Der Bayerische Landesbeauftragte für den Datenschutz informiert die Öffentlichkeit

25. Tätigkeitsbericht

Berichtzeitraum
2011/2012

25. Tätigkeitsbericht des Landesbeauftragten für den Datenschutz

(gemäß Artikel 30 Absatz 5
des Bayerischen Datenschutzgesetzes)

Berichtzeitraum: 2011/2012
Veröffentlichungsdatum: 23.01.2013

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 Reform des Europäischen Datenschutzrechtsrahmens

Der Friedensnobelpreis des Jahres 2012 wurde an die Europäische Union (EU) vergeben. Über sechs Jahrzehnte hinweg haben die Union und ihre Vorgänger den Frieden und die Versöhnung der Völker in Europa gefördert (siehe Stellungnahme des Nobelpreiskomitees auf www.nobelprize.org). Seit den Römischen Verträgen des Jahres 1957 hat die EU zugleich gewaltige Integrationsschritte unternommen. Schon im letzten Tätigkeitsbericht bin ich kurz auf den vorerst letzten bedeutenden Wegabschnitt dieser Integration, auf das Inkrafttreten des Vertrags von Lissabon, eingegangen (siehe hierzu 24. Tätigkeitsbericht, Nr. 1.2). In der Präambel des Vertrags über die Europäische Union heißt es, die Vertragsparteien seien „entschlossen, den Prozess der Schaffung einer immer engeren Union der Völker Europas“ weiterzuführen, „in der die Entscheidungen entsprechend dem Subsidiaritätsprinzip möglichst bürgernah getroffen werden“. Was dies konkret für die Fortentwicklung des Europäischen Datenschutzrechtsrahmens bedeutet, beschreiben vor Allem die Art. 16 des Vertrags über die Arbeitsweise der Europäischen Union (AEUV) und Art. 8 Abs. 1 der Charta der Grundrechte der Europäischen Union (GRC).

Art. 16 AEUV
(1) Jede Person hat das Recht auf Schutz der sie betreffenden personenbezogenen Daten.
(2) Das Europäische Parlament und der Rat erlassen gemäß dem ordentlichen Gesetzgebungsverfahren Vorschriften über den Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die Organe, Einrichtungen und sonstigen Stellen der Union sowie durch die Mitgliedstaaten im Rahmen der Ausübung von Tätigkeiten, die in den Anwendungsbereich des Unionsrechts fallen, und über den freien Datenverkehr. Die Einhaltung dieser Vorschriften wird von unabhängigen Behörden überwacht.
Die auf der Grundlage dieses Artikels erlassenen Vorschriften lassen die spezifischen Bestimmungen des Artikels 39 des Vertrags über die Europäische Union unberührt.

Art. 8 GRC Schutz personenbezogener Daten
(1) Jede Person hat das Recht auf Schutz der sie betreffenden personenbezogenen Daten.
(2) Diese Daten dürfen nur nach Treu und Glauben für festgelegte Zwecke und mit Einwilligung der betroffenen Person oder auf einer sonstigen gesetzlich geregelten legitimen Grundlage verarbeitet werden. Jede Person hat das Recht, Auskunft über die sie betreffenden erhobenen Daten zu erhalten und die Berichtigung der Daten zu erwirken.
(3) Die Einhaltung dieser Vorschriften wird von einer unabhängigen Stelle überwacht.

Zurzeit wird der Datenschutz im Wesentlichen noch durch vier allgemeine EU-Rechtsakte geregelt. Vereinfacht ausgedrückt sieht dabei die Verordnung 45/2001/EG Vorschriften des Datenschutzes für die Institutionen der EU vor. Der Rahmenbeschluss des Rates 2008/977/JI soll einen angemessenen Schutz des Persönlichkeitsrechts hinsichtlich der Datenverarbeitung im Rahmen der polizeilichen und der justiziellen Zusammenarbeit in Strafsachen gewährleisten. Den allgemeinen Datenschutz regelt die Richtlinie 95/46/EG, die zugleich einen rechtlichen Rahmen für den freien Verkehr personenbezogener Daten zwischen den EU-Mitgliedstaaten setzt. Sie wird durch die Richtlinie 2002/58/EG ergänzt. Diese Richtlinie enthält besondere Regelungen für die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation.

Diese allgemeinen Datenschutzrechtsakte sollen jetzt teilweise ersetzt werden. Auf Grundlage der beiden zitierten Vorschriften Art. 16 AEUV und Art. 8 GRC hat die Europäische Kommission am 25.01.2012 zwei Rechtsakte zur Reform des Europäischen Datenschutzrechtsrahmens vorgeschlagen (Dokumente KOM (2012) 11 endg. und KOM (2012) 10 endg.).

Schon am 01.03.2012 hat der Bayerische Landtag sich in einer gemeinsamen Sitzung des Ausschusses für Verfassung, Recht, Parlamentsfragen und Verbraucherschutz und des Ausschusses für Bundes- und Europaangelegenheiten mit den beiden geplanten Neuregelungen des EU-Datenschutzrechtsrahmens eingehend auseinandergesetzt. Zu meiner großen Freude haben alle Fraktionen im Bayerischen Landtag im Grundsatz meine Einschätzung des Reformvorhabens geteilt. Danach ist die Reform des EU-Datenschutzrechtsrahmens zwar dringend erforderlich. Sie sollte jedoch in erster Linie darauf gerichtet sein, einen europaweiten Mindestdatenschutzstandard festzulegen. Die Vorschläge der Kommission zielen demgegenüber auf eine starke Vereinheitlichung des Datenschutzes ab und würden aus meiner Sicht insbesondere die Spielräume der mitgliedstaatlichen Gesetzgeber für einen weitergehenden Datenschutz im Bereich der öffentlichen Verwaltung unangemessen einengen.

Auch die 83. Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat eine Stellungnahme zu den beiden Reformvorschlägen verabschiedet, die in der Entschließung „Ein hohes Datenschutzniveau für ganz Europa!“ vom 21./22.03.2012 zusammengefasst wird.

Entschließung der 83. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 21./22.03.2012
Ein hohes Datenschutzniveau für ganz Europa!

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder unterstützt die Absicht der Europäischen Kommission, den Datenschutz in der Europäischen Union zu modernisieren und zu harmonisieren.

Der Entwurf einer Datenschutz-Grundverordnung enthält Regelungen, die zu einer Weiterentwicklung des europäischen Datenschutzrechts führen können. Dazu gehören vor allem

- *das Prinzip Datenschutz durch Technik,*
- *der Gedanke datenschutzfreundlicher Voreinstellungen,*
- *der Grundsatz der Datenübertragbarkeit,*
- *das Recht auf Vergessen,*

– *die verbesserte Transparenz durch Informationspflichten der verantwortlichen Stellen und*
– *die verschärften Sanktionen bei Datenschutzverstößen.*

Hervorzuheben ist zudem die Geltung des europäischen Rechts für Anbieter aus Drittstaaten, deren Dienste sich auch an europäische Bürgerinnen und Bürger richten.

Die Datenschutzbeauftragten des Bundes und der Länder halten es für wesentlich, dass bei der Harmonisierung des Datenschutzrechts ein möglichst hohes Niveau für alle Mitgliedsstaaten vorgeschrieben wird. Die Konferenz hatte bereits im Konsultationsverfahren die Auffassung vertreten, dass diesem Ziel angesichts der gewachsenen Traditionen und Rechtsstandards in den Mitgliedsstaaten und der eingeschränkten begrenzten Rechtssetzungskompetenz der EU in Bezug auf innerstaatliche Datenverarbeitungsvorgänge im öffentlichen Bereich am wirksamsten durch eine Richtlinie Rechnung getragen werden kann. Wenn jetzt stattdessen der Entwurf einer unmittelbar geltenden Verordnung vorgelegt wird, muss diese im Sinne eines europäischen Mindestdatenschutzniveaus den Mitgliedsstaaten zumindest in Bezug auf die Datenverarbeitung der öffentlichen Verwaltung die Möglichkeit eröffnen, durch einzelstaatliches Recht weitergehende Regelungen zu treffen, die entsprechend der jeweiligen Rechtstradition die Grundrechte der Bürgerinnen und Bürger absichern und Raum für eine innovative Rechtsfortbildung schaffen. Nur so können beispielsweise in Deutschland die in der Rechtsprechung des Bundesverfassungsgerichts entwickelten Datenschutzgrundsätze bewahrt und weiterentwickelt werden.

Die Konferenz erkennt an, dass die Institution der betrieblichen Datenschutzbeauftragten erstmals verbindlich in Europa eingeführt werden soll. Die Erfahrungen in Deutschland mit den betrieblichen Datenschutzbeauftragten als unabhängige Kontroll- und Beratungsstellen in Unternehmen sind ausgesprochen positiv. Die Konferenz bedauert deshalb, dass die Kommission grundsätzlich nur Unternehmen mit mindestens 250 Beschäftigten zur Bestellung von Datenschutzbeauftragten verpflichten will. Dieses Vorhaben bedroht eine gewachsene und erfolgreiche Kultur des betrieblichen Datenschutzes in Deutschland.

Über die bereits in dem Verordnungsentwurf vorgeschlagenen Modernisierungen hinaus hält die Konferenz weitere Schritte für erforderlich, die sie etwa in ihrem Eckpunktepapier für ein modernes Datenschutzrecht vom 18.03.2010 vorgeschlagen hat:

– *eine strikte Reglementierung der Profilbildung, insbesondere deren Verbot bei Minderjährigen,*
– *ein effektiver Schutz von Minderjährigen, insbesondere in Bezug auf das Einwilligungserfordernis eine Anhebung der Altersgrenze,*
– *die Förderung des Selbstdatenschutzes,*
– *pauschalierte Schadensersatzansprüche bei Datenschutzverstößen,*
– *einfache, flexible und praxistaugliche Regelungen zum technisch-organisatorischen Datenschutz, welche vor allem die Grundsätze der Vertraulichkeit, der Integrität, der Verfügbarkeit, der Nichtverkettbarkeit, der Transparenz und der Intervenierbarkeit anerkennen und ausgestalten,*
– *das Recht, digital angebotene Dienste anonym oder unter Pseudonym nutzen zu können und*
– *die grundsätzliche Pflicht zur Löschung der angefallenen Nutzerdaten nach dem Ende des Nutzungsvorganges.*

Die Regelungen zur Risikoanalyse, Vorabkontrolle und zur Zertifizierung bedürfen der weiteren Präzisierung in der Verordnung selbst.

Für besonders problematisch hält die Konferenz die vorgesehenen zahlreichen Ermächtigungen der Europäischen Kommission für delegierte Rechtsakte, die dringend auf das unbedingt erforderliche Maß zu reduzieren sind. Alle für den Grundrechtsschutz wesentlichen Regelungen müssen in der Verordnung selbst bzw. durch Gesetze der Mitgliedsstaaten getroffen werden.

Die Konferenz weist darüber hinaus darauf hin, dass das im Entwurf der Datenschutz-Grundverordnung vorgesehene Kohärenzverfahren, welches die Aufsichtsbehörden in ein komplexes Konsultationsverfahren einbindet, die Unabhängigkeit der Datenschutzaufsicht beeinträchtigen und zu einer Bürokratisierung des Datenschutzes führen würde. Es muss deshalb vereinfacht und praktikabler gestaltet werden.

Die durch Artikel 8 der EU-Grundrechte-Charta und Artikel 16 des Vertrags über die Arbeitsweise der Europäischen Union gewährleistete Unabhängigkeit der Datenschutzaufsichtsbehörden gilt auch gegenüber der Europäischen Kommission. Die vorgesehenen Befugnisse der Kommission in Bezug auf konkrete Maßnahmen der Aufsichtsbehörden bei der Umsetzung der Verordnung wären damit nicht vereinbar.

Wiederholt hat die Konferenz auf die Bedeutung eines hohen und gleichwertigen Datenschutzniveaus auch im Bereich der polizeilichen und justiziellen Zusammenarbeit in Strafsachen in Europa hingewiesen. Sie bedauert, dass der für diesen Bereich vorgelegte Richtlinienentwurf in vielen Einzelfragen hinter dem Entwurf für eine Datenschutz-Grundverordnung und hinter dem deutschen Datenschutzniveau zurückbleibt, etwa im Hinblick auf die Prinzipien der Datenverarbeitung (wie den Grundsatz der Erforderlichkeit) und auf die Rechte der Betroffenen (insbesondere zum Schutz des Kernbereiches der privaten Lebensgestaltung). Auch in diesem Bereich sollte die Richtlinie unter angemessener Berücksichtigung der mitgliedsstaatlichen Verfassungstraditionen ein EU-weit möglichst hohes Mindestniveau festschreiben.

Die Konferenz erklärt, dass sie den Gang des Gesetzgebungsverfahrens konstruktiv und kritisch begleiten wird.

Im Rahmen des ordentlichen Gesetzgebungsverfahrens zur Reform sind mittlerweile der Ausschuss der Regionen und das Europäische Parlament mit den Vorschlägen der Kommission befasst worden. Das weitere Gesetzgebungsverfahren wird den Regeln des Art. 294 AEUV folgen. Im Rahmen meiner Möglichkeiten werde ich den Reformprozess auch weiterhin konstruktiv-kritisch begleiten.

1.2 Cloud Computing-Initiative der EU-Kommission

Auch im Berichtszeitraum hat mich das Thema Cloud Computing vielfach beschäftigt. Unter anderem hat die Europäische Kommissarin für die Digitale Agenda, Neelie Kroes, eine neue Strategie der „Freisetzung des Cloud-Computing-Potenzials in Europa“ gestartet (Mitteilung vom 27.09.2012, KOM 529/2012). Sie erhofft sich durch einen breiten Einsatz von Cloud-Lösungen durch Unternehmen und durch den öffentlichen Sektor erhebliche volkswirtschaftliche Vor-

teile. Die Auslagerung von Verfahren und Daten auf externe, virtuelle Systeme im Sinne des Cloud Computing mag chancenreich sein, ist allerdings auch mit einer Vielzahl von Risiken für den Datenschutz und die Datensicherheit verbunden (siehe hierzu 24. Tätigkeitsbericht, Nr. 2.1.5). Nähere datenschutzrechtliche Anforderungen werden in einer Stellungnahme der EU-Datenschutz-Arbeitsgruppe 29 formuliert (Opinion 05/2012 on Cloud Computing, WP 196, abrufbar unter http://ec.europa.eu/justice/data-protection/article-29/ unter <documentation>). In dem Papier werden die – anspruchsvollen – Voraussetzungen für einen datenschutzgerechten Einsatz des Cloud Computing beschrieben. Auch die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat durch einige ihrer Arbeitskreise eine Orientierungshilfe Cloud Computing erarbeiten lassen (siehe Nr. 2.3.3).

1.3 Die Bayerische Verwaltung im Zeitalter des Social Web

Vor etwa zweiundzwanzig Jahren entwickelte Tim Berners-Lee das World Wide Web (WWW). Das System einer verteilten Informationsverwaltung im Netz wurde bald zum erfolgreichsten Internetdienst. Informationen im WWW werden seither in der Seitenbeschreibungssprache Hypertext Markup Language (HTML) auf Webservern bereitgestellt. HTML ermöglicht eine grafische Aufbereitung und Verknüpfung von Daten.

Aus datenschutzrechtlicher Sicht leidet das WWW allerdings nach wie vor unter einem Geburtsfehler: Für die Nutzer erfolgt der Zugriff auf Daten im WWW zumeist nicht anonym. Ruft ein Nutzer oder eine Nutzerin eine Webseite auf, wird aufgrund unvermeidbarer technischer Notwendigkeit zur Erbringung des Dienstes zunächst die Internetprotokoll-Adresse (IP-Adresse) übertragen, die eine Art Adresse des Rechners im Internet darstellt (siehe Nr. 2.1.1). Daneben werden aber auch regelmäßig Daten über das Betriebssystem, sowie Art und Version des verwendeten Browsers mitsamt der verwendeten Einstellungen erfasst. Die meisten Anbieter von Webseiten legen überdies Cookies oder vergleichbare Kleindateien auf den Rechnern der Nutzer ab. Jedenfalls soweit eine solche Speicherung ohne Einwilligung der betroffenen Nutzer über den Nutzungsvorgang hinaus erfolgt, steht dies nicht mit den Vorgaben des Art. 5 Abs. 3 der EU-Richtlinie 2002/58/EG im Einklang. Das Ablegen von Cookies ist gleichwohl weit verbreitet, weil sie beispielsweise bei etwaigen mehrfachen Besuchen ein und derselben Webseite Aufschluss über frühere Aufrufe geben. Beim Besuch von Webseiten hinterlassen Normalnutzer also regelmäßig Datenspuren, die zusammengetragen sehr schnell zu einem genauen Profil der Interessen und Gewohnheiten des Betroffenen führen. Insbesondere wenn sich der Nutzer gegenüber einem Anbieter, etwa einem Sozialen Netzwerk identifiziert, können entsprechende Zuordnungsmöglichkeiten zu einer nun namentlich bekannten Person entstehen.

Der Bundes- und die Ländergesetzgeber wollten jedoch solchen Datenerfassungen, die nicht zwingend für die Erbringung von Diensten erforderlich sind, Grenzen setzen. Sie regelten daher den Umgang der WWW-Dienste im Jahr 1997 mit verhältnismäßig fortschrittlichen Gesetzen (Teledienste-Datenschutzgesetz, Teledienstegesetz, Mediendienste-Staatsvertrag), die im Jahr 2007 in dem heute noch geltenden Telemediengesetz (TMG) gebündelt worden sind. Vereinfacht ausgedrückt sieht das TMG in den §§ 7 - 10 eine beschränkte Verantwortlichkeit der Anbieter von Telemediendiensten für fremde Inhalte vor. Wie die allgemeinen Datenschutzgesetze sieht auch das TMG in § 12 ein Verbot mit

Erlaubnisvorbehalt vor und statuiert den Grundsatz der Zweckbindung. Nach § 13 TMG sind Anbieter gegenüber ihren Nutzern zur **Transparenz der Erhebung und Verwendung** personenbezogener Daten verpflichtet. Soweit eine gesetzliche Erlaubnis zum Umgang mit personenbezogenen Daten fehlt, ist bei den Nutzern eine **Einwilligung** einzuholen. Sie kann zwar elektronisch erteilt werden. Allerdings muss der Anbieter dann u.a. gewährleisten, dass der Nutzer seine Erklärung auch zu einem späteren Zeitpunkt nachvollziehen kann. Werden die Nutzer an andere Dienste weitergeleitet, ist ihnen dies anzuzeigen. Im Rahmen des Zumutbaren muss ein Dienst die anonyme und **pseudonyme Nutzung** ermöglichen. Der Umgang mit Bestandsdaten nach § 14 TMG und Nutzungsdaten nach § 15 TMG folgt strikt dem **Prinzip der Erforderlichkeit**. Bei aller Kritik im Einzelnen hat das Telemediengesetz im Großen und Ganzen sachgerechte Antworten auf das WWW des 20. Jahrhunderts gegeben.

1.3.1 Soziale Netzwerke: Mehr Chancen – mehr Risiken

Ob dieses Gesetz auch noch auf die Herausforderungen des Web2.0 („Social Web") des 21. Jahrhunderts angemessen antworten kann, ist allerdings äußerst fraglich. Im sogenannten Web2.0 wirken technische Fortentwicklungen (z.B. einfache Suche mittels wirkmächtiger Suchmaschinen, Erweiterung von Speicher- und Übertragungskapazitäten), veränderte ökonomische Rahmenbedingungen (z.B. Finanzierung der Datenverarbeitung für breite Bevölkerungsschichten) und soziokulturelle Veränderungen (Wertewandel) zusammen. Was den Umgang mit personenbezogenen Daten anbelangt, schlüpfen Nutzer in die Rolle von „produsern" (Nutzer und Datenverarbeitende). Daten werden mehr und mehr vernetzt, immer neue Angebote und Nutzungsmöglichkeiten entstehen, Datenverarbeitungsträger werden immer kleiner und leistungsfähiger, können überall und jederzeit genutzt werden – die Datenverarbeitung wird mit anderen Worten allgegenwärtig. Gerade Telemediendienste werden auf vielfache Weise miteinander verschränkt und verknüpft, ohne dass dies für die Nutzer erkennbar wäre.

Vor Allem private Betreiberunternehmen von Webangeboten pflegen auf die unbestritten großen Chancen zu verweisen. Hervorgehoben werden die Möglichkeiten zur Selbstverwirklichung, neuartige Kooperationsformen und enorme wirtschaftliche Potenziale. Überdies sei das Web2.0 auch gut für unsere Zivilgesellschaft, weil seine neuen Kommunikationsformen auch die demokratische Willensbildung befördere. Der Beweis sei unter anderem durch den arabischen Frühling erbracht worden.

Worüber weniger gern gesprochen wird, ist der Umstand, dass die Nutzung von Chancen im Social Web an eine ganze Reihe von **Voraussetzungen** geknüpft und überdies mit erheblichen Risiken für das Persönlichkeitsrecht der Nutzer verbunden ist. Ihnen werden unter anderem eine extrem **hohe Medienkompetenz** und eine extrem **hohe Privatsphärenkompetenz** abverlangt. Wer beispielsweise das größte Soziale Netzwerk (Facebook) nutzt, kann dabei seine Privatsphäre zwar nicht gegenüber dem Anbieter (und den hieraus entstehenden Konsequenzen), wohl aber gegenüber der Öffentlichkeit mehr oder weniger leidlich bewahren. Dazu muss man freilich bereit und fähig sein, zwischen 30 und 40 datenschutzfeindliche Voreinstellungen abzuändern. Wiederholungen dieser Prozedur können erforderlich sein, wenn Facebook wieder einmal beschließt, die Rahmenbedingungen seines Angebots zu verändern.

Das Erfordernis einer hohen Medien- und Privatsphärenkompetenz gilt nicht nur im Hinblick auf den Selbstschutz, sondern ist auch auf die **Netzkultur** bezogen. Über die konkreten Auswirkungen eines vorschnell richtenden Publikums habe ich bereits in meinem letzten Tätigkeitsbericht informieren müssen (siehe hierzu 24. Tätigkeitsbericht, Nr. 1.1 und Nr. 8.19).

Ein unter Anbietern ebenso unbeliebtes Thema ist die lange Liste von schwer wiegenden **Datensicherheitspannen**, welche die kurze Geschichte insbesondere von einigen großen Sozialen Netzwerke begleiten.

1.3.2 Was öffentliche Stellen zu beachten haben

Wenn sich öffentliche Stellen für die Nutzung Sozialer Netzwerke entscheiden, müssen sie sich weiterhin darüber im Klaren sein, dass die angebotenen Dienstleistungen ökonomiebestimmt ausgestaltet sind. Im Berichtszeitraum habe ich beispielsweise an einem Symposium zum sogenannten **Litigation PR** mitgewirkt. Die Veranstaltung verdeutlichte eindrucksvoll, dass die Justizbehörden gut beraten sind, bei der Recherche personenbezogener Daten der öffentlichen Berichterstattung im Allgemeinen und speziell den Ergebnissen von Suchmaschinen nicht vorbehaltlos zu vertrauen. Denn mit Geld und einem guten Reputationsmanagement lassen sich derartige Suchergebnisse ganz erheblich beeinflussen. Ganz allgemein sollte sich die öffentliche Verwaltung bei der Nutzung von Suchmaschinen immer wieder in Erinnerung zu rufen, dass die Kriterien für die Auswahl und Reihenfolge von Suchergebnissen nicht transparent sind. Mit anderen Worten darf auch soweit die Erhebung personenbezogener Daten über das WWW zulässig ist, die Richtigkeit der erhobenen Daten nicht unterstellt, sondern muss sorgfältig geprüft werden.

Im Berichtszeitraum stellte eine Vielzahl von öffentlichen Stellen an mich die Frage, wie sie im Rahmen ihrer **Öffentlichkeitsarbeit eine Fanseite in einem Sozialen Netzwerk** datenschutzkonform errichten könne. Das große Interesse freut mich, weil hierdurch die Sensibilität der weitaus meisten bayerischen öffentlichen Stellen deutlich wird. Zumeist beziehen sich derartige Anfragen auf die Einrichtung von Fanseiten bei Facebook oder von Profilen bei Google+. Die Unsicherheit der öffentlichen Stellen verdeutlicht zugleich ein Unbehagen bei einem Engagement bei diesen Diensten. Sowohl Facebook als auch Google+ standen wiederholt wegen datenschutzrechtlich problematischen Entscheidungen in der öffentlichen Kritik. Sie setzen die oben sehr allgemein beschriebenen Anforderungen des TMG allenfalls teilweise um (siehe Nr. 1.3). Vor diesem Hintergrund hat sich die 82. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 28./29.09.2011 in einer Entschließung nicht nur, aber insbesondere zu Angeboten dieser Dienste kritisch geäußert.

Entschließung der 82. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 28./29.09.2011
Datenschutz bei sozialen Netzwerken jetzt verwirklichen!

Anlässlich der aktuellen Diskussionen um den Datenschutz bei sozialen Netzwerken, wie beispielsweise Facebook, stellt die Konferenz der Datenschutzbeauftragten des Bundes und der Länder klar, dass sich die Anbieter solcher Plattformen, die auf den europäischen Markt zielen, auch dann an europäische Datenschutzstandards halten müssen, wenn sie ihren Sitz außerhalb Europas haben.

Die Konferenz stellt insbesondere fest, dass die direkte Einbindung von Social-Plugins beispielsweise von Facebook, Google+, Twitter und anderen Plattformbetreibern in die Webseiten deutscher Anbieter ohne hinreichende Information der Internet-Nutzenden und ohne Einräumung eines Wahlrechtes nicht mit deutschen und europäischen Datenschutzstandards in Einklang steht. Die aktuelle von Social-Plugin-Anbietern vorgesehene Funktionsweise ist unzulässig, wenn bereits durch den Besuch einer Webseite und auch ohne Klick auf beispielsweise den "Gefällt-mir"-Knopf eine Übermittlung von Nutzendendaten in die USA ausgelöst wird, auch wenn die Nutzenden gar nicht bei der entsprechenden Plattform registriert sind.

Die Social-Plugins sind nur ein Beispiel dafür, wie unzureichend einige große Betreiber sozialer Plattformen den Datenschutz handhaben. So verwendet Facebook mittlerweile Gesichtserkennungs-Technik, um Bilder im Internet bestimmten Personen zuzuordnen; Betroffene können sich dem nur mit erheblichem Aufwand entziehen. Sowohl Facebook als auch Google+ verlangen, dass die Nutzenden sich identifizieren, obwohl nach deutschem Recht aus guten Gründen die Möglichkeit zumindest einer pseudonymen Nutzung solcher Dienste eröffnet werden muss.

Die Datenschutzbeauftragten des Bundes und der Länder fordern daher alle öffentlichen Stellen auf, von der Nutzung von Social-Plugins abzusehen, die den geltenden Standards nicht genügen. Es kann nicht sein, dass die Bürgerinnen und Bürger, die sich auf den Seiten öffentlicher Stellen informieren wollen, mit ihren Daten dafür bezahlen. Unbeschadet der rechtlichen Verantwortung sollten die öffentlichen Stellen auf solchen Plattformen keine Profilseiten oder Fanpages einrichten.

Die Obersten Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich haben bereits 2008 und zuletzt 2010 in Beschlüssen Anforderungen an die datenschutzkonforme Gestaltung sozialer Netzwerke formuliert. Die Konferenz der Datenschutzbeauftragten fordert die Anbieter sozialer Netzwerke auf, diese Beschlüsse umzusetzen, soweit dies noch nicht geschehen ist. In diesem Zusammenhang unterstützen die Datenschutzbeauftragten Bestrebungen zur Entwicklung von technischen Lösungen zur datenschutzkonformen Gestaltung von Webangeboten.

Bedauerlicherweise hat die Bundesregierung ihrer schon im letzten Jahr gemachten Ankündigung, gesetzgeberische Maßnahmen gegen die Profilbildung im Internet vorzuschlagen, keine Taten folgen lassen. Der bloße Verweis darauf, dass die Diensteanbieter Selbstverpflichtungen eingehen sollten, wird dem akuten Schutzbedarf der immer zahlreicher werdenden Nutzerinnen und Nutzer nicht gerecht. Die Konferenz der Datenschutzbeauftragten unterstützt den Gesetzentwurf des Bundesrates zur Änderung des Telemediengesetzes (BT-Drs. 17/6765) als einen Schritt in die richtige Richtung.

Wie Artikel 20 Absatz 3 unseres Grundgesetzes verdeutlicht, sind öffentliche Stellen in besonderer Weise an Gesetz und Recht gebunden. Sie haben daher auch im Zusammenhang mit ihrer Öffentlichkeitsarbeit eine Vorbildfunktion. Mit dieser **Vorbildfunktion der öffentlichen Hand** verträgt es sich im Grundsatz nicht, wenn sie durch ihr eigenes Marktverhalten Anbieter fördern, die nach Maßstäben des deutschen Datenschutzrechts wiederholt erhebliche Rechtsverstöße begangen haben. In zahlreichen Gesprächen haben sich in Deutschland ansässi-

ge Anbieter bei mir darüber beschwert, dass sie durch die Einhaltung der deutschen Datenschutzgesetze erhebliche Wettbewerbsnachteile erleiden würden.

Unabhängig davon ist vor Allem die Frage der unmittelbaren **datenschutzrechtlichen Verantwortlichkeit von öffentlichen Stellen** aufzuwerfen, die **Fanseiten oder Profile** in sozialen Netzwerken einrichten. Verschiedene Rechtsfragen hierzu sind weiterhin strittig und insbesondere gerichtlich noch nicht geklärt.

Eine Entscheidung des Landgerichts Aschaffenburg vom 19.08.2011 bestärkt allerdings meine Auffassung, dass hier eine (Mit-) Verantwortlichkeit öffentlicher Stellen auch im Hinblick auf die Einhaltung telemedienrechtlicher Vorschriften nahe liegt. Das Landgericht hat im dortigen Fall entschieden, dass die Informationspflicht nach § 5 TMG („Impressumspflicht") auch eine GmbH trifft, wenn diese als Nutzer von Social Media einen Facebook-Account zu Marketingzwecken benutzt. § 5 TMG knüpft dabei – wie auch andere Vorschriften des TMG – an die Diensteanbietereigenschaft an.

Ich bin auch aus nachfolgenden Gründen der Auffassung, dass öffentliche Stellen eine datenschutzrechtliche Verantwortung für die Rechtmäßigkeit des Datenumgangs auf Fanseiten tragen. Zum einen ist es schließlich die öffentliche Stelle, die eine Fanseite oder ein Profil überhaupt erst einrichtet. Zum anderen hängt zwar die Gestaltung derartiger Fanseiten von bestimmten Rahmenbedingungen ab, die das jeweilige Soziale Netzwerk (z.B. Facebook oder Google+) setzt. Innerhalb dieses Rahmens bestimmen jedoch die öffentlichen Stellen selbst die Art und den Umfang der Kommunikation mit den Nutzern mit. Dabei ergibt es insofern einen erheblichen Unterschied, ob eine öffentliche Stelle eine Fanseite einrichtet, auf der sie lediglich auf eine „eigene" Webseite verweist oder ob sie auf der Fanseite die Nutzer zu Äußerungen auffordert.

Angesichts noch strittiger Rechtsfragen habe ich u.a. die Ressorts der Staatsregierung zunächst gebeten, jedenfalls keine neuen Fanseiten einzurichten, bestehende Seiten zurückhaltend auszugestalten und nicht im Besonderen zu bewerben.

Überdies gilt: Eine bayerische öffentliche Stelle, die Nutzer hier aktiv zur Kommunikation ermuntert, hält Bürgerinnen und Bürger zur Offenbarung von personenbezogenen Daten in einem rechtlich und technisch unsicheren virtuellen Umfeld an. Dies kann – je nach Ausgestaltung – auch besonders sensible Daten betreffen. Spätestens hier wird dann eine Grenze zum beanstandenswerten Datenschutzverstoß überschritten.

Empfehlenswert wäre aus meiner Sicht natürlich, von der Einrichtung von Fanseiten oder entsprechenden Profilen grundsätzlich abzusehen.

Auf immer mehr Webangeboten sind sogenannte **Social Plugins** wie der Like-Button („Gefällt mir") von Facebook oder der „+1-Button" von Google zu finden. Auch bayerische öffentliche Stellen versuchen hiermit eine kostengünstige Erhöhung der Reichweite eigener Webangebote zu erreichen. Problematisch hieran ist der Umstand, dass Social Plugins oft als iFrames in die Webseiten direkt eingebunden werden. Beim Laden der Webseite (etwa www.meineverwaltung_xyz.de) wird der Browser dabei angewiesen, eine weitere Webseite von dem Sozialen Netzwerk zu laden und an der vorgesehenen Stelle innerhalb der anderen Webseite anzuzeigen. Dabei werden zumindest der Zeitpunkt des Aufrufs der Referenzwebseite und die IP-Adresse des Nutzerrechners an das Soziale Netz-

werk übertragen. Dies geschieht ohne jegliche Mitwirkung der Nutzer, regelmäßig auch ohne deren Wissen.

Nach meiner Einschätzung verstößt eine solche Datenübertragung ohne Wissen der Nutzer gegen deutsches Datenschutzrecht. Für dieses Ergebnis spielt es keine Rolle, ob man die Datenübertragung rechtlich als Übermittlung personenbezogener Daten ansieht oder als eine andere Verwendung qualifiziert. Denn das Telemediengesetz (TMG) unterscheidet in den §§ 11 ff. hinsichtlich der rechtlichen Voraussetzungen nicht zwischen einer Datenübermittlung oder einer anderen Art der Weiterleitung personenbezogener Nutzerdaten.

Bei einigen Stellen habe ich mittlerweile feststellen können, dass sie diese datenschutzrechtlichen Bedenken aufgegriffen haben. Anstatt einer direkten Einbindung von Social Plugins sehen sie eine mittelbare Einbindung vor (mittels „Vorschaltbutton"). Bei dieser Variante erfolgt beim Aufruf des Webangebots keine Datenübertragung ohne Wissen und Willen der Nutzer. Sie erfolgt erst, wenn man den entsprechenden Vorschaltbutton betätigt. Die Einrichtung eines solchen Vorschaltbuttons ist zwar nur die zweitbeste Lösung: auch hier gibt es etwa im Hinblick auf eine Pflicht des Webseitenbetreibers zur Unterrichtung des Nutzers über Datenumgänge noch Ungeklärtes. Diese sogenannte Zwei-Klick-Lösung ist dennoch deutlich datenschutzfreundlicher als die gänzlich abzulehnende direkte Einbindung von Social Plugins.

Die beste Lösung wäre natürlich auch hier, ganz auf Social Plugins zu verzichten.

Eine der neueren Spezialitäten von Facebook ist die mittlerweile obligatorische Chronikfunktion TimeLine. Wohl in Anlehnungen an den gleichnamigen US-amerikanischen Science-Fiction-Roman von Michael Crichton sollen Besucherinnen und Besucher einer Fanseite alle Ereignisse von der Einrichtung der Fanseite bis zur Gegenwart nachvollziehen können. Der Soziologe und Datenschutzexperte Martin Rost hat TimeLine treffend als perfekt privat organisierte öffentliche Vorratsdatenspeicherung charakterisiert. Sie bestärkt mich in meinen erheblichen Vorbehalten gegen die Nutzung von Facebook durch öffentliche Stellen. Abgesehen von meinen grundsätzlichen Bedenken kann ich öffentlichen Stellen nur dringend empfehlen, fremde Beiträge insoweit durch entsprechende Einstellungen zuverlässig auszuschließen.

1.4 Bundesgesetzgebung

1.4.1 Bekämpfung des Rechtsextremismus

Im November 2011 wurde in der Öffentlichkeit bekannt, dass die rechtsextremistische Vereinigung „Nationalsozialistischer Untergrund (NSU)" in den Jahren 2000 bis 2007 eine ganze Reihe von Morden begangen hatte. Nach wie vor nicht abschließend geklärt ist die Frage, warum die Verbrechen erst im Jahr 2011 einem rechtsextremistischen Motiv zugeordnet werden konnten. Neben dem Bundestag hat auch der Bayerische Landtag einen NSU-Untersuchungsausschuss eingerichtet, der die vergangene Zusammenarbeit der Sicherheitsbehörden bei der Bekämpfung des gewalttätigen Rechtsextremismus auf etwaige Mängel durchleuchtet.

Eine sehr schnelle Folgerung hat der Bundesgesetzgeber mit dem **Rechtsextremismus-Datei-Gesetz (RED-G)** vom 20.08.2012 gezogen. Dieses Gesetz ist am 31.08.2012 in Kraft getreten (BGBl. I S. 1798) und zielt auf die Verbesserung des Informationsaustauschs zwischen Polizei und Nachrichtendiensten durch die Errichtung einer gemeinsamen Datei ab. In dieser Verbunddatei sind Personen zu erfassen, die unter den Voraussetzungen des § 2 des RED-G einen mehr oder weniger engen Bezug zum Rechtsextremismus aufweisen. Aus datenschutzrechtlicher Sicht weist das RED-G große Ähnlichkeiten mit dem Gesetz zur Errichtung einer standardisierten zentralen **Antiterrordatei** von Polizeibehörden und Nachrichtendiensten von Bund und Ländern auf (Antiterrordateigesetz-ATDG, vom 22.12.2006, BGBl. I S. 3409). Gegen dieses Gesetz sind erhebliche verfassungsrechtliche Bedenken erhoben worden, über die ich bereits berichtet habe (siehe hierzu 22. Tätigkeitsbericht, Nr. 5.4). Das RED-G weist gegenüber dem ATDG einige datenschutzrechtliche Verbesserungen auf, insbesondere ist der Kreis der zu erfassenden Personen enger gefasst. Die grundsätzlichen verfassungsrechtlichen Bedenken gegen die Errichtung einer bundesweiten Verbunddatei von Polizei und Nachrichtendiensten sind jedoch vergleichbar. Ob diese Bedenken durchgreifen, wird das Bundesverfassungsgericht möglicherweise schon zeitnah klären. Denn gegen das ATDG ist eine Verfassungsbeschwerde eingelegt worden, über die im November 2012 bereits mündlich verhandelt worden ist. Dabei wird das Bundesverfassungsgericht möglicherweise auch auf die heftig umstrittene Frage eingehen, ob und inwieweit das sogenannte Trennungsgebot einer Zusammenarbeit von Polizei und Nachrichtendiensten entgegensteht.

Des Weiteren gibt es aufgrund der fehlerhaften Ermittlungen im Zusammenhang mit den NSU-Verbrechen Überlegungen, die Struktur und Arbeitsweise der Polizei- und Verfassungsschutzbehörden zu reformieren. Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat diesbezüglich darauf hingewiesen, dass bei einer Reform der Sicherheitsbehörden der Datenschutz jedoch nicht auf der Strecke bleiben darf.

Entschließung der 84. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 07./08.11.2012
Reform der Sicherheitsbehörden:
Der Datenschutz darf nicht auf der Strecke bleiben

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder weist Versuche zurück, vermeintlich „überzogene" Datenschutzanforderungen für das Versagen der Sicherheitsbehörden bei der Aufdeckung und Verfolgung rechtsextremistischer Terroristen verantwortlich zu machen und neue Datenverarbeitungsbefugnisse zu begründen.

Sie fordert die Bundesregierung und die Landesregierungen auf, vor einer Reform der Struktur und Arbeitsweise der Polizei- und Verfassungsschutzbehörden zunächst die Befugnisse, den Zuschnitt und die Zusammenarbeit der Verfassungsschutzbehörden vor dem Hintergrund der aufgetretenen Probleme zu evaluieren. Nur auf dieser Grundlage kann eine Diskussion über Reformen seriös geführt und ein Mehrwert für Grundrechtsschutz und Sicherheit erreicht werden.

In datenschutzrechtlicher Hinsicht geklärt werden muss insbesondere, ob die bestehenden Vorschriften in der Vergangenheit richtig angewandt, Arbeitsschwerpunkte richtig gesetzt und Ressourcen zielgerichtet verwendet worden sind. In diesem Zusammenhang ist auch zu untersuchen, ob die gesetzlichen Vorgaben

den verfassungsrechtlichen Anforderungen genügen, also verhältnismäßig, hinreichend klar und bestimmt sind. Nur wenn Ursachen und Fehlentwicklungen bekannt sind, können Regierungen und Gesetzgeber die richtigen Schlüsse ziehen. Gründlichkeit geht dabei vor Schnelligkeit.

Schon jetzt haben die Sicherheitsbehörden weitreichende Befugnisse zum Informationsaustausch. Die Sicherheitsgesetze verpflichten Polizei, Nachrichtendienste und andere Behörden bereits heute zu umfassenden Datenübermittlungen. Neue Gesetze können alte Vollzugsdefizite nicht beseitigen.

Bei einer Reform der Sicherheitsbehörden sind der Grundrechtsschutz der Bürgerinnen und Bürger, das Trennungsgebot, die informationelle Gewaltenteilung im Bundesstaat und eine effiziente rechtsstaatliche Kontrolle der Nachrichtendienste zu gewährleisten. Eine effiziente Kontrolle schützt die Betroffenen und verhindert, dass Prozesse sich verselbständigen, Gesetze übersehen und Ressourcen zu Lasten der Sicherheit falsch eingesetzt werden. Nur so kann das Vertrauen in die Arbeit der Sicherheitsbehörden bewahrt und gegebenenfalls wieder hergestellt werden.

Datenschutz und Sicherheit sind kein Widerspruch. Sie müssen zusammenwirken im Interesse der Bürgerinnen und Bürger.

1.4.2 Gesetz zur Fortentwicklung des Meldewesens

Erwähnenswert sind zwei ins Stocken geratene Gesetzgebungsverfahren der Bundesregierung. Nach gegenwärtigem Sachstand wird der Entwurf eines Gesetzes zum Beschäftigtendatenschutz wohl dem Grundsatz der Diskontinuität zum Opfer fallen (siehe hierzu 24. Tätigkeitsbericht, Nr. 1.2.7).

Bessere Erfolgsaussichten hat demgegenüber das Vorhaben der Bundesregierung, ein Gesetz zur Fortentwicklung des Meldewesens (MeldFortG) auf den Weg zu bringen (was entsprechende Vorüberlegungen zur Neuordnung des Meldewesens anbelangt, siehe hierzu 23. Tätigkeitsbericht, Nr. 10.1). Der Bundestag hatte bereits am 28.06.2012 in 2. und 3. Lesung den Entwurf eines Gesetzes zur Fortentwicklung des Meldewesens (MeldFortG) angenommen. Eine öffentliche Diskussion löste dabei der Beschluss aus, einfache Melderegisterauskünfte an Werbewirtschaft und Adresshandel selbst bei erfolgtem Widerspruch der betroffenen Einwohner zuzulassen, soweit die Abfrage zur Bestätigung oder Berichtigung vorhandener Datenbestände dient. Noch der Entwurf der Bundesregierung hatte demgegenüber insoweit das Erfordernis einer Einwilligung für die Datenweitergabe durch die Meldebehörden vorgesehen. Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat in einer Entschließung vom 22.08.2012 eine datenschutzkonforme Ausgestaltung des künftigen Melderechts eingefordert.

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.

Die Forderungen der Konferenz teile ich. Was die einfache Melderegisterauskunft anbelangt, bin ich insbesondere der Auffassung, dass den Bürgerinnen und Bürgern zumindest ein generelles Recht zum Widerspruch zustehen sollte, sofern der Auskunftssuchende kein rechtliches Interesse am Erhalt der begehrten Information hat. Die generelle Widerspruchslösung hätte den Vorzug, dass sie das Persönlichkeitsrecht angemessen schützt und gleichzeitig die Meldebehörden nicht mit umfassenden Prüf- und Abwägungsaufgaben überfrachtet.

1.5 Öffentlichkeitsarbeit

In meinem letzten Tätigkeitsbericht habe ich bereits darüber informiert, dass ich eine Broschüre zum Thema „Datenschutz im Krankenhaus“ herausgegeben habe. Mein Ziel war es dabei, die Bürgerinnen und Bürger auf unterhaltsame und verständliche Weise über ihre grundlegenden Datenschutzrechte im Bereich des Klinikwesens zu informieren. Der Erfolg dieser Broschüre hat mich ermutigt, das zugrundeliegende Konzept weiter zu verfolgen. Im Berichtszeitraum sind deshalb drei weitere Broschüren zu den Themen „Datenschutz im Rathaus“, „Datenschutz in der Schule“ und „Datenschutz bei der Polizei“ entstanden, die ebenfalls binnen kurzer Zeit einen erheblichen Absatz gefunden haben.

Darüber hinaus war ich jeweils mit einem Informationsstand bei dem Tag der offenen Tür des Bayerischen Landtags und anlässlich des Tags der Deutschen Einheit am 03.10.2012 auf der Ländermeile vertreten. Die große Nachfrage durch die Bürgerinnen und Bürger ermutigt mich, auch diesen Weg der Öffentlichkeitsarbeit fortzusetzen.

Zugleich bedanke ich mich hiermit ausdrücklich bei der Landtagsverwaltung und bei allen bayerischen Stellen in der Staatsverwaltung, die mich tatkräftig bei meiner Öffentlichkeitsarbeit unterstützt haben.

1.6 Schlussbemerkung

Die nachfolgenden Kapitel geben einen Überblick über meine Beteiligung an wesentlichen, hier nicht erwähnten Gesetzgebungsverfahren und meine Praxis der Datenschutzkontrolle der bayerischen öffentlichen Stellen im Berichtszeitraum 2011/2012.

2 IuK-Technik (IKT) und Organisation

2.1 Grundsatzthemen

2.1.1 IPv6

Auch wenn das Internet Protocol Version 6 (IPv6) bereits vor mehr als 20 Jahren standardisiert wurde, ist der Anteil des „neuen" Protokolls am gesamten Internetverkehr immer noch sehr gering. Es finden sich aber immer mehr Zugangs- und Diensteanbieter, die IPv6 unterstützen und somit erstmals im Produktivbetrieb auch den Endkunden zur Verfügung stellen.

Im Bezug auf den Datenschutz ist bei **IPv6 vor allem die deutlich längere IP-Adresse gegenüber dem IPv4-Adressraum** genauer zu betrachten. IPv6 bietet eine enorme Vervielfachung der Anzahl von möglichen Adressen, die es – bildlich gesprochen – ermöglichen würde, jedes Sandkorn der Erde mit mehreren Adressen zu versorgen.

Jede IPv6-Adresse besteht grundsätzlich aus zwei Teilen, einem „Präfix", das das jeweilige Netzsegment kennzeichnet und einem gerätespezifischen Anteil („Interface Identifier"), der das jeweilige Gerät innerhalb des Netzwerks adressiert.

Neu gegenüber IPv4 ist, dass nicht nur die ganze IPv6-Adresse ein Gerät und damit potentiell auch eine Person identifizierbar machen kann, sondern **dass unter Umständen auch schon das Präfix oder der Interface Identifier allein ausreicht, um einen Personenbezug herzustellen.**

Das Präfix kann dabei zumindest der Provider analog zur IP-Adresse bei IPv4 seinem Kunden zuordnen. Es gibt aber auch viele Endgeräte, die einen weltweit eindeutigen Interface Identifier benutzen, so dass sie, egal über welchen Provider – also mit wechselndem Präfix – sie das Internet nutzen, immer wiedererkannt werden könnten.

Daraus ergibt sich, dass beim IPv6-Einsatz Maßnahmen für beide Adressbestandteile zu treffen sind, um den Datenschutz zu gewährleisten.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat deshalb in ihrer 82. Konferenz gefordert, bereits mit der Einführung von IPv6 Datenschutz in das Netz einzubauen:

Entschließung der 82. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 28./29.09.2011
Einführung von IPv6 steht bevor: Datenschutz ins Netz einbauen!

Viele Betreiber und Anwender stellen in diesen Monaten ihre Netzwerktechnik auf das Internet-Protokoll Version 6 (IPv6) um. Grundsätzlich darf es mit einer Migration von IPv4 zu IPv6 nicht zu einer Verschlechterung der technischen

Rahmenbedingungen zur Ausgestaltung von Privacy kommen. Neuen Herausforderungen muss mit wirksamen Konzepten begegnet werden.

IPv6 stellt eine nahezu unbegrenzte Anzahl von statischen IP-Adressen zur Verfügung, die eine dynamische Vergabe von IP-Adressen, wie sie zur Zeit bei Endkunden gängig ist, aus technischer Sicht nicht mehr erforderlich macht. Aber durch die Vergabe statischer Adressen erhöht sich das Risiko, dass Internetnutzende identifiziert und ihre Aktivitäten auf einfache Weise webseitenübergreifend zu individuellen Profilen zusammen geführt werden können. Sowohl der von den Internet-Providern bereitgestellte Adressanteil (Präfix) als auch gerätespezifische Anteile in den IPv6-Adressen machen eine dauerhafte Identifizierung möglich. Die Zuordnung einer IP-Adresse zu einer bestimmten Person bedarf nicht zwingend einer Beteiligung des Zugangsanbieters. Mit Hilfe von Zusatzinformationen, die dem Betreiber eines Internet-Angebots vorliegen oder ihm offenstehen, beispielsweise Identifikationskonten von Online-Shops oder Sozialen Netzen, ist eine eindeutige Zuordnung von Nutzern möglich. Die vereinfachten Möglichkeiten zur Profilbildung und Zusammenführung von Profilen erhöhen zudem das Risiko und verstärken die Auswirkungen krimineller Handlungen. Mit Blick darauf, dass sich ein Identifikationsrisiko aus beiden Teilen der neuen Adressen ergeben kann, sind Maßnahmen in unterschiedlichen Bereichen erforderlich.

Die Datenschutzbeauftragten des Bundes und der Länder fordern, bei der Umstellung auf IPv6 Datenschutz und IT-Sicherheit zu gewährleisten. Anbieter von Internetzugängen und Diensten sowie Hersteller von Hard- und Software-Lösungen sollten ihre Produkte datenschutzgerecht gestalten (privacy by design) und dementsprechende Voreinstellungen wählen (privacy by default). Internetnutzenden sollten bei der Beschaffung von Hard- und Software sowie beim Abschluss von Verträgen auf diese Aspekte besonders achten.

- *Access Provider sollten Kundinnen und Kunden statische und dynamische Adressen ohne Aufpreis zuweisen. Auf Kundenwunsch sollten statische Adressen gewechselt werden können.*
- *Kundinnen und Kunden sollten mit nutzerfreundlichen Bedienelementen bei der Auswahl der Adressen für jeden von ihnen genutzten Dienst unterstützt werden.*
- *Hard- und Softwarehersteller sollten die „Privacy Extensions“ unterstützen und standardmäßig einschalten (privacy by default), um die Wiedererkennung von Nutzenden anhand von Hardwareadressen zu erschweren.*
- *Die Hard- und Softwarehersteller sollten Lösungen für dezentrale Kommunikationsdienste (peer to peer) in Kundensystemen entwickeln, die den Verzicht auf zentrale Plattformen und Portale ermöglichen. Sie sollten interessierten Dritten die Entwicklung solcher Dienste gestatten.*
- *Content Provider dürfen zur Reichweitenmessung nur die ersten 4 Bytes der IPv6-Adresse heranziehen und müssen den Rest der Adresse löschen, denn eine Analyse von Nutzungsdaten ist nach Ansicht der Datenschutzaufsichtsbehörden nur auf der Grundlage anonymisierter IP-Adressen zulässig. Die ersten 4 Bytes sind für eine Geolokalisierung ausreichend.*
- *Zugangsanbieter und Betreiber von Internetangeboten sollten nicht protokollierende Proxy-Server einsetzen und die Voraussetzungen schaffen, dass ein Internetzugang oder die Nutzung von im Internet bereitgestellten Inhalten in anonymer Form möglich ist (Anonymisierungsdienste).*
- *Hersteller und Anbieter von Betriebssystemen und vorkonfigurierten Geräten (wie PCs, Smartphones und Routern) sollten ihre Anstrengungen bei der Pflege und Weiterentwicklung ihrer Produkte intensivieren und re-*

gelmäßig Fehler bereinigte Versionen ihrer IPv6-fähigen Software anbieten.

- *Angesichts häufig mangelnder Reife von IPv6-fähigen Produkten ist Anwendern vom Einsatz von IPv6 innerhalb von lokalen Netzen noch abzuraten, wenn dort sensible personenbezogene Daten verarbeitet werden sollen und funktionsfähige Filtereinrichtungen weder zentral noch auf den einzelnen Rechnern im LAN vorhanden und aktiviert sind.*
- *Eigentümerinnen und Eigentümer von IP-Adressen dürfen nur auf Wunsch in das weltweite, stark zentralisierte „Internet-Telefonbuch" whois aufgenommen werden. Die Bundesregierung wird aufgefordert, sich für eine datenschutzfreundliche Gestaltung des whois-Dienstes einzusetzen, dahingehend, dass die Internet-Verwaltung ICANN den whois-Dienst künftig als verteilte Datenbank gestaltet, so dass die Daten der Eigentümerinnen und Eigentümer jeweils durch lokale Dienstleister oder Selbstverwaltungsgremien gespeichert, gepflegt und von ihnen nach Maßgabe des lokalen Rechts an Dritte übermittelt werden.*

Die Datenschutzbeauftragten des Bundes und der Länder werden die Einführung von IPv6 wachsam beobachten und bieten allen Akteuren ihre Unterstützung an.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat in ihrer 84. Konferenz am 07./08.11.2012 mit der Orientierungshilfe „Datenschutz bei Ipv6 - Hinweise für Hersteller und Provider im Privatkundengeschäft" diese Hinweise präzisiert.

Behörden, die im internen Netz IPv6 einsetzen, müssen **darauf achten, nur Endgeräte mit aktivierten „Privacy Extensions" einzusetzen**, da diese unterschiedliche Interface Identifier für die einzelnen Verbindungen generieren und somit ein spezielles Gerät nicht mehr zu erkennen geben. Sollte auch im IPv6-Netz ein **Web-Proxy** zum Einsatz kommen, **sollte** dieser **zumindest den Interface Identifier gegenüber dem Internet verbergen.**

Im Bezug auf die Netzwerksicherheit ist zu beachten, dass es immer noch viele Sicherheitsprodukte (Firewalls etc.) gibt, die im IPv6-Bereich nicht die gleiche Sicherheit und Zuverlässigkeit bieten, wie in bereits sehr lange bewährten IPv4-Umgebungen.

Sobald öffentliche Stellen ihren Internetauftritt „IPv6-tauglich" machen, müssen sie dies bei der Protokollierung der Webzugriffe und gegebenenfalls daraus generierten Statistiken beachten. **Bei der Protokollierung von IPv6-Datenverkehr** reicht es nicht mehr aus, das letzte Segment wie bei IPv4 zu löschen (siehe hierzu 23. Tätigkeitsbericht, Nr. 25.2), sondern es ist notwendig, **alle Adressbestandteile außer den ersten vier Bytes** zu **löschen**, um einen möglichen Personenbezug zu vermeiden.

Diese datenschutzrechtlichen Maßstäbe sind bei einer in Zukunft stattfindenden Umstellung der Internetauftritte von Beginn an zu beachten.

2.1.2 Externe Zugriffe auf dienstliche E-Mails

Aktuelle Versionen von Microsoft Exchange ermöglichen es, über Outlook Web Access / Outlook Web App (OWA) Mitarbeitern von überall Zugang zu ihrem dienstlichen Postfach zu eröffnen. Hierzu ist im einfachsten Fall nur ein Web-

browser nötig, der Zugriff kann von jedem beliebigen Internetrechner erfolgen. Darin liegt jedoch auch die Gefahr aus Sicht des Datenschutzes: In vielen Fällen muss davon ausgegangen werden, dass in den E-Mail-Postfächern auch schützenswerte personenbezogene Daten abgelegt sind. Ein **Zugriff von einem beliebigen Rechner** aus, also auch von ungesicherten Umgebungen wie Internet-Cafés, Privatrechnern oder **mobilen Geräten wie Smartphones** erhöht das Risiko einer unbefugten Kenntnisnahme oder des Verlusts von Daten deutlich. So könnten beispielsweise Trojaner oder Keylogger die Dateneingaben erfassen oder auf dem Privatgerät gespeicherte E-Mails oder Anhänge für weitere Nutzer des Rechners (z.B. Familienmitglieder) einsehbar sein.

Bei mobilen Geräten wie Smartphones ist das Risiko eines Geräteverlusts relativ hoch, so dass zusätzlich die Gefahr besteht, dass der Finder Einsicht in die gespeicherten Daten nehmen kann. Zudem besteht derzeit die Problematik, dass die technische Entwicklung im Bereich der IT-Sicherheit hinter dem Stand für Notebooks und PCs hinterherhinkt, so dass derzeit nicht alle Anforderungen zur sicheren Anbindung an die dienstliche Infrastruktur erfüllt werden können (siehe Nr. 2.1.3).

Für eine Freischaltung des externen Zugriffs auf dienstliche E-Mails sind daher einige Vorabprüfungen und sodann geeignete technisch-organisatorische Maßnahmen erforderlich:

In einem ersten Schritt muss geprüft werden, welchen **Schutzbedarf** die abrufbaren Daten besitzen. Sind potentiell Daten mit hohem oder sehr hohem Schutzbedarf (z.B. medizinische Daten, Personaldaten, Sozialdaten) in den E-Mails enthalten, ist ein Zugriff auf den E-Mail-Server von außerhalb kritisch zu bewerten. Insbesondere zu beachten sind gesetzliche Sonderregelungen zu bestimmten Datentypen wie z.B. Sozialdaten oder medizinischen Daten eines Krankenhauses, die den Regelungen des Art. 27 Bayerisches Krankenhausgesetz (BayKrG) unterliegen. Unzulässig ist der Zugriff auf Daten mit hohem oder sehr hohem Schutzbedarf insbesondere von Privatgeräten oder öffentlich zugänglichen Geräten (Internet-Café), da diese nicht der Hoheit des Dienstherrn unterliegen.

Des Weiteren muss geprüft werden, ob der externe **Zugriff auf dienstliche E-Mails tatsächlich erforderlich** ist. Eine pauschale Freischaltung für alle Mitarbeiter ist nicht akzeptabel, es sei denn es kann ausgeschlossen werden, dass in den E-Mails personenbezogene Daten enthalten sein können. Andernfalls müssen Festlegungen getroffen werden, welcher Personenkreis überhaupt für einen externen Zugriff in Frage kommt und mit welchem Verfahren ein **externer Zugriff beantragt** werden kann. Die Genehmigung sollte ebenso wie die Pflichten des Mitarbeiters schriftlich dokumentiert werden, um das Missbrauchsrisiko gering zu halten.

Sollten die rechtlichen Vorprüfungen ergeben haben, dass ein Zugriff für bestimmte Benutzergruppen zulässig ist, sind gewisse technisch-organisatorische Mindestanforderungen zu erfüllen. Für den Zugriff auf das Portal des E-Mail-Servers ist eine **Benutzeridentifikation und -authentifikation** erforderlich. Bei normalem Schutzbedarf ist die Verwendung von Benutzerkennung und hinreichend komplexem Passwort ausreichend, wenn der Zugang nach einer gewissen Anzahl von Fehlversuchen gesperrt wird. Bei sensiblen Daten ist eine 2-Faktor-Authentifizierung z.B. mit Chipkarte, RSA-Token etc. vorzusehen.

Da für den Zugriff in der Regel das Internet verwendet wird, ist eine **Transportverschlüsselung** erforderlich. Hierzu kommen in der Regel virtuelle private Netzwerke (VPN) zum Einsatz. Zudem sollte geprüft werden, ob wirklich ein Zugang von beliebigen Rechnern aus nötig ist oder ob nur bestimmte, vorher bekanntgegebene Rechner zum Verbindungsaufbau zugelassen werden.

