und Schüler zwischen Schule und Mittagsbetreuung enthält allerdings weder das als Spezialvorschrift gemäß Art. 2 Abs. 7 BayDSG grundsätzlich vorrangige Bayerische Gesetz über das Erziehungs- und Unterrichtswesen noch das Bayerische Datenschutzgesetz.

Somit bedarf es nach Art. 15 Abs. 1 Nr. 2 BayDSG für die Rechtmäßigkeit des Informationsaustausches einer **ausdrücklichen Einwilligung der Erziehungsberechtigten** der betroffenen Schülerinnen und Schüler, bei Minderjährigen ab Vollendung des 14. Lebensjahres zusätzlich auch einer ausdrücklichen Einwilligung der Minderjährigen selbst. Die gesetzlichen Anforderungen an eine wirksame Einwilligung sind in Art. 15 Abs. 2 bis 4 und 7 BayDSG im Einzelnen geregelt. Eine datenschutzkonforme Einwilligung muss danach insbesondere **freiwillig, informiert und schriftlich** erfolgen sowie **jederzeit widerruflich** sein.

Aus diesen Gründen sieht auch die **Handreichung des Staatsinstituts für Schulqualität und Bildungsforschung (ISB) „Mittagsbetreuung an bayerischen Grundschulen“** ein entsprechendes Einwilligungserfordernis vor. Diese Broschüre ist im Internet von der Homepage des ISB unter www.isb.bayern.de/schulartspezifisches/materialien/mittagsbetreuung-an-bayerischen-grundschulen/ abrufbar.

Die Handreichung enthält unter anderem in den Anlagen 5 und 6 Musterformulare für die Anmeldung zur Mittagsbetreuung. Hier ist die Einwilligungserklärung der Erziehungsberechtigten allerdings **ausdrücklich auf den Informationsaustausch** zwischen Mittagsbetreuungspersonal und Lehrkräften **bezüglich der Hausaufgaben begrenzt.**

Um einen möglichst sparsamen Umgang mit den personenbezogenen Daten der betroffenen Schülerinnen und Schüler zu gewährleisten, empfehle ich grundsätzlich, die Einwilligungserklärungen nicht auf den Austausch zusätzlicher Informationen zu erweitern. Nur so kann annähernd eine Gleichbehandlung mit den Schülerinnen und Schülern gewährleistet werden, die Betreuungsangebote außerhalb der Schule – wie etwa Horte oder Kindertagesstätten – in Anspruch nehmen.

10.8 Übermittlung von Schülerdaten durch Berufsschulen an Ausbildungsbetriebe

Als eine der herausragenden Stärken unseres Bildungssystems wird immer wieder die **duale Berufsausbildung** hervorgehoben, die durch eine Kombination von

theoretischer Ausbildung an der Berufsschule und praktischer Ausbildung im Ausbildungsbetrieb gekennzeichnet ist. Die duale Berufsausbildung ist nicht zuletzt wegen der **engen Zusammenarbeit von Berufsschule und Ausbildungsbetrieb** so erfolgreich.

Doch genau diese Zusammenarbeit wirft immer wieder **datenschutzrechtliche Problemstellungen** auf. Insbesondere zu der Frage, ob und inwieweit eine öffentliche Berufsschule Schülerdaten an den jeweiligen Ausbildungsbetrieb übermitteln darf, erreichen mich regelmäßig Eingaben und Anfragen. Zu dieser Problematik nehme ich wie folgt Stellung:

10.8.1 Übermittlung von Einzelnoten, Notenübersichten oder Zeugnissen

Einzelnoten, Notenübersichten und Zeugnisse stellen personenbezogene Daten der Berufsschülerinnen und Berufsschüler im Sinne des Art. 4 Abs. 1 BayDSG dar. Bei der Übermittlung dieser Daten durch die Berufsschule an den Ausbildungsbetrieb handelt es sich um eine Datenverarbeitung gemäß Art. 4 Abs. 6 Satz 1, Satz 2 Nr. 3 BayDSG. Nach der schuldatenschutzrechtlichen Spezialregelung des Art. 85 Abs. 1 Satz 1 Bayerisches Gesetz über das Erziehungs- und Unterrichtswesen (BayEUG) dürfen die Schulen allerdings nur die zur Erfüllung der ihnen durch Rechtsvorschriften zugewiesenen Aufgaben erforderlichen Daten erheben, verarbeiten und nutzen.

Zu den Rechtsvorschriften im Sinne des Art. 85 Abs. 1 Satz 1 BayEUG, die den bayerischen öffentlichen Berufsschulen Aufgaben zuweisen, gehören unter anderem das Berufsbildungsgesetz (BBiG) und die Berufsschulordnung (BSO).

§ 37 Abs. 2 Satz 2 BBiG enthält eine bundesrechtliche Befugnisnorm zur Bekanntgabe von Schülerleistungsdaten an die jeweiligen Ausbildungsbetriebe. Danach werden **Ausbildenden – auf deren Verlangen – von der Berufsschule die Ergebnisse der Abschlussprüfung der Auszubildenden übermittelt.**

§ 37 BBiG Abschlussprüfung
(2) [1]Dem Prüfling ist ein Zeugnis auszustellen. [2]Ausbildenden werden auf deren Verlangen die Ergebnisse der Abschlussprüfung der Auszubildenden übermittelt. [3]Sofern die Abschlussprüfung in zwei zeitlich auseinander fallenden Teilen durchgeführt wird, ist das Ergebnis der Prüfungsleistungen im ersten Teil der Abschlussprüfung dem Prüfling schriftlich mitzuteilen.

Landesrechtlich sieht die Regelung des **§ 21 Abs. 1 Sätze 1 und 2 BSO** vor, dass die jeweiligen **Ausbildungsbetriebe von der Berufsschule im Rahmen der vertrauensvollen Zusammenarbeit insbesondere über bedeutsame Angelegenheiten, welche die Ausbildung der Schülerin oder des Schülers betreffen, zu unterrichten** sind. § 21 Abs. 1 Sätze 1 und 2 BSO lässt damit im Ergebnis eine weiter gehende Datenübermittlung als § 37 Abs. 2 Satz 2 BBiG zu.

§ 21 BSO Zusammenarbeit mit Ausbildenden, Arbeitgeberinnen und Arbeitgebern sowie Arbeitnehmervertreterinnen und Arbeitnehmervertretern
(1) [1]Die Berufsschulen wirken im Rahmen ihrer Zuständigkeit mit den Ausbildenden, den Arbeitgeberinnen und Arbeitgebern und den Arbeitnehmervertreterinnen und Arbeitnehmervertretern der jeweiligen Ausbildungsbetriebe vertrauensvoll zusammen. [2]Dabei sind die jeweiligen Ausbildungsbetriebe insbesondere über be-

deutsame Angelegenheiten, welche die Ausbildung der Schülerin oder des Schülers betreffen, zu unterrichten. [3]Mindestens für jedes Schulhalbjahr werden den Ausbildungsbetrieben auf Antrag über die Schülerinnen oder Schüler die Themenbereiche für die einzelnen Fächer übermittelt. [4]Auf Einladung soll die Berufsschule Vertreterinnen oder Vertreter zu Versammlungen der örtlichen bzw. regionalen Gremien der Ausbildungsbetriebe entsenden.

Ob und inwieweit die Übermittlung von Einzelnoten, Notenübersichten oder Zeugnissen an den jeweiligen Ausbildungsbetrieb zur sachgerechten Erfüllung der in § 21 Abs. 1 Sätze 1 und 2 BSO statuierten Verpflichtung der Berufsschule erforderlich ist, kann allerdings nur **im konkreten Einzelfall vor Ort in Wahrnehmung der pädagogischen Verantwortung entschieden** werden. Dabei ist das Informationsinteresse des Ausbildungsbetriebs insbesondere mit dem Grundrecht der Schülerin oder des Schülers auf informationelle Selbstbestimmung abzuwägen. Aus datenschutzrechtlicher Sicht ist hier ein **strenger Maßstab anzulegen.** Dies gilt insbesondere für die Beurteilung, ob tatsächlich eine von § 21 Abs. 1 Sätze 1 und 2 BSO als Übermittlungsvoraussetzung zwingend geforderte „bedeutsame Angelegenheit, welche die Ausbildung der Schülerin oder des Schülers betrifft" vorliegt.

10.8.2 Übermittlung von weiteren personenbezogenen Schülerdaten

Nicht selten verfügt die Berufsschule über weitere personenbezogene Schülerdaten, die für den jeweiligen Ausbildungsbetrieb ebenfalls von Interesse sein können. So wurde mir beispielsweise die Frage vorgelegt, ob eine Berufsschule den betreffenden Ausbildungsbetrieb darüber informieren darf, dass gegen einen Schüler eine Jugendstrafe verhängt worden war; hierüber war die Berufsschule zuvor gemäß § 70 Satz 1 bzw. § 109 Abs. 1 Satz 2 Jugendgerichtsgesetz unterrichtet worden.

Für die Beurteilung, ob und inwieweit die Übermittlung weiterer Schülerdaten an den Ausbildungsbetrieb zur Aufgabenerfüllung der Berufsschule erforderlich – und damit datenschutzrechtlich zulässig – ist, kommt es gemäß § 21 Abs. 1 Sätze 1 und 2 Berufsschulordnung wiederum **entscheidend** darauf an, dass es sich um eine **bedeutsame Angelegenheit** handelt, **welche die Ausbildung der Schülerin oder des Schülers betrifft.** Hier hat die Berufsschule in jedem Einzelfall in Wahrnehmung ihrer pädagogischen Verantwortung zwischen dem Informationsinteresse des Ausbildungsbetriebs und dem Grundrecht des Schülers auf informationelle Selbstbestimmung abzuwägen. Aus datenschutzrechtlicher Sicht ist dabei ein **strenger Maßstab anzulegen.**

Unter dieser Maßgabe kann eine Information des Ausbildungsbetriebs durch die Berufsschule etwa zulässig sein, wenn aus dem Vorenthalten der Information eine **Gefahr für den Ausbildungsbetrieb, dessen Kunden, sonstige Dritte oder den Schüler selbst** erwachsen könnte. Dies ist beispielsweise denkbar bei einer Verurteilung eines Schülers wegen eines Betäubungsmittel- oder Vermögensdeliktes und einer Ausbildung in einem Alten- oder Pflegeheim oder in einer sonstigen medizinischen Einrichtung. Letztendlich kommt es aber stets auf die **Umstände des konkreten Einzelfalles** an, die nur vor Ort in Wahrnehmung der pädagogischen Verantwortung abschließend beurteilt werden können.

10.9 Außenprüfungen öffentlicher Schulen

Auch im Berichtszeitraum habe ich wieder bei bayerischen öffentlichen – staatlichen wie kommunalen – Schulen die Einhaltung datenschutzrechtlicher Vorschriften vor Ort überprüft. Bei meinen Außenprüfungen zeigte sich zwar zumeist ein grundsätzliches Bestreben nach datenschutzgerechtem schulischem Handeln. Dennoch musste ich die geprüften Schulen immer wieder auf **wesentliche schuldatenschutzrechtliche Vorgaben** aufmerksam machen, von denen ich nur beispielhaft folgende herausgreifen möchte:

10.9.1 Videoaufzeichnung an Schulen

Eine Videoaufzeichnung darf an Schulen nur unter den **in Art. 21a BayDSG in Verbindung mit Anlage 8 „Videoaufzeichnung an Schulen" der** vom Staatsministerium für Bildung und Kultus, Wissenschaft und Kunst erlassenen **Verordnung zur Durchführung des Art. 28 Abs. 2 des Bayerischen Datenschutzgesetzes** (im Folgenden: Durchführungsverordnung) **detailliert geregelten Voraussetzungen** erfolgen. Danach muss die Videoaufzeichnung zum Schutz von Leben, Gesundheit, Freiheit und Eigentum der Personen, die sich im Bereich der Schule oder in deren unmittelbarer Nähe aufhalten, oder zum Schutz der schulischen Einrichtung vor Sachbeschädigung und Diebstahl **im konkreten Einzelfall erforderlich** sein. Von der Videoaufzeichnung betroffen sein dürfen nur Personen, die sich im Eingangsbereich der Schule aufhalten oder die sich außerhalb von schulischen oder sonstigen von der Schule zugelassenen Veranstaltungen zwischen 22:00 Uhr und 6:30 Uhr, an Feiertagen, an Wochenenden oder in den Ferien auf dem Schulgelände befinden. Zudem müssen die gespeicherten Daten grundsätzlich spätestens drei Wochen nach der Aufzeichnung gelöscht werden. Zu den Einzelheiten verweise ich auf meine Ausführungen im 23. Tätigkeitsbericht 2008 unter Nr. 12.2.2 sowie im 25. Tätigkeitsbericht 2012 unter Nr. 10.5.

10.9.2 Schulhomepage

In Bezug auf die Einstellung von personenbezogenen Daten in die Schulhomepage müssen die Schulen insbesondere **Anlage 9 „Internetauftritt von Schulen" der Durchführungsverordnung** beachten. Handelt es sich nicht um dienstliche Kommunikationsdaten der Schulleitung und von Lehrkräften, die an der Schule eine Funktion mit Außenwirkung wahrnehmen, setzt die Veröffentlichung von personenbezogenen Daten der am Schulleben Beteiligten eine schriftliche, informierte und freiwillige Einwilligung voraus. Sind die Betroffenen minderjährig, so muss die erforderliche Einwilligung bis zur Vollendung des 14. Lebensjahres durch die Erziehungsberechtigten und ab Vollendung des 14. Lebensjahres zusätzlich auch durch die Minderjährigen selbst erfolgen. Im Einzelnen verweise ich auf meine Ausführungen im 23. Tätigkeitsbericht 2008 unter Nr. 12.2.3 und im 24. Tätigkeitsbericht 2010 unter Nr. 10.2.

Um den Schulen die Einholung rechtlich einwandfreier Einwilligungserklärungen zu erleichtern, habe ich in Abstimmung mit dem Staatsministerium für Bildung und Kultus, Wissenschaft und Kunst **vier differenzierte Muster-Einwilligungserklärungen für alle Gruppen von Schulangehörigen** entwickelt. Diese sind mittlerweile der vom Staatsministerium erlassenen Bekanntmachung „Erläuternde Hinweise zum Vollzug der datenschutzrechtlichen Bestimmungen für die Schulen"

(siehe Nr. 10.2 dieses Tätigkeitsberichts) als Anlage beigefügt, aber auch auf meiner Homepage https://www.datenschutz-bayern.de unter „Themen“ – „Schulen“ abrufbar. Das Staatsministerium hat die Muster allen staatlichen Schulen ab dem Schuljahr 2011/2012 verbindlich vorgegeben sowie allen kommunalen Schulen und staatlich anerkannten Ersatzschulen zur Verwendung empfohlen. Zu den Einzelheiten verweise ich auf meinen 25. Tätigkeitsbericht 2012 unter Nr. 10.3. Im Hinblick auf Schülerfotos mache ich zudem auf meine Ausführungen in Nr. 10.4.4 dieses Tätigkeitsberichts aufmerksam.

Darüber hinaus haben die Schulen ihre **bereits bestehenden Internetauftritte** daraufhin **zu überprüfen,** ob für jede Person, deren Daten veröffentlicht wurden, tatsächlich eine den Erfordernissen des Datenschutzes genügende Einwilligungserklärung vorliegt. Fehlt es an einer solchen datenschutzgerechten Einwilligung, darf die entsprechende Internetveröffentlichung nicht länger aufrechterhalten werden.

10.9.3 Passwortgeschützter Bereich der Schulhomepage

Im Berichtszeitraum hat das Staatsministerium für Bildung und Kultus, Wissenschaft und Kunst die **Durchführungsverordnung** unter meiner Beteiligung um eine neue **Anlage 11 „Schulinterner passwortgeschützter Bereich“** erweitert. Im Einzelnen verweise ich hierzu auf meine Ausführungen unter Nr. 10.1.3 dieses Tätigkeitsberichts.

Entsprechend einem herkömmlichen Aushang am „Schwarzen Brett“ können die Schulen danach vor allem **Sprechstundenlisten und Vertretungspläne** auch ohne schriftliche Einwilligung der Betroffenen in einen geschützten Bereich der Schulhomepage einstellen, auf den nur berechtigte Lehrkräfte, Schülerinnen und Schüler sowie Erziehungsberechtigte mittels eines Passwortes Zugriff haben. Bei **Elternbriefen und sonstigen klassen- und fachbezogenen Informationen** kommt es hingegen auf den Inhalt an. Enthalten diese Texte personenbezogene Daten, deren Bekanntgabe unabhängig von der Veröffentlichungsform nur mit Einwilligung der Betroffenen zulässig ist – wie etwa die Schwangerschaft einer Lehrerin –, ist auch hier das Einwilligungserfordernis zu beachten.

10.9.4 Notenverwaltungsprogramm

Die elektronischen Einsichtsrechte in Schülernoten sind detailliert in **Anlage 6 „Verfahren Notenverwaltungsprogramm“ der Durchführungsverordnung** geregelt. Fächerübergreifenden Zugriff auf Leistungsdaten dürfen danach erhalten:

- die **Schulleitung** nur im konkreten Einzelfall, soweit dies zur Erfüllung ihrer pädagogischen, organisatorischen und rechtlichen Aufgaben erforderlich ist,

- **Beratungslehrkräfte und Schulpsychologen** nur im konkreten Einzelfall, soweit dies zur Erfüllung ihrer pädagogisch-psychologischen und rechtlichen Aufgaben im Rahmen der Schulberatung erforderlich ist,

- die **Lehrkräfte** für die jeweils von ihnen unterrichteten Schülerinnen und Schüler nur im konkreten Einzelfall, insbesondere für den Zeitraum, für den

dies zur Erfüllung ihrer Aufgaben als Mitglied der Klassenkonferenz (insbesondere Zeugniserstellung, Entscheidung über das Vorrücken, Empfehlung an die Lehrerkonferenz im Fall des Vorrückens auf Probe) erforderlich ist,

– die **Klassenleitungen** darüber hinaus für die Schülerinnen und Schüler ihrer Klasse, um schulische oder häusliche Probleme erkennen zu können, die sich durch einen plötzlichen Leistungsabfall in mehreren Fächern gleichzeitig bemerkbar machen, sowie für die Zeugnisvorbereitung und -erstellung,

– die **Lehrkräfte an Berufsschulen** darüber hinaus wegen der dort bestehenden schulorganisatorischen und didaktischen Besonderheiten für die jeweils von ihnen unterrichteten Schülerinnen und Schüler während des gesamten Schuljahres.

Hintergrund dieser differenzierten Regelung ist, dass die betroffenen Personengruppen jeweils **nur in dem sachlichen und zeitlichen Umfang ein fächerübergreifendes Zugriffsrecht auf Schülernoten** – also auf sensible personenbezogene Daten – erhalten dürfen, der **für die Erfüllung ihrer jeweiligen Aufgaben erforderlich** ist. Zu den Einzelheiten verweise ich auf Nr. 10.1.1 dieses Tätigkeitsberichts.

10.9.5 Passwortgeschützte Lernplattform

Schulen, die sich im Rahmen ihrer pädagogischen Eigenverantwortung für den Einsatz einer passwortgeschützten Lernplattform entscheiden, müssen die Vorgaben der **Anlage 10 „Passwortgeschützte Lernplattform" der Durchführungsverordnung** beachten. Insbesondere sind hier regelmäßig qualifizierte Einwilligungserklärungen bei den Lehrkräften, Schülern und/oder Erziehungsberechtigten mittels der vom Staatsministerium für Bildung und Kultus, Wissenschaft und Kunst zur Verfügung gestellten und mit mir abgestimmten **Muster-Einverständniserklärungen** einzuholen; diese sind inzwischen als Anlagen 5.1 und 5.2 der „Handreichung für Datenschutzbeauftragte an bayerischen staatlichen Schulen" von der Homepage des Staatsministeriums unter www.km.bayern.de/ministerium/recht/datenschutz.html abrufbar. Zu den beim Einsatz passwortgeschützter Lernplattformen von den Schulen zu beachtenden Datenschutzanforderungen verweise ich im Einzelnen auf meine Ausführungen im 24. Tätigkeitsbericht 2010 unter Nr. 10.3 sowie auf die Beiträge Nr. 10.1.2 und Nr. 10.3 dieses Tätigkeitsberichts.

10.9.6 Schulischer Jahresbericht

Gibt eine Schule für die Schülerinnen und Schüler und Erziehungsberechtigten einen papiergebundenen Jahresbericht heraus, so dürfen darin nach der **gesetzlichen Regelung des Art. 85 Abs. 3 Bayerisches Gesetz über das Erziehungs- und Unterrichtswesen** folgende personenbezogene Daten enthalten sein: Name, Geburtsdatum, Jahrgangsstufe und Klasse der Schülerinnen und Schüler, Name, Fächerverbindung und Verwendung der einzelnen Lehrkräfte, Angaben über besondere schulische Tätigkeiten und Funktionen einzelner Lehrkräfte, Schülerinnen und Schüler und Erziehungsberechtigter.

In Anbetracht dieses klaren, abschließenden gesetzlichen Rahmens sollte im Hinblick auf die Aufnahme weiterer personenbezogener Daten in den schulischen Jahresbericht aus Datenschutzsicht Zurückhaltung geübt werden. Voraussetzung ist hierfür jedenfalls stets eine schriftliche, informierte und freiwillige Einwilligung der Betroffenen. Bei Minderjährigen müssen bis zur Vollendung des 14. Lebensjahres die Erziehungsberechtigten, ab Vollendung des 14. Lebensjahres zusätzlich auch die Minderjährigen selbst einwilligen. Die staatlichen Schulen müssen, die kommunalen Schulen sollten hierbei die bereits oben unter Nr. 10.9.2 erwähnten **vier differenzierten Muster-Einwilligungserklärungen für alle Gruppen von Schulangehörigen** verwenden. In der Praxis ist dies vor allem für die Einstellung von **Klassenfotos** in den schulischen Jahresbericht notwendig; hierzu verweise ich im Einzelnen auch auf meine Ausführungen in Nr. 10.4.3 dieses Tätigkeitsberichts.

10.9.7 Weitergabe von Schülerdaten zu Werbezwecken

Nach Art. 85 Abs. 1 Satz 1 und Abs. 2 Satz 1 Bayerisches Gesetz über das Erziehungs- und Unterrichtswesen (BayEUG) ist den Schulen die Weitergabe von Daten und Unterlagen über Schülerinnen und Schüler sowie Erziehungsberechtigte an außerschulische Stellen untersagt, es sei denn, die Weitergabe ist zur Erfüllung der den Schulen durch Rechtsvorschriften zugewiesenen Aufgaben erforderlich oder es besteht ein rechtlicher Anspruch auf die Herausgabe der Daten.

Korrespondierend mit dem in Art. 84 Abs. 1 BayEUG vom bayerischen Gesetzgeber aufgestellten **Verbot der kommerziellen Werbung** ist es den Schulen daher untersagt, Schülerdaten zu Werbezwecken weiterzugeben. Dabei macht es keinen Unterschied, ob die Schulen die Daten selbst weitergeben oder ob sie Datenerhebungen durch außerschulische Stellen – oftmals getarnt als Geschenkauslobungen oder (Wissens-)Wettbewerbe – in der Schule dulden. In der Vergangenheit aufgefallen sind mir hier vor allem Kreditinstitute, Krankenkassen und (Buch-)Direktvertriebsunternehmen. Im Einzelnen verweise ich diesbezüglich auf meinen 24. Tätigkeitsbericht 2010 unter Nr. 10.4.

10.9.8 Evaluation an Schulen

Bei schulischen Evaluationen sind die **in Art. 113c Bayerisches Gesetz über das Erziehungs- und Unterrichtswesen detailliert geregelten Vorgaben** einzuhalten. Insbesondere dürfen personenbezogene Daten nur insoweit erhoben, verarbeitet und genutzt werden, als das öffentliche Interesse die schutzwürdigen Belange der Betroffenen erheblich überwiegt und der Zweck der Evaluation auf andere Weise nicht oder nur mit unverhältnismäßigem Aufwand erreicht werden kann. Eine Verarbeitung und Nutzung der im Rahmen der Evaluation erlangten personenbezogenen Daten zu anderen Zwecken ist nicht zulässig. Die personenbezogenen Daten müssen zudem so bald wie möglich anonymisiert werden; Ergebnisse der Evaluation dürfen ausschließlich in nicht-personenbezogener Form veröffentlicht werden. Zu den näheren Einzelheiten verweise ich auf meinen 23. Tätigkeitsbericht 2008 unter Nr. 12.1.

10.9.9 Ausblick

Ich hoffe, dass diese Kurzübersicht dazu beiträgt, an den bayerischen öffentlichen – also staatlichen und kommunalen – Schulen das Bewusstsein für wesentliche schuldatenschutzrechtliche Anforderungen zu schärfen. Nach meinem Eindruck hat sich die mittlerweile abgeschlossene Bestellung behördlicher Datenschutzbeauftragter an den staatlichen Schulen bzw. Schulämtern auch insoweit bereits positiv ausgewirkt.

Meine Prüfungen öffentlicher Schulen werde ich auch in Zukunft fortsetzen.

10.10 Videoüberwachung bei staatlichen Museen und Hochschulen

Zulässigkeit und Grenzen der Videoüberwachung durch bayerische öffentliche Stellen hat der bayerische Gesetzgeber – vorbehaltlich bereichsspezifischer Sonderregelungen wie etwa Art. 32 Abs. 2 Polizeiaufgabengesetz oder Art. 9 Bayerisches Versammlungsgesetz – seit dem 01.07.2008 **in Art. 21a BayDSG detailliert geregelt** (siehe hierzu ausführlich meinen 23. Tätigkeitsbericht 2008 Nr. 9.2). Beabsichtigen bayerische öffentliche Stellen eine Video**beobachtung** (Erhebung personenbezogener Daten mit Hilfe von optisch-elektronischen Einrichtungen) oder gar eine noch eingriffsintensivere Video**aufzeichnung** (Speicherung personenbezogener Daten mit Hilfe von optisch-elektronischen Einrichtungen), müssen folglich die gesetzlichen Anforderungen des Art. 21a BayDSG erfüllt sein.

Art. 21a BayDSG gilt im Übrigen auch für bayerische öffentliche Stellen, die gemäß Art. 3 Abs. 1 Satz 1 BayDSG als **Unternehmen am Wettbewerb** teilnehmen, da eine Videoüberwachung nicht der Erbringung der Wettbewerbsleistung dient und es mithin nicht zur Anwendung des Bundesdatenschutzgesetzes kommt. Auch die Zulässigkeit von **Kameraattrappen** richtet sich nach Art. 21a BayDSG, da diese ebenfalls eine Verhaltensbeeinflussung bezwecken und damit in ähnlicher Weise wie eine „echte" Videoüberwachung in das verfassungsrechtlich in Art. 1 Abs. 1 in Verbindung mit Art. 2 Abs. 1 Grundgesetz gewährleistete Grundrecht auf informationelle Selbstbestimmung der Betroffenen eingreifen.

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

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

zu schützen. [2]Es dürfen keine Anhaltspunkte dafür bestehen, dass überwiegende schutzwürdige Interessen der Betroffenen beeinträchtigt werden.
(2) Die Videoüberwachung und die erhebende Stelle sind durch geeignete Maßnahmen erkennbar zu machen.
(3) Die Daten dürfen für den Zweck verarbeitet und genutzt werden, für den sie erhoben worden sind, für einen anderen Zweck nur, soweit dies zur Abwehr von

Gefahren für die öffentliche Sicherheit oder Ordnung oder zur Verfolgung von Ordnungswidrigkeiten von erheblicher Bedeutung oder von Straftaten erforderlich ist.
(4) Werden durch Videoüberwachung erhobene Daten einer bestimmten Person zugeordnet, ist diese über die Tatsache der Speicherung entsprechend Art. 10 Abs. 8 zu benachrichtigen.
(5) Die Videoaufzeichnungen und daraus gefertigte Unterlagen sind spätestens drei Wochen nach der Datenerhebung zu löschen, soweit sie nicht zur Verfolgung von Ordnungswidrigkeiten von erheblicher Bedeutung oder von Straftaten oder zur Geltendmachung von Rechtsansprüchen benötigt werden.
(6) [1]Art. 26 bis 28 gelten für die Videoaufzeichnung entsprechend. [2]Öffentliche Stellen haben ihren behördlichen Datenschutzbeauftragten rechtzeitig vor dem Einsatz einer Videoaufzeichnung neben den in Art. 26 Abs. 3 Satz 1 genannten Beschreibungen die räumliche Ausdehnung und Dauer der Videoaufzeichnung, die Maßnahmen nach Abs. 2 und die vorgesehenen Auswertungen mitzuteilen.

Im Berichtszeitraum habe ich – unter anderem veranlasst durch entsprechende Bürgereingaben – verstärkt die Videoüberwachung durch staatliche Museen und Hochschulen überprüft. Hierbei musste ich eine nicht unerhebliche Anzahl von **Prüfungsfeststellungen** aussprechen. Diese betrafen im Wesentlichen folgende Punkte:

10.10.1 Defizite schon bei der Bestellung behördlicher Datenschutzbeauftragter

Öffentliche Stellen, die personenbezogene Daten mit Hilfe von automatisierten Verfahren verarbeiten oder nutzen, haben gemäß Art. 25 Abs. 2 Satz 1 BayDSG einen ihrer Beschäftigten zum **behördlichen Datenschutzbeauftragten** zu bestellen. Nach Art. 26 Abs. 1 BayDSG bedürfen der erstmalige Einsatz ebenso wie die wesentliche Änderung solcher automatisierter Verfahren in der Regel der vorherigen schriftlichen Freigabe durch die das Verfahren einsetzende öffentliche Stelle. Erteilt wird die **datenschutzrechtliche Freigabe** gemäß Art. 26 Abs. 3 Satz 2 BayDSG grundsätzlich durch den behördlichen Datenschutzbeauftragten. Dieser hat gemäß Art. 27 BayDSG zudem ein **Verzeichnis** der bei der öffentlichen Stelle eingesetzten und datenschutzrechtlich freigegebenen automatisierten Verfahren zu führen.

Aufgrund der Rechtsfolgenverweisung des Art. 21a Abs. 6 Satz 1 BayDSG unterfällt den letztgenannten gesetzlichen Bestimmungen auch der **Betrieb einer Videoaufzeichnungsanlage.** In diesem Zusammenhang weise ich insbesondere auf das „Prüfungsschema zur Videobeobachtung und Videoaufzeichnung (Videoüberwachung)“ und das „Muster zur Beschreibung der tech. und org. Maßnahmen beim Einsatz einer Videoaufzeichnungsanlage“ hin, die von meiner Homepage https://www.datenschutz-bayern.de unter „Veröffentlichungen“ – „Broschüren“ – „Mustervordrucke“ abrufbar sind.

Diesen zwingenden gesetzlichen Vorgaben haben die geprüften öffentlichen Stellen oftmals schon mangels Bestellung eines behördlichen Datenschutzbeauftragten nicht entsprochen.

10.10.2 Unzureichende Prüfung der gesetzlichen Zulässigkeitsvoraussetzungen

Der bayerische Gesetzgeber hat in Art. 21a Abs. 1 und 2 BayDSG die Zulässigkeit einer Videoüberwachung von der Einhaltung strenger gesetzlicher Anforderungen abhängig gemacht. **Kurz gefasst darf eine Videoüberwachung nur zu Zwecken des Personen- und Objektschutzes erfolgen, muss hierfür erforderlich sein, darf keine überwiegenden schutzwürdigen Interessen der Betroffenen beeinträchtigen und muss zudem transparent gestaltet sein.**

Bei meinen Prüfungen habe ich allerdings immer wieder festgestellt, dass die betroffenen öffentlichen Stellen das Vorliegen dieser materiell-datenschutzrechtlichen Voraussetzungen vor der Inbetriebnahme einer Videoüberwachungsanlage nicht hinreichend geprüft haben. Im Einzelnen:

– Strafverfolgung als unzulässiger Überwachungszweck

So musste ich die geprüften öffentlichen Stellen regelmäßig darauf hinweisen, dass die Ermöglichung einer repressiven Strafverfolgung, etwa hinsichtlich Vandalismus oder Diebstahl, **allein Aufgabe von Polizei und Staatsanwaltschaft** ist und daher nach dem in Art. 21a Abs. 1 Satz 1 BayDSG zum Ausdruck kommenden Willen des bayerischen Gesetzgebers als zulässiger Hauptzweck für eine behördliche Videoüberwachung von vornherein ausscheidet.

Aus diesem Grund habe ich die betroffenen öffentlichen Stellen aufgefordert, mir nachvollziehbar darzulegen, dass und wie mit der Videoüberwachung **präventiv** zur Verhinderung derartiger Geschehnisse beigetragen werden kann. Dazu waren die geprüften öffentlichen Stellen aber oftmals nicht in der Lage.

– Unzureichende Prüfung der Erforderlichkeit

Regelmäßig nur unzureichend geprüft wurde in der Praxis die vom bayerischen Gesetzgeber in Art. 21a Abs. 1 Satz 1 BayDSG als Zulässigkeitsvoraussetzung ausdrücklich normierte Erforderlichkeit der Videoüberwachung.

Um dieser zwingenden gesetzlichen Anforderung zu entsprechen, habe ich die betroffenen öffentlichen Stellen darauf hingewiesen, dass in einem ersten Schritt die **generelle Erforderlichkeit einer Videoüberwachung** grundsätzlich anhand einer detaillierten und regelmäßig – in etwa halbjährlichem Abstand – fortgeschriebenen Vorfallsdokumentation belegt werden muss. In einem zweiten Schritt müssen zudem der Standort **jeder einzelnen Kamera** sowie deren Erfassungswinkel anhand separater Standortbegründungen hinreichend gerechtfertigt werden. Die Videoüberwachung ist dabei zum einen **räumlich** auf die „gefährdeten" Bereiche zu begrenzen, insbesondere also auf „Tote Winkel" und auf Bereiche, bei denen aufgrund von Schadensfällen in der Vergangenheit auch künftig mit vergleichbaren Vorkommnissen zu rechnen ist. Der jeweilige Kameraerfassungsbereich ist dort, wo er über die gefährdeten Bereiche hinausgeht, durch geeignete technische Maßnahmen – beispielsweise Schwarzschaltungen, mechanische Sperren, Umsetzen der Kameras, softwaretechnische Sperren bestimmter möglicher Beobachtungsbereiche – einzuschränken. Zum ande-

ren ist die Videoüberwachung auch in **zeitlicher** Hinsicht auf das erforderliche Maß – also in der Regel auf die Zeiten, in denen mit Schadensfällen zu rechnen ist – zu beschränken.

Sollten sich bei den danach notwendigen, eingehenden Prüfungen **alternative, weniger einschneidende Maßnahmen** – wie etwa verstärkte Überwachung durch Aufsichtspersonal, Alarmanlagen, mechanische Sperren – als ebenso geeignet zur Erreichung der gesetzlich zulässigen Schutzzwecke erweisen, ist von vornherein auf diese Maßnahmen zurückzugreifen. In diesem Zusammenhang habe ich die geprüften öffentlichen Stellen insbesondere darauf aufmerksam gemacht, dass eine Videoüberwachung kein bloßes Mittel zur Einsparung von Wachpersonal sein darf, sondern stets Teil eines umfassenden Gesamtkonzeptes sein muss.

– **Unzureichende Prüfung einer Beeinträchtigung überwiegender schutzwürdiger Interessen**

Um gemäß Art. 21a Abs. 1 Satz 2 BayDSG eine Beeinträchtigung überwiegender schutzwürdiger Interessen der Betroffenen zu vermeiden, dürfen insbesondere **(höchst)persönliche Bereiche** – wie etwa (der Zugang zu) Toilettenanlagen und reine Aufenthaltsbereiche – grundsätzlich **nicht videoüberwacht** werden. Auch diese gesetzliche Anforderung wurde in der Praxis nicht durchgehend beachtet.

In diesem Zusammenhang habe ich die geprüften öffentlichen Stellen überdies auf den personalvertretungsrechtlichen Mitbestimmungstatbestand des Art. 75a Abs. 1 Nr. 1 Bayerisches Personalvertretungsgesetz (BayPVG) aufmerksam gemacht. Diese Vorschrift ist nach der Rechtsprechung bereits dann einschlägig, wenn Beschäftigte von einer Videoüberwachung mitbetroffen sind. Schon aus Transparenzgründen rate ich in solchen Fällen stets zum **Abschluss einer Dienstvereinbarung** im Sinne des Art. 73 BayPVG. In dieser sollte insbesondere geregelt werden, welche Beschäftigtendaten aufgezeichnet werden, wie lange die aufgezeichneten Daten gespeichert werden und welche Personen Zugriff auf diese Daten haben. Zudem sollte in der Dienstvereinbarung festgehalten werden, dass die Videoüberwachung nicht zum Zweck der Verhaltens- und/oder Leistungskontrolle der Beschäftigten eingesetzt werden darf.

– **Unzureichende Beachtung des Transparenzgebots**

Nach Art. 21a Abs. 2 BayDSG sind die Videoüberwachung und die erhebende Stelle durch geeignete Maßnahmen erkennbar zu machen. Diese Informationen werden regelmäßig durch **entsprechende Hinweisschilder** zu geben sein. Dadurch soll der Betroffene nicht nur auf den mit der Videoüberwachung einhergehenden Eingriff in sein Grundrecht auf informationelle Selbstbestimmung aufmerksam gemacht werden; vielmehr soll ihm auf diese Weise auch die Möglichkeit gegeben werden, seine Datenschutzrechte effektiv wahrzunehmen.

Bei meinen Prüfungen hat sich allerdings gezeigt, dass dieses gesetzliche Transparenzgebot in der Praxis nicht immer ausreichend beachtet wurde. Die geprüften öffentlichen Stellen habe ich daher dazu aufgefordert, die Betroffenen zukünftig insbesondere durch eine deutlich **sichtbare Anbringung von Piktogrammen** gemäß DIN 33450 (weißes Kamerasymbol auf

blauem Hintergrund) vor Betreten des videoüberwachten Bereichs auf die Videoüberwachung hinzuweisen.

10.10.3 Ergebnis und Ausblick

Meine datenschutzrechtlichen Hinweise haben nicht nur bei den konkret geprüften staatlichen Museen und Hochschulen zu einer **deutlichen Verbesserung des Datenschutzniveaus** – teilweise bis hin zu einer nahezu vollständigen Einstellung der Videoüberwachung – geführt, sondern auch über die jeweils geprüften Einzelfälle hinaus Wirkung erzielt. So konnte ich beispielsweise erreichen, dass das Staatsministerium für Bildung und Kultus, Wissenschaft und Kunst bei allen bayerischen staatlichen Museen auf die Bestellung behördlicher Datenschutzbeauftragter hingewirkt hat und alle bayerischen staatlichen Museen und Hochschulen eindringlich an die Beachtung der gesetzlichen Anforderungen des Art. 21a BayDSG bei Videoüberwachungen erinnert hat.

Auch in Zukunft werde ich meine Überprüfung von Videoüberwachungen durch bayerische öffentliche Stellen fortsetzen.

10.11 Ausgabe von Audioguides gegen Hinterlegung von Ausweisdokumenten bei staatlichen Museen

Viele Museumsbesucher möchten zwar nähere Erläuterungen zu den einzelnen Ausstellungsgegenständen erhalten, nicht jedoch an einer terminabhängigen oder sogar anmeldepflichtigen (Gruppen-)Führung teilnehmen. Zahlreiche Museen bieten ihren Besuchern daher sogenannte **Audioguides** an, bei denen – zumeist über Kopfhörer – detaillierte Informationen zu den Ausstellungsstücken individuell abgerufen werden können. Auch wenn die Überlassung derartiger Audioguides mitunter sogar kostenlos ist, so verlangen doch einige Museen, dass hierfür an der Kasse der **Personalausweis oder ein anderes amtliches Lichtbilddokument „als Pfand"** hinterlegt wird. Im Berichtszeitraum erreichten mich in diesem Zusammenhang Beschwerden von Besuchern eines staatlichen Museums, die sich durch die Forderung nach Hinterlegung des Personalausweises in ihren Datenschutzrechten verletzt sahen.

In datenschutzrechtlicher Hinsicht stellt das Verlangen nach Hinterlegung des Personalausweises eine Datenerhebung im Sinne von Art. 4 Abs. 5 BayDSG dar. Diese Erhebung personenbezogener Daten ist mangels Einwilligung der Betroffenen gemäß Art. 15 Abs. 1 Nr. 1 BayDSG in Verbindung mit Art. 16 Abs. 1 BayDSG allerdings nur zulässig, wenn die Kenntnis der Personalausweisdaten zur Erfüllung der in der Zuständigkeit der erhebenden Stelle – hier also des Museums – liegenden Aufgaben erforderlich ist.

Zunächst vermag ich schon nicht zu erkennen, inwieweit die Kenntnis der in den Personalausweisen enthaltenen, sensiblen personenbezogenen Daten der Besucher für die Aufgabenerfüllung eines Museums erforderlich sein sollte.

Unabhängig davon widerspricht aber jedenfalls das Verlangen, den Personalausweis als „Pfand" zu hinterlegen, den klaren gesetzlichen Vorgaben des am 01.11.2010 in Kraft getretenen **Gesetzes über Personalausweise und den elektronischen Identitätsnachweis (Personalausweisgesetz – PAuswG)**. Da-

nach kann der Ausweisinhaber den Ausweis zwar bei öffentlichen und nichtöffentlichen Stellen als Identitätsnachweis und Legitimationspapier verwenden (§ 20 Abs. 1 PAuswG). Außer in wenigen, eng begrenzten und hier nicht einschlägigen Fallkonstellationen **darf vom Ausweisinhaber** allerdings gemäß § 1 Abs. 1 Satz 3 PAuswG **nicht verlangt werden, den Personalausweis zu hinterlegen oder in sonstiger Weise den Gewahrsam aufzugeben.** Nach dem in der Gesetzesbegründung niedergelegten Willen des Bundesgesetzgebers soll darüber hinaus **auch eine freiwillige Abgabe des Personalausweises an Dritte nicht** erfolgen.

§ 1 PAuswG Ausweispflicht; Ausweisrecht
(1) [1]Deutsche im Sinne des Artikels 116 Abs. 1 des Grundgesetzes sind verpflichtet, einen Ausweis zu besitzen, sobald sie 16 Jahre alt sind und der allgemeinen Meldepflicht unterliegen oder, ohne ihr zu unterliegen, sich überwiegend in Deutschland aufhalten. [2]Sie müssen ihn auf Verlangen einer zur Feststellung der Identität berechtigten Behörde vorlegen. [3]Vom Ausweisinhaber darf nicht verlangt werden, den Personalausweis zu hinterlegen oder in sonstiger Weise den Gewahrsam aufzugeben. [4]Dies gilt nicht für zur Identitätsfeststellung berechtigte Behörden sowie in den Fällen der Einziehung und Sicherstellung.

Bereits nach diesen personalausweisrechtlichen Vorschriften ist es (bundes-)rechtlich nicht zulässig, den Personalausweis von Museumsbesuchern als „Pfand" zu verlangen oder auch nur entgegenzunehmen. Zudem stehen die **Personalausweise** nach der Vorschrift des § 4 Abs. 2 PAuswG ausdrücklich **nicht im Eigentum des jeweiligen Ausweisinhabers, sondern allein der Bundesrepublik Deutschland**, weshalb sie schon von vornherein als „Pfand" ausscheiden.

Im Hinblick auf den Schutz der Museumsbesucher in ihrem Grundrecht auf informationelle Selbstbestimmung (Art. 1 Abs. 1 in Verbindung mit Art. 2 Abs. 1 Grundgesetz) halte ich es **überdies für datenschutzrechtlich äußerst problematisch**, für die Überlassung eines Audioguides während des Museumsbesuchs als „Pfand" ein **Dokument mit sensiblen personenbezogenen Daten von den Besuchern zu verlangen**. Gleiches gilt im Übrigen, wenn statt des Personalausweises die Hinterlegung eines anderen amtlichen Lichtbilddokumentes – wie beispielsweise des Führerscheins – gefordert wird. In Bezug auf letzteren ist zusätzlich anzumerken, dass längst nicht jeder Museumsbesucher Inhaber eines Führerscheins ist, weshalb der Führerschein schon an sich nicht als „Pfand" geeignet ist. Soweit in Anbetracht des zumeist geringen Sachwerts von Audioguides die Hinterlegung einer Sicherheit überhaupt als notwendig erachtet wird, kann dem Interesse des Museums, die Rückgabe der Audioguides zu gewährleisten, ebenso wirkungsvoll durch **Hinterlegung eines bestimmten Geldbetrages als Sicherheit** Rechnung getragen werden.

Nach Erläuterung dieser Rechtslage hat mir das gegenständliche staatliche Museum erfreulicherweise umgehend zugesichert, die Entgegennahme von Personalausweisen sowie anderen Personaldokumenten als „Pfand" für die Ausgabe von Audioguides ersatzlos einzustellen.

An dieser Stelle **fordere ich alle bayerischen öffentlichen – also insbesondere staatlichen und kommunalen – Museen auf**, die **Ausgabe von Audioguides** oder vergleichbaren Medien **nicht von der Hinterlegung von Personalausweisen oder anderen amtlichen Lichtbilddokumenten abhängig zu machen.**

11 Personalwesen

11.1 Gesetzliche Regelung der elektronischen Personalakte

Eine **Personalakte** umfasst eine **Vielzahl äußerst schutzwürdiger sensibler Daten** (auch im Sinne des Art. 15 Abs. 7 BayDSG); sie wird daher vom Gesetzgeber unmittelbar in § 50 Beamtenstatusgesetz (BeamtStG) in Verbindung mit Art. 102 ff. Bayerisches Beamtengesetz (BayBG) unter den Schutz eines besonderen Geheimnisses, des sogenannten **Personalaktengeheimnisses**, gestellt. Als allgemein gültige Schutzprinzipien für alle öffentlichen Bediensteten sind die detaillierten Regelungen des Personalaktenrechts der bayerischen Beamtinnen und Beamten dabei nach meiner seit jeher vertretenen Auffassung im Grundsatz auch auf die nicht-verbeamteten Beschäftigten des bayerischen öffentlichen Dienstes entsprechend anzuwenden.

Gerade in diesem grundrechtlich besonders sensiblen Bereich kann bei einer **elektronischen Aktenführung** die Gefahr von erheblichen Datenschutzverletzungen – etwa durch Manipulationen, unberechtigte Zugriffe, Datenverluste usw. – gegenüber der herkömmlichen papiergebundenen Aktenführung signifikant ansteigen. Daher stehe ich der Einführung der elektronischen Personalakte **aus Datenschutzsicht generell zurückhaltend** gegenüber.

Unabhängig davon habe ich in den vergangenen Jahren gegenüber der Staatsregierung immer wieder deutlich gemacht, dass **für die elektronische Personalaktenführung** im Sinne der Wesentlichkeitstheorie des Bundesverfassungsgerichts eine **ausdrückliche gesetzliche Rechtsgrundlage erforderlich** ist. Die personalaktenrechtliche Schutzvorschrift des Art. 111 BayBG gestattet zwar die elektronische Verarbeitung und Nutzung einzelner Personalaktendaten – beispielsweise in Personalverwaltungssystemen –, nicht jedoch die Führung des gesamten Personalakts in elektronischer Form.

Vor diesem Hintergrund habe ich für den Fall, dass trotz meiner prinzipiellen Bedenken an der Einführung der elektronischen Personalakte im Freistaat Bayern festgehalten wird, das innerhalb der Staatsregierung für das öffentliche Dienstrecht federführende **Staatsministerium der Finanzen, für Landesentwicklung und Heimat nachdrücklich dazu aufgefordert**, eine den Geboten der Normenklarheit und Normenbestimmtheit genügende gesetzliche Rechtsgrundlage für die elektronische Personalaktenführung im bayerischen Personalaktenrecht auf den Weg zu bringen.

In diesem Zusammenhang habe ich – da bei einer elektronischen Personalaktenführung die Risiken für das Persönlichkeitsrecht der Betroffenen erheblich ansteigen können – das Staatsministerium zudem darauf hingewiesen, dass **auch die notwendigen flankierenden Sicherungsmaßnahmen vom Gesetzgeber selbst angeordnet** werden müssen. Dazu gehört zum einen das gesetzliche **Verbot inhaltsgleicher „Hybrid-Akten“**, also das gesetzliche Verbot der parallelen Führung von inhaltsgleichen Papier- und elektronischen Personalakten(teilen). Zum anderen sind die notwendigen technischen und organisatorischen **Maßnahmen zur**

Gewährleistung der Integrität, Authentizität und Beweiskraft der elektronischen Personalakte zumindest in der Gesetzesbegründung ausdrücklich festzulegen.

Meinen zentralen Datenschutzforderungen wurde im Wesentlichen durch § 4 Nr. 1 des „Gesetzes zur Änderung des Leistungslaufbahngesetzes und anderer Rechtsvorschriften“ vom 22.05.2013 (GVBl Seite 301) Rechnung getragen. Im Einzelnen:

– Der bayerische Gesetzgeber hat durch Anfügung eines neuen zweiten Halbsatzes im Gesetzestext des **Art. 104 Abs. 1 Satz 1 BayBG** eine **ausdrückliche gesetzliche Rechtsgrundlage für die elektronische Personalakte** geschaffen.

– Zudem hat der bayerische Gesetzgeber die **Unzulässigkeit der parallelen Vorhaltung und Führung inhaltsgleicher Personalakten(teile) sowohl in elektronischer als auch in papiergebundener Form** (inhaltsgleiche „Hybrid-Akte“) durch Einfügung des neuen **Art. 104 Abs. 1 Satz 5 BayBG** im Gesetz selbst ausdrücklich verankert.

  Doppelte Datenhaltungen – und noch dazu in verschiedenen Medien – erhöhen stets die Gefahr unzulässiger Datenzugriffe. Diese Gefahr muss im Anwendungsbereich des Personalaktengeheimnisses, welches besonders sensible und daher auch besonders schutzwürdige Daten gegen unberechtigte Kenntnisnahmen absichern soll, schon von vornherein wirksam ausgeschlossen werden.

Art. 104 BayBG Gliederung und Gestaltung von Personalakten
(1) [1]Die Personalakte kann nach sachlichen Gesichtspunkten in Grundakte und Teilakten gegliedert und in Teilen oder vollständig elektronisch geführt werden. [2]Teilakten können bei der für den betreffenden Aufgabenbereich zuständigen Behörde geführt werden. [3]Nebenakten (Unterlagen, die sich auch in der Grundakte oder in Teilakten befinden) dürfen nur geführt werden, wenn die personalverwaltende Behörde nicht zugleich Beschäftigungsbehörde ist oder wenn mehrere personalverwaltende Behörden zuständig sind; sie dürfen nur solche Unterlagen enthalten, deren Kenntnis zur rechtmäßigen Aufgabenerledigung der betreffenden Behörde erforderlich ist. [4]In der Grundakte ist ein vollständiges Verzeichnis aller Teil- und Nebenakten aufzunehmen. [5]Wird die Personalakte nicht vollständig in Schriftform oder vollständig elektronisch geführt, legt die personalverwaltende Behörde jeweils schriftlich fest, welche Teile in welcher Form geführt werden, und nimmt dies in das Verzeichnis nach Satz 4 auf.

– Schließlich wurde in der **Gesetzesbegründung** (siehe Landtags-Drucksache 16/15832, Seite 16) ausdrücklich klargestellt, dass **an die elektronische Personalaktenführung hohe technische und organisatorische Anforderungen** zu stellen sind.

  Besonderer Wert ist hierbei auf ein **manipulationssicheres Einscannen von papiergebundenen Personalakten** zu legen. Es muss sichergestellt sein, dass die in der elektronischen Personalakte gespeicherten Dokumente auch tatsächlich mit den Originaldokumenten übereinstimmen.

  Zudem sind insbesondere die informationstechnischen Schutzziele der In-

tegrität und der Authentizität zu erreichen sowie der Beweiswert jedes gespeicherten elektronischen Dokuments zu gewährleisten. Dazu ist jedes gespeicherte elektronische Personalaktendokument zumindest mit der fortgeschrittenen elektronischen Signatur zu signieren. Vorzugswürdig ist es aus heutiger Sicht jedoch, **jedes gespeicherte elektronische Personalaktendokument mit der qualifizierten elektronischen Signatur** nach dem Signaturgesetz **zu versehen**, welche die Identifizierung der Person des Signaturschlüsselinhabers ermöglicht. Sobald die technischen und organisatorischen Voraussetzungen hierfür unter wirtschaftlich vertretbaren Bedingungen geschaffen werden können, stellt die Gesetzesbegründung daher klar, dass statt der fortgeschrittenen ausschließlich eine qualifizierte elektronische Signatur vorzunehmen ist. Gerade letztgenannte **ausdrückliche Verpflichtung** ist aus Datenschutzsicht besonders zu begrüßen.

Die gesetzliche Regelung der elektronischen Personalakte in **Art. 104 BayBG** ist mit Wirkung vom **01.01.2013 in Kraft getreten**.

11.2 Adressenweitergabe an Versicherungen

In den vergangenen Jahren haben mich **vereinzelt Beschwerden über die missbräuchliche Weitergabe von Adressdaten** (angehender) bayerischer öffentlicher Bediensteter erreicht. Dabei äußerten die Beschwerdeführer den Verdacht, dass Beschäftigte von personalverwaltenden Behörden ihre privaten Kommunikationsdaten an Versicherungen oder Versicherungsvermittlungen weitergegeben hätten. Diese Vermutung wurde regelmäßig mit einer zeitlichen Nähe der Kontaktaufnahme durch eine Versicherungsgesellschaft oder einen Versicherungsvermittler zu einer vorangegangenen Bewerbung bei der öffentlichen Hand begründet.