Zudem dürfen bei Daten mit hohem oder sehr hohem Schutzbedarf die Daten nicht unverschlüsselt auf dem Gerät des Benutzers abgelegt werden. Es muss daher auf dem Gerät des Benutzers entweder entsprechende Verschlüsselungssoftware installiert oder auf dem E-Mail-Server ein ausschließlicher Read-Only-Zugriff eingestellt werden.

Zusätzlich zu den technischen Maßnahmen müssen organisatorische Maßnahmen und Regelungen getroffen werden, die den **Benutzer auf die Einhaltung gewisser Mindestanforderungen im sicheren Umgang mit dem E-Mail-Zugriff verpflichten**. Hierzu gehört das Verbot, Familienmitgliedern oder anderen Personen Einsicht in die Daten zu gewähren, die Nutzung des Online-Zugriffs auf E-Mails nur auf Geräten mit Virenschutz, eine begrenzte Gültigkeit der Nutzungsberechtigung etc.

2.1.3 Mobile Geräte

In vielen Bereichen ist es üblich, dass Mitarbeiter von unterwegs auf dienstliche Daten zugreifen können. Klassischerweise kamen hierbei Notebooks zum Einsatz. Mit der zunehmenden Verbreitung von Smartphones und Tablet-PCs im privaten Umfeld steigt der Bedarf der Mitarbeiter, solche Geräte auch im dienstlichen Umfeld zu nutzen. Dabei stellt sich zum einen die Problematik, dienstliche Smartphones und Tablet-PCs gemäß den Wünschen der Anwender zur Verfügung zu stellen. Zum anderen ist jedoch auch der Trend zu beobachten, Privatgeräte der Mitarbeiter für den Zugriff auf dienstliche Daten zu nutzen (Bring Your Own Device, BYOD). Daraus ergibt sich eine Vielzahl von datenschutzrechtlichen Herausforderungen.

Eignung von Smartphones und Tablet-PCs als Dienstgeräte

Smartphones und Tablet-PCs wie iPhone, iPad, Android-Geräte haben ihren Ursprung im Consumerbereich und sind mit umfangreichen Möglichkeiten zu einer schnellen Orientierung vor Ort, Auffinden von Informationen, Social Networking ausgestattet. Die Sicherheit der Daten, eine sichere Einbindung in Unternehmensnetze oder Datenschutz generell sind bei der Konzipierung ganz offenkundig nicht die oberste Priorität. Beim Einsatz derartiger Geräte für dienstliche Zwecke ist daher z.B. zu beachten, dass umfassende Möglichkeiten zur Ortung von Mitarbeitern oder zur Bildung von Bewegungsprofilen vorhanden sein können. Zum anderen haben häufig die Betriebssystem- und Apps-Hersteller die Möglichkeit, auf das Smartphone zuzugreifen, um z.B. Apps zu löschen. Neben den Gefahren eines Zugriffs durch Hacker stellt sich damit die Frage, wie eventuell auf dem Smartphone gespeicherte personenbezogene Daten oder Zugangsdaten zu Systemen einer öffentlichen Stelle dagegen geschützt werden können. **Die Verwendung von Smartphones und Tablet-PCs verlangt daher umfassende Sicherheitsmaßnahmen.**

Bei einem Einsatz von Smartphones und Tablet-PCs in bayerischen öffentlichen Stellen muss zudem geprüft werden, ob die gewählten Geräte den Anforderun-

gen der **IKT-Sicherheitsrichtlinien für die bayerische Staatsverwaltung** genügen. Insbesondere relevant für mobile Geräte sind die Richtlinie „IT-Standards für die bayerische Staatsverwaltung – Verschlüsselung mobiler Endgeräte und Datenträger (BayITS-19)“, die Vorgaben zur verschlüsselten Datenspeicherung auf mobilen Geräten macht, sowie die Richtlinie „IT-Sicherheitsrichtlinien für die bayerische Staatsverwaltung – Einsatz mobiler Geräte (BayITSiR-07)“, in der die erforderlichen Sicherheitsmaßnahmen für die Anbindung mobiler Geräte an das Bayerische Behördennetz formuliert sind.

Anforderungen an dienstlich bereitgestellte Smartphones und Tablet-PCs

Möchte der Dienstherr seinen Mitarbeitern Smartphones oder Tablet-PCs zum Zugriff auf dienstliche Daten zur Verfügung stellen, müssen umfassende Sicherheitsmaßnahmen ergriffen werden. **Im einfachsten Fall dient das mobile Gerät nur als Zugangspunkt zu den Servern der öffentlichen Stelle**, d.h. es erfolgt ein Remote-Zugriff auf den Server und die nötigen Tätigkeiten werden dort ausgeführt. Auf dem mobilen Gerät werden keine Daten abgelegt. Eine solche Lösung ist insbesondere für Daten mit besonderem Schutzbedarf wie Personaldaten oder medizinische Daten von Interesse.

Leider sind **die technischen Entwicklungen zu Sicherheitsfragen im Bereich von Smartphones noch nicht so fortgeschritten**. Virtualisierungslösungen, wie sie für den Remote-Zugriff und die Trennung der Verarbeitungsumgebungen im Bereich der PCs und Notebooks möglich sind, existieren daher noch nicht im benötigten Umfang. Deswegen ist es häufig nötig, dass Daten auf dem Smartphone abgelegt werden, z.B. bei der E-Mail-Synchronisation. Dann sind **folgende Maßnahmen erforderlich**:

- Der Zugriff auf das Gerät muss mittels eines ausreichend sicheren Passworts / PIN abgesichert werden, wobei nach einer mehrmaligen **Falscheingabe der PIN** eine **automatisch vollständige Löschung der auf dem Gerät gespeicherten Daten** erfolgen sollte.

- Es muss Regelungen geben, ob das Dienstgerät auch für private Zwecke genutzt werden darf und wie dann verhindert wird, dass dienstliche personenbezogene Daten in als privat eingestufte Online-Dienste (wie Facebook, Twitter oder Google Mail) kopiert und damit verschickt werden können und dass privat installierte Apps auf dienstliche Daten zugreifen können. **Es sollte daher festgelegt werden, welche Anwendungen auf dem Gerät installiert und genutzt werden dürfen.**

- **Werden dienstliche personenbezogene Daten auf dem Gerät (temporär) gespeichert**, z.B. im Rahmen einer E-Mail-Synchronisation, **so ist eine Verschlüsselung erforderlich.**

- Zur weiteren Erhöhung der Sicherheit **bei Verlust oder Diebstahl des Geräts** sollte für die IT-Abteilung die Möglichkeit bestehen, **sämtliche dienstlichen personenbezogenen Daten vom Smartphone oder Tablet-PC aus der Ferne** zu **löschen.**

- Es muss die für das jeweilige Gerät verfügbare **Sicherheitssoftware** (Virenschutz etc.) installiert sein.

– Es müssen Maßnahmen ergriffen werden, dass ein durch Viren, Trojaner oder einen Hackerangriff kompromittiertes Gerät keine Bedrohung für die gesamte IT-Infrastruktur der öffentlichen Stelle wird. Deshalb sollten die **Sicherheitseinstellungen möglichst zentral konfiguriert und verteilt** werden.

– Es muss geregelt sein, wie die **Entsorgung der Geräte** erfolgt, so dass sichergestellt ist, dass darauf **keine personenbezogenen Daten mehr gespeichert** sind.

Solange diese Anforderungen nicht erfüllt werden, ist von einer Verwendung dienstlich bereit gestellter Smartphones und Tablet-PCs abzusehen.

Verwendung von Privatgeräten

Eine Nutzung privater Geräte für den Zugriff auf dienstliche IT-Systeme macht personenbezogene Daten der öffentlichen Stelle auf Geräten zugänglich, die nicht ihrer vollen Kontrolle unterliegen. Dies wirft eine Vielzahl ungeklärter Fragen auf: Es ist beispielsweise offen, wie auf dem privaten Gerät ausreichende Sicherheitsmaßnahmen sichergestellt werden oder wie die Nutzung durch andere Personen, wie z.B. Familienmitglieder und Freunde, unterbunden werden kann, um so eine unbefugte Offenbarung von schutzwürdigen (dienstlichen) Daten zu verhindern. Auch der Austausch von Geräten und die datenschutzgerechte Entsorgung sind für die öffentliche Stelle nicht kontrollierbar. Darüber hinaus stellt sich die Frage, ob über dienstliche Vereinbarungen rechtswirksam erzwungen werden kann, dass der Mitarbeiter bestimmte Anforderungen in Bezug auf sein privates Gerät erfüllt, wie z.B. die Einwilligung in eine Remote-Löschung durch die IT-Abteilung bei einem Verlust des Geräts.

Die Nutzung von Privatgeräten ist daher in Analogie zu den „IT-Sicherheitsrichtlinien für die bayerische Staatsverwaltung – Telearbeits- und mobile Arbeitsplätze (Bay-ITSiR-05)“ nicht zu empfehlen. **Insbesondere bei der Verarbeitung von personenbezogenen Daten mit besonderem Schutzbedarf bzw. Daten, die durch besondere gesetzliche Regelungen** wie z.B. das Bayerische Krankenhausgesetz (BayKrG) **geschützt sind, halte ich den Einsatz von Privatgeräten für unzulässig** (siehe Nr. 2.2.5 und Nr. 7.3).

In Bereichen mit normalem Schutzbedarf kann der Einsatz nach eingehender Einzelfallprüfung zulässig sein, wenn zusätzlich zu den oben aufgeführten Maßnahmen folgende Anforderungen erfüllt sind:

– Der Mitarbeiter als Eigentümer des Geräts muss verpflichtet werden, Sicherheitsmaßnahmen auf seinem Gerät umzusetzen und insbesondere auf Funktionen wie Jailbreak zu verzichten.

– Es muss sichergestellt sein, dass eine Trennung zwischen privaten Anwendungen und Daten sowie dienstlichen Anwendungen und Daten erfolgt. So darf z.B. eine private App nicht auf das dienstliche Adressbuch zugreifen können. Auch die Datenablage muss in getrennten Verzeichnissen erfolgen.

– Bei der Nutzung von Schnittstellen wie Bluetooth muss sichergestellt sein, dass der Kommunikationspartner keinen Zugriff auf dienstliche Daten erhält.

– Die Speicherung dienstlicher personenbezogener Daten muss verschlüsselt erfolgen. Dabei ist darauf zu achten, dass private Daten und dienstliche Daten separat verschlüsselt vorgehalten werden, so dass auch ein Administrator der öffentlichen Stelle nicht auf die privaten Daten des Nutzers zugreifen kann.

– Scheidet ein Bediensteter aus, müssen alle dienstlichen personenbezogenen Daten von seinem privaten IT-Gerät gelöscht werden.

– Es muss möglich sein, sämtliche dienstlichen personenbezogenen Daten auf dem Gerät aus der Ferne zu löschen, wenn das Gerät gestohlen wurde oder verloren gegangen ist.

– Es muss arbeitsrechtlich abgeklärt sein, dass die IT-Abteilung auch im Streitfall zwischen Dienstherren und Mitarbeiter insoweit Verfügungsgewalt über das Privatgerät besitzt, dass eine Löschung der dienstlichen Daten sichergestellt werden kann.

Soweit diese Anforderungen aufgrund des technischen Entwicklungsstandes auf den gewünschten Geräten nicht zum Einsatz kommen können (z.B. fehlende Verschlüsselung, mangelnde Möglichkeiten zur Virtualisierung und Datentrennung), ist von einer Verwendung privater Smartphones und Tablet-PCs abzusehen.

2.1.4 Telearbeit

Zum Thema Telearbeit habe ich mich bereits in früheren Tätigkeitsberichten geäußert (siehe hierzu 17. Tätigkeitsbericht, Nr. 18.3.3 und 18. Tätigkeitsbericht, Nr. 19.3.6). Ich habe dort insbesondere die Auffassung vertreten, dass auf die Bearbeitung von sensitiven Daten, insbesondere von Personaldaten im häuslichen Bereich verzichtet werden sollte. In datenschutzrechtlicher Hinsicht haben sich die Anforderungen zum Schutz von sensiblen Daten, insbesondere Sozialdaten, seither nicht verändert. In technisch-organisatorischer Hinsicht haben sich jedoch die Möglichkeiten zum Schutz von sensiblen Daten im Vergleich zu damals weiter entwickelt (siehe Nr. 2.2.5 und Nr. 7.3).

Da auch immer mehr Kommunen und Behörden es ihren Mitarbeitern ermöglichen wollen, von zu Hause oder unterwegs remote auf die Daten im lokalen Netz zuzugreifen und sich hinsichtlich der zu ergreifenden Datenschutz- und Datensicherheitsmaßnahmen von meiner Dienststelle beraten lassen, gehe ich nachfolgend nochmals auf die dem jetzigen Stand der Technik entsprechenden Maßnahmen für Telearbeitsplätze ein.

Telearbeiter arbeiten ausschließlich oder zeitweise außerhalb der Gebäude des Dienstherrn. Das bedeutet, dass für die Telearbeit teilweise andere Sicherheitsmaßnahmen zu ergreifen sind, als für die Arbeit innerhalb eines Behördengebäudes. Deshalb ist es notwendig, dass – aufbauend auf dem übergreifenden Sicherheitskonzept der Behörde – ein Sicherheitskonzept für die Telearbeitsplätze erstellt wird, in dem die Sicherheitsziele, der Schutzbedarf der bei der Telearbeit zu bearbeitenden Daten sowie die Risiken und zu ergreifenden Sicherheitsmaßnahmen aufgezeigt werden.

Die für die Telearbeit im Umgang mit Daten und der Informations- und Kommunikationstechnik notwendigerweise umzusetzenden Sicherheitsmaßnahmen sind zusätzlich in einer **Sicherheitsrichtlinie** zur Telearbeit zu dokumentieren. An Hand dieser Sicherheitsrichtlinie müssen dem Telearbeiter die bestehenden Risiken für die Gewährleistung der Vertraulichkeit, der Integrität, der Authentizität und der Verfügbarkeit der Telearbeit aufgezeigt werden. Außerdem sind die Telearbeiter in die entsprechenden Sicherheitsmaßnahmen einzuweisen und eventuell im Umgang damit zu schulen. Fehlende Schulungen können bei Problemen zu Ausfallzeiten oder Datenverlust führen.

Da für die Ausgestaltung der Rahmenbedingungen für Telearbeit verschiedene arbeitsrechtliche und arbeitsschutzrechtliche Aspekte zu beachten sind, sollten potentiell strittige Punkte entweder durch **Dienstvereinbarungen** mit der Personalvertetung oder/und individuelle Vereinbarungen zwischen Telearbeiter und Arbeitgeber geregelt werden.

Im Rahmen einer Telearbeit erfolgt in der Regel eine Übertragung personenbezogener Daten vom Standort des Dienstherrn zu einem „entfernten" Arbeitsplatz. Allerdings handelt es sich bei dieser Weitergabe von Daten weder um eine Datenübermittlung an Dritte noch stellt sie eine Auftragsdatenverarbeitung durch Dritte dar. Es handelt sich vielmehr um eine Nutzung von Daten innerhalb der speichernden Stelle. Trotzdem sind natürlich auch bei dieser Art der Datenverwendung die gesetzlichen Vorschriften zu beachten. Soweit keine vorrangigen bereichsspezifischen Rechtsvorschriften bestehen, findet auf die Datenverwendung im häuslichen Bereich das Bayerische Datenschutzgesetz (BayDSG) Anwendung.

Gemäß Art. 7 Abs. 2 BayDSG muss **im Rahmen einer Telearbeit insbesondere gewährleistet** werden, dass

– Unbefugte keinen Zugang zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet werden, erhalten (Zugangskontrolle),

– Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können (Datenträgerkontrolle),

– Datenverarbeitungssysteme nicht mit Hilfe von Einrichtungen zur Datenübertragung von Unbefugten genutzt werden können (Benutzerkontrolle),

– überprüft und festgestellt werden kann, an welche Stellen personenbezogene Daten durch Einrichtungen zur Datenübertragung übermittelt werden können (Übermittlungskontrolle),

– bei der Übertragung personenbezogener Daten sowie beim Transport von Datenträgern die Daten nicht unbefugt gelesen, kopiert, verändert oder gelöscht werden können (Transportkontrolle).

Den mit der Telearbeit verbundenen zusätzlichen Risiken lässt sich nur durch geeignete hochwertige Sicherheitsmaßnahmen begegnen. Dabei ist zu bedenken, dass sich die sicherheitstechnischen Anforderungen an den Telearbeitsplatz nach dem Schutzbedarf der zu bearbeitenden Daten richten. Je höher der Schutzbedarf, desto mehr Maßnahmen müssen ergriffen werden, um diesen Schutz zu gewährleisten.

Insbesondere sind im Rahmen einer Telearbeit **folgende technisch-organisatorische Maßnahmen** zu ergreifen:

– In den bereits erwähnten **schriftlichen Vereinbarungen zur Telearbeit** sind **Art und Umfang der Aufgaben und die Rahmenbedingungen**, unter denen die Aufgaben abzulaufen haben, zu definieren und **alle notwendigen Sicherheitsmaßnahmen** zur Gewährleistung der Vertraulichkeit, der Integrität, der Authentizität und der Verfügbarkeit der Telearbeit aufzunehmen. Sie müssen außerdem detaillierte Aussagen über die **Pflichten der in Telearbeit stehenden Mitarbeiter** enthalten.

– Alle **Telearbeiter** sind auf die Einhaltung der vorgegebenen Sicherheitsmaßnahmen **schriftlich zu verpflichten**. Außerdem hat der Telearbeiter dem Kontrollrecht des Dienstherrn und des behördlichen Datenschutzbeauftragten im häuslichen Bereich zuzustimmen.

– Natürlich sollte – wie bereits erwähnt – auch eine **Dienstvereinbarung** mit der Personalvertretung **bezüglich der erforderlichen Kontrollmaßnahmen** (z.B. Einsatz und Auswertung von Protokollierungen) getroffen werden. Dabei sollte auch den Datenschutzzielen der Nichtverkettbarkeit und der Transparenz Rechnung getragen werden.

– Bei der Telearbeit sollten die erforderlichen **IKT-Geräte und** die für die Verarbeitung **notwendige Software vom Dienstherrn gestellt und von einer zentralen Stelle konfiguriert** werden. Das Ausstatten eines Telearbeitsplatzes mit einem **Drucker** sollte **nur in unabdingbaren Fällen** erfolgen; dadurch kann auch das Risiko einer unberechtigten Offenbarung dienstlicher Angelegenheiten und personenbezogener Daten am Telearbeitsplatz sowie das Risiko einer nicht datenschutzkonformen Entsorgung von Fehldrucken erheblich reduziert werden.

– Die Telearbeiter sind dazu zu verpflichten, die vom Dienstherrn zur Verfügung gestellte **technische Infrastruktur ausschließlich für dienstliche Zwecke** und nur durch sie selbst zu nutzen.

– Das **Einspielen privater Software, das Verändern der vorgegebenen Systemeinstellungen und das Anschließen privater Hardware** (z.B. Drucker, USB-Sticks) **sind zu verbieten und soweit möglich technisch zu verhindern**.

– Die am Telearbeitsplatz installierten Endgeräte müssen über die notwendige **Zugangs- und Zugriffssicherung** verfügen. So sollte darauf geachtet werden, dass alle Rechner mit einer Sicherheitskomponente gegen eine unbefugte Inbetriebnahme abgesichert sind. Außerdem ist dafür Sorge zu tragen, dass sich jeder Telearbeiter mittels Benutzerkennung und geeignetem Passwort – möglichst mit Chipkarte oder RSA-Token gekoppelt – an seinem Telearbeitsplatz und im Netzwerk des Dienstherrn identifizieren und authentifizieren muss.

– Aus Sicherheitsgründen sollten soweit möglich **alle Daten zentral beim Dienstherrn gespeichert** und damit eine dezentrale Speicherung des Datenbestands beim Telearbeiter vermieden werden. Dazu empfiehlt sich insbesondere der Einsatz sogenannter Thin Clients (IT-Geräte ohne inte-

grierte Speichermedien). Wenn überhaupt sollte auf den Endgeräten eine ausschließlich begrenzte Speicherhaltung der Nutzdaten gestattet werden und die Anweisung bestehen, diese Daten unverzüglich zu löschen, sobald sie für eine weitere Bearbeitung nicht mehr benötigt werden.

– Bei der im Rahmen der Telearbeit stattfindenden Datenübertragung zwischen einem Telearbeitsrechner und dem Kommunikationsrechner der Dienststelle werden dienstliche Informationen üblicherweise über öffentliche Kommunikationsnetze übertragen. Da weder die Dienststelle noch die Telearbeiter großen Einfluss darauf nehmen können, ob die Vertraulichkeit, Integrität und Verfügbarkeit in einem öffentlichen Kommunikationsnetz gewahrt werden, sind zusätzliche Maßnahmen erforderlich. **Zur Sicherstellung der Vertraulichkeit während der Datenübertragung ist daher eine geeignete Datenverschlüsselung einzusetzen.**

– Der **sichere Verbindungsaufbau zur Dienststelle** (z.B. mittels so genannter Call Back-Funktion und Einsatz eines VPN) sowie der Einsatz **sicherer Identifikations- und Authentifizierungsmechanismen** sind ebenfalls zu gewährleisten.

– Natürlich muss auch der **Aktentransport** geregelt sein. Dabei ist darauf zu achten, dass personenbezogene Unterlagen **ausschließlich in verschlossenen Behältnissen** transportiert werden. Außerdem sind die mit dem Transport Beschäftigen darauf hinzuweisen, dass sie – soweit beim Transport öffentliche Verkehrsmittel benützt werden – darauf zu achten haben, dass die Behältnisse dort nicht unbeaufsichtigt abgestellt oder womöglich ganz vergessen werden.

– Für die **Aufbewahrung der Arbeitsunterlagen im häuslichen Bereich** sollte ein **verschließbarer Schrank** zur Verfügung stehen. Unter Umständen lassen sich auch die **verschließbaren Transportbehältnisse** zur Aufbewahrung heranziehen. Die Unterlagen dürfen in keinem Fall in der Wohnung für Dritte offen zugänglich sein – auch nicht für Familienangehörige.

– Ein häufiger Schwachpunkt bei der Telearbeit ist die eventuell anfallende **datenschutzgerechte Entsorgung nicht mehr benötigter Daten und Unterlagen**. Damit diese gewährleistet werden kann, sollten – soweit erforderlich – die dazu notwendigen Hilfsmittel (z.B. Software zum Löschen der auf dem Rechner gespeicherten Daten) auf dem Telearbeitsrechner auch vorhanden sein. Ist der Telearbeitsplatz (ausnahmsweise) mit einem Drucker ausgestattet, so sollte zur Sicherstellung einer datenschutzgerechten Entsorgung von Papierunterlagen (z.B. Fehldrucken) diese ausschließlich in der Dienststelle erfolgen.

2.1.5 Systeme zur Verkehrsplanung / -steuerung und Autofahrerinformation

Bluetoothbasierte Reisezeitmessung

Neben der im letzten Tätigkeitsbericht dargestellten kennzeichenbasierten Reisezeitmessung (siehe hierzu 24. Tätigkeitsbericht, Nr. 2.2.9) haben Verkehrsplaner in den Städten sowie bei den Autobahndirektionen insbesondere aus Kostengründen zunehmend Interesse an einer bluetoothbasierten Reisezeitmes-

sung. Hierbei soll nicht mehr das Kennzeichen des vorbeifahrenden Kraftfahrzeugs, sondern die **Bluetooth-Geräte-Adresse** von im Fahrzeug vorhandenen Bluetooth-Geräten (wie z.B. Handys, Smartphones, Freisprechanlagen) an Messpunkten ausgelesen werden. Die Messstationen schicken die erfassten Daten an eine Datenbank zur weiteren Auswertung.

Dabei stellt sich zunächst die Frage, ob die Bluetooth-Geräte-Adressen, oder allgemeiner gesprochen, die MAC-Adressen (Media-Access-Control-Adresse) von Geräten, als personenbezogene oder personenbeziehbare Daten anzusehen sind. Im Gegensatz zur gleichlautenden Frage bei IP-Adressen sind hierzu noch keine Gerichtsentscheidungen ergangen.

Bei einer Bewertung dieser Frage ist in jedem Fall zu berücksichtigen, dass **MAC-Adressen weltweit eindeutig und für die gesamte Lebensdauer eines Gerätes diesem fest zugeordnet** sind. Wird die MAC-Adresse ohne weitere Modifizierung in einer Datenbank zur Auswertung von Verkehrsflüssen gespeichert, so ist hier eine umfassende und langfristige Bildung von Bewegungsprofilen möglich.

Bezüglich derartiger Profile kann nicht vollständig ausgeschlossen werden, dass über Zusatzinformationen eine Identifizierung des Gerätebesitzers möglich ist. Im Internet gibt es beispielsweise eine Vielzahl von Stellen, an denen MAC-Adressen mit identifizierenden Daten verknüpft werden können, z.B. bei der Anmeldung an Web-Portalen, beim Hersteller / Verkäufer eines Geräts etc. Auch kann nicht ausgeschlossen werden, dass zukünftig Zuordnungslisten zur Reidentifizierung z.B. für Diensthandys beim Arbeitgeber oder für Strafverfolgungsbehörden geführt werden. Wenn dann dazu umfassende Datenbestände zu Bewegungsprofilen der Bluetooth-Geräte vorlägen, böten sich sicher interessante Auswertungsmöglichkeiten.

Schon allein die **Möglichkeit zur Bildung von Bewegungsprofilen** ist daher kritisch zu sehen und es sind technische Maßnahmen erforderlich, um einerseits sicherzustellen, dass keine langfristigen Bewegungsprofile entstehen können und andererseits eine Reidentifizierung der erfassten Bewegungsdaten unmöglich ist.

Dies bedeutet, dass für eine Realisierung von Projekten zur bluetoothbasierten Reisezeitmessung die im letzten Tätigkeitsbericht aufgeführten **Voraussetzungen** erfüllt und die **technischen und organisatorischen Maßnahmen** analog ergriffen werden müssen (siehe hierzu 24. Tätigkeitsbericht, Nr. 2.2.9). Dazu zählen insbesondere die sofortige Umwandlung der erfassten Bluetooth-Geräte-Adresse in einen Hashwert und das Verwerfen der erfassten Bluetooth-Geräte-Adresse schon in der Messstation sowie Maßnahmen zur Verhinderung der Zusammenführung von erfassten Daten über mehrere Tage hinweg. Die erfassten Bluetooth-Geräte-Adressen dürfen keinesfalls von der Messstation an die Auswertungsdatenbank weitergegeben werden. Zur Absicherung des Gesamtsystems sollte ein Datenschutz- und Sicherheitskonzept erstellt werden. Dabei sind auch Fragen wie Diebstahlschutz bei den Messstationen etc. zu betrachten.

Ein besonderes Augenmerk ist zudem auf die **Beteiligung externer Dienstleister** zu richten. Externe Dienstleister sind z.B. als Anbieter oder Betreiber der technischen Infrastruktur, für die Auswertung und Bereitstellung von Daten oder Wartungsaufgaben denkbar. Externe Dienstleister sollten grundsätzlich keinen Zugriff auf besonders sensible Bereiche des Gesamtverfahrens besitzen. Dies

betrifft vor allem die **Messstationen**, in denen kurzzeitig die erfasste Bluetooth-Geräte-Adresse vorliegt. Diese sollten sich **im ausschließlichen Hoheitsbereich der öffentlichen Stelle**, die die Reisezeitmessungen durchführt, befinden. Der Dienstleister darf höchstens in Ausnahmefällen und unter Kontrolle der öffentlichen Stelle auf die Messstationen zugreifen. Die üblichen Vorgaben der Fernwartung sind analog anzuwenden.

Des Weiteren müssen sich **auch das Hashverfahren und die hierbei verwendeten Schlüssel bzw. verwendete Schlüsselerzeugungssoftware** in der ausschließlichen Hoheit der öffentlichen Stellen befinden. Bezüglich der Auswertungsdatenbank muss sichergestellt sein, dass sie nur für die Zwecke der öffentlichen Stelle genutzt und getrennt von anderen Systemen zur Reisezeitmessung des externen Dienstleisters betrieben wird. Zur Regelung dieser Punkte sind entsprechende Verträge mit dem Dienstleister abzuschließen.

Webcams auf Autobahnen

Zur umfassenden Information der Bürger über das aktuelle Verkehrsgeschehen planen die bayerischen Autobahndirektionen den Einsatz von Webcams an Baustellen und kritischen Verkehrspunkten, so dass sich der Bürger über das Internet direkt selbst einen Einblick in die **dortige aktuelle Verkehrslage** verschaffen kann.

Ich halte den Einsatz von Webcams für **akzeptabel**, wenn sichergestellt ist, dass dabei keine personenbezogenen oder personenbeziehbaren Daten erhoben werden, d.h. wenn im Internet weder Kfz-Kennzeichen noch Personen identifizierbar sind und auch keine Verfolgung von Einzelfahrzeugen (z.B. grünes Auto mit Anhänger) über mehrere Streckenabschnitte hinweg möglich ist. **Die Autobahndirektionen setzen dementsprechend eigene Kameras nur für den Zweck der Bürgerinformation ein. Die Systeme zur Verkehrsüberwachung** (z.B. Standstreifenfreigabe), die deutlich mehr Möglichkeiten bieten, **sind davon völlig getrennt.**

Die Webcams haben eine feste Konfiguration, die sicherstellt, dass die Auflösung ausreichend grob ist, so dass keine Details zu erkennen sind und auch über Grafikprogramme keine Nachbearbeitung (Vergrößerung etc.) möglich ist. Zudem sind die Standorte so gewählt, dass nur Übersichtsaufnahmen über einen Streckenabschnitt erzeugt werden. Ich habe die Autobahndirektionen außerdem darauf hingewiesen, dass **kein flächendeckender Aufbau von Webcams über das gesamte Autobahnnetz hinweg** erfolgen darf, um auch so eine optische Verfolgungsmöglichkeit von Einzelfahrzeugen zu verhindern.

Idealerweise sollten die Bilder der Webcams nicht gespeichert werden, um Begehrlichkeiten zu vermeiden. Wird eine Speicherung im Einzelfall dennoch als erforderlich angesehen, so muss geprüft werden, zu welchen Zwecken dies erfolgt, welche Auswertungen vorgesehen sind und welche Personen diese durchführen dürfen. Sowohl für die Speicherung und Nutzung zu anderen Zwecken (als der allgemeinen Bürgerinformation) als auch für eine etwaige Weitergabe an andere Stellen muss eine Rechtsgrundlage vorhanden sein. Zudem müssen entsprechende technisch-organisatorische Maßnahmen nach Art. 7 BayDSG zum Schutz der gespeicherten Daten ergriffen werden.

2.1.6 Auftragsdatenverarbeitung durch die staatlichen Rechenzentren

In meinem letzten Tätigkeitsbericht hatte ich ausgeführt, dass der Freistaat Bayern seit dem Beschluss des Ministerrats vom 29.07.2003 damit befasst ist, die bisherigen Rechen- und IT-Betriebszentren der Staatsverwaltung organisatorisch in zwei Rechenzentren zusammenzufassen (siehe hierzu 24. Tätigkeitsbericht, Nr. 2.1.3). Dabei habe ich auch darauf hingewiesen, dass die einzige Möglichkeit, die Administration und den IT-Betrieb außerhalb des eigenen Bereichs zu geben, aus datenschutzrechtlicher Sicht in der sogenannten Datenverarbeitung im Auftrag gemäß Art. 6 BayDSG besteht. In diesem Zusammenhang hatte ich auch darauf hingewiesen, dass ich die zwischen den Rechenzentren und den entsprechenden Dienststellen getroffenen Vereinbarungen zur Datenverarbeitung im Auftrag sowie deren technische Umsetzung zum gegebenen Zeitpunkt überprüfen werde.

Art. 6 BayDSG Erhebung, Verarbeitung oder Nutzung personenbezogener Daten im Auftrag
(1) [1]Werden personenbezogene Daten durch andere Stellen im Auftrag erhoben, verarbeitet oder genutzt, bleibt der Auftraggeber für die Einhaltung der Vorschriften dieses Gesetzes und anderer Vorschriften über den Datenschutz verantwortlich. [2]Die im Zweiten Abschnitt genannten Rechte sind ihm gegenüber geltend zu machen.
(2) [1]Auftragnehmer sind unter besonderer Berücksichtigung der Eignung der von ihnen getroffenen technischen und organisatorischen Maßnahmen sorgfältig auszuwählen. [2]Der Auftrag ist schriftlich zu erteilen, wobei Datenerhebung, -verarbeitung oder -nutzung, die technischen und organisatorischen Maßnahmen und etwaige Unterauftragsverhältnisse festzulegen sind. [3]Der Auftraggeber hat sich soweit erforderlich von der Einhaltung der getroffenen technischen und organisatorischen Maßnahmen beim Auftragnehmer zu überzeugen.
(3) [1]Ist eine öffentliche Stelle Auftragnehmer, so gelten für sie nur die Art. 5, 7, 25, 29 bis 31, 32 Abs. 1 bis 3, Art. 33 und 37. [2]Der Auftragnehmer darf die Daten nur im Rahmen der Weisungen des Auftraggebers erheben, verarbeiten oder nutzen. [3]Ist er der Ansicht, daß eine Weisung des Auftraggebers gegen dieses Gesetz oder andere Vorschriften über den Datenschutz verstößt, hat er den Auftraggeber unverzüglich darauf hinzuweisen.
(4) [1]Die Absätze 1 bis 3 gelten entsprechend, wenn die Prüfung oder Wartung automatisierter Verfahren oder Datenverarbeitungsanlagen durch andere Stellen vorgenommen wird und dabei ein Zugriff auf personenbezogene Daten nicht ausgeschlossen werden kann. [2]Ist eine schriftliche Auftragserteilung nach Absatz 2 Satz 2 nicht möglich, so ist diese unverzüglich nachzuholen.

Um den hohen Aufwand von Einzelvereinbarungen und das Risiko von widersprüchlichen Anforderungen an die Rechenzentren zu vermeiden, haben das Bayerische Staatsministerium des Innern und die CIO-Stabsstelle den Entwurf einer Musterrahmenvereinbarung erarbeitet, die jedes Ressort für sich und alle seine Behörden mit dem jeweils beauftragten Rechenzentrum abschließen können und mit der die gesetzlichen Grundanforderungen abdeckt werden sollen. Der CIO-Rat hat in seiner 11. Sitzung im November 2012 den vorgelegten Vorschlag der Musterrahmenvereinbarung Auftragsdatenverarbeitung gebilligt und der Staatskanzlei und den Ressorts empfohlen, die entsprechenden Vereinbarungen mit den Rechenzentren und dem Landesamt für Finanzen zu schließen. Ich weise darauf hin, dass u.U. durch Zusatzvereinbarungen über die in der Musterrahmenvereinbarung geregelten Inhalte hinaus weitere Einzelregelungen getroffen werden müssten.

2.2 Prüfungen, Beanstandungen und Beratungen

Nach wie vor erfreulich ist, dass die Nachfragen öffentlicher Stellen nach Beratung sowohl postalisch als auch per E-Mail und telefonisch auch in diesem Berichtszeitraum sehr ausgeprägt waren. Gerne komme ich diesen Wünschen nach, muss allerdings dafür um Verständnis bitten, dass ich in Anbetracht meiner begrenzten Personalresourcen und der Vielzahl der Anfragen und Eingaben weiterhin auf einer Vorabbewertung des behördlichen Datenschutzbeauftragten beharren muss und dass auch manche Beratungsleistungen nicht immer in der gewünschten kurzen Zeitspanne erbracht werden können.

2.2.1 Prüfungen

Im Berichtszeitraum 2011/2012 wurde von mir eine ganze Reihe öffentlicher Stellen unter technisch-organisatorischen Datenschutzaspekten geprüft und beraten. Teilweise wurden diese Prüfungen und Beratungen von meinem Technikreferat gemeinsam mit dem jeweils zuständigen Rechtsreferat durchgeführt. Besonders hervorzuheben sind folgende Stellen:

- AOK Bayern – Die Gesundheitskasse
- Autobahndirektion Südbayern München
- Bezirk Oberbayern
- Mehr als 2.500 staatliche und kommunale Behörden
- Gesundheitsamt Nürnberg
- iMVS-Koordinierungsstelle Kempten
- Isar-Amper-Kliniken Taufkirchen an der Vils
- Klinikum Garmisch-Partenkirchen
- Klinisches Krebsregister Bayreuth
- Klinisches Krebsregister München-Großhadern
- Klinisches Krebsregister Regensburg
- Landesamt für Gesundheit und Lebensmittelsicherheit Oberschleißheim
- Landesamt für Verfassungsschutz
- Landeskriminalamt
- Landratsamt Bayreuth
- Psychiatrische Klinik des Universitätsklinikum Würzburg
- 6 Sozialbürgerhäuser in München
- Städtische Klinikum München GmbH
- Universitätsklinikum München
- 8 Erhebungsstellen zum Zensus 2011

Auf wesentliche Projekte und Anfragen gehe ich in den unteren Abschnitten im Einzelnen ein.

2.2.2 Beanstandungen

Leider musste ich in diesem Berichtszeitraum im technisch-organisatorischen Bereich auch mehrere Beanstandungen nach Art. 31 Abs. 1 BayDSG aussprechen.

16 Beanstandungen betrafen Städte und Gemeinden, die trotz Aufforderung, den unzulässigen Einsatz von Google Analytics zur Analyse der Nutzerzugriffe (siehe Nr. 2.3.2) auf ihre Webseiten und damit den Einsatz IP-adressenbe-

zogener Auswertungen des Verhaltens von Internetnutzern zu beenden, fortgesetzt haben. Erst nach der formell ausgesprochenen Beanstandung haben auch diese Gemeinden von einer weiteren unzulässigen Nutzung von Google Analytics abgesehen.

Eine Beanstandung betraf ein Kreisjugendamt, weil ich dort tatsächliche Verstöße gegen die Vorschriften des § 35 Abs. 1 Satz 1 SGB I, des § 78 a Satz 1 SGB X und des Art. 7 Abs. 1 BayDSG dergestalt festgestellt habe, dass

– eine unberechtigte Kenntnisnahme von personenbezogenen Daten (Sozialdaten) von außerhalb des Gebäudes durch die Kellerfenster nicht verhindert und so wenigstens in einem Fall personenbezogene Daten (Sozialdaten) tatsächlich an unberechtigte Dritte offenbart,

– keine Maßnahmen zur Verhinderung des unberechtigten Zugangs und Zugriffs auf die im Kellerflur des Archivbereichs gelagerten Akten ergriffen und

– keine ausreichenden technisch-organisatorischen Maßnahmen zur datenschutzgerechten Entsorgung von Fehlablichtungen getroffen worden waren.

Ein Absehen von der Beanstandung gem. Art. 31 Abs. 3 BayDSG schied im vorliegenden Fall aus, da eine unberechtigte Offenbarung von personenbezogenen Daten tatsächlich erfolgt war und nicht mehr ungeschehen gemacht werden konnte. Außerdem war dieser Verstoß schwerwiegend und nicht unerheblich, da es sich bei den offenbarten Daten um besonders schutzwürdige Sozialdaten handelte.

Eine weitere Beanstandung betraf ein Klinikum, weil ich dort einen schwerwiegenden Verstoß gegen den Datenschutz und die Pflicht zur Ergreifung von angemessenen technisch-organisatorischen Maßnahmen zum Schutz von personenbezogenen Daten mit besonderem Schutzbedarf (Personalaktendaten) dergestalt feststellen musste, dass

– zum einen das Kündigungsschreiben des Klinikums an eine Mitarbeiterin in einem Umschlag unter den Scheibenwischer des Fahrzeugs der Mitarbeiterin, das vor ihrer Wohnung geparkt war, angebracht und

– zum anderen das Kündigungsschreiben in dreifacher Form in drei Briefumschlägen an der Außentüre des Mehrparteienwohnhauses der Mitarbeiterin befestigt worden war.

Ein Absehen von der Beanstandung gem. Art. 31 Abs. 3 BayDSG schied auch in diesem Fall aus, da das Hinterlegen von Personalaktendaten (Kündigungsschreiben) im öffentlichen Raum an einem Fahrzeug und an der Haustüre keine geeignete Maßnahme zur sicheren Übermittlung von besonders schutzwürdigen Daten darstellt und es sich im vorliegenden Fall zwar nicht um den Regelfall, aber doch auch nicht um ein einmaliges Versehen hinsichtlich der Zustellungsart gehandelt hatte.

2.2.3 Nutzung externer Wäschereidienstleistungen in Krankenhäusern und Pflegeeinrichtungen

Im Berichtszeitraum erreichten mich eine ganze Reihe von Eingaben und Anfragen zum Thema der Reinigung von Dienstbekleidung sowie der Reinigung von Patientenbekleidung in Krankenhäusern und Pflegeeinrichtungen durch externe Dienstleister. Dies wird in den verschiedenen Einrichtungen sehr unterschiedlich gehandhabt. Ein Teil der Einrichtungen betreibt hauseigene Wäschereien, ein Teil nutzt externe Dienstleister. Welche Leistungen dabei in Anspruch genommen werden ist sehr vielfältig.

Eine **Relevanz aus Datenschutzsicht** gewinnt die Nutzung externer Wäschereidienstleister **bei der Reinigung von Mitarbeiter- oder Patientenbekleidung** immer dann, **wenn personenbezogene Daten wie Namen, Funktionsbezeichnung etc. an den externen Dienstleister weitergeben werden**. Dies kann zum einen der Fall sein, wenn die zu reinigende Bekleidung mit den Namen der Mitarbeiter oder Patienten beschriftet ist, zum anderen wenn Zusatzleistungen wie z.B. die Erstellung von Namensschildern oder die Verwaltung und Ausgabe beschrifteter Kleidung durch den Dienstleister erbracht werden sollen.

Einordnung aus Datenschutzsicht

Wird dem externen Dienstleister Wäsche übergeben, die mit dem Namen des Mitarbeiters oder des Patienten versehen ist, so handelt es sich um eine Datennutzung durch den externen Dienstleister. Auch wenn der Dienstleister die Namen nicht für seine Aufgabenerfüllung, also die Reinigung der Wäsche benötigt, ist davon auszugehen, dass die Mitarbeiter bei ihren Arbeiten Kenntnis von den Namen erlangen können. Es sind daher gewisse Schutzmaßnahmen erforderlich. Ein besonderes Augenmerk ist hierbei auf infektiöse Wäsche zu richten: Ist infektiöse Wäsche als solche besonders gekennzeichnet und mit personenbezogenen Daten versehen oder weist die einer Person zuzuordnende Wäsche sonstige, besondere Eigenschaften auf, werden nicht nur die Patienten- bzw. die Bewohnereigenschaft, sondern zusätzliche, überdies besonders sensible Gesundheitsdaten weitergegeben. Es bedarf einer Offenbarungsbefugnis auf Seiten des Krankenhauses bzw. der Alten- und/oder Pflegeeinrichtung, die im Normalfall in einer **ausdrücklichen Einwilligung des Betroffenen** zu sehen sein wird (im Rahmen der vertraglichen Regelung zwischen Einrichtung und Patient oder Bewohner).

Übernimmt die Wäscherei Zusatzaufgaben wie **Erstellung von Namensschildern oder die Verwaltung und Ausgabe von mit Namen beschrifteter Bekleidung**, müssen personenbezogene Daten (Namen der Mitarbeiter, ggf. Angaben zur Position und zur Tätigkeit etc.) an den externen Dienstleister übermittelt werden. In diesen Fällen handelt es sich um eine Auftragsdatenverarbeitung, für die entsprechende Regelungen getroffen werden müssen. Dies kann in einem eigenen **Vertrag zur Auftragsdatenverarbeitung** oder aber als Teil des Dienstleistungsvertrags erfolgen.

Erforderliche Schutzmaßnahmen

Grundsätzlich ist immer das **Prinzip der Datensparsamkeit** zu beachten, d.h. die Abläufe, Bestellungen, Rechnungen etc. müssen so organisiert sein, dass möglichst wenig personenbezogene Daten übermittelt werden bzw. nicht ohne Weiteres einsehbar sind.

Bei einer externen Reinigung beschrifteter Mitarbeiterbekleidung müssen die Mitarbeiter der Einrichtung hierüber im Rahmen des Beschäftigungsverhältnisses informiert werden. Handelt es sich um personenbezogene Patientenbekleidung, müssen die Weitergabe der Wäsche sowie die Schutzmaßnahmen vertraglich zwischen Patient und Auftrag gebender Einrichtung geregelt werden.

Die **Beschäftigten des externen Dienstleisters** müssen in beiden Fällen über den Umgang mit den personenbezogenen Kleidungsstücken und Namensangaben **belehrt und zur Verschwiegenheit verpflichtet** werden. Sowohl **beim Transport der Wäsche als auch während der Reinigung** ist darauf zu achten, dass **Unbefugte keine Einsicht** in die Beschriftung der Kleidung erhalten können und die für die Reinigung zuständigen Beschäftigten des externen Dienstleisters möglichst wenig Einsicht erhalten.

Besondere Schutzmaßnahmen sind bei **personenbezogener infektiöser Wäsche** erforderlich, insbesondere **darf** auf der Verpackung der Wäsche **nicht ersichtlich sein, um welchen Patienten es sich handelt**. Zudem dürfen Auftragsformulare, Rechnungen etc. keine Angaben zum Namen des Patienten bzw. zur Infektion enthalten.

Die **ergriffenen Schutzmaßnahmen** sowie die **Pflichten des Dienstleisters** und des Auftraggebers beim Umgang mit personenbezogener Kleidung müssen im **Vertrag mit der Wäscherei** mit festgelegt werden.

Handelt es sich nicht nur um eine Datennutzung, sondern eine Auftragsdatenverarbeitung, bei der der externe Dienstleister Namenslisten etc. erhält, um gewisse Tätigkeiten damit auszuführen, ist eine vertragliche Regelung zur Auftragsdatenverarbeitung erforderlich. Hierbei müssen u.a. folgende Punkte geregelt werden: Aufgaben des Auftragnehmers, Zweckbindung der Daten, Verschwiegenheitspflichten der Mitarbeiter des Dienstleisters, Kontrollrechte des Auftraggebers, Regelungen zum Umgang mit den Daten, technisch-organisatorische Sicherheitsmaßnahmen insbesondere wenn die Daten per E-Mail übermittelt werden, Datenlöschung. Für eine ausführliche Darstellung der Thematik Auftragsdatenverarbeitung siehe auch die Orientierungshilfe Auftragsdatenverarbeitung, abrufbar unter www.datenschutz-bayern.de.

Insgesamt betrachtet sollten **vor dem Einsatz eines externen Dienstleisters** von der Auftrag gebenden Stelle daher **unter Beachtung des Prinzips der Datensparsamkeit immer folgende Punkte geprüft und entsprechend geregelt werden**:

– Festlegung der vom externen Dienstleister zu erbringenden Leistungen und Prüfung, ob personenbezogene Wäschestücke oder Daten weitergegeben werden

– Information der eigenen Mitarbeiter im Rahmen des Beschäftigungsverhältnisses über die Weitergabe beschrifteter Kleidung oder von Namenslisten

– Vertragliche Regelungen mit dem Patienten bei der externen Reinigung personenbezogener Patientenwäsche

- Prüfung der erforderlichen vertraglichen Regelungen mit dem externen Dienstleister

  - Vertragliche Regelungen zum Umgang mit personenbezogener Wäsche
  - Auftragsdatenverarbeitung bei der Weitergabe von Namenslisten
  - Regelung von Unterauftragsverhältnissen

- Inhaltlich zu klärende Aspekte

  - Datenschutzgerechte Abläufe bei Bestellung und Erstellung von personalisierter Kleidung beim Dienstleister
  - Verfahrensweisen zum datenschutzgerechten Transport der Wäsche
  - Regelungen zum Umgang mit beschrifteter Kleidung während der Reinigung beim externen Dienstleister
  - Regelungen zum Umgang mit Namenslisten durch die Beschäftigten des externen Dienstleisters
  - Verschwiegenheitspflichten der Beschäftigten des externen Dienstleisters
  - Umgang mit personenbezogener infektiöser Wäsche
  - Technisch-organisatorische Maßnahmen beim Dienstleister zum Schutz vor unbefugter Kenntnisnahme
  - Datenschutzgerechte Gestaltung von Rechnungen

2.2.4 Teleradiologie mit externem Dienstleister

Es ist zu beobachten, dass Krankenhäuser zunehmend im Bereich der Teleradiologie kooperieren. Um nicht selbst eine Kommunikationsinfrastruktur zum Austausch von Radiologiedaten schaffen zu müssen, besteht von Seiten der Krankenhäuser häufig der Wunsch nach einer Beteiligung externer Dienstleister. Demgemäß sind verschiedenste kommerzielle Anbieter aus der Privatwirtschaft tätig. Deren Angebote umfassen z.B. die Bereitstellung einer technischen Kommunikationsinfrastruktur inklusive Sicherheitsmaßnahmen wie Authentifizierung, VPN etc., an die das Krankenhaus nur noch angebunden werden muss. Zudem wird die benötigte Software zum Bereitstellen, Empfangen und Betrachten von Daten etc. angeboten. Der Betrieb und die Wartung der Infrastruktur sowie die Installation vor Ort werden ebenfalls vom Dienstleister angeboten.

Allerdings ist bei einer Beteiligung externer Dienstleister immer zu beachten, dass personenbezogene medizinische Daten mit einem erhöhten Schutzbedarf versehen und durch die ärztliche Schweigepflicht besonders geschützt sind. Zudem gilt in Bayern Art. 27 Abs. 4 Bayerisches Krankenhausgesetz (BayKrG), der festlegt, dass personenbezogene medizinische Daten im Gewahrsam des Krankenhauses verbleiben müssen.

Art. 27 Abs. 4 Bayerisches Krankenhausgesetz (BayKrG)
Die Krankenhausärzte dürfen Patientendaten nutzen, soweit dies im Rahmen des krankenhausärztlichen Behandlungsverhältnisses, zur Aus-, Fort- und Weiterbildung im Krankenhaus, zu Forschungszwecken im Krankenhaus oder im Forschungsinteresse des Krankenhauses erforderlich ist. Sie können damit andere Personen im Krankenhaus beauftragen, soweit dies zur Erfüllung dieser Aufgaben erforderlich ist; zu Zwecken der Forschung nach Satz 1 können sie anderen

Personen die Nutzung von Patientendaten gestatten, wenn dies zur Durchführung des Forschungsvorhabens erforderlich ist und die Patientendaten im Gewahrsam des Krankenhauses verbleiben. Diese Personen sind zur Verschwiegenheit zu verpflichten. Die Krankenhausverwaltung darf Patientendaten nutzen, soweit dies zur verwaltungsmäßigen Abwicklung der Behandlung der Patienten erforderlich ist. Das Krankenhaus kann sich zur Verarbeitung und Mikroverfilmung von Patientendaten anderer Personen oder Stellen bedienen, wenn es sicherstellt, dass beim Auftragnehmer die besonderen Schutzmaßnahmen nach Abs. 6 eingehalten werden, und solange keine Anhaltspunkte dafür bestehen, dass durch die Art und Ausführung der Auftragsdatenverarbeitung schutzwürdige Belange von Patienten beeinträchtigt werden. Zur Verarbeitung oder Mikroverfilmung von Patientendaten, die nicht zur verwaltungsmäßigen Abwicklung der Behandlung der Patienten erforderlich sind, darf sich das Krankenhaus jedoch nur anderer Krankenhäuser bedienen.

Daher ist ein besonderes Augenmerk auf die **genaue vertragliche Ausgestaltung und die Eigentumsverhältnisse bezüglich der Infrastrukturkomponenten** zu richten:

Es ist beispielsweise denkbar, dass sich die Infrastrukturkomponenten im Eigentum und auch in den Räumen eines Krankenhauses befinden und der **externe Dienstleister nur mit Wartungsaufgaben** betraut ist. Die Daten würden somit nicht den Gewahrsam eines Krankenhauses verlassen. Für die Beteiligung des externen Dienstleisters wären dann Maßnahmen analog zur Fernwartung erforderlich (siehe hierzu 18. Tätigkeitsbericht, Nr. 3.3.4).

Befinden sich die Komponenten dagegen in einem **Rechenzentrum des Dienstleisters**, so muss sichergestellt sein, dass dieser nicht auf personenbezogene medizinische Daten zugreifen kann – dies kann nur durch eine geeignete Datenverschlüsselung oder Pseudonymisierung erreicht werden. Zudem muss die Frage geklärt werden, wie eine Trennung von Datenströmen und Kommunikationsbeziehungen anderer Kunden des Dienstleisters erfolgt.

Die Nutzung der Kommunikationsinfrastruktur eines externen Dienstleisters stellt hohe Anforderungen an die **Absicherung der Datenübertragung**. Wie auch im Bereich der externen elektronischen Archivierung gilt die Grundannahme, dass medizinische Daten nur an externe Dienstleister weitergegeben werden dürfen, wenn für den Dienstleister auch bei einer Möglichkeit zur Einsichtnahme in die übertragenen Daten kein Personenbezug herstellbar ist (siehe hierzu 21. Tätigkeitsbericht, Nr. 22.2.3.2). Dies kann z.B. über eine **Pseudonymisierung oder über eine Ende-zu-Ende-Verschlüsselung** erreicht werden.

Eine **Pseudonymisierung** muss so ausgestaltet sein, dass auf Seiten des Krankenhauses, das die Daten übertragen möchte, alle identifizierenden Daten (Name, Adresse, Geburtsdatum, KV-Nummer etc.) aus den Daten entfernt werden. Dies betrifft sowohl DICOM-Bilder und Metadaten als auch Textdokumente wie z.B. Befunde. Die identifizierenden Daten müssen durch ein nichtsprechendes Pseudonym ersetzt werden. Das Verfahren zur Pseudonymgenerierung sowie entsprechende Schlüssel dürfen dem Dienstleister nicht bekannt oder zugänglich sein, sondern müssen in der ausschließlichen Hoheit des Krankenhauses verbleiben. Dies betrifft insbesondere auch die Hardware-Komponenten, auf denen die Schlüssel abgelegt werden bzw. die Pseudonymisierung erfolgt. Hier dürfen keine Wartungszugänge für den Dienstleister bestehen.

Bei einer **Verschlüsselung** der übertragenen Daten muss ebenfalls sichergestellt sein, dass der Dienstleister keine Möglichkeit zur Entschlüsselung der Daten hat. Dies bedeutet, dass eine Ende-zu-Ende-Verschlüsselung nötig ist: Die Ver- und Entschlüsselung darf nur innerhalb eines Krankenhauses erfolgen und der externe Dienstleister darf keinen Zugriff auf die Schlüssel und die entsprechenden Speicherkomponenten nehmen können. Während des gesamten Datentransports über die technische Infrastruktur, ebenso wie bei (temporären) Speicherungen auf Servern des Dienstleisters müssen die Daten verschlüsselt bleiben; der Dienstleister darf auch im Rahmen von Wartungsaufgaben keinen Zugriff auf personenbezogene medizinische Daten erhalten.

Neben diesen Spezialfragen zur Datenübertragung müssen für die Infrastruktur sowie für die angeschlossenen Endgeräte im Krankenhaus **Maßnahmen zur Sicherstellung der Integrität, Authentizität, Vertraulichkeit, Verfügbarkeit und Revisionsfähigkeit** bzw. die Anforderungen des Art. 7 BayDSG umgesetzt werden. Es empfiehlt sich daher immer die Erstellung eines **Datenschutz- und Sicherheitskonzepts** sowohl von Seiten des Dienstleisters als auch bezüglich der Anbindung des Klinikums an die Infrastruktur bzw. der Nutzung der Teleradiologie im Klinikum.

2.2.5 Telearbeit im Krankenhaus und mit Sozialdaten

Bisher wurde Telearbeit mit Sozialdaten sowie im Krankenhausbereich aufgrund der besonderen Sensibilität der Daten als unzulässig angesehen. Ohne dass rechtliche Änderungen eingetreten sind, gibt es jedoch aus technischer Sicht einige Entwicklungen, die zumindest einen Teil der bisherigen technischen Hinderungsgründe ausräumen können, so dass auch in diesen Bereichen nach genauer Prüfung und Abwägung verschiedener Aspekte eine Telearbeit denkbar sein kann (siehe Nr. 2.1.4 und Nr. 7.3).

Durch technische Entwicklungen wie Desktop-Virtualisierung, Terminalserver und VPNs kann heute Telearbeit derart realisiert werden, dass der Rechner am Telearbeitsplatz ausschließlich dazu dient, eine gesicherte Verbindung zu den Servern der Dienststelle aufzubauen und die Eingaben des Benutzers an den Server weiterzuleiten bzw. Daten am Bildschirm anzuzeigen. Hierzu wird dem Benutzer an seinem Telearbeitsplatz eine eigene virtuelle Umgebung bereitgestellt, über die das Login auf den zentralen Systemen der Dienststelle erfolgt. Alle Tätigkeiten werden dann direkt auf dem Server der Dienststelle ausgeführt, eine lokale Speicherung am Telearbeitsplatz ist nicht möglich. Nach dem Beenden der virtuellen Umgebung sind auf dem Telearbeitsrechner keinerlei Daten mehr vorhanden. Damit entfällt beispielsweise der Bedarf einer Festplattenverschlüsselung, Absicherung gegen Verlust des Geräts etc. Allerdings müssen weiterhin diverse Maßnahmen zur technischen Sicherung des Systems getroffen werden:

- **Keine Nutzung von Privatgeräten**: Die Rechner (PC, Notebook etc.), über die ein Zugriff erfolgt, müssen Eigentum des Dienstherrn sein und von dessen Administratoren gewartet werden.

- **Beschränkter Systemzugriff**: Ein Zugriff darf nur auf diejenigen Systeme möglich sein, die für die konkrete Aufgabe erforderlich sind.

- **Protokollierung**: Alle Zugriffe müssen protokolliert werden, um eine missbräuchliche Nutzung feststellen zu können.

– **Authentifizierung**: Es muss ein starkes Authentifizierungsverfahren verwendet werden, das über die Verwendung von Benutzerkennung und Passwort hinausgeht. Für medizinische Daten ist hierbei die Entschließung „Mindestanforderungen an den technischen Datenschutz bei der Anbindung von Praxis-EDV-Systemen an medizinische Netze“ der 81. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 16./07.03.2011 zu beachten.

– **Gesicherte Datenübertragung**: Die Datenübertragung zwischen den Servern der Dienststelle und dem Telearbeitsplatz muss verschlüsselt erfolgen. Zudem empfiehlt sich eine gegenseitige Hardware-Authentifizierung der Geräte. Des Weiteren muss sichergestellt sein, dass keine Unbefugten sich über diese technische Zugangsmöglichkeit Zugriff auf die Systeme des Klinikums und die darauf gespeicherten Daten verschaffen können.

– **Schriftliche Regelungen**: Es muss schriftliche Dienstanweisungen/Dienstvereinbarungen/Richlinien geben, wie mit den Geräten und Zugriffsmöglichkeiten zu verfahren ist und welche Pflichten für den Nutzer bestehen.