Konkrete Belege für eine Datenweitergabe aus dem Bereich bestimmter bayerischer öffentlicher Stellen konnte ich jedoch bislang – trotz intensiver Bemühungen um Sachverhaltsaufklärung – **in keinem Fall** erlangen. Die Aufdeckung eines möglichen Fehlverhaltens einzelner Beschäftigter wird insbesondere dadurch erschwert, dass die – als Privatunternehmen ohnehin nicht meiner Datenschutzkontrolle unterliegenden – Versicherungen über die Datenherkunft nur ausweichende Auskünfte geben. Regelmäßig wird etwa behauptet, die Adressdaten seien von anderen Schülern, Studenten, Referendaren, Kollegen oder Bekannten „auf Empfehlung“ weitergegeben worden. Auch habe ich nicht feststellen können, dass sich Vorwürfe gegen bestimmte personalverwaltende Behörden häuften.

Mangels tatsachengestützter Anhaltspunkte war mir daher ein **gezieltes, Erfolg versprechendes datenschutzrechtliches Tätigwerden** gegenüber einzelnen bayerischen öffentlichen Stellen **bisher nicht möglich**.

Im Berichtszeitraum hat nunmehr die **Presse** eingehend darüber berichtet, dass aus dem Behördenbereich – angeblich bundesweit und über Jahre hinweg – unbefugt Personaldaten, insbesondere Adress- und sonstige private Kommunikationsdaten (angehender) öffentlicher Bediensteter an Versicherungen und Versicherungsvermittlungen weitergegeben worden seien. In diesem Zusammenhang stand auch der **Vorwurf** im Raum, **Beschäftigte bayerischer öffentlicher Stellen hätten Adressdaten (angehender) bayerischer öffentlicher Bediensteter an Versicherungen verkauft.** Konkrete und hinreichende Anhaltspunkte für

Datenschutzverstöße bestimmter bayerischer öffentlicher Stellen waren allerdings auch diesen Presseberichten leider nicht zu entnehmen.

Bei den **Adress- und sonstigen privaten Kommunikationsdaten** gegenwärtiger wie angehender bayerischer öffentlicher Bediensteter handelt es sich um **sensible, dem Personalaktengeheimnis unterliegende Personalaktendaten**, die von den bayerischen öffentlichen Stellen vertraulich zu behandeln sind (siehe im Einzelnen § 50 Beamtenstatusgesetz – BeamtStG – in Verbindung mit Art. 102 ff. Bayerisches Beamtengesetz – BayBG). Insbesondere dürfen entsprechende Auskünfte an Dritte nur mit Einwilligung des Beamten oder der Beamtin erteilt werden, es sei denn, dass die Abwehr einer erheblichen Beeinträchtigung des Gemeinwohls oder der Schutz berechtigter, höherrangiger Interessen des Dritten die Auskunftserteilung zwingend erfordert; in diesen – sehr eng begrenzten – Ausnahmefällen sind Inhalt und Empfänger der Auskunft dem Beamten oder der Beamtin schriftlich mitzuteilen (siehe Art. 108 Abs. 2 BayBG). **Ohne Einwilligung** der Betroffenen ist die **Weitergabe** von Adress- und sonstigen privaten Kommunikationsdaten gegenwärtiger wie angehender bayerischer öffentlicher Bediensteter **durch bayerische öffentliche Stellen an Versicherungen und Versicherungsvermittlungen** somit **unzulässig**.

Art. 108 BayBG Vorlage von Personalakten und Auskunft aus Personalakten
(2) [1]Auskünfte an Dritte dürfen nur mit Einwilligung des Beamten oder der Beamtin erteilt werden, es sei denn, dass die Abwehr einer erheblichen Beeinträchtigung des Gemeinwohls oder der Schutz berechtigter, höherrangiger Interessen des Dritten die Auskunftserteilung zwingend erfordert. [2]Inhalt und Empfänger der Auskunft sind dem Beamten oder der Beamtin schriftlich mitzuteilen.

Die **Achtung des Personalaktengeheimnisses** ist mir ebenso wie die **Wahrung der Datenschutzrechte** aller gegenwärtigen wie angehenden bayerischen öffentlichen Bediensteten ein **besonderes Anliegen**. Unter Bezugnahme auf die Presseberichterstattung habe ich deshalb das innerhalb der Staatsregierung für das öffentliche Dienstrecht in Bayern federführende **Staatsministerium der Finanzen, für Landesentwicklung und Heimat gebeten, alle geeigneten Maßnahmen zu ergreifen**, um die bayerischen öffentlichen Stellen für die grundlegende Bedeutung des Personalaktengeheimnisses zu sensibilisieren. Zudem habe ich das Staatsministerium gebeten, alle geeigneten Maßnahmen zu ergreifen, um das verfassungsrechtlich in Art. 1 Abs. 1 in Verbindung mit Art. 2 Abs. 1 Grundgesetz garantierte Grundrecht auf informationelle Selbstbestimmung aller gegenwärtigen wie angehenden bayerischen öffentlichen Bediensteten vor der unzulässigen Weitergabe ihrer personenbezogenen Daten durch bayerische öffentliche Stellen wirkungsvoll zu schützen.

Das **Staatsministerium** hat meiner Bitte umgehend entsprochen und mit Rundschreiben vom 14.02.2014 (Az.: 21-P 1060/1-023-47691/13) **alle staatlichen obersten Dienstbehörden** unter Hinweis auf die beamten-, disziplinar-, straf- und datenschutzrechtliche Rechtslage **für die Problematik sensibilisiert** und gebeten, alle Beschäftigten im jeweiligen Geschäftsbereich entsprechend zu informieren. Ebenfalls im Februar 2014 hat das Staatsministerium **die bayerischen kommunalen Spitzenverbände und die Spitzenorganisationen der zuständigen Gewerkschaften und Berufsverbände in Bayern** gebeten, die jeweiligen Mitglieder auf die Sensibilität und die Vertraulichkeit von Personaldaten aufmerksam zu machen.

Aufgrund der Presseberichterstattung hat sich **auch der Bayerische Landtag** – ebenfalls in übergreifender Form – **mit der vorliegenden Thematik befasst** (siehe insbesondere Landtags-Drucksache 17/705).

11.3 Nochmals: Datenschutz beim Betrieblichen Eingliederungsmanagement

Nach § 84 Abs. 2 Sozialgesetzbuch Neuntes Buch – Rehabilitation und Teilhabe behinderter Menschen – (SGB IX) ist der Arbeitgeber verpflichtet, allen Beschäftigten, die innerhalb eines Jahres länger als sechs Wochen ununterbrochen oder wiederholt arbeitsunfähig sind, ein **Betriebliches Eingliederungsmanagement (BEM)** anzubieten. Diese Verpflichtung besteht sowohl für private wie für öffentliche Arbeitgeber; im öffentlichen Dienst sind davon neben den Tarifbeschäftigten auch die Beamtinnen und Beamten betroffen. Das BEM umfasst **alle Aktivitäten, Maßnahmen und Leistungen**, die im Einzelfall **zur Wiedereingliederung nach längerer Arbeitsunfähigkeit** erforderlich sind. Ziele des BEM sind es, durch Einleitung rehabilitierender oder präventiver Maßnahmen vorhandene Arbeitsunfähigkeiten zu überwinden, erneuten Arbeitsunfähigkeiten vorzubeugen und den Arbeitsplatz zu sichern bzw. Berufs-/Dienstunfähigkeiten zu vermeiden.

§ 84 SGB IX Prävention
(2) [1]Sind Beschäftigte innerhalb eines Jahres länger als sechs Wochen ununterbrochen oder wiederholt arbeitsunfähig, klärt der Arbeitgeber mit der zuständigen Interessenvertretung im Sinne des § 93, bei schwerbehinderten Menschen außerdem mit der Schwerbehindertenvertretung, mit Zustimmung und Beteiligung der betroffenen Person die Möglichkeiten, wie die Arbeitsunfähigkeit möglichst überwunden werden und mit welchen Leistungen oder Hilfen erneuter Arbeitsunfähigkeit vorgebeugt und der Arbeitsplatz erhalten werden kann (betriebliches Eingliederungsmanagement). [2]Soweit erforderlich wird der Werks- oder Betriebsarzt hinzugezogen. [3]Die betroffene Person oder ihr gesetzlicher Vertreter ist zuvor auf die Ziele des betrieblichen Eingliederungsmanagements sowie auf Art und Umfang der hierfür erhobenen und verwendeten Daten hinzuweisen. [4]Kommen Leistungen zur Teilhabe oder begleitende Hilfen im Arbeitsleben in Betracht, werden vom Arbeitgeber die örtlichen gemeinsamen Servicestellen oder bei schwerbehinderten Beschäftigten das Integrationsamt hinzugezogen. [5]Diese wirken darauf hin, dass die erforderlichen Leistungen oder Hilfen unverzüglich beantragt und innerhalb der Frist des § 14 Abs. 2 Satz 2 erbracht werden. [6]Die zuständige Interessenvertretung im Sinne des § 93, bei schwerbehinderten Menschen außerdem die Schwerbehindertenvertretung, können die Klärung verlangen. [7]Sie wachen darüber, dass der Arbeitgeber die ihm nach dieser Vorschrift obliegenden Verpflichtungen erfüllt.

Regelmäßig fallen bei der Durchführung eines BEM besonders sensible Personalaktendaten im Sinne der § 50 Beamtenstatusgesetz, Art. 102 ff. Bayerisches Beamtengesetz wie auch Gesundheitsdaten im Sinne des Art. 15 Abs. 7 BayDSG in großem Umfang an. Die hier zu beachtenden **datenschutzrechtlichen Anforderungen** habe ich ebenso wie den **BEM-Leitfaden und** das **BEM-Informationsfaltblatt** des Staatsministeriums der Finanzen, für Landesentwicklung und Heimat bereits in meinem 25. Tätigkeitsbericht 2012 unter Nr. 11.2 eingehend erläutert. An diesen Ausführungen halte ich weiterhin fest.

Auch im Berichtszeitraum haben mich Fragen der datenschutzkonformen Gestaltung des BEM in der bayerischen staatlichen und kommunalen Verwaltung vor Ort intensiv beschäftigt. Im Vordergrund steht immer wieder die Problematik, **welche**

Beschäftigtendaten die Dienststelle in diesem Zusammenhang ohne Einwilligung der Betroffenen an die Personal- und an die Schwerbehindertenvertretung weitergeben darf. Nach § 84 Abs. 2 Satz 7 SGB IX haben die Personalvertretung und bei Schwerbehinderten die Schwerbehindertenvertretung nämlich darüber zu wachen, dass der Arbeitgeber seine Pflicht zur Anbietung und gegebenenfalls zur Durchführung eines BEM erfüllt. Daher ist der Personal- bzw. der Schwerbehindertenvertretung insoweit regelmäßig – etwa im „Monatsgespräch" gemäß Art. 67 Abs. 1 Bayerisches Personalvertretungsgesetz – zu unterrichten. Aus datenschutzrechtlicher Sicht sollte dabei – in anonymisierter Form – insbesondere dargestellt werden, in wie vielen Fällen die Voraussetzungen für die Durchführung eines BEM vorgelegen haben, sowie ob und mit welchen Ergebnissen ein BEM durchgeführt wurde. In Rechtsprechung und Praxis ist allerdings höchst umstritten, ob die Dienststelle die Personal- und die Schwerbehindertenvertretung zur Erfüllung dieser Überwachungsaufgabe über Beschäftigte, die die Voraussetzungen für ein BEM erfüllen, auch ohne deren Zustimmung namentlich informieren darf.

Zu dieser Problematik nehme ich aus datenschutzrechtlicher Sicht wie folgt Stellung:

11.3.1 Namentliche Information der Personalvertretung

Für die Beurteilung der Reichweite des Informationsanspruchs bayerischer Personalvertretungen ist gemäß Art. 81 Abs. 2 Satz 2 Bayerisches Personalvertretungsgesetz (BayPVG) die Rechtsprechung des Bayerischen Verwaltungsgerichtshofs maßgeblich. Dieser hat mit Beschluss vom 12.06.2012 (Az.: 17 P 11.1140) im Anschluss an seinen Beschluss vom 30.04.2009 (Az.: 17 P 08.3389) entschieden, dass Art. 69 Abs. 2 Sätze 1 und 2 BayPVG in Verbindung mit § 84 Abs. 2 Satz 7 Sozialgesetzbuch Neuntes Buch – Rehabilitation und Teilhabe behinderter Menschen (SGB IX) der Personalvertretung kein Recht verleihen, vom Leiter einer Dienststelle ohne Einwilligung der Betroffenen die Bekanntgabe der Namen der Personen verlangen zu können, denen ein Betriebliches Eingliederungsmanagement (BEM) angeboten wurde. Dies wird damit begründet, dass dem Grundrecht der Betroffenen auf informationelle Selbstbestimmung nach Art. 1 Abs. 1 in Verbindung mit Art. 2 Abs. 1 Grundgesetz auch in der ersten Phase des BEM, dem Herantreten der Dienststelle an die jeweils in Frage kommende Person (§ 84 Abs. 2 Satz 3 SGB IX), der Vorrang gegenüber den Informationsinteressen der Personalvertretung gebührt.

An meiner im 25. Tätigkeitsbericht 2012 unter Nr. 11.2 geäußerten Auffassung halte ich daher ungeachtet des Beschlusses des Bundesverwaltungsgerichts vom 04.09.2012 (Az.: 6 P 5.11) weiterhin fest. Das Bundesverwaltungsgericht ist nicht zuständig für die Kontrolle der Anwendung des bayerischen Personalvertretungsrechts, da insoweit gemäß Art. 81 Abs. 2 Satz 2 BayPVG die Entscheidung des Bayerischen Verwaltungsgerichtshofs endgültig ist.

Dementsprechend sieht der mit mir abgestimmte, im Bayerischen Behördennetz unter www.stmf.bybn.de/default.asp?url=personal%2Fpe%2Feingliederungsmanagement%2F&item=209 abrufbare „Leitfaden Betriebliches Eingliederungsmanagement § 84 Abs. 2 SGB IX" des Staatsministeriums der Finanzen, für Landesentwicklung und Heimat unter Abschnitt II. Nr. 6.1 folgendes Vorgehen vor:

„ … Wenn kein besonderer Anlass in Gestalt eines begründeten Hinweises auf die nicht vollständige Erfüllung der Pflichten des Dienstherrn/Arbeitgebers vorliegt, ist es nach diesen Vorschriften ausreichend, wenn dem Personalrat und der Schwerbehindertenvertretung regelmäßig (z.B. im Monatsgespräch nach Art. 67 BayPVG) berichtet wird. Hierbei sollte – jedoch ohne Namensnennung – dargestellt werden, in wie vielen Fällen die Voraussetzungen für die Durchführung eines Betrieblichen Eingliederungsmanagements vorlagen, sowie ob und mit welchen Ergebnissen ein Betriebliches Eingliederungsmanagement durchgeführt wurde. Jede Weitergabe personenbezogener Daten an die Interessensvertretungen bedarf der Zustimmung der betroffenen Person."

11.3.2 Namentliche Information der Schwerbehindertenvertretung

Anders stellt sich die Rechtslage jedoch hinsichtlich des Informationsanspruchs der Schwerbehindertenvertretung im Rahmen eines Betriebliches Eingliederungsmanagements (BEM) dar. Die Rechtsstellung der Schwerbehindertenvertretung bemisst sich nach §§ 93 ff. Sozialgesetzbuch Neuntes Buch – Rehabilitation und Teilhabe behinderter Menschen (SGB IX), mithin nach Bundesrecht. Zuständig zur Entscheidung von Streitigkeiten zwischen Dienststelle und Schwerbehindertenvertretung über den Umfang des Informationsanspruchs nach § 95 Abs. 1 Satz 2 Nr. 1 in Verbindung mit Abs. 2 Satz 1 SGB IX im Rahmen eines BEM sind – anders als bei den Personalvertretungen – nicht die Verwaltungsgerichte, sondern gemäß § 2a Abs. 1 Nr. 3a Arbeitsgerichtsgesetz die Gerichte für Arbeitssachen. Aussagen zum konkreten Umfang dieses Informationsanspruchs im Rahmen eines BEM hat die höchstrichterliche Rechtsprechung bisher, soweit ersichtlich, zwar noch nicht getroffen. Nach meiner derzeitigen rechtlichen Einschätzung kommt in diesem Zusammenhang allerdings der Auslegung des § 84 Abs. 2 Satz 7 SGB IX durch das Bundesarbeitsgericht entscheidende Bedeutung zu.

Innerhalb der Arbeitsgerichtsbarkeit ist inzwischen höchstrichterlich entschieden, dass der **Arbeitgeber auch ohne Zustimmung der Betroffenen verpflichtet** ist, dem Betriebsrat die **Arbeitnehmer namentlich zu benennen**, die innerhalb eines Jahres länger als sechs Wochen ununterbrochen oder wiederholt arbeitsunfähig waren (siehe den Beschluss des **Bundesarbeitsgerichts** vom 07.02.2012, Az.: 1 ABR 46/10). Ich halte es daher für durchaus wahrscheinlich, dass ein mit der Frage des Umfangs des Informationsanspruchs bayerischer Schwerbehindertenvertretungen im Rahmen eines BEM befasstes Arbeitsgericht diese auf Betriebsräte bezogene Rechtsprechung auf Schwerbehindertenvertretungen übertragen würde. Für diese Einschätzung spricht insbesondere, dass das durch § 95 Abs. 2 Satz 1 SGB IX der **Schwerbehindertenvertretung gewährte personenbezogene Unterrichtungs- und Anhörungsrecht** vom Umfang her über den in § 80 Abs. 2 Sätze 1 und 2 Betriebsverfassungsgesetz niedergelegten Unterrichtungsanspruchs des Betriebsrats – und im Übrigen auch **über den Unterrichtungsanspruch des Personalrats** nach Art. 69 Abs. 2 Sätze 1 und 2 Bayerisches Personalvertretungsgesetz – **hinausgeht**.

Der bereits oben erwähnte **„Leitfaden Betriebliches Eingliederungsmanagement § 84 Abs. 2 SGB IX"** des Staatsministeriums der Finanzen, für Landesentwicklung und Heimat sieht daher unter Abschnitt II. Nr. 6.2 **folgendes Vorgehen** vor:

„Die Schwerbehindertenvertretung ist bei schwerbehinderten und gleichgestellten Menschen zusätzlich über den Erstkontakt bzw. das Angebot eines Betrieblichen Eingliederungsmanagements zu informieren."

Zudem enthält das dem Leitfaden angehängte „Musteranschreiben zum BEM-Erstkontakt/BEM-Angebot im Falle einer noch andauernden Abwesenheit des/der Bediensteten" folgende

„Option bei schwerbehinderten Menschen:
Die örtliche Schwerbehindertenvertretung erhält einen Abdruck dieses Schreibens. Über eine weitergehende Beteiligung der Schwerbehindertenvertretung entscheiden jedoch ausschließlich Sie. Sollten noch Unklarheiten bestehen, können Sie sich auch vertrauensvoll an die Schwerbehindertenvertretung wenden."

11.3.3 Ergebnis

Im Ergebnis ist der **Umfang des Unterrichtungsanspruchs** von Personalvertretung einerseits und von Schwerbehindertenvertretung andererseits im Rahmen eines Betrieblichen Eingliederungsmanagements **nicht deckungsgleich**. In Bezug auf **dieselben Beschäftigten** können sich hier durchaus **Unterschiede** ergeben.

11.4 Einstellungsuntersuchung von Beamtenbewerbern

Nach der gesetzlichen Regelung des § 9 Beamtenstatusgesetz (BeamtStG) sind beamtenrechtliche Ernennungen ausschließlich anhand der Kriterien der Eignung, Befähigung und fachlichen Leistung vorzunehmen. Zur **Feststellung der gesundheitlichen Eignung** ist eine **Einstellungsuntersuchung** unerlässlich, welche in der Regel dem Gesundheitsamt obliegt (siehe die Aufgabenzuweisungsnorm des Art. 11 Gesundheitsdienst- und Verbraucherschutzgesetz). In diesem Zusammenhang wenden sich immer wieder Beamtenbewerber – insbesondere mit Fragen zum Umfang der Einstellungsuntersuchung, zur Auskunftserteilung über Vorerkrankungen und zur Entbindung von der Schweigepflicht – an mich. Aus datenschutzrechtlicher Sicht gebe ich dazu folgende Hinweise:

Angaben zur Gesundheit gehören zu den besonders sensiblen personenbezogenen Daten und unterliegen daher einem **besonderen Schutz** (siehe auch Art. 15 Abs. 7 BayDSG). Das nach Art. 33 Abs. 2 Grundgesetz (GG) geschützte Interesse des Dienstherrn, die gesundheitliche Eignung von Bewerbern für die Übernahme in das Beamtenverhältnis festzustellen, kann daher **nur unter strenger Wahrung des Verhältnismäßigkeitsprinzips** einen **Zugriff** auf diese Daten rechtfertigen.

Art. 33 GG
(2) Jeder Deutsche hat nach seiner Eignung, Befähigung und fachlichen Leistung gleichen Zugang zu jedem öffentlichen Amte.

Die **gesetzliche Befugnis des Dienstherrn, Gesundheitsdaten von Beamtenbewerbern zu erheben**, ergibt sich **aus Art. 102 Satz 1 Bayerisches Beamtengesetz.** Danach darf der Dienstherr personenbezogene Daten erheben, soweit dies u.a. zur Begründung, Durchführung, Beendigung oder Abwicklung des Dienstverhältnisses erforderlich ist. Hierunter fällt auch das Recht des Dienstherrn,

Bewerber nach gesundheitlichen Beeinträchtigungen zu fragen, die der Aufnahme der angestrebten Tätigkeit entgegenstehen könnten. **Gesundheitsfragen** im Rahmen einer Einstellungsuntersuchung – **etwa zu Vorerkrankungen** – sind somit aus datenschutzrechtlicher Sicht nur **zulässig, wenn und soweit** die angeforderten Informationen **zur Beurteilung der gesundheitlichen Eignung erforderlich** sind.

Gleichzeitig begründet das in Art. 33 Abs. 2 GG verankerte Recht des Dienstherrn, die gesundheitliche Eignung des Beamtenbewerbers zu prüfen, eine **korrespondierende Mitwirkungsobliegenheit für den Bewerber** (vgl. Oberverwaltungsgericht Mecklenburg-Vorpommern, Beschluss vom 23.04.1998, Az.: 2 M 168/97). Ein Bewerber kann danach zwar selbst entscheiden, ob er an einer Einstellungs- oder Folgeuntersuchung teilnimmt, mit der Weitergabe der Untersuchungsergebnisse an die Einstellungsbehörde einverstanden ist oder die untersuchenden Ärzte von der Schweigepflicht entbindet. Eine einmal erteilte **Entbindung von der Schweigepflicht** kann auch wieder mit Wirkung für die Zukunft zurückgenommen werden. Eine verweigerte Mitwirkung kann jedoch – soweit sie zur Aufklärung des Sachverhalts erforderlich gewesen wäre – von der Einstellungsbehörde zum Nachteil des Bewerbers dahin verwertet werden, dass die gesundheitliche Eignung als nicht gewährleistet angesehen wird (siehe hierzu Weiß/Niedermaier/Summer/Zängl, Beamtenrecht in Bayern, Band I, § 37 BeamtStG Anm. 211). Der Bewerber trägt insoweit die Beweislast. Der konkrete Umfang der Mitwirkungsobliegenheit hängt von den jeweiligen Umständen des Einzelfalls ab.

Ob die gesundheitliche Eignung bejaht werden kann, steht im gerichtlich nur beschränkt überprüfbaren Beurteilungsspielraum der Einstellungsbehörde (vgl. Bundesverwaltungsgericht, Urteil vom 15.06.1989, Az.: 2 A 3/86, m.w.N.). Zum Schutz des Persönlichkeitsrechts des Bewerbers **erhält die Einstellungsbehörde** vom Gesundheitsamt hierfür grundsätzlich **nur ein Gesundheitszeugnis mit** einer zusammenfassenden Beurteilung über das **Ergebnis der Einstellungsuntersuchung, während** die Beurteilungsgrundlagen mit dem **genauen Untersuchungsbefund beim Gesundheitsamt verbleiben** (siehe Weiß/Niedermaier/Summer/Zängl, a.a.O., § 9 BeamtStG Anm. 44). Dies gilt vor allem dann, wenn keine Zweifel an der gesundheitlichen Eignung vorhanden sind. Bestehen allerdings Bedenken gegen die gesundheitliche Eignung, müssen diese auch in dem zusammenfassenden Bericht soweit konkretisiert werden, dass die Einstellungsbehörde darüber befinden kann, ob ergänzende ärztliche Untersuchungen erforderlich sind, ob trotz der getroffenen medizinischen Feststellungen die gesundheitliche Eignung noch bejaht werden kann oder ob die gesundheitliche Eignung nicht mehr gewährleistet ist.

Ob und ggf. welche **gesonderten Untersuchungen hinsichtlich bestimmter Erkrankungen** oder Risikofaktoren vorzunehmen sind, steht grundsätzlich **im Ermessen des Dienstherrn.** Der Dienstherr muss aber stets zwischen dem eigenen Informationsinteresse und den schutzwürdigen Belangen des Bewerbers abwägen. Eine **Grenze für gezielte Untersuchungen** ist jedenfalls dort zu ziehen, wo sie **erheblich in die Intimsphäre eingreifen** würden (beispielsweise bei einer **Genomanalyse** zur Ermittlung veranlagungsbedingter Risiken für künftige Erkrankungen). In diesem Zusammenhang möchte ich auch auf meine Ausführungen im 24. Tätigkeitsbericht 2010 unter Nr. 11.3 hinweisen, in dem ich mich zur Zulässigkeit von **Drogentests** bei der Einstellung neuer Mitarbeiter durch ein öffentliches Wettbewerbsunternehmen eingehend geäußert habe.

11.5 Datenschutz beim besonderen Auswahlverfahren für die Einstellung in die Finanzverwaltung

Jeder Deutsche hat gemäß Art. 33 Abs. 2 Grundgesetz (GG) nach seiner Eignung, Befähigung und fachlichen Leistung gleichen Zugang zu jedem öffentlichen Amte. Dieses verfassungsrechtlich verankerte **Prinzip der Bestenauslese** ist insbesondere von Bedeutung **für die Berufung in ein Beamtenverhältnis**.

Zur Konkretisierung dieses auch in Art. 94 Abs. 2 Satz 1 Verfassung des Freistaates Bayern niedergelegten Verfassungsgrundsatzes hat der Landtag in Art. 22 Abs. 1 Satz 2 Alternative 2 Gesetz über die Leistungslaufbahn und die Fachlaufbahnen der bayerischen Beamten und Beamtinnen (Leistungslaufbahngesetz – LlbG) vorgesehen, dass das **Vorliegen der persönlichen Eignung für öffentliche Ämter**, wozu vornehmlich soziale Kompetenz, Kommunikations- und Organisationskompetenz zählen, **auch Gegenstand eines gesonderten wissenschaftlich fundierten Auswahlverfahrens, insbesondere eines Assessment-Centers oder eines Strukturierten Interviews,** sein kann. Nähere Einzelheiten, etwa über die Anforderungen an die Mitglieder der Auswahlkommissionen oder das zu prüfende Anforderungsprofil, hat der Gesetzgeber maßgeblich in Art. 22 Abs. 8 LlbG festgelegt.