Nach wie vor besteht allerdings das Problem einer unberechtigten Einsichtnahme in die gerade am Bildschirm angezeigten Daten durch z.B. Familienmitglieder. Bei Verzicht auf einen lokalen Drucker am Telearbeitsplatz werden auch die Probleme der Fertigung von Bildschirmausdrucken, Behandlung von Fehldrucken, unberechtigte Kenntnisnahme, Transport der Ausdrucke sowie der zugehörigen Logistik vermieden.

Es ist daher immer eine Abwägung zwischen dem Nutzen und den Risiken der Telearbeit erforderlich. Ist im Rahmen der Telearbeit auch der Transport von Akten oder die Möglichkeit zur Erstellung von Ausdrucken zu Hause nötig, so gelten weiterhin die Anforderungen der entsprechenden älteren Tätigkeitsberichte.

Entschließung der 81. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 16./17.03.2011
Mindestanforderungen an den technischen Datenschutz bei der Anbindung von Praxis-EDV-Systemen an medizinische Netze

Niedergelassene Ärztinnen und Ärzte sowie andere Angehörige von Heilberufen übermitteln vielfach medizinische Daten an andere Stellen mithilfe von Netzwerken. Dies dient Abrechnungs-, Behandlungs- und Dokumentationszwecken. Seit dem 01.01.2011 müssen beispielsweise an der vertragsärztlichen Versorgung teilnehmende Ärzte Abrechnungsdaten leitungsgebunden an die jeweilige Kassenärztliche Vereinigung übermitteln (§ 295 Abs. 4 SGB V in Verbindung mit den Richtlinien der Kassenärztlichen Bundesvereinigung für den Einsatz von IT-Systemen in der Arztpraxis zum Zweck der Abrechnung; siehe http://www.kbv.de/rechtsquellen/24631.html).

An medizinische Netze sind hohe Anforderungen hinsichtlich der Vertraulichkeit und Integrität zu stellen, denn sowohl in den Netzen selbst als auch auf den angeschlossenen Praxissystemen werden Daten verarbeitet, die der ärztlichen Schweigepflicht (§ 203 StGB) unterliegen. Bei der Anbindung von Praxis-EDV-Systemen an medizinische Netze ist daher die „Technische Anlage zu den Emp-

fehlungen zur ärztlichen Schweigepflicht, Datenschutz und Datenverarbeitung in der Arztpraxis" der Bundesärztekammer und der Kassenärztlichen Bundesvereinigung (siehe Deutsches Ärzteblatt, Jg. 105, Heft 19 vom 09.05.2008) zu beachten.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder fordert, dabei insbesondere folgende Mindestanforderungen zu stellen:

1. *Die Kommunikation im Netz muss verschlüsselt ablaufen. Hierzu sind dem Stand der Technik entsprechende Verfahren zu nutzen.*
2. *Ein unbefugter Zugriff auf die internen Netze der Praxis oder Einrichtung muss ausgeschlossen sein.*
3. *Die Auswirkungen von Fehlkonfigurationen im internen Netz müssen wirksam begrenzt werden.*
4. *Die Endpunkte der Kommunikation müssen sich gegenseitig durch dem Stand der Technik entsprechende Verfahren authentisieren.*
5. *Die Wartung der zum Netzzugang eingesetzten Hard- und Software-Komponenten muss kontrollierbar sein, indem die Wartung durch eine aktive Handlung freizuschalten ist und alle Wartungsaktivitäten protokolliert werden.*
6. *Zum Netzzugang sind zertifizierte Hard- und Software-Komponenten einzusetzen.*
7. *Grundstandards – wie beispielsweise die Revisionssicherheit – sind einzuhalten.*

Für die verwendeten Verschlüsselungs- und Authentisierungskomponenten sollten Hardware-Lösungen genutzt werden, da bei Software ein erhöhtes Manipulationsrisiko besteht.

Software-Lösungen kommen allenfalls in Ausnahmefällen in Betracht, wenn die zur Kommunikation mit anderen Stellen genutzten Rechner und Komponenten nicht mit dem internen Netz der Praxis verbunden sind. Zusätzlich ist sicherzustellen, dass

entweder

a) nur solche Daten gesendet werden, die bereits innerhalb des Praxisnetzes verschlüsselt und integritätsgeschützt wurden

oder

b)

- *eine Zwei-Faktor-Authentifikation des Berechtigten stattfindet,*
- *mit der zum Zugang verwendeten Hard- und Software ausschließlich Zu gang zu medizinischen Netzen besteht sowie*
- *die KBV-Richtlinien zur Online-Anbindung von Praxis-EDV-Systemen an das KV-SafeNet eingehalten werden.*

2.2.6 IT-Abschottung von Statistikstellen

Im Berichtszeitraum haben sich mehrere Kommunen mit der Bitte um Beratung an mich gewandt, weil sie eigene Statistikstellen einrichten wollen. Werden Statistiken außerhalb des Landesamts für Statistik und Datenverarbeitung (LfStaD) durchgeführt, so sind insbesondere die Vorgaben der Art. 20 und 21 Bayerisches Statistikgesetz (BayStatG) zu beachten:

Art. 20 Bayerisches Statistikgesetz (BayStatG)
(1) Werden Statistiken außerhalb des Landesamts durchgeführt, so sind besondere Statistikstellen einzurichten. Nichtstatistische Aufgaben des Verwaltungsvollzugs dürfen ihnen nicht übertragen werden. Statistikstellen veröffentlichen die Ergebnisse ihrer Statistiken oder stellen sie in sonstiger Weise bereit.
(2) Für jede Statistikstelle ist jemand zu bestimmen, der diese leitet. Statistikstellen sind räumlich und organisatorisch von anderen Verwaltungsstellen zu trennen, gegen den Zutritt unbefugter Personen hinreichend zu sichern und mit Personal auszustatten, das die Gewähr für Zuverlässigkeit und Verschwiegenheit bietet.

Art. 21 Bayerisches Statistikgesetz (BayStatG)
(1) Das Landesamt ist bei Statistiken, die es als allgemeine Aufgabe durchführt, Erhebungsstelle.
(2) Die Staatsregierung wird ermächtigt, durch Rechtsverordnung zu bestimmen, dass andere staatliche Stellen sowie Gemeinden Erhebungsstellen einzurichten oder in sonstiger Weise an der Durchführung amtlicher Statistiken mitzuwirken haben, wenn das wegen der Art der Erhebung, der Zahl oder der räumlichen Verteilung der zu Befragenden oder zur Sicherung der Qualität der Erhebung zweckmäßig ist. Eine aufsichtliche Zuständigkeit des Landesamts wird durch eine solche Bestimmung nicht begründet. Landratsämter erfüllen die Aufgaben der Erhebungsstellen als Staatsaufgaben; für Gemeinden handelt es sich um Aufgaben des übertragenen Wirkungskreises, die sie auch nach den Vorschriften des Gesetzes über die kommunale Zusammenarbeit erfüllen können.
(3) Die Erhebungsstellen nach Absatz 2 Satz 1 führen in ihrem jeweiligen Zuständigkeitsbereich die statistischen Erhebungen durch. Art. 20 Abs. 2 und 3 gelten entsprechend mit der Maßgabe, dass die räumliche und organisatorische Trennung von anderen Verwaltungsstellen ab dem Eingang der Erhebungsunterlagen bis zu ihrer Ablieferung sicherzustellen ist. …

Unter dieses von Art. 21 Abs. 3 Satz 1 BayStatG geforderte **Abschottungsgebot** fällt auch die Trennung der IT-Infrastruktur der Statistikstellen vom übrigen Verwaltungsnetz. Die Trennung der IT-Infrastruktur der Statistikstellen vom übrigen Verwaltungsnetz trägt in besonderer Weise dem Datenschutzziel der Nichtverkettbarkeit Rechnung. Da es in Bayern für die dabei zu treffenden Abschottungsmaßnahmen – insbesondere im IT-Bereich – keine weiterführende rechtliche Regelung gibt, hat das LfStaD in Abstimmung mit meiner Geschäftstelle einen **„Leitfaden zur Einrichtung abgeschotteter kommunaler Statistikstellen in Bayern“** erstellt. In diesem Leitfaden wird dargestellt, welche Maßnahmen zu ergreifen sind, um die Anforderung nach ausreichender Abschottung zu erfüllen.

Insbesondere werden den kreisfreien Städten und Landkreisen zwei Varianten bezüglich der IT-Abschottung ihrer Statistikstellen aufgezeigt.

Bei der **ersten Variante** befinden sich **sämtliche IT-Komponenten innerhalb der abgeschotteten Statistikstelle** und werden ausschließlich vom eigenen Personal der Statistikstelle betrieben. Diese Vorgehensweise ist grundsätzlich zu bevorzugen, da hier sämtliche Zuständigkeiten in der Hand der Statistikstelle bleiben und somit die Abschottung am zuverlässigsten gewährleistet werden kann.

Nach der **zweiten Variante** werden ein oder mehrere Server, auf dem/denen statistische Einzeldaten gespeichert sind, außerhalb der abgeschotteten Statis-

tikstellen in einem **kommunalen Rechenzentrum** installiert. **In diesem Fall müssen die Daten verschlüsselt gespeichert werden**. Die Verschlüsselung muss auch gegenüber der Systemverwaltung wirken, soweit sie nicht von Mitarbeitern der Statistikstelle gestellt wird (d.h. die Verschlüsselung muss bereits vor der Übertragung der Einzeldaten auf den Statistikdatenserver erfolgen).

Zusätzlich besteht **in Anlehnung an die Variante 1** die Möglichkeit, dass **mehrere kleinere Gemeinden** die Aufgaben einer abgeschotteten Statistikstelle im Wege der interkommunalen Zusammenarbeit (nach dem Gesetz über die kommunale Zusammenarbeit – KommZG) **einer gemeinsamen Statistikstelle** übertragen und so eine bestmögliche Abschottung erfüllbar machen.

Das LfStaD hat zugesagt, diesen Leitfaden dem Bayerischen Städtetag und dem Landkreistag zu präsentieren.

Ich werde zukünftig bei der Kontrolle von Statistikstellen die Einhaltung der beiden aufgezeigten Wahlmöglichkeiten überprüfen.

2.2.7 Bestellung eines externen Datenschutzbeauftragten

Auch in diesem Berichtszeitraum haben sich wieder eine Reihe öffentlicher Stellen mit dem Vorbringen, die Funktion des behördlichen Datenschutzbeauftragten einem Externen übertragen zu wollen, an mich gewandt und diesbezüglich um Beratung gebeten. Hierzu ist unter Beachtung der Bestimmungen der Art. 25 Abs. 2 und Art. 28 Abs. 2 Bayerisches Datenschutzgesetz (BayDSG) Folgendes festzustellen:

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

Art. 25 Abs. 2 Satz 1 BayDSG bestimmt, dass **grundsätzlich jede öffentliche Stelle in Bayern einen behördlichen Datenschutzbeauftragten zu bestellen hat**. Nur wenn die Voraussetzungen des Art. 28 Abs. 2 BayDSG vorliegen, sind bayerische öffentliche Stellen von der Pflicht, einen behördlichen Datenschutzbeauftragten zu haben, entbunden.

Art. 28 Abs. 2 Bayerisches Datenschutzgesetz (BayDSG)
(2) Die Bestellung behördlicher Datenschutzbeauftragter, die datenschutzrechtliche Freigabe und die Führung eines Verfahrensverzeichnisses sind nicht erforderlich, wenn in öffentlichen Stellen ausschließlich automatisierte Verfahren eingesetzt werden, von denen unter Berücksichtigung der erhobenen, verarbeiteten oder genutzten Daten eine Beeinträchtigung der Rechte und Freiheiten der Betroffenen unwahrscheinlich ist. Die Staatsministerien regeln für ihren Geschäftsbereich und für die unter ihrer Aufsicht stehenden juristischen Personen des öffentlichen Rechts durch Rechtsverordnung, bei welchen öffentlichen Stellen die Voraussetzungen des Satzes 1 erfüllt sind.

Desweiteren bestimmt Art. 25 Abs. 2 Satz 1 BayDSG, dass der **behördliche Datenschutzbeauftragte ein eigener Beschäftigter** sein muss – die Bestellung ei-

nes Externen scheidet danach aus. **Ein Externer kann nur dann behördlicher Datenschutzbeauftragter einer öffentlichen Stelle sein, wenn ein Bediensteter aus einer öffentlichen Stelle für mehrere öffentliche Stellen gemeinsam** zum behördlichen Datenschutzbeauftragten bestellt wurde – dann ist dieser aus Sicht der anderen öffentlichen Stellen ein externer Beschäftigter (Art. 25 Abs. 2 Satz 2 BayDSG).

Den an mich herangetragenen Fragestellungen und Absichten lag jedoch keine der o.g. Bestimmungen zugrunde, sondern vielmehr, ein **Unternehmen oder einen freiberuflich Tätigen** mit der Aufgabe des behördlichen Datenschutzbeauftragten zu betrauen – also einen im wahrsten Sinne des Wortes Externen zum behördlichen Datenschutzbeauftragten zu bestellen. Dies ist wie oben ausgeführt **nach der bestehenden Rechtslage jedoch nicht zulässig.**

Auch wenn öffentliche Stellen keinen Externen (im klassischen Sinn) zum behördlichen Datenschutzbeauftragten berufen dürfen, so ist ihnen aber gleichwohl unbenommen, mit einem Externen einen Beratungsvertrag bezüglich des Datenschutzes abschließen.

Sollte eine entsprechende Änderung im BayDSG angestrebt werden, so würde ich zu dieser erhebliche Bedenken geltend machen; denn im Rahmen seiner Aufgabenerfüllung als behördlicher Datenschutzbeauftragter würde der Externe/private Dritte ggf. Kenntnis von personenbezogenen Daten von Bürgerinnen und Bürgern erhalten (müssen), die diese nicht immer freiwillig, sondern u.U. nur aufgrund gesetzlicher Vorschriften und Normen öffentlichen Stellen gegenüber offenbart und diesen überlassen haben. Dies würde m.E. die besondere Schutzverpflichtung der öffentlichen Stellen hinsichtlich dieser Daten konterkarieren.

Weitere Informationen zum Thema „Der behördliche Datenschutzbeauftragte“ enthält die gleichnamige Orientierungshilfe, abrufbar auf meiner Homepage www.datenschutz-bayern.de im Bereich „Veröffentlichungen / Broschüren / Orientierungshilfen“.

2.2.8 Einsatz von Praktikanten

Gemäß Art. 17 Abs. 1 Nr. 1 Bayerisches Datenschutzgesetz (BayDSG) darf jeder Mitarbeiter einer Behörde oder Kommune nur auf die personenbezogenen Daten zugreifen, die er zur Erfüllung seiner Aufgaben benötigt.

Diese strenge gesetzliche Verpflichtung gilt natürlich erst recht für Praktikanten. Bei dieser Personengruppe ist außerdem die Bestimmung aus Art. 17 Abs. 3 Satz 2 BayDSG zu beachten, nach der die Verarbeitung und die Nutzung der bei einer öffentlichen Stelle gespeicherten personenbezogenen Daten zu Ausbildungszwecken nur zulässig sind, soweit nicht offensichtlich überwiegende schutzwürdige Interessen der Betroffenen – also der Personen, deren Daten gespeichert sind – entgegenstehen.

Offensichtlich überwiegende schutzwürdige Interessen stehen insbesondere dann der Verwendung der personenbezogenen Daten zu Ausbildungszwecken entgegen, wenn die Betroffenen dem Auszubildenden bekannt sind und deshalb möglicherweise ein über das Ausbildungsinteresse hinausgehendes Interesse des Auszubildenden an der Kenntnis der personenbezogenen Daten der Betroffenen besteht.

In einer kleinen Gemeinde ist typischerweise davon auszugehen, dass jeder Praktikant zumindest einen Großteil der Gemeindebürger und -bürgerinnen persönlich kennt. Da in der Gemeinde aber viele schutzwürdige Daten der Gemeindebürger – und bürgerinnen verarbeitet und genutzt werden, besteht hier das Risiko der zweckwidrigen Verwendung durch einen Praktikanten.

In diesen Fällen stehen daher aus datenschutzrechtlicher Sicht die offensichtlich überwiegenden schutzwürdigen Interessen der Bürgerinnen und Bürger, deren personenbezogene Daten bei der öffentlichen Stelle gespeichert sind und verarbeitet werden, dem Einsatz von Praktikanten entgegen.

2.3 Fortentwicklungen aus vorangegangenen Tätigkeitsberichten

2.3.1 Zentralisierung des Active Directory Betriebs

Da die Gefahr noch nicht beseitigt ist, dass auch möglicherweise schwerwiegende Probleme beim Betrieb der Active Directory (AD) Umgebung im Freistaat Bayern entstehen können, wurde von den IuK-Leitern der Staatskanzlei und der Ressorts (CIO-Vorrunde) beschlossen, eine konzeptionelle Grundlage für die Neustrukturierung des AD zu erarbeiten (siehe hierzu 24. Tätigkeitsbericht, Nr. 2.1.3). Der erste Schritt dieses Vorhabens ist dabei die Zentralisierung der Betriebsverantwortung für die einzelnen Domänen des AD in den beiden Rechenzentren des Freistaats.

Wie bereits in meinem 24. Tätigkeitsbericht geschildert, besteht aus datenschutzrechtlicher Sicht die einzige Möglichkeit, die Administration und den IT-Betrieb außerhalb des eigenen Bereichs zu geben, in der sogenannten Datenverarbeitung im Auftrag gemäß Art. 6 BayDSG. Nach Art. 6 Abs. 2 Satz 2 BayDSG ist der Auftrag schriftlich zu erteilen, wobei Datenerhebung, -verarbeitung oder -nutzung, die technischen und organisatorischen Maßnahmen und etwaige Unterauftragsverhältnisse festzulegen sind.

Bis zum Ende dieses Berichtszeitraums wurden meines Wissens noch keine derartigen Verträge geschlossen, so dass mir eine Prüfung bis jetzt nicht möglich war. Ich wurde aber in die Erarbeitung einer Mustervereinbarung eingebunden, die als Grundlage für einen Vertragsschluss dienen kann (siehe Nr. 2.1.6).

In naher Zukunft werde ich das Vorliegen und die Inhalte der Vereinbarungen zwischen den Rechenzentren und den entsprechenden Auftrag gebenden Dienststellen prüfen. Eine Auftragsdatenverarbeitung ohne schriftliche vertragliche Regelung werde ich als unzulässig bewerten.

2.3.2 Google Analytics – Benutzerstatistiken von Internetauftritten

Bereits im September 2010 habe ich die bayerischen Behörden aufgefordert, auf den Einsatz von Google Analytics gänzlich zu verzichten oder zumindest einen Zusatzcode zu verwenden, der die Identität von Webnutzern verschleiert (siehe hierzu 24. Tätigkeitsbericht, Nr. 2.1.6).

Im Laufe des Jahres 2011 prüfte ich daraufhin über 2500 Internetauftritte von Ministerien, Fachbehörden, Landratsämtern, Städten und Gemeinden in Bayern hinsichtlich der dortigen Verwendung von Google Analytics. Dabei stellte ich bei 222 überprüften Behörden – ganz überwiegend Kommunen – einen unzulässigen Einsatz von Google Analytics zur Analyse der Nutzerzugriffe auf ihre Webseiten fest. Nur zwei Behörden hatten dabei Anonymisierungsmechanismen verwandt.

Der daraufhin folgenden, direkten Aufforderung an die betroffenen 222 Behörden, unverzüglich auf den Einsatz IP-adressenbezogener Auswertungen des Verhaltens von Internetnutzern zu verzichten, folgten 208 öffentliche Stellen

Die Betreiber der 14 Webseiten, die meiner Aufforderung nicht nachkamen, habe ich förmlich beanstandet, wonach auch diese von einem weiteren unzulässigen Einsatz absahen.

Im Jahr 2012 führte ich mehrere Nachprüfungen durch, die immer wieder einigen neu hinzugekommenen, unzulässigen Gebrauch von Google Analytics bei bayerischen Behörden aufdeckten und in letzter Konsequenz zwei weitere Beanstandungen ergaben.

Noch nie zuvor hat der Bayerische Landesbeauftragte für den Datenschutz derartig viele öffentliche Stellen gleichzeitig geprüft. Auch die Anzahl der Beanstandungen und Nachprüfungen lag weit über dem bisher Üblichen. Das Datenschutzniveau auf mehreren hundert Webseiten sowie das Datenschutzbewusstsein bei vielen öffentlichen Stellen wurde dadurch deutlich verbessert. Bei meiner letzten Überprüfung aller über 2500 Webseiten im Jahre 2012 konnte ich keinen einzigen unzulässigen Einsatz mehr feststellen.

An der aus dem Telemediengesetz (TMG) resultierenden rechtlichen Unzulässigkeit, Google Analytics ohne zusätzliche Maßnahmen einzusetzen, hat sich nach wie vor nichts geändert. Ein Einsatz kann jedoch zulässig sein, wenn

– die Google Analytics Funktion _anonymizeIP zur automatischen Verkürzung der IPv4-Adressen der Webseitenbesucher bei der Datenspeicherung bei Google verwendet wird,

– die Nutzer der Webseite in deutlicher Form etwa in der Datenschutzerklärung auf ihr Recht hingewiesen werden, einer Auswertung ihrer Daten zu widersprechen und

– derartige Widersprüche wirksam umgesetzt werden können, etwa durch einen Verweis in der Datenschutzerklärung auf geeignete Browser-Plugins.

Google bietet darüber hinaus für die Verwendung der anonymizeIP einen Vertrag zur Auftragsdatenverarbeitung an, der den ordnungsgemäßen Umgang mit den Daten der Webseitenbesucher regelt.

2.3.3 Cloud Computing

Auch wenn die Verwendung von Cloud Computing im öffentlichen Bereich noch keine große Verbreitung gefunden hat, so erreichen mich doch vereinzelte An-

fragen, ob bayerische öffentliche Stellen Cloud Dienste einsetzen können und unter welchen Voraussetzungen dies möglich sein kann (siehe hierzu 24. Tätigkeitsbericht, Nr. 2.1.5).

Entschließung der 82. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 28./29.09.2011
Datenschutzkonforme Gestaltung und Nutzung von Cloud-Computing

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder fordert Cloud-Anbieter auf, ihre Dienstleistungen datenschutzkonform zu gestalten. Cloud-Anwender hingegen dürfen Cloud-Services nur dann in Anspruch nehmen, wenn sie in der Lage sind, ihre Pflichten als verantwortliche Stelle in vollem Umfang wahrzunehmen und die Umsetzung der Datenschutz- und Informationssicherheitsanforderungen geprüft haben.

Dies betrifft neben den Anforderungen an Vertraulichkeit, Integrität und Verfügbarkeit der Daten insbesondere die in diesem Umfeld schwierig umzusetzenden Anforderungen an Kontrollierbarkeit, Transparenz und Beeinflussbarkeit der Datenverarbeitung. Cloud-Computing darf nicht dazu führen, dass Daten verarbeitende Stellen, allen voran ihre Leitung, nicht mehr in der Lage sind, die Verantwortung für die eigene Datenverarbeitung zu tragen.

Zu verlangen sind also mindestens

- *offene, transparente und detaillierte Informationen der Cloud-Anbieter über die technischen, organisatorischen und rechtlichen Rahmenbedingungen der von ihnen angebotenen Dienstleistungen einschließlich der Sicherheitskonzeption, damit die Cloud-Anwender einerseits entscheiden können, ob Cloud-Computing überhaupt in Frage kommt und andererseits Aussagen haben, um zwischen den Cloud-Anbietern wählen zu können,*
- *transparente, detaillierte und eindeutige vertragliche Regelungen der Cloud-gestützten Datenverarbeitung, insbesondere zum Ort der Datenverarbeitung und zur Benachrichtigung über eventuelle Ortswechsel, zur Portabilität und zur Interoperabilität,*
- *die Umsetzung der abgestimmten Sicherheits- und Datenschutzmaßnahmen auf Seiten von Cloud-Anbieter und Cloud-Anwender und*
- *aktuelle und aussagekräftige Nachweise (bspw. Zertifikate anerkannter und unabhängiger Prüfungsorganisationen) über die Infrastruktur, die bei der Auftragserfüllung in Anspruch genommen wird, die insbesondere die Informationssicherheit, die Portabilität und die Interoperabilität betreffen.*

Die Datenschutzbeauftragten des Bundes und der Länder bieten ihre Unterstützung bei der Entwicklung und bei der Nutzung von Cloud-Computing-Diensten an. Details zur datenschutzgerechten Ausgestaltung dieser Dienste sind einer Orientierungshilfe der Arbeitskreise „Technik“ und „Medien“ zu entnehmen, die die Datenschutzkonferenz zustimmend zur Kenntnis genommen hat.

Gerade bezüglich der transparenten, detaillierten und eindeutigen vertraglichen Regelungen zum Ort der Datenverarbeitung gibt es bei vielen Anbietern nach wie vor meist keine den gesetzlichen Vorgaben für bayerische öffentliche Stellen genügenden Angebote.

Im Grundsatz hat sich unter anderem deswegen gegenüber meiner bisherigen Empfehlung für öffentliche Stellen keine Veränderung ergeben, bei der Inan-

spruchnahme von Cloud Diensten äußerste Zurückhaltung walten zu lassen. Auf die europäischen Entwicklungen bin ich weiter oben bereits eingegangen (siehe Nr. 1.2).

2.3.4 Sparen an der falschen Stelle

In meinem letzten Tätigkeitsbericht habe ich darauf hingewiesen, dass monetäre Einsparungen bei der Briefzustellung unerwünschte datenschutzrechtliche Auswirkungen haben können (siehe hierzu 24. Tätigkeitsbericht, Nr. 2.2.2).

Ich hatte in dem erwähnten Beitrag darüber berichtet, dass sich verschiedene Petenten an meine Geschäftstelle gewandt und sich darüber beschwert hatten, dass der Datenschutz bei der Zustellung von Schreiben aus den Bereichen des Landesamtes für Finanzen und des Landesamtes für Steuern nicht gewährleistet sei. Aufgrund dieser Beschwerden hatten die beiden Landesämter den Vertrag mit dem damaligen Postzusteller gekündigt und einen neuen damit beauftragt.

Seitdem wurden mir keine neuen Beschwerden über die ungeeignete Zusendung von personenbezogenen Daten bekannt, sodass sich zumindest bisher meine Hoffnung erfüllt hat, dass nunmehr der Datenschutz beim Briefpostversand der beiden Landesämter gewährleistet ist. Manchmal ist es eben doch besser, nicht den billigsten, sondern den zuverlässigsten Dienstleister zu beauftragen.

2.3.5 Datenschutzrechtliche Vorgaben für den Internetauftritt staatlicher Behörden

Das Bayerische Staatsministerium des Innern hat ein – mit mir abgestimmtes – Muster für das Impressum und die Datenschutzerklärung der Internetseiten staatlicher Behörden erarbeitet.

Mit dem Muster soll den Verantwortlichen die rechtssichere Formulierung dieser Pflichtbestandteile des Internetauftritts erleichtert und eine möglichst einheitliche Erfüllung gesetzlicher Anforderungen erreicht werden.

Dieses – zum Zeitpunkt des Redaktionsschlusses für diesen Tätigkeitsbericht leider noch nicht veröffentlichte – Muster wurde sowohl den Obersten Dienstbehörden im staatlichen Bereich als auch dem Bayerischen Landkreistag, dem Bayerischen Städtetag und dem Bayerischen Gemeindetag zur Verfügung gestellt. Die kommunalen Spitzenverbände werden gebeten, das Muster den Kommunen in geeigneter Form zur Verfügung zu stellen.

2.3.6 Bereitstellung von Zugangsmöglichkeiten zu medizinischen Netzen, KV-Ident, KV-Safenet, Zuweiserportale

Sowohl die Kassenärztlichen Vereinigungen als auch medizinische Einrichtungen wie Krankenhäuser bieten niedergelassenen Ärzten verstärkt Möglichkeiten zur elektronischen Übermittlung von Daten an. In manchen Bereichen besteht sogar die Pflicht, Daten wie z.B. Abrechnungsdaten ausschließlich elektronisch einzureichen. Aus diesem Grund hat die 81. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 16./07.03.2011 die Entschließung „Mindestan-

forderungen an den technischen Datenschutz bei der Anbindung von Praxis-EDV-Systemen an medizinische Netze“ gefasst. Die in dieser Entschließung festgelegten Maßnahmen gelten aus meiner Sicht für alle Arten von Vernetzungsprojekten, bei denen eine öffentliche Stelle niedergelassenen Ärzten Möglichkeiten zur elektronischen Anbindung und Übermittlung personenbezogener medizinischer Daten bietet, also z.B. auch Zuweiserportale, Ärztenetze, einrichtungsübergreifende Fall- und Patientenakten etc.

Entschließung der 81. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 16./17.03.2011
Mindestanforderungen an den technischen Datenschutz bei der Anbindung von Praxis-EDV-Systemen an medizinische Netze

Niedergelassene Ärztinnen und Ärzte sowie andere Angehörige von Heilberufen übermitteln vielfach medizinische Daten an andere Stellen mithilfe von Netzwerken. Dies dient Abrechnungs-, Behandlungs- und Dokumentationszwecken. Seit dem 01.01.2011 müssen beispielsweise an der vertragsärztlichen Versorgung teilnehmende Ärzte Abrechnungsdaten leitungsgebunden an die jeweilige Kassenärztliche Vereinigung übermitteln (§ 295 Abs. 4 SGB V in Verbindung mit den Richtlinien der Kassenärztlichen Bundesvereinigung für den Einsatz von IT-Systemen in der Arztpraxis zum Zweck der Abrechnung; siehe http://www.kbv.de/rechtsquellen/24631.html).

An medizinische Netze sind hohe Anforderungen hinsichtlich der Vertraulichkeit und Integrität zu stellen, denn sowohl in den Netzen selbst als auch auf den angeschlossenen Praxissystemen werden Daten verarbeitet, die der ärztlichen Schweigepflicht (§ 203 StGB) unterliegen. Bei der Anbindung von Praxis-EDV-Systemen an medizinische Netze ist daher die „Technische Anlage zu den Empfehlungen zur ärztlichen Schweigepflicht, Datenschutz und Datenverarbeitung in der Arztpraxis“ der Bundesärztekammer und der Kassenärztlichen Bundesvereinigung (siehe Deutsches Ärzteblatt, Jg. 105, Heft 19 vom 09.05.2008) zu beachten.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder fordert, dabei insbesondere folgende Mindestanforderungen zu stellen:

1. *Die Kommunikation im Netz muss verschlüsselt ablaufen. Hierzu sind dem Stand der Technik entsprechende Verfahren zu nutzen.*
2. *Ein unbefugter Zugriff auf die internen Netze der Praxis oder Einrichtung muss ausgeschlossen sein.*
3. *Die Auswirkungen von Fehlkonfigurationen im internen Netz müssen wirksam begrenzt werden.*
4. *Die Endpunkte der Kommunikation müssen sich gegenseitig durch dem Stand der Technik entsprechende Verfahren authentisieren.*
5. *Die Wartung der zum Netzzugang eingesetzten Hard- und Software-Komponenten muss kontrollierbar sein, indem die Wartung durch eine aktive Handlung freizuschalten ist und alle Wartungsaktivitäten protokolliert werden.*
6. *Zum Netzzugang sind zertifizierte Hard- und Software-Komponenten einzusetzen.*
7. *Grundstandards – wie beispielsweise die Revisionssicherheit – sind einzuhalten.*

Für die verwendeten Verschlüsselungs- und Authentisierungskomponenten sollten Hardware-Lösungen genutzt werden, da bei Software ein erhöhtes Manipulationsrisiko besteht.

Software-Lösungen kommen allenfalls in Ausnahmefällen in Betracht, wenn die zur Kommunikation mit anderen Stellen genutzten Rechner und Komponenten nicht mit dem internen Netz der Praxis verbunden sind. Zusätzlich ist sicherzustellen, dass

entweder

a) nur solche Daten gesendet werden, die bereits innerhalb des Praxisnetzes verschlüsselt und integritätsgeschützt wurden

oder

b)

- *eine Zwei-Faktor-Authentifikation des Berechtigten stattfindet,*
- *mit der zum Zugang verwendeten Hard- und Software ausschließlich Zu gang zu medizinischen Netzen besteht sowie*
- *die KBV-Richtlinien zur Online-Anbindung von Praxis-EDV-Systemen an das KV-SafeNet eingehalten werden.*

2.3.7 Projekt elektronische Fallakte (eFA) beim Städtischen Klinikum München GmbH

Das Projekt zum Einsatz der eFA für die Versorgung von Darmkrebspatienten ist nach wie vor mit einem ausgewählten Benutzerkreis aktiv. Zudem gibt es Planungen beim Städtischen Klinikum München GmbH, die eFA auch für andere Bereiche einzusetzen. Auch für diese Projekte gelten aus Datenschutzsicht die bereits früher aufgestellten Anforderungen (siehe hierzu 24. Tätigkeitsbericht, Nr. 2.2.10).

2.3.8 TIZIAN

Auch in diesem Berichtszeitraum hat es aus technisch-organisatorischer Sicht Fortschritte beim Verfahren TIZIAN gegeben. So wurden die Arbeiten am Löschkonzept sowie am Protokollierungskonzept fortgeführt. Insbesondere zu den Protokollierungs- und Auswertungsmöglichkeiten in TIZIAN wurde eine technisch-organisatorische Prüfung durchgeführt. Die Protokollierung in TIZIAN dient dazu, unerlaubte Benutzerzugriffe feststellen zu können. Um dies zu ermöglichen, sind sowohl eine einzelfallbezogene Auswertung wie auch eine regelmäßige Auswertung in Stichproben nötig. Für die Festlegung eines Stichprobenkonzepts müssen folgende Schritte ausgeführt werden:

Definition unbefugter bzw. unerwünschter Zugriffsmuster

Für die Auswertung muss festgelegt werden, welche Zugriffe oder Zugriffsmuster auf eine unbefugte Nutzung hindeuten können. Dabei kann sich die Auswertung sowohl auf quantitative als auch auf qualitative Kriterien beziehen.

Eine quantitative Auswertung betrachtet mengenmäßige Auffälligkeiten. Hierbei ist zunächst zu erfassen, was das durchschnittliche Aufkommen bei bestimmten Zugriffsarten ist. Daraus können für das Stichprobenkonzept Schwellenwerte

festgelegt werden, bei deren Überschreitung ein weiteres Nachfassen erforderlich ist.

Auch in qualitativer Hinsicht ist eine Definition unerwünschter Zugriffsmuster nötig. So kann z.B. das „Durchbrowsern“ (nacheinander immer die gleiche Abfrage durch einen Benutzer) auf eine unzulässige Verhaltens- und Leistungskontrolle hindeuten. Derartige Zugriffsmuster müssen für das Stichprobenkonzept festgelegt werden.

Auch kann festgelegt werden, welche Daten besonderes schützenswert sind, so dass Zugriffe hierauf besonders kritisch zu sehen sind.

Festlegung der Stichproben und Auswertungen

Auf Basis der Definition der unerwünschten Zugriffsmuster können nunmehr Vorgehensweisen für die Auswertung und eventuell benötigte Auswertungsmöglichkeiten festgelegt werden.

Eine Auswertung in Stichproben sollte dabei nicht standardmäßig alle Zugriffe umfassen, sondern immer nur eine Teilauswahl, z.B. 10% der Zugriffe, jeden zweiten Samstag, Zugriffsanzahlen in bestimmter Höhe, besonders sensible Betriebe / Themen.

Datenschutzgerechte Protokollauswertung

Auch bei der Auswertung der Protokolldaten sollte ein Zugriff auf personenbezogene Daten (also die Benutzerkennung) nach Möglichkeit nur erfolgen, wenn dies erforderlich ist.

So könnte beispielsweise ein mehrstufiges Verfahren gewählt werden: Für quantitative Auswertungen wird im ersten Schritt nur die Zugriffsanzahl angezeigt. Erst wenn es dort Auffälligkeiten gibt, wird Einsicht in die personenbezogene Protokollierung genommen. Ebenso sollte bei qualitativen Auswertungen zunächst eine anonymisierte / pseudonymisierte Ansicht gewählt werden, bei der die Benutzerkennungen ausgeblendet sind. Erst bei Auffälligkeiten sollte ein Zugriff auf die Benutzerkennung möglich sein.

Festlegung der beteiligten Personen sowie Auswertungszeitpunkt

Analog zu den Regelungen zur anlassbezogenen Protokollauswertung muss unter Wahrung der Beteiligungsrechte von Beschäftigtenvertretungen festgelegt werden, welche Personen an der regelmäßigen Auswertung in Stichproben beteiligt sind und wann diese stattfindet. Auch das weitere Vorgehen bei Auffälligkeiten muss geregelt werden. Die Mitarbeiter müssen über das Vorgehen sowie den Zweck und Inhalt der Auswertungen informiert werden.

3 Polizei

In diesem Berichtszeitraum habe ich u.a. wieder mehrere Polizeidienstellen geprüft und es ist mir bei einigen Themen gelungen, datenschutzrechtliche Verbesserungen zu erreichen. Vielen Bürgern konnte ich im Zusammenhang mit Fragen zur Zulässigkeit polizeilicher Speicherungen mit Rat und Tat zur Seite stehen. Aber auch regelmäßige Vorträge bei Aus- und Fortbildungsveranstaltungen der Polizei gehörten zu meiner Tätigkeit. Die nachfolgenden Beiträge, die eine Auswahl meiner Feststellungen sind, zeigen, wie vielfältig die datenschutzrechtlichen Fragestellungen sind, die im Polizeibereich auftauchen.

3.1 Vorratsdatenspeicherung

Bereits in meinem letzten Tätigkeitsbericht habe ich unter „Ausgestaltung der Vorratsdatenspeicherung verfassungswidrig“ über das Urteil des Bundesverfassungsgerichts vom 02.03.2010 zur Vorratsdatenspeicherung berichtet (siehe hierzu 24. Tätigkeitsbericht, Nr. 3.3). Das Gericht hat darin die im Jahr 2008 in Kraft getretenen gesetzlichen Regelungen zur Vorratsdatenspeicherung für verfassungswidrig erklärt. Die EU-Kommission hat zwischenzeitlich Klage gegen die Bundesrepublik Deutschland vor dem Europäischen Gerichtshof erhoben, weil diese die Richtlinie zur Vorratsdatenspeicherung bisher nicht in wirksamer Weise umgesetzt habe.

Nach wie vor wird die Diskussion in dieser Sache sehr kontrovers geführt. In diesem Zusammenhang habe ich als Vorsitzender der Konferenz der Datenschutzbeauftragten des Bundes und der Länder im Jahr 2011 anlässlich des 6. Europäischen Datenschutztages eine zentrale Veranstaltung mit verschiedenen Diskussionsteilnehmern zum Thema „Vorratsdatenspeicherung“ ausgerichtet, die auf breites Interesse gestoßen ist. Ich hoffe, mit dieser Veranstaltung einen förderlichen Beitrag zur Diskussion dieses Thema geleistet zu haben.

Befassen muss sich der Europäische Gerichtshof nun auch mit einem Vorabentscheidungsverfahren, das von einem irischen Gericht angestoßen wurde. Anders als beim Verfahren gegen die Bundesrepublik Deutschland, in dem es inhaltlich nur um die nicht rechtzeitige Umsetzung der Richtlinie geht, kann im Rahmen dieser Klage möglicherweise geklärt werden, ob die Richtlinie inhaltlich überhaupt mit EU-Recht, insbesondere mit den Grundrechten der EU-Grundrechtecharta und der EMRK vereinbar ist.

Ich meine nach wie vor, dass die Befürworter einer anlasslosen Vorratsdatenspeicherung konkret belegen müssen, bei welchen Straftaten welche Daten wie lange unbedingt gespeichert werden müssen, um das legitime Ziel einer effektiven Strafverfolgung sicherzustellen. Auch ist zu berücksichtigen, dass es laut Bundesverfassungsgericht bei der Zulässigkeit einer Datenspeicherung auf Vorrat nicht zuletzt auch auf eine Gesamtbilanz der über den einzelnen Bürger anlasslos gespeicherten Daten ankommt. Beispielsweise angesichts der Pläne, künftig auch Fluggastdaten anlasslos zu speichern, drängt sich – ungeachtet eines Überblicks der Kommission über das Informationsmanagement im Bereich Freiheit, Sicherheit und Recht vom 20.07.2010 (KOM/2010/0385 endg.) – die Frage auf, ob es auf europäischer Ebene ein schlüssiges Gesamtkonzept zur Speicherung von Daten auf Vorrat gibt. Wenn nicht, wovon momentan auszuge-

hen ist, wäre ein solches Konzept angesichts der Rechtsprechung des Bundesverfassungsgerichts dringend notwendig. Es bleibt zu hoffen, dass sich der Europäische Gerichtshof mit diesen Aspekten auseinandersetzt.

3.2 Quellen-Telekommunikationsüberwachung

Mit dem Thema „Quellen-Telekommunikationsüberwachung" habe ich mich bereits in meinem letzten Tätigkeitsbericht auseinandergesetzt und darauf hingewiesen, dass solche Maßnahmen nicht auf die Regelungen zur herkömmlichen Telekommunikationsüberwachung gestützt werden können (siehe hierzu 24. Tätigkeitsbericht, Nr. 3.7). Im Berichtszeitraum habe ich eine umfassende Prüfung repressiver Quellen-Telekommunikationsmaßnahmen bayerischer Strafverfolgungsbehörden durchgeführt (siehe Nr. 5.3.1). Auch wenn ich im Rahmen dieser Prüfung keine entsprechenden Maßnahmen zu Zwecken der Gefahrenabwehr festgestellt habe, gelten die Wertungen meines unten näher dargestellten Prüfberichts vergleichbar auch für den Bereich präventivpolizeilicher Quellen-Telekommunikationsüberwachungen.

3.3 Datenschutz und Versammlungsrecht

3.3.1 Verfassungsbeschwerde gegen das Bayerische Versammlungsgesetz

In meinem letzten Tätigkeitsbericht habe ich über die umfangreichen Änderungen des Bayerischen Versammlungsgesetzes (BayVersG) berichtet, die einige wesentliche datenschutzrechtliche Verbesserungen enthalten (siehe hierzu 24. Tätigkeitsbericht, Nr. 3.2). Sie waren eine Reaktion des Gesetzgebers auf die nach einer Verfassungsbeschwerde ergangene einstweilige Anordnung des Bundesverfassungsgerichts zum Bayerischen Versammlungsgesetz vom 17.02.2009. In dieser Anordnung hat das Gericht insbesondere die Befugnis zur Anfertigung von Übersichtsaufzeichnungen und Übersichtsaufnahmen beschränkt.

Zum Zeitpunkt meines letzten Tätigkeitsberichts war noch nicht abzusehen, ob das Bundesverfassungsgericht in seiner damals noch ausstehenden endgültigen Entscheidung noch einen weiteren Änderungsbedarf für erforderlich halten würde. Dem mittlerweile ergangenen Beschluss des Bundesverfassungsgerichts vom 21.03.2012 (Az.: 1 BvR 2492/12) ist zu entnehmen, dass dies nicht der Fall ist. Die Pressemitteilung Nr. 29/12 des Bundesverfassungsgerichts vom 08.05.2012, die auf der Homepage des Gerichts eingesehen werden kann, informiert ausführlich über die Erwägungen, die dieser Entscheidung zugrunde liegen.

Meine Ausführungen im letzten Tätigkeitsbericht zu den Änderungen des Bayerischen Versammlungsgesetzes (siehe hierzu 24. Tätigkeitsbericht, Nr. 3.2) bedürfen daher keiner Ergänzung.

3.3.2 Übersichtsaufnahmen von Versammlungen zum Zwecke der polizeilichen Aus- und Fortbildung

Über die Änderungen des Bayerischen Versammlungsgesetzes (BayVersG), die zum 01.06.2010 in Kraft getreten sind, habe ich bereits ausführlich in meinem letzten Tätigkeitsbericht berichtet (siehe hierzu 24. Tätigkeitsbericht, Nr. 3.2).

Sofern die Polizei Übersichtsaufnahmen von Versammlungen zu Aus- und Fortbildungszwecken verwenden will, ist dies nun in Art. 9 Absatz 4 des BayVersG so geregelt, dass dann eine eigene Fassung der Aufnahmen hergestellt werden muss, die eine Identifizierung der darauf abgebildeten Personen unumkehrbar ausschließt. Die Aufnahmen dürfen nicht für andere Zwecke genutzt werden. Die Herstellung dieser eigenen Fassung ist nur so lange zulässig, als die Originalaufzeichnung nicht nach Art. 9 Absatz 3 BayVersG zu löschen ist. Außerdem wurden in Art. 9 Absatz 5 BayVersG erstmals Dokumentationspflichten bei der Herstellung solcher Aufnahmen eingeführt.

Art. 9 BayVersG Bild- und Tonaufnahmen oder -aufzeichnungen
(1) [1]Die Polizei darf bei oder im Zusammenhang mit Versammlungen Bild- und Tonaufnahmen oder -aufzeichnungen von Teilnehmern nur offen und nur dann anfertigen, wenn tatsächliche Anhaltspunkte die Annahme rechtfertigen, dass von ihnen erhebliche Gefahren für die öffentliche Sicherheit oder Ordnung ausgehen. [2]Die Maßnahmen dürfen auch durchgeführt werden, wenn Dritte unvermeidbar betroffen werden.
(2) [1]Die Polizei darf Übersichtsaufnahmen von Versammlungen unter freiem Himmel und ihrem Umfeld zur Lenkung und Leitung des Polizeieinsatzes nur offen und nur dann anfertigen, wenn dies wegen der Größe oder Unübersichtlichkeit der Versammlung im Einzelfall erforderlich ist. [2]Übersichtsaufnahmen dürfen aufgezeichnet werden, soweit Tatsachen die Annahme rechtfertigen, dass von Versammlungen, von Teilen hiervon oder ihrem Umfeld erhebliche Gefahren für die öffentliche Sicherheit oder Ordnung ausgehen. [3]Die Identifizierung einer auf den Übersichtsaufnahmen oder -aufzeichnungen abgebildeten Person ist nur zulässig, soweit die Voraussetzungen nach Abs. 1 vorliegen.
(3) [1]Die nach Abs. 1 oder 2 angefertigten Bild-, Ton- und Übersichtsaufzeichnungen sind nach Beendigung der Versammlung unverzüglich auszuwerten und spätestens innerhalb von zwei Monaten zu löschen, soweit sie nicht benötigt werden

1. *zur Verfolgung von Straftaten bei oder im Zusammenhang mit der Versammlung oder*
2. *im Einzelfall zur Gefahrenabwehr, weil die betroffene Person verdächtig ist, Straftaten bei oder im Zusammenhang mit der Versammlung vorbereitet oder begangen zu haben, und deshalb zu besorgen ist, dass von dieser Person erhebliche Gefahren für künftige Versammlungen ausgehen.*

[2]Soweit die Identifizierung von Personen auf Bild-, Ton- und Übersichtsaufzeichnungen für Zwecke nach Satz 1 Nr. 2 nicht erforderlich ist, ist sie technisch unumkehrbar auszuschließen. [3]Bild-, Ton- und Übersichtsaufzeichnungen, die aus den in Satz 1 Nr. 2 genannten Gründen nicht gelöscht wurden, sind spätestens nach Ablauf von sechs Monaten seit ihrer Entstehung zu löschen, es sei denn, sie werden inzwischen zur Verfolgung von Straftaten nach Satz 1 Nr. 1 benötigt.
(4) [1]Soweit Übersichtsaufzeichnungen nach Abs. 2 Satz 2 zur polizeilichen Aus- und Fortbildung benötigt werden, ist hierzu eine eigene Fassung herzustellen, die eine Identifizierung der darauf abgebildeten Personen unumkehrbar ausschließt. [2]Sie darf nicht für andere Zwecke genutzt werden. [3]Die Herstellung einer eigenen

Fassung für Zwecke der polizeilichen Aus- und Fortbildung ist nur zulässig, solange die Aufzeichnung nicht nach Abs. 3 zu löschen ist.
(5) [1]Die Gründe für die Anfertigung von Bild-, Ton- und Übersichtsaufzeichnungen nach Abs. 1 und 2 und für ihre Verwendung nach Abs. 3 Satz 1 Nrn. 1 und 2 sind zu dokumentieren. [2]Werden von Übersichtsaufzeichnungen eigene Fassungen nach Abs. 4 Satz 1 hergestellt, sind die Notwendigkeit für die polizeiliche Aus- und Fortbildung, die Anzahl der hergestellten Fassungen sowie der Ort der Aufbewahrung zu dokumentieren.
(6) Die Befugnisse zur Erhebung personenbezogener Daten nach Maßgabe der Strafprozessordnung und des Gesetzes über Ordnungswidrigkeiten bleiben unberührt.

Meine Prüfung, ob diese neuen rechtlichen Vorgaben eingehalten werden, habe ich bei der Bayerischen Bereitschaftspolizei durchgeführt, da diese für die Aus- und Fortbildung der bayerischen Polizei federführend zuständig ist. Nach den Angaben der Bayerischen Bereitschaftspolizei sind die technischen Vorgaben des Art. 9 Absatz 4 des BayVersG nicht mit angemessenem Aufwand umzusetzen. Mit anderen Worten soll eine Technik zur einfachen Verpixelung von Personen (noch) nicht vorhanden sein. Demzufolge gebe es auch keine Filmaufnahmen oder Dokumentationen, die mir zur Prüfung zur Verfügung gestellt werden könnten.

Ich habe mit dem Präsidium der Bayerischen Bereitschaftspolizei vereinbart, dass ich informiert werde, falls zukünftig eigene Aufnahmen zu Schulungszwecken hergestellt werden sollten.

3.3.3 Datenerhebungen im Zusammenhang mit Versammlungen

Bereits in meinem letzten Tätigkeitsbericht habe ich mitgeteilt, auch in Zukunft verstärkt polizeiliche Datenerhebungen im Zusammenhang mit Versammlungen zu überprüfen (siehe hierzu 24. Tätigkeitsbericht, Nr. 3.4.3). Deshalb habe ich die Ankündigung von bayernweiten Demonstrationen anlässlich des sogenannten „Bildungsstreiks“ am 17.11.2011 zum Anlass genommen, bei drei Polizeipräsidien die polizeilichen Datenerhebungen im Rahmen dieser Demonstrationen zu prüfen. Die Versammlungen sollten sich inhaltlich an Schüler und Studenten richten und standen unter dem Motto „Widerstand bilden! Bildungsstreik in München, Europa und weltweit! Schülerinnen- und Studierendenproteste gegen die Bildungspolitik“. Die Demonstrationen im Bereich der drei verschiedenen Polizeipräsidien wiesen zwischen 100 und 1500 Teilnehmern auf und verliefen durchwegs friedlich und ohne Störungen.

Bei meiner Prüfung stellte ich fest, dass weder Speicherungen im bayerischen polizeilichen Speichersystem zur Erfassung von Personen- und Falldaten (IGVP) noch im bundesweiten Informationssystem der Polizei (INPOL) stattfanden. Lediglich in einem Fall hat mir die Polizei auf meine Anfrage hin mitgeteilt, dass Videoaufzeichnungen durchgeführt worden seien. Sie hat mir auf meine Nachfrage geantwortet, dass die Videoaufnahmen deshalb erfolgten, weil einzelne Teilnehmer die sich fortbewegende Versammlung durch eine Sitzblockade gestört haben sollen. Da mir versichert wurde, die Aufnahmen seien noch am gleichen Tag gelöscht worden, weil die Gruppe die Aktion schnell wieder abgebrochen habe, habe ich darauf verzichtet, in diesem konkreten Fall weitere Maßnahmen zu ergreifen. Gleichwohl habe ich das zuständige Polizeipräsidium darauf hingewiesen, dass sich das in Art. 8 BayVersG normierte Verbot, eine Versammlung zu

stören, zwar grundsätzlich an jedermann richtet, jedoch primär auf Nichtteilnehmer abzielt. Die Versammlungsteilnehmer können sich auf das Grundrecht der Versammlungsfreiheit nach Art. 8 GG berufen und sind somit als Grundrechtsträger grundsätzlich frei in der Wahl von Inhalt und Form einer Versammlung. Das bedeutet allerdings nicht, dass dieses Recht nicht seine Schranken dann findet, wenn andere Teilnehmer einer Versammlung wiederum in ihren Rechten gestört werden. Hier obliegt es primär dem Leiter der Versammlung, es zu beurteilen, ob es sich um eine ordnungsgemäße Durchführung der Versammlung oder um eine Störung der von ihm angemeldeten und verantworteten Versammlung handelt. All diese Erwägungen hat die Polizei bei der Frage zu berücksichtigen, ob wegen der Störung einer Versammlung gefilmt und aufgezeichnet werden darf oder nicht.

3.4 Einsatz von Videotechnik

Bewegt sich der Bürger heutzutage im öffentlichen Raum, kann er der Erfassung seiner Bilddaten in zunehmendem Maße nicht mehr entgehen. Oft sind ihm die Datenerhebungen in den ganz unterschiedlichen Lebenssituationen, in denen sie ihn treffen, auch überhaupt nicht bewusst. Die immer wieder kontrovers geführten öffentlichen Diskussionen zu diesem Thema belegen jedoch, dass die Sensibilität der Bürger gegenüber Videoüberwachungen zunehmend steigt. Auch soweit Bilddaten durch Sicherheitsbehörden erhoben werden, führte dies in der Vergangenheit immer wieder zu heftigen Reaktionen in der Öffentlichkeit.

Vor diesem Hintergrund habe ich mich in den zurückliegenden Jahren – neben der Aufklärung der Bürger – auch vehement für die korrekte Umsetzung der geltenden gesetzlichen Bestimmungen eingesetzt. Soweit es gerade in den Anfangsphasen der Videoüberwachung noch keine ausreichenden Richtlinien und Regelungen für den Einsatz der Videotechnik gab, habe ich zudem stetig versucht, im Dialog mit den Sicherheitsbehörden grundrechtsverträgliche und trotzdem praktikable Lösungen zu erarbeiten. Die nachfolgenden Beispiele sind insoweit auch als Fortschreibung früherer Beiträge aus meinen Tätigkeitsberichten zum Thema „Videoüberwachung“ zu sehen. Nebenbei zeigen die Beiträge auch, wo wir solchen Videoüberwachungen inzwischen im täglichen Leben überall begegnen können.

3.4.1 Öffentlich geförderte Forschungsprojekte zur Entdeckung abweichenden Verhaltens im öffentlichen Raum

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder betrachtet es kritisch, dass immer mehr Forschungsprojekte, die teils mit erheblichen öffentlichen Mitteln gefördert werden, zum Ziel haben, mit Hilfe moderner Technik menschliches Verhalten zu analysieren. Verhalten, das in sicherheitsrelevanter Weise normabweichend ist, soll mittels intelligenter Analysesysteme herausgefiltert und frühzeitig entdeckt werden. Hierbei kommen insbesondere neue Systeme zur Gesichts- und Verhaltenserkennung durch Videotechnik zum Einsatz.

Ein Beispiel für ein solches Forschungsvorhaben ist das Projekt „INDECT“. Dieses von der EU-Kommission geförderte Forschungsprojekt ist darauf ausgerichtet, ein „intelligentes Informationssystem zur Unterstützung von Beobachtung, Suche und Erkennen für die Sicherheit der Bürger in städtischen Umgebungen“

zu erforschen. Ziel ist es, ein abnormes Verhalten von Personen schnell zu erkennen und zu unterbinden. Letztlich kann damit auch die Polizeiarbeit in computergestützter Weise automatisiert werden.

Aus datenschutzrechtlicher Sicht müssen sich solche Forschungsprojekte auch mit den Auswirkungen der zu entwickelnden Technologien auf die Wahrnehmung der Freiheitsgrundrechte des Einzelnen beschäftigen. Zum Beispiel muss der Frage nachgegangen werden, welche gesellschaftlichen und rechtlichen Folgen es hat, wenn eine an sich legale Grundrechtsausübung (z.B. das ziellose Herumgehen an einem Flughafen) besonders von einem Überwachungssystem registriert und aufgezeichnet wird, weil es vom „normalen" Verhalten (im Beispielsfall zielgerichtetes Gehen zum Flugsteig) abweicht. Zum einen ergibt es keinen Sinn, öffentliche Forschungsgelder für eine Sicherheitstechnik auszugeben, deren späterer Einsatz unzulässig ist. Zum anderen ist aber auch zu befürchten, dass eine Technik, die einmal entwickelt wurde, erfahrungsgemäß auch die Begehrlichkeit weckt, sie einzusetzen, mit der Folge gravierender datenschutzrechtlicher Auswirkungen.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat am 21./22.03.2012 deshalb im Rahmen einer Entschließung an alle öffentlichen Stellen appelliert, bei solchen Projekten bereits im Stadium der Ausschreibung auch Fragen des Datenschutzes in ihre Entscheidung einzubeziehen. Gleichzeitig brachte sie damit ihre Besorgnis über möglicherweise grundrechtsbeeinträchtigende Überwachungsprojekte zum Ausdruck.

Entschließung der 83. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 21./22.03.2012
Öffentlich geförderte Forschungsprojekte zur Entdeckung abweichenden Verhaltens im öffentlichen Raum – nicht ohne Datenschutz

Mit erheblichen öffentlichen Mitteln werden derzeit zahlreiche Forschungsprojekte finanziert, die darauf abzielen, mit Hilfe modernster Technik – insbesondere der Videoüberwachung und dem Instrument der Mustererkennung – menschliche Verhaltensweisen zu analysieren. Dadurch sollen in öffentlich zugänglichen Bereichen mit hohem Sicherheitsbedarf „potentielle Gefährder" frühzeitig entdeckt werden. Zu derartigen Forschungsvorhaben zählen beispielsweise das Projekt „INDECT" (Intelligentes Informationssystem zur Überwachung, Suche und Detektion für die Sicherheit der Bürger in urbaner Umgebung), das von der Europäischen Union gefördert wird, oder in Deutschland Projekte wie ADIS (Automatisierte Detektion interventionsbedürftiger Situationen durch Klassifizierung visueller Muster), CamInSens (Verteilte, vernetzte Kamerasysteme zur in situ-Erkennung personeninduzierter Gefahrensituationen) oder die Gesichtserkennung in Fußballstadien.

Bei der Mustererkennung soll auf Basis von Video- oder anderen Aufzeichnungen, die mit Daten aus anderen Informationsquellen kombiniert werden, das Verhalten aller erfassten Personen computerunterstützt ausgewertet werden. Menschen, deren Verhalten als ungewöhnlich eingestuft wird, können so in Verdacht geraten, zukünftig eine Straftat zu begehen. Gerade bei der Mustererkennung von menschlichem Verhalten besteht daher die große Gefahr, dass die präventive Analyse einen Anpassungsdruck erzeugt, der die Persönlichkeitsrechte der betroffenen Bürgerinnen und Bürger verletzen würde.

Insoweit ist generell die Frage aufzuwerfen, inwieweit die grundrechtliche Zulässigkeit des Einsatzes der zu erforschenden Überwachungstechnik hinreichend untersucht wird. Bei Projekten, bei denen öffentliche Stellen des Bundes und der Länder beteiligt sind, sollten jeweils die zuständigen Datenschutzbehörden frühzeitig über das Projektvorhaben informiert und ihnen Gelegenheit zur Stellungnahme eingeräumt werden.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder appelliert an alle öffentlichen Stellen von Bund und Ländern, aber auch an die der Europäischen Union, die solche Projekte in Auftrag geben oder Fördermittel hierfür zur Verfügung stellen, bereits bei der Ausschreibung oder Prüfung der Förderfähigkeit derartiger Vorhaben rechtliche und technisch-organisatorische Fragen des Datenschutzes in ihre Entscheidung mit einzubeziehen. Nur so kann verhindert werden, dass Vorhaben öffentlich gefördert werden, die gegen Datenschutzvorschriften verstoßen.

Auf eine entsprechende Anfrage hin erfuhr ich, dass die Bayerische Polizei in beratender Funktion in ein vom Bundesministerium für Bildung und Forschung gefördertes Projekt zur Verhaltenserkennung eingebunden ist. Das Bayerische Staatsministerium des Innern teilte mir diesbezüglich mit, dass in diesem Projekt auch der Aspekt des Schutzes der Privatsphäre und des Datenschutzes mit untersucht werde.

Die Beteiligung bayerischer öffentlicher Stellen an derartigen Forschungsprojekten werde ich weiter genau beobachten.

3.4.2 Videoüberwachung öffentlicher Straßen und Plätze

Die Videoüberwachung öffentlicher Straßen und Plätze durch die Polizei ist ein Thema, mit dem ich mich bereits in den letzten Berichtszeiträumen regelmäßig beschäftigt habe. In meinem letztem Tätigkeitsbericht habe ich u.a. von meiner Diskussion mit dem Bayerischen Staatsministerium des Innern berichtet, mit welchen Maßnahmen eine Einsichtnahme in Privaträume umliegender Gebäude verhindert werden kann (siehe hierzu 24. Tätigkeitsbericht, Nr. 3.8.1). Zwischenzeitlich konnte ich die Zusicherung erreichen, das Staatsministerium des Innern werde in den Dienstanweisungen der Bayerischen Polizei für die polizeiliche Videoüberwachung einen eigenen Hinweis aufnehmen, dass Art. 13 GG (Unverletzlichkeit der Wohnung) zu beachten sei. Bei der zukünftigen Einrichtung von Videoüberwachungsanlagen würden neben Aspekten wie Standortwahl und Anbringung der Kameras besonders auch die technischen Möglichkeiten zur Begrenzung des Erfassungsbereichs der Kameras in die Prüfung einbezogen.

Ich werde die polizeiliche Videoüberwachung von öffentlichen Straßen und Plätzen weiterhin kritisch begleiten und hierbei vor allem auch darauf achten, dass eine Einsichtnahme in private Wohn- oder Geschäftsräume nicht möglich ist.

3.4.3 Polizeiliche Videobeobachtung und -aufzeichnung in Fußballstadien

Das Filmen und Fotografieren in und um Fußballstadien zählt seit Jahren zum Standardrepertoire polizeilicher Maßnahmen zur Einsatzbewältigung im Bundesligaspielbetrieb oder bei vergleichbaren großen Sportereignissen. Verantwortliche Organisationen wie der Deutsche Fußballbund (DFB) und die Deutsche

Fußballliga (DFL) haben sich daher in ihren Sicherheitsrichtlinien verpflichtet, der Polizei in allen Fußballstadien entsprechende Videoüberwachungsanlagen mit Zoom- und Aufzeichnungsfunktion bereitzustellen. Nachdem ich mich in meinen zurückliegenden Tätigkeitsberichten immer wieder mit den erforderlichen rechtlichen Voraussetzungen für polizeiliche Videobeobachtungen und Videoaufzeichnungen im öffentlichen Raum, an Kriminalitätsschwerpunkten oder bei Sport- und Großveranstaltungen befasst habe, habe ich im Berichtszeitraum die Ausgestaltung der Maßnahmen in Fußballstadien in den Blick genommen. Hierzu habe ich ein Bundesligastadion in Bayern ausgewählt, um dort die betreffenden Regelungen sowie die technische und organisatorische Umsetzung in datenschutzrechtlicher Hinsicht näher zu betrachten.

In dem zur Prüfung ausgewählten Stadion kann die Polizei auf eine Videoüberwachungsanlage mit mehreren getrennten Systemen und insgesamt 19 Kameras zugreifen, die entsprechend der o.g. DFB-Sicherheitsrichtlinien vom Veranstalter zur Verfügung gestellt wird. Die Bedienung und die Steuerung der Anlage sowie der Zugriff auf die unterschiedlichen Speichermedien obliegen dabei grundsätzlich nur der Polizei, die Wartung und die Instandhaltung aber dem Stadionbetreiber. Soweit die Polizei – wie im vorliegenden Fall – die Videotechnik im Stadion eigenverantwortlich nutzt, handelt sie in der Regel im Rahmen ihrer Befugnis nach Art. 32 Abs. 1 PAG (ggf. auch in Verbindung mit den entsprechenden Bestimmungen der Strafprozessordnung).

Art. 32 Abs. 1 PAG
Die Polizei kann bei oder im Zusammenhang mit öffentlichen Veranstaltungen oder Ansammlungen personenbezogene Daten auch durch den Einsatz technischer Mittel zur Anfertigung von Bild- und Tonaufnahmen oder -aufzeichnungen über die für eine Gefahr Verantwortlichen erheben, wenn tatsächliche Anhaltspunkte die Annahme rechtfertigen, daß dabei Ordnungswidrigkeiten von erheblicher Bedeutung oder Straftaten begangen werden. [2]Die Maßnahmen dürfen auch durchgeführt werden, wenn Dritte unvermeidbar betroffen werden.

Die Polizei handelt hierbei als die speichernde Stelle im Sinne des Art. 4 Abs. 9 BayDSG, mit der Folge, dass ihr somit die datenschutzrechtliche Verantwortung für die Videoüberwachung obliegt. In diesem Rahmen fällt der Polizei neben der Verantwortung für den datenschutzkonformen Umgang bis hin zur rechtzeitigen Löschung der Aufzeichnungen auch die systemtechnische und organisatorische Verantwortung zu. Diese Anforderung setzt eine klare Regelungslage der Nutzungs- und Überlassungsstruktur sowie der begeleitenden Rahmenbedingungen für den Umgang mit den Bilddaten voraus.

Da die Polizei – unabhängig von den Eigentumsverhältnissen der Anlage – als speichernde Stelle handelt, die System- oder Wartungsarbeiten aber vom Stadionbetreiber übernommen oder an private Firmen vergeben werden, kann der Zugriff Dritter auf polizeilich gespeicherte personenbezogene Daten nicht ausgeschlossen werden. Derartige Konstellationen sind als Auftragsdatenverarbeitung im Sinne des Art. 6 BayDSG zu bewerten und erfordern die Einhaltung entsprechender technischer und organisatorischer Rahmenbedingungen sowie eine schriftliche Auftragsfestlegung. In der Vereinbarung zwischen dem Stadionbetreiber und der Polizei sind alle erforderlichen Rahmenbedingungen für die Nutzungsüberlassung der Anlage an die Polizei sowie die ausschließliche Verfügungsbefugnis der Polizei über die polizeilich gespeicherten Daten festzulegen. Soll neben der Polizei beispielsweise auch der im Stadion tätige Ordnungsdienst die polizeilichen Videobilder einsehen können, muss die Regelung um eine kon-

krete Vereinbarung hinsichtlich der Überlassung der Bilddaten an den Ordnungsdienst erweitert werden. Auch eine solche Regelung darf nur in Übereinstimmung mit den entsprechenden polizeilichen Datenübermittlungsvorschriften getroffen werden.

Im vorliegenden Fall habe ich mit dem zuständigen Polizeipräsidium vereinbart, dass die Rahmenbedingungen für den Betrieb des Systems in einer Verfahrensbeschreibung der Polizei festgelegt werden. Ich habe darauf hingewiesen, dass insbesondere die Aufzeichnungsdauer und die Zugriffsrechte auf die Bilddaten konkret zu regeln sind. Bislang hatte nur der Einsatz von Ringspeichern mit einer entsprechenden Speicherkapazität, die ihre Aufzeichnungen nach und nach wieder überschrieben, die im Polizeiaufgabengesetz vorgesehene Maximalspeicherdauer von drei Wochen im Regelfall gewährleistet. Für Spielzeitunterbrechungen oder auch für den Fall der Auswechslung eines Speicherelements waren jedoch keine schriftlichen Löschvorgaben vorhanden. Darüber hinaus bestand im geprüften Fall auch keine schriftliche Vereinbarung zwischen Polizei, Stadionbetreiber und Wartungsfirmen zur Auftragsdatenverarbeitung sowie für eine mögliche Übermittlung von Videobildern an den Ordnungsdienst. Das betroffene Präsidium ist inzwischen meinen Forderungen gefolgt und hat entsprechende Regelungen und Vereinbarungen mit den zuständigen Stellen getroffen. Ich werde mich mit diesen abgestimmten Regelungen nun an das Bayerische Staatsministerium des Innern wenden und diese auch für andere bayerische Polizeipräsidien einfordern.

3.4.4 Videoüberwachung von Polizeidienststellen

Nachdem ich im letzten Berichtszeitraum die Videoüberwachung mehrerer Gebäude aus den verschiedenen Bereichen der Justiz überprüft habe, habe ich mich diesmal verstärkt 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. 21 a BayDSG. Sofern die Anlagen zur Videoüberwachung auch eine Aufzeichnung ermöglichen, ist nach Art. 49 PAG und Art. 21 a Abs. 6 i.V.m. Art. 26 und Art. 27 BayDSG eine datenschutzrechtliche Freigabe und die Aufnahme in das Verfahrensverzeichnis erforderlich. Im Rahmen meiner Prüfung stellte ich fest, dass diese Anforderungen nicht immer umgesetzt bzw. die entsprechenden Unterlagen wegen einer Umorganisation der Dienststelle nicht mehr auffindbar waren. Teilweise fehlte auch eine ordnungsgemäße Kennzeichnung der Videoüberwachung. Diese soll es dem Bürger ermöglichen, vor Betreten des öffentlichen Straßenraums, der teilweise von den Überwachungskameras mit erfasst wird, frei zu entscheiden, ob er diesen Bereich betreten will. Bei Gebäuden, in denen sich auch private Büros oder andere Einrichtungen befinden, ist zu kennzeichnen, wer konkret die jeweilige Überwachung veranlasst und dafür verantwortlich ist. Im Rahmen meiner Prüfung wurden die festgestellten Mängel von den betroffenen Dienststellen beseitigt.

Als positiven Befund konnte ich feststellen, dass die rechtlich maximale Aufbewahrungsdauer der aufgezeichneten Aufnahmen von drei Wochen nach Art. 21 a Abs. 5 BayDSG in keinem der von mir überprüften Fälle überschritten wurde. Ebenfalls positiv zu bewerten ist der Umstand, dass die geprüften Dienststellen den Zugriff auf aufgezeichnete Aufnahmen und den Grund des Zugriffs protokollierten.

3.4.5 Vorortprüfung bei einer Hundertschaft der Bereitschaftspolizei zum Thema Videoaufzeichnungen

Polizeiliche Videoaufzeichnungen von Versammlungen oder Großereignissen habe ich in der Vergangenheit regelmäßig kontrolliert. Auch wenn ich – wie oben dargestellt (siehe Nr. 3.3.3) – in diesem Berichtszeitraum erfreulicherweise keine grundlegenden Mängel feststellen musste, kam es bei früheren Prüfungen durch die verspätete Überlassung der Aufzeichnungen wiederholt zu erheblichen zeitlichen Verzögerungen (siehe hierzu 24. Tätigkeitsbericht, Nr. 3.4.3). Letztlich bleibt es für mich in der Praxis kaum feststellbar, ob auch tatsächlich alle angefertigten polizeilichen Aufzeichnungen zur Prüfung vorgelegt werden.

Nachdem die von mir überprüften Videoaufzeichnungen bei Versammlungen häufig von dort eingesetzten Bereitschaftspolizisten angefertigt werden, entschloss ich mich, an der „Quelle“ selbst eine datenschutzrechtliche Prüfung zur Verfahrensweise bei der Speicherung, Bearbeitung und Löschung von polizeilichen Videoaufzeichnungen vorzunehmen. Ein besonderes Augenmerk legte ich dabei auch auf die Art und Weise, wie die Beamten auf die Praxis vorbereitet werden, in der sie dann spontan über die rechtliche Zulässigkeit einer Aufzeichnung entscheiden müssen, bevor sie den Aufnahmeknopf drücken. Einen Teil der konzeptionellen Umsetzung gesetzlicher Neuerungen anlässlich der Neufassung des Bayerischen Versammlungsgesetzes im Jahr 2010 habe ich bereits oben angesprochen (siehe Nr. 3.3.2).

Insgesamt musste ich bei der Prüfung Anfang des Jahres 2011 feststellen, dass die Richtlinien für die Beweissicherung und Dokumentation bei der Bayerischen Bereitschaftspolizei noch den Stand des Jahres 2002 aufwiesen. Ich halte dies für besonders bedenklich, da seither die einschlägige Rechtslage in Teilen grundlegenden Änderungen unterzogen wurde. Zwar entgegnete mir das zuständige Polizeipräsidium, die Richtlinien würden derzeit überarbeitet, bislang wurde mir aber noch keine endgültige Neufassung zugeleitet. Ein Entwurf wurde mir kurz vor Redaktionsschluss des Tätigkeitsberichts übersandt.

Hingegen erschienen die vor Ort festgestellten technischen und organisatorischen Sicherungsmaßnahmen zur Registrierung der Aufzeichnungen und zur Aufbewahrung der Datenträger zumeist als ausreichend. Auch die in diesem Zusammenhang erläuterten Arbeitsabläufe bei der Auswertung der Speicherungen durch einzelne Sachbearbeiter an den vorgesehenen Videoarbeitsplätzen bieten einen ausreichenden Schutz der erfolgten Aufzeichnungen gegen unberechtigte Zugriffe.

3.4.6 Videoaufzeichnung an Notrufsäulen

Unter der Überschrift „Fahrkartenautomat mit direktem Draht zur Polizei – für Notfälle“ bin ich auf eine Neuerung im öffentlichen Personennahverkehr einer bayerischen Kommune aufmerksam geworden. Wie mir das zuständige Polizeipräsidium mitteilte, haben die dortigen Stadtwerke rund 200 Fahrscheinautomaten mit einer integrierten Notruffunktion ausgerüstet, um die Sicherheit für Fahrgäste an den Haltestellen zu verbessern. Neben der Sprachübertragung verfügt die Notrufeinrichtung als Neuerung auch über eine Bildübertragung in die Einsatzzentrale des betreffenden Polizeipräsidiums. Die Video- und Sprachübertragung beginnt mit dem Betätigen der Notruftaste und endet mit Gesprächsabschluss oder, sofern kein Gesprächsaufbau erfolgt, nach zwei Minuten. Eine Akti-

vierung des Mikrophons oder der Kamera durch die Polizei ist systemtechnisch ausgeschlossen.

Die Begründungen der Polizei zu den Vorzügen einer solchen Bildübertragung sind nicht von der Hand zu weisen. So können die Bilder in Notsituationen unter bestimmten Umständen – beispielsweise bei Sprachschwierigkeiten – eine verbesserte Hilfeleistung ermöglichen. Aus datenschutzrechtlicher Sicht vertretbar erscheint auch eine vorübergehende Speicherung der Bilddaten, wie sie bei Sprachdaten von Notrufen üblich ist. Auch hierzu führte die Polizei nachvollziehbare Gründe an, wie die mögliche Nachermittlung von Zeugen oder die Bekämpfung des Missbrauchs solcher Notrufeinrichtungen. Aus datenschutzrechtlicher Sicht nicht akzeptabel erschien jedoch die von der Polizei zunächst beabsichtigte Speicherdauer der Aufzeichnungen über drei Monate hinweg. Da im Fall der Ermittlung wichtiger Zeugen von Sicherheitsstörungen oder des Täters bei einem strafbaren Notrufmissbrauch die gespeicherten Daten als Bestandteil der Ermittlungsunterlagen ohnehin einer längeren Speicherdauer unterliegen, habe ich das Polizeipräsidium aufgefordert, in Anlehnung an Art. 21 a Abs. 5 BayDSG die Speicherdauer auf maximal drei Wochen zu beschränken. Letztendlich hat das Polizeipräsidium dieser Aufforderung zugestimmt und die Speicherdauer reduziert.

3.5 Speicherungen in polizeilichen Dateien

3.5.1 Freitextrecherche im Integrationsverfahren der Bayerischen Polizei (IGVP)

Das Bayerische Staatsministerium des Innern hatte mich zum Jahresende 2010 darüber informiert, nach einer Erprobungsphase nunmehr die Freitextrecherche im Integrationsverfahren der Bayerischen Polizei (IGVP) auf die dort gespeicherten Kurzsachverhalte auszudehnen. Zu dieser Erweiterung habe ich bereits in meinem letzten Tätigkeitsbericht Stellung genommen und dabei die Befürchtung geäußert, die Einhaltung von Prüfungs- und Löschungsterminen für die suchfähige Speicherung personenbezogener Daten in der Datei könne dann ggf. nicht mehr eingehalten werden (siehe hierzu 24. Tätigkeitsbericht, Nr. 3.5.2). Als Reaktion darauf hat das Bayerische Staatsministerium des Innern die Anweisung erteilt, in den gespeicherten Kurzsachverhalten auf bestehende Daten – wie beispielsweise Namensangaben – in strukturierten Datenfeldern zu verweisen, in denen automatisiert gelöscht werden kann und solche Angaben im Sachverhalt nicht zu wiederholen. Mit dieser Regelung konnte nun zumindest in diesem Teilbereich der Problematik bei Volltextsuchen eine vertretbare Lösung gefunden werden. Im Rahmen meiner Prüftätigkeit werde ich darauf achten, dass diese Anweisung auch in der Praxis umgesetzt wird.

3.5.2 Kurzsachverhalte im Integrationsverfahren der Bayerischen Polizei (IGVP)

Ein Bürger beschwerte sich bei mir darüber, dass die Polizei sein Auskunftsersuchen über Speicherungen zu seiner Person teilweise abgelehnt habe. Konkret wollte die Polizei in diesem Fall den Inhalt eines Kurzsachverhaltes zu einem Dateneintrag in der polizeilichen Vorgangsverwaltungsdatei (Integrationsverfahren der Bayerischen Polizei) nicht mitteilen. Da es im vorliegenden Fall so schien, als würde keiner der in Art. 48 Abs. 2 PAG abschließend genannten Versagungs-

gründe für eine Auskunftserteilung greifen, habe ich beim zuständigen Polizeipräsidium die Gründe für die Verweigerung hinterfragt.

Art 48 Abs. 1 und 2 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, geheimgehalten werden müssen, und das Interesse des Betroffenen an der Auskunftserteilung nicht überwiegt.

Das betreffende Polizeipräsidium entgegnete dann auch nicht mit einem Auskunftsversagungsgrund im Rahmen des Polizeiaufgabengesetzes, sondern argumentierte folgendermaßen: Kurzsachverhalte würden zu Beginn der Ermittlungen vom Sachbearbeiter erfasst. Es handle sich dabei um Erstinformationen, die häufig vom späteren Ermittlungsergebnis abweichen würden. In der Regel werde der Kurzsachverhalt auch nicht fortgeschrieben, was zur Folge habe, dass im Falle einer Auskunftserteilung dem Auskunftssuchenden ungesicherte und womöglich in Teilbereichen unzutreffende Sachverhalte zukämen. Aus diesen grundsätzlichen Erwägungen wolle die Polizei die Auskunftserteilung zum Inhalt des Kurzsachverhalts weiterhin ablehnen.

Eine solche Rechtfertigung ist aus datenschutzrechtlicher Sicht offenkundig nicht haltbar. Sollten sich Angaben, die im Erstzugriff durchaus vom späteren Ermittlungsergebnis abweichen können, als falsch erweisen, müssen sie in den betreffenden polizeilichen Dateien berichtigt oder zumindest klarstellend ergänzt werden. Personenbezogene Daten sind gemäß Art. 45 Abs. 1 PAG zu berichtigen, wenn sie unrichtig sind. Laut den Richtlinien für die Führung polizeilicher personenbezogener Sammlungen gilt dies sowohl für den Kriminalaktennachweis als auch für Daten der Vorgangsverwaltungsdatei.

Art. 45 Abs. 1 PAG, Berichtigung, Sperrung und Löschung von Daten
(1) [1]Personenbezogene Daten sind zu berichtigen, wenn sie unrichtig sind. [2]Sind Daten in nichtautomatisierten Dateien oder in Akten zu berichtigen, reicht es aus, in geeigneter Weise kenntlich zu machen, zu welchem Zeitpunkt und aus welchem Grund diese Daten unrichtig geworden sind. [3]Erweisen sich personenbezogene Daten nach ihrer Übermittlung durch die Polizei als unrichtig, sind sie unverzüglich gegenüber dem Empfänger zu berichtigen, wenn dies zur Wahrung schutzwürdiger Interessen des Betroffenen erforderlich ist.

Auch wenn die Polizei sich im vorliegenden Fall meinen Ausführungen angeschlossen hat und dem Betroffenen die geforderte Auskunft erteilte, verdeutlicht die Aussage des Polizeipräsidiums eine grundlegende Problematik innerhalb des Integrationsverfahren der Bayerischen Polizei.

Das System dient unter anderem allen Bayerischen Polizeidienststellen gemeinsam zur Erfassung und Verarbeitung erhobener Personen- und Falldaten, zur Vorgangsverwaltung und Dokumentation polizeilicher Maßnahmen aber auch zur Informationsgewinnung für die polizeiliche Aufgabenerfüllung. Diese Verwendung des Systems bedingt nicht nur eine enorme Fülle dort gespeicherter Daten, sondern auch vielfältige Auswertungsmöglichkeiten. Die oben zitierte Aussage des Polizeipräsidiums in Bezug auf den Inhalt der dort gespeicherten Kurzsachverhalte ist daher zwar verständlich. Oftmals handelt es sich gerade bei den im polizeilichen Erstzugriff angefertigten Sachverhaltszusammenfassungen eben um unbestätigte Erstinformationen, die häufig vom späteren Ermittlungsergebnis abweichen. Aus datenschutzrechtlicher Sicht ist es jedoch unzulässig, diese Datenspeicherungen, die später in anderen Situationen – beispielsweise für eine polizeiliche Prognoseentscheidung – herangezogen werden, unberichtigt zu belassen. In diesem Sinne werde ich mich auch weiterhin dem Thema Integrationsverfahren der Bayerischen Polizei zuwenden und Speicherungen auf deren Zulässigkeit hin kontrollieren.

3.5.3 Bayernweite Recherchen im Integrationsverfahren der Bayerischen Polizei (IGVP)

Wie eben ausgeführt, verfügt die Bayerische Polizei mit ihrem Integrationsverfahren über ein komplexes Dateisystem zur Unterstützung der polizeilichen Sachbearbeitung, Vorgangsverwaltung, Kriminalitätsbekämpfung und Gefahrenabwehr, in dem Daten über nahezu alle polizeilich relevanten Ereignisse aus dem gesamten Spektrum schutz- und kriminalpolizeilicher Aufgaben in Bayern gespeichert werden. Dies führt nicht nur zu einer enormen Fülle an dort gespeicherten Daten, sondern auch zu vielfältigen Auswertungsmöglichkeiten. Anlässlich der bayernweiten Übernahme des Dateisystems habe ich daher schon in meinem 22. Tätigkeitsbericht angemahnt, die Berechtigungen für landesweite Datenzugriffe auf einen eng begrenzten Personenkreis funktionsbezogen weiter einzuschränken und nur in angemessenen Fällen landesweite Recherchen im Integrationsverfahren der Bayerischen Polizei zu ermöglichen (siehe hierzu 22. Tätigkeitsbericht, Nr. 4.2).

Meine bislang in diesem Bereich durchgeführten datenschutzrechtlichen Überprüfungen haben immer wieder Fälle zum Vorschein gebracht, bei denen auch nach eigener Bewertung der betreffenden Polizeidienststellen eine bayernweite Abfrage nicht erforderlich bzw. zulässig gewesen ist. Nach wie vor sehe ich die große Zahl der zugriffsberechtigten Funktionen, über die zu viele Polizeibedienstete einen landesweiten Zugriff erhalten, als einen wesentlichen Risikofaktor für unberechtigte Datenabrufe. Einen Fall, bei dem sich zunächst auch das betreffende Polizeipräsidium uneinsichtig zeigte, will ich hier kurz skizzieren.

Ausschlaggebend für die bayernweite Recherche eines Polizeibeamten im IGVP war eine geringfügige Verkehrsordnungswidrigkeit, bei der zunächst der Fahrer des betreffenden Fahrzeuges nicht ermittelt werden konnte. Der Polizeibeamte wurde schließlich in einer gänzlich unabhängigen Speicherung fündig, da der vermeintliche Fahrer als Zeuge schon einmal im Zusammenhang mit demselben Fahrzeug gespeichert wurde.

Nach den Verfahrensregelungen für das oben beschriebene Integrationsverfahren darf in diesem System aber grundsätzlich nicht im gesamten bayernweiten Datenbestand, sondern lediglich im Datenbestand des jeweiligen Polizeipräsidi-

ums recherchiert werden, dem der Beamte angehört. Zwar gibt es Ausnahmen, die auch bayernweite Recherchen gestatten, geringfügige Verkehrsverstöße gehören aber nicht dazu. Nach längerer Prüfung der Vorschriftenlage hat das betreffende Polizeipräsidium dann auch eingelenkt, den Datenabruf für unzulässig erklärt und die betreffende Polizeidienststelle auf die bestehende Regelungslage hingewiesen.

3.5.4 Speicherung eines ausländischen Touristen in der Staatsschutzdatei

Neben dem polizeilichen Integrationsverfahren (IGVP) und dem Kriminalaktennachweis (KAN) verfügt die Bayerische Polizei noch über zahlreiche weitere Dateien zur Gefahrenabwehr und Strafverfolgung, die teilweise auch als Verbunddateien der verschiedenen Polizeipräsidien konzipiert sind. Der jeweilige Dateizweck ist bei diesen Dateien auf bestimmte Kriminalitätsbereiche, teilweise auch auf einzelne komplexe Ermittlungsverfahren begrenzt.

Ein Beispiel für eine solche Datei stellt die Staatsschutz-Arbeitsdatei der Bayerischen Polizei – ISIS – dar. Die Datei dient der Sammlung, Zusammenführung und Auswertung von bedeutsamen Erkenntnissen im Zusammenhang mit politisch motivierten Straftaten und Ordnungswidrigkeiten oder verfassungsfeindlichen Handlungen. Da es sich um eine Verbunddatei handelt, können zudem landesweit relevante Datensätze von den lokalen bayerischen Staatsschutzdienststellen der Polizei für die Übernahme in die Zentraldatei beim Landeskriminalamt freigegeben werden. Bei meinen regelmäßigen Kontrollen achte ich stets darauf, ob neben Speicherungen im Integrationsverfahren oder im Kriminalaktennachweis auch Speicherungen in solchen „Fachdateien“ erfolgen.

So habe ich anlässlich einer öffentlichen Gelöbnisfeier der Bundeswehr auf dem Münchner Marienplatz auch die Zulässigkeit von Speicherungen im Zusammenhang mit den dort erfolgten Polizeimaßnahmen datenschutzrechtlich überprüft. Besonders aufgefallen ist mir hierbei die Speicherung eines ausländischen Touristen in der o.g. Staatsschutzdatei. Der Mann war bereits am Vormittag in der Münchner Innenstadt festgenommen worden, da er auf seinem T-Shirt einen Aufnäher mit der Aufschrift „ACAB“ (ein aus der US-amerikanischen Rapper-Szene stammendes Kürzel mit der Bedeutung „All Cops are Bastards“) trug. Zivilkräfte des zuständigen Polizeipräsidiums erkannten den Aufnäher und fühlten sich durch dessen Aufschrift beleidigt. Auch die Erklärung, er habe durch die Aufschrift niemanden beleidigen wollen, seine Entschuldigung sowie das unverzügliche Entfernen des Aufnähers von seinem T-Shirt konnten den Tourist nicht vor der Anzeigeerstattung bewahren.

Nicht zuletzt, da der Mann der deutschen Sprache nicht mächtig war, in Deutschland keinen Wohnsitz hatte und auch sonst hier laut Polizei noch nie polizeilich in Erscheinung getreten ist, scheint die in diesem Zusammenhang von der Polizei angenommene Beziehung der vorgeworfenen Beleidigung zu der am Nachmittag in der Innenstadt geplanten Gelöbnisfeier der Bundeswehr doch sehr weit hergeholt. Zudem gab der Tourist an, lediglich wegen eines am Abend tatsächlich in der Allianz Arena stattfindenden Fußballspiels mit einer Gruppe von Freunden nach München gereist zu sein. Er erklärte sich umgehend mit der Einziehung des Aufnähers einverstanden und konnte schon nach kurzem aus dem Polizeigewahrsam entlassen werden. Auch die zuständige Staatsanwaltschaft sah nach der Überprüfung des Schuldvorwurfs von einer weiteren strafrechtlichen Verfolgung der im Raum stehenden Beleidigung ab.

Trotz dieser Umstände speicherte die Polizei den Sachverhalt im Integrationsverfahren mit dem Hinweis auf ein „politisches Motiv“ der Tat. Neben dieser Erfassung wurden die Daten des Betroffenen auch in der oben erläuterten lokalen Staatsschutz-Arbeitsdatei Innere Sicherheit Informationssystem – ISIS gespeichert und an die Zentraldatei beim Landeskriminalamt übermittelt. Darüber hinaus leitete die Polizei die Daten im Rahmen des Meldedienstes für Staatsschutzdelikte an das Landesamt für Verfassungsschutz und an das Bayerische Staatsministerium des Innern weiter. Der Sachverhalt wurde zudem in die polizeiliche Statistik für politisch motiviert begangene Delikte aufgenommen.

Auf meine Intervention hin hat das zuständige Polizeipräsidium inzwischen die betreffenden Speicherungen berichtigt bzw. aus der Staatsschutzdatei gelöscht. Ebenso informierte die Polizei nach meiner Aufforderung die zuvor benachrichtigten Sicherheitsbehörden über die Neubewertung des Falles. Das Landesamt für Verfassungsschutz hatte nach eigener Aussage den vorliegenden Fall ohnehin als nicht extremistisch bewertet und dementsprechend keine Speicherung der übermittelten Daten vorgenommen.

3.5.5 Erkennungsdienstliche Behandlungen

Auch in diesem Berichtszeitraum bin ich meiner Ankündigung aus dem letzten Tätigkeitsbericht nachgekommen, weiterhin die Gründe für die Speicherung erkennungsdienstlicher Daten genau zu überprüfen (siehe hierzu 24. Tätigkeitsbericht, Nr. 3.9).

Gemäß § 81 b Alt. 2 Strafprozessordnung (StPO) dürfen, soweit es für die Zwecke des Erkennungsdienstes notwendig ist, Lichtbilder und Fingerabdrücke eines Beschuldigten auch gegen seinen Willen aufgenommen werden.

§ 81 b StPO
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.

Nach der Rechtsprechung setzt eine solche Datenspeicherung zu präventivpolizeilichen Zwecken aber u.a. voraus, dass eine Wiederholungsgefahr angenommen werden kann. Eine lediglich formelhafte und unspezifische Begründung für die Annahme einer solchen Wiederholungsgefahr, genügt dabei nicht. Maßgebend ist letztlich, ob Anhaltspunkte dafür vorliegen, dass der Beschuldigte in ähnlicher oder anderer Weise erneut straffällig werden könnte und ob die erkennungsdienstlichen Unterlagen zur Förderung der dann zu führenden Ermittlungen geeignet erscheinen. Insbesondere kommt es hierbei auf die Umstände des Einzelfalls an, wie etwa die Schwere der Tat, die Begehungsweise der dem Betroffenen im strafrechtlichen Anlassverfahren zur Last gelegten Straftaten, seine Persönlichkeit sowie den Zeitraum, seit dem der Betroffene nicht mehr strafrechtlich in Erscheinung getreten ist.

Ob die genannten Voraussetzungen eingehalten werden, überprüfe ich regelmäßig bei anlassunabhängigen Kontrollen oder aufgrund von Bürgereingaben. Dass diese Überprüfung nach wie vor notwendig ist, zeigt folgendes Beispiel:

Durch einen Zeitungsbericht wurde ich auf den Fall zweier Minderjähriger aufmerksam, die einen mit Wasser gefüllten Müllsack aus dem 8. Stock eines Hauses geworfen hatten und dabei eine Kindergartengruppe nur knapp verfehlten. Dem Zeitungsartikel zufolge waren die Jugendlichen im Rahmen des eingeleiteten Strafverfahrens erkennungsdienstlich behandelt worden, obwohl sie bisher bei der Polizei noch nicht aktenkundig gewesen waren. Erst nach mehrmaligem Schriftwechsel mit dem zuständigen Polizeipräsidium konnte ich erreichen, dass die Speicherung der erkennungsdienstlichen Unterlagen wieder gelöscht wurde.

Aus Datenschutzsicht problematisch war hierbei die Argumentation, mit der die Polizei die Notwendigkeit der Erfassung zu begründen suchte: Die Jugendlichen würden in einem Problemviertel wohnen und in einem Umfeld verkehren, in dem auch Jugendliche anzutreffen seien, die bereits mehrfach kriminalpolizeilich in Erscheinung getreten seien. Ich halte es für unzulässig, das Verhalten anderer als Kriterium heranzuziehen, wenn es um die Beurteilung der Persönlichkeit der Betroffenen geht. Voraussetzung der Speicherung von erkennungsdienstlichen Unterlagen ist nämlich allein, dass tatsächlich Anhaltspunkte dafür vorliegen, dass die betroffene Person zukünftig eine Straftat begehen wird, d.h., dass gegen sie wieder ein Ermittlungsverfahren zu führen sein wird. Zudem führte die Polizei an, es sei aufgrund der von den Jugendlichen gezeigten hohen kriminellen Energie notwendig gewesen, eine erkennungsdienstliche Behandlung durchzuführen, da es sich nicht um einen bloßen Jugendstreich gehandelt habe. Eine hohe kriminelle Energie konnte ich hier nicht erkennen; die Jugendlichen hatten sich bei der Begehung ihrer Tat nicht besonders listig angestellt und die Tat auch, unmittelbar nachdem sie ausfindig gemacht wurden, umfassend gestanden. Auch die Staatsanwaltschaft teilte wohl meine Einschätzung bzgl. der Schwere der Tat. Sie legte den Beschuldigten lediglich auf, 20 Stunden gemeinnützige Arbeit zu leisten.

3.5.6 Prüfung retrograder DNA-Speicherungen

Schon in meinen zurückliegenden Tätigkeitsberichten habe ich mich mehrfach unter verschiedenen Gesichtspunkten mit DNA-Speicherungen befasst. Dies gerade auch wegen der Erweiterung der Befugnisnorm im Jahr 2005, wonach solche Maßnahmen nicht nur beim Verdacht einer Straftat von erheblicher Bedeutung oder einer Sexualstraftat möglich sind, sondern auch bei der wiederholten Begehung von sonstigen Straftaten, die im Unrechtsgehalt einer Straftat von erheblicher Bedeutung gleichstehen.

§ 81 g StPO
(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.

In der Folge dieser Befugniserweiterung gaben dann auch Maßnahmen, die auf die wiederholte Begehung sonstiger Straftaten gestützt wurden, immer wieder Anlass für datenschutzrechtliche Kritik. Oftmals konnten hier die verantwortlichen

Stellen nicht nachvollziehbar darlegen, weshalb die der Speicherung zugrunde gelegten Taten im Unrechtsgehalt einer Straftat von erheblicher Bedeutung gleichstehen sollten. Nach der Rechtsprechung des Bundesverfassungsgerichts müssen Straftaten von erheblicher Bedeutung mindestens dem Bereich der mittleren Kriminalität zuzurechnen sein, den Rechtsfrieden empfindlich stören und geeignet sein, das Gefühl der Rechtssicherheit der Bevölkerung erheblich zu stören. Soll eine DNA-Speicherung auf § 81 g Absatz 1 Satz 2 StPO gestützt werden, ist im Einzelfall abzuwägen, ob die Gesamtschau für die wiederholte Begehung sonstiger Straftaten einen gleichen Unrechtsgehalt wie bei einer Straftat von erheblicher Bedeutung ergibt.

Vor diesem Hintergrund entschloss ich mich, erneut DNA-Maßnahmen – in diesem Fall sogenannte Retrograderfassungen – zu prüfen. Entgegen der Vorwärtserfassung im Zusammenhang mit laufenden Strafverfahren, handelt es sich hierbei um die systematische Abarbeitung zurückliegender Fälle. Nach Einführung der gesetzlichen Voraussetzungen für DNA-Maßnahmen begann die Polizei mit der rückwärtsgerichteten Abarbeitung früherer Verurteilungen nach Deliktskatalogen, angefangen mit den schwerwiegendsten Delikten. Dies bedingt, dass bei der rückwärtsgerichteten Abarbeitung nunmehr die für die DNA-Maßnahmen zu überprüfenden Anlassdelikte in einem Straftatenbereich angelangt sind, in dem oftmals schon von vornherein die erforderliche Bedeutung der Tat nur schwer begründbar erscheint. So wurden beispielsweise einige der von mir geprüften DNA-Maßnahmen nach Betrugs- oder Untreuedelikten durchgeführt, die jedenfalls bei Betrachtung des konkreten Einzelfalls keine erhebliche Bedeutung aufwiesen. Erschwerend kommt hinzu, dass DNA-Maßnahmen grundsätzlich nur dann durchgeführt werden dürfen, wenn dadurch ein Aufklärungserfolg bei künftig zu erwartenden Strafverfahren prognostiziert werden kann. Auch dies scheint bei dieser Art von Delikten oft problematisch, da die Täter bei solchen Tatausführungen oftmals keine abgesonderten Körperzellen als Spur für spätere Ermittlungen hinterlassen.

Beispielhaft hierfür waren DNA-Maßnahmen bei zwei Personen, die fortgesetzt Betrügereien begingen, indem sie Waren bestellten, die sie nicht bezahlen konnten. Einer DNA-Spur kommt bei diesen Taten in der Regel kein Beweiswert zu. Ähnlich verhielt es sich in einem anderen Fall, in dem die betroffene Person wiederholt Betrugsdelikte zum Nachteil der Sozialversicherung begangen hat, der geschädigten Stelle also namentlich bekannt war. Über die fragliche „Erheblichkeit“ der Anlasstaten hinaus war auch hier kein Beweiswert der DNA-Speicherung im Falle der polizeilich prognostizierten Tatwiederholung zu erwarten.

Ich stehe im Rahmen der genannten Prüfungen in einigen Fällen noch im Schriftwechsel mit den geprüften Polizeipräsidien. Teilweise war der Polizei aber schon bei der Zusammenstellung der Kriminalakten für meine Prüfung aufgefallen, dass die den DNA-Analysen als Anlassdelikt zugrunde gelegten Delikte nicht den erforderlichen rechtlichen Vorgaben entsprechen. Ein Polizeipräsidium hatte daher schon vor meiner Prüfung angekündigt, eine Reihe von Speicherungen zu löschen.

Aufgrund der datenschutzrechtlichen Bedeutung des Themas werde ich hierzu noch weitere Polizeipräsidien prüfen.

3.6 Abfragen aus dem Zentralen Verkehrsinformationssystem ZEVIS

Das Bayerische Polizeiverwaltungsamt (PVA) ist zuständig für die zentrale Ahndung von Verkehrsordnungswidrigkeiten, die im Bereich des Freistaates Bayern begangen und festgestellt werden. Die Aufgaben umfassen sowohl den Bereich der Verwarnungen als auch den Erlass von Bußgeldbescheiden und die anschließende Abwicklung des gesamten Bußgeldverfahrens. In Erfüllung dieser Aufgaben ist das PVA die von der Landesregierung bestimmte zuständige Verwaltungsbehörde zur Ahndung von Verkehrsordnungswidrigkeiten nach dem Straßenverkehrsgesetz. Im Rahmen dieser Aufgabe darf das PVA Fahrzeug- und Halterdaten grundsätzlich auch im automatisierten Abrufverfahren aus dem Datenbestand des Kraftfahrtbundesamtes abfragen. Hierfür gelten aber bestimmte gesetzliche Regelungen. Abrufe der Fahrzeug- und Halterdaten aus dem zentralen Verkehrsinformationssystem ZEVIS sind hierbei nur dann zulässig, wenn der Abfragende dazu das Kennzeichen des fraglichen Fahrzeugs oder die Fahrzeugidentifizierungsnummer verwendet, er also die Fahrzeugdaten kennt.

Aufgrund eines Hinweises habe ich festgestellt, dass vereinzelt auch Abfragen erfolgten, bei denen nur die Personendaten als Abfragekriterium verwendet wurden. Ich habe das PVA daher darauf hingewiesen, dass ich solche Abfragen nach der bestehenden Gesetzeslage für nicht zulässig erachte. Das PVA hat bereits im Verlauf meiner Prüfung die bestehende Abfragepraxis geändert.

3.7 Unerlaubte Datenabfragen

Nachdem ich bereits in vorangegangenen Tätigkeitsberichten das Problem von Datenabfragen im sozialen Nahfeld der abfragenden Polizeibeamten immer wieder thematisiert habe (siehe hierzu 22. Tätigkeitsbericht, Nr. 4.17 und 23. Tätigkeitsbericht, Nr. 4.15), habe ich mich in diesem Berichtszeitraum mit der Ahndungspraxis solcher datenschutzrechtlicher Verstöße beschäftigt.

Datenabfragen zu privaten Zwecken sind unzulässig und stellen Ordnungswidrigkeiten dar, die mit Bußgeldern geahndet werden können. Das Bayerischen Datenschutzgesetz (Art. 37 Absatz 1 Nr. 3 BayDSG) sieht in Verbindung mit der zugehörigen Zuständigkeitsverordnung (§ 6 Abs. 3 ZuVOWiG) vor, dass die dem Bayerischen Staatsministerium des Innern unmittelbar nachgeordneten Polizeidienststellen die Ahndung dieser Ordnungswidrigkeiten jeweils selbst vollziehen.

Art. 37 BayDSG
(1) Mit Geldbuße bis zu dreißigtausend Euro kann belegt werden, wer unbefugt von diesem Gesetz oder von nach Art. 2 Abs. 7 diesem Gesetz vorgehenden Rechtsvorschriften geschützte personenbezogene Daten, die nicht offenkundig sind,

1. *speichert, verändert oder übermittelt,*
2. *zum Abruf mittels automatisierten Verfahrens bereithält oder*
3. *abruft oder sich oder einem anderen aus Dateien verschafft.*

(2) Ferner kann mit Geldbuße bis zu dreißigtausend Euro belegt werden, wer

1. *die Übermittlung von durch dieses Gesetz oder durch nach Art. 2 Abs. 7 diesem Gesetz vorgehenden Rechtsvorschriften geschützten personenbezogenen Daten, die nicht offenkundig sind, durch unrichtige Angaben erschleicht,*

2. entgegen Art. 19 Abs. 4 Satz 1, Art. 22 Satz 1 oder Art. 23 Abs. 1 die übermittelten Daten für andere Zwecke nutzt, indem er sie an Dritte weitergibt oder

3. entgegen Art. 23 Abs. 3 Satz 3 die in Art. 23 Abs. 3 Satz 2 bezeichneten Merkmale mit den Einzelangaben zusammenführt.

(3) [1]Wer eine der in den Absätzen 1 und 2 bezeichneten Handlungen gegen Entgelt oder in der Absicht, sich oder einen anderen zu bereichern oder einen anderen zu schädigen, begeht, wird mit Freiheitsstrafe bis zu zwei Jahren oder mit Geldstrafe bestraft. [2]Die Tat wird nur auf Antrag verfolgt. [3]Antragsberechtigt sind die Betroffenen, die speichernde öffentliche Stelle und der Landesbeauftragte für den Datenschutz.

Ich habe daher überprüft, wie im Bereich der Bayerischen Polizei mit der Thematik unerlaubter Datenabfragen umgegangen wird. Dabei habe ich festgestellt, dass die einzelnen Polizeiverbände selbst anlassunabhängige Kontrollen durchführen und bei der Feststellung von Verstößen entsprechende Bußgeldverfahren einleiten.

Regelmäßige anlasslose Kontrollen und eine spürbare Ahndung bei Verstößen halte ich gerade im Bereich unerlaubter Abfragen aus polizeilichen Dateien für unbedingt erforderlich. Polizeiliche Dateien enthalten höchst sensible Informationen und ihre missbräuchliche Verwendung zu privaten Zwecken ist aufgrund des erheblichen Eingriffs in das Persönlichkeitsrecht des Betroffenen nicht zu tolerieren. Bereits aus generalpräventiven Gründen müssen missbräuchliche Abrufe deutliche Konsequenzen zur Folge haben.

Aus diesem Grund stoße auch ich selbst immer wieder die anlassunabhängige Überprüfung von polizeilichen Datenabfragen an. In einem Fall habe ich um Auswertung der Protokolldateien hinsichtlich der Abfragen aus den polizeilichen Informationssystemen zu den Daten eines Prominenten gebeten. Dieser Prominente stand zum Zeitpunkt meiner Prüfung unter dem Verdacht, eine schwere Straftat begangen zu haben. Bei vier von zehn geprüften Polizeiverbänden wurden daraufhin Ordnungswidrigkeitenverfahren gegen insgesamt acht Polizeiangehörige durchgeführt, da sie vermutlich lediglich aus eigenem Sensationsinteresse heraus und nicht aufgrund eines dienstlichen Anlasses die fraglichen Datenabfragen durchgeführt hatten.

Das Ergebnis dieser Prüfung zeigt mir ebenfalls, dass die Praxis, in diesem Bereich regelmäßig anlassunabhängige Kontrollen durchzuführen, der richtige Weg ist. Auch dieses Thema werde ich weiter beobachten.

3.8 Datenübermittlung von der Polizei an Dritte

Ein aus datenschutzrechtlicher Sicht besonders sensibles Thema ist die Weitergabe polizeilicher Daten an Dritte, also an Personen oder Stellen außerhalb des öffentlichen Bereichs. Das Polizeiaufgabengesetz bietet hierzu nur ausnahmsweise und in wenigen eingeschränkten Fällen eine gesetzliche Grundlage. Besonders zu beachten ist dabei regelmäßig, ob ein schutzwürdiges Interesse des Betroffenen am Ausschluss der Datenübermittlung anzunehmen ist. Liegt eine solche Annahme nahe, wird der Spielraum für Datenübermittlungen nochmals erheblich verringert. Die Polizei muss sich hierbei ständig bewusst sein, dass aus der Weitergabe personenbezogener Daten an Dritte für den Betroffenen erhebliche Nachteile erwachsen können, die gegen den angestrebten Nutzen sorgfältig

abzuwägen sind. Das folgende Beispiel aus meiner Überprüfungspraxis zeigt, dass solche Abwägungen im Polizeialltag nicht immer im Sinne des Datenschutzes erfolgen.

Der Feuerwehrverein in einer kleineren bayerischen Gemeinde veranstaltet regelmäßig Partys für die dortige Dorfjugend. Nachdem sich ein Anwohner von der nach seiner Ansicht überlauten Musik bei einer solchen Party gestört fühlte, wandte er sich an die örtliche Polizei und bat um Abhilfe. Laut deren Darstellung ist zur Beseitigung einer solchen Lärmbelästigung grundsätzlich ein Tätigwerden der Polizei angezeigt. Im vorliegenden Fall entschied man sich, den Partyveranstalter und gleichzeitigen Feuerwehrkommandanten telefonisch über die Beschwerde zu informieren und ihm dabei auch – für eine persönliche Kontaktaufnahme – den Namen des Beschwerdeführers mitzuteilen. Gerade dies wollte der Beschwerdeführer aber nicht und er hatte die Polizei nach seinen Angaben auch ausdrücklich darauf hingewiesen. Trotzdem habe zur Überraschung des Anwohners kurze Zeit später der Partyveranstalter vor dessen Tür gestanden, „um etwaige Differenzen ausräumen zu können". So zumindest ging es aus dem Antwortschreiben der Behördenleitung des betreffenden Polizeipräsidiums hervor, nach dem sich der Anwohner über seine Namensweitergabe dort beklagt hatte. Nach Ansicht des Polizeipräsidiums war an dieser Datenübermittlung der Polizei an den Partyveranstalter auch nichts auszusetzen, da man bei unterschiedlichen Interessenslagen allgemein eine direkte Kommunikation der widerstrebenden Parteien befürworte. Dies gelte umso mehr in einer dörflichen Gemeinschaft. Darüber hinaus bewertete die Polizei die Datenweitergabe in diesem Sinne als förderlich und der polizeilichen Aufgabenerfüllung dienlich.

Der Betroffene hat sich mit dieser für ihn nicht zufriedenstellenden Antwort an mich gewandt. Auf meine Nachfrage hin berief sich die Polizei dann zunächst auf ihre Datenübermittlungsbefugnis gegenüber öffentlichen Stellen, schließlich handle es sich bei der Freiwilligen Feuerwehr ja um eine Stelle im Sinne dieser Vorschrift.

Eine solche Datenweitergabe der Polizei an die Feuerwehr als gemeindliche Einrichtung ist jedoch nur zulässig, wenn sie im Rahmen der rechtmäßigen Erfüllung der in der Zuständigkeit der Feuerwehr liegenden Aufgaben erforderlich ist. Nur in diesen Fällen kann eine Datenübermittlung der Polizei an eine freiwillige Feuerwehr nach Art. 40 PAG bewertet werden.

Als Aufgaben der Freiwilligen Feuerwehr sind nach dem Bayerischen Feuerwehrgesetz der abwehrende Brandschutz und technische Hilfsdienste zu sehen. Richtet aber ein Feuerwehrverein Poolpartys oder ähnlichen Veranstaltungen aus, erfüllt sie damit keine Aufgabe im Sinne des Bayerischen Feuerwehrgesetzes. Soweit die Polizei dann – wie im gegebenen Sachverhalt – beabsichtigt, personenbezogene Daten eines Beschwerdeführers an den Partyausrichter zu übermitteln, muss sie daher nicht das Vorliegen der rechtlichen Voraussetzung für die Datenübermittlung an eine öffentliche Stelle nach Art. 40 PAG, sondern die Zulässigkeit für eine Datenübermittlung an Dritte nach Art. 41 PAG prüfen.

Art. 41 PAG Datenübermittlung an Personen und Stellen außerhalb des öffentlichen Bereichs
(1) Die Polizei kann von sich aus personenbezogene Daten an Personen oder Stellen außerhalb des öffentlichen Bereichs übermitteln, soweit dies erforderlich ist
1. zur Erfüllung polizeilicher Aufgaben,

2. zur Verhütung oder Beseitigung erheblicher Nachteile für das Gemeinwohl oder
3. zur Wahrung schutzwürdiger Interessen Einzelner und kein Grund zur Annahme besteht, daß der Betroffene ein schutzwürdiges Interesse an dem Ausschluß der Übermittlung hat.

(2) Die Polizei kann auf Antrag von Personen oder Stellen außerhalb des öffentlichen Bereichs personenbezogene Daten übermitteln, soweit der Auskunftsbegehrende

1. ein rechtliches Interesse an der Kenntnis der zu übermittelnden Daten glaubhaft macht und kein Grund zu der Annahme besteht, daß der Betroffene ein schutzwürdiges Interesse an dem Ausschluß der Übermittlung hat oder
2. ein berechtigtes Interesse geltend macht, offensichtlich ist, daß die Datenübermittlung im Interesse des Betroffenen liegt, und kein Grund zu der Annahme besteht, daß er in Kenntnis der Sachlage seine Einwilligung verweigern würde.

Ich habe das zuständige Polizeipräsidium darauf hingewiesen, es müsse sich auch dann an die rechtlichen Rahmenvorgaben halten, wenn es beim Vorliegen unterschiedlicher Interessenslagen eine direkte Kommunikation zwischen den widerstrebenden Parteien befürworte. Soweit die Datenübermittlung – wie geschildert – in Folge einer Nachfrage des verantwortlichen Partyveranstalters erfolgt, kann diese daher nur in den Grenzen des Art. 41 Abs. 2 PAG als zulässig betrachtet werden. Die amtliche Begründung zum Gesetzesentwurf aus dem Jahr 1990 stellt hierfür klar, *„dass die Datenübermittlung von Amts wegen oder auf Antrag durch die Polizei an Personen oder Stellen außerhalb der öffentlichen Verwaltung die Ausnahme bleiben muss."*

Im vorliegenden Fall war für die Übermittlung an den Veranstalter weder ein überwiegendes rechtliches Interesse an der Kenntnis der Daten, noch ein berechtigtes Interesse im Sinne des Art. 41 Abs. 2 PAG erkennbar. Die Datenübermittlung hätte daher unterbleiben müssen.

Das schutzwürdige Interesse eines Behördeninformanten an der Geheimhaltung seines Namens im Allgemeinen habe ich bereits in meinem letzten Tätigkeitsbericht ausführlich behandelt (siehe hierzu 24. Tätigkeitsbericht, Nr. 6.10).

3.9 Sicherheitsüberprüfungen von Abschlepppersonal

Im Berichtszeitraum haben sich verschiedene Abschleppunternehmer bei mir über die umfangreichen Sicherheitsüberprüfungen beklagt, die erforderlich sind, um von der Polizei vermittelte Abschleppaufträge zu erhalten. Im Wesentlichen ging es hierbei um die vom Bayerischen Staatsministerium des Innern festgelegten Richtlinien zum Betrieb einer privaten Abschleppzentrale für Bayern. Wendet sich beispielsweise ein Verkehrsteilnehmer an die Polizei, da sein Fahrzeug nach einem Unfall nicht mehr fahrbereit ist, leitet die Polizei solche Abschleppaufträge an diese zentrale Vermittlungsstelle weiter. Von dort aus wird dann ein geeigneter Abschleppunternehmer beauftragt, der in einem Unternehmensverzeichnis registriert worden ist. Um aber in dieses Unternehmensverzeichnis der Abschleppzentrale zu gelangen, muss der Betrieb bestimmte Qualitätsmerkmale erfüllen, die in den genannten Richtlinien festgeschrieben wurden.

Ein Passus darin betrifft die „Qualitätsstandards hinsichtlich der persönlichen Zuverlässigkeit“ des eingesetzten Personals als auch der beauftragten Unternehmer selbst. Um diese „Zuverlässigkeit“ zu gewährleisten, müssen die Beschäftigten ihre Einwilligung zu einer jährlichen Sicherheitsüberprüfung durch die Polizei geben. Die Polizei überprüft die Personen dann anhand ihres Datenbestandes. Ich habe gegenüber dem Bayerischen Staatsministerium des Innern deutlich meine Ablehnung dieses Verfahrens zum Ausdruck gebracht. Auch wenn sich die Polizei bei den Überprüfungen auf eine angenommene „Garantenpflicht“ gegenüber den Verkehrsteilnehmern – die sich wegen eines geeigneten Abschleppunternehmers an sie wenden – beruft, sieht nicht einmal das Bayerische Sicherheitsüberprüfungsgesetz eine solche Überprüfungsintensität vor.

Schon die Vornahme der Überprüfungen auf Grundlage „informierter Einwilligungen“ der Beschäftigten sehe ich problematisch. An der Freiwilligkeit einer solchen Einwilligung hege ich erhebliche Zweifel, wenn der Betroffene unzumutbare Nachteile befürchten muss, sobald er seine Einwilligung verweigert (siehe hierzu 23. Tätigkeitsbericht, Nr. 4.14.2). So ist durchaus denkbar, dass ein Arbeitnehmer eines Abschleppunternehmens bei der Verweigerung seiner Einwilligung den Verlust seines Arbeitsplatzes zu befürchten hat – eine Freiwilligkeit der Entscheidung im Sinne des Art. 15 BayDSG ist dann kaum anzunehmen.

Darüber hinaus gilt zu bedenken, dass derartige erhebliche Grundrechtseingriffe – zumal sie hier regelmäßig erfolgen – angesichts der vom Bundesverfassungsgericht entwickelten Wesentlichkeitslehre nicht auf „informierte Einwilligungen“ gestützt werden können. Bereichsspezifische gesetzliche Vorschriften, wie das Luftsicherheitsgesetz, das Atomgesetz oder das Bayerische Sicherheitsüberprüfungsgesetz erlauben solche Eingriffe auch nur in wenigen herausragenden Konstellationen.

Zu berücksichtigen gilt zudem, dass durch die Erhebung und Überprüfung anhand polizeilicher Daten die Werteentscheidungen des Bundeszentralregistergesetzes (BZRG) umgangen werden. So speichert die Polizei auch Daten, die in das Bundeszentralregister gar nicht erst eingetragen werden, die im Bundeszentralregister bereits getilgt sind oder die – sofern es sich um ein Führungszeugnis und nicht um eine unbeschränkte Auskunft handelt – nach dem BZRG nicht übermittelt werden dürfen.

In diesem Sinne konnte ich mich mit dem Bayerischen Staatsministerium des Innern darauf einigen, die bisherige Praxis der Überprüfungen von Abschlepppersonal zu ändern. Überprüfungen anhand polizeilicher Datenspeicherungen werden nicht mehr vorgenommen. Künftig wird es für Mitarbeiter der Unternehmen genügen, ihre „persönliche Zuverlässigkeit“ bei Vertragsbeginn durch die Vorlage eines Führungszeugnisses nach § 30 Abs. 1 BZRG nachzuweisen.

3.10 Akkreditierungsverfahren bei Großveranstaltungen

Erneut gaben mir im Zeitraum dieses Tätigkeitsberichts polizeiliche Überprüfungsverfahren im Rahmen der Akkreditierungen zu Sportgroßereignissen Anlass dazu, gegenüber der Polizei und dem Bayerischen Staatsministerium des Innern meine datenschutzrechtlichen Bedenken mitzuteilen. Nach wie vor bin ich der Ansicht, dass solche Zuverlässigkeitsüberprüfungen aufgrund ihrer Bedeutung und ihres Umfangs zu erheblichen Eingriffen in das Grundrecht auf informationelle Selbstbestimmung einer Vielzahl Betroffener führen und daher eine be-

reichsspezifische gesetzliche Grundlage benötigen (siehe hierzu 24. Tätigkeitsbericht, Nr. 3.11 und 23. Tätigkeitsbericht, Nr. 4.14.1 sowie Entschließung anlässlich der 74. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 25./26.10.2007 in Saalfeld).

Die Planungen der Bayerischen Polizei anlässlich der Alpinen Ski-Weltmeisterschaft 2011 in Garmisch-Partenkirchen und der Biathlon-Weltmeisterschaft 2012 in Ruhpolding nahm ich daher zum Anlass für erneute datenschutzrechtliche Prüfungen. Unabhängig von meinen oben erwähnten grundsätzlichen Bedenken, legte ich bei diesen Kontrollen mein Augenmerk insbesondere auf die Ausgestaltung des Akkreditierungsverfahrens.

Kritikwürdig war bereits der für die Überprüfungen herangezogene Kriterienkatalog der Delikte, nach denen die Überprüften als „sicherheitsbedenklich" eingestuft werden. Soll durch ein Akkreditierungsverfahren der Gefahr eines terroristischen Anschlags bei einer Veranstaltung von herausragender internationaler Bedeutung begegnet werden, dürfen im Rahmen der Sicherheitsüberprüfung nur solche Speicherungen herangezogen werden, die zur Prüfung einer gewaltbereiten extremistischen Neigung erforderlich sind. Nach entsprechenden Gesprächen mit der Polizei konnte ich eine erhebliche Reduzierung des Kriterienkatalogs für die Versagung von Akkreditierungen erreichen. So wurden beim Akkreditierungsverfahren im Rahmen der Biathlon-Weltmeisterschaft beispielsweise Bagatelldelikte oder nicht relevante Kriminalitätsfelder aus dem Kriterienkatalog gestrichen.