Art. 22 LlbG Arten der Prüfungen, Prüfungsgrundsätze, Prüfungsordnungen, besondere Auswahlverfahren
(1) [1]Die Prüfungen sind Einstellungs-, Zwischen- und Qualifikationsprüfungen. [2]Das Vorliegen der persönlichen Eignung für öffentliche Ämter, insbesondere soziale Kompetenz, Kommunikationskompetenz sowie Organisationskompetenz kann Gegenstand von Prüfungen nach Satz 1 oder eines gesonderten wissenschaftlich fundierten Auswahlverfahrens, insbesondere eines Assessment-Centers oder eines strukturierten Interviews, sein (Abs. 8).
(8) [1]Wird ein Auswahlverfahren nach Abs. 1 Satz 2 Alternative 2 durchgeführt, setzt die Einstellung dessen Bestehen voraus. [2]Zuständig für die Durchführung des Verfahrens ist die gemäß Art. 18 BayBG für die Ernennung nach Art. 2 Abs. 1 zuständige Behörde. [3]Diese bestimmt die Mitglieder der Auswahlkommission. [4]Es können nur Beamte und Beamtinnen als Kommissionsmitglieder bestimmt werden, die für die Durchführung des Auswahlverfahrens geschult wurden und mindestens dem von den Bewerbern bzw. Bewerberinnen angestrebten Eingangsamt angehören; im nichtstaatlichen Bereich können auch Tarifbeschäftigte bestimmt werden, die neben der in Halbsatz 1 genannten Schulung mindestens über eine dem angestrebten Eingangsamt entsprechende Qualifikation verfügen. [5]Das zu prüfende Anforderungsprofil setzt die oberste Dienstbehörde fest. [6]Das Ergebnis des Auswahlverfahrens, „geeignet" oder „nicht geeignet", ist den Bewerbern und Bewerberinnen mitzuteilen; auf Verlangen der Bewerber oder Bewerberinnen ist das Ergebnis schriftlich zu begründen. [7]Das Auswahlverfahren nach Abs. 1 Satz 2 Alternative 2 kann einmal wiederholt werden. [8]Die obersten Dienstbehörden können mit Zustimmung des Landespersonalausschusses durch Rechtsverordnung, im nichtstaatlichen Bereich durch Satzung, von den Sätzen 1 bis 7 abweichende oder diese ergänzende Regelungen treffen.

Im Berichtszeitraum habe ich durch eine Eingabe davon Kenntnis erlangt, dass zu Beginn des Strukturierten Interviews im Rahmen des besonderen Auswahlverfahrens für die Einstellung in die Finanzverwaltung die **Lebensläufe aller Bewerberinnen und Bewerber in der Gruppe vorgestellt und sodann auch – durchaus kritisch – diskutiert werden**. Die Prüflinge erfahren auf diese Weise sensible und persönliche Daten ihrer Mitbewerber. Eine datenschutzgerechte Einwilligung der

Bewerber (vgl. Art. 15 Abs. 2 bis 4 und 7 BayDSG) – an deren Freiwilligkeit in Anbetracht der Bewerbungssituation ohnehin erhebliche Zweifel bestünden – wird dabei nicht eingeholt.

Im Zuge einer intensiven und langwierigen Diskussion habe ich das – innerhalb der Staatsregierung für das Dienstrecht federführende und damit auch vorbildhafte – Staatsministerium der Finanzen, für Landesentwicklung und Heimat mehrmals eindringlich darauf hingewiesen, dass das besondere Auswahlverfahren im Sinne des Art. 22 Abs. 1 Satz 2 Alternative 2 LlbG im Hinblick auf das Grundrecht jeder Bewerberin und jedes Bewerbers auf informationelle Selbstbestimmung (Art. 1 Abs. 1 in Verbindung mit Art. 2 Abs. 1 GG) so zu gestalten ist, dass die Prüflinge möglichst wenige Daten ihrer Mitbewerber erfahren. **Aus datenschutzrechtlicher Sicht** sind daher alle sensiblen und persönlichen Daten der Mitbewerber in einem individuellen Vorgespräch bzw. Nachgespräch zu klären. Sollten jedoch Teile des Strukturierten Interviews aus fachlichen Gründen zwingend in Gruppen durchzuführen sein, so **dürfen die Prüflinge nur die für die fachliche Auswahl unbedingt erforderlichen personenbezogenen Daten ihrer Mitbewerber erfahren**.

Das Staatsministerium hat sich zunächst auf den Standpunkt gestellt, dass die von mir kritisierte Ausgestaltung des Strukturierten Interviews so in **DIN 33430 „Anforderungen an Verfahren und deren Einsatz bei berufsbezogenen Eignungsbeurteilungen“** vorgesehen ist. Nach genauer Durchsicht dieser Norm musste ich das Staatsministerium allerdings darauf aufmerksam machen, dass die DIN 33430 gerade keine Aussage, Empfehlung oder gar Vorgabe enthält, bei Verfahren der berufsbezogenen Eignungsbeurteilung die Lebensläufe aller Bewerberinnen und Bewerber in der Gruppe vorzustellen und sodann auch zu diskutieren. Vielmehr **fordert** diese DIN sogar **ausdrücklich** in Nr. 7.4 sowie in Anhang B unter B.2, bei Verfahren der berufsbezogenen Eignungsbeurteilung **die Datenschutzvorschriften zu beachten und ein unberechtigtes Eindringen in die Privatsphäre zu vermeiden**. Im Übrigen würde auch eine rechtswidrige DIN die Finanzverwaltung im Hinblick auf die verfassungsrechtlich in Art. 20 Abs. 3 GG verankerte Bindung der Verwaltung an Gesetz und Recht nicht von der Einhaltung datenschutzrechtlicher Vorschriften entbinden. Ohnehin ist eine DIN-Zertifizierung des besonderen Auswahlverfahrens in Art. 22 Abs. 8 LlbG gesetzlich nicht vorgeschrieben.

Schließlich hat mir das Staatsministerium Ende des Jahres 2013 zugesagt, den Ablauf des Strukturierten Interviews im Rahmen des besonderen Auswahlverfahrens für die Einstellung in die Finanzverwaltung umzustellen und **die Vorstellung der Bewerberinnen und Bewerber sowie die Erörterung lebenslaufbezogener Daten nicht mehr in der Gruppe, sondern in Einzelgesprächen vorzunehmen**.

Auch künftig werde ich die Ausgestaltung gesonderter wissenschaftlich fundierter Auswahlverfahren nach Art. 22 Abs. 1 Satz 2 Alternative 2 LlbG aus Datenschutzsicht aufmerksam beobachten.

Schließlich möchte ich an dieser Stelle noch einmal ausdrücklich betonen, dass ich es **aus datenschutzrechtlicher Sicht generell** für **vorzugswürdig** halte, die **Auswahl der einzustellenden Bewerberinnen und Bewerber** nicht in Gruppen, sondern soweit wie möglich **in Einzelgesprächen** vorzunehmen.

11.6 Information des Dienstherrn über eine Kur

Kuren bringen es zumeist mit sich, dass Bedienstete für eine längere Zeit der Dienststelle fernbleiben. Auch während dieser Zeit obliegt es allerdings dem Dienstherrn, den ordnungsgemäßen Ablauf des Dienstbetriebs sicherzustellen. Um rechtzeitig die dazu notwendigen Vorkehrungen treffen zu können, hat der Dienstherr ein Interesse daran, schon möglichst frühzeitig – im Grunde bereits bei Beantragung – über das Kurvorhaben eines Bediensteten informiert zu werden. Eine derart frühzeitige Information liegt jedoch nicht im Interesse des Bediensteten: Wird die beantragte Kur nämlich von den jeweils zuständigen privaten und/oder öffentlichen Versicherungs-/Beihilfeträgern nicht bewilligt/anerkannt, hätte der Bedienstete seinem Dienstherrn ohne Not besonders sensible Gesundheitsdaten (siehe Art. 15 Abs. 7 BayDSG) offenbart.

Vor diesem Hintergrund hat mir eine bayerische Kommune die Frage vorgelegt, **zu welchem Zeitpunkt bayerische öffentliche Bedienstete ihren Dienstherrn über eine Kur informieren müssen.**

Für die datenschutzrechtliche Bewertung dieser Frage ist zunächst zwischen den nicht-verbeamteten Beschäftigten des bayerischen öffentlichen Dienstes einerseits und den bayerischen Beamtinnen und Beamten andererseits zu unterscheiden:

– Die **nicht-verbeamteten Beschäftigten** des bayerischen öffentlichen Dienstes sind bei der medizinischen Vorsorge und Rehabilitation nur **verpflichtet, dem Dienstherrn** den Zeitpunkt des Antritts der Maßnahme, die voraussichtliche Dauer und die Verlängerung der Maßnahme unverzüglich mitzuteilen sowie die **entsprechende (Bewilligungs-)Bescheinigung unverzüglich vorzulegen** (siehe § 9 Abs. 2 Gesetz über die Zahlung des Arbeitsentgelts an Feiertagen und im Krankheitsfall – EFZG – in Verbindung mit § 22 Tarifvertrag für den öffentlichen Dienst – Bereich der Vereinigung der kommunalen Arbeitgeberverbände – bzw. § 22 Tarifvertrag für den öffentlichen Dienst der Länder).

  Eine **Pflicht** der nicht-verbeamteten Beschäftigten **zur Information des Dienstherrn vor der Bewilligung** der Kur – etwa im Zeitpunkt der Beantragung beim Sozialversicherungsträger –, ist dagegen **weder im Gesetz noch im Tarifvertrag** vorgesehen.

  In Anbetracht der genannten gesetzlichen und tarifvertraglichen Regelungen halte ich **auch** die innerbehördliche Begründung einer solchen frühzeitigen Mitteilungspflicht **in** einer **Dienstanweisung oder in** einer **Dienstvereinbarung** (vgl. insoweit schon die Sperrvorschrift des Art. 73 Abs. 1 Satz 1 Halbsatz 1 Bayerisches Personalvertretungsgesetz) aus Datenschutzsicht **nicht** für **zulässig.**

§ 9 EFZG Maßnahmen der medizinischen Vorsorge und Rehabilitation
(2) Der Arbeitnehmer ist verpflichtet, dem Arbeitgeber den Zeitpunkt des Antritts der Maßnahme, die voraussichtliche Dauer und die Verlängerung der Maßnahme im Sinne des Absatzes 1 unverzüglich mitzuteilen und ihm
a) eine Bescheinigung über die Bewilligung der Maßnahme durch einen Sozialleistungsträger nach Absatz 1 Satz 1 oder

b) eine ärztliche Bescheinigung über die Erforderlichkeit der Maßnahme im Sinne des Absatzes 1 Satz 2
unverzüglich vorzulegen.

– Fordert ein bayerischer Dienstherr von seinen **Beamtinnen und Beamten** eine möglichst frühzeitige Information bei (der Beantragung) einer Kur, so erhebt er personenbezogene Daten im Sinne des Art. 102 Satz 1 Bayerisches Beamtengesetz (BayBG). Nach dieser Vorschrift ist eine Erhebung von Personalaktendaten allerdings **nur** zulässig, **soweit** dies zur Begründung, Durchführung, Beendigung oder Abwicklung des Dienstverhältnisses oder zur Durchführung organisatorischer, personeller und sozialer Maßnahmen, insbesondere auch zu Zwecken der Personalplanung und des Personaleinsatzes, **erforderlich** ist oder eine Rechtsvorschrift dies erlaubt.

Art. 102 BayBG Erhebung personenbezogener Daten
[1]Der Dienstherr darf personenbezogene Daten über Bewerber, Bewerberinnen, Beamte und Beamtinnen sowie ehemalige Beamte und Beamtinnen nur erheben, soweit dies zur Begründung, Durchführung, Beendigung oder Abwicklung des Dienstverhältnisses oder zur Durchführung organisatorischer, personeller und sozialer Maßnahmen, insbesondere auch zu Zwecken der Personalplanung und des Personaleinsatzes, erforderlich ist oder eine Rechtsvorschrift dies erlaubt.

Für die Zulässigkeit des Informationsverlangens des Dienstherrn kommt es daher nach Art. 102 Satz 1 BayBG entscheidend darauf an, ob – und vor allem wann – die Datenerhebung zur Durchführung organisatorischer und personeller Maßnahmen erforderlich ist. Hier ist das **Informationsinteresse des Dienstherrn** einerseits **mit dem Persönlichkeitsschutz der Beamtin oder des Beamten** andererseits **abzuwägen.**

Der Dienstherr hat sicherlich ein Interesse daran, möglichst frühzeitig – im Grunde bereits im Zeitpunkt der Beantragung – zu erfahren, dass eine Beamtin oder ein Beamter auf Grund einer Kur in absehbarer Zeit abwesend sein könnte, um entsprechende personelle und organisatorische (Vorbereitungs-)Maßnahmen treffen zu können. Andererseits ist aber zu bedenken, dass die Beamtin oder der Beamte hierbei besonders sensible Gesundheitsdaten (siehe Art. 15 Abs. 7 BayDSG) gegenüber dem Dienstherrn offenbaren muss. Insbesondere steht im Zeitpunkt der Beantragung einer Kur noch gar nicht fest, ob sie von den jeweils zuständigen privaten und/oder öffentlichen Versicherungs-/Beihilfeträgern überhaupt bewilligt/anerkannt wird und, wenn ja, wann die Kur – je nach den persönlichen Umständen der Beamtin oder des Beamten und je nach Auslastung der gewünschten Kureinrichtung – auch tatsächlich angetreten werden kann. Für den Fall, dass die beantragte Kur nicht bewilligt/anerkannt wird, hätte die Beamtin oder der Beamte somit bei einer frühzeitigen Information dem Dienstherrn besonders sensible Gesundheitsdaten offenbart, obwohl keine Notwendigkeit dazu bestanden hätte. Für den Fall, dass die Kur erst viel später angetreten werden kann, wäre jedenfalls eine derart vorzeitige Information des Dienstherrn nicht erforderlich gewesen.

Der bayerische Gesetzgeber hat diese Problematik erkannt und sowohl die Interessen der Beamtinnen und Beamten am Schutz ihrer Gesundheitsdaten als auch die Interessen der Dienstherrn an einer rechtzeitigen Disposition in § 30 Abs. 6 Satz 2 Nr. 3 Verordnung über die Beihilfefähigkeit von

Aufwendungen in Krankheits-, Geburts-, Pflege- und sonstigen Fällen (BayBhV) zu einem angemessenen Ausgleich gebracht. Diese Vorschrift besagt, dass für aktive Bedienstete **Beihilfe zu Heilkuren** u.a. **nur gewährt** wird, **wenn** die **Heilkur innerhalb eines im Anerkennungsbescheid unter Beachtung der dienstlichen Belange zu bestimmenden Zeitraums begonnen wird.** Nach Nr. 5 der Verwaltungsvorschriften zu § 30 Abs. 6 BayBhV beträgt dieser Zeitraum vier Monate nach Bekanntgabe des Anerkennungsbescheides, soweit amtsärztlich nichts anderes bestimmt ist. Eine **Information des Dienstherrn über eine beabsichtigte Kur** kann damit **erst nach Erhalt des Anerkennungsbescheides** gefordert werden.

§ 30 BayBhV Beihilfe bei Kuren
(6) … [2]Abweichend davon wird Beihilfe zu Heilkuren für aktive Bedienstete (§ 2 Abs. 1 Nr. 1) nur gewährt, wenn die Voraussetzungen des Satzes 1 Nrn. 1 und 2 vorliegen und

1. *durch amts- oder vertrauensärztliches Gutachten nachgewiesen ist, dass die Heilkur zur Wiederherstellung oder Erhaltung der Dienstfähigkeit erforderlich ist,*
2. *die Beihilfestelle die Beihilfefähigkeit vor Beginn der Heilkur anerkannt hat, und*
3. *die Heilkur innerhalb eines im Anerkennungsbescheid unter Beachtung der dienstlichen Belange zu bestimmenden Zeitraums begonnen wird.*

Durch diese Regelung ist nicht nur gewährleistet, dass – nach der Anerkennung der Kur durch den Beihilfeträger – der Beamtin oder dem Beamten ein angemessener zeitlicher Spielraum für den Beginn der Heilkur verbleibt, sondern auch, dass bei der Festlegung des konkreten Antrittszeitpunkts die Interessen des Dienstherrn gewahrt werden.

Vor dem aufgezeigten gesetzlichen und tarifvertraglichen Hintergrund müssen **im Ergebnis sowohl** die **nicht-verbeamteten Beschäftigten** des bayerischen öffentlichen Dienstes **als auch** die bayerischen **Beamtinnen und Beamten ihren Dienstherrn nicht schon bei der Beantragung, sondern erst nach der Bewilligung/Anerkennung über den beabsichtigten Beginn einer Kur unverzüglich informieren.**

11.7 Speicherung von Beschäftigtenbeschwerden beim Personalrat

Mit der Problematik der Aufbewahrung von personenbezogenen Beschäftigtendaten, die der Personalrat im Rahmen von Mitbestimmungsverfahren ohne Einwilligung der Betroffenen berechtigterweise erhalten hat, habe ich mich bereits in meinem 25. Tätigkeitsbericht 2012 unter Nr. 11.7 ausführlich befasst.

Ein Personalrat erkundigte sich nun bei mir, ob, inwieweit und wie lange er personenbezogene Beschäftigtendaten speichern darf, die er im Rahmen von Beschäftigtenbeschwerden erhalten hat. Schließlich gehört es gemäß Art. 69 Abs. 1 lit. c) Bayerisches Personalvertretungsgesetz (BayPVG) zu den **allgemeinen Aufgaben des Personalrats, Anregungen und Beschwerden von Beschäftigten entgegenzunehmen** und, falls sie berechtigt erscheinen, durch Verhandlung mit dem Leiter der Dienststelle auf ihre Erledigung hinzuwirken.

Dazu hat mir ein Personalratsmitglied folgenden Sachverhalt vorgetragen: Oftmals wendeten sich Beschäftigte mit ihren Anliegen schriftlich an den Personalrat,

etwa wenn sie Schwierigkeiten mit ihrem Vorgesetzten hätten. Der Personalrat lege diese Schreiben in einem Ordner ab. Im Falle einer Personalratsneuwahl stelle sich nun die Frage, ob dieser Ordner dem neu gewählten Personalrat übergeben werden dürfe. Denn in den neuen Personalrat könnte auch der betreffende Vorgesetzte gewählt werden und somit von der gegen ihn gerichteten Beschwerde erfahren.

Zu dieser Problematik nehme ich aus datenschutzrechtlicher Sicht wie folgt Stellung:

Das BayPVG enthält keine Bestimmungen über die Aufbewahrung und Vernichtung von papiergebundenen wie elektronischen Personalratsunterlagen, die personenbezogene Daten im Sinne des Art. 4 Abs. 1 BayDSG enthalten. Mangels spezialgesetzlicher Regelungen ist somit auf die allgemeine datenschutzrechtliche Löschungsbestimmung des Art. 12 BayDSG zurückzugreifen. Danach **darf der Personalrat personenbezogene Daten der Beschäftigten** – gleich ob in Dateien oder in Akten – **nur soweit und solange speichern, wie es zur Erfüllung der in seiner Zuständigkeit liegenden Aufgaben erforderlich ist.** Andernfalls hat er die personenbezogenen Beschäftigtendaten zu löschen (siehe Art. 12 Abs. 1 Nr. 2 und Abs. 4 BayDSG).

Demzufolge darf der Personalrat auch personenbezogene Daten, die er aufgrund der Beschwerde eines Beschäftigten erhalten hat, nur soweit und solange – beispielsweise in einem eigenen Ordner – speichern, wie es für die Behandlung der Beschwerde durch den Personalrat gemäß Art. 69 Abs. 1 lit. c) BayPVG erforderlich ist.

In diesem Zusammenhang ist allerdings zu beachten, dass **mit Ablauf der Amtszeit des Personalrats** (siehe Art. 26 ff. BayPVG) die rechtliche Existenz und die Befugnisse des Personalrats enden (siehe den Standardkommentar zum Bayerischen Personalvertretungsgesetz von Ballerstedt/Schleicher/Faber, Art. 26 BayPVG Rn. 19 und 19a m.w.N.). **Spätestens** zu diesem Zeitpunkt sind daher die **im Rahmen der Behandlung der Beschäftigtenbeschwerde durch den Personalrat angefallenen personenbezogenen Daten zu löschen.** Dies gilt auch, wenn die Behandlung der Beschäftigtenbeschwerde am Ende der Amtszeit des Personalrats noch nicht abgeschlossen ist. Im Grundsatz muss der Personalrat also den betreffenden Beschwerdeordner vernichten.

Eine Ausnahme ist nur vorzunehmen, wenn sich der betroffene Beschäftigte gegenüber dem scheidenden Personalrat ausdrücklich mit einer weiteren Behandlung seiner noch offenen Beschwerde durch den neu gewählten Personalrat einverstanden erklärt. Voraussetzung hierfür ist allerdings eine datenschutzgerechte, also insbesondere schriftliche, informierte und freiwillige Einwilligung des Beschäftigten (siehe im Einzelnen Art. 15 Abs. 2 bis 4 und 7 BayDSG).

Fehlt es an einer solchen rechtswirksamen Einwilligung, dürfen die die Beschäftigtenbeschwerde betreffenden papiergebundenen wie elektronischen Personalratsunterlagen mit personenbezogenen Daten nach einer Personalratsneuwahl **dem neuen Personalrat nicht übergeben oder auf andere Weise zugänglich gemacht werden.**

12 E-Government, Telemedienrecht, Soziale Medien

12.1 E-Government Gesetze

Im Berichtszeitraum sind neue Regelungen zum E-Government geschaffen bzw. entsprechende Initiativen gestartet worden.

So ist auf Bundesebene das Gesetz zur Förderung der elektronischen Verwaltung sowie zur Änderung weiterer Vorschriften (BGBl. I 2013, Seite 2749) in seinen wesentlichen Teilen am 01.08.2013 in Kraft getreten. Ziel des Gesetzes ist es, durch den Abbau bundesrechtlicher Hindernisse die elektronische Kommunikation mit der Verwaltung zu erleichtern. Dadurch soll es Bund, Ländern und Kommunen ermöglicht werden, einfachere, nutzerfreundlichere und effizientere elektronische Verwaltungsdienste anzubieten.

Es beinhaltet insbesondere das Gesetz zur Förderung der elektronischen Verwaltung (E-Government-Gesetz – EGovG), das auch Regelungen für die öffentlich-rechtliche Verwaltungstätigkeit der Behörden der Länder, der Gemeinden und Gemeindeverbände und der sonstigen der Aufsicht des Landes unterstehenden juristischen Personen des öffentlichen Rechts enthält, wenn sie Bundesrecht ausführen.

Das Gesetz hat zudem bestehende Vorschriften geändert, beispielsweise sind mit ihm weitere Regelungen zum Ersatz der Schriftform durch bestimmte elektronische Formen eingeführt worden.

Im Rahmen meiner Stellungnahme zum Gesetzesentwurf habe ich insbesondere hervorgehoben, dass die Veröffentlichung personenbezogener Daten im Internet weltweit einen ungleich größeren Personenkreis als jede auflagenbegrenzte schriftliche Veröffentlichung erreicht. Darüber hinaus können im Internet veröffentlichte Daten grundsätzlich auf einfache Weise beliebig verknüpft werden. Im Grunde wird dabei das datenschutzrechtlich zentrale Zweckbindungsprinzip gelockert, weil die veröffentlichten Daten letztlich in persönlicher, räumlicher und zeitlicher Hinsicht allgemein verfügbar werden. Sind die Veröffentlichungen überdies suchmaschinenfähig, werden betroffene Personen insoweit zu einem allgemein verfügbaren Rechercheobjekt.

Die Veröffentlichung personenbezogener Daten im Internet beeinträchtigt das informationelle Selbstbestimmungsrecht Betroffener daher deutlich stärker als bei einer Veröffentlichung in Papierform. Dies ist schon bei der Frage relevant, ob personenbezogene Daten überhaupt im Internet veröffentlicht werden. Bejahendenfalls müssen aber auch der Umfang, die Dauer und die technische Ausgestaltung der Veröffentlichung einbezogen werden.

In Bayern hat die Staatsregierung die Gestaltung der mit der Digitalisierung einhergehenden politischen, gesellschaftlichen und rechtlichen Veränderungen zu einem Schwerpunkt des Regierungsprogramms der laufenden Legislaturperiode gemacht.

Ergänzend zu bzw. über das oben angesprochene E-Government-Gesetz hinaus wurde daher ein Referentenentwurf eines Gesetzes zum Ausbau der elektronischen Verwaltung in Bayern und zur Änderung anderer Rechtsvorschriften erarbeitet.

Ich wurde bereits im Vorfeld der Entwurfserstellung eingebunden und konnte datenschutzrechtliche Positionen aus meiner Sicht einbringen. Auch anlässlich der Ressortanhörung zum Gesetzentwurf beabsichtige ich, meine datenschutzrechtlichen Standpunkte geltend zu machen.

Der Entwurf sieht auch Änderungen des Bayerischen Datenschutzgesetzes vor. Hier wäre es angezeigt, bei dieser Gelegenheit schon länger von mir erhobenen Forderungen nachzukommen, also etwa die Grundsätze der Datenvermeidung und der Datensparsamkeit ausdrücklich im Gesetz zu verankern (siehe 24. Tätigkeitsbericht 2010 Nr. 1.2.6).

12.2 Plattformen und Verfahren

Da die Verwaltung den Ausbau von E-Government vorantreibt (siehe Nr. 12.1), hatte ich im Berichtszeitraum zu diversen Projekten aus diesem Bereich zu beraten. Zu nennen sind unter anderem ein De-Mail-Pilotierungstest (siehe Nr. 2.2.5) und die Plattform für sichere Kommunikation in Bayern – BayMail (siehe Nr. 2.2.6).

Auch zum Bürgerservice-Portal bin ich um eine Einschätzung bzw. um Beratung gebeten worden. Dabei handelt es sich um eine E-Government-Plattform für digitale Verwaltungsdienstleistungen im Internet. Eine abschließende Bewertung konnte ich bislang noch nicht vornehmen.

Entsprechende Projekte und Verfahren sind zudem bei Inkrafttreten eines Gesetzes zum Ausbau der elektronischen Verwaltung in Bayern und zur Änderung anderer Rechtsvorschriften (siehe Nr. 12.1) unter Berücksichtigung der dann geltenden Regelungen zu beurteilen.