Außerdem wurde im Gegensatz zu früheren Veranstaltungen bei den genannten Überprüfungsverfahren der überprüfte Personenkreis wesentlich eingeschränkt. Letztlich wurden noch das Sicherheitspersonal und Personen mit Zugang zu besonders sensiblen Bereichen überprüft, nicht mehr aber etwa einfache Mitarbeiter an Verkaufsständen oder Servicepersonal. Meine Überprüfungen von Ablehnungsfällen anlässlich beider Veranstaltungen zeigten schließlich, dass diese durchgehend im Rahmen des Kriterienkataloges lagen und die Begründungen der Polizei anhand der vorgelegten Akten nachvollziehbar erschienen.

Bis auf wenige Ausnahmen nicht mehr überprüft wurden bei der Biathlon-WM auch Journalisten. Parallel zu der durch die Datenschutzbeauftragten vorgebrachten Kritik an der Zunahme von Zuverlässigkeitsüberprüfungsverfahren bei Großveranstaltungen, haben sich auch Journalisten- und Medienverbände sowie Medienunternehmen kritisch mit diesem Thema auseinandergesetzt. Ich habe mich dabei an Gesprächen zwischen Innenministerium und Journalistenvertretern beteiligt, um eine datenschutzgerechte Lösung zu entwickeln. Den differenzierten Ansatz bei Sicherheitsüberprüfungen von Journalisten bei der Biathlon-WM erachte ich auch vor diesem Hintergrund als Erfolg für den Datenschutz.

3.11 Lagebericht der Bayerischen Polizei

Im Berichtszeitraum informierte mich das Bayerische Landeskriminalamt über die neu geschaffene zentrale Lagedatei der Bayerischen Polizei und legte mir die hierfür erarbeitete Errichtungsanordnung vor. Zweck der Datei ist die Sammlung und Zusammenführung relevanter Erkenntnisse zur Unterstützung der polizeilichen Aufgaben im Rahmen des Art. 2 PAG – insbesondere der Gefahrenabwehr und der Aufklärung von Straftaten und Ordnungswidrigkeiten. So soll die Datei beispielsweise möglichst frühzeitig Gefahren- und Kriminalitätsentwicklungen

aufzeigen, Zusammenhänge und Verflechtungen für deren Bekämpfung verdeutlichen oder Fahndungshinweise geben. Als Basis dienen der Datei in erster Linie die täglichen Speicherungen aus dem Integrationsverfahren der Bayerischen Polizei (siehe Nr. 3.5.1, Nr. 3.5.2 und Nr. 3.5.3). Die Datensätze werden dann ggf. mit anderen polizeilichen und außerpolizeilichen Dateien abgeglichen und in entsprechend aufbereiteter Form sowohl Basisdienststellen als auch den Führungsebenen der Polizei zur Verfügung gestellt. Nachdem sich aus datenschutzrechtlicher Sicht bei der Ausgestaltung des Verfahrens einige Fragen ergaben, habe ich dieses Verfahren beim Bayerischen Landeskriminalamt geprüft.

Bei der Prüfung habe ich gegenüber dem Bayerischen Landeskriminalamt verdeutlicht, dass im Rahmen der Lageberichterstattung Personendaten von Beschuldigten oder Tatverdächtigen einem breiten Benutzerkreis innerhalb der Polizei zur Kenntnis gebracht werden. Zulässig ist diese Datennutzung jedoch auch im Rahmen einer Lageeinschätzung nur im erforderlichen Umfang. Darüber hinaus unterliegt die Verwendung der Daten von Jugendlichen, Kindern, Geschädigten oder Zeugen weiteren Einschränkungen. Im besonderen Maße gilt dies auch, wenn beispielsweise Bilddaten in die Lageberichte aufgenommen werden sollen. Das Landeskriminalamt hat auf meine Veranlassung hin die Errichtungsanordnung nachgebessert und diese Einschränkungen hervorgehoben.

Da sich die einzelnen Beiträge in der Lagedatei regelmäßig auf Ausgangsdaten des Integrationsverfahrens (IGVP) beziehen, besteht die Möglichkeit durch einfaches „Anklicken“ des Aktenzeichenfeldes den ursprünglichen Datensatz im IGVP aufzurufen. Nach meinen Feststellungen konnten auf diesem Weg die geltenden lokalen Benutzereinschränkungen des IGVP umgangen und auch Datensätze anderer Polizeipräsidien mit einfacher Zugriffsberechtigung aufgerufen werden. Das Landeskriminalamt hat mir zugesichert, diesen Systemmangel mit der Einführung eines neuen Berechtigungskonzepts für IGVP zu beheben.

Wie ich darüber hinaus feststellen konnte, stellt das Landeskriminalamt die Lageinformationen nicht nur den Bayerischen Polizeibehörden zur Verfügung, sondern in Teilen auch Polizeibehörden anderer Bundesländer, des Bundes oder angrenzender Nachbarstaaten. Grundsätzlich können solche Datenübermittlungen nach Maßgabe des Art. 40 Abs. 1 PAG (Inland) und Art. 40 Abs. 5 PAG (Ausland) zur Erfüllung polizeilicher Aufgaben vorgenommen werden. Da diesbezüglich aber kein aussagekräftiges Übermittlungskonzept mit Benennung aller angeschriebenen Stellen und den im Einzelfall zutreffenden Übermittlungsgrundlagen bestand, habe ich das Landeskriminalamt aufgefordert, ein solches Konzept zu erstellen und der Errichtungsanordnung beizufügen. Dieses Übermittlungskonzept liegt mir inzwischen vor.

3.12 Interpolfahndung wegen angeblicher Kindesentführung

Zum Abschluss des Themenbereichs der polizeilichen Speicherungen möchte ich noch einen Fall skizzieren, der im Ausland seinen Ursprung nahm und in Folge der zunehmenden internationalen Zusammenarbeit zwischen Polizeibehörden möglicherweise auch einen Blick auf zukünftige datenschutzrechtliche Problemstellungen verdeutlicht.

Eine junge Mutter hatte sich an mich gewandt, da über sie und ihre Kinder im Internet Fahndungsnotierungen von Interpol veröffentlicht waren. Nach meinen ersten Recherchen ging der Öffentlichkeitsfahndung durch Interpol eine Aus-

schreibung amerikanischer Sicherheitsbehörden voraus. Der geschiedene Ehemann der Frau hatte dies im Rahmen eines Sorgerechtsstreits in den USA veranlasst. Ungeachtet der Tatsache, dass zuvor schon vor einem deutschen Gericht eine beiderseitig einvernehmliche Einigung über das Sorgerecht für die Kinder zugunsten der Mutter erzielt worden war, hatte der Ex-Ehemann in den USA erneut ein Sorgerechtsverfahren angestrengt.

In diesem Zusammenhang stellte Interpol Washington dann auch ein Ermittlungsersuchen auf dem üblichen Behördenweg über die Zentralstelle Lyon und das Bundeskriminalamt an die Bayerische Polizei. Die Mutter konnte die bereits beschriebene Entscheidung des hiesigen Amtsgerichts vorlegen und die zuständige Staatsanwaltschaft stellte das hier zusätzlich eingeleitete Ermittlungsverfahren zügig ein. Die anfragenden Stellen wurden hierüber wiederum auf dem dargestellten Behördenweg informiert.

Bei meiner Überprüfung zeigte sich jedoch, dass seitens des Bundeskriminalamts eine Speicherung der Frau mitsamt deren Foto und dem Hinweis „Internationale Fahndung / Rotecke“ im nationalen polizeilichen Informationssystem (INPOL) erfolgt war. Solche „Rotecke-Fahndungen“ weisen in der Regel auf internationale Haftbefehle oder Fahndungsersuchen hin. Bei einer Polizeikontrolle in Deutschland hätte dies durchaus – zumindest vorübergehend bis zur Klärung der Sachlage – zu einer Festhaltung der Frau führen können. Zudem speicherte auch die Bayerische Polizei im Kriminalaktennachweis den Hinweis auf das Vergehen der Entziehung Minderjähriger nach § 235 StGB.

Auf meine Anfrage hin, löschte die Bayerische Polizei den von ihr angelegten Datensatz umgehend.

Das Bundeskriminalamt entgegnete in der Sache hingegen, es habe grundsätzlich keine Möglichkeit, eine internationale Fahndung von Interpol-Mitgliedsstaaten zu korrigieren oder zu löschen. Die Petentin solle sich in der Angelegenheit doch an die dafür zuständige „Commission for the Control of Interpol’s Files (CCF)“ beim Generalsekretariat in Lyon wenden. Die Kontaktdaten könne sie im Internet abrufen.

Die junge Mutter hat mittlerweile mit nicht unerheblichem Aufwand eine Einstellung des in den USA eingeleiteten Strafverfahrens bewirkt. Die Interpolausschreibung wurde also letztlich aufgehoben.

Gleichwohl verdeutlicht dieser Fall sehr klar, welche Probleme Betroffenen entstehen können, wenn es aufgrund internationaler Vereinbarungen zu nationalen und internationalen Datenspeicherungen bei Sicherheitsbehörden kommt. Betroffenen und deren Kindern drohen durch die durchaus notwendige internationale Zusammenarbeit erhebliche negative Auswirkungen, die bis hin zu einer Festnahme durch die Polizei reichen können. Auch unschuldig betroffene Bürger können diese Folgen in solchen Fällen nur mit unverhältnismäßig hohem Aufwand abwenden, wenn für sie keine eindeutige nationale Stelle bei den Sicherheitsbehörden ersichtlich ist, die zentral sowohl für die nationalen als auch die internationalen Speicherungen als Ansprechpartner dient. Gerade im Rahmen der stetig wachsenden länderübergreifenden Zusammenarbeit zwischen Strafverfolgungsbehörden wird es nicht ausbleiben, dass auch solche ungewollten grenzüberschreitenden „Missverständnisse“ zwischen internationalen Polizeibehörden zunehmend zu belastenden Datenspeicherungen führen können. Im Sinne eines effektiven Grundrechtsschutzes wäre es deshalb notwendig, dass im

Rahmen der hierzu jeweils abzuschließenden internationalen Vereinbarungen auch die eben genannten Aspekte verstärkt Berücksichtigung finden.

3.13 Benachrichtigungspflicht nach verdeckten polizeilichen Maßnahmen

„Bei nicht erkennbaren Eingriffen steht dem Grundrechtsträger aufgrund der Gewährleistung effektiven Grundrechtschutzes grundsätzlich ein Anspruch auf spätere Kenntnis der staatlichen Maßnahme zu. Ohne eine solche Kenntnis können die Betroffenen weder die Unrechtmäßigkeit der Informationsgewinnung noch etwaige Rechte auf Löschung der Aufzeichnungen geltend machen." Diese Feststellung des Bundesverfassungsgerichts aus seinem Urteil zum „Großen Lauschangriff“ vom 03.03.2004 unterstreicht die Bedeutung der Benachrichtigungspflicht.

3.13.1 Benachrichtigungspflicht nach einer präventivpolizeilichen Telekommunikationsüberwachung

Die Einführung der präventivpolizeilichen Möglichkeiten für verdeckte Eingriffe in den Telekommunikationsbereich hat in den vergangenen Jahren erhebliche Diskussionen ausgelöst. Hintergrund für die Auseinandersetzung war der Umstand, dass die Eingriffsvoraussetzungen der präventiven Telekommunikationsüberwachung (TKÜ) im Vergleich zur repressiven TKÜ erheblich unbestimmter ausgestaltet sind. Ich hatte bereits bei Einführung der entsprechenden Regelungen in das Polizeiaufgabengesetz auf diese Problematik hingewiesen und davor gewarnt, dass hierbei die Gefahr einer Ausweitung der Maßnahme hin zu einem Verdachtsschöpfungsinstrument besteht.

Gerade deswegen ist auch die Beachtung der klaren Verfahrensregelungen im Polizeiaufgabengesetz von besonderer Bedeutung. Insbesondere sieht das Polizeiaufgabengesetz eine grundsätzliche Benachrichtigungspflicht der betroffenen Personen vor. Soweit die Benachrichtigung nicht spätestens binnen sechs Monaten nach Beendigung der Maßnahme erfolgt, bedarf die weitere Zurückstellung der richterlichen Zustimmung. In bestimmten Fällen kann dann mit richterlicher Zustimmung die Unterrichtung auch auf Dauer unterbleiben.

Im Gegensatz zur repressiven TKÜ steht in präventivpolizeilichen Verfahren aber die Polizei selbst und nicht die Staatsanwaltschaft in der Pflicht, die Benachrichtigung zu gewährleisten oder die richterliche Entscheidung über die (ggf. vorläufige) Nichtbenachrichtigung herbeizuführen. Bei zwei von mir geprüften Fällen musste ich leider feststellen, dass weder die Benachrichtigung noch die richterliche Zustimmung zeitgerecht veranlasst wurden. Erst auf mein Hinwirken holte der zuständige Polizeiverband die richterlichen Zustimmungen nach – in beiden Fällen mit siebenmonatiger Verspätung.

3.13.2 Benachrichtigungspflicht nach einer polizeilichen Beobachtung

In meinem letzten Tätigkeitsbericht habe ich auf die Regelung der Benachrichtigungspflicht bei einer polizeilichen Beobachtung nach Art. 36 PAG hingewiesen (siehe hierzu 24. Tätigkeitsbericht, Nr. 3.1.2). Grundsätzlich muss die Polizei demnach über eine abgeschlossene Beobachtung nach Art. 36 Abs. 5 PAG diejenige Person unterrichten, gegen die die Maßnahme gerichtet war, sowie dieje-

nigen Personen, deren personenbezogene Daten gemeldet worden sind. Die Umsetzung dieser Vorschrift in der Praxis habe ich stichprobenartig bei mehreren Polizeiverbänden überprüft. Hierbei habe ich einen Fall festgestellt, bei dem es das zuständige Polizeipräsidium versäumt hat, einen richterlichen Beschluss über die Zurückstellung der Benachrichtigung einzuholen.

Art. 36 Abs. 5 PAG (Auszug)
Von Maßnahmen nach Abs. 1 sind
1. die Personen zu unterrichten, gegen die die Maßnahme gerichtet war, sowie
2. diejenigen, deren personenbezogene Daten gemeldet worden sind.
Die Unterrichtung erfolgt, sobald dies ohne Gefährdung des Zwecks der Maßnahme oder der eingesetzten nicht offen ermittelnden Beamten geschehen kann. Ist wegen desselben Sachverhalts ein strafrechtliches Ermittlungsverfahren gegen den Betroffenen eingeleitet worden, ist die Unterrichtung in Abstimmung mit der Staatsanwaltschaft nachzuholen, sobald dies der Stand der Ermittlungen zulässt. Erfolgt die Benachrichtigung nicht binnen zwölf Monaten nach Beendigung der Maßnahme, bedarf die weitere Zurückstellung der richterlichen Zustimmung.

3.14 Nutzung sozialer Netzwerke für polizeiliche Zwecke

Mit zunehmender Nutzung sozialer Netzwerke durch Bürgerinnen und Bürger wächst bei Behörden das Interesse an den dort vorhandenen Informationen. Mit einfachen Mitteln, oft schon durch einen Blick auf das Profil, können Behörden eine ganze Reihe von Informationen über die Betroffenen erlangen. Zugleich bieten soziale Netzwerke Möglichkeiten zur Selbstdarstellung.

Die Polizei hat daher ein großes Interesse, soziale Netzwerke auch für Eigenwerbung, zur Öffentlichkeitsfahndung sowie für sonstige Ermittlungen zu nutzen. In diesem Zusammenhang hat eine Arbeitsgruppe der Bayerischen Polizei einen Bericht erarbeitet. Sie hat darin die Nutzung sozialer Netzwerke durch die Bayerische Polizei unter Berücksichtigung fachlicher, rechtlicher, organisatorischer, technischer und finanzieller Aspekte untersucht. Die Vorschläge umfassen eine Nutzung sozialer Netzwerke für die Einrichtung von sogenannten „Fanpages“ zur Öffentlichkeitsarbeit, z.B. zur Nachwuchswerbung oder zur Prävention von Straftaten. Auch eine Nutzung zur Öffentlichkeitsfahndung und zu Ermittlungszwecken wird als für die Bayerische Polizei wichtige Möglichkeit dargestellt. Ich habe zu dem Bericht Stellung genommen.

Sofern die Polizei soziale Netzwerke zu Zwecken der behördlichen Selbstdarstellung nutzen will, unterscheidet sie sich nicht von anderen Behörden. Im Einklang mit der Konferenz der Datenschutzbeauftragten des Bundes und der Länder rate ich angesichts der zahlreichen datenschutzrechtlichen Missstände bei großen Anbietern von sozialen Netzwerken dringend davon ab, Fanseiten in solchen sozialen Netzwerken einzurichten, bei denen eine datenschutzrechtskonforme Nutzung nicht sicherzustellen ist (siehe Nr. 1.3.1).

Ich verkenne nicht, dass die Ermittlungsbehörden ein legitimes Interesse an der Informationserhebung in sozialen Netzwerken haben können. Gegenüber der Polizei habe ich gleichwohl auch u.a. deutlich meine Bedenken geäußert, soziale Netzwerke privater Betreiber (wie z.B. Facebook) zu Fahnungszwecken zu nutzen. Denn durch die weltweit recherchierbare Veröffentlichung von Fahndungsdaten wird in weitaus schwerwiegenderer Weise in die Grundrechte Betroffener

(Tatverdächtige oder auch Zeugen) eingegriffen, als dies bei der Nutzung klassischer Medien der Fall ist. Dazu trägt vor allem der Umstand bei, dass die Daten nicht nur einfach recherchierbar sind, sondern mit geringem Aufwand weiter verbreitet, kopiert und auf anderen Webseiten veröffentlicht werden können. Dadurch wird eine Löschung der einmal veröffentlichten Ausschreibung wesentlich erschwert, in vielen Fällen gar unmöglich. Vor allem dann, wenn etwa gegen eine ausgeschriebene Person im Nachhinein der Tatverdacht entfällt, ist der entstandene Ansehensverlust nur schwerlich wieder auszugleichen. Eine zentrale Voraussetzung für einen Fahndungsaufruf im Internet ist daher, dass die ausschreibende Behörde als datenschutzrechtlich verantwortliche Stelle ihre Verantwortung für die Verarbeitung der Daten sowohl rechtlich als auch tatsächlich wahrnehmen kann. Aus diesem Grund sieht die Anlage B zu den Richtlinien für das Strafverfahren und das Bußgeldverfahren in Ziffer 3.2 zu Recht und ganz bewusst vor, dass private Internetanbieter grundsätzlich nicht für Fahndungsaufrufe eingeschaltet werden sollen.

RiStBV Anlage B
3.2 Nutzung des Internets
Um die Aufmerksamkeit der Internetnutzer für die Öffentlichkeitsfahndung zu erlangen, ist es zweckmäßig, die staatlichen Fahndungsaufrufe im Internet auf speziellen Seiten – etwa der Polizei – zu bündeln. Private Internetanbieter sollen grundsätzlich nicht eingeschaltet werden.

Die Öffentlichkeitsfahndung in von privaten Anbietern betriebenen sozialen Netzwerken unterscheidet sich von der Online-Fahndung auf einer polizeieigenen Homepage vor allem in dem Problem des Löschens von veralteten Aufrufen und der Protokollierung von Hinweisen, Kommentaren etc. durch den privaten Anbieter. Werden Fahndungsaufrufe der Polizei etwa auf einer Facebook-Fanpage vollständig veröffentlicht und gespeichert, muss man sich darüber im Klaren sein, dass dann auch die weitere damit verbundene Datenverarbeitung nicht mehr in der Hand der verantwortlichen Polizei liegt. Insbesondere ist die vollständige unwiederbringliche Löschung solcher Fahndungsaufrufe derzeit nicht sichergestellt. Damit ist ein zentrales Kriterium einer datenschutzkonformen Öffentlichkeitsfahndung nicht erfüllt, nämlich dass mit dem Außerkrafttreten der Anordnung auch die getroffenen Maßnahmen beendet werden.

Aus diesen Gründen halte ich eine Öffentlichkeitsfahndung, bei der Fahndungsaufrufe bei einem privaten Anbieter wie etwa Facebook gespeichert werden, aus datenschutzrechtlicher Sicht für nicht akzeptabel und eine Änderung der in der Anlage B zur RiStBV enthaltenen gemeinsamen Bekanntmachung für nicht angezeigt.

Des Weiteren habe ich das Bayerische Staatministerium des Innern darauf hingewiesen, dass ich erhebliche Bedenken habe, verdeckte Recherchen in nicht öffentlich zugänglichen Bereichen sozialer Netzwerke auf die Ermittlungsgeneralklauseln (Art. 11 PAG, §§ 161, 163 StPO) zu stützen. Verdeckte Ermittlungsmaßnahmen stellen gegenüber offenen Maßnahmen grundsätzlich einen schwerwiegenderen Grundrechtseingriff dar. Bereits aus diesem Grund ist es äußerst fraglich, ob die genannten Generalklauseln als Rechtsgrundlage für solche Recherchen in Betracht kommen. Des Weiteren werden bei derartigen Maßnahmen auch die Daten anderer Nutzer erhoben und es werden Informationen erfasst, die sich über einen langen Zeitraum erstrecken. Das Gewicht eines solchen Eingriffs kann somit sogar das einer verdeckten Telekommunikationsüberwachung erreichen oder gar übersteigen.

Vor diesem Hintergrund werde ich die Planungen der Bayerischen Polizei bzgl. der Nutzung sozialer Netzwerke weiter kritisch verfolgen.

3.15 Übergabe digitaler Datenträger durch Fundämter an die Polizei zu Testzwecken

Ein Fundamt hat sich an mich gewandt und geschildert, eine für technische Angelegenheiten zuständige Fachdienststelle der Polizei habe schriftlich um die Überlassung von digitalen Datenträgern, Mobiltelefonen und Navigationsgeräten gebeten, die weder vom Eigentümer, noch vom Finder abgeholt würden. Nach eigenen Angaben wollte die Polizei mit diesen Fundgeräten Datenausleseversuche und Tests vornehmen, um solche technischen Erkenntnisse dann in späteren Strafverfahren zu nutzen.

Da ich zu der immer relevanter werdenden Problematik des Umgangs mit Fundsachen mit digitalen Inhalten ohnehin schon in meinem 24. Tätigkeitsbericht eindeutig Stellung bezogen habe, bat ich zunächst die Polizei, die geplante Vorgehensweise zu schildern. Dabei versicherte mir die Polizei zwar, dass sie kein Interesse an den gespeicherten Daten habe, sondern lediglich an den Geräten selbst. Bislang seien solche Geräte aber teilweise in einem „ungelöschten" Zustand von verschiedenen Fundämtern übergeben worden. Die Löschung erfolge dann erst in der Polizeiwerkstatt.

Ich habe gegenüber dem Polizeipräsidium diese Vorgehensweise kritisiert. Schließlich ist zu erwarten, dass sich auf den Fundstücken Daten der früheren Eigentümer befinden. Soweit Gemeinden solche Datenträger mitsamt den darauf gespeicherten personenbezogenen Daten des ehemaligen Eigentümers herausgeben, ist dies als Datenübermittlung zu werten, für die ich hier keine Rechtsgrundlage erkennen kann. Vor der Herausgabe einer entsprechenden Fundsache an die Polizei sind daher die darauf gespeicherten personenbezogenen Daten des ehemaligen Eigentümers zu löschen.

Fehlt den Fundämtern hierzu die erforderliche Fachkenntnis, können die Gemeinden ihrer Löschpflicht beispielsweise auch durch – datenschutzkonforme – Kooperationen mit Fachfirmen nachkommen. Im datenschutzrechtlichen Sinn ist eine solche Kooperation zur Löschung der Daten als Auftragsdatenverarbeitung im Sinne des Art. 6 BayDSG zu bewerten. Der Auftragnehmer, der die Löschung tatsächlich vornimmt, muss demzufolge dafür geeignet sein. Aus technischen und organisatorischen Gesichtspunkten könnte diese Eignung sicherlich auch auf Polizeidienststellen zutreffen, wenn sich durch die erlangte Verfügungsgewalt über die Daten nicht eine Pflichtenkollision für die Polizei entwickeln würde. Per Gesetz unterliegt die Polizei dem Legalitätsprinzip, also dem Zwang ihr bekannt gewordene strafbare Handlungen weiter zu erforschen und zu verfolgen. Durch eine Löschungsanweisung der Fundämter könnte dieser gesetzliche Strafverfolgungszwang in keinem Fall wirksam eingeschränkt werden. Eine entsprechende Regelung wäre daher schon dann hinfällig, wenn auch nur die Möglichkeit des Zugriffs auf die Daten besteht – die bei der Vornahme der Datenlöschung in einer Polizeiwerkstatt ohne Zweifel gegeben ist. Das betreffende Polizeipräsidium hat mir inzwischen zugesichert, es werde keine Datenträger von Fundbehörden mehr entgegennehmen, deren Daten nicht zuvor gelöscht worden seien.

3.16 Pressearbeit der Polizei

Die Grundsätze zur datenschutzkonformen Pressearbeit der Polizei habe ich in meinem letzten Tätigkeitsbericht geschildert (siehe hierzu 24. Tätigkeitsbericht, Nr. 3.6). Dort habe ich auch angekündigt, auf eine landesweit einheitliche Handhabung der polizeilichen Berichterstattung hinzuwirken.

Im Berichtszeitraum hat sich die polizeiliche Berichterstattung gegenüber der Presse aus meiner Sicht im Grundsatz positiv entwickelt. Es wird von der Presse zwar nicht immer gutgeheißen, wenn die Polizei mit Hinweis auf den Datenschutz weniger Angaben über einzelne Vorfälle macht. Diese datenschutzfreundliche Vorgehensweise der Polizei entspricht aber meinen Empfehlungen und wird deshalb von mir ausdrücklich positiv bewertet.

Nur in einzelnen Fällen habe ich im Rahmen meiner Kontrollen festgestellt, dass die Polizei im Rahmen ihrer Pressearbeit datenschutzrechtliche Regelungen nicht ausreichend beachtet hat:

Zur Pressearbeit zählt nicht nur die regelmäßige Herausgabe von Pressemitteilungen, sondern auch die Auskunftserteilung an die Presse, z.B. bei Nachfragen durch Journalisten. Hierzu habe ich auch in diesem Berichtszeitraum der Polizei gegenüber betont, dass ich auch die Bestätigung bereits allgemein bekannter Tatsachen als eine Datenübermittlung ansehe, die ihrerseits wieder eine Rechtsgrundlage benötigt. So war dies der Fall, als die Polizei auf Nachfrage eines Journalisten bestätigte, dass es sich bei der in der Öffentlichkeit randalierenden Person um einen Prominenten handelte. Erst durch diese Bestätigung erlangt die Nachricht eine amtliche Autorisierung und damit eine Qualitätssteigerung.

In Bezug auf einen schweren Unfall gab die Polizei aus generalpräventiven Erwägungen ein Foto der Unfallstelle an die Medien, auf dem noch das Kennzeichen des Fahrzeugs ersichtlich war. Das betroffene Polizeipräsidium teilte mir auf meine Anfrage mit, dass man ebenfalls der Ansicht sei, dass die Herausgabe des Fotos ohne Anonymisierung nicht zu rechtfertigen sei und sicherte mir zu, die Dienststellen bezüglich dieses Themas zu sensibilisieren.

Aufgrund weiterer Einzelfälle sah ich mich außerdem veranlasst, die Polizei darauf aufmerksam zu machen, dass durch die Summe der in einer Pressemitteilung enthaltenen personenbezogenen Daten für das soziale Umfeld kein Rückschluss auf die betroffene Person ermöglicht werden darf. Gerade die Erkennbarkeit im sozialen Umfeld wird von den betroffenen Bürgern als besonders gravierend empfunden.

Aufgrund der erheblichen Bedeutung dieses Themas für die Betroffenen, werde ich die Pressearbeit der Polizei auch weiterhin kritisch beobachten.

3.17 Broschüre „Datenschutz bei der Polizei“

„Wann und wie lange darf die Polizei Daten über mich speichern?“ „Wie erfahre ich, ob und welche Daten die Polizei über mich gespeichert hat?“ „Bei wem kann ich die Löschung gespeicherter Daten beantragen?“ Solche und ähnliche für den Betroffenen wichtige Fragen erreichen mich immer wieder. Mir ist es daher ein Anliegen, die bayerischen Bürgerinnen und Bürger auch über das Thema „Datenschutz bei der Polizei“ in allgemein verständlicher Weise zu informieren. Aus

diesem Grund habe ich im Berichtszeitraum neben den Broschüren „Datenschutz im Rathaus“ und „Datenschutz in der Schule“ auch für diesen Bereich ein Informationsheft veröffentlicht. Mein besonderer Dank gilt an dieser Stelle dem Bayerischen Staatsministerium der Justiz und für Verbraucherschutz sowie dem Bayerischen Staatsministerium des Innern, die sich bereit erklärt haben, die Broschüre in Gerichtsgebäuden und Polizeidienststellen auszulegen. Selbstverständlich kann die Broschüre aber auch von meiner Homepage heruntergeladen oder über meine Geschäftsstelle kostenfrei bestellt werden.

4 Verfassungsschutz

Auch in diesem Berichtszeitraum habe ich sowohl anlassunabhängig, als auch aufgrund von Eingaben, beim Landesamt für Verfassungsschutz datenschutzrechtliche Prüfungen vorgenommen. Insbesondere habe ich mich dabei mit dem Dokumentenmanagementsystem, der Auskunftserteilungspraxis sowie mit Speicherungen im Zusammenhang mit Demonstrationen gegen das Versammlungsgesetz beschäftigt.

4.1 Allgemeines

Mit einer Entschließung forderte die Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 28./29.09.2011 eine unabhängige Prüfung der Antiterrorgesetze in Deutschland. Insbesondere seien die Auswirkungen der bestehenden Sicherheitsgesetze – gerade in ihrem Zusammenwirken – durch eine unabhängige wissenschaftliche Evaluierung zu untersuchen. Die Wirksamkeit der Regelungen, ihre Erforderlichkeit für den gesetzgeberischen Zweck und ihre Angemessenheit, insbesondere im Hinblick auf die Bedrohungslage sowie die Auswirkungen für die Betroffenen sollten vor einer weiteren Befristung kritisch überprüft werden.

Entschließung der 82. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 28./29.09.2011
Antiterrorgesetze zehn Jahre nach 9/11 – Überwachung ohne Überblick

In der Folge der Anschläge vom 11.09.2001 wurden der Polizei, den Strafverfolgungsbehörden und den Nachrichtendiensten zahlreiche neue Befugnisse eingeräumt, die sich durch eine große Streubreite auszeichnen und in die Grundrechte zahlreicher Bürgerinnen und Bürger eingreifen. Zunehmend werden Menschen erfasst, die nicht im Verdacht stehen, eine Straftat begangen zu haben oder von denen keine konkrete Gefahr ausgeht. Unbescholtene geraten so verstärkt in das Visier der Behörden und müssen zum Teil weitergehende Maßnahmen erdulden. Wer sich im Umfeld von Verdächtigen bewegt, kann bereits erfasst sein, ohne von einem Terrorhintergrund oder Verdacht zu wissen oder in entsprechende Aktivitäten einbezogen zu sein.

Zunehmend werden Daten, z.B. über Flugpassagiere und Finanztransaktionen, in das Ausland übermittelt, ohne dass hinreichend geklärt ist, was mit diesen Daten anschließend geschieht (vgl. dazu Entschließung der 67. Konferenz vom 25./26.03.2004 „Übermittlung von Flugpassagierdaten an die US-Behörden"; Entschließung der 78. Konferenz vom 08./09.10.2009 „Kein Ausverkauf von europäischen Finanzdaten an die USA!").

Das Bundesverfassungsgericht hat in seinem Urteil zur Vorratsdatenspeicherung von Telekommunikationsdaten vom 02.03.2010 (1 BvR 256/08) klargestellt: Es gehört zur verfassungsrechtlichen Identität der Bundesrepublik Deutschland, dass die Freiheitswahrnehmung der Bürgerinnen und Bürger nicht total erfasst und registriert werden darf. Die Verfassung fordert vielmehr ein austariertes System, bei dem jeder Eingriff in die Freiheitsrechte einer strikten Prüfung seiner Verhältnismäßigkeit standhält.

Von einem austarierten System der Eingriffsbefugnisse kann schon deshalb keine Rede sein, weil die Wechselwirkungen zwischen den verschiedenen Eingriffsinstrumentarien nie systematisch untersucht worden sind. Bundesregierung und Gesetzgeber haben bislang keine empirisch fundierten Aussagen vorgelegt, zu welchem Überwachungs-Gesamtergebnis die verschiedenen Befugnisse in ihrem Zusammenwirken führen. Die bislang nur in einem Eckpunktepapier angekündigte Regierungskommission zur Überprüfung der Sicherheitsgesetze ersetzt die erforderliche unabhängige wissenschaftliche Evaluation nicht.

Viele zunächst unter Zeitdruck erlassene Antiterrorgesetze waren befristet worden, um sie durch eine unabhängige Evaluation auf den Prüfstand stellen zu können. Eine derartige umfassende, unabhängige Evaluation hat jedoch nicht stattgefunden. Dies hat die Bundesregierung nicht davon abgehalten, gleichwohl einen Entwurf für die Verlängerung und Erweiterung eines der Antiterrorpakete in den Gesetzgebungsprozess einzubringen (BT-Drs. 17/6925).

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder fordert daher erneut, die Auswirkungen der bestehenden Sicherheitsgesetze – gerade in ihrem Zusammenwirken – durch eine unabhängige wissenschaftliche Evaluierung (so bereits die Entschließung der 79. Konferenz vom 17./18.03.2010 „Für eine umfassende wissenschaftliche Evaluierung im Sicherheitsbereich") zu untersuchen. Die Wirksamkeit der Regelungen, ihre Erforderlichkeit für den gesetzgeberischen Zweck und ihre Angemessenheit, insbesondere im Hinblick auf die Bedrohungslage sowie die Auswirkungen für die Betroffenen müssen vor einer weiteren Befristung endlich kritisch überprüft werden.

Im Rahmen einer Änderung des Bundesverfassungsschutzgesetzes kam die Überlegung auf, auch den Landesverfassungsschutzbehörden eine Kontostammdatenabfrage beim Bundeszentralamt für Steuern zu ermöglichen. Ich habe gegenüber dem Bayerischen Staatsministerium des Innern darauf hingewiesen, dass ich es aus datenschutzrechtlicher Sicht ablehne, dem Bayerischen Landesamt für Verfassungsschutz eine solche Befugnis einzuräumen. Die Möglichkeit des Abrufs von Kontostammdaten wurde in den letzten Jahren kontinuierlich ausgebaut, so dass sich mittlerweile Finanz-, Strafverfolgungs- und Sozialbehörden Kenntnis über das Bestehen von Konten und Depots verschaffen können. Wird diese Möglichkeit nun auch noch den Verfassungsschutzbehörden der Länder eingeräumt, so stellt dies eine datenschutzrechtlich problematische Ausweitung der Zwecke dar, zu denen die Kontostammdaten ursprünglich vorrätig gehalten wurden. Auch bestätigen sich damit Befürchtungen, dass die Einführung neuer Dateien Begehrlichkeiten weckt und der Kreis der Zugriffsberechtigten im Lauf der Zeit regelmäßig erweitert wird. Die Ermittlungen über Kontostammdaten können Maßnahmen vorbereiten, die ohne die erlangten Kenntnisse nicht ohne weiteres möglich sind und die die Belange der Betroffenen erheblich berühren. Kontenabrufe können damit Grundrechtseingriffe von großem Gewicht nach sich ziehen. Dies gilt umso mehr, wenn es sich um Ermittlungen durch Nachrichtendienste handelt, die sich typischerweise weit im Vorfeld des Verdachts kriminellen Handelns bewegen. Insbesondere das Argument, ein Abruf der Kontostammdaten wäre der mildere Eingriff gegenüber der Ermittlung der kontoführenden Kreditinstitute mit nachrichtendienstlichen Mitteln, verfängt in diesem Zusammenhang nicht. Entscheidend ist hier aus meiner Sicht, dass die rechtstaatlichen Sicherungen beim Einsatz dieser Maßnahme nicht in der erforderlichen Weise geregelt sind. Die angedachte Ergänzung des Bundesverfassungsschutzgesetzes wurde im Ergebnis nicht verabschiedet.

4.2 Neues Dokumentenmanagementsystem beim LfV

Mit Einführung des neuen Dokumentenmanagementsystems DMS steuert das Landesamt für Verfassungsschutz nun auf eine überwiegend „papierlose" Sach- und Vorgangsbearbeitung zu. Dem neuen Dateisystem obliegt dabei nunmehr nicht nur die recherchierbare Ablage von Dokumenten, sondern insbesondere auch die gesamte papierlose elektronische Vorgangsbearbeitung. Aus datenschutzrechtlicher Sicht bedingt dies beispielsweise, dass innerhalb der generierten Arbeitsabläufe, Vorgangsverknüpfungen oder durch Bearbeitungsvermerke – neben den „eigentlichen Dokumenten" und den dazu erfassten Metadaten – eine Vielzahl weiterer Speicherungen innerhalb des Verfahrens entstehen. Das Landesamt für Verfassungsschutz hat mir bereits frühzeitig den Entwurf einer Errichtungsanordnung für das Verfahren zugeleitet, zu dem ich aus dem vorgenannten Grund eine ganze Reihe von Veränderungsvorschlägen angemerkt habe.

Insbesondere muss in einem so umfassenden System, das Daten sowohl für die Fachaufgabenerfüllung des Verfassungsschutzes als auch zur reinen Vorgangsverwaltung vereint, hinsichtlich des jeweiligen Speicherungszwecks eine deutliche Trennung in den angewandten Überprüfungs- und Speicherungsfristen gewährleisten sein. Bei Dokumenten, die nach den gesetzlichen Vorschriften zur Aufgabenerfüllung des Verfassungsschutzes im Informationssystem für die Beschaffung und Auswertung (IBA) oder im Nachrichtendienstlichen Informationssystem (NADIS) gespeichert werden können, muss sich die zulässige Frist grundsätzlich an den dort vorgegebenen Fristen orientieren.

Für die Löschung der Daten, die ausschließlich im Rahmen der Vorgangsverwaltung und Vorgangsbearbeitung gespeichert werden, sind hingegen kürzere und den jeweiligen Umständen angepasste Fristen festzulegen. Bei meiner Vorortprüfung im Landesamt für Verfassungsschutz konnte ich bei mehreren Speicherungen feststellen, dass von Seiten des Systems teilweise eine Speicherdauer von 99 Jahren automatisch festgelegt war. Auch wenn neben der festgelegten Speicherdauer beispielsweise Wiedervorlagefristen zu einer früheren bzw. rechtzeitigen Löschung der Vorgänge beitragen können, halte ich diese systemseitige Frist aus datenschutzrechtlicher Sicht für problematisch. Ändert bzw. verkürzt der Sachbearbeiter diese im Rahmen der Wiedervorlage nicht, erfolgt auch keine frühere Löschung. Ich habe daher das Landesamt für Verfassungsschutz aufgefordert – ähnlich der Regelungen für die polizeiliche Vorgangsverwaltung – je nach Vorgangsrelevanz abgestufte Speicherfristen für „Verwaltungsvorgänge" festzulegen und gleichzeitig auch entsprechende technische Vorkehrungen zu treffen, welche die Festsetzung dieser Fristen gewährleisten. Eine nähere Erörterung meiner Prüfungsfeststellungen mit dem Landesamt für Verfassungsschutz steht noch aus.

Neben dieser Thematik werde ich mich bei dem neuen System weiterhin auch für die Realisierung einer technischen Protokollierungsdatei einsetzen, die eine tatsächliche datenschutzrechtliche Kontrolle erlaubt. Auch hierzu dauern meine Gespräche mit dem Landesamt für Verfassungsschutz noch an.

4.3 Speicherungen von Versammlungsteilnehmern

Für meine Prüfung von Personenspeicherungen beim Landesamt für Verfassungsschutz habe ich diesmal das Thema Versammlungsteilnehmer ausgewählt.

Zunächst lies ich mir eine Liste aller Veranstaltungen eines bestimmten Zeitraumes und Themenbereiches vorlegen, zu denen beim Landesamt für Verfassungsschutz Personendaten gespeichert sind. Aus dieser Aufstellung habe ich mehrere Veranstaltungen für meine Prüfung ausgewählt. Die Speicherungen wurden dann stichprobenartig vor Ort hinsichtlich ihrer Plausibilität und der rechtlichen Zulässigkeit geprüft. Bei allen geprüften Personenspeicherungen konnten den Dateien hinreichend konkrete Anhaltspunkte entnommen werden, die eine Speicherung im Sinne des BayVSG und der darauf aufbauenden Arbeitsanweisung für die Speicherung und Löschung personenbezogener Daten zur Extremismusbeobachtung zulässig erscheinen lassen. Alle geprüften Speicherungen waren jeweils mit mehreren Dokumenten hinterlegt, aufgrund derer die Einschätzung des Verfassungsschutzes über die Betroffenen als Funktionäre, informelle Führer oder Aktivisten einer extremistischen oder extremistisch beeinflussten Gruppenbestrebung plausibel erschienen. Neben der Kontrolle der Speicherungsvoraussetzungen konnte ich mich hierbei auch davon überzeugen, dass in diesen Prüffällen auch die jeweils festgesetzten Speicherungs- bzw. Wiedervorlagefristen entsprechend der vorgegebenen Arbeitsanweisungen korrekt vergeben waren. Offensichtliche Speicherungsfehler konnte ich dabei nicht erkennen.

4.4 Überprüfung einzelner Auskunftserteilungen

Wie schon anlässlich früherer Prüfungen habe ich auch diesmal Auskunftserteilungen des Landesamtes für Verfassungsschutz auf deren Vollständigkeit überprüft. Soweit trotz dargelegtem besonderen Auskunftsinteresses den Betroffenen keine Auskunft erteilt wurde, habe ich auch geprüft, ob ein hinreichender Unterlassungsgrund im Sinne des Art. 11 Abs. 3 BayVSG vorgelegen hat.

Hierbei fiel mir auf, dass Speicherungen im neuen Dokumentenmanagementsystem des Landesamtes für Verfassungsschutz, die nicht der Fachaufgabenerfüllung im Sinne des Art. 3 BayVSG, sondern reinen Verwaltungsangelegenheiten zuzurechnen sind, in den Auskunftsschreiben nicht erwähnt waren. Nicht in die Auskunft aufgenommen wurden beispielsweise allgemeine Anfragen der Betroffenen an das Landesamt oder Anforderungen von Verfassungsschutzberichten und die zugehörigen Antworten. Ergänzend zu meinen Ausführungen unter dem Thema „neues Dokumentenmanagementsystem“, in dem ich für solche Speicherungen möglichst kurze Löschungsfristen fordere, erachte ich aus datenschutzrechtlicher Sicht auch für solche Speicherungen einen Auskunftsanspruch des Betroffenen als gegeben. Art. 11 Abs. 1 BayVSG unterscheidet in der dort festgelegten Auskunftsverpflichtung – bei ausreichend dargelegtem besonderen Interesse – nicht zwischen personenbezogenen Daten, die der Erfüllung der Aufgaben des LfV dienen und sonstigen Vorgängen, in denen personenbezogene Daten der Antragsteller gespeichert sind. Mein diesbezüglicher Dialog mit dem Landesamt für Verfassungsschutz ist noch nicht abgeschlossen.

Art 11 BayVSG Auskunftserteilung
(1) [1]Das Landesamt für Verfassungsschutz erteilt dem Betroffenen auf Antrag kostenfrei Auskunft über die zu seiner Person in Dateien oder Akten gespeicherten Daten. [2]Die Auskunftsverpflichtung besteht nur, soweit der Betroffene ein besonderes Interesse an einer Auskunft darlegt. [3]Sie erstreckt sich nicht auf die Herkunft der Daten und die Empfänger von Übermittlungen. [4]Das Landesamt für Verfassungsschutz bestimmt das Verfahren, insbesondere die Form der Auskunftserteilung, nach pflichtgemäßem Ermessen.

(2) Soweit eine Person einer Sicherheitsüberprüfung nach Art. 3 Abs. 2 unterzogen wird oder zu einer Person Auskunft nach Art. 3 Abs. 3 Nr. 1 erteilt wird, hat diese Person abweichend von Absatz 1 einen Anspruch auf Auskunft über die Daten des Landesamts für Verfassungsschutz, die es im Rahmen der Erfüllung dieser Aufgaben übermittelt hat.

(3) Die Auskunftserteilung unterbleibt, soweit

1. *eine Gefährdung der Erfüllung der Aufgaben nach Art. 3 durch die Auskunftserteilung zu besorgen ist,*
2. *durch die Auskunftserteilung nachrichtendienstliche Zugänge gefährdet sein können oder die Ausforschung des Erkenntnisstandes oder der Arbeitsweise des Landesamts für Verfassungsschutz zu befürchten ist,*
3. *die Auskunft die öffentliche Sicherheit gefährden oder sonst dem Wohl des Bundes oder eines Landes Nachteile bereiten würde oder*
4. *die Information oder die Tatsache der Speicherung nach einer Rechtsvorschrift oder ihrem Wesen nach, insbesondere wegen der überwiegenden berechtigten Interessen eines Dritten, geheimgehalten werden muss.*

(4) [1]Die Ablehnung der Auskunftserteilung bedarf keiner Begründung. [2]Wird die Auskunftserteilung abgelehnt, ist der Betroffene auf die Rechtsgrundlage für das Fehlen der Begründung und darauf hinzuweisen, dass er sich hinsichtlich der Verarbeitung personenbezogener Daten an den Landesbeauftragten für den Datenschutz wenden kann. [3]Dem Landesbeauftragten für den Datenschutz ist auf sein Verlangen Auskunft zu erteilen, soweit nicht das Staatsministerium des Innern im Einzelfall feststellt, dass dadurch die Sicherheit des Bundes oder eines Landes gefährdet würde. [4]Mitteilungen des Landesbeauftragten an den Betroffenen dürfen keine Rückschlüsse auf den Kenntnisstand des Landesamts für Verfassungsschutz zulassen, sofern dieses nicht einer weitergehenden Auskunft zustimmt.

5 Justiz

Meine Tätigkeit im Bereich Justiz war im Berichtszeitraum von den Erkenntnissen im Zusammenhang mit der Aufdeckung des sog. „Staats-Trojaners“ durch den Chaos-Computer-Club geprägt. Nachdem sich kurze Zeit nach der Veröffentlichung des Chaos-Computer-Clubs herausgestellt hatte, dass es sich hierbei um eine Software handelt, die vom Bayerischen Landeskriminalamt im Rahmen der Durchführung einer Quellen-Telekommunikationsüberwachung eingesetzt worden war, nahm ich eine umfassende Prüfung in diesem Bereich vor. Hierbei habe ich die Einhaltung der rechtlichen Vorgaben und technischen Vorkehrungen bei den durch bayerische Behörden durchgeführten Maßnahmen im Rahmen der Quellen-Telekommunikationsüberwachung überprüft. Über das Ergebnis meiner Überprüfung habe ich die Öffentlichkeit am 02.08.2012 informiert und hierzu auch meinen Prüfungsbericht veröffentlicht (im Internet abrufbar unter www.datenschutz-bayern.de/0/bericht-qtkue.pdf).

Darüber hinaus habe ich eine bayerische Justizvollzugsanstalt umfassend und insgesamt 10 bayerische Justizbehörden hinsichtlich des Vorhandenseins und der Stellung des behördlichen bzw. gerichtlichen Datenschutzbeauftragten, sowie dessen Darstellung im Geschäftsverteilungsplan und im Telefonverzeichnis überprüft. In diesem Zusammenhang ist es mir aus datenschutzrechtlicher Sicht besonders wichtig, dass dem Recht suchenden Bürger bei sämtlichen bayerischen Justizbehörden die Person und Erreichbarkeit des behördlichen bzw. gerichtlichen Datenschutzbeauftragten unmittelbar benannt werden kann.

Neben diesen anlassunabhängigen Prüfungen habe ich anlassbezogen aufgrund von Bürgereingaben auch Prüfungen konkreter Einzelfälle vorgenommen. Bei Gesetzentwürfen, Verordnungsentwürfen und Bekanntmachungsentwürfen habe ich auf die Umsetzung datenschutzrechtlicher Anforderungen hingewirkt.

Die nachfolgenden Darstellungen sind eine Auswahl meiner Feststellungen im Justizbereich.

5.1 Gesetze und Rechtsverordnungen

5.1.1 Allgemeines

Im Berichtszeitraum habe ich zu verschiedenen Gesetzes- und Verordnungsentwürfen (etwa zum Bayerischen Sicherungsverwahrungsvollzugsgesetz) Stellung genommen. Dabei konnte ich zahlreiche datenschutzrechtliche Verbesserungen anregen.

Bereits in den letzten beiden Tätigkeitsberichten habe ich eine normenklare Rechtsgrundlage für die Durchführung des Maßregelvollzugs in Bayern angemahnt. Ein Bayerisches Maßregelvollzugsgesetz, zu dessen Entwurf ich in der Vergangenheit bereits Stellung genommen hatte, ist bedauerlicherweise gleichwohl im Berichtszeitraum nicht verabschiedet worden.

5.1.2 Schaffung einer Rechtsgrundlage zur Übermittlung von Grundbuchdaten zur Entwicklung eines Migrationprogramms

Seitens des Bayerischen Staatsministeriums der Justiz und für Verbraucherschutz wurde mir mitgeteilt, dass die Umstellung sämtlicher Grundbücher in eine Grundbuchdatenbank (elektronisches Grundbuch) geplant sei. In diesem Zusammenhang solle eine Software (Migrationsprogramm) entwickelt werden, die in der Lage sei, den Inhalt sämtlicher Grundbücher in Deutschland zu erfassen und zu digitalisieren. Zur Entwicklung dieser Software sollten Originalgrundbücher an die Herstellerfirma übermittelt werden.

Ich wies das hier federführende Bayerische Staatsministerium der Justiz und für Verbraucherschutz darauf hin, dass eine Überlassung von Originalgrundbüchern nur aufgrund einer gesetzlichen Rechtsgrundlage möglich wäre, die jedoch seinerzeit nicht vorhanden war. Das Bayerische Staatsministerium der Justiz und für Verbraucherschutz hat meine datenschutzrechtlichen Bedenken aufgegriffen und gegenüber dem Bundesministerium der Justiz darauf hingewirkt, dass auf Bundesebene eine Regelung in Form des § 134 a Grundbuchordnung (GBO) durch den Gesetzgeber geschaffen wurde.

§ 134 a GBO
(1) Die Landesjustizverwaltungen können dem Entwickler eines automatisierten optischen Zeichen- und Inhaltserkennungsverfahrens (Migrationsprogramm) nach Maßgabe der Absätze 2 bis 5 Grundbuchdaten zur Verfügung stellen; im Übrigen gelten das Bundesdatenschutzgesetz und die Datenschutzgesetze der Länder. Das Migrationsprogramm soll bei der Einführung eines Grundbuchs, das in strukturierter Form mit logischer Verknüpfung der Inhalte geführt wird (Datenbankgrundbuch), die Umwandlung der Grundbuchdaten in voll strukturierte Eintragungen sowie deren Speicherung unterstützen.
(2) Der Entwickler des Migrationsprogramms darf die ihm übermittelten Grundbuchdaten ausschließlich für die Entwicklung und den Test des Migrationsprogramms verwenden. Die Übermittlung der Daten an den Entwickler erfolgt zentral über eine durch Verwaltungsabkommen der Länder bestimmte Landesjustizverwaltung. Die beteiligten Stellen haben dem jeweiligen Stand der Technik entsprechende Maßnahmen zur Sicherstellung von Datenschutz und Datensicherheit zu treffen, insbesondere zur Wahrung der Vertraulichkeit der betroffenen Daten. Die nach Satz 2 bestimmte Landesjustizverwaltung ist für die Einhaltung der Vorschriften des Datenschutzes verantwortlich und vereinbart mit dem Entwickler die Einzelheiten der Datenverarbeitung.
(3) Die Auswahl der zu übermittelnden Grundbuchdaten erfolgt durch die Landesjustizverwaltungen. Ihr ist ein inhaltlich repräsentativer Querschnitt des Grundbuchdatenbestands zugrunde zu legen. Im Übrigen erfolgt die Auswahl nach formalen Kriterien. Dazu zählen insbesondere die für die Grundbucheintragungen verwendeten Schriftarten und Schriftbilder, die Gliederung der Grundbuchblätter, die Darstellungsqualität der durch Umstellung erzeugten Grundbuchinhalte sowie das Dateiformat der umzuwandelnden Daten. Es dürfen nur so viele Daten übermittelt werden, wie für die Entwicklung und den Test des Migrationsprogramms notwendig sind, je Land höchstens 5 Prozent des jeweiligen Gesamtbestands an Grundbuchblättern.
(4) Der Entwickler des Migrationsprogramms kann die von ihm gespeicherten Grundbuchdaten sowie die daraus abgeleiteten Daten der nach Absatz 2 Satz 2 bestimmten Landesjustizverwaltung oder den jeweils betroffenen Landesjustizverwaltungen übermitteln. Dort dürfen die Daten nur für Funktionstests des Migrationsprogramms sowie für die Prüfung und Geltendmachung von Gewähr-

leistungsansprüchen in Bezug auf das Migrationsprogramm verwendet werden; die Daten sind dort zu löschen, wenn sie dafür nicht mehr erforderlich sind.
(5) Der Entwickler des Migrationsprogramms hat die von ihm gespeicherten Grundbuchdaten sowie die daraus abgeleiteten Daten zu löschen, sobald ihre Kenntnis für die Erfüllung der in Absatz 2 Satz 1 genannten Zwecke nicht mehr erforderlich ist. An die Stelle einer Löschung tritt eine Sperrung, soweit und solange die Kenntnis der in Satz 1 bezeichneten Daten für die Abwehr von Gewährleistungsansprüchen der Landesjustizverwaltungen erforderlich ist. Ihm überlassene Datenträger hat der Entwickler der übermittelnden Stelle zurückzugeben.
(6) Für den im Rahmen der Konzeptionierung eines Datenbankgrundbuchs zu erstellenden Prototypen eines Migrationsprogramms mit eingeschränkter Funktionalität gelten die Absätze 1 bis 5 entsprechend.

5.1.3 Staatsvertrag und Verwaltungsvereinbarung zur elektronischen Aufenthaltsüberwachung

Der Bundesgesetzgeber hat mit der Neuregelung des § 68 b Abs. 1 Satz 1 Nr. 12 Strafgesetzbuch (StGB) den Gerichten die Möglichkeit eingeräumt, eine verurteilte Person für die Dauer der Führungsaufsicht oder für eine kürzere Zeit anzuweisen, die für eine elektronische Überwachung ihres Aufenthaltsortes erforderlichen technischen Mittel ständig in betriebsbereitem Zustand bei sich zu führen und deren Funktionsfähigkeit nicht zu beeinträchtigen (elektronische Aufenthaltsüberwachung).

§ 68 b Abs. 1 Satz 1 Nr. 12 StGB
Das Gericht kann die verurteilte Person für die Dauer der Führungsaufsicht oder für eine kürzere Zeit anweisen, …
Nr. 12 die für eine elektronische Überwachung ihres Aufenthaltsortes erforderlichen technischen Mittel ständig in betriebsbereitem Zustand bei sich zu führen und deren Funktionsfähigkeit nicht zu beeinträchtigen.

Alle Bundesländer haben sich entschlossen, zur Durchführung dieser elektronischen Aufenthaltsüberwachung eine einheitliche Infrastruktur zu schaffen. Insbesondere wurde die fachliche Überwachung der Delinquenten der neu gegründeten Gemeinsamen elektronischen Überwachungsstelle der Länder (GÜL) in Bad Vilbel (Hessen) übertragen. Die Gründung und den Betrieb der GÜL haben die beteiligten Bundesländer durch einen Staatsvertrag geregelt, dem zwischenzeitlich fast alle Bundesländer beigetreten sind. Daneben hat auf der Grundlage einer Verwaltungsvereinbarung der Bundesländer mit Hessen die Hessische Zentrale für Datenverarbeitung (HZD) in Hünefeld den Betrieb der technischen Überwachungszentrale und alle mit der Beschaffung, Anlegung und Wartung der Überwachungsgeräte verbundenen Aufgaben übernommen.

Durch das Bayerische Staatsministerium der Justiz und für Verbraucherschutz bin ich hinsichtlich beider Rechtsakte eingebunden worden. Aus datenschutzrechtlicher Sicht konnte ich hier kurzfristig einige datenschutzrechtliche Verbesserungen erreichen. So wurde etwa in dem Staatsvertrag klargestellt, dass, sofern private Dritte in den Prozess einbezogen werden (etwa um das Überwachungsgerät zu warten), dies diskriminierungsfrei geschehen muss. Dazu gehört beispielsweise, dass Mitarbeiter mit neutralen Fahrzeugen beim Delinquenten vorfahren. Weiterhin konnte ich erreichen, dass in dem Staatsvertrag die Daten-

schutzkontrolle ausdrücklich geregelt wird. Grundsätzlich ist diese danach dem Hessischen Datenschutzbeauftragten übertragen.

5.1.4 Online-Zugriffe auf das elektronische Schuldnerverzeichnis

Mit dem Gesetz zur Reform der Sachaufklärung in der Zwangsvollsteckung aus dem Jahr 2009 wurden die rechtlichen Voraussetzungen dafür geschaffen, dass der Inhalt des Schuldnerverzeichnisses ab dem 01.01.2013 über eine zentrale und länderübergreifende Abfrage im Internet eingesehen werden kann. Die Ausgestaltung der damit wesentlich erleichterten Einsicht wird vom Bundesministerium der Justiz durch Rechtsverordnung im Einzelnen geregelt.

Ein erster Entwurf dieser Schuldnerverzeichnisführungsverordnung (SchuFV) begegnete großen datenschutzrechtlichen Bedenken. Der Entwurf sah etwa vor, dass bereits nach Eingabe eines Nachnamens und des zuständigen Vollstreckungsgerichts eine Ergebnisliste mit allen Personen angezeigt wird, auf die diese beiden Kriterien zutreffen. Da Vollstreckungsgerichte jeweils zentral für ein Bundesland eingerichtet sind, hätte die anfragende Person bei einer Vielzahl von zu erwartenden Namensgleichheiten auch Auskunft über Schuldner erhalten, deren Kenntnis sie nicht benötigt.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat daher mit Entschließung vom 07.02.2012 gefordert, dass bei der Regelung der Einsicht in das Schuldnerverzeichnis die zwingende Angabe weiterer Identifizierungsmerkmale vorzusehen ist.

Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 07.02.2012
Schuldnerverzeichnis im Internet: Anzeige von Schuldnerdaten nur im Rahmen der gesetzlich legitimierten Zwecke

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder fordert das Bundesministerium der Justiz auf, für einen besseren Datenschutz bei der geplanten Internetabfrage aus dem Schuldnerverzeichnis Sorge zu tragen. Es sollen möglichst nur diejenigen Personen angezeigt werden, auf die sich der Abfragezweck bezieht.

Wer eine Wohnung vermieten oder einen Ratenkredit einräumen will, möchte wissen, ob sein zukünftiger Schuldner Zahlungsschwierigkeiten hat. Er hat unter bestimmten Voraussetzungen ein legitimes Interesse an der Einsicht in das von den zentralen Vollstreckungsgerichten geführte Schuldnerverzeichnis. So können sich mögliche Geschäftspartner darüber informieren, ob ihr Gegenüber in wirtschaftliche Not geraten ist.