12.3 Apps

Schon seit geraumer Zeit nutzen viele Bürgerinnen und Bürger Apps etwa Sozialer Netzwerke oder anderer Online-Plattformen. Unter einer App ist hier eine „Mobile App“ zu verstehen, also eine spezielle Anwendungssoftware für mobile Endgeräte wie insbesondere Smartphones.

Auch so manche Behörde will eine App anbieten, um interessierten Bürgerinnen und Bürgern den Zugriff auf Web-Inhalte der Verwaltung über Smartphones zu erleichtern. Dabei findet die Entwicklung bzw. Programmierung der Software meistens nicht durch die Behörde, sondern durch einen externen Dienstleister statt. Entscheidend ist, dass bereits hier darauf geachtet wird, die App so zu gestalten, dass die für die App-anbietende Behörde geltenden Datenschutzvorschriften beachtet sind. Die Inhalte werden regelmäßig von der Behörde bereitgestellt.

Im Berichtszeitraum habe ich bayerische Behörden verschiedentlich zu den datenschutzrechtlichen Aspekten beraten. Wenn eine bayerische öffentliche Stelle

eine App anbietet, ist sie auch für die Zulässigkeit ihrer damit verbundenen Datenerhebungen, -verarbeitungen und -nutzungen verantwortlich. Zum einen wird hier das Telemediengesetz relevant, zum anderen – im Hinblick auf die Inhaltsdaten – grundsätzlich das Bayerische Datenschutzgesetz. Allerdings können Letzterem gegenüber spezielle Datenschutzvorschriften vorrangig zu beachten sein, etwa im Anwendungsbereich des Sozialgesetzbuchs.

Die Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich (Düsseldorfer Kreis) haben eine Orientierungshilfe zu den Datenschutzanforderungen an App-Entwickler und App-Anbieter erarbeitet, die im Juni 2014 veröffentlicht wurde. Sie bezieht sich allerdings auf nicht-öffentliche Stellen und dementsprechend bei den Inhaltsdaten auf das Bundesdatenschutzgesetz.

Diese Orientierungshilfe ist auf meiner Homepage https://www.datenschutz-bayern.de unter „Veröffentlichungen" – „Broschüren und Orientierungshilfen" abrufbar und enthält auch für bayerische öffentliche Stellen hilfreiche Ausführungen. Allerdings geht sie nicht detailliert auf speziell von öffentlichen Stellen zu beachtende Vorschriften ein.

12.4 Soziale Medien, insbesondere Soziale Netzwerke

Auf die steigende Bedeutung und Entwicklung des „Social Web" sowie auf die datenschutzrechtlichen Konsequenzen für die bayerische Verwaltung bin ich bereits im 25. Tätigkeitsbericht 2012 unter Nr. 1.3 eingegangen.

Soziale Medien sind inzwischen fester Bestandteil des Alltags vieler Menschen, zudem steigt die Zahl der Nutzer weiter an. Die Angebote Sozialer Medien, deren Nutzungsbedingungen und Datenschutzerklärungen sowie Umfang und Zweck der Datenverarbeitungen können sich dabei immer wieder ändern.

Dementsprechend haben mich vermehrt Beratungsanfragen von bayerischen Behörden erreicht, die Soziale Medien nutzen wollen. Auch die inhaltliche Bandbreite der Anfragen hat zugenommen. Zwar ging es häufig um die Einrichtung einer Fanpage auf Facebook zum Zweck der Öffentlichkeitsarbeit (siehe Nr. 12.4.1). Darüber hinaus wurden aber verschiedene andere Themen angesprochen, wie beispielsweise die Nutzung einer Blogplattform eines außereuropäischen Anbieters.

Die anfragenden Stellen haben die aus ihrer Sicht bestehende Erforderlichkeit der Nutzung Sozialer Medien dabei regelmäßig sehr engagiert dargestellt. Vielfach wurden Bürgernähe, Serviceorientierung und ein zeitgemäßes Image angeführt, „die Menschen sollen dort abgeholt werden, wo sie sind".

Und wo befinden sich viele Internetnutzer? In Sozialen Netzwerken. Allein bei Facebook gibt es in Deutschland mehr als 27 Millionen Nutzer, die man dort – möglicherweise – erreichen und „abholen" könnte.

Aber selbst wenn Soziale Medien die Chance eröffnen sollten, auch Menschen anzusprechen, die eine Behörde ansonsten möglicherweise nicht oder nicht so erreichen würde, bleibt Folgendes entscheidend:

Grundlage und Maßstab für das Handeln bayerischer öffentlicher Stellen ist das im Grundgesetz verankerte Rechtsstaatsprinzip.

Die jeweilige Behörde ist also dafür verantwortlich, dass sie rechtmäßig handelt, auch und gerade soweit es um die Erhebung, Verarbeitung und Nutzung personenbezogener Daten geht. Dies gilt unabhängig davon, wie „in" die Nutzung Sozialer Medien ist, ob diese „Chancen" eröffnen oder ob diese von anderen Stellen oder Personen genutzt werden. Hier kann es grundsätzlich auch keine Abwägung zwischen der Einhaltung datenschutzrechtlicher Vorschriften einerseits und der Anzahl der erreichbaren Personen oder dem vermeintlichen Image einer „zeitgemäßen, innovativen Behörde" andererseits geben. Die rechtliche Zulässigkeit darf nicht als ein (abwägbarer) Entscheidungsfaktor unter vielen angesehen werden.

Bei allem Verständnis für vorgetragene Motive wie etwa Serviceorientierung blieb Maßstab meiner Beratungen und Prüfungen daher die Einhaltung datenschutzrechtlicher Vorschriften durch bayerische öffentliche Stellen.

Im Berichtszeitraum gab es bei meinen Beratungen und Prüfungen im Zusammenhang mit der Nutzung Sozialer Medien drei Schwerpunkte, auf die ich nachfolgend näher eingehe.

12.4.1 Soziale Netzwerke, Fanpage zum Zweck der Öffentlichkeitsarbeit

Zahlreiche Behörden wandten sich mit der Frage an mich, ob und inwieweit sie zum Zweck der Öffentlichkeitsarbeit bei Facebook eine Fanpage einrichten und betreiben könnten. Bereits im 25. Tätigkeitsbericht 2012 unter Nr. 1.3.2 hatte ich empfohlen, von der Einrichtung einer Fanpage abzusehen und dabei auf noch strittige Rechtsfragen hingewiesen. Sie betrafen und betreffen immer noch die Anwendbarkeit des deutschen Datenschutzrechts auf Facebook und die (Mit-)Verantwortlichkeit der Fanpagebetreiber für eine unzulässige Verarbeitung von Nutzungsdaten durch Facebook.

Angesichts der zahlreichen Anfragen habe ich im März 2013 die **Orientierungshilfe „Fanpages bayerischer öffentlicher Stellen in Sozialen Netzwerken zum Zweck der Öffentlichkeitsarbeit"** veröffentlicht. Die Orientierungshilfe habe ich unter anderem allen Ressorts und den kommunalen Spitzenverbänden mit der Bitte übersandt, sie im jeweiligen Verantwortungsbereich bekannt zu machen.

Die Kernaussagen der Orientierungshilfe vom März 2013 sind,

- dass ich zu dieser Zeit nicht davon ausgehe, dass die Einrichtung bzw. Nutzung einer Fanpage bei Facebook (oder einem vergleichbaren Sozialen Netzwerk) datenschutzkonform ist

- dass ich empfehle, grundsätzlich keine entsprechende Fanpage einzurichten oder zu nutzen

- dass ich bayerische Behörden, die dieser Empfehlung nicht folgen, derzeit insbesondere angesichts noch umstrittener Fragen in bestimmten – in der Orientierungshilfe dargestellten – Konstellationen grundsätzlich nicht beanstande

- dass ich mir in darüber hinausgehenden Konstellationen ausdrücklich eine Beanstandung vorbehalte, insbesondere wenn eine bayerische öffentliche Stelle Bürgerinnen und Bürger zur Offenbarung besonders sensibler Daten auf der Fanpage ermuntern sollte.

Dementsprechend habe ich im Berichtszeitraum grundsätzlich Anfragen beantwortet und bayerische Behörden in Besprechungen beraten.

Auch die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat eine Orientierungshilfe („Soziale Netzwerke“) veröffentlicht. Sie soll die Einhaltung des Datenschutzes im Zusammenhang mit Sozialen Netzwerken unterstützen und ist ebenfalls auf meiner Homepage https://www.datenschutz-bayern.de unter „Veröffentlichungen“ – „Broschüren und Orientierungshilfen“ abrufbar.

Die 85. Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat zudem folgende Entschließung verabschiedet:

Entschließung der 85. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 13./14.03.2013
Soziale Netzwerke brauchen Leitplanken – Datenschutzbeauftragte legen Orientierungshilfe vor

Angesichts der zunehmenden Bedeutung sozialer Netzwerke erinnert die Datenschutzkonferenz deren Betreiber an ihre Verpflichtung, die Einhaltung datenschutzrechtlicher Anforderungen sicherzustellen. Auch Unternehmen und öffentliche Stellen, die soziale Netzwerke nutzen, müssen diesen Anforderungen Rechnung tragen. Die Erfahrung der Aufsichtsbehörden zeigt, dass der Schutz der Privatsphäre von den Betreibern sozialer Netzwerke nicht immer hinreichend beachtet wird.

Häufig vertrauen die Nutzenden den Betreibern dieser Dienste sehr persönliche Informationen an. Auch die Vielfalt der Informationen, die innerhalb eines Netzwerkes aktiv eingestellt oder über die Nutzerinnen und Nutzer erhoben werden, ermöglicht einen tiefen Einblick in deren persönliche Lebensgestaltung.

Es zeichnet sich ab, dass die angekündigte Selbstregulierung für soziale Netzwerke – insbesondere auf Grund der mangelnden Bereitschaft einiger großer Netzwerk-Betreiber – den erforderlichen Datenschutzstandard nicht gewährleisten kann. Deshalb haben die Datenschutzbeauftragten des Bundes und der Länder die Orientierungshilfe "Soziale Netzwerke" erarbeitet. Sie soll die Betreiber sozialer Netzwerke und die die Netzwerke nutzenden öffentlichen und privaten Stellen bei der datenschutzgerechten Gestaltung und Nutzung der Angebote unterstützen. Die Konferenz weist darauf hin, dass der vorhandene Rechtsrahmen zur Gewährleistung eines angemessenen Datenschutzes bei sozialen Netzwerken weiterentwickelt werden muss, insbesondere in Bezug auf konkrete und präzise Vorgaben zu datenschutzfreundlichen Voreinstellungen, zum Minderjährigenschutz, zur Löschungsverpflichtung bei Dritten und zum Verhältnis von Meinungsfreiheit und Persönlichkeitsrecht. Ferner wird die Verantwortlichkeit für den Umgang mit Nutzungsdaten in Bezug auf Social Plug-Ins, Fanpages sowie für den Einsatz von Cookies von vielen Unternehmen und Behörden in Abrede gestellt. Der europäische und nationale Gesetzgeber bleiben aufgefordert, für die notwendige Klarheit zu sorgen und damit einen ausreichenden Datenschutzstandard zu sichern. Darauf weist die Konferenz der Datenschutzbeauftragten erneut nachdrücklich hin.

Die in meiner Orientierungshilfe angenommene (Mit-)Verantwortlichkeit eines Fanpagebetreibers insbesondere für Nutzungsdatenverarbeitungen von Facebook verneint das Oberverwaltungsgericht Schleswig in einem Urteil vom 04.09.2014 (Az.: 4 LB 20/13).

Dieses Urteil des Oberverwaltungsgerichts Schleswig habe ich zur Kenntnis genommen und es bei meinen Beratungen und meiner Vorgehensweise ab dem 04.09.2014 auch nicht außer Betracht gelassen. Das Unabhängige Landeszentrum für Datenschutz Schleswig-Holstein hat Revision gegen die Entscheidung des Oberverwaltungsgerichts eingelegt. Der Ausgang des Verfahrens bleibt daher abzuwarten.

Auch bei Zugrundelegung der Rechtsauffassung des Oberverwaltungsgerichts Schleswig wäre dies allerdings kein allgemeiner Freifahrtschein für die Nutzung einer Fanpage. Denn das Oberverwaltungsgericht geht im Kern nur auf die Frage ein, ob Stellen, die eine Fanpage auf Facebook betreiben, sich auch die Nutzungsdatenverarbeitung von Facebook zurechnen lassen müssen. Wie in meiner Orientierungshilfe dargestellt, gibt es für bayerische Behörden als Fanpagebetreiber – unabhängig von dieser Frage – einzuhaltende (Datenschutz-)Vorschriften bezüglich der Inhaltsdaten sowie auch nach dem Telemediengesetz zu beachtende Impressums- und Unterrichtungspflichten.

Außerdem bin ich weiterhin der Auffassung, dass bayerische öffentliche Stellen eine Vorbildfunktion haben (siehe 25. Tätigkeitsbericht 2012 Nr. 1.3.2). Bereits aus diesem Grund sollten bayerische öffentliche Stellen Soziale Netzwerke, die sich wiederholt bzw. dauerhaft nicht an europäische bzw. deutsche Datenschutzstandards halten, grundsätzlich nicht nutzen.

Dass deutsche Datenschutzstandards von international agierenden Sozialen Netzwerken als hinderlich angesehen werden, ist nicht verwunderlich. Das Geschäftsmodell Sozialer Netzwerke wie Facebook beruht darauf, mittels der Daten der Nutzer Geld zu verdienen, während die Datenschutzbestimmungen gerade den Schutz der personenbezogenen Daten gewährleisten sollen.

Bislang hat Facebook deutsches Datenschutzrecht auf seine Nutzungsdatenverarbeitungen bezüglich Nutzern in Deutschland allerdings grundsätzlich als nicht anwendbar angesehen. Auch das Oberverwaltungsgericht Schleswig hat bei seinen Beschlüssen vom 22.04.2013 (Az.: 4 MB 10/13, 4 MB 11/13) auf den Sitz der Facebook Ireland Limited in Irland abgestellt und insoweit nicht deutsches, sondern irisches Datenschutzrecht zugrundegelegt.

Demgegenüber hat das Landgericht Berlin in seinem Urteil vom 06.03.2012 (Az.: 16 O 551/10) ausdrücklich deutsches Datenschutzrecht angewandt, obwohl Facebook auch in diesem Verfahren vorgetragen hat, es gelte irisches Datenschutzrecht. Das Landgericht ging von einer wirksamen Rechtswahl (Vereinbarung) deutschen Datenschutzrechts aus. Das Kammergericht Berlin hat die hiergegen eingelegte Berufung mit Urteil vom 24.01.2014 (Az.: 5 U 42/12) zurückgewiesen und die Anwendbarkeit deutschen Datenschutzrechts zudem auch darauf begründet, dass insoweit auf den Sitz der Muttergesellschaft Facebook Inc. in den USA (und nicht auf den von Facebook Limited in Irland) abzustellen ist. Deutsches Datenschutzrecht hat das Landgericht Berlin auch in seiner Entscheidung vom 30.04.2013 (Az.: 15 O 92/12) angewandt.

Der Europäische Gerichtshof hat nunmehr in einem Verfahren zu Google als Suchmaschinenbetreiber (Urteil vom 13.05.2014, Az.: C – 131/12) die Formulierung „im Rahmen der Tätigkeiten einer Niederlassung“ des Art. 4 Abs. 1 Buchst. a der Richtlinie 95/46/EG (Europäische Datenschutzrichtlinie) weit ausgelegt. Im Ergebnis nimmt der Europäische Gerichtshof in diesem Verfahren eine insofern relevante Niederlassung in einem Mitgliedstaat an, wenn der Suchmaschinenbetreiber (mit Sitz in einem Drittstaat) in dem Mitgliedstaat für die Förderung des Verkaufs der Werbeflächen der Suchmaschine und diesen Verkauf selbst eine Zweigniederlassung oder Tochtergesellschaft gründet, deren Tätigkeit auf die Einwohner dieses Staates gerichtet sind. Dies führt dann zur Anwendung des nationalen Datenschutzrechts dieses Mitgliedstaates.

Ich werde daher aufmerksam verfolgen, wie sich diese Entscheidung des Europäischen Gerichtshofs im Hinblick auf Soziale Netzwerke auswirkt, die Niederlassungen in Deutschland mit den in der Entscheidung des Europäischen Gerichtshofs genannten Geschäftszwecken haben.

Das Thema Fanpages wird mich und andere unter Berücksichtigung aktueller Entwicklungen weiterhin beschäftigen. Selbstverständlich wende ich mich dabei nicht gegen die Nutzung Sozialer Netzwerke durch bayerische Behörden, wenn die datenschutzrechtlichen Vorschriften von den verantwortlichen und handelnden Stellen eingehalten werden.

12.4.2 Facebook als dienstlicher Kommunikationskanal

Behörden haben mich in verschiedenen Zusammenhängen um Beratung gebeten, ob es zulässig ist, mittels einer Facebook-Profilseite bzw. eines Facebook-Accounts dienstlich mit Bürgerinnen und Bürgern zu kommunizieren. Diese Fallgestaltung ist von der allgemeinen Öffentlichkeitsarbeit mittels einer Fanpage (siehe Nr. 12.4.1) zu unterscheiden.

Beispielhaft ist das zunächst beabsichtigte Projekt einer Behörde, bei dem Beschäftigte dienstliche Profilseiten bzw. Accounts bei Facebook anlegen wollten, um im Rahmen geschlossener Benutzergruppen Bürgerinnen und Bürger zu bestimmten Themenbereichen zu beraten. Durch geschlossene Benutzergruppen sollte – nach Auffassung der Behörde – die Vertraulichkeit der ausgetauschten personenbezogenen Daten ausreichend abgesichert werden.

Mit anderen Worten sollte eine Einzelfallbearbeitung bzw. -beratung mit entsprechenden personenbezogenen Daten erfolgen. Damit würden auch sensible personenbezogene Daten über einen „unsicheren“ Kommunikationskanal ausgetauscht und bei einem „unsicheren“ Anbieter gespeichert. Gegenüber einer allgemeinen Öffentlichkeitsarbeit mittels einer Fanpage hätte das Projekt also insofern ein deutlich höheres Gefährdungspotential gehabt.

Bayerische öffentliche Stellen, die personenbezogene Daten erheben, verarbeiten oder nutzen, müssen auch die technisch-organisatorischen Maßnahmen treffen, um die Einhaltung der datenschutzrechtlichen Vorschriften zu gewährleisten. Insbesondere müssen sie unbefugte Zugriffe technisch-organisatorisch unterbinden. Hier kann jedoch nicht davon ausgegangen werden, dass die Vertraulichkeit im Sinne der für die bayerischen Behörden geltenden Datenschutzbestimmungen gewährleistet ist.

Zudem würden eventuelle Kenntnisnahmen durch andere Gruppenmitglieder weitere datenschutzrechtliche Fragen aufwerfen.

Auf dieser Basis habe ich entsprechende Anfragen beantwortet und das genannte Projekt dementsprechend als datenschutzrechtlich unzulässig eingeordnet. Die Behörde hat von dem Projekt Abstand genommen.

Meine Einschätzung in dem genannten Fall deckt sich mit dem Leitfaden, der vom IT-Beauftragten der Staatsregierung für die Beschäftigten der Staatsverwaltung zum Umgang mit Sozialen Medien im Februar 2013 herausgegeben worden ist. Vor Veröffentlichung hatte ich Gelegenheit, mich zum Entwurf des Leitfadens zu äußern.

Der Leitfaden bezieht sich zwar ausdrücklich nicht auf die Nutzung Sozialer Medien als Kommunikationskanal der Öffentlichkeitsarbeit von Verwaltungen. Im Hinblick auf eine darüber hinaus gehende Nutzung führt der Leitfaden aber unter anderem aus, dass eine Nutzung Sozialer Netzwerke durch öffentliche Beschäftigte zu Zwecken des Austauschs personenbezogener Daten zu unmittelbaren oder mittelbaren dienstlichen Zwecken aus datenschutzrechtlicher Sicht in aller Regel unzulässig ist.

12.4.3 Social Plugins auf Webseiten bayerischer öffentlicher Stellen

Zur direkten Einbindung von Social Plugins, etwa des Like-Buttons („Gefällt mir") von Facebook in Internetauftritte bayerischer öffentlicher Stellen hatte ich mich bereits im 25. Tätigkeitsbericht 2012 unter Nr. 1.3.2 geäußert. Bei der direkten Einbindung von Social Plugins fließen unmittelbar mit Aufruf der Behördenwebseite Daten an das hinter dem Plugin stehende Soziale Netzwerk. Auf diese Weise werden unter Verstoß gegen das Telemediengesetz zumindest die IP-Adresse des Nutzerrechners und der Zeitpunkt des Seitenaufrufs weitergeleitet. Im 25. Tätigkeitsbericht 2012 unter Nr. 1.3.2 hatte ich auch auf die sogenannte Zwei-Klick-Lösung hingewiesen, die verhindert, dass entsprechende Daten unmittelbar bei Aufruf der Behördenseite weitergegeben werden.

Mittlerweile habe ich eine Orientierungshilfe zu Social Plugins veröffentlicht, die auf meiner Homepage https://www.datenschutz-bayern.de unter „Veröffentlichungen" – „Broschüren und Orientierungshilfen" abrufbar ist. Die Orientierungshilfe habe ich zudem kommunalen Spitzenverbänden sowie dem Staatsministerium des Innern, für Bau und Verkehr mit der Bitte übersandt, sie den bayerischen Städten, Märkten und Gemeinden bekannt zu geben, da insbesondere Stellen aus diesem Kreis Social Plugins in ihre Webauftritte einbinden. Dabei hatte ich eine stichprobenartige Überprüfung angekündigt.

Die darauf folgende Überprüfung von 5592 Webseiten bayerischer öffentlicher Stellen ergab, dass 66 Stellen weiterhin Social Plugins direkt in ihren Internetauftritt eingebunden hatten. Diese Stellen habe ich sodann konkret angeschrieben und aufgefordert, dies zu unterlassen. Fast alle der angeschriebenen Stellen haben unmittelbar reagiert und Social Plugins entweder ganz entfernt oder die Zwei-Klick-Lösung verwendet. Lediglich eine Stelle zeigte sich zunächst uneinsichtig und wurde von mir beanstandet. Nach Einschaltung der Aufsichtsbehörde hat auch diese Stelle letztlich von einer direkten Einbindung von Social Plugins Abstand genommen.

Im Ergebnis konnte ich diese Prüfung damit Ende 2013 erfolgreich abschließen. Auch in der Folge habe ich die Einbindung von Social Plugins in Webseiten bayerischer öffentlicher Stellen stichprobenartig geprüft und werde dies weiter fortsetzen.

13 Spezielle datenschutzrechtliche Themen

13.1 Cloud Computing

Zum Cloud Computing habe ich mich schon in meinem 24. Tätigkeitsbericht 2010 unter Nr. 2.1.5 und in meinem 25. Tätigkeitsbericht 2012 unter Nrn. 1.2 und 2.3.3 geäußert.

Schon aus den dort genannten Gründen empfehle ich bayerischen öffentlichen Stellen weiterhin, jedenfalls bei der Inanspruchnahme von Public-Cloud-Diensten grundsätzlich äußerste Zurückhaltung walten zu lassen.

Im Berichtszeitraum habe ich zahlreiche bayerische Behörden nach dieser Maßgabe und folgenden Punkten beraten.

Soweit eine bayerische öffentliche Stelle personenbezogene Daten im Auftrag durch eine andere Stelle innerhalb eines Mitgliedstaates der Europäischen Union verarbeiten lassen will, ist dies grundsätzlich an den Vorgaben des Art. 6 BayDSG (oder vorgehender Spezialvorschriften) zu messen. Soll dabei Cloud-Computing zur Anwendung kommen, bedarf es einer besonders sorgfältigen Prüfung.

Eine Vereinbarung zur Auftragsdatenverarbeitung muss dabei die entsprechenden Regelungen beinhalten. Bei mir von Behörden zur Beratung vorgelegten Vertragsbedingungen von Cloud-Anbietern konnte ich feststellen, dass die Anforderungen so nicht erfüllt wurden. Zu anderen Vereinbarungen waren solche Cloud-Anbieter offenbar nicht gewillt.

Folgenden Auszug aus der Stellungnahme der Artikel-29-Datenschutzgruppe (siehe Art. 29 der Richtlinie 95/46/EG – Europäische Datenschutzrichtlinie) vom 01.07.2012 (01037/12/DE, WP 196) kann ich nur unterstreichen:

„Es sollte angemerkt werden, dass Anbieter von Cloud-Diensten in vielen Fällen Standarddienste und von den für die Verarbeitung Verantwortlichen zu unterzeichnende Standardverträge anbieten, die ein Standardformat für die Verarbeitung personenbezogener Daten festlegen. Das Ungleichgewicht in der Vertragsposition zwischen einem kleinen für die Verarbeitung Verantwortlichen und großen Dienstleistern darf nicht als Rechtfertigung dafür gelten, dass für die Verarbeitung Verantwortliche Vertragsklauseln und -bedingungen akzeptieren, die gegen das Datenschutzrecht verstoßen.“

Darüber hinaus stand auch Cloud Computing mit Datenverarbeitungen außerhalb der Mitgliedstaaten der Europäischen Union und der anderen Vertragsstaaten des Abkommens über den Europäischen Wirtschaftsraum zur Debatte.

Hierfür bedürfte es dann daneben einer gesonderten Rechtsgrundlage, da eine solche Verarbeitung personenbezogener gemäß Art. 4 Abs. 10 BayDSG in Verbindung mit Art. 4 Abs. 6 Satz 2 Nr. 3 BayDSG als Datenübermittlung einzuordnen ist.

In den von mir beratenen Fällen konnte ich eine gesetzliche Übermittlungsbefugnis weder erkennen, noch haben mir die Behörden eine entsprechende Befugnis begründet dargelegt.

Cloud-Anbieter haben hier Behörden offenbar auch auf Äußerungen bzw. Gesichtspunkte aus dem nicht-öffentlichen Bereich hingewiesen, die auf bayerische öffentliche Stellen so nicht übertragbar sind. Beispielsweise findet § 28 Bundesdatenschutzgesetz (BDSG) für bayerische Behörden grundsätzlich keine Anwendung.

Die bisherige Orientierungshilfe Cloud Computing der Arbeitskreise Technik und Medien der Konferenz der Datenschutzbeauftragten des Bundes und der Länder wurde an aktuelle Entwicklungen angepasst und im Oktober 2014 in einer überarbeiteten Version veröffentlicht. Die Orientierungshilfe thematisiert auch Zugriffsermächtigungen von US-Behörden auf der Grundlage von US-amerikanischem Recht.

Die Ausführungen der Orientierungshilfe beziehen sich zwar grundsätzlich nur auf das für die nicht-öffentlichen Stellen und die Bundesverwaltung geltende Bundesdatenschutzgesetz. Sie enthält jedoch auch für bayerische öffentliche Stellen interessante Informationen und ist daher auf meiner Homepage https://www.datenschutz-bayern.de unter „Veröffentlichungen“ – „Broschüren und Orientierungshilfen“ abrufbar.