Mit dem Gesetz zur Reform der Sachaufklärung in der Zwangsvollstreckung aus dem Jahr 2009 will der Gesetzgeber die Stellung des Gläubigers stärken. Das Gesetz sieht unter anderem vor, dass der Inhalt des Schuldnerverzeichnisses ab dem 01.01.2013 über eine zentrale und länderübergreifende Abfrage im Internet eingesehen werden kann. Die Ausgestaltung der damit wesentlich erleichterten Einsicht wird derzeit vom Bundesministerium der Justiz durch eine Rechtsverordnung im Einzelnen vorbereitet.

Die gesetzliche Regelung erlaubt Privatpersonen die Einsicht in das Schuldnerverzeichnis nur für bestimmte Zwecke, die bei einer Anfrage darzulegen sind, zum Beispiel, um wirtschaftliche Nachteile abzuwenden, die daraus entstehen können, dass Schuldner ihren Zahlungsverpflichtungen nicht nachkommen. Dennoch ist es derzeit vorgesehen, dass bereits nach Eingabe eines Nachnamens und des zuständigen Vollstreckungsgerichts eine Ergebnisliste mit allen Personen angezeigt wird, auf die diese beiden Kriterien zutreffen. Da Vollstreckungsgerichte jeweils zentral für ein Bundesland eingerichtet sind, erhielte die anfragende Person bei einer Vielzahl von zu erwartenden Namensgleichheiten auch Einsicht zu Angaben über Schuldner, deren Kenntnis sie zum angestrebten Zweck nicht benötigt.

Es ist zu befürchten, dass beispielsweise Vermieter Mietinteressenten nicht berücksichtigen, weil im Schuldnerverzeichnis namensgleiche Personen stehen und es ihnen zu mühsam oder zu schwierig erscheint, anhand weiterer Angaben zu prüfen, ob es sich beim Mietinteressenten tatsächlich um eine der eingetragenen Personen handelt. Auch aus der Sicht der Gläubiger ist die Anzeige von derart umfangreichen Ergebnislisten wenig hilfreich, denn um den auf die Anfrage bezogenen Datensatz aus der Liste auswählen zu können, müssen ohnehin weitere Daten wie zum Beispiel der Vorname bekannt sein. Da es für Geschäftspartner erforderlich ist, mehr als nur den Nachnamen und den Sitz des zuständigen Vollstreckungsgerichts voneinander zu kennen, ist es auch nicht unangemessen, eine Einsicht von vornherein von weiteren Angaben abhängig zu machen.

Aus Sicht des Datenschutzes ist eine Anzeige von Schuldnerdaten, die nicht vom legitimen Abfragezweck erfasst werden, zu vermeiden. Deshalb halten es die Datenschutzbeauftragten des Bundes und der Länder für notwendig, bei der Regelung der Einsicht in das Schuldnerverzeichnis die zwingende Angabe weiterer Identifizierungsmerkmale vorzusehen.

Die Bayerische Staatsministerin der Justiz und für Verbraucherschutz hat mir mitgeteilt, dass sie die geäußerten Bedenken teilt und gegenüber dem Bundesministerium der Justiz fordert, dass eine Ergebnisübersicht erst dann angezeigt werden darf, wenn zuvor zumindest drei unveränderliche Merkmale der gesuchten Person, d.h. Familienname, Vorname und Geburtsdatum oder Geburtsort, angegeben wurden.

Die vom Bundesministerium der Justiz mittlerweile erlassene Schuldnerverzeichnisführungsverordnung (SchuFV) erfordert demgemäß mindestens die Eingabe des Namens und Vornamens des Schuldners oder die Firma des Schuldners und den Sitz des zuständigen zentralen Vollstreckungsgerichts oder den Wohnsitz des Schuldners oder den Ort, an dem der Schuldner seinen Sitz hat. Für den Fall, dass mehrere Datensätze (mehrere Schuldner) vorhanden sind, hat der Nutzer nunmehr zusätzlich das Geburtsdatum des Schuldners einzugeben. Ergibt auch diese Abfrage mehrere Treffer, hat der Nutzer außerdem den Geburtsort des Schuldners einzugeben. Erst wenn weiterhin mehrere Treffer vorhanden sind, sind diese danach zu übermitteln.

Der nunmehr vorliegende Entwurf stellt aus datenschutzrechtlicher Sicht eine erhebliche Verbesserung dar. Insbesondere die tatsächliche Umsetzung des Zugriffs auf das elektronische Schuldnerverzeichnis werde ich weiterhin kritisch begleiten.

5.2 Aus der Justiz allgemein

5.2.1 In welchem Umfang können Gerichte Akten an Sachverständige weitergeben?

Im Rahmen meiner Tätigkeit schildern mir Petenten regelmäßig Verfahren, in denen Gerichte Sachverständigenunterlagen in erheblichem Umfang – meistens die vollständige Verfahrensakte – übermitteln, obwohl dieser Umfang für die Begutachtung aus Sicht der betroffenen Petenten nicht erforderlich sei. Eine konkrete Überprüfung ist mir aufgrund der richterlichen Unabhängigkeit nicht möglich. Aus diesem Grunde hat auch das Bayerische Staatsministerium der Justiz und für Verbraucherschutz darauf verzichtet, hier Vorgaben zu machen.

Gleichwohl stimmen das Bayerische Staatsministerium der Justiz und für Verbraucherschutz und ich darin überein, dass die Gerichte im Rahmen pflichtgemäßen Ermessens zu entscheiden haben, welche Unterlagen dem Sachverständigen zugänglich gemacht werden. Da es sich bei der Vorlage der Verfahrensakte an einen Sachverständigen um eine Datenübermittlung an Dritte handelt, gilt auch hier der allgemeine datenschutzrechtliche Erforderlichkeitsgrundsatz („Datensparsamkeit"). Es sind damit nur solche Daten und Akten (-bestandteile) dem Sachverständigen zu übermitteln, die für die Begutachtung erforderlich sind. Seitens des Bayerischen Staatsministeriums der Justiz und für Verbraucherschutz wurde mir mitgeteilt, dass beabsichtigt sei, die Thematik bei geeigneter Gelegenheit mit den betroffenen Stellen zu erörtern.

5.2.2 Anonymisierung bei der Veröffentlichung von Gerichtsentscheidungen

Im Rahmen von Bürgereingaben war ich mehrfach mit der Problematik unzureichender Anonymisierung bei der Veröffentlichung von Gerichtsentscheidungen, wie z.B. in Onlinedatenbanken zur Rechtsprechung oder auf eigenen Homepages der Gerichte befasst. Dabei steht generell das Informationsinteresse der Öffentlichkeit an Gerichtsentscheidungen und deren Gründen dem Datenschutzrecht der Betroffenen gegenüber. Im Regelfall genügt zwar eine Anonymisierung der Namen und Anschriften. In Einzelfällen sind jedoch weitere Angaben (wie z.B. Ortsangaben, berufliche Tätigkeit, u.ä.) zu tilgen, soweit mit diesen Angaben eine Identifizierung ohne größeren Aufwand auch für Dritte möglich ist. In diesen Fällen kann es wiederum dazu kommen, dass durch derartige weitergehende Anonymisierung der Inhalt der Gerichtsentscheidung nicht mehr aus sich heraus verständlich ist und daher das Informationsinteresse der Öffentlichkeit nicht mehr gewahrt ist. Es ist daher in solchen Fällen eine Abwägung des Informationsinteresses der Öffentlichkeit gegen das Datenschutzrecht des Betroffenen im Einzelfall erforderlich. In jedem Fall zu anonymisieren sind aber besonders sensible personenbezogene Daten, wie z.B. Gesundheitsdaten, deren Kenntnis für das Verständnis der Entscheidung nicht zwingend notwendig ist. Die Einhaltung dieser auch von der Rechtsprechung aufgestellten Grundsätze (vgl. VGH Baden-Würtemberg vom 23.07.2010, Az: 1 S 501/10) werde ich auch künftig überprüfen.

5.2.3 Nennung des Namens eines Angeklagten auf einem Parkverbotsschild

Im Rahmen eines besonders öffentlichkeitsträchtigen Strafverfahrens gegen mehrere Angeklagte beantragte der Präsident eines Landgerichts bei der zuständigen Behörde für die Sitzungstage die vorübergehende Einrichtung einer Halteverbotszone mit dem Zusatz: „Frei für Pressevertreter der Jugendkammer beim Landgericht …“. Für die Sitzungstage wurden entsprechende Schilder aufgestellt. Bei der Zusatzbeschilderung wurde zusätzlich zum Text „Frei für Pressevertreter der Jugendkammer beim Landgericht …“ auch der Hinweis „Für Strafverfahren … und andere“ aufgenommen. In dem Hinweis befand sich der Vor- und Zuname des Hauptangeklagten.

Auf Nachfrage teilte mir der Vizepräsident des betroffenen Landgerichts mit, dass er, nachdem er von der Beschilderung durch die Berichterstattung in der Presse erfahren habe, angeordnet habe, dass der Hinweis auf das Strafverfahren entfernt werde. Außerdem sei mit der zuständigen Behörde besprochen worden, dass das für die Halteverbotszone Anlass gebende Strafverfahren zukünftig in keinem Fall in der Beschilderung anzugeben ist.

Zusätzlich habe ich gegenüber dem betroffenen Landgericht darauf hingewiesen, dass ich keine Notwendigkeit für die Nennung des Namens des Angeklagten beim Antrag auf Einrichtung einer Halteverbotszone sehe.

Der Präsident des Landgerichts hat daraufhin mit der zuständigen Behörde vereinbart, dass zukünftig in den Anträgen nur mehr die entsprechende Strafkammer des Landgerichts genannt wird und weitergehende Hinweise auf das Verfahren unterbleiben.

5.3 Strafverfolgung

5.3.1 Quellen-Telekommunikationsüberwachung

Mit dem Thema „Quellen-Telekommunikationsüberwachung“ habe ich mich bereits in meinem letzten Tätigkeitsbericht auseinandergesetzt und darauf hingewiesen, dass solche Maßnahmen aus meiner Sicht nicht auf die Regelungen zur herkömmlichen Telekommunikationsüberwachung gestützt werden können (siehe hierzu 24. Tätigkeitsbericht, Nr. 3.7). Auch die Konferenz der Datenschutzbeauftragten des Bundes und der Länder teilt diese Auffassung und hat daher am 16./17.03.2011 in Würzburg die Entschließung „Ohne gesetzliche Grundlage keine Telekommunikationsüberwachung auf Endgeräten“ verabschiedet.

Entschließung der 81. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 16./17.03.2011
Ohne gesetzliche Grundlage keine Telekommunikationsüberwachung auf Endgeräten

Wollen Strafverfolgungsbehörden verschlüsselte Internetkommunikationsvorgänge (z.B. Internettelefonie oder E-Mails) überwachen und aufzeichnen, muss regelmäßig auf dem Endgerät des Betroffenen eine Software angebracht werden, die die Daten aus dem laufenden Kommunikationsvorgang vor ihrer Ver-

schlüsselung erfasst und an die Behörde weiterleitet (sog. Quellen-Telekommunikationsüberwachung). Die hierbei anzuwendende Technik entspricht der der Online-Durchsuchung, die grundsätzlich auch Zugriffe auf gespeicherte Inhalte ermöglicht.

Telekommunikationsüberwachungsmaßnahmen durch Zugriffe auf Endgeräte müssen sich auf Daten aus laufenden Telekommunikationsvorgängen beschränken. Dies ist durch technische Vorkehrungen und rechtliche Vorgaben sicherzustellen. Nur so wird der Rechtsprechung des Bundesverfassungsgerichts entsprochen.

Die Strafprozessordnung enthält keine Regelung, die diesen Anforderungen gerecht wird. Im grundrechtsrelevanten Bereich muss der Gesetzgeber alle wesentlichen Vorgaben selbst treffen. Es reicht nicht aus, wenn derartige Schutzvorkehrungen nur im Rahmen eines Gerichtsbeschlusses auf der Grundlage von §§ 100 a, 100 b Strafprozessordnung angeordnet werden. Vielmehr müssen die vom Bundesverfassungsgericht geforderten rechtlichen Vorgaben und technischen Vorkehrungen gesetzlich verankert sein.

Die Datenschutzbeauftragten des Bundes und der Länder fordern den Gesetzgeber auf, Rechtssicherheit – auch für die Strafverfolgungsbehörden – zu schaffen und die Zulässigkeit und die Voraussetzungen der Quellen-Telekommunikationsüberwachung unter strenger Beachtung der Vorgaben des Bundesverfassungsgerichts zu klären.

Wie eingangs bereits erwähnt, habe ich im Berichtszeitraum des Weiteren die Einhaltung der rechtlichen Vorgaben und technischen Vorkehrungen bei den durch bayerische Behörden durchgeführten Maßnahmen im Rahmen der Quellen-Telekommunikationsüberwachung umfangreich geprüft. Der vollständige Bericht hierzu ist über meine Homepage abrufbar (www.datenschutz-bayern.de). An dieser Stelle möchte ich folgende zusammenfassende Feststellungen und Bewertungen des Prüfberichts vorstellen:

– In dem Zeitraum vom 01.01.2008 bis zum 31.12.2011 führten bayerische Strafverfolgungsbehörden 23 Maßnahmen der sogenannten Quellen-Telekommunikationsüberwachung (Quellen-TKÜ) durch. Zu allen Maßnahmen lagen richterliche Anordnungen vor. Zu Zwecken der Gefahrenabwehr wurden für den überprüften Zeitraum keine Maßnahmen festgestellt.

– In tatsächlicher Hinsicht hat die Prüfung bestätigt, dass die gegenwärtigen strafprozessualen Befugnisnormen auf die konventionelle TKÜ ausgerichtet sind. Es ist eben ein erheblicher Unterschied, ob eine Vorschrift die Überwachung allein von Telefongesprächen erlaubt oder auch Vorbereitungs- und Begleitmaßnahmen gestatten soll, die bereits für sich allein erheblich in die Grundrechte eingreifen. Sofern an der Notwendigkeit der Quellen-TKÜ festgehalten wird, ist deshalb die Verabschiedung von weiteren Vorschriften zu empfehlen, die den Besonderheiten der Quellen-TKÜ besser gerecht werden. Vergleichbares gilt für die Quellen-TKÜ im Rahmen der Gefahrenabwehr.

– Zur Durchführung der Maßnahmen verwendete das Bayerische Landeskriminalamt (BLKA) durchweg Software des Unternehmens DigiTask. Dabei unterstützte das Unternehmen die Einrichtung einer Überwa-

chungskonsole beim BLKA und lieferte je Einzelmaßnahme die Überwachungssoftware („Trojaner"), die vom BLKA anschließend auf den jeweiligen Zielrechnern eingebracht wurde. Im Zusammenhang mit der jeweiligen Auftragserteilung konnten die Geschehensabläufe dabei mangels hinreichender Dokumentation beim BLKA nicht vollständig nachvollzogen werden. Im Hinblick auf die Eingriffsintensität der Maßnahmen sind derartige Dokumentationsdefizite als Datenschutzverstöße anzusehen.

– Die Aufträge an DigiTask waren in mehrfacher Hinsicht mängelbehaftet. So wäre es etwa angezeigt gewesen, DigiTask vertraglich ausdrücklich zu verpflichten, keine überschießenden Überwachungsfunktionalitäten zu liefern und die Möglichkeit einer Einsichtnahme in den Quellcode vorzusehen. Überdies fehlte die gebotene Regelung zur Verpflichtung des privaten Wartungspersonals auf das Datengeheimnis und nach dem Verpflichtungsgesetz.

– Nach der Lieferung von Überwachungssoftware führte das BLKA jeweils Funktions- und Abnahmetests durch. Dabei ist es datenschutzrechtlich nicht zu beanstanden, dass das BLKA nicht in jedem Fall hierzu Einsicht in den jeweiligen Quellcode der Software genommen hat. Eine Einsichtnahme in den Quellcode sollte allerdings stichprobenartig erfolgen, um zuverlässig verdeckte Funktionalitäten auszuschließen.

– Was die Einbringung der Überwachungssoftware auf den Zielrechnern anbelangt, hat das BLKA – soweit nachvollziehbar – die datenschutzrechtlich gebotenen Sorgfaltspflichten beachtet, um sicherzustellen, dass nur die von einer richterlichen Anordnung umfassten Zielrechner infiltriert wurden.

– Hinsichtlich der Funktionsweise der Überwachungssoftware konnte ich feststellen, dass das BLKA bemüht war, die Beeinträchtigung der Stabilität des jeweils überwachten IT-Systems so gering wie möglich zu gestalten.

– Bei den zwanzig insoweit überprüften Maßnahmen konnten in vier Maßnahmen Aufzeichnungen von Anwendungsfensterinhalten (Applicationshots) von Browsern durchgeführt werden, in zwei weiteren Maßnahmen konnten nur Applicationshots von Instant Messengern gefertigt werden. In zwei weiteren, noch nicht abgeschlossenen, Maßnahmen habe ich anhand meiner in meinem Haus aufgebauten Testumgebung festgestellt, dass die Software nicht nur die Übertragung eines Browserfensters, sondern auch eines gesamten Bildschirms ermöglicht. Da es mir lediglich möglich war, die einzelnen Binärdateien zu testen, kann ich insoweit keine Aussage treffen, ob das BLKA von der Funktion tatsächlich Gebrauch gemacht hat, komplette Screenshots aufzuzeichnen.

– Unabhängig von der rechtlichen Frage, ob Applicationshots einer laufenden Telekommunikation entnommen sind und damit nach gegenwärtiger Gesetzeslage im Grundsatz zulässig sein können, sollte die Frage durch den jeweiligen Gesetzgeber geklärt werden. Denn die Fertigung von Applicationshots ist sowohl aus sicherheitsbehördlicher Perspektive als auch aus grundrechtlicher Sicht von hoher Relevanz.

– Soweit überprüfbar enthielt die Überwachungssoftware keine zuverlässige technische Begrenzung auf bestimmte Überwachungsfunktionen. Eine

solche Funktionsbeschränkung wäre aus datenschutzrechtlicher Sicht nicht nur über die Beschränkung der Benutzeroberfläche der Überwachungskonsole geboten gewesen. Unabhängig hiervon habe ich im Rahmen meiner Prüfung keine Anhaltspunkte dafür gefunden, dass das BLKA (mit Ausnahme der Deinstallation in einem Fall) von derartigen Funktionen Gebrauch gemacht hätte.

– Das BLKA hat die Überwachungssoftware nicht nach einem bestimmten Zeitpunkt automatisch deinstalliert. Dementsprechend war eine erfolgreiche Deinstallation davon abhängig, dass der bei der Überwachung verwendete Proxy-Server in Betrieb blieb. Insbesondere bei Proxy-Servern im Ausland hätte das BLKA eine dauerhafte Verfügbarkeit sicherstellen müssen.

– In Bezug auf die abgeschlossenen Maßnahmen konnte die Verschlüsselung der Übertragungswege zum damaligen Zeitpunkt zu den damaligen Rahmenbedingungen noch als ausreichend angesehen werden. Zum gegenwärtigen Zeitpunkt wäre die Verschlüsselung allerdings als unzureichend anzusehen.

– Das technische Gesamtsystem der Überwachung setzt eine zuverlässige Authentisierung zwischen der Überwachungssoftware auf dem infiltrierten IT-System und der Überwachungskonsole voraus. Eine solche Zuverlässigkeit war nicht hinreichend gegeben.

– Die Überwachungskonsole wurde ohne Sicherheitsupdates betrieben, was ich zumindest als bedenklich bewerte.

– Die Vergabe und Verwaltung der Nutzerkennungen sowie die Sicherungsmaßnahmen der einzelnen Kennungen entsprachen nicht den üblichen und gebotenen datenschutzrechtlichen Anforderungen.

– Es erfolgte keine ausreichende Protokollierung auf der Überwachungskonsole. Demgegenüber habe ich bei der Protokollierung auf der Firewall keine wesentlichen Mängel feststellen können.

– Konkrete Hinweise auf Maßnahmen, die den Kernbereich privater Lebensgestaltung beeinträchtigt hätten, habe ich nicht vorgefunden.

– Zur Vorbereitung der Quellen-TKÜ wurden diverse Begleitmaßnahmen eingesetzt:

  a) In neun von zwanzig geprüften Maßnahmen wurden auf dem IT-System befindliche Softwarelisten ausgelesen; insoweit ist es zumindest fraglich, ob dieser Ausleseprozess von den richterlichen Anordnungen erfasst war;

  b) in zwei Fällen wurde durch das anordnende Gericht eine Durchsuchung gestattet, um die Überwachungssoftware aufzubringen; eine rechtliche Bewertung ist mir insoweit verwehrt. Ich weise allerdings darauf hin, dass für den Bereich der Gefahrenabwehr eine Wohnungsbetretung als Begleitmaßnahme in vergleichbaren Fällen unzulässig wäre.

– Nach Abschluss einer Quellen-TKÜ ist der Betroffene des infiltrierten Gerätes regelmäßig nicht nur über Beeinträchtigungen der Vertraulichkeit eines Gesprächs, sondern auch über eine etwaige Beeinträchtigung der Integrität eines infiltrierten IT-Systems zu unterrichten. Aus den mir vorgelegten Unterlagen ergibt sich, dass die Betroffenen nicht über die Integritätsbeeinträchtigung informiert wurden.

Diese Feststellungen des Berichts unterstreichen insbesondere folgenden Regelungsbedarf:

– Sofern Begleitmaßnahmen (z.B. das Auslesen von Softwarelisten zur Vorbereitung der Installation der Software) als notwendig angesehen werden, müssen auch die Art und Weise ihrer Durchführung gesetzlich eindeutig geregelt werden.

– Die Quellen-TKÜ ist durch klare Vorgaben von der Online-Durchsuchung abzugrenzen. Hierbei ist insbesondere die Problematik der Überwachung von Texten außerhalb einer laufenden Telekommunikation zu klären (z.B. Überwachung noch nicht abgesandter E-Mail-Entwürfe).

– Gesetzliche Bestimmungen zur Quellen-TKÜ sind aufgrund ihrer erhöhten Eingriffsintensität in ihren Voraussetzungen enger als die derzeitigen Bestimmungen zur konventionellen Telekommunikationsüberwachung zu fassen.

– Geboten sind weiterhin Regelungen, die technisch und organisatorisch unzulässige Überwachungsfunktionalitäten unterbinden und eine effektive Kontrolle ermöglichen (z.B. Verbot oder Begrenzung von Nachladefunktionen, Möglichkeit einer Einsichtnahme in den Quelltext der Überwachungssoftware).

– Klargestellt werden sollte weiterhin, dass Betroffene nicht nur über die Telekommunikationsüberwachung als solche, sondern auch über den erfolgten Eingriff in ihr IT-System nachträglich zu unterrichten sind.

Soweit politisch an der Quellen-TKÜ zur Strafverfolgung und zur Gefahrenabwehr festgehalten wird, empfehle ich den Gesetzgebern in Bund und Bayern daher dringend, Bestimmungen zu schaffen, die der erhöhten Eingriffsintensität und den technischen Besonderheiten der Quellen-TKÜ gerecht werden.

5.3.2 Entschließung zur Funkzellenabfrage

Aufgrund der Funkzellenabfrage durch die Strafverfolgungsbehörden in Dresden anlässlich von Versammlungen am 19.02.2011 hat die Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 27.07.2011 im Rahmen einer Entschließung eine Einschränkung der Funkzellenabfrage gefordert. Der Bundesgesetzgeber wird darin aufgefordert, den Anwendungsbereich für eine nicht individuelle Funkzellenabfrage einzuschränken, dem Grundsatz der Verhältnismäßigkeit zu stärkerer Beachtung in der Praxis zu verhelfen, das Erforderlichkeitsprinzip zu stärken sowie die Löschungsvorschrift des § 101 Abs. 8 StPO zu präzisieren.

Auch wenn mir vergleichbare Maßnahmen wie in Dresden in Bayern nicht bekannt geworden sind, habe ich die Entschließung unterstützt, da bei derartigen Funkzellenabfragen ein besonders hohes Risiko dafür besteht, dass auch eine unüberschaubar große Anzahl Unbeteiligter von der Maßnahme betroffen wird. Eine normenklare Rechtsgrundlage, die den neuen technischen Entwicklungen besser entspricht, ist daher in diesem sensiblen Bereich der Verkehrsdaten von Mobilfunkverbindungen für einen effektiven Schutz der personenbezogenen Daten der Betroffenen in besonderem Maße notwendig.

Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 27.07.2011
Funkzellenabfrage muss eingeschränkt werden!

Die Strafverfolgungsbehörden in Dresden haben mit einer sog. Funkzellenabfrage anlässlich von Versammlungen und dagegen gerichteter Demonstrationen am 19.02.2011 Hunderttausende von Verkehrsdaten von Mobilfunkverbindungen erhoben, darunter die Rufnummern von Anrufern und Angerufenen, die Uhrzeit sowie Angaben zur Funkzelle, in der eine Mobilfunkaktivität stattfand. Dadurch sind zehntausende Versammlungsteilnehmerinnen und Versammlungsteilnehmer, darunter Abgeordnete von Landtagen und des Deutschen Bundestages, Rechtsanwältinnen und Rechtsanwälte, sowie Journalistinnen und Journalisten in Ausübung ihrer Tätigkeit, aber auch Anwohnerinnen und Anwohner der dicht besiedelten Dresdener Innenstadt, in ihrer Bewegung und ihrem Kommunikationsverhalten erfasst worden. Dieser Vorfall verdeutlicht die Schwäche der gesetzlichen Regelung.

Rechtsgrundlage der nichtindividualisierten Funkzellenabfrage ist bisher § 100 g Abs. 2 S. 2 StPO, wonach im Falle einer Straftat von erheblicher Bedeutung eine räumlich und zeitlich hinreichend bestimmte Bezeichnung der Telekommunikation ausreichend sein soll, um Verkehrsdaten bei den Telekommunikationsdiensteanbietern erheben zu dürfen. Diese Aussage wird mit einer allgemeinen Subsidiaritätsklausel verknüpft. Diese 2001 in die Strafprozessordnung eingefügte Regelung ist unzureichend, da sie weder hinreichend bestimmt ist noch den heutigen technischen Gegebenheiten entspricht. Aktuelle Geräte erzeugen durch ihren Datenverkehr ohne aktives Zutun des Besitzers eine Vielzahl von Verkehrsdaten, die später in einer Funkzellenabfrage erhoben werden können.

Die Funkzellenabfrage ist ein verdeckter Eingriff in das Fernmeldegeheimnis (Art. 10 GG). Sie richtet sich unterschiedslos gegen alle in einer Funkzelle anwesenden Mobilfunkgerätebesitzer, nicht nur – wie etwa eine Telekommunikationsüberwachung nach § 100 a StPO – gegen bestimmte einzelne Tatverdächtige. Sie offenbart Art und Umstände der Kommunikation von u.U. Zehntausenden von Menschen, die selbst keinen Anlass für einen staatlichen Eingriff gegeben haben. Sie schafft damit des Weiteren die Möglichkeit, diese Personen rechtswidrig wegen Nicht-Anlasstaten, etwa Verstößen gegen das Versammlungsgesetz, zu verfolgen. Sie ist bezogen auf einzelne Personen ein Instrument der Verdachtsgenerierung. Die Strafprozessordnung regelt nicht näher, wie die Behörden mit den erhobenen Daten umzugehen haben, insbesondere nicht, über welche Zeiträume, zu welchen Personen und in welchen anderen Zusammenhängen die erhobenen Daten polizeilich weiter verwendet werden dürfen.

Das Bundesverfassungsgericht hat stets betont, dass die Erhebung von Verkehrsdaten erhebliche Rückschlüsse auf das Kommunikationsverhalten zulässt. Verkehrsdaten können das soziale Netz des Betroffenen widerspiegeln; allein aus

ihnen kann die Verbindung zu Parteien, Gewerkschaften oder Bürgerinitiativen deutlich werden.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder fordert daher den Bundesgesetzgeber auf, den Anwendungsbereich für eine nichtindividualisierte Funkzellenabfrage einzuschränken, dem Grundsatz der Verhältnismäßigkeit zu stärkerer Beachtung in der Praxis zu verhelfen, das Erforderlichkeitsprinzip zu stärken (etwa durch die Pflicht zur unverzüglichen Reduzierung der erhobenen Daten auf das zur Strafverfolgung oder gerichtlichen Auseinandersetzung Erforderliche) sowie die Löschungsvorschrift des § 101 Abs. 8 StPO zu präzisieren.

5.3.3 Entschließung zur europäischen Ermittlungsanordnung

Die 83. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 21./22.03.2012 in Potsdam hat in einer Entschließung gefordert, dass die Richtlinie über die europäische Ermittlungsanordnung in Strafsachen, die derzeit auf europäischer Ebene beraten wird, nicht zu Lasten des Grundrechtschutzes der Betroffenen geht. Vielmehr sind die Anforderungen der EU-Grundrechte-Charta konsequent einzuhalten.

Entschließung der 83. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 21./22.03.2012
Europäische Ermittlungsanordnung darf Grundrechtsgarantien nicht aushebeln

Zurzeit wird auf europäischer Ebene der Entwurf einer Richtlinie über die Europäische Ermittlungsanordnung in Strafsachen beraten. Diese hat massive Auswirkungen auf den Grundrechtsschutz der Bürgerinnen und Bürger in den EU-Mitgliedstaaten. Sie kann dazu führen, dass der verfahrensrechtliche Schutzstandard bei strafprozessualen Maßnahmen europaweit auf niedrigstes Niveau abgesenkt wird. So kann sie etwa zur Folge haben, dass ein Mitgliedstaat für einen anderen Daten oder Beweismittel erhebt und diesem übermittelt, obwohl die Erhebung nach eigenem Recht nicht zulässig wäre.

Der Richtlinienentwurf verfolgt vorrangig das Ziel einer weitgehenden gegenseitigen Anerkennung von Eingriffsentscheidungen der Strafverfolgungsbehörden, ohne dass einheitliche Verfahrensgarantien geschaffen werden. Dies wirft Probleme auf, wenn der Anordnungsstaat niedrigere Schutzstandards aufweist als der Vollstreckungsstaat. Die Möglichkeiten der Mitgliedstaaten, eine entsprechende Anordnung eines anderen Mitgliedstaates zurückzuweisen, sind nicht immer ausreichend. Eingriffsschwellen, Zweckbindungs- und Verfahrensregelungen müssen gewährleisten, dass die Persönlichkeitsrechte der Betroffenen gewahrt werden.

Eine effektive grenzüberschreitende Strafverfolgung im vereinten Europa darf nicht zu Lasten des Grundrechtsschutzes der Betroffenen gehen. Die Anforderungen der EU-Grundrechte-Charta sind konsequent einzuhalten. Die Europäische Ermittlungsanordnung muss in ein schlüssiges Gesamtkonzept zur Datenerhebung und -verwendung im Bereich der inneren Sicherheit und der Strafverfolgung eingebettet werden, das die Grundrechte der Bürgerinnen und Bürger gewährleistet.

5.3.4 Überprüfung von „Alias"-Personalien in Strafbefehlsanträgen

Im Rahmen einer Eingabe wurde mir ein Strafbefehl vorgelegt, in dem neben den Personalien des Angeschuldigten ein „Alias" mit einem abweichenden Geburtsdatum angegeben wurde. Insbesondere da dieser Strafbefehl auch an eine Ärztekammer übermittelt wurde, fühlte sich der Petent durch die Angabe der „Alias"-Personalien stigmatisiert. Die abweichenden Daten habe er schließlich nie verwendet.

Im Rahmen meiner Überprüfung habe ich festgestellt, dass die „Alias"-Personalien automatisch von der EDV in den Strafbefehlsantrag eingesetzt worden waren. Wie das abweichende Geburtsdatum in die EDV der Staatsanwaltschaft gelangt war, konnte nicht mehr festgestellt werden. Eine Überprüfung durch das Bayerische Staatsministerium der Justiz und für Verbraucherschutz ergab jedoch, dass es sich um einen Anwendungsfehler bei der Bedienung der Software im Einzelfall gehandelt haben muss.

Um die oben dargestellte Stigmatisierung durch Übersendung von unrichtigen Strafbefehlen oder Anklageschriften zu verhindern, habe ich den zuständigen Leitenden Oberstaatsanwalt gebeten, seine Mitarbeiter darauf hinzuweisen, dass die Personalien – gerade auch vor dem Hintergrund etwaiger „Alias"-Personalien – vor Abschluss des Verfahrens zu überprüfen sind. Dies wurde mir zugesagt. Weiterhin wurde mir mitgeteilt, dass die Staatsanwälte angewiesen worden seien, bei Zweifeln „Alias"-Personalien in den Anklageschriften bzw. Strafbefehlsanträgen zu löschen.

5.3.5 Inhalt der Benachrichtigung im Anschluss an eine Telekommunikationsüberwachung

Nach § 101 Abs. 4 Nr. 3 Strafprozessordnung (StPO) sind die Beteiligten einer überwachten Telekommunikation im Anschluss an die Maßnahme zu benachrichtigen. In diesem Zusammenhang sind die Beteiligten auch auf die Möglichkeit nachträglichen Rechtschutzes hinzuweisen.

§ 101 Abs. 1 und 4 StPO
(1) Für Maßnahmen nach den §§ 98 a, 99, 100 a, 100 c bis 100 i, 110 a, 163 d bis 163 f gelten, soweit nichts anderes bestimmt ist, die nachstehenden Regelungen.
. . .
(4) Von den in Absatz 1 genannten Maßnahmen sind im Falle
1. des § 98 a die betroffenen Personen, gegen die nach Auswertung der Daten weitere Ermittlungen geführt wurden,
2. des § 99 der Absender und der Adressat der Postsendung,
3. des § 100 a die Beteiligten der überwachten Telekommunikation,
4. des § 100 c
a) der Beschuldigte, gegen den sich die Maßnahme richtete,
b) sonstige überwachte Personen,
c) Personen, die die überwachte Wohnung zur Zeit der Durchführung der Maßnahme innehatten oder bewohnten,
5. des § 100 f die Zielperson sowie die erheblich mitbetroffenen Personen,
6. des § 100 g die Beteiligten der betroffenen Telekommunikation,
7. des § 100 h Abs. 1 die Zielperson sowie die erheblich mitbetroffenen Personen,

8. des § 100 i die Zielperson,
9. des § 110 a
a) die Zielperson,
b) die erheblich mitbetroffenen Personen,
c) die Personen, deren nicht allgemein zugängliche Wohnung der Verdeckte Ermittler betreten hat,
10. des § 163 d die betroffenen Personen, gegen die nach Auswertung der Daten weitere Ermittlungen geführt wurden,
11. des § 163 e die Zielperson und die Person, deren personenbezogene Daten gemeldet worden sind,
12. des § 163 f die Zielperson sowie die erheblich mitbetroffenen Personen zu benachrichtigen.

Dabei ist auf die Möglichkeit nachträglichen Rechtsschutzes nach Absatz 7 und die dafür vorgesehene Frist hinzuweisen. Die Benachrichtigung unterbleibt, wenn ihr überwiegende schutzwürdige Belange einer betroffenen Person entgegenstehen. Zudem kann die Benachrichtigung einer in Satz 1 Nr. 2, 3 und 6 bezeichneten Person, gegen die sich die Maßnahme nicht gerichtet hat, unterbleiben, wenn diese von der Maßnahme nur unerheblich betroffen wurde und anzunehmen ist, dass sie kein Interesse an einer Benachrichtigung hat. Nachforschungen zur Feststellung der Identität einer in Satz 1 bezeichneten Person sind nur vorzunehmen, wenn dies unter Berücksichtigung der Eingriffsintensität der Maßnahme gegenüber dieser Person, des Aufwands für die Feststellung ihrer Identität sowie der daraus für diese oder andere Personen folgenden Beeinträchtigungen geboten ist.

Als Beteiligte sind dabei nicht nur beschuldigte Personen anzusehen, sondern auch deren Gesprächspartner, die nicht Beschuldigte in dem Ermittlungs- oder Strafverfahren sind.

Im Rahmen einer Eingabe habe ich in Erfahrung gebracht, dass die bayerischen Staatsanwaltschaften uneinheitlich bei der Frage verfahren, ob im Betreff des Anschreibens an nichtbeschuldigte Betroffene auch der Name des Beschuldigten und der Tatverdacht (etwa Verfahren gegen Max Mustermann wegen Betruges) mitgeteilt werden. Aufgrund dieser unterschiedlichen Vorgehensweise habe ich die Frage nach der Erforderlichkeit dieser Angaben aufgeworfen. Das Bayerische Staatsministerium der Justiz und für Verbraucherschutz hat mir dazu mitgeteilt, dass man die Angaben für erforderlich hält, um dem nichtbeschuldigten Betroffenen einen effektiven Rechtsschutz zu ermöglichen. Insofern erfordere die Gewährung eines effektiven Rechtsschutzes die Möglichkeit einer Überprüfung durch den nichtbeschuldigten Betroffenen selbst. Dementsprechend müsse dieser anhand der Angaben über den Beschuldigten erkennen können, in welchem Bezug die jeweilige Maßnahme zu ihm stand. Weiterhin sei der nichtbeschuldigte Betroffene auf die Mitteilung der Straftat angewiesen, um prüfen zu können, ob eine Katalogtat als Voraussetzung einer Telekommunikationsüberwachung vorlag. Ich halte diese Überlegungen für nachvollziehbar.

Darüber hinaus war allerdings in der EDV der Staatsanwaltschaften bei der Mitteilung an nichtbeschuldigte Betroffene der Hinweis vorgesehen, dass sich das Verfahren nicht gegen sie richtete. Insofern war der Satz „gegen Sie wurden keine Ermittlungen geführt." hinterlegt. Ich habe das Bayerische Staatsministerium der Justiz und für Verbraucherschutz darauf hingewiesen, dass dieser Satz zumindest dann missverständlich ist, wenn gegen den nichtbeschuldigten Beteiligten zwar nicht in diesem Verfahren, jedoch in einem weiteren Verfahren Ermittlungen geführt werden oder geführt worden sind. Da sich in diesem Zusammen-

hang auch der Hinweis „Sie müssen keine Maßnahmen ergreifen." fand, habe ich gegenüber dem Staatsministerium den Standpunkt vertreten, dass hierdurch zumindest die Gefahr besteht, dass Beschuldigte falsch informiert und ggf. von der Wahrung ihrer Rechte abgehalten werden, da der Hinweis nur auf dieses Verfahren Fehlvorstellungen auslösen kann.

Vom Bayerischen Staatsministerium der Justiz und für Verbraucherschutz wurde mir daraufhin mitgeteilt, dass dieser Punkt zwar in der EDV hinterlegt sei, jedoch eine Prüfung durch den Sachbearbeiter bei der Staatsanwaltschaft erforderlich sei. In einem mir insoweit vorliegenden Verfahren seien weitere Verfahren übersehen worden. Um hier Fehler zukünftig auszuschließen, werde künftig auf die Vorbelegung dieses Punktes in der EDV verzichtet.

5.4 Straf- und Maßregelvollzug

5.4.1 Keine Sichtkontrolle von Verteidigerpost in Abwesenheit des Gefangenen

Eingehende Verteidigerpost in einer Justizvollzugsanstalt unterliegt gemäß Art. 32 Abs. 1 Bayerisches Strafvollzugsgesetz (BayStVollzG) nicht der Briefkontrolle. Eine ausdrückliche Regelung, wie Verteidigerpost im Haftraum zu lagern ist, existiert jedoch nicht. Somit sind eingehende Schreiben gemäß Art. 33 Abs. 3 BayStVollzG grundsätzlich unverschlossen zu verwahren.

Art. 32 Abs. 1 BayStVollzG
Der Schriftwechsel der Gefangenen mit ihren Verteidigern wird nicht überwacht. [2] *Liegt dem Vollzug der Freiheitsstrafe eine Straftat nach § 129 a StGB, auch in Verbindung mit § 129 b Abs. 1 StGB, zugrunde, gelten § 148 Abs. 2, § 148 a der Strafprozessordnung (StPO) entsprechend; dies gilt nicht, wenn die Gefangenen sich in einer Einrichtung des offenen Vollzugs befinden oder wenn ihnen Lockerungen des Vollzugs gemäß Art. 13 Abs. 1 Nr. 1 oder 2 zweite Alternative oder Urlaub gemäß Art. 14 oder Art. 17 Abs. 3 gewährt worden sind und ein Grund, der den Anstaltsleiter oder die Anstaltsleiterin nach Art. 16 Abs. 2 zum Widerruf oder zur Rücknahme von Lockerungen und Urlaub ermächtigt, nicht vorliegt.* [3] *Satz 2 gilt auch, wenn gegen Strafgefangene im Anschluss an die dem Vollzug der Freiheitsstrafe zugrunde liegende Verurteilung eine Freiheitsstrafe wegen einer Straftat nach § 129 a StGB, auch in Verbindung mit § 129 b Abs. 1 StGB, zu vollstrecken ist.*

Art. 33 BayStVollzG
(1) Gefangene haben Absendung und Empfang ihrer Schreiben durch die Anstalt vermitteln zu lassen, soweit nichts anderes gestattet ist.
(2) Eingehende und ausgehende Schreiben sind unverzüglich weiterzuleiten.
(3) Gefangene haben eingehende Schreiben unverschlossen zu verwahren, sofern nichts anderes gestattet wird; sie können sie verschlossen zur Habe geben.

Um den Schutz des besonderen Vertrauensverhältnisses zwischen Verteidiger und Mandant zu gewährleisten, dürfen Anstaltsbedienstete im Rahmen der Haftraumdurchsuchung die Verteidigerpost nur darauf hin sichten, ob sich in den entsprechend beschrifteten Ordnern, Heftern, Blattsammlungen oder Ähnlichem Unterlagen befinden, die der Textkontrolle unterworfen sind oder ob sich darin andere, verbotene, Gegenstände oder Unterlagen befinden. Eine inhaltliche Kon-

trolle der geschützten Dokumente darf nicht erfolgen. Derartige Sichtungen dürfen im Übrigen demnach nur im Beisein des Gefangenen stattfinden.

Im Rahmen von zwei Eingaben bin ich darauf aufmerksam gemacht worden, dass zumindest in zwei bayerischen Justizvollzugsanstalten Einverständniserklärungen zum Einsatz kamen, mit denen die Gefangenen ihr Einverständnis zu einer Sichtkontrolle in ihrer Abwesenheit geben konnten.

Ich habe daraufhin dem Bayerischen Staatsministerium der Justiz und für Verbraucherschutz mitgeteilt, dass ich erhebliche datenschutzrechtliche Bedenken gegen die Verwendung einer solchen Einverständniserklärung habe. Vor dem Hintergrund des besonderen Hierarchieverhältnisses im Strafvollzug hege ich insbesondere Zweifel an der Freiwilligkeit eines solchen Einverständnisses.

Das Staatsministerium der Justiz und für Verbraucherschutz hat sich meinen Bedenken angeschlossen. Es teilte mir mit, im Rahmen einer Dienstbesprechung sei mit den Leiterinnen und Leitern der bayerischen Justizvollzugsanstalten und dem Leiter der bayerischen Justizvollzugsschule vereinbart worden, dass die Sichtkontrolle des im Haftraum befindlichen Schriftverkehrs nach Art. 32 Bayerisches Strafvollzugsgesetz zukünftig stets in Anwesenheit des Gefangenen erfolge, sofern diese Unterlagen als solche erkennbar seien. Die bislang in zwei bayerischen Justizvollzugsanstalten verwendeten Einwilligungserklärungen sollen nicht mehr verwendet werden.

5.4.2 Ermittlung des tatsächlichen Wohnortes bei heimatnaher Verlegung von Gefangenen

Ein Gefangener einer bayerischen Justizvollzugsanstalt hat sich bei mir darüber beschwert, dass diese zur Feststellung seines tatsächlichen Wohnorts eine Anfrage an seine Heimatgemeinde durchgeführt habe.

Die betreffende Justizvollzugsanstalt teilte mir dazu mit, dass es bei der heimatnahen Verlegung eines Gefangenen äußerst wichtig sei, den tatsächlichen Wohnort exakt zu ermitteln. So könne ein Gefangener zwar mehrere Wohnsitze, jedoch nur einen – vorherigen – Wohnort als Lebensmittelpunkt haben. Daneben zeige sich in der Praxis, dass sich die aus den Ausweispapieren ergebenden Angaben zum Wohnsitz oftmals nicht mehr zutreffend seien. Die Überprüfung bei der Heimatgemeinde sei daher erforderlich gewesen.

Ich habe hiergegen datenschutzrechtliche Bedenken erhoben, da insofern gesetzlich geregelt ist, dass wohnortbezogene Daten grundsätzlich beim Betroffenen selbst zu erheben sind. Eine Datenerhebung ohne Mitwirkung des Betroffenen darf nur ausnahmsweise erfolgen und ist an besondere Voraussetzungen geknüpft (Art. 196 Abs. 2 BayStVollzG i.V.m.. Art. 16 Abs. 2 BayDSG).

Art. 196 Abs. 2 BayStVollzG
Personenbezogene Daten sind bei dem oder der Betroffenen zu erheben. Für die Erhebung ohne Mitwirkung des oder der Betroffenen, die Erhebung bei anderen Personen oder Stellen und für die Hinweis- und Aufklärungspflichten gelten Art. 16 Abs. 2 bis 4 des Bayerischen Datenschutzgesetzes (BayDSG).

Art. 16 Abs. 2 BayDSG
Personenbezogene Daten, die nicht aus allgemein zugänglichen Quellen entnommen werden, sind beim Betroffenen mit seiner Kenntnis zu erheben. Personenbezogene Daten dürfen bei Dritten nur erhoben werden, wenn
1. eine Rechtsvorschrift eine solche Erhebung vorsieht oder zwingend voraussetzt
2. a) die zu erfüllende Verwaltungsaufgabe ihrer Art nach oder im Einzelfall eine solche Erhebung erforderlich macht oder
b) die Erhebung beim Betroffenen einen unverhältnismäßigen Aufwand erfordern würde oder keinen Erfolg verspricht und keine Anhaltspunkte dafür bestehen, dass überwiegende schutzwürdige Interessen des Betroffenen beeinträchtigt werden, oder
3. die Daten nach Art. 18 Abs. 1 oder einer anderen Rechtsvorschrift von einer öffentlichen Stelle an die erhebende Stelle übermittelt werden dürfen.
Werden Daten beim Betroffenen ohne seine Kenntnis erhoben, gelten Nummern 1 und 2 Buchst. a des Satzes 2 entsprechend.

Dementsprechend ist weiterhin darauf zu achten, dass auch im Falle einer zulässigen Datenerhebung bei den Heimatgemeinden an diese nur die für die Wohnsitzanfrage zwingend notwenigen Daten übermittelt werden, nicht jedoch darüber hinausgehende sensible Haftdaten wie z.B. zur Art und Schwere einer Verurteilung.

Das Bayerische Staatsministerium der Justiz und für Verbraucherschutz hat auf meine Anregung eine Umfrage unter sämtlichen Leiterinnen und Leitern der bayerischen Justizvollzugsanstalten gestartet. Dabei hat sich gezeigt, dass lediglich zwei Justizvollzugsanstalten im Falle einer heimatnahen Verlegung von Gefangenen die Daten des letzten Wohnorts regelmäßig ohne die Mitwirkung der betroffenen Gefangenen einholten bzw. überprüften. Das Staatsministerium veranlasste daraufhin, dass zukünftig auch bei diesen zwei Justizvollzugsanstalten nur noch in begründeten Einzelfällen ohne Mitwirkung des Gefangenen eine Datenübermittlung zur Ermittlung des Wohnortes erfolgt. Wie in allen übrigen bayerischen Justizvollzugsanstalten werde dort in Zukunft etwa nur bei widersprüchlichen oder nicht ausreichenden und unvollständig erscheinenden Angaben des Gefangenen zu seinem letzten Wohnort eine weitere Überprüfung des Wohnorts ohne Mitwirkung des Gefangenen durchgeführt.

5.4.3 Unzulässige Brieföffnungen in Justizvollzugsanstalten

Bereits in meinem letzten Tätigkeitsbericht habe ich auf das Problem hingewiesen, dass Briefe von Abgeordneten und von mir an Gefangene in bayerischen Justizvollzugsanstalten im Rahmen der Briefkontrolle zumindest geöffnet wurden, obwohl gemäß Art. 32 Abs. 2 BayStVollzG Schreiben von Abgeordneten des Bundestags und der Landtage sowie der Datenschutzbeauftragten des Bundes und der Länder nicht überwacht werden, sofern die Identität des Absenders zweifelsfrei feststeht (siehe hierzu 24. Tätigkeitsbericht, Nr. 5.4.1).

Art. 32 Abs. 2 BayStVollzG
[1]Nicht überwacht werden ferner Schreiben der Gefangenen an Volksvertretungen des Bundes und der Länder sowie an deren Mitglieder, soweit die Schreiben an die Anschriften dieser Volksvertretungen gerichtet sind und den Absender zutreffend angeben. [2]Entsprechendes gilt für Schreiben an das Europäische Parla-

ment und dessen Mitglieder, den Europäischen Gerichtshof für Menschenrechte, den Europäischen Ausschuss zur Verhütung von Folter und unmenschlicher oder erniedrigender Behandlung oder Strafe und die Datenschutzbeauftragten des Bundes und der Länder. [3]Schreiben der in den Sätzen 1 und 2 genannten Stellen, die an Gefangene gerichtet sind, werden nicht überwacht, sofern die Identität des Absenders zweifelsfrei feststeht.

Ich bin deshalb dazu übergegangen, Schreiben von mir an Gefangene mit einem Begleitschreiben an die Justizvollzugsanstalt zu versehen, in dem ich bitte, mein anliegendes Schreiben dem Gefangenen ungeöffnet zu übergeben. Das verschlossene Schreiben an den Gefangenen und ein Begleitschreiben sende ich in einem gemeinsamen Umschlag an die Justizvollzugsanstalt. Im Hinblick auf die Regelung des Art. 32 Abs. 2 Bayerisches Strafvollzugsgesetz weise ich bei dieser Vorgehensweise nach, dass das anliegende Schreiben für den Gefangenen tatsächlich von mir stammt („sofern die Identität des Absenders zweifelsfrei feststeht"). Darüber hinaus gehe ich davon aus, dass diese Vorgehensweise insbesondere auch irrtümliche Öffnungen verhindert. Im Berichtszeitraum wurde mir kein Fall bekannt, in dem ein Schreiben von mir an Gefangene in bayerischen Justizvollzugsanstalten geöffnet wurde.

Aufgrund meiner Erfahrungen lege ich eine entsprechende Vorgehensweise den übrigen in Art. 32 Abs. 2 Bayerisches Strafvollzugsgesetz genannten Stellen – etwa den Abgeordneten des Bayerischen Landtags – nahe. Auch wenn ich in der Vergangenheit keine Anhaltspunkte dafür hatte, dass von den Bediensteten in den Justizvollzugsanstalten Kenntnis vom Inhalt der (ggf. irrtümlich) geöffneten Schreiben genommen worden ist, halte ich es für wesentlich, dass die Schreiben etwa von Abgeordneten die Gefangenen verschlossen erreichen.

5.4.4 Versand von Gerichtsschreiben an Gefangene in Sammelumschlägen

Im Rahmen einer Eingabe bin ich darauf aufmerksam gemacht worden, dass von einigen bayerischen Gerichten Schreiben an Gefangene, die sich in der gleichen Justizvollzugsanstalt befinden, in Sammelumschlägen versandt worden sind. Diese Sammelumschläge wurden in der Poststelle der jeweiligen Justizvollzugsanstalt geöffnet und die innen liegenden Schreiben wurden dann ohne Umschlag an die Gefangenen verteilt. Gegenüber dem Bayerischen Staatministerium der Justiz und für Verbraucherschutz habe ich gegen diese Praxis datenschutzrechtliche Bedenken erhoben. Diesen Bedenken hat sich das Staatsministerium angeschlossen und es hat veranlasst, dass zukünftig Schreiben an Gefangene von sämtlichen Bayerischen Gerichten einzeln kuvertiert werden.

5.4.5 Keine inhaltliche Kontrolle von Anwaltspost bei Abschiebungshäftlingen

Im Rahmen einer Anfrage ist die Frage aufgetaucht, inwieweit der Schriftverkehr von Abschiebungshäftlingen der inhaltlichen Kontrolle unterliegt, wie sie auch bei Strafgefangenen vorgesehen ist. Da bei Strafgefangenen jedoch zumindest die Post mit dem Verteidiger von dieser inhaltlichen Briefkontrolle ausgenommen ist, habe ich gegenüber dem Bayerischen Staatsministerium der Justiz und für Verbraucherschutz darauf hingewiesen, dass dieses zumindest auch für den Schriftverkehr von Abschiebungsgefangenen mit Rechtsanwälten zu gelten hat, die den Abschiebungsgefangenen in dem der Haft zugrunde liegenden ausländerrechtlichen Verfahren vertreten.

Das Bayerische Staatsministerium der Justiz und für Verbraucherschutz hat sich dieser Haltung angeschlossen und mir mitgeteilt, dass bei Nachweis der Anwaltseigenschaft im dem ausländerrechtlichen Verfahren und entsprechender Kennzeichnung des Schriftwechsels dieser keiner inhaltlichen Briefkontrolle unterzogen werde. Man hat mir insofern zugesichert, die Leiterinnen und Leiter der Bayerischen Justizvollzugsanstalten in diesem Sinne nochmals zu sensibilisieren.

5.4.6 Abschließbare Schränke in Gemeinschaftshafträumen

Im Rahmen einer Eingabe wurde mir bekannt, dass den Gefangenen in bayerischen Justizvollzugsanstalten in Gemeinschaftshafträumen teilweise keine eigenen abschließbaren Schränke zur Verfügung stehen. Ein wirksamer Schutz etwa gegen eine unberechtigte Einsichtnahme in vertrauliche Unterlagen durch Mitgefangene bei Abwesenheit des Gefangenen besteht nur, wenn dieser die Unterlagen zur Verwahrung in die sog. „Kammer" gibt und sie sich bei Bedarf von den Justizvollzugsbediensteten wieder aushändigen lässt. Zusätzlich teilte mir das Bayerische Staatsministerium der Justiz und für Verbraucherschutz mit, dass auch die Möglichkeit bestehe, entsprechende Schriftstücke und Dokumente bei Verlassen des Haftraums regelmäßig im Dienstzimmer der Stationsbediensteten zu hinterlegen.

Beide Möglichkeiten halte ich aus datenschutzrechtlicher Sicht für nicht ausreichend. Die Möglichkeit der Verwahrung in der „Kammer" hat zwingend zur Folge, dass der Gefangene nicht ständig Zugriff auf die dort befindlichen Unterlagen hat. Auch eine Deponierung beim Stationsbeamten halte ich nicht für eine gleichwertige Lösung etwa im Vergleich zur Möglichkeit eines abschließbaren Schrankes im Haftraum.

Auf mein Tätigwerden hin hat mir das Bayerische Staatsministerium der Justiz und für Verbraucherschutz mitgeteilt, die Justizvollzugsanstalten mit der sukzessiven Ausstattung der betreffenden Gemeinschaftshafträume mit abschließbaren Schränken oder verschließbaren Wertfächern zu betrauen. Mit einem Abschluss der Maßnahme sei noch im Jahr 2012 zu rechnen.

5.4.7 Speicherung von eingestellten Straf- und Ermittlungsverfahren in der EDV der Justizvollzugsanstalten

Im Rahmen einer Eingabe bin ich darauf aufmerksam gemacht worden, dass in der überwiegenden Zahl der bayerischen Justizvollzugsanstalten Straf- und Ermittlungsverfahren, die nicht Gegenstand der aktuellen Haft sind, sowohl Eingang in die Gefangenenpersonalakten finden als auch im IT-Vollzugsprogramm abgespeichert werden.

Das Bayerische Staatsministerium der Justiz und für Verbraucherschutz hat mir dazu mitgeteilt, dass diese Speicherung erforderlich für den Vollzug der Freiheitsstrafe sei. Die Kenntnis von weiteren laufenden oder eingestellten Straf- und Ermittlungsverfahren sei für die Behandlung der Gefangenen, deren Wiedereingliederung nach der Haft und eine Vielzahl von vollzuglichen Entscheidungen unerlässlich. So seien Straf- und Ermittlungsverfahren nicht nur ein wichtiges Kriterium für die Prüfung der Gewährung vollzuglicher Maßnahmen, sondern auch ein wesentlicher Gesichtspunkt bei der Behandlung und Betreuung der Gefan-

genen. Nur wenn die Justizvollzugsanstalten möglichst umfassende Kenntnisse über bestehende Defizite in der Persönlichkeit und den Lebensverhältnissen der Gefangenen hätten, könne im Rahmen einer zielgerichteten Vollzugsplanung eine einzelfallorientierte Behandlung im Vollzug erfolgen und die Wiedereingliederung nach der Entlassung durch geeignete Maßnahmen gefördert und begleitet werden.

Grundsätzliche datenschutzrechtliche Bedenken habe ich hiergegen nicht erhoben. Ich habe gegenüber dem Bayerischen Staatsministerium der Justiz und für Verbraucherschutz jedoch zum Ausdruck gebracht, dass ich aus datenschutzrechtlicher Sicht einen unbeschränkten Zugriff auf diese Daten für nicht erforderlich und somit unzulässig erachte.

Seitens des Staatsministeriums wurden meine Bedenken aufgegriffen. So soll in Zukunft der Zugriff durch die Bediensteten der Justizvollzugsanstalten auf eine begrenzte Anzahl von Mitarbeitern beschränkt werden. Die IT-Leitstelle des bayerischen Justizvollzugs sei bereits mit der Erstellung einer entsprechenden Lösung beauftragt worden.

Im Berichtszeitraum ist diese Umstellung noch nicht erfolgt, ich werde die Umsetzung jedoch im Auge behalten.

5.4.8 Lichtbildausweise für Gefangene

Im Rahmen einer datenschutzrechtlichen Überprüfung einer bayerischen Justizvollzugsanstalt habe ich mir auch die dortigen Lichtbildausweise für Gefangene und deren Hintergrund erläutern lassen. Dabei wurde mir insbesondere erläutert, dass die Lichtbildausweise bei der Essensausgabe vorgezeigt werden müssen, da sich die Gefangenen für jeweils sechs Monate für eine Essensart (normal, ohne Schweinefleisch, vegetarisch) entscheiden müssten. Andernfalls sei eine Kalkulation bei der Essenszubereitung und Essensausgabe nicht möglich.

Ich habe bereits im Rahmen meiner datenschutzrechtlichen Überprüfung darauf hingewiesen, dass die Daten auf dem Lichtbildausweis auf das unbedingt erforderliche Maß zu begrenzen sind. Dabei habe ich insbesondere deutlich gemacht, dass ich die Aufnahme des Geburtsdatums für nicht erforderlich erachte.

Die überprüfte Justizvollzugsanstalt hat sich meinen datenschutzrechtlichen Bedenken angeschlossen und gibt nunmehr neue Lichtbildausweise aus, die das Geburtsdatum des Gefangenen nicht mehr enthalten. Weiterhin dürfen die Gefangenen gegenüber dem mit der Kostausgabe betrauten Mitgefangenen ihren Namen auf dem Lichtbildausweis abdecken.