13.2 Einsatz von Wildvideokameras durch bayerische öffentliche Stellen

Im Berichtszeitraum wurde ich mehrfach und von verschiedener Seite mit der Problematik des Einsatzes von Wildvideokameras befasst. Dies nehme ich zum Anlass, nochmals in allgemeiner Form auf Folgendes hinzuweisen:

1. Der Einsatz von Wildvideokameras durch bayerische öffentliche Stellen unterliegt – anders als insbesondere deren Einsatz durch Private wie zum Beispiel Jäger oder Jagdpächter – meiner datenschutzrechtlichen Kontrolle nach Art. 30 Abs. 1 BayDSG.

2. Angesichts des in Art. 141 Abs. 3 Bayerische Verfassung enthaltenen Jedermannsrechts zum freien Betreten des Waldes besteht beim Einsatz derartiger Kameras durch bayerische öffentliche Stellen grundsätzlich stets die Gefahr, dass es auch zur Erhebung personenbezogener Daten im Sinne des Art. 4 Abs. 1 BayDSG kommt. Ist dies der Fall, beurteilt sich die datenschutzrechtliche Zulässigkeit des Einsatzes von Wildvideokameras durch bayerische öffentliche Stellen nach Art. 21a BayDSG und muss vollumfänglich dessen Tatbestandsvoraussetzungen (insbesondere dessen Abs. 1 und 2) genügen. Dagegen kommt der weniger strenge § 6b Abs. 1 Bundesdatenschutzgesetz auch für solche bayerische öffentliche Stellen, welche als Unternehmen im Sinne des Art. 3 Abs. 1 Satz 1 BayDSG am Wettbewerb teilnehmen nicht zur Anwendung, da in Bezug auf eine Videoüberwachung gerade keine Wettbewerbssituation im Sinne des Art. 3 Abs. 1 Satz 1 BayDSG vorliegt (vgl. „soweit“).

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

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

zu schützen. [2]Es dürfen keine Anhaltspunkte dafür bestehen, dass überwiegende schutzwürdige Interessen der Betroffenen beeinträchtigt werden.
(2) Die Videoüberwachung und die erhebende Stelle sind durch geeignete Maßnahmen erkennbar zu machen.

3. Eine Erhebung und Speicherung personenbezogener Daten beim Einsatz von Wildvideokameras dürften im Ergebnis danach regelmäßig nicht zulässig sein, weil sie nicht zum Schutz der in Art. 21a Abs. 1 Satz 1 Nr. 1 und 2 BayDSG genannten Rechtsgüter erforderlich sind. Werden die Kameras allerdings so aufgestellt, dass ein Aufenthalt natürlicher Personen im Beobachtungsbereich technisch ausgeschlossen oder unwahrscheinlich ist bzw. eine Identifikation einzelner Personen mit den gemachten Aufnahmen ausscheidet, sind datenschutzrechtliche Vorschriften dagegen von vornherein nicht anwendbar. **Beim Einsatz von Wildvideokameras durch öffentliche Stellen ist deshalb stets darauf zu achten, dass natürliche Personen nicht erfasst bzw. zumindest nicht identifiziert werden können.**

4. Sofern öffentliche Stellen in einzelnen Ausnahmefällen zu der Einschätzung gelangen sollten, dass die Tatbestandsvoraussetzungen des Art. 21a Abs. 1 BayDSG gleichwohl gegeben sind – dies erscheint mir derzeit zum Beispiel dann denkbar, wenn im Einzelfall konkrete Anhaltspunkte für eine Gesundheitsgefährdung von Personen vorliegen – ist insbesondere Art. 21a Abs. 2 BayDSG zu beachten. Danach sind die Videoüberwachung und die erhebende Stelle durch geeignete Maßnahmen erkennbar zu machen.

5. Vor diesem rechtlichen Hintergrund rate ich daher, insbesondere bei der Beobachtung von Wildtieren im Rahmen von forstlichen Monitoring-Maßnahmen bzw. der wissenschaftlichen Forschung (zum Beispiel im Rahmen des Wildtier-Monitorings) mittels Wildvideokameras aus datenschutzrechtlicher Sicht Folgendes zu beachten:

   — Aufstellung der Kameras so, dass entweder eine Aufzeichnung bestimmter oder bestimmbarer natürlicher Personen so weit als möglich technisch ausgeschlossen ist oder ein Aufenthalt natürlicher Personen im Kamerabereich nicht wahrscheinlich ist (z.B. abseits von Waldwegen) und

— Begrenzung der Beobachtungsmaßnahme in zeitlicher und räumlicher Hinsicht auf das zur Erreichung des angestrebten Zwecks erforderliche Maß (zum Beispiel auf bestimmte Tageszeiten) und

— Anbringung für die Waldbesucher deutlich sichtbarer Hinweise auf die Beobachtungsmaßnahme und deren (zeitlichen) Umfang.

Aufnahmen gleichwohl versehentlich erfasster natürlicher Personen müssen unverzüglich nach deren Entdeckung gelöscht werden.

13.3 Übermittlung von Unterlagen aus der Fahrerlaubnisakte an eine Begutachtungsstelle für Fahreignung

Ein Bürger beschwerte sich über eine Fahrerlaubnisbehörde.

Der Beschwerdeführer hatte eine Begutachtungsstelle für Fahreignung beauftragt, seine Fahreignung zu begutachten. Die Fahrerlaubnisbehörde übermittelte daraufhin der Begutachtungsstelle ein in der Fahrerlaubnisakte befindliches Führungszeugnis, welches auch eine Eintragung über eine im Bundeszentralregister bereits getilgte Straftat wegen einer vorsätzlichen Verletzung der Buchführungspflicht enthielt.

Das betreffende Führungszeugnis durfte noch in der Fahrerlaubnisakte bleiben, da die Zehnjahresfrist des § 2 Abs. 9 Satz 2 Straßenverkehrsgesetz (StVG) zum Zeitpunkt des Aktenversands an die Begutachtungsstelle für Fahreignung noch nicht überschritten war. Zum Vorbringen der Fahrerlaubnisbehörde, der Begutachtungsstelle für Fahreignung seien gemäß § 11 Abs. 6 Satz 4 Fahrerlaubnis-Verordnung (FeV) die vollständigen Unterlagen übersandt worden, habe ich auf Folgendes hingewiesen:

Die Fahrerlaubnisbehörden dürfen den Begutachtungsstellen für Fahreignung die Daten übermitteln, die diese zur Erfüllung ihrer Aufgaben, mithin zur Durchführung einer Fahreignungsbegutachtung benötigen (vgl. § 2 Abs. 14 Satz 1 StVG). Gemäß § 11 Abs. 6 Satz 4 FeV sind dabei der Begutachtungsstelle die vollständigen Unterlagen zu übersenden, allerdings nur soweit sie unter Beachtung der gesetzlichen Verwertungsverbote verwendet werden dürfen. Zu beachten ist dabei insbesondere das Verbot der Verwertung gelöschter Eintragungen im Fahreignungsregister (§ 29 Abs. 7 StVG) bzw. das – hier maßgebliche – Verbot der Verwertung von getilgten Straftaten im Bundeszentralregister (§§ 51, 52 Bundeszentralregistergesetz – BZRG). Im vorliegenden Fall war die Eintragung wegen der vorsätzlichen Verletzung der Buchführungspflicht nach den Bestimmungen des Bundeszentralregistergesetzes bereits getilgt worden. Ein ebenfalls in der Fahrerlaubnisakte befindliches Führungszeugnis neueren Datums wies diese Eintragung auch nicht mehr auf. Im Übrigen kam auch eine Verwertung der Verurteilung nach den Vorschriften der §§ 28 bis 30b des Straßenverkehrsgesetzes nicht in Betracht (vgl. § 52 Abs. 2 Satz 1 BZRG). Im Ergebnis hätte daher die nicht mehr verwertbare Eintragung im älteren Führungszeugnis vor einer Übersendung an die Begutachtungsstelle für Fahreignung geschwärzt bzw. unkenntlich gemacht werden müssen, auch um eine mögliche Beeinflussung des Gutachters von vornherein auszuschließen.

§ 2 StVG Fahrerlaubnis und Führerschein
(9) [1]Die Registerauskünfte, Führungszeugnisse, Gutachten und Gesundheitszeugnisse dürfen nur zur Feststellung oder Überprüfung der Eignung oder Befähigung verwendet werden. [2]Sie sind nach spätestens zehn Jahren zu vernichten, es sei denn, mit ihnen im Zusammenhang stehende Eintragungen im Fahreignungsregister oder im Zentralen Fahrerlaubnisregister sind nach den Bestimmungen für diese Register zu einem späteren Zeitpunkt zu tilgen oder zu löschen. [3]In diesem Fall ist für die Vernichtung oder Löschung der spätere Zeitpunkt maßgeblich. …

§ 11 FeV Eignung
(6) … [3]Der Betroffene hat die Fahrerlaubnisbehörde darüber zu unterrichten, welche Stelle er mit der Untersuchung beauftragt hat. [4]Die Fahrerlaubnisbehörde teilt der untersuchenden Stelle mit, welche Fragen im Hinblick auf die Eignung des Betroffenen zum Führen von Kraftfahrzeugen zu klären sind und übersendet ihr die vollständigen Unterlagen, soweit sie unter Beachtung der gesetzlichen Verwertungsverbote verwendet werden dürfen. [5]Die Untersuchung erfolgt auf Grund eines Auftrags durch den Betroffenen.

13.4 Datenschutz im Schornsteinfegerwesen

13.4.1 Nutzung von Kehrbuchdaten durch bevollmächtigte Bezirksschornsteinfeger

Zum 01.01.2013 wurde das Kaminkehrerwesen (teilweise) für den Wettbewerb geöffnet. Seitdem dürfen bestimmte Schornsteinfegertätigkeiten – soweit diese nicht den sog. bevollmächtigten Bezirksschornsteinfegern vorbehalten sind – von einem vom Haus- und Wohnungseigentümer frei auszuwählenden und entsprechend berechtigten Schornsteinfegerbetrieb ausgeführt werden. Das Gesetz über das Berufsrecht und die Versorgung im Schornsteinfegerhandwerk – Schornsteinfeger-Handwerksgesetz (SchfHwG) – legt dabei den Bereich fest, der auch künftig hoheitlich ausgestaltet ist. Zu den hoheitlichen Tätigkeiten, die weiterhin den bevollmächtigten Bezirksschornsteinfegern (den bisherigen Bezirksschornsteinfegermeistern) vorbehalten sind, zählen danach insbesondere die Feuerstättenschau, der Erlass des Feuerstättenbescheids, anlassbezogene Überprüfungen, Bauabnahmen, Ersatzvornahmen, das Führen des Kehrbuches sowie die Prüfung der Einhaltung der Eigentümerpflichten. Für die übrigen (nicht-hoheitlichen) Aufgaben hat am 01.01.2013 der Wettbewerb begonnen (z.B. hinsichtlich der Durchführung der im Feuerstättenbescheid festgelegten Arbeiten wie Messen, Kehren, Reinigen).

Soweit bevollmächtigte Bezirksschornsteinfeger als sog. „beliehene Unternehmer“ tätig werden, d.h. die ihnen gesetzlich zugewiesenen (hoheitlichen) Aufgaben wahrnehmen, sind sie nach Art. 4 Abs. 2 Satz 4 BayDSG öffentliche Stellen, auf die das Bayerische Datenschutzgesetz gemäß Art. 2 Abs. 1 BayDSG Anwendung findet.

Im Berichtszeitraum war ich des Öfteren mit Fragen und Beschwerden im Zusammenhang mit der Nutzung von Kehrbuchdaten (z.B. für private Werbezwecke) durch bevollmächtigte Bezirksschornsteinfeger befasst. Dies hat mich veranlasst, auf Folgendes hinzuweisen:

Das SchfHwG enthält bereichsspezifische gesetzliche Regelungen hinsichtlich des Umgangs mit personenbezogenen Daten. So ist etwa die Zulässigkeit der Nutzung von Kehrbuchdaten durch bevollmächtigte Bezirksschornsteinfeger in § 19 Abs. 5 Satz 1 SchfHwG geregelt. Danach dürfen bevollmächtigte Bezirksschornsteinfeger die im Kehrbuch eingetragenen (z.B. Eigentümer-)Daten nur nutzen, soweit das zur Erfüllung ihrer hoheitlichen Aufgaben nach diesem Gesetz erforderlich ist. Eine Nutzung dieser hoheitlich erlangten Daten für andere Zwecke, wie etwa das Werben für nicht-hoheitliche Tätigkeiten, hinsichtlich derer der bevollmächtigte Bezirksschornsteinfeger als Gewerbetreibender am Wettbewerb teilnimmt, ist demnach ausgeschlossen. Die Regelung zur Datennutzung in § 19 Abs. 5 Satz 1 SchfHwG bezieht sich dabei nur auf das Kehrbuch, mithin auf die Daten nach § 19 Abs. 1 SchfHwG. Hierauf hat das Staatsministerium des Innern, für Bau und Verkehr ergänzend hingewiesen.

13.4.2 Datenübermittlung durch bevollmächtigte Bezirksschornsteinfeger für die Erstellung eines Energienutzungsplans

Ob bevollmächtigte Bezirksschornsteinfeger für die Erstellung eines Energienutzungsplans Daten aus dem Kehrbuch gemäß § 19 Abs. 1 Nr. 2 Schornsteinfeger-Handwerksgesetz (SchfHwG) (Art, Brennstoff, Nennwärmeleistung und Alter der Anlage sowie Angaben über ihren Betrieb und Standort) an öffentliche Stellen (in der Regel sind dies Gemeinden) übermitteln dürfen, beurteilt sich anhand von § 19 Abs. 5 Satz 2 SchfHwG. Danach dürfen Daten aus dem Kehrbuch an öffentliche Stellen nur übermittelt werden, soweit das Landesrecht dies zulässt. Die Übermittlung von Kehrbuchdaten zur Erstellung eines Energienutzungsplans stellt eine Zweckänderung der zur Erfüllung hoheitlicher Tätigkeiten nach dem Schornsteinfeger-Handwerksgesetz erhobenen Daten dar. Neben der Erforderlichkeit zur Aufgabenerfüllung müsste diese Zweckänderung zulässig sein (Art. 18 Abs. 1 BayDSG in Verbindung mit Art. 17 Abs. 1 Nr. 2, Abs. 2 bis 4 BayDSG). Das ist hier jedoch nicht der Fall. Insbesondere kann nicht nach Art. 17 Abs. 2 Nr. 3 BayDSG angenommen werden, dass die Datenübermittlung zur Erstellung des Energienutzungsplans offensichtlich im Interesse der betroffenen Bürgerinnen und Bürger liegt. Im Ergebnis besteht somit eine Befugnis zur Datenübermittlung nur mit Einwilligung des Grundeigentümers oder in anonymisierter Form.

§ 19 SchfHwG Führung des Kehrbuchs
(5) [1]Bevollmächtigte Bezirksschornsteinfeger und Bezirksschornsteinfegermeister dürfen die Daten nach Abs. 1 nur nutzen, soweit das zur Erfüllung ihrer Aufgaben nach diesem Gesetz erforderlich ist. [2]An öffentliche Stellen dürfen die Daten übermittelt werden, soweit das Landesrecht dies zulässt.

13.5 Nochmals: Anhörung des Bayerischen Bauernverbands bei Verfahren nach dem Grundstücksverkehrsgesetz; Weitergabe personenbezogener Daten vom Bayerischen Bauernverband an die Obmänner dieses Verbandes

Im Berichtszeitraum haben sich wiederholt Parteien land- und forstwirtschaftlicher Grundstücksveräußerungsverträge mit der Frage an mich gewandt, ob und inwieweit sie es hinnehmen müssen, dass Vertragsbestandteile und damit personenbezogene Daten von der Kreisverwaltungsbehörde an den Bayerischen Bauernverband (BBV), beziehungsweise von diesem an seine Obmänner weitergeleitet wer-

den. Obwohl ich die in diesem Zusammenhang maßgeblichen Datenschutzanforderungen bereits im 16. Tätigkeitsbericht 1994 unter Nr. 8.6 ausführlich dargestellt habe, musste ich jedoch feststellen, dass diese in der Praxis nicht hinreichend bekannt sind. Ich weise daher nochmals auf Folgendes hin:

Veräußerungen land- und forstwirtschaftlicher Grundstücke bedürfen nach § 2 des (Bundes-)Gesetzes über Maßnahmen zur Verbesserung der Agrarstruktur und zur Sicherung land- und forstwirtschaftlicher Betriebe (Grundstücksverkehrsgesetz – GrdstVG) grundsätzlich der Genehmigung der Kreisverwaltungsbehörde (§ 3 Abs. 1 GrdstVG in Verbindung mit Art. 1 Abs. 1 Satz 1 des bayerischen (Landes-)Ausführungsgesetzes – AGGrdstLPachtVG).

§ 2 GrdstVG Genehmigungspflichtige Geschäfte
(1) [1]Die rechtsgeschäftliche Veräußerung eines Grundstücks und der schuldrechtliche Vertrag hierüber bedürfen der Genehmigung.

§ 3 GrdstVG Genehmigungsbehörde; Antragsberechtigter
(1) Über den Antrag auf Genehmigung entscheidet die nach Landesrecht zuständige Behörde (Genehmigungsbehörde), soweit nicht das Gericht zu entscheiden hat.

Art. 1 AGGrdstLPachtVG
(1) [1]Genehmigungsbehörde im Sinn des Grundstücksverkehrsgesetzes ist die Kreisverwaltungsbehörde.

Die Kreisverwaltungsbehörde hat in diesem Zusammenhang zu prüfen, ob die Genehmigung aufgrund der in § 9 GrdstVG genannten Gründe zu versagen, durch Auflagen (§ 10 GrdstVG) oder Bedingungen (§ 11 GrdstVG) einzuschränken oder uneingeschränkt zu erteilen ist (insbesondere nach § 8 GrdstVG).

§ 9 GrdstVG Versagung oder Einschränkung der Genehmigung
(1) Die Genehmigung darf nur versagt oder durch Auflagen (§ 10) oder Bedingungen (§ 11) eingeschränkt werden, wenn Tatsachen vorliegen, aus denen sich ergibt, daß
1. die Veräußerung eine ungesunde Verteilung des Grund und Bodens bedeutet oder
2. durch die Veräußerung das Grundstück oder eine Mehrheit von Grundstücken, die räumlich oder wirtschaftlich zusammenhängen und dem Veräußerer gehören, unwirtschaftlich verkleinert oder aufgeteilt würde oder
3. der Gegenwert in einem groben Mißverhältnis zum Wert des Grundstücks steht.

§ 10 GrdstVG Genehmigung unter Auflagen
(1) Dem Erwerber kann die Auflage gemacht werden,
1. das erworbene Grundstück an einen Landwirt zu verpachten;
2. das erworbene Grundstück ganz oder zum Teil zu angemessenen Bedingungen entweder an einen Landwirt oder an ein von der Siedlungsbehörde zu bezeichnendes Siedlungsunternehmen zu veräußern;
3. an anderer Stelle binnen einer bestimmten, angemessenen Frist Land abzugeben, jedoch nicht mehr, als der Größe oder dem Wert des erworbenen Grundstücks entspricht;
4. zur Sicherung einer ordnungsgemäßen Waldbewirtschaftung einen Bewirtschaftungsvertrag mit einem forstlichen Sachverständigen oder einer

Forstbehörde abzuschließen oder nach einem genehmigten Wirtschaftsplan zu wirtschaften.

§ 11 GrdstVG Genehmigung unter Bedingungen
(1) Die Genehmigung kann unter der Bedingung erteilt werden, daß binnen einer bestimmten Frist
1. *die Vertragsparteien einzelne Vertragsbestimmungen, denen Bedenken aus einem der in § 9 aufgeführten Tatbestände entgegenstehen, in bestimmter Weise ändern,*
2. *der Erwerber das landwirtschaftliche Grundstück auf eine bestimmte Zeit an einen Landwirt verpachtet,*
3. *der Erwerber an anderer Stelle Land abgibt, jedoch nicht mehr, als der Größe oder dem Wert des zu erwerbenden Grundstücks entspricht.*

Vor der Entscheidung über einen Genehmigungsantrag hat die Kreisverwaltungsbehörde nach § 19 GrdstVG in Verbindung mit § 2 der zugehörigen (Landes) Durchführungsverordnung (DVGrdstVG) die Kreisgeschäftsstelle des BBV zu hören. Diese bindet den BBV Obmann der jeweiligen Gemeinde ein.

§ 2 DVGrdstVG
[1]Vor der Entscheidung über den Genehmigungsantrag hat die Kreisverwaltungsbehörde die Kreisgeschäftsstelle des Bayerischen Bauernverbands zu hören.

Eine im Rahmen dieser Anhörung erfolgende Übermittlung personenbezogener Daten durch die Kreisverwaltungsbehörde an den BBV – der als Körperschaft des öffentlichen Rechts eine öffentliche Stelle darstellt – muss insbesondere mit dem in Art. 18 Abs. 1 BayDSG niedergelegten Erforderlichkeitsgrundsatz vereinbar sein. Das bedeutet, dass die Kreisverwaltungsbehörde **stets nur diejenigen personenbezogenen Daten an den BBV übermitteln darf, die dieser zur Abgabe einer sachgerechten Stellungnahme nach dem Grundstücksverkehrsgesetz im konkreten Einzelfall tatsächlich benötigt**. Je nach Lage des Einzelfalls dürfen somit personenbezogene Daten in unterschiedlichem Umfang übermittelt werden. So kann z.B. die Übermittlung des Kaufpreises zur Beurteilung eines groben Missverhältnisses von Kaufpreis und Grundstückswert – dies wäre ein Versagungsgrund gemäß § 9 Abs. 1 Nr. 3 GrdstVG – in einem entsprechend gelagerten Einzelfall erforderlich sein. Eine standardmäßige Übermittlung des gesamten Kaufvertrages an den BBV wird danach aber regelmäßig unzulässig sein, ebenso eine in etwaigen Mustervordrucken vorgesehene pauschale Übermittlung des Kaufpreises. Daran ändert sich auch in Fällen nichts, in denen Vorkaufsrechte nach dem Reichssiedlungsgesetz bestehen. Auch insoweit bleibt der BBV auf seine aus dem GrdstVG folgenden Aufgaben beschränkt.

Im Rahmen der anhand der konkreten Umstände des Einzelfalles zu beurteilenden Erforderlichkeit ist auch die Nutzung beim BBV vorhandener personenbezogener Daten durch dessen Ortsobleute – als satzungsmäßige Organe des BBV – gemäß Art. 17 Abs. 1 Nr. 1 BayDSG zulässig. Bei Beachtung des Erforderlichkeitsgrundsatzes ist ebenso die entsprechende (Rück-)Übermittlung personenbezogener Daten durch den BBV an die Kreisverwaltungsbehörde datenschutzrechtlich zulässig. Da Genehmigungsauflagen gemäß § 10 Abs. 1 Nr. 1 und 2 GrdstVG – also das erworbene Grundstück an einen Landwirt zu verpachten oder ganz oder teilweise zu angemessenen Bedingungen zu veräußern – behördlicherseits nur dann in Betracht kommen, wenn an diesem Grundstück Landwirte interessiert sind, ist es dem BBV nicht von vornherein verwehrt, entsprechende Ermittlungen

unter den Landwirten (mit der gebotenen Zurückhaltung) anzustellen und diesbezügliche Erkenntnisse in seiner Stellungnahme niederzulegen.

14 Datenschutzkommission

Der Datenschutzkommission beim Bayerischen Landtag gehörten in den vergangenen zwei Jahren folgende Mitglieder bzw. stellvertretende Mitglieder an:

Für den Landtag:

Bis zum Ende der 16. Wahlperiode:

Mitglieder:

Eberhard Rotter, CSU
Walter Taubeneder, CSU
Prof. Dr. Winfried Bausback, CSU
Dr. Florian Herrmann, CSU
Florian Ritter, SPD
Alexander Muthmann, Freie Wähler
Christine Kamm, BÜNDNIS 90/DIE GRÜNEN
Dr. Andreas Fischer, FDP

stellvertretende Mitglieder:

Peter Schmid, CSU
Alexander König, CSU
Manfred Ländner, CSU
Dr. Franz Rieger, CSU
Horst Arnold, SPD
Mannfred Pointner, Freie Wähler
Susanna Tausendfreund, BÜNDNIS 90/DIE GRÜNEN
Karsten Klein, FDP

Ab dem 04.12.2013:

Mitglieder:

Eberhard Rotter, CSU
Max Gibis, CSU
Walter Nussel, CSU
Florian Ritter, SPD
Eva Gottstein, Freie Wähler
Verena Osgyan, BÜNDNIS 90/DIE GRÜNEN

stellvertretende Mitglieder:

Tobias Reiß, CSU
Thorsten Schwab, CSU
Michael Brückner, CSU
Alexandra Hiersemann, SPD
Bernhard Pohl, Freie Wähler
Ulrike Gote, BÜNDNIS 90/DIE GRÜNEN

Auf Vorschlag der Staatsregierung:

Mitglied:

Christian Peter Wilde, Ltd. Ministerialrat a.D. im Staatsministerium des Innern, für Bau und Verkehr **bis zum 24.02.2014**

Friederike Sturm, Ministerialrätin im Staatsministerium der Finanzen, für Landesentwicklung und Heimat **ab dem 25.02.2014**

stellvertretendes Mitglied:

Armin Schwimmbeck, Ministerialrat im Staatsministerium für Wirtschaft und Medien, Energie und Technologie **bis zum 24.02.2014**

Michael Will, Ministerialrat im Staatsministerium des Innern, für Bau und Verkehr **ab dem 25.02.2014**

Auf Vorschlag der kommunalen Spitzenverbände in Bayern:

Mitglied:

Rudolf Schleyer, Mitglied des Vorstands der AKDB

stellvertretendes Mitglied:

Doris Kirmeyer, Datenschutzbeauftragte bei der AKDB **bis zum 24.02.2014**

Gudrun Aschenbrenner, Abteilungsleiterin der AKDB **ab dem 25.02.2014**

Auf Vorschlag des Staatsministeriums für Arbeit und Soziales, Familie und Integration aus dem Bereich der gesetzlichen Sozialversicherungsträger:

Mitglied:

Werner Krempl, Erster Direktor und Vorsitzender der Geschäftsführung der Deutschen Rentenversicherung Nordbayern

stellvertretendes Mitglied:

Dr. Helmut Platzer, Vorstandsvorsitzender der AOK Bayern

Auf Vorschlag des Verbands Freier Berufe in Bayern e.V.:

Mitglied:

Hans-Ulrich Sorge, Notar **bis zum 24.02.2014**

Dr. Till Schemmann, Notar **ab dem 25.02.2014**

stellvertretendes Mitglied:

Dr. Janusz Rat, Vorsitzender der Kassenzahnärztlichen Vereinigung Bayerns

Herr Eberhard Rotter, MdL, führt den Vorsitz in der Datenschutzkommission; stellvertretender Vorsitzender ist Herr Florian Ritter, MdL.

Die Datenschutzkommission beim Bayerischen Landtag tagte im vergangenen Berichtszeitraum sechs Mal. Dabei befasste sie sich u.a. mit folgenden Themen:

— Vorberatung des 26. Tätigkeitsberichts 2014
— Berichte über Beanstandungen
— Berichte von Datenschutzkonferenzen
— Berichte vom Europäischen Datenschutztag
— Vorratsdatenspeicherung
— Videoüberwachung
— Neues Melderecht
— Nutzung von Sozialen Netzwerken durch bayerische öffentliche Stellen

Anlage 1:
Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 25.01.2013
Beschäftigtendatenschutz nicht abbauen, sondern stärken!

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder erinnert an ihre Entschließung vom 16./17.03.2011 und ihre Forderung nach speziellen Regelungen zum Beschäftigtendatenschutz. Bei einer Gesamtbetrachtung ist die Konferenz enttäuscht von dem jetzt veröffentlichten Änderungsentwurf der Koalitionsfraktionen.

Bereits der ursprünglich von der Bundesregierung vorgelegte Entwurf enthielt aus Datenschutzsicht erhebliche Mängel. Der nun vorgelegte Änderungsentwurf nimmt zwar einzelne Forderungen – etwa zum Konzerndatenschutz – auf und stärkt das informationelle Selbstbestimmungsrecht auch gegenüber Tarifverträgen und Betriebsvereinbarungen. Das Datenschutzniveau für die Beschäftigten soll jedoch in einigen wesentlichen Bereichen sogar noch weiter abgesenkt werden.

Besonders bedenklich sind die folgenden Regelungsvorschläge:

— Die Möglichkeiten der offenen Videoüberwachung am Arbeitsplatz sollen noch über das bisher Geplante hinaus ausgeweitet werden. Überdies ist die Beschreibung der zuzulassenden Überwachungszwecke unverständlich und würde deshalb nicht zur Rechtssicherheit beitragen.

— Beschäftigte in Call-Centern sollen noch stärker überwacht werden können, als dies der Regierungsentwurf ohnehin schon vorsah. Die Beschäftigten müssen sich nunmehr auf eine jederzeit mögliche, unbemerkte Überwachung einstellen. Hierdurch kann ein unzumutbarer Überwachungsdruck entstehen.

— Die Datenerhebungsbefugnisse im Bewerbungsverfahren sollen erweitert werden. Der noch im Regierungsentwurf vorgesehene Ausschluss von Arbeitgeberrecherchen über Bewerberinnen und Bewerber in sozialen Netzwerken außerhalb spezieller Bewerbungsportale wurde gestrichen. Damit wird der Grundsatz der Direkterhebung bei den Betroffenen weiter unterlaufen.

— Dem Arbeitgeber soll es gestattet sein, auch nicht allgemein zugängliche Beschäftigtendaten bei Dritten zu erheben, wenn die Beschäftigten eingewilligt haben. Die tatsächliche Freiwilligkeit einer solchen Einwilligung ist fraglich.

— Die im Regierungsentwurf enthaltene Vorgabe, Eignungstests grundsätzlich nach wissenschaftlich anerkannten Methoden durchzuführen, soll wieder entfallen.

Die Konferenz appelliert an den Bundestag, bei seinen Beratungen zum Gesetz den Forderungen der Datenschutzbeauftragten Rechnung zu tragen.

Anlage 2:
Entschließung der 85. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 13./14.03.2013
Datenschutz auch in einer transatlantischen Freihandelszone gewährleisten

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder weist auf die Notwendigkeit hin, bei den angekündigten Verhandlungen zwischen der Europäischen Union und der Regierung der Vereinigten Staaten über eine transatlantische Freihandelszone auch die unterschiedlichen datenschutzrechtlichen Rahmenbedingungen zu thematisieren. Dabei muss sichergestellt werden, dass das durch die Europäische Grundrechtecharta verbriefte Grundrecht auf Datenschutz und die daraus abgeleiteten Standards gewahrt bleiben.

Von der Kommission erwartet die Konferenz der Datenschutzbeauftragten des Bundes und der Länder, dass sie bei den Verhandlungen das Ziel einer grundrechtsorientierten Wertegemeinschaft nicht aus dem Auge verliert. Keineswegs dürfen durch die angestrebte transatlantische Wirtschaftsunion europäische Grundrechtsgewährleistungen abgeschwächt werden. Auch wäre es nicht hinzunehmen, wenn sich die Verhandlungen negativ auf den durch die Europäische Kommission angestoßenen Reformprozess des EU-Datenschutzrechts auswirken würden.

Die Konferenz sieht in der vom US-Präsidenten vorgeschlagenen Freihandelszone die Chance, international eine Erhöhung des Datenschutzniveaus zu bewirken. Sie begrüßt daher die vom US-Präsidenten angekündigte Initiative für verbindliche Vorgaben zum Datenschutz in der Wirtschaft. Sie erinnert daran, dass nach den Vorgaben der Welthandelsorganisation der Datenschutz kein Handelshindernis darstellt.

Anlage 3:
Entschließung der 85. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 13./14.03.2013
Pseudonymisierung von Krebsregisterdaten verbessern

In allen Ländern werden Daten über individuelle Fälle von Krebserkrankungen in Krebsregistern gespeichert, um sie der epidemiologischen Forschung zur Verfügung zu stellen. Zum Schutz der Betroffenen werden die Daten in allen Ländern (außer Hamburg) mit Kontrollnummern nach § 4 Bundeskrebsregisterdatengesetz (BKRG) pseudonymisiert gespeichert. Als Pseudonyme werden so genannte Kontrollnummern verwendet. Kontrollnummern werden darüber hinaus von allen Ländern zum Abgleich der Daten der epidemiologischen Krebsregister untereinander und mit dem Zentrum für Krebsregisterdaten nach § 4 BKRG verwendet.

Die Datenschutzbeauftragten von Bund und Ländern sind der Auffassung, dass das vor ca. 20 Jahren entwickelte Verfahren zur Bildung der Kontrollnummer den erforderlichen Schutz dieser höchst sensiblen Daten nicht mehr in ausreichendem Maße gewährleisten kann. Dies ist auf die folgenden Entwicklungen zurückzuführen:

- Das Anwachsen der für eine Depseudonymisierung verfügbaren Rechenkapazität hat die Schutzwirkung der bei den Krebsregistern genutzten kryptographischen Hashfunktion aufgehoben, die derzeit als erste Komponente bei der Kontrollnummernbildung verwendet wird.

- Die Wechselwirkungen zwischen mehreren Verfahren im Umfeld der epidemiologischen Krebsregistrierung verursachen Risiken im Zuge der erforderlichen Entschlüsselungen und der gemeinsamen Verwendung von geheimen Schlüsseln, die bisher nicht berücksichtigt wurden.

Diese Entwicklungen machen es erforderlich, die Regeln zur Bildung der Kontrollnummern zu überarbeiten. Hierbei ist das Umfeld aller Verfahren in Betracht zu ziehen, in dem Kontrollnummern zum Einsatz kommen beziehungsweise absehbar kommen sollen. Hierzu hat der Arbeitskreis "Technische und organisatorische Datenschutzfragen" der Datenschutzkonferenz einen entsprechenden Anforderungskatalog formuliert (siehe Anlage zu dieser Entschließung (PDF)).

Die Datenschutzkonferenz fordert die zuständigen Fachaufsichtsbehörden der Länder auf, für eine koordinierte Umstellung des Verfahrens bei den ihrer Aufsicht unterstehenden Stellen zu sorgen, die Kontrollnummern bilden oder verwenden. Sie empfiehlt den Ländern, für den Datenaustausch klinischer Krebsregister mit den Auswertungsstellen der klinischen Krebsregistrierung auf Landesebene nach dem Krebsfrüherkennungs- und -registergesetz ein Pseudonymisierungsverfahren anzuwenden, das im Wesentlichen den gleichen Anforderungen genügt.

Die entsprechenden Vorgaben für den Datenabgleich nach § 4 BKRG sollten durch das Bundesministerium für Gesundheit in einer Verordnung nach § 4 Abs. 3 BKRG festgelegt werden.

Anlage 4:
Erläuterungen zur Entschließung der 85. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 13./14.03.2013
„Europa muss den Datenschutz stärken“

- **Jedes personenbeziehbare Datum muss geschützt werden**

  Nach Art. 8 Abs. 1 der Charta der Grundrechte der Europäischen Union (Grundrechtecharta) hat jede Person das Recht auf Schutz der sie betreffenden personenbezogenen Daten. Daher muss das europäische Datenschutzrecht unterschiedslos alle Daten erfassen, die einer natürlichen Person zugeordnet werden können. Personenbezogene Daten sollten als Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren Person definiert werden. Dies schließt auch pseudonyme Daten oder Identifizierungsmerkmale wie zum Beispiel IP-Adressen, Kenn-Nummern, Standortdaten ein.

- **Es darf keine grundrechtsfreien Räume geben**

  Die Bestrebungen, ganze Datenkategorien wie etwa Beschäftigtendaten und ganze Berufsgruppen wie Freiberufler aus dem Anwendungsbereich

des Datenschutzgrundrechtes herauszunehmen, kollidiert mit dem Grundsatz der universalen Geltung von Grundrechten. Die pauschale Entbindung von kleinen, mittleren und Kleinstunternehmen von zentralen datenschutzrechtlichen Verpflichtungen verkennt, dass es für den Grad des Eingriffes in das Grundrecht unerheblich ist, wie viele Beschäftigte das in dieses Recht eingreifende Unternehmen hat.

— Einwilligungen müssen ausdrücklich erteilt werden

Die Einwilligung in die Verarbeitung personenbezogener Daten kann nur dann rechtswirksam sein, wenn sie auf einer eindeutigen und ausdrücklichen Willensbekundung des Betroffenen in Kenntnis der Sachlage beruht. An der Anforderung, dass eine wirksame Einwilligung auf tatsächlich freiwilliger Entscheidung beruhen muss, darf es keine Abstriche geben. Eine unter faktischem Zwang abgegebene Erklärung muss auch weiterhin unwirksam sein. Aufweichungen der Vorschläge der Kommission und des Berichterstatters im federführenden Ausschuss für Bürgerrechte sowie der Forderungen des Europäische Parlaments in dessen Entschließung vom 6. Juli 2011 (Punkte 11, 12) darf es – auch mit Blick auf Art. 8 Abs. 2 der Grundrechtecharta – nicht geben. Es gilt, die Kompetenz zum Selbstdatenschutz zu fördern.

— Datenverarbeiter dürfen ihre Ziele nicht eigenmächtig verändern

Der bestehende Grundsatz der Zweckbindung ist ein zentraler Baustein zur Gewährleistung der Transparenz und Vorhersehbarkeit der Datenverarbeitung und muss erhalten bleiben, so wie es auch – in Anlehnung an Art. 8 Abs. 2 der Grundrechtecharta – das Europäische Parlament in der Entschließung vom 6. Juli 2011 (Punkt 11) gefordert hat. Daten sollen auch zukünftig nur für den Zweck verarbeitet werden dürfen, zu dem sie erhoben wurden. Ergänzend sollte geregelt werden, dass die Zwecke, für die personenbezogene Daten erhoben werden, konkret festzulegen sind.

— Profilbildung muss beschränkt werden

Die Profilbildung, also die Zusammenführung vieler Daten über eine bestimmte Person, muss effektiv beschränkt werden. Die vorgelegten Vorschläge dürfen nicht minimiert werden. Die Anforderungen an die Rechtmäßigkeit der Profilbildung müssen vielmehr erhöht und festgelegt werden, dass besondere Kategorien personenbezogener Daten wegen ihrer hohen Sensitivität nicht in eine Profilbildung einfließen dürfen. Die Profilbildungsregelung muss auf jede systematische Verarbeitung zur Profilbildung Anwendung finden. Zudem muss klargestellt werden, dass auch der Online-Bereich, beispielsweise die Auswertung des Nutzerverhaltens oder die Bildung von Sozialprofilen in sozialen Netzwerken zur adressatengerechten Werbung und Scoring-Verfahren mit erfasst sind.

— Stärkung der Eigenverantwortung der Datenverarbeiter durch betriebliche Datenschutzbeauftragte

Die Konferenz weist auf die positiven Erfahrungen mit den betrieblichen Datenschutzbeauftragten in Deutschland hin. Das Vorhaben der Kommission, eine Bestellungspflicht für einen Datenschutzbeauftragten erst ab 250 Beschäftigten zu normieren, bedroht insofern eine gewachsene und

erfolgreiche Struktur des betrieblichen Datenschutzes in Deutschland. Bei risikobehafteter Datenverarbeitung sollte die Bestellungspflicht unabhängig von der Mitarbeiterzahl bestehen. Die Eigenverantwortung der Datenverarbeiter darf auch nicht dadurch abgeschwächt werden, dass die Aufsichtsbehörden Verfahren in großem Umfang vorab genehmigen oder dazu vorab zu Rate gezogen werden müssen. Vielmehr muss die Eigenverantwortlichkeit zunächst durch eine leistungsfähige Selbstkontrolle gewährleistet werden.

– **Datenverarbeiter dürfen sich ihre Aufsichtsbehörde nicht aussuchen können**

Ein kohärenter Datenschutz in der EU setzt neben einer einheitlichen Regelung auch eine einheitliche Auslegung und einen einheitlichen Rechtsvollzug durch die Aufsichtsbehörden voraus. Bei einer ausschließlichen Zuständigkeit einer Aufsichtsbehörde ist zu befürchten, dass das Unternehmen seine Hauptniederlassung jeweils in dem Mitgliedstaat nimmt, in dem mit einem geringeren Grad an Durchsetzungsfähigkeit oder Durchsetzungswillen der jeweiligen Aufsichtsbehörde gerechnet wird. Eine Aufweichung der Datenschutzstandards wäre die Folge. Für den Fall der Untätigkeit einer federführenden Behörde müssen rechtliche Strukturen gefunden werden, die einen effektiven Vollzug des Datenschutzrechts gewährleisten.

– **Völlige Unabhängigkeit der Aufsichtsbehörden auch gegenüber der Kommission**

Ein Letztentscheidungsrecht der Kommission bei der Rechtsdurchsetzung, wie im Kommissionsentwurf vorgesehen, verletzt die Unabhängigkeit der datenschutzrechtlichen Aufsichtsbehörden und des europäischen Datenschutzausschusses und ist daher abzulehnen. Diese Kompetenzen der Kommission sind mit Art. 8 Abs. 3 der Grundrechtecharta und Art. 16 Abs. 2 Satz 2 des Vertrages über die Arbeitsweise der EU (AEUV) nicht vereinbar, wonach die Einhaltung des EU-Datenschutzes unabhängigen Aufsichtsbehörden übertragen ist. In Anlehnung an die Forderungen des Europäischen Parlaments in der Entschließung vom 6. Juli 2011 (Punkte 42 bis 44) sollte als Folge der Unabhängigkeit der Aufsichtsbehörden statt der Kommission ausschließlich der Europäische Datenschutzausschuss über Sachverhalte und Maßnahmen, die dem Kohärenzverfahren unterfallen, entscheiden.

– **Grundrechtsschutz braucht effektive Kontrollen**

Die Sanktionen müssen – wie schon das Europäische Parlament in der Entschließung vom 6. Juli 2011 (Punkt 33) deutlich gemacht hat – abschreckend und damit geeignet sein, dass die Verantwortlichen und Datenverarbeiter die Datenschutzvorschriften nachhaltig einhalten. Die Aufsichtsbehörden müssen im Rahmen ihrer Unabhängigkeit darüber entscheiden können, ob und inwieweit sie von den Sanktionsmöglichkeiten Gebrauch machen. Ohne spürbare Bußgelddrohungen würde die Datenschutzkontrolle gegen Unternehmen zahnlos bleiben. Die von der Kommission vorgesehenen Sanktionsmöglichkeiten sollten daher auf jeden Fall beibehalten werden.

– Hoher Datenschutzstandard für ganz Europa

Für Bereiche ohne konkreten Bezug zum Binnenmarkt sehen einige Mitgliedstaaten bereits heute zahlreiche Regelungen vor, die den Datenschutzstandard der allgemeinen Datenschutzrichtlinie 95/46 EG hinausgehen. Sie berücksichtigen unter anderem besondere Schutzbedarfe und haben maßgeblich zur Fortentwicklung des europäischen Datenschutz-Rechtsrahmens beigetragen. Deshalb sollte eine Datenschutz-Grundverordnung Gestaltungsspielräume für einen weitergehenden Datenschutz eröffnen.

Anlage 5:
Entschließung der 86. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 01./02.10.2013
Sichere elektronische Kommunikation gewährleisten

Ende-zu-Ende-Verschlüsselung einsetzen und weiterentwickeln

Die elektronische Datenübermittlung zwischen den Bürgern beziehungsweise der Wirtschaft und der öffentlichen Verwaltung im Zusammenhang mit E-Government-Verfahren erfordert insbesondere auch mit Blick auf die umfassenden und anlasslosen Überwachungsmaßnahmen ausländischer Geheimdienste technische und organisatorische Maßnahmen, um den Anforderungen an Datenschutz und Datensicherheit gerecht zu werden. Zur Sicherung der Vertraulichkeit, Integrität, Authentizität, Zweckbindung und Transparenz bei der Datenübertragung sind kryptographische Verfahren erforderlich. Diese Verfahren können sowohl die Verbindungen zwischen den Endpunkten der Übertragung (Ende-zu-Ende-Verschlüsselung) als auch die Verbindungen zwischen den an der Übertragung beteiligten Netzknoten (Verbindungsverschlüsselung) sichern.

Für die Ende-zu-Ende-Verschlüsselung steht mit dem Online Services Computer Interface (OSCI-Transport) bereits seit einigen Jahren ein bewährter Standard zur Verfügung, den die Datenschutzkonferenz bereits im Jahr 2005 mit der Entschließung "Sicherheit bei E-Government durch Nutzung des Standards OSCI" Bund, Ländern und Kommunen empfohlen hat. Das so genannte Verbindungsnetz, über das nach dem Netzgesetz ab 2015 jegliche Datenübermittlung zwischen den Ländern und dem Bund erfolgen muss, stellt hingegen nur eine Verbindungsverschlüsselung zwischen den Übergabepunkten zur Verfügung.

Die Datenschutzbeauftragten von Bund und Ländern weisen darauf hin, dass beide Ansätze sich ergänzen und dass deshalb auch nach Inbetriebnahme des Verbindungsnetzes der OSCI-Standard erforderlich ist.

Beide Ansätze haben ihre spezifischen Vor- und Nachteile, aus denen sich unterschiedliche Einsatzgebiete ergeben. Das Verbindungsnetz ist als geschlossenes Netz konzipiert. Durch die Infrastruktur des Verbindungsnetzes kann eine bestimmte Verfügbarkeit garantiert und die Vertraulichkeit der Nachrichten zwischen den Netzknoten gesichert werden.

An der OSCI-Infrastruktur kann hingegen prinzipiell jede deutsche Behörde teilnehmen. Mit OSCI kann die Vertraulichkeit der übertragenen Inhalte zwischen

zwei Kommunikations-Endpunkten gesichert werden, so dass an keiner Zwischenstation im Netz Nachrichten im Klartext unbefugt gelesen oder geändert werden können. Anders als bei der Verbindungsverschlüsselung kann mit OSCI die Integrität und Authentizität der übermittelten Nachricht gegenüber Dritten nachgewiesen werden. Darüber hinaus können OSCI-gesicherte Nachrichten nicht unbemerkt verloren gehen und der Zugang von Sendungen kann mittels Quittungen bestätigt werden. Schließlich ist das Anbringen elektronischer Signaturen nach dem Signaturgesetz möglich.

Deshalb halten die Datenschutzbeauftragten des Bundes und der Länder den Einsatz von Standards zur Ende-zu-Ende-Verschlüsselung wie OSCI-Transport für geboten und fordern den IT-Planungsrat auf, diese kontinuierlich weiterzuentwickeln und verbindlich festzulegen. Sie fordern daneben Bund, Länder und Kommunen auf, die vorhandenen Standards bereits jetzt einzusetzen.

Anlage 6:
Entschließung der 86. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 01./02.10.2013
Stärkung des Datenschutzes im Sozial- und Gesundheitswesen

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

Vor dem Hintergrund des sich verschärfenden Wettbewerbs der Beteiligten im Sozial- und Gesundheitswesen geraten die Rechte der Patientinnen und Patienten und Versicherten immer stärker unter Druck. Dies zeigt sich zum Beispiel darin, dass eine Reihe von Krankenkassen und andere Sozialleistungsträger im Rahmen der Informationsbeschaffung die Empfänger von gesetzlichen Leistungen (zum Beispiel Krankengeld) über ihren Gesundheitszustand über das erforderliche Maß hinaus befragen und dabei gesetzlich vorgesehene Verfahren wie zum Beispiel die Einschaltung des Medizinischen Dienstes der Krankenversicherung umgehen.

Auch durch die Einbindung des Internets bei der Informationsverarbeitung im Gesundheitswesen, zum Beispiel durch Nutzung von Cloud-Diensten, sozialen Netzwerken und Big-Data-Strukturen, sowie durch die weit verbreitete Arbeitsteilung im Medizinbereich und insbesondere die Einschaltung von informationstechnischen Dienstleistern (Outsourcing) wird die Gefahr von "gläsernen Patientinnen und Patienten oder Versicherten" weiter verstärkt.

Der Wettbewerb im Sozial- und Gesundheitswesen darf nicht zu Lasten der Rechte von Patientinnen und Patienten und Versicherten ausgetragen werden. Bei der künftigen Ausgestaltung des Gesundheitsbereichs müssen die Schutzrechte für die Privat- und Intimsphäre nachhaltig gestärkt und für Transparenz gesorgt werden.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder appelliert an die Regierungen und Parlamente des Bundes und der Länder:

— Bei der Nutzung neuer technischer Möglichkeiten muss das Recht auf informationelle Selbstbestimmung als unverzichtbares Grundrecht von vornherein berücksichtigt werden (privacy by design). Die Entwicklung datenschutzfreundlicher Technologien, zum Beispiel von Anonymisierungs-, Pseudonymisierungs- und Verschlüsselungsverfahren, sollte gefördert und deren Einsatz nach dem aktuellen Stand der Technik gesetzlich abgesichert werden.

— Die Telematikinfrastruktur ist umgehend und funktionsfähig so zu realisieren, dass die medizinische Kommunikation zwischen den Beteiligten im Gesundheitsbereich vertraulich und zuverlässig realisiert wird und die Patientinnen und Patienten praktisch in die Lage versetzt werden, ihr Recht auf informationelle Selbstbestimmung wahrzunehmen.

— Für die zunehmende Einschaltung technischer Dienstleister durch Leistungserbringer, insbesondere niedergelassene Ärztinnen und Ärzte, müssen angemessene datenschutzgerechte gesetzliche Regelungen verabschiedet werden.

Anlage 7:
Entschließung der 86. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 01./02.10.2013
Handlungsbedarf zum Datenschutz im Bereich der Öffentlichen Sicherheit in der 18. Legislaturperiode des Deutschen Bundestages

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

Die internationalen Überwachungsaktivitäten von Nachrichtendiensten machen dies deutlich. Die Bundesrepublik Deutschland ist verpflichtet, sich dagegen zu wenden und auf europäischer und internationaler Ebene dafür einzusetzen, dass es keine umfassende Überwachung gibt. Hierzu hat die Konferenz bereits die Entschließung "Keine umfassende und anlasslose Überwachung durch Nachrichtendienste! Zeit für Konsequenzen" verabschiedet. Die Konferenz erwartet von der Bundesregierung außerdem, dass sie sich für die Aufhebung der EU-Richtlinie zur anlasslosen Vorratsdatenspeicherung von Telekommunikationsdaten einsetzt.

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

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

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

Anlage 8:
Entschließung der 86. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 01./02.10.2013
Forderungen für die neue Legislaturperiode: Die Datenschutzgrundrechte stärken!

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

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

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

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

- Angesichts der mit dem zunehmenden Wettbewerb im Sozial- und Gesundheitswesen verbundenen Risiken für die informationelle Selbstbestimmung müssen die Schutzrechte für die Privat- und Intimsphäre von Patientinnen, Patienten und Versicherten gestärkt werden.

- Die Vertraulichkeit und Integrität elektronischer Kommunikation sind zu fördern. Der öffentliche Bereich muss hier mit gutem Beispiel vorangehen und die Ende-zu-Ende-Verschlüsselung z.B. mit Hilfe von OSCI-Transport flächendeckend einsetzen.

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

Anlage 9:
Entschließung der 88. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 08./09.10.2014
Datenschutz im Kraftfahrzeug – Automobilindustrie ist gefordert

Der Konferenz der Datenschutzbeauftragten des Bundes und der Länder weist auf die datenschutzrechtlichen Risiken hin, die mit der zunehmenden Datenverarbeitung in Kraftfahrzeugen und ihrer Vernetzung untereinander, mit ihrer Umgebung und mit dem Internet entstehen. Die Datenverarbeitung in modernen Fahrzeugen schafft Begehrlichkeiten, die dort anfallenden Daten für die verschiedensten Zwecke nutzen zu wollen – etwa bei Arbeitgebern und Versicherungen. Dabei besteht die Gefährdungslage bereits im Zeitpunkt des Erfassens von Daten in den im Auto integrierten Steuergeräten und nicht erst mit deren Auslesen oder Übermitteln. Bereits diese personenbezogenen Daten geben Auskunft über Fahrverhalten und Aufenthaltsorte und können zur Informationsgewinnung über den Fahrer bzw. den Halter bis hin zur Bildung von Persönlichkeitsprofilen herangezogen werden.

Um eine selbstbestimmte Fahrzeugnutzung frei von Furcht vor Überwachung zu gewährleisten, sind Automobilhersteller, Händler, Verkäufer, Werkstätten ebenso wie Anbieter von Kommunikations- und Telediensten rund um das Kraftfahrzeug im Rahmen ihres Wirkungskreises in der Pflicht, informationelle Selbstbestimmung im und um das Kraftfahrzeug zu gewährleisten.

Dazu gehört:

- Bereits in der Konzeptionsphase sind bei der Entwicklung neuer Fahrzeugmodelle und neuer auf Fahrzeuge zugeschnittene Angebote für Kommunikations- und Teledienste die Datenschutzgrundsätze von privacy by design bzw. privacy by default zu verwirklichen.

- Datenverarbeitungsvorgängen im und um das Fahrzeug muss das Prinzip der Datenvermeidung und Datensparsamkeit zu Grunde liegen. Daten sind in möglichst geringem Umfang zu erheben und umgehend zu löschen, nachdem sie nicht mehr benötigt werden.

- Die Datenverarbeitungen müssen entweder vertraglich vereinbart sein oder sich auf eine ausdrückliche Einwilligung stützen.