5.5 Übersendung von Lichtbildern in Ordnungswidrigkeitenverfahren grundsätzlich nur mit „geschwärztem“ Beifahrer

Bereits in meinem 17. Tätigkeitsbericht habe ich darauf hingewiesen, dass Lichtbilder unbeteiligten Dritten im Rahmen der Fahrerermittlung zur Verfolgung und Ahndung von Verkehrsordnungswidrigkeiten in der Form vorzulegen sind, dass unbeteiligte Personen (Beifahrer, bzw. sonstige Mitfahrer) grundsätzlich nicht zu erkennen sind (siehe hierzu 17. Tätigkeitsbericht, Nr. 7.5.5). Nur soweit es im Interesse der Fahrerermittlung im Einzelfall erforderlich ist, (zunächst) den Beifah-

rer zu identifizieren, darf das Beweisfoto unbeteiligten Dritten vollständig zur Ansicht vorgelegt werden.

Im Berichtszeitraum wurden diese Vorgaben nach meinem Kenntnisstand überwiegend berücksichtigt. In einem Verfahren wurde jedoch ein Lichtbild mit nichtgeschwärztem Beifahrer an die Halterin – ein Autohaus – übersandt, da man seitens der Ahndungsbehörde davon ausgegangen war, dass eine Identifizierung des Fahrers einfacher sei, wenn auch die Person des Beifahrers – also etwa des mitfahrenden Autoverkäufers – bekannt gegeben werde. Auf meinen Hinweis hin, dass zum Zeitpunkt des Versands des Lichtbildes keine Anhaltspunkte vorlagen, dass eine Zuordnung des Fahrers ohne geschwärztes Lichtbild nicht möglich sei, hat die betroffene Ahndungsbehörde ihre zuvor vertretene Auffassung geändert und ist meinen datenschutzrechtlichen Bedenken beigetreten.

6 Kommunales

6.1 Veröffentlichung von kommunalen Amtsblättern im Internet

Ich erhebe keine grundsätzlichen Einwendungen, wenn Gemeinden und Landkreise ihr Amtsblatt im Rahmen ihrer Aufgabenerfüllung im Internet veröffentlichen. Durch Eingaben und Anfragen ist mir nun allerdings bekannt geworden, dass Gemeinden und Landkreise ihr Amtsblatt oftmals pauschal und viele Jahrgänge zurückreichend im Internet veröffentlichen. Die eigentlich geforderte Differenzierung auf Seiten der Gemeinde bzw. des Landkreises danach, ob die Internetveröffentlichung gerade des konkreten Teils des Amtsblattes zur Aufgabenerfüllung auch tatsächlich erforderlich ist, findet in diesen Fällen dann nicht statt. In der Praxis führt das dazu, dass personenbezogene Daten von Bürgern, in einem Fall z.B. die Tatsache der öffentlichen Bekanntmachung einer Baugenehmigung zugunsten eines bestimmten Bauherrn im Jahr 2002, auch nach vielen Jahren noch von der Internetseite einer betroffenen Gemeinde bzw. eines Landratsamtes abrufbar sind. Statt der eigentlich erforderlichen Abwägung vor der Internetveröffentlichung des Amtsblattes findet hier vielmehr eine pauschale und dauerhafte Archivierung nur einstmals für die Aufgabenerfüllung erforderlicher personenbezogener Daten im Internet statt. Dies halte ich für datenschutzrechtlich äußerst problematisch aufgrund der beliebigen Verknüpfbarkeit und Auswertbarkeit dieser Daten im Internet. Bekanntermaßen bestehen bei der Einstellung von personenbezogenen Daten in das Internet besondere Gefahren für das Recht auf informationelle Selbstbestimmung.

Da ich außerdem feststellen musste, dass bei den betroffenen Gemeinden und Landkreisen erhebliche Unsicherheiten bestehen, habe ich das Bayerische Staatsministerium des Innern gebeten, die Kommunen und Landkreise in geeigneter Weise für die Problematik zu sensibilisieren und insbesondere klarzustellen, dass vor der Internetveröffentlichung von Amtsblättern stets genau untersucht werden muss, ob gerade die Internetveröffentlichung des konkreten Teils des Amtsblattes zur Aufgabenerfüllung auch tatsächlich erforderlich ist.

Das Bayerische Staatsministerium des Innern hat meine Anregung aufgegriffen und die nachgeordneten Behörden durch ein Rundschreiben entsprechend unterrichtet.

6.2 Bereitstellung von Sitzungsunterlagen und -niederschriften im elektronischen Ratsinformationssystem der Kommune zum Abruf durch die Gemeinderatsmitglieder

In meinem 22. Tätigkeitsbericht habe ich mich dazu geäußert, unter welchen Voraussetzungen Unterlagen mit personenbezogenem Inhalt aus datenschutzrechtlicher und aus technisch-organisatorischer Sicht in elektronischen Ratsinformationssystemen zum Abruf durch die Gemeinderatsmitglieder bereitgestellt werden können (siehe hierzu 22. Tätigkeitsbericht, Nr. 8.5). Danach sind bei internen Ausarbeitungen, die zur Sitzungsvorbereitung oder sonstigen Information für den Gemeinderat bestimmt sind, bei Einladungen zu Sitzungen, die auch die Angaben der Tagesordnungspunkte der nichtöffentlichen Sitzungen erfordern,

und bei Sitzungsniederschriften, die nur für die Gemeinderatsmitglieder bestimmt sind, unbefugte Kenntnisnahmen und Zugriffe durch Dritte auszuschließen. Eine Stadt hat sich nun an mich mit der Frage gewandt, ob es datenschutzrechtlich zulässig ist, den Stadtratsmitgliedern die Niederschriften über die nichtöffentlichen Stadtrats- und Ausschusssitzungen über ein Ratsinformationssystem zur Verfügung zu stellen. Dies beurteilt sich nach Art. 54 Abs. 3 Satz 1 der Gemeindeordnung (GO).

Art. 54 Abs. 3 Satz 1 GO
Die Gemeinderatsmitglieder können jederzeit die Niederschrift einsehen und sich Abschriften der in öffentlicher Sitzung gefassten Beschlüsse erteilen lassen.

Schon in meinem 16. Tätigkeitsbericht habe ich mich in Übereinstimmung mit dem Bayerischen Staatsministerium des Innern unter der Nr. 8.2 dahin gehend geäußert, dass eine Herausgabe der Niederschriften über nichtöffentliche Sitzungen aus Gründen der Gewährleistung der Geheimhaltung und des Datenschutzes grundsätzlich nicht in Betracht kommt. Diese Auffassung wird auch in der Literatur vertreten. Nach Bauer/Böhle/Ecker, Bayerische Kommunalgesetze, Art. 54 Rdnr. 9 ist die Gemeinde zwar nicht gehindert, den Gemeinderatsmitgliedern Abschriften der Niederschriften öffentlicher Sitzungen zuzuleiten, im Interesse der Geheimhaltung nicht jedoch der in nichtöffentlicher Sitzung gefassten Beschlüsse samt Niederschrift, solange die Gründe für die Geheimhaltung noch nicht weggefallen sind. Ebenso Widtmann/Grasser/Glaser, Bayerische Gemeindeordnung, Art. 54 Rdnr. 13, die darauf hinweisen, dass der Gemeinderat insoweit durch die Geschäftsordnung auch keine abweichende Regelung treffen kann.

In elektronischen Ratsinformationssystemen werden den Ratsmitgliedern Unterlagen zum Abruf bereitgestellt. Auch wenn danach durch technisch-organisatorische Maßnahmen ein Ausdruck der am Bildschirm aufgerufenen Unterlagen verhindert werden kann, ist es doch regelmäßig möglich, den am Bildschirm sichtbar gemachten Text abzufotografieren oder ein Screenshot anzufertigen. Durch diese Möglichkeiten kann der Aufruf einer Unterlage am Bildschirm mit einer Ablichtung verglichen werden. Soweit daher eine Ablichtung nicht zulässig ist, scheidet auch eine Zurverfügungstellung im elektronischen Ratsinformationssystem zum Abruf aus. Dies gilt neben Niederschriften nichtöffentlicher Sitzungen auch für sonstige vertrauliche Informationen, die z.B. lediglich als Tischvorlagen für die Dauer der Sitzung zur Verfügung gestellt werden und von denen keine Ablichtungen angefertigt werden dürfen.

6.3 Keine Veröffentlichung von Schreiben mit personenbezogenem Inhalt auf der Homepage der Gemeinde

Der erste Bürgermeister einer Gemeinde wandte sich an mich mit dem Vorbringen, ein Gemeinderatsmitglied habe beim Landratsamt eine Dienstaufsichtsbeschwerde gegen ihn erhoben. Das Landratsamt habe die Dienstaufsichtsbeschwerde zurückgewiesen. Seinen Antrag auf Übernahme der Rechtsanwaltskosten, die ihm im Zusammenhang mit der Dienstaufsichtsbeschwerde entstanden seien, habe der Gemeinderat abgelehnt. Das von ihm daraufhin eingeschaltete Landratsamt habe ihm mitgeteilt, dass er keinen Anspruch auf Erstattung der von ihm verauslagten Rechtsanwaltkosten habe. Das Gemeinderatsmitglied verkünde nun unablässig in der Öffentlichkeit, es sei mit seiner Dienstaufsichtsbeschwerde voll „durchgedrungen“. Auch lasse es über die Presse die falsche Be-

hauptung verbreiten, die Angelegenheit sei zumindest „in einem Patt“ verlaufen. Da er sich nach eigenem Bekunden weder in einen öffentlichen Meinungsstreit noch eine langwierige Diskussion über die Presse verstricken wollte, beabsichtigte er, die Dienstaufsichtsbeschwerde des Gemeinderatsmitglieds und den Schriftwechsel dazu mit dem Landratsamt auf der Homepage der Gemeinde zu veröffentlichen. Dies wäre ein Verstoß gegen datenschutzrechtliche Bestimmungen gewesen. Ich habe dem ersten Bürgermeister deshalb aus den folgenden Gründen davon abgeraten:

Die Dienstaufsichtsbeschwerde bezog sich auf ein dienstliches Verhalten des ersten Bürgermeisters der Gemeinde. Die von diesem dazu beabsichtigte Veröffentlichung von Schriftstücken wäre ein Handeln in amtlicher Eigenschaft als erster Bürgermeister gewesen und wäre der Gemeinde zugerechnet worden (vgl. BayVGH, Beschluss vom 24.05.2006 – 4 CE.1217).

Die Veröffentlichung der Schriftstücke mit personenbezogenem Inhalt wäre eine Datenübermittlung an eine Vielzahl unbekannter Dritter gewesen (Art. 4 Abs. 6 Nr. 3 a BayDSG). Mangels Einwilligung der Betroffenen wäre eine solche Datenübermittlung nur auf der Grundlage einer Rechtsvorschrift zulässig gewesen (Art. 15 Abs. 1 BayDSG). Nach der hier in Betracht kommenden Regelung des Art. 19 Abs. 1 Nr. 1 BayDSG ist die Übermittlung personenbezogener Daten an nichtöffentliche Stellen zulässig, wenn sie zur Erfüllung der in der Zuständigkeit der übermittelnden Stelle liegenden Aufgaben erforderlich ist und der Grundsatz der Zweckbindung beachtet wird.

Anlass für die vom ersten Bürgermeister beabsichtigte Veröffentlichung von Schriftstücken mit personenbezogenem Inhalt im Zusammenhang mit der gegen diesen erhobenen Dienstaufsichtsbeschwerde waren öffentliche Äußerungen des Gemeinderatsmitglieds, er sei mit seiner Dienstaufsichtsbeschwerde „durchgedrungen“ bzw. die Angelegenheit sei zumindest „in einem Patt“ verlaufen. Die geplante Veröffentlichung sollte der Richtigstellung falscher Tatsachenbehauptungen durch das Gemeinderatsmitglied dienen. **Bei Äußerungen eines Dritten in der Öffentlichkeit ist eine Entgegnung der (betroffenen) öffentlichen Stelle (nur) insoweit zulässig, als es erforderlich ist für die Richtigstellung unwahrer Tatsachenbehauptungen des Betroffenen im Zusammenhang mit einem Verhalten der öffentlichen Stelle. Die Gebote der Zurückhaltung und Sachlichkeit sind dabei strikt zu beachten.**

Im vorliegenden Fall war es dazu nicht erforderlich, die Dienstaufsichtsbeschwerde und weitere Schriftstücke in diesem Zusammenhang zu veröffentlichen. Diese enthielten eine Vielzahl personenbezogener Aussagen, die für eine Richtigstellung der vom ersten Bürgermeister genannten unwahren Tatsachenbehauptungen nicht notwendig waren. Hinzu wäre gekommen, dass bei einer Veröffentlichung der Dienstaufsichtsbeschwerde die Anschrift und die Formulierungen im Einzelnen der Allgemeinheit mitgeteilt würden. Durch die Veröffentlichung von Schreiben, die ein Bürger an eine öffentliche Stelle richtet, oder die Weitergabe an die Presse, ohne dessen Einwilligung, werden regelmäßig schutzwürdige Interessen des betroffenen Bürgers beeinträchtigt (siehe hierzu 19. Tätigkeitsbericht, Nr. 8.9).

Verschärfend wäre im vorliegenden Fall noch die weltweite Veröffentlichung auf der Homepage der Gemeinde, verbunden mit der dadurch möglichen Auswertung nach verschiedenen Kriterien, die Übernahme durch Suchmaschinen und eine praktisch zeitlich unbegrenzte Speicherung hinzugekommen.

Im Ergebnis habe ich deshalb dem ersten Bürgermeister für eine Richtigstellung falscher Tatsachenbehauptungen in der Öffentlichkeit zu einer eigenen Darstellung des Sachverhalts durch die Gemeinde unter Beachtung der oben genannten Grundsätze, z.B. in Form einer Presseerklärung, geraten.

6.4 Auskunftsanspruch der Presse über nichtöffentliche Sitzungen des Gemeinderats?

Eine Kommune teilte mir mit, die örtliche Presse habe ihr gegenüber den Wunsch auf Erhalt der Tagesordnungen für die nichtöffentlichen Gemeinderatssitzungen geäußert. Die von der Kommune dagegen vorgetragenen Bedenken teile ich aus den folgenden Gründen:

Art. 4 Abs. 1 Satz 1 i.V.m. Abs. 2 Satz 2 des Bayerischen Pressegesetzes (BayPrG) gibt der Presse unter den dort genannten Voraussetzungen ein Recht auf Auskunft gegenüber Behörden, stellt für diese mangels entsprechender normenklarer bereichsspezifischer Regelung jedoch keine Rechtsgrundlage für die Übermittlung personenbezogener Daten dar (vgl. Wilde/Ehmann/Niese/Knoblauch, Bayerisches Datenschutzgesetz, Art. 19 Rdnr. 11 a). Die Übermittlung personenbezogener Daten an die Presse (als nichtöffentliche Stelle) setzt daher das Vorliegen einer (eigenständigen) Übermittlungsbefugnis voraus. Soweit keine bereichsspezifischen Regelungen vorliegen, richtet sich die Zulässigkeit einer Datenübermittlung an die Presse regelmäßig nach Art. 19 Abs. 1 BayDSG. Die Nummern 1 und 2 dieser Vorschrift sind zwar als Befugnisnormen konzipiert, sie enthalten jedoch bei Nichtvorliegen der Voraussetzungen im Umkehrschluss auch eine Verschwiegenheitspflicht, da dann eine Datenübermittlung nicht erfolgen darf (ebenso Wilde/Ehmann/Niese/Knoblauch, a.a.O., Art. 19 Rdnr. 11 a).

Mangels einer bereichsspezifischen Übermittlungsbefugnis war das Auskunftsverlangen der Presse in dem zu entscheidenden Fall nach Art. 19 Abs. 1 Nr. 2 BayDSG zu beurteilen. Datenübermittlungen an nichtöffentliche Stellen sind danach zulässig, wenn diese ein berechtigtes Interesse an der Kenntnis der zu übermittelnden Daten glaubhaft darlegen und der Betroffene kein schutzwürdiges Interesse an dem Ausschluss der Übermittlung hat. Das berechtigte Interesse der Presse ergibt sich aus Art. 4 Abs. 1 Satz 1 i.V.m. Abs. 2 Satz 2 BayPrG. Sind die Voraussetzungen dieser Vorschriften erfüllt, hat die Presse grundsätzlich ein Recht auf Auskunft, sofern nicht ein schutzwürdiges Interesse die Übermittlung ausschließt.

Ob der Betroffene ein schutzwürdiges Interesse an einem Ausschluss der Übermittlung hat, ist im jeweiligen Einzelfall im Rahmen einer Abwägung mit dem Übermittlungsinteresse der Presse zu prüfen. Auch der Bayerische Verwaltungsgerichtshof geht in seinem Beschluss vom 13.08.2004 von dem Erfordernis einer Güterabwägung zwischen der Notwendigkeit der öffentlichen Information und den entgegenstehenden Geheimhaltungsinteressen aus (BayVGH, Beschluss vom 13.08.2004, Az.: 7 CE 04.1601 – KommunalPraxis 2004, 394 ff.). In der Entscheidung wird insbesondere das Persönlichkeitsrecht als schutzwürdig hervorgehoben. Da nach Art. 52 Abs. 2 Satz 1 GO schutzwürdige personenbezogene Angelegenheiten in nichtöffentlicher Sitzung zu behandeln sind, stehen einer Information der Presse darüber regelmäßig überwiegende Geheimhaltungsinteressen der betroffenen Bürger entgegen.

6.5 Anhörung des von einer Dienstaufsichtsbeschwerde Betroffenen

Eine Petentin hat sich mit folgendem Sachverhalt an mich gewandt:

Ein Behördenmitarbeiter habe beim Aussteigen aus einem Dienst-Kfz ihr unmittelbar daneben geparktes Fahrzeug leicht beschädigt. Von ihr hierauf angesprochen, habe der Behördenmitarbeiter den von ihm verursachten Schaden in einer Art und Weise bagatellisiert, den sie als beleidigend empfand. Sie habe sich deshalb unter Angabe ihrer privaten Kontaktdaten beim Leiter der unschwer anhand des Dienst-Kfz zu ermittelnden Behörde über das Verhalten seines Mitarbeiters beschwert und verlangt, dass dieser Mitarbeiter sich bei ihr entschuldige. Der Name des Betroffenen sei ihr zu diesem Zeitpunkt nicht bekannt gewesen. Kurze Zeit später habe sie ein Schreiben der Rechtsanwältin eben dieses Behördenmitarbeiters erhalten. In diesem Schreiben sei sie beschuldigt worden, sich unwahr bzw. diffamierend über den Betroffenen bei dessen Anstellungsbehörde geäußert zu haben. Weiters sei sie aufgefordert worden, sich dahingehend zu erklären, diese Anschuldigungen nicht länger aufrechtzuerhalten.

In ihrer an mich gerichteten Eingabe hat die Petentin vor allem den Umstand gerügt, dass ihre privaten Kontaktdaten behördenintern zu einem Zeitpunkt an den Betroffenen weitergegeben wurden, in dem ihr als Beschwerdeführerin dessen Identität noch gar nicht bekannt war.

Im Rahmen meiner Sachverhaltsaufklärung bei der betroffenen Behörde hat sich zum einen herausgestellt, dass das Vorgehen der Petentin nachvollziehbarer Weise als Einlegung einer Dienstaufsichtsbeschwerde gegen den Betroffenen gewertet worden war und zum anderen, der von der Beschwerde betroffene Mitarbeiter in der Vergangenheit bereits mehrfach aufgrund seines aufbrausenden Charakterbildes negativ aufgefallen war.

In datenschutzrechtlicher Hinsicht habe ich die behördeninterne Weitergabe der privaten Kontaktdaten der Petentin an den von ihrer Beschwerde betroffenen Mitarbeiter wie folgt bewertet:

Es ist in der Behördenpraxis üblich, dass Dienstaufsichtsbeschwerden dem betroffenen Mitarbeiter zur Stellungnahme zugeleitet werden. Dies ist beamtenrechtlich grundsätzlich schon deswegen notwendig, da gemäß Art. 106 Bayerisches Beamtengesetz in den Personalakt Beschwerden, Behauptungen und Bewertungen, die für den Beamten ungünstig sind oder ihm nachteilig werden können, nur dann aufgenommen werden dürfen, wenn dieser vorher hierzu gehört worden ist.

Art. 106 Bayerisches Beamtengesetz
[1]Beamten und Beamtinnen sind zu Beschwerden, Behauptungen und Bewertungen, die für sie ungünstig sind oder ihnen nachteilig werden können, vor deren Aufnahme in die Personalakte zu hören, soweit die Anhörung nicht nach anderen Rechtsvorschriften erfolgt. [2]Ihre Äußerungen sind zur Personalakte zu nehmen.

Hierzu ist es aber nicht in jedem Einzelfall zwingend notwendig, dem betroffenen Mitarbeiter auch die persönlichen Kontaktdaten der/des Beschwerdeführerin/Beschwerdeführers zugänglich zu machen. In geeigneten Fällen sollte daher zukünftig in Erwägung gezogen werden, dem betroffenen Mitarbeiter nur den Sachverhalt ohne Nennung der Identität der/des Beschwerdeführerin/Beschwerdeführers zu unterbreiten.

Im vorstehend geschilderten Fall war dies letztlich schon deswegen nicht möglich, da aus der von der Petentin erhobenen Beschwerde eindeutig erkennbar war, dass diese eine Entschuldigung durch den betroffenen Mitarbeiter selbst erwartete. Bereits aus diesem Grunde benötigte der von ihrer Dienstaufsichtsbeschwerde Betroffene die persönlichen Kontaktdaten der Petentin. Ein Datenschutzverstoß lag somit nicht vor.

6.6 Herausgabe von Wahlvorschlägen zurückliegender Gemeinde- und Landkreiswahlen durch die Gemeindeverwaltung

Verschiedene Gemeinden wurden von privater Seite um Herausgabe der Adressdaten von Bewerbern zurückliegender Gemeinderatswahlen gebeten. Mit dem Bayerischen Staatsministerium des Innern vertrete ich dazu die folgende Auffassung, die das Ministerium in einem Rundschreiben den nachgeordneten Behörden mitgeteilt hat:

Nach Art. 33 des Gemeinde- und Landkreiswahlgesetzes (GLKrWG) und § 51 der Gemeinde- und Landkreiswahlordnung (GLKrWO) sind die zugelassenen Wahlvorschläge spätestens am 26. Tag vor dem Wahltag bekannt zu machen. Hierbei sind auch die Anschriften der Bewerber anzugeben (vgl. Anlagen 14, 15 zur GLKrWO i.V.m. § 101 GLKrWO). Bei Gemeindewahlen kann die Bekanntmachung entweder durch öffentlichen Anschlag oder entsprechend den Vorschriften, die für die Bekanntmachung von Satzungen der Gemeinde gelten (Art. 26 Abs. 2 GO und BekV), erfolgen (§ 98 Nr. 1 GLKrWO).

Die Verwendung der für die Durchführung der Kommunalwahlen erforderlichen Daten ist auf den gesetzlich bestimmten Zweck begrenzt, weshalb die Wahlvorschläge auch nur insoweit der Öffentlichkeit zugänglich gemacht werden dürfen, als das für die ordnungsgemäße Durchführung der Wahl notwendig ist (vgl. BVerfGE 5, 77, 82 und BVerfGE 65, 1, 46). Die öffentliche Bekanntgabe der Wahlvorschläge dient der Information der Wahlberechtigten und der Parteien und der Wählergruppen der jeweiligen kommunalen Gebietskörperschaft. Sie ist daher in örtlichem und zeitlichem Zusammenhang mit der jeweiligen Wahl zu sehen. Eine generelle Herausgabe der Wahlvorschläge an Dritte ist dagegen nicht von den gesetzlichen Datenübermittlungstatbeständen gedeckt und daher nicht zulässig, zumal dies ohne Einwilligung der Betroffenen erfolgen würde.

Soweit jedoch gesetzlich vorgesehene Veröffentlichungen in den Amtsblättern erfolgt sind, können sich Dritte diese Amtsblätter auf dem üblichen Weg beschaffen. Dies ist jedoch eine bloße Nebenfolge der im Interesse der Wahltransparenz erfolgenden Bekanntmachung bestimmter Daten im Zusammenhang mit Wahlen und bewirkt nicht, dass die Gemeinden die Daten der Betroffenen allgemein, ohne Rücksicht auf die Zweckbindung, weitergeben dürfen (siehe hierzu 12. Tätigkeitsbericht, Nr. 7.10.2, zur Herausgabe von Wahlvorschlagsdaten zu Werbezwecken).

6.7 Verwendung von Luftbildaufnahmen zur Ermittlung der Veranlagungsgrundlagen für Abwassergebühren

Ich erhalte immer wieder Anfragen von Bürgern, die wissen wollen, ob Kommunen zur Ermittlung der Veranlagungsgrundlagen für Abwassergebühren Luftbildaufnahmen heranziehen dürfen. Ich vertrete dazu folgende Auffassung:

Die datenschutzrechtliche Zulässigkeit von Luftbildaufnahmen durch Kommunen mit personenbezogenem Inhalt beurteilt sich, soweit keine bereichsspezifischen Regelungen (wie z.B. Satzungen) vorliegen, nach Art. 16 BayDSG. Nach Art. 16 Abs. 1 BayDSG ist die Datenerhebung zulässig, wenn die Kenntnis der Daten zur Erfüllung der in der Zuständigkeit der erhebenden Stelle liegenden Aufgaben erforderlich ist. Erforderlich ist eine Datenerhebung im datenschutzrechtlichen Sinne dann, wenn die Kenntnis der Daten zur Erreichung des Zwecks objektiv geeignet und im Verhältnis zu dem angestrebten Zweck auch angemessen erscheint. Die Datenkenntnis muss also zur Aufgabenerfüllung objektiv beitragen, das heißt, die Aufgabenerfüllung ermöglichen, unterstützen oder fördern. Auch eine rein zeitliche Beschleunigung genügt (siehe Wilde/Ehmann/Niese/Knoblauch, Bayerisches Datenschutzgesetz, Art. 16 Rdnr. 10).

Die Heranziehung von Luftbildaufnahmen ist zur Feststellung der genauen Größe der gebührenpflichtigen Flächen der einzelnen Grundstücke geeignet. Demgegenüber liegen hier auch keine überwiegenden schutzwürdigen Interessen des Betroffenen am Ausschluss der Datenerhebungen vor, wenn bei der Erstellung der Luftbildaufnahmen folgende Maßgaben beachtet werden:

- Die Datenerhebung ist als vorbereitende Maßnahme zur Gebührenerhebung erforderlich (z.B. weil aufgrund des Gebührenmaßstabs eine möglichst genaue Ermittlung der befestigten oder nicht befestigten Flächen eines Grundstücks vonnöten ist).

- Die Luftbildaufnahmen lassen aufgrund der Auflösung keine unmittelbaren personenbezogenen Daten erkennen, wie jedenfalls digitale Orthophotos mit einer Auflösung von 40 cm oder größer pro Bildpunkt.

- Eine Datenerhebung beim Betroffenen mit seiner Kenntnis (hier: im Rahmen einer Begehung des Grundstücks) würde zu einem unverhältnismäßigen Aufwand oder nicht zu dem gewünschten Erfolg führen (z.B. weil der Grundstückseigentümer die Größe der befestigten Flächen seines Grundstücks in der Regel nicht detailliert kennt und diese erst langwierig ermittelt werden müsste); darüber hinaus wäre eine Begehung des Grundstücks durch Mitarbeiter der für die Erhebung der Abwassergebühren zuständigen Stelle bzw. von ihr beauftragte Dritte (z.B. Ingenieure eines Vermessungsbüros) möglicherweise mit einem tieferen Eingriff in das informationelle Selbstbestimmungsrecht verbunden, da hier zwangsläufig eine detailgenaue Kenntnisnahme der jeweiligen Örtlichkeit erfolgen würde.

- Das Grundstück ist in der Regel von außen bzw. von oben für jedermann (z.B. Segelflieger) einsehbar.

- Die Luftbildaufnahmen werden nur zweckgebunden verwendet und auch nur solange aufbewahrt, wie dies zur Aufgabenerfüllung (hier: Gebührenermittlung) erforderlich ist.

Bei der Beurteilung der Frage, ob überwiegende schutzwürdige Interessen des Betroffenen einen Ausschluss der Datenerhebung in Form von Luftbildaufnahmen rechtfertigen können, ist auch zu berücksichtigen, dass es sich bei Luftbildaufnahmen, die z.B. aufgrund ihrer Auflösung nicht unmittelbar personenbezogene Daten erkennen lassen, lediglich um bloße Außenaufnahmen von Gebäuden und Aufnahmen von Grundstücken handelt, aus denen sich Rückschlüsse über die Persönlichkeit bzw. über persönliche Lebensumstände des Betroffenen nicht ableiten lassen. Das allgemeine Persönlichkeitsrecht des Betroffenen ist hier somit typischerweise eher geringfügig tangiert.

Gegen die Erstellung von derartigen Luftbildaufnahmen von Grundstücken zum Zwecke der Ermittlung der Veranlagungsgrundlagen für Abwassergebühren erhebe ich aus den oben genannten Gründen daher keine grundsätzlichen datenschutzrechtlichen Einwände. Eine Information des Betroffenen über die Erstellung von Luftbildaufnahmen zu diesem Zweck ist nach Art. 16 BayDSG weder vor der Erstellung der Aufnahmen noch im Nachhinein erforderlich. Aus datenschutzrechtlicher Sicht ist es jedoch wünschenswert, wenn dem betroffenen Grundstückseigentümer zumindest die Möglichkeit der Stellungnahme zu dem Ergebnis der Luftbildaufnahmen gegeben wird.

6.8 Datenschutzrechtliche Anforderungen bei Bürgerbefragungen

Kommunen, die sich mittels Fragebogenaktionen an die Bürger wenden, um daraus Informationen etwa für stadtplanerische Zwecke zu gewinnen, dürfen dabei die datenschutzrechtlichen Anforderungen nicht außer Acht lassen. Im Berichtszeitraum erreichten mich diverse Anfragen von Gemeinden, die sich nach den datenschutzrechtlichen Vorgaben bei der Durchführung solcher Bürgerbefragungen erkundigten, aber auch Beschwerden von betroffenen Bürgern, die die mangelnde Transparenz der behördlichen Datenerhebung kritisierten. Im Rahmen meiner Beratungs- und Prüftätigkeit habe ich dabei insbesondere auf Folgendes hingewiesen:

Bei der Durchführung von Bürgerbefragungen durch bayerische öffentliche Stellen, bei denen die abgefragten Daten einer bestimmten oder bestimmbaren Person zugeordnet werden können, handelt es sich um Datenerhebungen, die – soweit keine bereichsspezifischen Vorschriften zur Anwendung kommen – nach Art. 16 BayDSG zu beurteilen sind. Danach ist das Erheben personenbezogener Daten zulässig, wenn ihre Kenntnis zur Erfüllung der in der Zuständigkeit der erhebenden Stelle liegenden Aufgaben erforderlich ist (Art. 16 Abs. 1 BayDSG). Die Stadtplanung bzw. -entwicklung ist eine solche kommunale Aufgabe. Daher ist es grundsätzlich nicht zu beanstanden, wenn sich eine Kommune auf der Grundlage eines Fragebogens dahingehende Informationen beschafft. Die öffentliche Stelle hat dabei die Fragen so zu formulieren, dass die damit erhobenen Daten im Einzelnen zu ihrer Aufgabenerfüllung erforderlich sind. Soweit möglich, bietet sich eine geschlossene Fragestellung an, um den Bürger nicht zu überflüssigen, sprich nicht erforderlichen Angaben zu „verleiten".

Werden personenbezogene Daten beim Betroffenen mit seiner Kenntnis erhoben, so ist der Erhebungszweck ihm gegenüber anzugeben (Art. 16 Abs. 3 Satz 1 BayDSG). Soweit keine Auskunftspflicht aufgrund einer (bereichsspezifischen) Rechtsnorm besteht, ist die Beantwortung der einzelnen Fragen für den Betroffenen freiwillig. Er ist hierauf deutlich hinzuweisen (Art. 16 Abs. 3 Satz 2

BayDSG). Bei einer Datenerhebung auf schriftlichem Weg ist außerdem die Rechtsvorschrift stets anzugeben (Art. 16 Abs. 3 Satz 4 BayDSG). Besonders sensible personenbezogene Daten dürfen dabei nur unter den zusätzlichen Voraussetzungen des Art. 15 Abs. 7 BayDSG erhoben werden.

Vielfach sind jedoch zur behördlichen Aufgabenerfüllung statistische Angaben ausreichend, das heißt, es ist nicht erforderlich, die abgefragten Daten einer bestimmten oder bestimmbaren natürlichen Person zuordnen zu können; dies ist bereits bei der Erstellung des Fragebogens zu berücksichtigen. Insbesondere zur Durchführung kommunaler Planungen halte ich es grundsätzlich für ausreichend, wenn lediglich statistische Angaben erhoben werden. Der Fragebogen ist dabei so abzufassen, dass keine Rückschlüsse auf die betreffende(n) Person(en) möglich sind, d.h. es dürfen keine Angaben gefordert werden, welche (z.B. auch in Kombination) eine Identifizierbarkeit ermöglichen könnten. Um sicherzustellen, dass die Fragebögen anonym zurückgesandt werden, empfiehlt sich der Hinweis, auch auf dem Rückantwortkuvert auf die Angabe von Namen und Anschrift zu verzichten. Bei einer freiwilligen Angabe personenbezogener Daten (z.B. Name, Anschrift) ist klarzustellen, inwieweit diese Daten zur (weiteren) behördlichen Aufgabenerfüllung erforderlich sind und wofür sie verwendet werden. Falls eine Zuordnung der Kontaktdaten zum Fragebogen nicht erforderlich ist, ist sicherzustellen, dass diese getrennt vom Fragenteil (z.B. in einem separaten Kuvert) an die erhebende Stelle zurückgeschickt und dort auch separat gespeichert werden.

In jedem Fall dürfen die erhobenen Daten nur zu dem beabsichtigten (und mitgeteilten) Zweck genutzt und verarbeitet werden (Art. 17 Abs. 1 Nr. 2 BayDSG). Es ist außerdem sicherzustellen, dass ein unbefugter Zugriff Dritter auf die Daten nicht möglich ist. Die Fragebögen sind nach ihrer Auswertung unverzüglich zu vernichten (Art. 12 Abs. 1 Nr. 2 BayDSG).

6.9 Ein besonderes Jubiläum

Eine Stadt hatte auf Eingaben einiger weniger Bürger über einen längeren Zeitraum mit einer außergewöhnlichen Maßnahme reagiert, die eine datenschutzrechtliche Beanstandung unvermeidbar nach sich zog.

Unter der Überschrift „Jubiläum in der Stadt“ teilte die Kommune in einer Pressemitteilung mit, sie könne ein ganz besonderes „Jubiläum“ aus der Stadtverwaltung vermelden. Seit Dezember 2005 seien genau 50 Eingaben betreffend Angelegenheiten der Stadt bei der Kommunalaufsicht des Landratsamtes eingegangen. Für 90 Prozent dieser Eingaben seien nur drei Eingabeführer – die in der Pressemitteilung unter prozentualer Angabe ihrer Anteile an den 50 Eingaben namentlich genannt werden – verantwortlich. Weiter wird in der Pressemitteilung ausgeführt, dass lediglich 12 dieser Eingaben erfolgreich gewesen seien, während 38 und damit über 75 Prozent als unbegründet zurückgewiesen worden seien. Die erfolgreichen Eingaben hätten dabei in erster Linie Verstöße gegen Verfahrensbestimmungen in der Geschäftsordnung zum Gegenstand gehabt. Zum Schluss weist die Stadt in ihrer Pressemitteilung noch darauf hin, dass durch diese 50 Eingaben allein in der Stadtverwaltung ein Arbeitsaufwand von insgesamt 150 Arbeitstagen entstanden sei; damit sei allein ein Mitarbeiter mehr als ein halbes Jahr beschäftigt gewesen. Hinzu komme noch der Arbeitsaufwand in den von den Eingaben betroffenen und einbezogenen sonstigen Behörden.

Der Unmut der Stadt über den verursachten erheblichen Arbeitsaufwand ist verständlich. Doch selbst wenn die Eingaben offenbar überwiegend unbegründet eingelegt wurden: Die betroffenen Bürger haben mit ihren Eingaben von ihrem Petitionsrecht Gebrauch gemacht – und die Stadt hätte nicht derart überreagieren dürfen. Zwar kann der Umstand, dass Eingabeführer im Vorfeld selbst die Presse über die Erhebung von Eingaben informiert hatten, dazu führen, dass im Rahmen der Abwägung eine Datenübermittlung im Einzelfall zulässig sein kann, z.B. in Form einer Gegendarstellung als Erwiderung auf unwahre Tatsachenbehauptungen des Betroffenen im Zusammenhang mit einem Verhalten der öffentlichen Stelle. Dies ändert jedoch nichts daran, dass die in der Pressemitteilung namentlich erwähnten Personen jedenfalls ein schutzwürdiges Interesse hatten, nicht generell „an den Pranger" gestellt zu werden. Durch die Hervorhebung der niedrigen Erfolgsquote der Beschwerden und dem damit verbundenen Arbeitsaufwand in der Pressemitteilung wurde – auch durch die Art der Darstellung – suggeriert, es habe sich überwiegend um querulatorische Eingaben gehandelt. Dass es vorrangig nicht um die sachliche Information der Öffentlichkeit ging, legte auch die Titulierung „Jubiläum" nahe. Die Datenübermittlung stellte einen erheblichen Datenschutzverstoß dar, den ich beanstandet habe.

6.10 Fundsachen mit digitalen Inhalten

Mit dieser für die alltägliche Praxis in den Fundbehörden immer relevanter werdenden Thematik habe ich mich bereits in meinem letzten Tätigkeitsbericht befasst (siehe hierzu 24. Tätigkeitsbericht, Nr. 2.3.4). Der in diesem Beitrag geschilderte Sachverhalt betraf den Fall, dass es gemäß § 976 BGB zum **Eigentumsübergang auf die Gemeinde** kam. Insoweit bin ich der Auffassung, dass die nach dem Eigentumsübergang an der Fundsache grundsätzlich umfassend bestehende Befugnis der Gemeinde im Sinne des § 903 BGB, wie in meinem damaligen Beitrag im Einzelnen dargelegt, datenschutzrechtlich überlagert ist. Um die Thematik in datenschutzrechtlicher Hinsicht umfassend zu würdigen, weise ich ergänzend auf Folgendes hin:

In Übereinstimmung mit dem Bayerischen Staatsministerium der Justiz und für Verbraucherschutz vertrete ich die Auffassung, dass als **Fundsache** gemäß § 965 Abs. 1 BGB der **Datenträger einschließlich der darauf abrufbaren digitalen Daten** anzusehen ist und mit der Ablieferung der Fundsache bei der Fundbehörde damit insgesamt ein öffentlich-rechtliches Verwahrungsverhältnis entsteht.

Ebenfalls in Überstimmung mit dem Bayerischen Staatsministerium der Justiz und für Verbraucherschutz bin ich der Auffassung, dass damit eine Vernichtung der auf der Fundsache gespeicherten Daten durch die Fundbehörde **vor** Ablauf der fundrechtlichen Verwahrpflicht eine – ggf. schadensersatzpflichtige – Beschädigung der Fundsache darstellen kann.

Kommt es nach § 973 BGB zum **Eigentumsübergang auf den Finder**, erhält dieser damit zugleich einen Herausgabeanspruch gegen die Gemeinde aus dem öffentlich-rechtlichen Verwahrverhältnis. Insoweit bin ich der Auffassung, dass auch dieser Herausgabeanspruch wiederum datenschutzrechtlich überlagert ist. Im Einzelnen:

– Würde die Gemeinde die Fundsache mitsamt der auf dieser gespeicherten personenbezogenen Daten des ehemaligen Eigentümers an den Fin-

der herausgeben, läge darin eine Datenübermittlung an eine nichtöffentliche Stelle. Eine solche ist jedoch – mangels einschlägiger speziellerer Regelungen im Sinne des Art. 2 Abs. 7 BayDSG – nur unter den Voraussetzungen des Art. 19 Abs. 1 BayDSG zulässig. An diesen Voraussetzungen wird es aber regelmäßig fehlen. Weder ist die Herausgabe der Fundsache mitsamt den auf dieser gespeicherten Daten gemäß Art. 19 Abs. 1 Nr. 1 BayDSG zur Aufgabenerfüllung der Fundbehörde erforderlich bzw. liegen die Voraussetzungen der Art. 17 Abs. 1 Nr. 2, Abs. 2 bis 4 BayDSG vor noch ist ein schutzwürdiges Interesse des ehemaligen Eigentümers an einem Ausschluss der Übermittlung gemäß Art. 19 Abs. 1 Nr. 2 BayDSG auszuschließen.

– Daher sind vor einer Herausgabe der Fundsache an den Finder die auf dieser gespeicherten personenbezogenen Daten des ehemaligen Eigentümers zu löschen (siehe hierzu 24. Tätigkeitsbericht, Nr. 2.3.4). Ihren danach bestehenden Löschverpflichtungen können die Gemeinden beispielsweise auch durch – datenschutzkonforme – Kooperationen mit Fachgeschäften nachkommen. Auch kann es für die Beurteilung der Angemessenheit des Löschaufwands von Bedeutung sein, ob sich der Finder zur Übernahme der Kosten für eine Datenlöschung durch eine Fachwerkstatt bereit erklärt.

6.11 Weitergabe von Melderegisterdaten Minderjähriger an einen Adressbuchverlag

Nach Art. 32 Abs. 3 und 4 i.V.m. Art. 31 Abs. 7 Bayerisches Meldegesetz (MeldeG) darf Adressbuchverlagen Auskunft über den Vor- und Familiennamen, den Doktorgrad und die Anschriften sämtlicher Einwohner erteilt werden, die das 18. Lebensjahr vollendet haben, der Weitergabe ihrer Daten nicht widersprochen haben und für die keine Auskunftssperren vorliegen. In einem mir bekannt gewordenen Fall hatte eine Gemeinde dabei jedoch auch die Melderegisterdaten (Namen und Anschriften) von Minderjährigen an einen Adressbuchverlag übermittelt. In ihrer Stellungnahme teilte mir die betreffende Gemeinde mit, dass vermutlich ein Eingabefehler bei der im Fachverfahren vorgesehenen Selektierung des Auswertungszeitraums ursächlich für die unzulässige Datenübermittlung gewesen sei. Außerdem wurde mitgeteilt, dass schon bei der vorangegangenen Auflage des Adressbuches – bis dato unbemerkt – ein ähnlicher Fehler passiert sei.

Zwar hat die betreffende Gemeinde sofort nach Bekanntwerden des Vorgangs eine weitere Auslieferung der Adressbücher durch den Verlag gestoppt. Auch hat sie sich mit ihrem Verfahrensanbieter in Verbindung gesetzt, um künftig bereits programmtechnisch sicherzustellen, dass bei der Auswahl von Einwohnerdaten zur Übermittlung an Adressbuchverlage nur mehr die Melderegisterdaten der volljährigen Einwohner berücksichtigt werden. Die entsprechende Programmänderung wurde daraufhin unverzüglich umgesetzt. Jedoch war zum Zeitpunkt des Bekanntwerdens des Vorgangs bereits ca. ein Drittel der Auflage des Adressbuchs von 45.000 Stück ausgeliefert worden. Die damit erfolgte Bekanntgabe der Daten war somit nicht mehr rückgängig zu machen. Die unzulässige Datenübermittlung habe ich beanstandet.

Art. 32 Abs. 3 MeldeG
Adressbuchverlagen darf Auskunft über die in Art. 31 Abs. 1 Satz 1 bezeichneten Daten sämtlicher Einwohner, die das 18. Lebensjahr vollendet haben, erteilt werden. Die Betroffenen haben das Recht, der Weitergabe ihrer Daten nach Satz 1 zu widersprechen. Hierauf sind sie bei der Anmeldung hinzuweisen.

6.12 Weitergabe von Melderegisterdaten im Zusammenhang mit der Wahl eines Ausländerbeirats

Ein Bürger hat sich bei mir darüber beschwert, er sei von einer ihm nicht bekannten amerikanischen Mitbürgerin angeschrieben worden, mit der Bitte, ihren Wahlvorschlag zur Ausländerbeiratswahl zu unterstützen. Die Überprüfung des Vorgangs hat ergeben, dass die Wahlbewerberin die Wohnsitzgemeinde des Petenten um die Übermittlung einer Auflistung der amerikanischen Staatsbürger mit Wohnsitz in der betreffenden Kommune gebeten hatte, um für ihre Kandidatur zur Wahl als Ausländerbeirat im Landkreis zu werben. Die Gemeinde teilte ihr darauf die Namen und Anschriften der amerikanischen Mitbürger mit. Ich habe diesen Sachverhalt aus datenschutzrechtlicher Sicht wie folgt bewertet:

Nach Art. 32 Abs. 1 und 4 i.V.m. Art. 31 Abs. 7 Meldegesetz (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 und es liegt für ihn keine Auskunftssperre vor.

Zu den „allgemeinen" Wahlen zählen Wahlen zum Europäischen Parlament, Bundestag, Landtag, Bezirkstag, Kreistag, Landrat, Gemeinderat und Bürgermeister (vgl. Ziffer 35.2 VollzBekMeldeG). Eine Abstimmung findet bei einem Volksentscheid oder Bürgerentscheid statt. Wahlen zu Ausländerbeiräten (oder Seniorenbeiräten) sind keine „allgemeinen" Wahlen, dazu sind die wahlberechtigten Personenkreise zu sehr eingeschränkt (Böttcher/Ehmann, Pass-, Ausweis- und Melderecht in Bayern, Art. 32 Rdnr. 11). Darauf habe ich auch bereits in meinem 13. Tätigkeitsbericht unter der Nr. 8.3.3 1. Spiegelstrich hingewiesen. Die Weitergabe von Meldedaten im Zusammenhang mit solchen Wahlen ist daher unzulässig. Darüber hinaus halte ich es auch für zweifelhaft, ob die Bewerberin überhaupt als „andere Trägerin eines Wahlvorschlags" angesehen werden konnte, da sie ja erst um die nötigen Unterstützungsunterschriften geworben hatte.

Eine nach Art. 32 Abs. 1 Satz 1 MeldeG zulässige Gruppenauskunft muss sich außerdem auf eine Gruppe von Wahl- oder Stimmberechtigten beschränken, für deren Zusammensetzung ausschließlich das Lebensalter der Betroffenen maßgeblich ist, eine andere Differenzierung, z.B. nach der Staatangehörigkeit (wie vorliegend erfolgt), ist nicht zulässig.

Den Datenschutzverstoß habe ich beanstandet.

Art. 32 Abs. 1 MeldeG
(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 Klinische Krebsregister

Bereits in meinem letzten Tätigkeitsbericht habe ich mich mit der Bayerischen Krebsregistrierung befasst und auf die gewichtigen Unterschiede zwischen der Konzeption des bayerischen Krebsregistergesetzes (BayKRG) und der Praxis der Klinikregister hingewiesen, wenn es um die Erhebung, Verarbeitung und Nutzung von Daten krebserkrankter Personen geht (siehe hierzu 24. Tätigkeitsbericht, Nr. 7.1). Aufgrund zahlreicher Gespräche mit Vertretern des Bayerischen Staatsministeriums für Umwelt und Gesundheit und Verantwortlichen der Krebsregister sowie aufgrund von Besuchen und Kontrollen bei einzelnen Registern wurde bestätigt, dass insbesondere die Identitätsdaten entgegen der Gesetzeslage (Art. 6 Abs. 1 Satz 5 BayKRG) auch ohne Einwilligung der Betroffenen bei den Klinikregistern dauerhaft gespeichert und weiter verarbeitet bzw. genutzt werden. Damit dieser gesetzeswidrige Zustand sein Ende findet, habe ich eine umfassende Neuregelung der Konzeption der Krebsregistrierung in den Klinikregistern vorgeschlagen.

Art. 6 BayKRG Aufgaben und Befugnisse der Klinikregister
(1) …[5]Eine Verarbeitung und Nutzung der Identitätsdaten (Art. 4 Abs. 1) ist nur mit Einwilligung der Betroffenen zulässig.

Das Bayerische Staatsministerium für Umwelt und Gesundheit hat mir im Berichtszeitraum dazu einen ersten Entwurf zur Änderung des BayKRG vorgelegt. Der Arbeitsentwurf verdeutlichte schon im vorgesehenen Titel – „Gesetz über die Krebsregister in Bayern (BayKRG)“ – die Zielrichtung, nämlich nun auch die Aufgaben und Funktionen der klinischen Register einer umfassenden Regelung zuzuführen und entsprach inhaltlich den Intentionen des Nationalen Krebsplans, den das Bundesministerium für Gesundheit (BMG) gemeinsam mit der Deutschen Krebsgesellschaft, der Deutschen Krebshilfe und der Arbeitsgemeinschaft Deutscher Tumorzentren am 16.06.2008 vorgestellt hat. Dieser verfolgt unter anderem das Ziel einer aussagekräftigen Qualitätsberichterstattung durch klinische Krebsregister und unterstützt den flächendeckenden Ausbau der klinischen Krebsregister zur Erfassung der Qualität der Versorgung aller Krebskranken, die stärkere Vernetzung untereinander sowie mit den epidemiologischen Krebsregistern, die Einbindung in die sektorenübergreifende Qualitätssicherung nach § 137 SGB V, die einheitliche und transparente Dokumentation und Darstellung sowie die Rückmeldung der Daten an alle beteiligten Leistungserbringer. Zur gesetzgeberischen Umsetzung des Krebsplans liegt inzwischen auch ein Referentenentwurf des Bundesgesundheitsministeriums vor, der insbesondere den flächendeckenden Ausbau von klinischen Krebsregistern unter einheitlichen Rahmenbedingungen befördern soll. Die Länder sollen zur Einrichtung klinischer Krebsregister verpflichtet werden. Darüber hinaus sollen sie die behandlungsortbezogene Datenerfassung auf der Grundlage eines bundeseinheitlichen Tumordatensatzes (Datensatz der Arbeitsgemeinschaft Deutscher Tumorzentren und der Gesellschaft der epidemiologischen Krebsregister in Deutschland) regeln.

Der Arbeitsentwurf des Gesundheitsministeriums beschreibt dementsprechend bereits die Aufgaben der klinischen Krebsregister (Qualitätssicherung, Versor-

gungsunterstützung, Versorgungsforschung in der onkologischen Versorgung) und regelt den Umgang mit den Identitätsdaten auf der klinischen Registerebene. Es werden ausdrücklich die Zwecke (Funktionen) benannt, für die die gemeldeten Identitätsdaten dort verarbeitet und genutzt werden dürfen. Im Entwurf ist die getrennte Speicherung der Identitätsdaten von den medizinischen Daten vorgesehen. Ferner soll die Verarbeitung und Nutzung der Identitätsdaten durch das klinische Krebsregister ohne Einwilligung des Patienten vorgenommen werden können. Der Patient soll allerdings schon vor der ärztlichen Meldung an das epidemiologische Krebsregister über sein ihm zustehendes Widerspruchsrecht umfassend aufgeklärt werden. Neu eingeführt wird zudem die Befugnis zum Abgleich mit Daten des Melderegisters.

Die Einführung einer Widerspruchslösung für die dauerhafte Verarbeitung und Nutzung von Identitätsdaten durch die klinischen Krebsregister ist vor dem Hintergrund der schon existierenden gesetzlichen Konzeption zur epidemiologischen Krebsregistrierung und dem Ziel der Erlangung einer flächendeckenden, vollständigen und damit aussagekräftigen Datenbasis zu sehen. Ich habe allerdings deutlich zum Ausdruck gebracht, dass die Widerspruchslösung als Grundlage für die weitere zweckgebundene Verwendung sowohl der medizinischen als auch der Identitätsdaten auf Ebene der klinischen Krebsregister aus datenschutzrechtlicher Sicht nur dann mitgetragen werden kann, wenn die Unterrichtung und die Information über das Widerspruchsrecht den Patienten tatsächlich in die Lage versetzt, eine informierte und freie Entscheidung darüber zu treffen, ob er seine Daten für die Registrierung und ihre Zwecke zur Verfügung stellen will. Dreh- und Angelpunkt der datenschutzgerechten Gestaltung der Krebsregistrierung muss aus meiner Sicht daher die umfassende und allgemeinverständliche Aufklärung der Patienten darüber sein, was mit ihren Daten geschieht. Der Patient muss sein Recht zum Widerspruch kennen und wissen, was er damit bewirken kann. Anzustreben ist folglich eine gesetzliche Gestaltung, aus der sich im Vergleich zu einer Einwilligungslösung so wenige datenschutzrechtliche Nachteile wie möglich für den Patienten ergeben.

Dies setzt auch voraus, dass angemessene technische und organisatorische Maßnahmen durch die klinischen Krebsregister getroffen werden, insbesondere um unbefugte Zugriffe auf personenbezogene Patientendaten so weitgehend wie möglich auszuschließen. Im Hinblick auf den vorgesehenen Meldregisterabgleich, der automatisiert und in Zusammenarbeit mit der AKDB erfolgen soll, habe ich deshalb ausdrücklich gefordert, dass dieser nur mit Hilfe pseudonymisierter Daten erfolgen darf bzw. gewährleistet ist, dass der AKDB keine Identitätsdaten von Krebspatienten übermittelt werden.

Es sind noch umfangreiche Anstrengungen nötig, um ein in sich schlüssiges und an die datenschutzrechtlichen Erfordernisse angepasstes Konzept zur Neustrukturierung der klinischen Krebsregister zu erzielen. Allerdings bin ich zuversichtlich, dass dies gelingen kann. Den angestoßenen Diskussions- und Gesetzgebungsprozess werde ich auch weiterhin intensiv begleiten.

7.2 Orientierungshilfe Krankenhausinformationssysteme

Unter meinem Vorsitz hat die 81. Konferenz der Datenschutzbeauftragten des Bundes und der Länder in ihrer Sitzung am 16./17.03.2011 in Würzburg einstimmig eine „Orientierungshilfe Krankenhausinformationssysteme“ beschlossen.

Der Beschluss der Konferenz („Datenschutzkonforme Gestaltung und Nutzung von Krankenhauinformationssystemen“) sowie die Orientierungshilfe können auf meiner Homepage www.datenschutz-bayern.de unter der Rubrik „Konferenzen“ abgerufen werden. Dort ist auch die frühere Entschließung „Krankenhausinformationssysteme datenschutzgerecht gestalten!“ der 78. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 08./09.10.2009 in Berlin veröffentlicht.

Die Entschließungen gehen zurück auf Initiativen der Arbeitskreise der Datenschutzkonferenz für Gesundheit und Soziales sowie für Technische und organisatorische Datenschutzfragen, die in ihren Herbstsitzungen des Jahres 2009 die Einrichtung einer gemeinsamen Unterarbeitsgruppe „KIS“ beim Berliner Datenschutzbeauftragten zur Erstellung einer „Orientierungshilfe Krankenhausinformationssysteme“ mit datenschutzrechtlichen und technisch-organisatorischen Anforderungen an Klinikinformationssysteme vereinbart haben. An der Orientierungshilfe haben Datenschutzbeauftragte der Evangelischen Kirche in Deutschland und der Katholischen Kirche mitgearbeitet. Ferner wurden auch Hersteller von Krankenhausinformationssystemen, Betreiber, Anwendervereinigungen und Datenschutzbeauftragte von Krankenhäusern eingebunden.

Die Orientierungshilfe hat zum Ziel, Krankenhäusern und Softwareherstellern von Krankenhausinformationssystemen in ganz Deutschland einen einheitlichen Orientierungsrahmen für die datenschutzkonforme Ausgestaltung und Nutzung von informationstechnischen Systemen zur Verwaltung und Dokumentation elektronischer Patientendaten zur Verfügung zu stellen. Neben einem Begleitpapier und einem Glossar enthält die Orientierungshilfe im Teil 1 normative Eckpunkte zur Zulässigkeit von Zugriffen auf elektronische Patientendaten im Krankenhaus und im Teil 2 technische Anforderungen an die Gestaltung und den Betrieb von Krankenhausinformationssystemen.

Ich habe die Orientierungshilfe allen meiner Zuständigkeit unterliegenden Krankenhäusern zugeleitet, weil meine Erfahrungen, insbesondere aus Prüfungen und Beratungsgesprächen, gezeigt haben, dass derzeit eingesetzte Krankenhausinformationssysteme moderne Organisationsformen und Prozesse nur bedingt datenschutzkonform unterstützen können. So musste ich leider immer wieder feststellen, dass Krankenhausinformationssysteme insbesondere keine ausreichend differenzierten – am Grundsatz der Erforderlichkeit orientierten – Zugriffe bzw. Zugriffsbeschränkungen auf Patientendaten vorsehen. Ich habe jedoch auch den Eindruck gewonnen, dass die Verantwortlichen in den Krankenhäusern dem Thema gegenüber aufgeschlossen sind und erforderliche Anpassungen im Rahmen der Möglichkeiten vornehmen wollen. Ich hoffe deshalb, dass die Orientierungshilfe dazu beitragen wird, die Betreiber von Krankenhäusern und die Hersteller von Krankenhausinformationssystemen künftig dabei zu unterstützen, Krankenhausinformationssysteme datenschutzgerecht zu entwickeln und sie im Krankenhaus entsprechend einzusetzen.

7.3 Privatgerät im Krankenhaus

Ein neuer Trend in Krankenhäusern geht dahin, Mitarbeitern die Anbindung an das Unternehmensnetzwerk mit privaten Endgeräten (Laptops, Smartphones, Tablet PCs) sowie die ortsungebundene Nutzung dieser privaten Geräte für dienstliche Zwecke zu gestatten („Bring Your Own Device“). Insoweit verweise

ich auch auf meine weiteren Ausführungen zur Verwendung privater mobiler Geräte in diesem Tätigkeitsbericht (siehe Nr. 2.1.3). Hinzuweisen ist in diesem Zusammenhang auf meine Ausführungen zur Telearbeit in diesem Tätigkeitsbericht (siehe Nr. 2.1.4 und Nr. 2.2.5).

Für externe Zugriffe auf das Krankenhausinformationssystem misst Art. 27 Abs. 4 Sätze 1 bis 4 Bayerisches Krankenhausgesetz (BayKrG) dem allgemeinen datenschutzrechtlichen Erforderlichkeitsgrundsatz besonderes Gewicht bei, indem es die Nutzung von Patientendaten durch Krankenhausärzte, andere Personen im Krankenhaus und die Krankenhausverwaltung nur insoweit gestattet, als sie zur Erfüllung der jeweiligen Aufgaben erforderlich ist.

Art. 27 BayKRG Datenschutz
(4) [1]Die Krankenhausärzte dürfen Patientendaten nutzen, soweit dies im Rahmen des krankenhausärztlichen Behandlungsverhältnisses, zur Aus-, Fort- und Weiterbildung im Krankenhaus, zu Forschungszwecken im Krankenhaus oder im Forschungsinteresse des Krankenhauses erforderlich ist. [2]Sie können damit andere Personen im Krankenhaus beauftragen, soweit dies zur Erfüllung dieser Aufgaben erforderlich ist; zu Zwecken der Forschung nach Satz 1 können sie anderen Personen die Nutzung von Patientendaten gestatten, wenn dies zur Durchführung des Forschungsvorhabens erforderlich ist und die Patientendaten im Gewahrsam des Krankenhauses verbleiben. [3]Diese Personen sind zur Verschwiegenheit zu verpflichten. [4] Die Krankenhausverwaltung darf Patientendaten nutzen, soweit dies zur verwaltungsmäßigen Abwicklung der Behandlung der Patienten erforderlich ist . . . .