- Für Fahrer, Halter und Nutzer von Fahrzeugen muss vollständige Transparenz gewährleistet sein. Dazu gehört, dass sie umfassend und verständlich darüber zu informieren sind, welche Daten beim Betrieb des Fahrzeugs erfasst und verarbeitet sowie welche Daten über welche Schnittstellen an wen und zu welchen Zwecken übermittelt werden. Änderungen sind rechtzeitig anzuzeigen. Die Betroffenen müssen in die Lage versetzt werden, weitere Nutzer ebenfalls zu informieren.

- Auch bei einer vertraglich vereinbarten oder von einer Einwilligung getragenen Datenübermittlung an den Hersteller oder sonstige Diensteanbieter sind Fahrer, Halter und Nutzer technisch und rechtlich in die Lage zu versetzen, Datenübermittlungen zu erkennen, zu kontrollieren und ggf. zu unterbinden. Zudem muss Wahlfreiheit für datenschutzfreundliche Systemeinstellungen und die umfangreiche Möglichkeit zum Löschen eingeräumt werden.

- Schließlich muss durch geeignete technische und organisatorische Maßnahmen Datensicherheit und -integrität gewährleistet sein. Dies gilt insbesondere für die Datenkommunikation aus Fahrzeugen heraus.

Auf dieser Grundlage wirkt die Konferenz der Datenschutzbeauftragten des Bundes und der Länder darauf hin, dass Automobilhersteller, Zulieferer und ihre Verbände bundesweit einheitliche Datenschutzstandards auf hohem Niveau setzen, die dazu beitragen, dass Innovation auch mit gesellschaftlicher Akzeptanz einhergeht.

Anlage 10:
Entschließung der 88. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 08./09.10.2014
Unabhängige und effektive Datenschutzaufsicht für Grundrechtsschutz unabdingbar

(Enthaltung: Bayern)

Die Bundesregierung hat am 27. August 2014 einen Gesetzentwurf zur Stärkung der Unabhängigkeit der Datenschutzaufsicht im Bund beschlossen (siehe Bun-

desrats-Drucksache 395/14). Er sieht vor, dass die bisher beim Bundesministerium des Inneren eingerichtete Bundesbeauftragte für den Datenschutz und die Informationsfreiheit in eine eigenständige oberste Bundesbehörde umgewandelt wird.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder begrüßt, dass nunmehr auch der Bundesgesetzgeber die vom Europäischen Gerichtshof in mehreren Urteilen konkretisierten Voraussetzungen für eine völlig unabhängige Datenschutzaufsicht herstellen will. Es ist erfreulich, dass die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit künftig keiner Aufsicht durch eine andere Behörde mehr unterliegen wird und aufgrund ihres Status' als eigenständiger oberster Bundesbehörde ohne jeden Einfluss anderer Behörden selbst über ihren eigenen Haushalt und ihr eigenes Personal verfügen kann.

Die Konferenz weist jedoch auf wesentliche Punkte hin, denen auch der Gesetzesentwurf keine beziehungsweise nur unzureichend Rechnung trägt:

— Eine effektive Datenschutzaufsicht setzt die rechtliche Stärkung der Durchsetzungsbefugnisse der Bundesbeauftragten für den Datenschutz und die Informationsfreiheit zwingend voraus. Ihr müssen in ihrem Zuständigkeitsbereich gegenüber den Post- und Telekommunikationsanbietern die gleichen Anordnungs- und Untersagungsbefugnisse eingeräumt werden, wie sie den Aufsichtsbehörden der Länder gegenüber der Privatwirtschaft schon seit Jahren zustehen. Der Bundesbeauftragten ist in diesem Bereich auch die Stellung einer Obersten Bundes- und Bußgeldbehörde einzuräumen. Nur dann stehen auch ihr wirksame Eingriffsbefugnisse, wie sie die Europäische Datenschutzrichtlinie fordert, zur Verfügung.

— Eine unabhängige, funktionsfähige und effektive Datenschutzkontrolle setzt zudem voraus, dass die BfDI als künftige oberste Bundesbehörde mit ausreichenden personellen und sächlichen Mitteln ausgestattet ist, um ihren gesetzlichen Kontroll- und Beratungsaufgaben nachkommen zu können. Entsprechendes gilt für alle Datenschutzbehörden in den Ländern. Ebenso wie in vielen Ländern ist dies für die Bundesbeauftragte für den Datenschutz und Information im vorliegenden Entwurf des Bundesdatenschutzgesetz nicht der Fall.

— Die Genehmigung, als Zeugin auszusagen, wird durch den Gesetzesentwurf in problematischer Weise eingeschränkt. Zwar wird der generelle Genehmigungsvorbehalt des BMI aufgehoben, das Gesetz sieht aber weite Ausnahmen hiervon vor, diese sind zu streichen. Zumindest muss das Letztentscheidungsrecht bei der Bundesbeauftragten für den Datenschutz und die Informationsfreiheit verbleiben.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder appelliert an den Bundesgesetzgeber, der Bundesbeauftragten sowohl effektive Sanktionsmöglichkeiten an die Hand zu geben als auch die nötigen Personalmittel für eine den Aufgaben entsprechende Personalausstattung zur Verfügung zu stellen. Die Konferenz erinnert auch die Länder daran, dass auch sie ihren Datenschutzaufsichtsbehörden ausreichend Personalmittel zur Verfügung stellen müssen, um die bereits bestehenden Kontrolldefizite zu Lasten der Bürgerinnen und Bürger und deren Grundrechtsschutz abzubauen.

Anlage 11:
Entschließung der 88. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 08./09.10.2014
Marktmacht und informationelle Selbstbestimmung

Die Konzentration wirtschaftlicher Macht und der Missbrauch marktbeherrschender Stellungen ist bisher Gegenstand des Wettbewerbs- und insbesondere des Kartellrechts. So untersucht gegenwärtig die Europäische Kommission mögliche Verstöße von Google gegen das Europäische Wettbewerbsrecht wegen mangelhafter Neutralität der Suchergebnisse.

Darüber hinaus ist jedoch zu lange übersehen worden, dass die zunehmenden Unternehmenskäufe vor allem im Bereich der Internetwirtschaft zu einer massiven Anhäufung von personenbezogenen Daten bis hin zur Monopolbildung in bestimmten Bereichen führen können. Datenmacht wird zur Marktmacht. Im April 2007 kaufte Google für 3,1 Mrd. US-Dollar das Werbeunternehmen DoubleClick. Die Übernahme wurde sowohl von den Kartellbehörden in den USA und in Europa gebilligt, ohne dass die Auswirkungen dieser Übernahme auf den Datenschutz der Nutzer in diesen Entscheidungen berücksichtigt worden wäre. Facebook hat im vergangenen Jahr für die Übernahme von WhatsApp 18 Mrd. US-Dollar gezahlt. Auch dieser Zusammenschluss ist inzwischen sowohl in den USA als auch in der EU genehmigt worden, ohne dass es wirksame Garantien gegen eine weitere Verschlechterung des Datenschutzes gibt.

Sowohl der Europäische Datenschutzbeauftragte als auch die deutsche Monopolkommission haben inzwischen auf die möglichen Auswirkungen der Zusammenschlüsse gerade von solchen Internet-Unternehmen auf die informationelle Selbstbestimmung hingewiesen, deren Geschäftsmodelle wesentlich auf der Anhäufung von personenbezogenen Daten beruhen. Die massive Ausweitung von scheinbar kostenlosen Diensten und die wachsende Bedeutung von "Big Data" erfordert nach Ansicht des Europäischen Datenschutzbeauftragten einen intensiveren Dialog zwischen den Datenschutz- und den Kartellbehörden, um die Wahlfreiheit wie auch die informationelle Selbstbestimmung der Nutzer angesichts abnehmender Konkurrenz aufrechtzuerhalten oder wiederherzustellen und um die Aufsichtsbefugnisse koordiniert einzusetzen. Die Monopolkommission hat in ihrem XX. Hauptgutachten (2012/2013 – Kapitel I) für eine verstärkte Kooperation von Datenschutz- und Wettbewerbsbehörden plädiert und sich für eine schnelle Verabschiedung der europäischen Datenschutzgrundverordnung eingesetzt.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder setzt sich ebenfalls für eine Datenschutzgrundverordnung auf hohem Niveau ein. Sie ist davon überzeugt, dass insbesondere das Recht auf Datenportabilität sowohl die Souveränität des einzelnen Nutzers stärken als auch die auf der Sammlung personenbezogener Daten beruhende Machtposition einzelner Marktteilnehmer begrenzen kann.

Die Konferenz der Datenschutzbeauftragten weist daraufhin, dass eine stärkere Zusammenarbeit mit den Kartellbehörden sinnvoll ist. Ziel muss es dabei zugleich sein, den Datenschutz im Wettbewerb besser zu fördern.

Anlage 12:
Entschließung der 88. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 08./09.10.2014
Effektive Kontrolle von Nachrichtendiensten herstellen!

Die Enthüllungen über die Spähaktivitäten ausländischer Nachrichtendienste haben verdeutlicht, wie viele Kommunikationsdaten in der digitalisierten Welt anfallen, welche Begehrlichkeiten diese Daten offensichtlich auch bei Nachrichtendiensten demokratischer Länder wecken und mit welchen weitreichenden Methoden die Nachrichtendienste Informationen erfassen, sammeln und analysieren. Auch die deutschen Nachrichtendienste haben weitreichende Befugnisse zur Erhebung, Sammlung und Auswertung personenbezogener Daten sowie zum Austausch dieser untereinander bzw. mit Polizeibehörden. Die Befugnisse der Nachrichtendienste schließen auch die Überwachung der Telekommunikation ein. Damit einher geht im Bereich der strategischen Auslandsüberwachung des BND ein Kontrolldefizit. Auch eine Beteiligung des Bundesnachrichtendienstes durch Datenaustausch mit ausländischen Diensten steht im Raum. In den vergangenen Jahren wurden die gesetzlichen Befugnisse der Nachrichtendienste stetig erweitert. So wurden die Antiterrordatei und die Rechtsextremismusdatei als gemeinsame Dateien von Polizei und Nachrichtendiensten eingeführt sowie gemeinsame Zentren von Nachrichtendiensten und Polizeibehörden errichtet. Die Berichte der NSU-Untersuchungsausschüsse des Deutschen Bundestages und einiger Landesparlamente haben darüber hinaus erhebliche Kontrolldefizite auch bei den Verfassungsschutzämtern offengelegt. Nach der Einschätzung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder ist daher eine Reform der rechtsstaatlichen Kontrolle der deutschen Nachrichtendienste dringend geboten.

Für die Betroffenen ist die aufgrund der Befugnisse der Nachrichtendienste und Sicherheitsbehörden vorgenommene Datenverarbeitung in weitem Maße intransparent, daher ist auch der Individualrechtsschutz faktisch eingeschränkt. Umso wichtiger ist die Kontrolle durch unabhängige Stellen. In der Entscheidung zum Antiterrordateigesetz vom 24. April 2013 hat das Bundesverfassungsgericht insoweit hervorgehoben, dass der Verhältnismäßigkeitsgrundsatz bei Datenverarbeitungen, die für die Betroffenen nur eingeschränkt transparent sind, gesteigerte Anforderungen an eine wirksame Ausgestaltung der Kontrolle sowohl auf der Ebene des Gesetzes als auch der Verwaltungspraxis stellt. Eine wichtige Rolle kommt dabei den Datenschutzbeauftragten des Bundes und der Länder zu, die neben den parlamentarischen Kontrollinstanzen die Kontrolle über die Nachrichtendienste ausüben. Bestimmte Bereiche nachrichtendienstlicher Tätigkeiten sind der Eigeninitiativkontrolle durch die Datenschutzbeauftragten des Bundes und der Länder von vornherein entzogen. Es ist sinnvoll, das bei den Datenschutzbeauftragten des Bundes und der Länder bereits vorhandene Fachwissen auch in diesem Bereich zu nutzen und die Datenschutzbehörden mit den entsprechenden Prüfbefugnissen und den hierfür erforderlichen personellen Ausstattung und Sachmitteln auszustatten.

Das Bundesverfassungsgericht hat mit der Entscheidung vom 24. April 2013 zum Zusammenwirken zwischen den Datenschutzbeauftragten und den parlamentarischen Kontrollinstanzen festgestellt: „Wenn der Gesetzgeber eine informationelle Kooperation der Sicherheitsbehörden vorsieht, muss er auch die kontrollierende Kooperation zugunsten des Datenschutzes ermöglichen.“ In diesem Sinne darf die Verteilung der Kontrolle auf mehrere Stellen nicht die Effektivität der Kontrolle

einschränken. Für den Bereich der Telekommunikationsüberwachung nach dem Gesetz zur Beschränkung des Brief-, Post- und Fernmeldegeheimnisses ist die Kontrolle durch die G10-Kommission aus eigener Initiative derzeit gesetzlich nicht vorgesehen. Ebenso fehlt ein Kontrollmandat der Datenschutzbeauftragten für Beschränkungen des Fernmeldegeheimnisses. Vor dem Hintergrund der Ausführungen des Bundesverfassungsgerichtes erscheint eine Einbindung der Datenschutzbeauftragten neben den parlamentarischen Kontrollinstanzen aber erforderlich.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder fordert daher den Gesetzgeber auf, die Datenschutzbehörden mit entsprechenden Prüfbefugnissen auszustatten, damit das bei ihnen vorhandene Fachwissen auch in diesem Bereich genutzt werden kann.

Anlage 13:
Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 14.11.2014
Keine PKW-Maut auf Kosten des Datenschutzes!

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder (DSK) fordert die Bundesregierung auf, bei der geplanten Einführung einer allgemeinen Maut auf Bundesautobahnen und einzelnen Bundesfernstraßen auf eine automatisierte Erhebung, Verarbeitung und Nutzung von Fahrzeugkennzeichen aller Verkehrsteilnehmer über elektronische Kontrollpunkte zu verzichten. Für Abrechnungs- und Kontrollzwecke besteht hierfür kein Erfordernis, denn es stehen – beispielsweise durch Einführung einer physischen Vignette nach dem Vorbild anderer Staaten – mildere und gleichermaßen effektive Mittel zur Kontrolle der Entrichtung der Maut zur Verfügung, ohne täglich an hunderten Kontrollpunkten hunderttausende Kfz-Kennzeichen zu erfassen und zu speichern. Für die Kontrolle in Deutschland zugelassener Pkw ist die (optisch-)elektronische Überwachung schon deswegen nicht erforderlich, weil die Abrechnung über die Zulassungs- und Kfz-Steuerdaten erfolgen soll. Allein die Möglichkeit, sich die Infrastrukturabgabe für gänzlich ungenutzte Pkw erstatten zu lassen, rechtfertigt nicht die vorgesehene elektronische Erfassung und sogar dauerhafte – bis zu 13 Monaten währende – Speicherung von Bewegungsdaten in Deutschland zugelassener Pkw.

Die DSK lehnt die im Entwurf eines Infrastrukturabgabengesetzes geplante Einrichtung eines Zentralen Infrastrukturregisters beim Kraftfahrtbundesamt und einer Datei sämtlicher mautpflichtiger Autobahnnutzungen von Personenkraftwagen beim Bundesamt für Güterverkehr ab. Ebenso weist sie auf die Gefahren der Einbeziehung privater Betreiber in die Erhebung der Infrastrukturabgabe einerseits und eines privaten Dritten in die Überwachung der Infrastrukturabgabe andererseits im Hinblick auf die umfangreichen geplanten Befugnisse der Betreiber bzw. des Dritten zur Datenerhebung und -verarbeitung hin. Die DSK mahnt die Bundesregierung eindringlich zur Einhaltung der verfassungsrechtlich gebotenen Prinzipien der Datenvermeidung und Datensparsamkeit.

Anlage 14:
Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 14.11.2014
Anforderungen an den Schutz der Datenübermittlungen zwischen medizinischen Leistungserbringern und klinischen Krebsregistern

(Enthaltung: Bayern)

Zur Verbesserung der Versorgung von Krebspatienten bauen die Bundesländer derzeit auf bundesgesetzlicher Grundlage ein flächendeckendes Netz von klinischen Krebsregistern auf. Diese Register erhalten hierzu vielfältige Daten über alle krebskranken Personen von allen niedergelassenen Ärzten und Krankenhäusern, die sie behandeln. Andererseits sollen die Register den behandelnden Ärzten die empfangenen Patientendaten zum Abruf zur Verfügung stellen. Die hierbei übermittelten Daten sind hoch sensibel und können mannigfaltig missbraucht werden. Dem müssen die Maßnahmen zu ihrem Schutz entsprechen.

Mit dieser Entschließung legt die Konferenz einen Katalog von Anforderungen vor und ruft die Bundesländer auf, für deren Erfüllung bei der Ausgestaltung der Kommunikation zwischen medizinischen Leistungserbringern und den klinischen Krebsregistern Sorge zu tragen.

Abkürzungsverzeichnis

€	Euro
a.a.O.	am angegebenen Ort
a.D.	außer Dienst
ABl.	Amtsblatt der Europäischen Union
Abs.	Absatz
AGGrdstLPachtVG	Gesetz zur Ausführung des Grundstücksverkehrsgesetzes und des Landpachtverkehrsgesetzes
AGSG	Gesetz zur Ausführung der Sozialgesetze
AKDB	Anstalt für Kommunale Datenverarbeitung in Bayern
AKE	automatisierte Kennzeichenerfassung
Alt.	Alternative
Anm.	Anmerkung
AO	Abgabenordnung
App	Application, Anwendungsprogramm auf Smartphone
Art.	Artikel
ATD	Antiterrordatei
ATDG	Antiterrordateigesetz
AUC	Akademie für Unfallchirugie
Az.	Aktenzeichen
BayBG	Bayerisches Beamtengesetz
BayBhV	Bayerische Beihilfeverordnung
BayDSG	Bayerisches Datenschutzgesetz
BayEUG	Bayerisches Gesetz über das Erziehungs- und Unterrichtswesen
BayKiBiG	Bayerisches Kinderbildungs- und -betreuungsgesetz
BayKrG	Bayerisches Krankenhausgesetz
BayKRG	Bayerisches Krebsregistergesetz
BayMail	Plattform für sichere Kommunikation in Bayern
BayMRVG	Bayerisches Maßregelvollzugsgesetz
BayPVG	Bayerisches Personalvertretungsgesetz
BayRDG	Bayerisches Rettungsdienstgesetz
BayStVollzG	Bayerisches Strafvollzugsgesetz
BaySÜG	Bayerisches Sicherheitsüberprüfungsgesetz
BayUniKlinG	Bayerisches Universitätsklinikagesetz
BayVSG	Bayerisches Verfassungsschutzgesetz
BayVwVfG	Bayerisches Verwaltungsverfahrensgesetz
BayWoFG	Bayerisches Wohnraumförderungsgesetz
BBiG	Berufsbildungsgesetz
BBV	Bayerischer Bauernverband
BDSG	Bundesdatenschutzgesetz
BeamtStG	Beamtenstatusgesetz
BEM	Betriebliches Eingliederungsmanagement
BfDI	Die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit
BGB	Bürgerliches Gesetzbuch
BGBl.	Bundesgesetzblatt
BGH	Bundesgerichtshof
BKRG	Bundeskrebsregisterdatengesetz

BMF	Bundesministerium der Finanzen
BMI	Bundesministerium des Innern
BMV-Ä	Bundesmantelvertrag-Ärzte
BMV-Z	Bundesmantelvertrag-Zahnärzte
BND	Bundesnachrichtendienst
BRK	Bayerisches Rotes Kreuz
BSI	Bundesamt für Sicherheit in der Informationstechnik
BSO	Berufsschulordnung
BStBl	Bundessteuerblatt
Buchst.	Buchstabe
BV	Verfassung des Freistaates Bayern
BVerfGE	Entscheidungen des Bundesverfassungsgerichts (zitiert nach Band und Seite)
BWG	Bundeswahlgesetz
BYOD	Bring Your Own Device
BZRG	Bundeszentralregistergesetz
bzw.	beziehungsweise
ca.	circa
CD	Compact Disc
CDU	Christlich-Dekomokratische Union Deutschlands
CERT	Computer Emergency Response Team
CSU	Christlich-Soziale Union in Bayern
CT	Computertomographie
d.h.	das heißt
DBB	Digitales Bildungsnetz
DFN	Deutscher Forschungsnetzverein
DIN	Deutsches Institut für Normung e.V.
DIWO	Dialogorientiertes Wohngeldverfahren
DMDA	De-Mail-Diensteanbieter
DMS	Dokumentenmanagementsystem
DNA	Desoxyribonuclein Acid, Träger der Erbinformation
Durchführungsverordnung	Verordnung zur Durchführung des Art. 28 Abs. 2 des Bayerischen Datenschutzgesetzes
DV	Datenverarbeitung
DVBayDSG-KM	Verordnung zur Durchführung des Art. 28 Abs. 2 des Bayerischen Datenschutzgesetzes
DVGrdstVG	Verordnung zur Durchführung des Grundstücksverkehrsgesetzes
e.V.	eingetragener Verein
EDV	Elektronische Datenverarbeitung
EFZG	Entgeltfortzahlungsgesetz
EG	Europäische Gemeinschaft
E-Government	Elektronische Verwaltung
E-Learning	elektronisch unterstütztes Lernen
ELStAM	Elektronische Lohnsteuerabzugsmerkmale
E-Mail	Elektronische Post
EN	Europäische Normen
Erläuternde Hinweise	Bekanntmachung über erläuternde Hinweise zum Vollzug der datenschutzrechtlichen Bestimmungen für die Schulen
EStG	Einkommensteuergesetz
ESZ	Externes Sicherheitszentrum
etc.	et cetera

EU	Europäische Union
EuGH	Europäischer Gerichtshof
evtl.	eventuell
FDP	Freie Demokratische Partei
FeV	Fahrerlaubnis-Verordnung
ff.	fortfolgende
GBO	Grundbuchordnung
GBV	Grundbuchverfügung
GDVG	Gesundheitsdienst- und Verbraucherschutzgesetz
GG	Grundgesetz
ggf.	gegebenenfalls
GLKrWG	Gemeinde- und Landkreiswahlgesetz
GLKrWO	Gemeinde- und Landkreiswahlordnung
GmbH	Gesellschaft mit beschränkter Haftung
GrdstVG	Grundstücksverkehrsgesetz
GrSO	Grundschulordnung
GVBl	Bayerisches Gesetz- und Verordnungsblatt
GWG	Geldwäschegesetz
HSOG	Hessisches Gesetz über die öffentliche Sicherheit und Ordnung
https	Hyper Text Transfer Protocol Secure
i.S.d.	im Sinne des
IBA	Informationssystem für die Beschaffung und Auswertung
IfSG	Infektionsschutzgesetz
IGVP	Integrationsverfahren der Bayerischen Polizei
IMS	Rundschreiben des Staatsministeriums des Innern, für Bau und Verkehr
INPOL	Informationssystem der Polizei (bundesweit)
IP	Internet Protocol
IPbpR	Internationaler Pakt über die bürgerlichen und politischen Rechte
ISmed	Informationssystem der Medizinischen Dienste
IT	Informationstechnik
IuK	Informations- und Kommunikationstechnik
KAG	Kommunalabgabengesetz
KAN	Kriminalaktennachweis
Kfz	Kraftfahrzeug
KIS	Krankenhausinformationssystem
KMS	Schreiben des Staatsministeriums für Bildung und Kultus, Wissenschaft und Kunst
KPMD	kriminalpolizeilicher Meldedienst
KunstUrhG	Kunsturheberrechtsgesetz
KWMBl	Amtsblatt des Bayerischen Staatsministeriums für Bildung und Kultus, Wissenschaft und Kunst
lit.	Buchstabe
LlbG	Leistungslaufbahngesetz
Ltd.	Leitende(r)
LWG	Landtagswahlgesetz
m.w.N.	mit weiteren Nachweisen
MDK	Medizinischer Dienst der Krankenversicherung in Bayern
MdL	Mitglied des Landtages

MedHygV	Verordnung zur Hygiene und Infektionsprävention in medizinischen Einrichtungen
MeldeG	Meldegesetz
MeldFortG	Gesetz zur Fortentwicklung des Meldewesens
NADIS	Nachrichtendienstliches Informationssystem
NJW	Neue Juristische Wochenschrift
nPA	neuer Personalausweis
Nr.	Nummer
NSA	National Security Agency
o.ä.	oder ähnliches
o.g.	oben genannt
OH	Orientierungshilfe
OSCI	Online Services Computer Interface
OWiG	Ordnungswidrigkeitengesetz
PAG	Polizeiaufgabengesetz
PassG	Paßgesetz
PAuswG	Personalausweisgesetz
PC	Personalcomputer
PDF	Portable Document Format
PfleWoqG	Pflege- und Wohnqualitätsgesetz
PIAV	Polizeilicher Informations- und Analyseverbund
PIN	Personell Identification Number
PKI	Public-Key-Infrastruktur
PStV	Personenstandsverordnung
PUK	Personal Unblocking Key
RC4	Ron´s Code 4
RiStBV	Richtlinien für das Straf- und Bußgeldverfahren
Rn.	Randnummer
S/MIME	Secure/Mulitpurpose Internet Mail Extensions
SchfHwG	Schornsteigerfeger-Handwerksgesetz
SchKfrG	Schulwegkostenfreiheitsgesetz
SGB V	Sozialgesetzbuch Fünftes Buch – Gesetzliche Krankenversicherung
SGB VIII	Sozialgesetzbuch Achtes Buch – Kinder- und Jugendhilfe
SGB IX	Sozialgesetzbuch Neuntes Buch – Rehabilitation und Teilhabe behinderter Menschen
SGB X	Sozialgesetzbuch Zehntes Buch – Sozialverwaltungsverfahren und Sozialdatenschutz
SGB XI	Sozialgesetzbuch Elftes Buch – Soziale Pflegeversicherung
sog.	sogenannt
SPD	Sozialdemokratische Partei Deutschlands
SSL	Secure Socket Layer
StGB	Strafgesetzbuch
StPO	Strafprozessordnung
StVG	Straßenverkehrsgesetz
TK	Telekommunikation
TKG	Telekommunikationsgesetz
TKmed	medizinische Telekommunikationsplattform
TLS	Transportlayer Security
TMF	Technologie- und Methodenplattform für die vernetzte medizinische Forschung e.V.
TMG	Telemediengesetz

TR	Technische Richtlinie
u.a.	unter anderem/und andere(s)
u.U.	unter Umständen
URI	Uniform Resource Identifier
URL	Uniform Resource Locator
USB	Universal Serial Bus
usw.	und so weiter
vgl.	vergleiche
VPN	Virtuelles Privates Netz
WoGG	Wohngeldgesetz
WRV	Weimarer Reichsverfassung
www	World Wide Web
z.B.	zum Beispiel
ZAST	Zentrale Abrechnungsstelle für den Rettungsdienst Bayern GmbH
ZBFS	Zentrum Bayern Familie und Soziales

Stichwortverzeichnis

Der Bayerische
Landesbeauftragte
für den
Datenschutz

Wagmüllerstraße 18
80538 München
Postfach 22 12 19
80502 München
Telefon 089 21 26 72-0
Telefax 089 21 26 72-50

poststelle@datenschutz-bayern.de
www.datenschutz-bayern.de