In Bezug auf die Krankenhausärzte steht dabei die Aufgabe der krankenhausärztlichen Behandlung im Vordergrund. Generell gilt, dass alle Zugriffsmöglichkeiten auf klinische Informationssysteme strikt an die dienstlichen Notwendigkeiten anzupassen sind. In diesem Zusammenhang weise ich auch auf die Orientierungshilfe Krankenhausinformationssysteme hin, die von der 81. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 16./17.03.2011 beschlossen wurde (abrufbar auf meiner Homepage www.datenschutz-bayern.de unter der Rubrik Konferenzen). Darin sind die rechtlichen und technischen Anforderungen an eine datenschutzkonforme Gestaltung und Nutzung von Krankenhausinformationssystemen dargestellt, insbesondere ist dort auch der Grundsatz der Erforderlichkeit für den Zugriff auf Patientendaten im Krankenhaus berücksichtigt. Zur Orientierungshilfe Krankenhausinformationssysteme verweise ich auf obige Ausführungen (siehe Nr. 7.2).

Ich halte es aus datenschutzrechtlichen Erwägungen grundsätzlich nicht für zulässig, Mitarbeitern eines Krankenhauses durch den Einsatz privater Endgeräte den Zugriff auf klinische Informationssysteme des Krankenhauses zu ermöglichen. Vorausgesetzt, ein externer Abruf von Patientendaten wäre erforderlich, könnten und müssten den betroffenen Mitarbeitern Dienst-Geräte zur Nutzung zur Verfügung gestellt werden. Meines Erachtens kann bei privaten Geräten nicht hinreichend sichergestellt werden, dass kein Unbefugter Einsicht in die Daten des Klinikums nehmen kann bzw. Patientendaten im Gewahrsam des Krankenhauses bleiben (siehe Art. 27 Abs. 4 BayKrG). Durch den Abruf von Klinikdaten von außerhalb des Krankenhauses mittels privater Geräte von Mitarbeitern wären die mit einem Gewahrsam des Krankenhauses verbundenen ausschließlichen Verfügungs-, Einfluss- und Kontrollmöglichkeiten aus rechtlicher Sicht selbst dann nicht mehr gegeben, wenn Patientendaten nur einsehbar wären und eine Speicherung der Daten auf dem privaten Gerät tatsächlich technisch ausge-

schlossen werden könnte. Private Geräte sind der Kontrolle des Klinikums insbesondere im Hinblick auf die privat Verwendung findende Hard- und Software nicht hinreichend unterworfen. Der Besitzer kann das Gerät verleihen oder beliebige Software und damit auch Schadsoftware auf seinem Gerät installieren. Fraglich ist in diesem Zusammenhang auch, ob und in welchem Umfang aus Datenschutzsicht erforderliche Einschränkungen der privaten Nutzung durch eine vom Arbeitgeber eingeforderte Einwilligung des Mitarbeiters (z.B. zur Löschung sämtlicher, auch privater Daten bei mehrmaliger Falscheingabe einer PIN oder bei Verlust des Gerätes) rechtswirksam vereinbart bzw. durchgesetzt werden könnten.

Das Bayerische Staatsministerium für Wissenschaft, Forschung und Kunst teilt ausdrücklich meine Rechtsauffassung betreffend den Zugriff mittels privater Endgeräte auf das klinische Informationssystem in Universitätsklinika. Ich habe darüber hinaus die Auffassung vertreten, dass ich auch die Nutzung des persönlichen E-Mail Postfachs mittels privater Geräte grundsätzlich für unzulässig halte, wenn nicht ausgeschlossen werden kann, dass dort personenbezogene medizinische Informationen, insbesondere Patientendaten enthalten sind. Aufgrund der grundsätzlichen Bedeutung für alle Krankenhäuser in Bayern habe ich auch insoweit das Bayerische Staatsministerium für Umwelt und Gesundheit unterrichtet.

7.4 Aufbewahrung psychiatrischer Patientenunterlagen

Im Rahmen einer Prüfung eines Bayerischen Universitätsklinikums habe ich festgestellt, dass dort für die Aufbewahrung der psychiatrischen und psychosomatischen Patientenunterlagen keinerlei Regelungen bestanden, diese vielmehr unbefristet aufbewahrt wurden.

Die Klinik begründete diese Speicherpraxis zunächst damit, dass sich die Gegebenheiten im psychiatrischen Fachgebiet erheblich von anderen medizinischen Disziplinen unterscheiden würden. Es sei zu befürchten, dass für den einzelnen Patienten erhebliche Nachteile entstehen, wenn seine Patientenunterlagen vernichtet werden. Dies gelte insbesondere in Anbetracht der oft chronischen Krankheitsverläufe. Die Vernichtung von älteren Vorgängen schränke außerdem die Aussagekraft und Gültigkeit von wissenschaftlichen Untersuchungen, sog. Längs- und Familienuntersuchungen, gravierend ein. Beides könne kurz- bzw. langfristig für den Patienten zu inkorrekten Therapieentscheidungen zu seinem Nachteil führen. Ein anderer Aspekt seien eventuelle Ansprüche aus der Zeit des Nationalsozialismus, die einzelne Patienten noch geltend machen könnten. Solange einzelne Patienten keine andere Regelung wünschten, was zumeist jedoch nicht der Fall sei, würde die Klinik deshalb an der unbefristeten Aufbewahrung festhalten.

Ich habe im weiteren Schriftverkehr und bei einem persönlichen Gespräch mit den Verantwortlichen des Universitätsklinikums darauf hingewiesen, dass nach der einschlägigen Vorschrift des Art. 27 Abs. 2 Satz 1 BayKrG Patientendaten grundsätzlich nur erhoben und aufbewahrt werden dürfen, soweit dies zur Erfüllung der Aufgaben des Krankenhauses oder im Rahmen des krankenhausärztlichen Behandlungsverhältnisses **erforderlich** ist. Welche Patientenakten hierfür jeweils erforderlich sind, hat das Universitätsklinikum auf Grund fachlicher Erwägungen zu entscheiden und zu begründen. Zugleich habe ich auf Art. 14 BayArchivG hingewiesen, wonach die Einrichtung eines eigenen Archivs des

Universitätsklinikums möglich ist, sofern insbesondere die technisch-organisatorischen Voraussetzungen des Bayerischen Archivgesetzes beachtet werden.

Das Universitätsklinikum hat daraufhin begonnen, ein Archivierungskonzept zu entwickeln. Diesen Entwicklungsprozess werde ich aufmerksam verfolgen und dem Universitätsklinikum bei Bedarf beratend zur Seite stehen.

7.5 Krankenhausseelsorge

Im Berichtszeitraum war ich anlässlich eines Besuchs des Datenschutzbeauftragten der Bayerischen (Erz-)Diözesen mit Fragen zur Übermittlung von Patientendaten an die Krankenhausseelsorge befasst.

Zum Einen wurde die Frage aufgeworfen, in welcher Weise die Information der Krankenhauseelsorge über die für deren Arbeit notwendigen Patientendaten bereits im Zusammenhang mit der Aufnahme bzw. dem Abschluss des Behandlungsvertrages datenschutzgerecht sichergestellt werden kann.

Hierzu ist voranzustellen, dass schon die Tatsache der Aufnahme ins Krankenhaus der ärztlichen Schweigepflicht unterliegt. Sowohl nach § 203 Abs. 1 Strafgesetzbuch (StGB) wie auch aufgrund datenschutzrechtlicher Grundsätze ist deshalb eine Befugnis zur Offenbarung der Tatsache des Krankenhausaufenthaltes in Form der Bekanntgabe von Patientendaten an eine dem Krankenhaus angeschlossene haupt- oder nebenamtliche Krankenhausseelsorge erforderlich. Sie müsste daher entweder aus einer entsprechenden spezialgesetzlichen Regelung abgeleitet werden können oder sich aus der (ggf. mutmaßlichen) Einwilligung des betreffenden Patienten ergeben.

In Deutschland ist die Krankenhausseelsorge („Anstaltsseelsorge“) in der Verfassung garantiert (Art. 4 Abs. 1 und 2, Art. 140 GG in Verbindung mit Art. 141 Weimarer Reichsverfassung – WRV; für Bayern s. Art. 107 und 148 der Bayerischen Verfassung – BV). Soweit das Bedürfnis nach Gottesdienst und Seelsorge in Krankenhäusern besteht, sind die Religionsgesellschaften zur Vornahme religiöser Handlungen zuzulassen, wobei jeder Zwang fernzuhalten ist (Art. 141 WRV, vgl. Art. 148 BV). In ähnlicher Weise sichert auch der am 20.07.1933 zwischen dem Heiligen Stuhl und dem Deutschen Reich geschlossene und als Reichskonkordat bezeichnete Staatskirchenvertrag die Anstaltsseelsorge (s. Art. 28 sowie Schlussprotokoll zu Art. 28; zur weiteren Gültigkeit s. Konkordatsurteil des BVerfG vom 26.03.1957, 2 BvG 1/55). Danach ist die Kirche in Krankenhäusern der öffentlichen Hand im Rahmen der allgemeinen Hausordnung zur Vornahme seelsorgerlicher Besuche und gottesdienstlicher Handlungen zuzulassen. Bereits in Art. 11 des Konkordats zwischen seiner Heiligkeit Papst Pius XI. und dem Staate Bayern vom 29.03.1924 sowie in Art. 17 des Staatsvertrags zwischen dem Bayerischen Staate und der Evangelischen Landeskirche Bayern vom 15.11.1924 verpflichtete sich Bayern unter anderem dazu, in seinen „Krankenanstalten, sei es durch Anstellung eigener Geistlicher oder auf andere zweckmäßige Weise auf seine Kosten eine entsprechende Seelsorge einzurichten.“

Die genannten Vorschriften bilden die Grundlagen der Krankenhausseelsorge. Den betreffenden Religionsgemeinschaften steht danach ein Recht auf Zulassung und Vornahme religiöser Handlungen zu, soweit im Krankenhaus ein Bedürfnis der Patienten nach Gottesdienst und Seelsorge besteht. Hierfür muss der Staat die organisatorischen Voraussetzungen religiöser Betätigung entspre-

chend seiner Organisationshoheit in der jeweiligen Einrichtung schaffen. Dazu gehört, der Krankenhausseelsorge den Zugang zu ermöglichen, soweit ein Bedürfnis nach Gottesdienst und Seelsorge besteht und entsprechend erklärt worden ist (s. Korioth in Maunz/Dürig, GG, 62. Ergänzungslieferung 2011, Art. 141 WRV, Rdnr. 2 ff.). Befinden sich Mitglieder der Religionsgemeinschaften im Krankenhaus, kann (widerleglich) auf ein Bedürfnis nach Seelsorge geschlossen werden. Aus diesem Grund darf bei der Aufnahme nach der Zugehörigkeit zu einer Religionsgemeinschaft gefragt werden, wenn zugleich auf die Freiwilligkeit der Antwort hingewiesen wird. Nur wenn Mitglieder einer Religionsgemeinschaft ausdrücklich ein Bedürfnis nach Seelsorge verneinen, besteht insoweit kein Zulassungsrecht. Zum Anspruchsinhalt gehört zudem das Recht auf „Vornahme religiöser Handlungen". Zu ermöglichen sind also seelsorgerische Einzelgespräche, kultische und liturgische Handlungen wie Gottesdienste, Andachten, Gebets- und Bibelkreise, aber auch Gespräche und Hilfen zu Lebensfragen aller Art (zum Vorstehenden siehe Korioth in Maunz/Dürig, ebenda, Rdnr. 7 - 8).

Dem Vorgenannten Rechnung tragend habe ich in meinem Zuständigkeitsbereich immer vertreten, dass ein Patient nach einer Konfession, für die im konkreten Krankenhaus eine Krankenhauseelsorge angeboten wird, gefragt werden darf, sofern hierbei auf die Freiwilligkeit der Angabe hingewiesen wird. Erfolgt eine entsprechende und informiert freiwillige Auskunft durch den Patienten, kann diese auch bei fehlender ausdrücklicher Einwilligungserklärung dahingehend interpretiert werden, dass der Patient mit der Verständigung eines haupt- oder nebenamtlich am Krankenhaus tätigen Seelsorgers einverstanden ist und an diesen Name, Station und Zimmernummer des betreffenden Patienten weitergegeben werden dürfen (siehe hierzu 17. Tätigkeitsbericht, Nr. 3.4.4, 18. Tätigkeitsbericht, Nr. 3.3.1 und 22. Tätigkeitsbericht, Nr. 13.2.4).

Es bestehen nach alledem aus datenschutzrechtlicher Sicht keine Bedenken, wenn im Zusammenhang mit dem Abschluss des Behandlungsvertrags die als freiwillig gekennzeichnete Abfrage der Konfessionszugehörigkeit erfolgt. Mittels einer Ankreuzmöglichkeit für den Fall, dass der Patient der Weitergabe seiner Daten (Name, Station, Zimmernummer) widersprechen will, könnte auch insoweit Rechtssicherheit geschaffen werden.

Die Offenbarung von Patientendaten gegenüber der jeweiligen Heimatpfarrei, einem (Laien-)Besuchsdienst oder vergleichbarer Einrichtungen, die nicht der Krankenhausseelsorge zuzurechnen sind, wäre hingegen nur zulässig, wenn der Patient dieser Datenweitergabe zuvor ausdrücklich zugestimmt hat.

Eine weitere Frage betraf die Einbindung eines Seelsorgers in ein Behandlungsteam und die damit verbundene Offenbarung von Patientendaten einschließlich sensibler Gesundheitsdaten an den Seelsorger.

Die Einbindung der Krankenhausseelsorge in die Behandlung der Patienten wird durch die von Staatsseite zu schaffenden organisatorischen Voraussetzungen religiöser Betätigung ermöglicht, betrifft aber in erster Linie die Frage der speziellen Ausprägung und weniger den garantierten Rahmen seelsorgerischer Betätigung. Wird ein Seelsorger in ein Behandlungsteam aufgenommen, werden ihm zum Teil sensibelste Gesundheitsdaten weitergegeben. Die Weitergabe dieser Daten ist nur aufgrund einer ausdrücklichen, unter Umständen aber auch stillschweigenden oder mutmaßlichen Einwilligung des Patienten zulässig. Welche Patientendaten dem Seelsorger im Einzelfall offenbart werden dürfen, hängt von der Reichweite der jeweiligen Patienteneinwilligung ab; eine Zugriffsmöglichkeit

auf alle Patientendaten bzw. auf das Krankenhausinformationssystem ist meines Erachtens aber auch im Einzelfall nicht erforderlich, um seelsorgerische Aufgaben zu erfüllen.

Die Regelung der Offenbarungsbefugnisse gegenüber einem Seelsorger, der in ein Behandlungsteam aufgenommen wird, eignet sich aus datenschutzrechtlicher Sicht nicht dazu, zum regelmäßigen Gegenstand des Aufnahmeverfahrens gemacht zu werden. Für den Patienten ist zu diesem Zeitpunkt zumeist weder der Behandlungsverlauf noch sein zukünftiges Bedürfnis nach Einbindung eines Seelsorgers absehbar. Keinesfalls ausreichend wäre die Regelung einer Widerspruchslösung dergestalt, dass der Patient der Übermittlung von Daten an den Seelsorger im Aufnahmeblatt bzw. im Behandlungsvertrag widersprechen müsste.

7.6 Hygieneverordnung für medizinische Einrichtungen

Das Bayerische Staatsministerium für Umwelt und Gesundheit hat mir im Berichtszeitraum den Entwurf einer Verordnung zur Änderung der Verordnung zur Hygiene und Infektionsprävention in medizinischen Einrichtungen (MedHygV) zugeleitet. Diese Verordnung regelt die erforderlichen Maßnahmen zur Verhütung, Erkennung, Erfassung und Bekämpfung von nosokomialen Infektionen und Krankheitserregern mit Resistenzen in medizinischen Einrichtungen. Ich habe die Gelegenheit wahrgenommen, datenschutzrechtlich zu diesem Verordnungsentwurf Stellung zu nehmen. Erfreulicherweise fanden meine Vorschläge sehr weitreichend Berücksichtigung:

a) Ein wesentlicher Punkt aus datenschutzrechtlicher Sicht war die Einführung einer bereichsspezifischen datenschutzrechtlichen Regelung in der MedHygV, unter welchen Voraussetzungen die Einrichtungen personenbezogene Daten offenbaren dürfen, die der ärztlichen Schweigepflicht unterliegen. Zugleich sieht die Verordnung die Bedingungen vor, unter denen das Fachpersonal (Krankenhaushygieniker, Hygienefachkräfte, hygienebeauftragte Ärztinnen und Ärzte sowie Hygienebeauftragte in der Pflege) Patientendaten erheben, verarbeiten oder nutzen darf.

b) Eine datenschutzgerechte Lösung fand sich auch für den Spezialfall des externen, nicht im Krankenhaus beschäftigten, Krankenhaushygienikers. Der Einsatz von externen Dritten lässt sich nicht ohne weiteres mit den sich aus Art. 27 Abs. 4 und 5 Bayerisches Krankenhausgesetz ergebenden Grundsätzen vereinbaren, wonach Gesundheitsdaten von Patienten im Gewahrsam des Krankenhauses zu verbleiben haben. Ich habe jedoch im Hinblick auf den Gestaltungsspielraum des Verordnungsgebers eine Beratung durch externe Krankenhaushygieniker unter der Bedingung akzeptiert, dass Patientendaten im Zusammenhang mit der Verarbeitung und Nutzung durch diesen externen Dienstleister im Gewahrsam der Einrichtung verbleiben.

c) Ich habe darauf bestanden, dass die Aufzeichnungen der Einrichtungen über nosokomiale Infektionen, das Auftreten von Krankheitserregern mit speziellen Resistenzen und Multiresistenzen sowie den Antibiotikaverbrauch nach § 23 Abs. 4 Infektionsschutzgesetz – IfSG mangels entsprechender Erfordernisse nicht personenbeziehbar ausgestaltet sein dürfen.

d) In Bezug auf die in der Verordnung geregelte Rolle der Leiter von Einrichtungen bei der fortlaufenden, systematischen Erfassung von Infektionsdaten bzw. der Erfassung von Daten zu Antibiotikaresistenzen und zu Art und Umfang des Antibiotikaverbrauchs folgte man ebenfalls meiner Empfehlung und orientiert sich in Bezug auf den Verordnungstext nun an der Wortwahl des § 23 Abs. 4 IfSG. Mir kam es diesbezüglich vor allem darauf an, dass den Leitern der Einrichtungen zwar die Sicherstellung der genannten, nicht personenbezogenen Aufzeichnungen obliegt, sie aber nicht selbst die zugrundeliegenden personenbezogenen Daten erheben, verarbeiten oder nutzen dürfen. Die vorherige Formulierung wäre insoweit missverständlich gewesen.

e) Aufgrund von § 23 Abs. 8 Nr. 10 IfSG ist durch die Landesregierung auch eine Regelung zu treffen über die Information von aufnehmenden Einrichtungen und niedergelassenen Ärzten bei der Verlegung, Überweisung oder Entlassung von Patienten über Maßnahmen, die zur Verhütung und Bekämpfung von nosokomialen Infektionen und von Krankheitserregern mit Resistenzen erforderlich sind (sektorenübergreifender Informationsaustausch). Der mir vorgelegte Entwurf ging hierüber hinaus, indem die relevanten Einrichtungen Informationen über Maßnahmen auch an den Rettungsdienst und den Krankentransport weitergeben sollten. Ich habe insoweit keine entsprechenden Regelungsbedürfnisse gesehen. Für Krankentransporte, die als rettungsdienstliche Leistung im Sinne des Art. 1 Abs. 1 des Bayerischen Rettungsdienstgesetzes (BayRDG) zu bewerten sind (s. Art. 2 Abs. 5 BayRDG), gilt Art. 40 Abs. 2 BayRDG, wonach Besteller rettungsdienstlicher Leistungen verpflichtet sind, der Integrierten Leitstelle oder dem Unternehmer bei der Bestellung das Vorliegen oder den Verdacht einer Infektionskrankheit oder einer Besiedelung mit multiresistenten Erregern mitzuteilen. Zudem ist in Art. 40 Abs. 1 BayRDG vorgeschrieben, dass Patienten mit multiresistenten Erregern bzw. solche, bei denen die Möglichkeit der Keimstreuung besteht, nur mit nach dem BayRDG genehmigten und geeigneten Krankenkraftwagen transportiert werden dürfen. Bei Krankenfahrten, die keine rettungsdienstliche Leistung darstellen (z.B. Taxifahrten), ist der Besteller nach dem BayRDG zwar nicht dazu verpflichtet, über das Vorliegen oder den Verdacht einer Infektion oder Besiedelung mit multiresistenten Erregern zu informieren. Diese Transporte, die nicht durch medizinisches Fachpersonal durchgeführt werden müssen, kommen jedoch ohnehin nur in Betracht, wenn keine besonderen Schutzmaßnahmen erforderlich sind. Aus Klarstellungsgründen und mangels datenschutzrechtlicher Nachteile habe ich mich damit einverstanden erklärt, dass die Informationsweitergabe an den Rettungsdienst weiter Erwähnung findet. Sonstige Krankentransporte betrifft die Norm nicht mehr.

f) Auf meine Anregung hin wurde in die Begründung auch noch aufgenommen, dass im Rahmen des sektorenübergreifenden Informationsaustauschs nur diejenigen Informationen weitergegeben werden dürfen, die erforderlich sind, um die notwendigen Verhütungs- oder Bekämpfungsmaßnahmen festlegen zu können. Welche dies sind, ist einzelfallbezogen zu entscheiden.

Die Änderungsverordnung zur MedHygV ist im Wesentlichen mit den von mir vorgeschlagenen datenschutzrechtlichen Anmerkungen am 01.09.2012 in Kraft getreten.

7.7 Anzeigepflicht für die Betreiber von Einrichtungen für ambulantes Operieren

Dass einer Behörde zuweilen die Ausübung einer gesetzlich vorgeschriebenen Aufgabe nicht ausreichend ermöglicht wird, weil ihr notwendige Informationen nicht vorliegen und auch Vorschriften zum Datenschutz, insbesondere zum Sozialdatenschutz, diesen Mangel nicht heilen können, zeigt folgender Fall:

Nach § 23 Abs. 6 Satz 1 IfSG in Verbindung mit Art. 16 Abs. 2 GDVG sowie § 10 Abs. 1 MedHygV hat das Gesundheitsamt die sich im Zuständigkeitsbereich befindlichen Einrichtungen für ambulantes Operieren infektionshygienisch zu überwachen. Eine verbindliche Anmeldung derartiger Einrichtungen beim Gesundheitsamt war rechtlich bisher nicht vorgesehen. Um die gesetzlich zugewiesene Aufgabe erfüllen zu können, hat sich ein Landratsamt an die zuständige Bezirksstelle der Kassenärztlichen Vereinigung gewandt und um Mitteilung gebeten, welche Einrichtungen für ambulantes Operieren im Landkreis tätig sind. Da die Kassenärztliche Vereinigung Bayerns (KVB) die Genehmigungen zum ambulanten Operieren erteilt, lägen dieser die entsprechenden Daten vor.

Ungeachtet einer Erhebungsbefugnis des Gesundheitsamtes sah sich die Kassenärztliche Vereinigung Bayerns meines Erachtens völlig zu Recht außerstande, die geforderten Informationen dem Landratsamt zur Verfügung zu stellen, da es sich bei den von der Kassenärztlichen Vereinigung Bayerns erhobenen und gespeicherten Daten über die Ärzte bzw. die Praxen von Ärzten, die ambulante Eingriffe durchführen, um **Sozialdaten** im Sinne von § 67 Abs. 1 SGB X handelt, für deren Übermittlung an die Gesundheitsämter keine Befugnis im Sozialgesetzbuch besteht.

In § 285 SGB V befinden sich zwar spezielle Vorschriften für die Erhebung, Verarbeitung oder Nutzung von Sozialdaten der Ärzte durch die Kassenärztliche Vereinigung Bayerns. Die von der KVB rechtmäßig erhobenen und gespeicherten Sozialdaten dürfen gemäß § 285 Abs. 3 Satz 1 SGB V aber nur für die Zwecke der Aufgaben nach § 285 Abs. 1 SGB V in dem jeweils erforderlichen Umfang verarbeitet (insbesondere übermittelt) oder genutzt werden, für andere Zwecke nur, soweit dies durch Rechtsvorschriften des Sozialgesetzbuches angeordnet oder erlaubt ist. Eine Übermittlung von Arztdaten an ein Gesundheitsamt würde jedoch **zu anderen als den in § 285 Abs. 1 SGB V vorgesehenen Zwecken** erfolgen, nämlich zur Erfüllung der gesetzlichen Verpflichtung des Gesundheitsamtes, Einrichtungen für ambulantes Operieren infektionshygienisch zu überwachen, für die auch keine Rechtsvorschrift des Sozialgesetzbuches, insbesondere auch nicht § 69 Abs. 1 Nr. 1 SGB X, eine derartige Übermittlung anordnet oder erlaubt.

Um für dieses zwar datenschutzrechtlich korrekte, letztlich aber im Hinblick auf die Sicherstellung des Patientenschutzes doch sehr unbefriedigende Ergebnis Abhilfe zu schaffen, habe ich dem zuständigen Bayerischen Staatsministerium für Umwelt und Gesundheit vorgeschlagen, im Rahmen der anstehenden Novellierung der MedHygV (siehe Nr. 7.6) eine **Anzeigepflicht** für die Betreiber von Ein-

richtungen für ambulantes Operieren gegenüber dem zuständigen Gesundheitsamt einzuführen.

Dieser Vorschlag wurde vom Bayerischen Staatsministerium für Umwelt und Gesundheit aufgenommen. Nach § 14 Abs. 1 Sätze 2 und 3 MedHygV haben nunmehr seit Inkrafttreten dieser Verordnung am 01.09.2012 Einrichtungen für ambulantes Operieren die Aufnahme ihrer Tätigkeit bei der für den Ort der Niederlassung zuständigen unteren Behörde für Gesundheit, Veterinärwesen, Ernährung und Verbraucherschutz anzuzeigen. Einrichtungen, die im Zeitpunkt des Inkrafttretens dieser Verordnung ihre Tätigkeit schon aufgenommen haben, haben diese innerhalb von drei Monaten ab Inkrafttreten dieser Verordnung bei der zuständigen Behörde anzuzeigen.

Nach der Begründung dieser Verordnung dient diese Anzeigepflicht dem Zweck, dass die Überwachungsbehörden Kenntnis erlangen, bei welchen Einrichtungen in ihrem Zuständigkeitsbereich es sich um solche für ambulantes Operieren handelt. Die Anzeigepflicht betrifft alle Einrichtungen, die von der Kassenärztlichen Vereinigung Bayerns eine Genehmigung zur Ausführung und Abrechnung ambulanter Operationen einschließlich der notwendigen Anästhesien besitzen. Zwar fallen Privatärzte nicht unter diese Genehmigungspflicht, in diesem Fall handelt es sich jedoch dann um eine Einrichtung für ambulantes Operieren, wenn auch diese die Voraussetzungen für eine solche Genehmigungspflicht erfüllen würden und entsprechende Tätigkeiten vorgenommen werden.

Im Interesse des Patientenschutzes erschien mir die Einführung einer Anzeigepflicht für die Betreiber von Einrichtungen für ambulantes Operieren zweckmäßig, vor allem auch vor dem Hintergrund, dass nunmehr die Ausübung einer gesetzlich vorgeschriebenen Kontrolltätigkeit der Gesundheitsämter ermöglicht wird, ohne die Behörden zu veranlassen, „kreativ“ nach eigenen Wegen zu suchen, um an dringend erforderliche Informationen für ihre Aufgabenerfüllung zu gelangen.

7.8 Impfausweise und Impfbescheinigungen von Schülern

In meinem letzten Tätigkeitsbericht habe ich darüber berichtet, dass mir das Staatsministerium für Umwelt und Gesundheit einen Gesetzentwurf vorgelegt hat, der insbesondere eine **Pflicht zur Vorlage eines Impfausweises bei der Schuleingangsuntersuchung** beinhaltete (siehe hierzu 24. Tätigkeitsbericht, Nr. 7.2).

Im aktuellen Berichtszeitraum wurde mir erneut ein Gesetzentwurf zugeleitet, der bei **Schuleingangsuntersuchungen** und bei weiteren **schulischen Impfberatungen** die Vorlage **vorhandener Impfausweise und Impfbescheinigungen** der Kinder durch die Personensorgeberechtigten zwingend vorsieht. Die bisherige Praxis der **freiwilligen** Impfbuchvorlage habe gezeigt, dass in einem Teil der Fälle weder Impfbücher noch Impfbescheinigungen vorgelegt worden seien und somit eine fachliche Beratung zu fehlenden Impfungen nicht erfolgen konnte. Um dem öffentlichen Gesundheitsdienst zu ermöglichen, bei möglichst allen Schülerinnen und Schülern Impfberatungen durchzuführen und dadurch die Durchimpfungsrate zu erhöhen, sei es zwingend erforderlich, so argumentierte das Staatsministerium, eine Vorlagepflicht einzuführen.

Die Einführung einer Pflicht zur Vorlage des Impfausweises oder einer Impfbescheinigung stellt einen Grundrechtseingriff dar, der die Selbstbestimmung über sensible Gesundheitsdaten berührt. Zwar konnte ich die in der Gesetzesbegründung aufgeführten medizinfachlichen Erwägungen für eine Impfberatung bei möglichst allen Schülerinnen und Schülern und für eine Erhöhung der Durchimpfungsrate nachvollziehen.

Allerdings teilte ich nicht die Schlussfolgerung, dass es dazu zwingend erforderlich sei, eine Vorlagepflicht für vorhandene Impfausweise oder Impfbescheinigungen einzuführen. Bei – aus guten Gründen – fehlender Impfpflicht und bei fehlender Pflicht zum Besitz eines Impfausweises oder einer Impfbescheinigung wäre es auch künftig nicht gewährleistet, dass durch die Einführung einer Vorlagepflicht vorhandener Impfausweise oder Impfbescheinigungen eine Erhöhung der Durchimpfungsrate erzielt würde. Es würde auch künftig Personensorgeberechtigte geben, die von ihrem Recht Gebrauch machen würden, bei ihren Kindern bzw. Schutzbefohlenen keine Impfungen durchführen zu lassen oder (ggf. sogar nach durchgeführter Impfung) keine Impfausweise oder Impfbescheinigungen zu besitzen.

Anstelle der Einführung einer gesetzlichen Vorlagepflicht erschien mir eine intensive Aufklärung und Beratung durch die Gesundheitsbehörden, insbesondere in den Schulen, angezeigt und geeignet, Personensorgeberechtigte von der Durchführung einer Impfung und von der Notwendigkeit zur Überprüfung des Impfstatus durch die freiwillige Vorlage von Impfausweisen bzw. Impfbescheinigungen zu überzeugen.

Möglicherweise hätte die Einführung einer Vorlagepflicht sogar den unerwünschten Effekt, dass Personensorgeberechtigte, die bislang freiwillig Impfungen durchführen ließen und freiwillig Impfausweise bzw. Impfbescheinigungen in ihrem Besitz hatten und diese freiwillig den Gesundheitsbehörden für Impfkontrollen zur Verfügung stellten, sich künftig der „Zwangsmaßnahme“ zu entziehen versuchen, indem sie keine Impfungen mehr durchführen lassen oder zumindest keine (förmlichen) Impfausweise bzw. Impfbescheinigungen mehr besitzen wollen. Beschwerden von Personensorgeberechtigten, die immer wieder an mich herangetragen worden sind, wenn von Schülerinnen oder Schülern bzw. deren Sorgeberechtigten die Vorlage von Impfausweisen bzw. Impfbescheinigungen verlangt und dabei nicht ausdrücklich auf die Freiwilligkeit hingewiesen worden ist, zeigen deutlich, dass zahlreiche Bürgerinnen und Bürger äußerst sensibel darauf reagieren, wenn in das ihnen verfassungsrechtlich gewährte informationelle Selbstbestimmungsrecht eingegriffen wird. Dies gilt insbesondere für den Gesundheitsbereich.

Aus diesen Gründen habe ich dem Staatsministerium empfohlen, auf die **Einführung einer gesetzlichen Verpflichtung** zur Vorlage vorhandener Impfausweise und Impfbescheinigungen bei Schuleingangsuntersuchungen und weiteren schulischen Impfberatungen zu **verzichten.**

7.9 Videoüberwachung in Schwangerenberatungsstelle

Das Bayerische Staatsministerium für Arbeit und Sozialordnung, Familie und Frauen erbat meine datenschutzrechtliche Bewertung hinsichtlich einer geplanten Videoüberwachung im Zugangsbereich zu den Räumen einer staatlich aner-

kannten Beratungsstelle für Schwangerschaftsfragen der Gesundheitsverwaltung eines Landratsamtes.

Zum Sachverhalt hatte es mir mitgeteilt, dass die Beratungsstelle in einem Personalwohngebäude untergebracht sei. Aufgrund verschiedener Vorkommnisse (u.a. Diebstähle und Sachbeschädigungen) beabsichtige die zuständige Verwaltung die Installation von Videokameras im Eingangsbereich. Aufzeichnungen seien unter der Woche in den Abend- und Nachtstunden sowie am Wochenende und an Feiertagen ganztägig geplant. Ein Hinweisschild solle angebracht werden. Auswertungen seien nur anlassbezogen (Verdacht einer Straftat oder Ordnungswidrigkeit) vorgesehen. Ansonsten würden die Aufzeichnungen nach einer Woche gelöscht werden. Die regelmäßigen Öffnungszeiten der Beratungsstelle lägen zwar außerhalb des Zeitrahmens für die Aufzeichnungen, jedoch fänden Beratungstermine auch zu anderen Zeiten statt.

Die rechtliche Beurteilung richtete sich nach Art. 21 a des Bayerischen Datenschutzgesetzes (BayDSG). Danach ist die Videobeobachtung und Videoaufzeichnung 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. 21 a Abs. 1 Satz 2 BayDSG dürfen allerdings keine Anhaltspunkte dafür bestehen, dass überwiegende schutzwürdige Interessen der Betroffenen beeinträchtigt werden.

Die Überwachungsmaßnahme konnte grundsätzlich auf das Hausrecht zur Vermeidung weiterer Beeinträchtigungen öffentlichen Eigentums gestützt werden. Daneben kam die öffentliche Aufgabe der Aufrechterhaltung der Funktionsfähigkeit der öffentlichen Stelle im Hinblick auf ungestörten Besucherverkehr und ungestörte Nutzungsmöglichkeit in Betracht. Von Relevanz war insoweit, ob auch zukünftig und gehäuft mit vergleichbaren Vorkommnissen gerechnet werden muss.

Die Prüfung ergab zudem, dass sich die optisch-elektronische Überwachung des Eingangsbereiches des besagten Gebäudes in den Abend- und Nachtstunden bzw. ganztägig an Wochenenden und Feiertagen generell zum Schutz der betroffenen Rechtsgüter eignete, da das Vorhandensein von Kameras einerseits abschreckende Wirkung entfaltet und die vorübergehende Speicherung andererseits eine Möglichkeit der Aufklärung von Straftaten oder Ordnungswidrigkeiten bietet.

Ob die Videoüberwachung und -aufzeichnung in der vorgesehenen Form auch erforderlich ist, war einerseits danach zu beurteilen, ob die Erhebung und Speicherung der mit Hilfe der Videoüberwachung gewonnenen Daten notwendig ist, um den angestrebten Zweck zu erreichen. Andererseits muss aber auch feststellbar sein, dass die Erhebung und Verarbeitung personenbezogener Daten und die hiermit verbundenen Nachteile für die Betroffenen im Verhältnis zum angestrebten Zweck angemessen sind (Wilde/Ehmann/Niese/Knoblauch, Kommentar zum BayDSG, Art. 21 a, Rdnr. 26). Betroffen sind neben den Besuchern der Beratungsstelle auch sämtliche sonstige Nutzer des Gebäudes, insbesondere die Bewohner. Es war daher eine Güterabwägung unter Würdigung aller rechtlich relevanten, insbesondere auch verfassungsrechtlich geschützten Positionen vorzunehmen, wobei auf der Seite der von der Überwachung betroffenen Perso-

nen dem Grundrecht auf informationelle Selbstbestimmung gemäß Art. 2 Abs. 1 i. V. m. Art. 1 Abs. 1 GG besondere Bedeutung zukam.

Im Hinblick auf die Besucher der Beratungsstelle für Schwangerschaftsfragen war Art. 2 Abs. 3 des Gesetzes über die Schwangerenberatung (BaySchwBerG) zu beachten, wonach entsprechend den Vorgaben des BVerfG (Urteil vom 28.05.1993, 2 BvF 2/90, 2 BvF 4/92, 2 BvF 5/92) über die Beratung Verschwiegenheit zu wahren ist und diese auf Wunsch sogar anonym zu erfolgen hat.

Art. 2 BaySchwBerG Beratung
(3) [1] Über die Beratung ist Verschwiegenheit zu wahren. [2] Auf Wunsch kann die Beratung anonym erfolgen.

Das gesetzlich vorgesehene Beratungskonzept mit dem wesentlichen Aspekt der Geheimhaltung und der Möglichkeit der Schwangeren, anonym zu bleiben, ist Ausformung der staatlichen Pflicht zum Schutz des ungeborenen Lebens und muss Rahmenbedingungen bieten, die geeignet sind, positive Voraussetzungen für ein Handeln der Frau zugunsten des Ungeborenen zu schaffen (s. BVerfG, aaO.). Die Gewährleistung der Geheimhaltung dient dem Entstehen eines Vertrauensverhältnisses. Über die Schweige- und Geheimhaltungspflicht aller in der Beratungsstelle tätigen Personen soll daher möglichst frühzeitig informiert werden (bereits bei telefonischer Vereinbarung eines Gesprächstermins, durch gut sichtbare Schilder im Eingangsbereich der Beratungsstelle, zu Gesprächsbeginn). Um dem gesetzlich garantierten Recht auf Anonymität ausreichend Rechnung tragen zu können, sind zudem an die räumliche Unterbringung der Beratungsstelle erhöhte Anforderungen zu stellen. Das Aufsuchen der Einrichtung sollte so unauffällig und unbeobachtet wie möglich erfolgen können (zum gesamten Themenkomplex siehe hierzu 16. Tätigkeitsbericht, Nr. 2.4.2, 17. Tätigkeitsbericht, Nr. 3.5.1 und 19. Tätigkeitsbericht, Nr. 3.8).

Ich habe dem anfragenden Staatsministerium mitgeteilt, dass die Videoüberwachung auch dann, wenn sie außerhalb der regulären Beratungszeiten stattfindet und entsprechende Hinweise hierauf vorgesehen sind, dem äußerst sensiblen Interesse der Beratungswilligen an Vertraulichkeit und Geheimhaltung zuwiderläuft. Allein die Tatsache, dass Kameras installiert sind und der Passant oder die Passantin nicht ausschließen kann, dass sich diese in Betrieb befinden und aufzeichnen, genügt schon, um bei den potentiell Betroffenen das Gefühl des Beobachtet- oder Überwachtseins zu erzeugen. Hieraus kann eine gewisse Misstrauenshaltung resultieren bzw. könnten Beratungsbedürftige von der Inanspruchnahme der Beratungsleistung abgehalten werden. Hinzu kommt, dass Gesprächstermine auch außerhalb der üblichen Öffnungszeiten vergeben werden und somit die Gefahr besteht, dass der Besuch der Beratungsstelle zumindest vorübergehend optisch-elektronisch dokumentiert wird.

Bedenken habe ich im Übrigen auch im Hinblick auf die Bewohner des Personalwohnheims geäußert, da diese beim Betreten und Verlassen ihrer Wohnung bzw. des Wohngebäudes insbesondere in den zumeist dem Privatleben zuzuordnenden Abend- und Nachtstunden bzw. an Feiertagen und Wochenenden ganztägig permanenter Videoüberwachung ausgesetzt wären, ohne sich diesem Überwachungsdruck effektiv entziehen zu können.

Ich habe gebeten, darauf hinzuwirken, dass die Videoüberwachung im Eingansbereich des Personalwohngebäudes unterbleibt. Das betreffende Landratsamt hat in der Folge dauerhaft von seinen Plänen Abstand genommen.

7.10 Bekanntgabe eines amtsärztlichen Gutachtens

Aufgrund einer Eingabe erfuhr ich von einem datenschutzrechtlichen Verstoß, der mich zu einer förmlichen **Beanstandung** eines Gesundheitsamtes veranlasste. Die Eingabeführerin hatte mir geschildert, dass sie das für sie zuständige Gesundheitsamt zur Begutachtung über die Notwendigkeit einer Rehabilitationsmaßnahme aufgesucht hatte. Im Rahmen eines sich anschließenden Wiedereingliederungsgespräches der Petentin mit der dienstvorgesetzten Schulrätin wurde ihr offenbar, dass das die Petentin betreffende amtsärztliche Gutachten über die Notwendigkeit einer Behandlung in einer medizinischen Rehabilitationseinrichtung per Telefax an die Schulrätin gesandt worden war. Auf meine Aufforderung, zu der Eingabe Stellung zu nehmen, bestätigte mir das Gesundheitsamt den Vorfall. Es teilte hierzu mit, dass man den Weg der Versendung per Telefax aufgrund der Eilbedürftigkeit der zeitnah anstehenden Rehabilitationsmaßnahme gewählt habe. Die Übermittlung an die personalverwaltende Stelle sei nicht beabsichtigt gewesen und beruhe auf einer Verwechslung von Telefaxnummern.

Aus datenschutzrechtlicher Sicht ist die Weitergabe des amtsärztlichen Gutachtens an die Schulrätin durch das Gesundheitsamt als Verarbeitung personenbezogener Daten in Form der Datenübermittlung zu werten (Art. 4 Abs. 6 Satz 2 Nr. 3 a BayDSG).

Art. 30 Abs. 1 Satz 3 i.V.m. Satz 1 Gesundheitsdienst- und Verbraucherschutzgesetz (GDVG) enthält eine Vertraulichkeitspflicht für Angehörige des Gesundheitsamtes im Zusammenhang mit einer Untersuchung oder Begutachtung, der sich ein Betroffener freiwillig unterzogen hat.

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 … . [3]Die Behörden für Gesundheit, Veterinärwesen, Ernährung und Verbraucherschutz dürfen Geheimnisse nach den Sätzen 1 und 2 nicht übermitteln oder an andere Teile der öffentlichen Stelle, deren Bestandteil die Behörde für Gesundheit, Veterinärwesen, Ernährung und Verbraucherschutz ist, weitergeben.

Bei einer amtsärztlichen Untersuchung zur Feststellung der Beihilfefähigkeit von Aufwendungen bei stationären Maßnahmen in Einrichtungen nach § 29 Abs. 4 Bayerische Beihilfeverordnung (BayBhV) handelt es sich um eine freiwillige Untersuchung; sie kann von Seiten der Beihilfestelle nicht erzwungen werden (s. hierzu die Gesetzesbegründungen zu Art. 30 GDVG, LT-Drs. 14/11831, S. 38 sowie zu Art. 6 des Gesundheitsdienstgesetzes, LT-Drs. 10/8972, S. 14).

Auf eine Ausnahme vom Übermittlungsverbot konnte sich das Gesundheitsamt lediglich hinsichtlich der Übermittlung an die Beihilfestelle berufen, da das amtsärztliche Gutachten zur Vorlage bei der Beihilfestelle und zwecks Anerkennung

der Beihilfefähigkeit einer stationären Rehabilitationsmaßnahme gefertigt wurde (Art. 11 Abs. 1 GDVG i. V. m. § 29 Abs. 1 Nr. 3, Abs. 4 und 5 BayBhV). Insoweit konnte vom Einverständnis der Petentin ausgegangen werden (s. Art. 30 Abs. 2 Satz 1 Nr. 2 GDVG). Die Übermittlung des Gutachtens an die Schulrätin war dem gegenüber weder durch eine ausdrückliche, stillschweigende oder mutmaßliche Einwilligung gedeckt, noch durch Rechtsvorschrift zugelassen (Art. 30 Abs. 2 Satz 1 GDVG). In diesem Zusammenhang ist vielmehr das Gebot der organisatorischen Trennung der Beihilfebearbeitung von der übrigen Personalverwaltung von Bedeutung (Art. 105 des Bayerischen Beamtengesetzes – BayBG), dem mit der Regelung der Zuständigkeit des Landesamtes für Finanzen im staatlichen Bereich in Art. 96 Abs. 4 Satz 3 BayBG Genüge getan wurde.

Der Petentin ist darüber hinaus auch darin beizupflichten, dass an die Versendung eines amtsärztlichen Gutachtens besondere Anforderungen zu stellen sind. In Anbetracht der Sensibilität der übermittelten Daten muss der Versand an die Beihilfestelle grundsätzlich in einem als vertraulich bzw. als Arztsache gekennzeichneten und verschlossenen Umschlag erfolgen. Im Fall der Eilbedürftigkeit sollte die Nutzung der Telefaxtechnik ultima Ratio sein, sofern die Einwilligung des Untersuchten bejaht und gleichzeitig sichergestellt werden kann, dass es sich bei dem Telefaxempfänger um den zum Empfang befugten Adressaten (Sachbearbeiter der Beihilfestelle) handelt.

Im vorliegenden Fall war die Beanstandung nach Art. 31 Abs. 3 BayDSG schon deshalb geboten, weil die Datenübermittlung einen erheblichen Verstoß darstellte. Als besonders sensibel einzustufende Daten über die Gesundheit wurden unbefugt an eine personalverwaltende Stelle herausgegeben. Ich hatte in Anbetracht der beruflichen Stellung der Adressatin durchaus auch Zweifel, ob die Übermittlung tatsächlich nur aufgrund einer Verwechslung von Telefaxnummern versehentlich erfolgt ist. Jedenfalls ist damit deutlich geworden, dass dem Schutz personenbezogener Gesundheitsdaten im Gesundheitsamt nicht ausreichend Rechnung getragen wurde. Hinzu kam, dass ich wegen eines ähnlichen Vorfalles beim selben Gesundheitsamt bereits im Jahr 2007 einen Verstoß gegen Art. 30 Abs. 1 GDVG festgestellt hatte. Damals hatte ich von einer förmlichen Beanstandung abgesehen, nachdem die versehentliche datenschutzrechtliche Verfehlung eingeräumt worden war, die Datenübermittlung keine konkreten medizinischen Diagnosen oder Untersuchungsbefunde betroffen hatte und ich damals noch davon ausgehen konnte, dass es sich um einen bedauerlichen Einzelfall handelte.

Ich beanstandete daher nach Art. 31 Abs. 1 Satz 1 Bayerisches Datenschutzgesetz die Übermittlung des amtsärztlichen Gutachtens an die Schulrätin der Petentin. Zugleich forderte und überwachte ich organisatorische Vorkehrungen des Gesundheitsamtes, die einerseits die Übermittlung personenbezogener Daten an Unbefugte bzw. ähnlich geartete Verwechslungen von Adressaten zukünftig verhindern und andererseits den datenschutzgerechten Versand amtsärztlicher Unterlagen gewährleisten sollen.

7.11 Approbationsvoraussetzungen bei Auslandsaufenthalt

Ein Bürger teilte mir mit, dass die für ihn zuständige Behörde für seinen Antrag auf Erteilung der Approbation als Psychologischer Psychotherapeut zusätzlich zu dem deutschen Führungszeugnis den Nachweis der Straffreiheit während eines Auslandsaufenthaltes durch die Vorlage eines Strafregisterauszuges aus dem entsprechenden Land verlangt habe. Er wies auf ein Merkblatt der Behörde hin,

welches allgemein und auch den Beruf Psychologische Psychotherapeutin/Psychologischer Psychotherapeut betreffend, die einzureichenden Unterlagen erörterte. Bei Auslandsaufenthalten, die wie bei Aufenthalten zu Studien- und Berufsausübungszwecken nicht nur vorübergehend angelegt waren, sei danach neben dem Führungszeugnis der Belegart „O“ auch ein Strafregisterauszug aus dem entsprechenden Land/den entsprechenden Ländern nötig.

Die Behörde berief sich mir gegenüber darauf, dass die Vorlage des deutschen Führungszeugnisses nicht genüge, wenn der Antragsteller aus dem Ausland komme oder sich dort nennenswert lang aufgehalten habe und mit dem Staat kein Abkommen über den Strafnachrichtenaustausch im Sinne der §§ 54 ff. des Gesetzes über das Zentralregister und Erziehungsregister bestehe. Ein ausländischer Strafregisterauszug werde angefordert, wenn der Auslandsaufenthalt so kurz zurückliege, dass eine etwaige Verfehlung noch zu berücksichtigen wäre und die Beschaffung des Dokuments nicht mit einem unverhältnismäßigen Aufwand für die Antragsteller verbunden sei.

Ich habe die Behörde darauf hingewiesen, dass die Erhebung, Verarbeitung oder Nutzung personenbezogener Daten durch eine öffentliche Stelle nur zulässig ist, wenn sie durch eine Rechtsvorschrift erlaubt oder angeordnet ist oder der Betroffene einwilligt. § 19 PsychTh-APrV i.V.m. § 8 Abs. 1 Satz 2 des Gesetzes über die Berufe des Psychologischen Psychotherapeuten und des Kinder- und Jugendlichenpsychotherapeuten (PsychThG) regelt die für die Erteilung der Approbation notwendigen Nachweise und ist damit als bereichsspezifische Rechtsvorschrift für die Erhebung personenbezogener Daten anzusehen. In § 19 Abs. 1 Satz 2 PsychTh-APrV sind die Unterlagen aufgezählt, die dem Antrag auf Approbation beizufügen sind. Unter Nr. 4 ist bestimmt, das hierzu ein „amtliches Führungszeugnis“ gehört, „das nicht früher als einen Monat vor der Vorlage ausgestellt sein darf“. Die zuständigen Behörden verlangen bundeseinheitlich ein behördliches Führungszeugnis nach § 30 Abs. 5 des Bundeszentralregistergesetzes (Belegart „O“). Für die zusätzliche Anforderung eines ausländischen Strafregisterauszugs fehlt es an einer Rechtsgrundlage. Entgegen der Argumentation der zuständigen Behörde und des Bayerischen Staatsministeriums für Umwelt und Gesundheit, welches am Verfahren beteiligt war, rechtfertigt auch § 19 Abs. 3 PsychTh-APrV nicht die zusätzliche Erhebung, da sich die Vorschrift speziell auf Staatsangehörige eines anderen Mitgliedsstaates der Europäischen Union (EU) oder eines anderen Vertragsstaates des Abkommens über den Europäischen Wirtschaftsraum (EWR) bezieht und nur diesen die Vorlage alternativer Bescheinigungen bzw. der Approbationsbehörde nur für die insoweit genannten Personen Auskunftsbefugnisse und die Möglichkeit von Ermittlungsersuchen gegenüber Behörden eröffnet.

Eine vergleichbare Problematik ergab sich im Hinblick auf die Approbationen von Ärzten, Zahnärzten, Kinder- und Jugendpsychologen sowie Tierärzten, nachdem sich das oben genannte Merkblatt auch auf diese Berufsgruppen bezog, die jeweiligen Approbationsordnungen aber ebenso wie die der Psychologischen Psychotherapeuten keine ausdrücklichen Regelungen zur Vorlage ausländischer Strafregisterauszüge enthielten.

Ich habe die zuständige Behörde aufgefordert, ihre Verwaltungspraxis an die gültige Rechtslage anzupassen und die Formulare zur Beantragung der Approbation so abzuändern, dass sich keine über den Wortlaut der heilberuflichen Approbationsordnungen hinausgehenden Nachweisanforderungen ergeben.

§ 19 Ausbildungs- und Prüfungsverordnung für Psychologische Psychotherapeuten Antrag auf Approbation

(1) Die Approbation wird von der zuständigen Behörde auf Antrag erteilt. Dem Antrag sind beizufügen:

1. *ein tabellarischer Lebenslauf,*
2. *die Geburtsurkunde und alle Urkunden, die eine spätere Namensänderung ausweisen,*
3. *ein Identitätsnachweis,*
4. *ein amtliches Führungszeugnis, das nicht früher als einen Monat vor der Vorlage ausgestellt sein darf,*
5. *eine Erklärung darüber, ob gegen den Antragsteller ein gerichtliches Strafverfahren oder ein staatsanwaltliches Ermittlungsverfahren anhängig ist,*
6. *eine ärztliche Bescheinigung, die nicht älter als einen Monat sein darf, aus der hervorgeht, dass der Antragsteller nicht in gesundheitlicher Hinsicht zur Ausübung des Berufs ungeeignet ist und*
7. *das Zeugnis über die staatliche Prüfung für Psychologische Psychotherapeuten nach § 12 Abs. 2 Satz 1.*

In den Fällen, in denen die Approbation auf Grund eines Ausbildungsnachweises nach § 2 Abs. 2, 3 oder Abs. 3 a des Psychotherapeutengesetzes erteilt werden soll, können von den Antragstellern die in Satz 2 Nr. 1 und 2 genannten Nachweise nicht gefordert werden, es sei denn, ihre in einem Drittland ausgestellten Ausbildungsnachweise sind noch in keinem anderen Mitgliedstaat anerkannt worden . . . .

(3) Staatsangehörige eines anderen Mitgliedstaates der Europäischen Union oder eines anderen Vertragsstaates des Abkommens über den Europäischen Wirtschaftsraum können anstelle des in Absatz 1 Nr. 4 genannten Zeugnisses eine von der zuständigen Behörde des Herkunftsmitgliedstaats ausgestellte entsprechende Bescheinigung oder einen von einer solchen Behörde ausgestellten Strafregisterauszug oder, wenn ein solcher nicht beigebracht werden kann, einen gleichwertigen Nachweis vorlegen. Hat der Antragsteller einen dem Beruf des Psychologischen Psychotherapeuten entsprechenden Beruf im Herkunftsmitgliedstaat bereits ausgeübt, so kann die für die Erteilung der Approbation als Psychologischer Psychotherapeut zuständige Behörde bei der zuständigen Behörde des Herkunftsmitgliedstaats Auskünfte über etwa gegen den Antragsteller verhängte Strafen oder sonstige berufs- oder strafrechtliche Maßnahmen wegen schwerwiegenden standeswidrigen Verhaltens oder strafbarer Handlungen, die die Ausübung des Berufs im Herkunftsmitgliedstaat betreffen, einholen. Hat die für die Erteilung der Approbation zuständige Behörde in den Fällen des Satzes 1 oder 2 von Tatbeständen Kenntnis, die außerhalb des Geltungsbereichs des Psychotherapeutengesetzes eingetreten sind und im Hinblick auf die Voraussetzungen des § 2 Abs. 1 Nr. 3 des Psychotherapeutengesetzes von Bedeutung sein können, hat sie die zuständige Stelle des Herkunftsmitgliedstaats zu unterrichten und sie zu bitten, diese Tatbestände zu überprüfen und ihr das Ergebnis und die Folgerungen, die sie hinsichtlich der von ihr ausgestellten Bescheinigungen und Nachweise daraus zieht, mitzuteilen. Die in Satz 1 bis 3 genannten Bescheinigungen und Mitteilungen sind vertraulich zu behandeln. Sie dürfen der Beurteilung nur zugrunde gelegt werden, wenn bei der Vorlage die Ausstellung nicht mehr als drei Monate zurückliegt.

7.12 Forschungsprojekt Evaluation forensisch-psychiatrischer Ambulanzen

Im Berichtszeitraum hatte ich mich mit einem Forschungsprojekt zur Evaluation forensisch-psychiatrischer Ambulanzen in Bayern zu befassen.

Dem mir übermittelten Studienkonzept war zu entnehmen, dass die Evaluation vor allem die Beantwortung zweier Fragestellungen bezweckte. Zunächst sollte sie klären, ob die ambulante Nachbetreuung forensischer Patienten Effekte im Hinblick auf die kriminelle Rückfälligkeit bzw. die Stabilität forensischer Patienten zeigt. Weiteres Forschungsziel war die Beantwortung der Frage, ob die forensische Nachsorge zu einer Verkürzung von Aufenthaltszeiten im Maßregelvollzug bzw. zur Einsparung finanzieller Mittel beitragen kann. Um hierzu Aussagen treffen zu können, sollten im Rahmen einer Vollerhebung zu festen Terminen in den einzelnen Fachambulanzen mittels strukturierter Fragebögen und schriftlicher Verlaufsstellungnahmen Daten der in Bayern forensisch-ambulant betreuten Patienten erhoben, sodann verarbeitet und wissenschaftlich ausgewertet werden. Zusätzlich war die Erhebung und weitere Verwendung von Bundeszentralregisterdaten der an der Studie teilnehmenden Patienten vorgesehen.

Um fundierte Hinweise geben zu können, habe ich mir zunächst ein umfassendes Datenschutzkonzept vorlegen lassen und in der Folge daran mitgewirkt, dass dieses ausreichend konkrete Aussagen zu den Abläufen der beabsichtigten Datenerhebungen, -verarbeitungen und -nutzungen und den jeweiligen Rechtsgrundlagen hierfür sowie zu den erforderlichen technisch-organisatorischen Datenschutzmaßnahmen traf.

Wie sich aufgrund meiner Prüfungen herausstellte, war der vorgesehene Umgang mit personenbezogenen Daten der im Rahmen des Forschungsprojekts zu betrachtenden Patienten nur auf der Grundlage freiwilliger, widerruflicher und informierter Einwilligungen zulässig. Die Gestaltung der entsprechenden Formulare (Einwilligungserklärungen, Patienteninformationen) begleitete ich mit Hinweisen zum Inhalt, zur Gestaltung und zur Verwendung. Insbesondere merkte ich an, dass eine wirksame Einwilligung die Einsichtsfähigkeit des betreffenden Patienten voraussetzt. Gerade diese Voraussetzung ist bei Patienten, die unter Betreuung stehen, in besonderer Weise zu hinterfragen.

Das ursprünglich vorgesehene Pseudonymisierungsverfahren entsprach nicht den sonst in der medizinischen Forschung geforderten Standards. Generell gilt für personenbezogene Daten, die für Forschungsvorhaben wissenschaftlicher Art erhoben werden, dass sie zu anonymisieren sind, sobald dies nach dem Forschungszweck möglich ist. Bis dahin sind die Merkmale, mit denen Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren Person zugeordnet werden können, gesondert zu speichern. Sie dürfen mit den Einzelangaben nur zusammengeführt werden, soweit der Forschungszweck dies erfordert (hier wegen fortgesetzter Datenerfassung und Abfrage beim Bundeszentralregister, s. Art. 23 Abs. 3 BayDSG sowie § 42 a Abs. 4 - 6 , insbesondere Abs. 5 BZRG). Ich habe darauf hingewirkt, dass ein mehrstufiges Pseudonymisierungsverfahren mit Aufgabenteilung im Sinne einer Trennung der Funktionen „Pseudonymisierung“ und „Forschungsdatenbank“ vorgesehen wurde und die Einführung einer die Daten zusammenführenden Stelle als Vertrauensstelle empfohlen. Das Datenschutzkonzept wurde entsprechend abgeändert, sodass nun eine dort näher bezeichnete Stelle mit Hilfe der von den Ambulanzen zu liefernden identifizierenden Daten der teilnehmenden Patienten eine Patientenliste zu erstellen und für jeden Patienten ein Pseudonym zu generieren hat, das sie an die Ambulanzen zurückmeldet. Die Ambulanzen übermitteln die Fragebögen und Verlaufsberichte unter dem jeweiligen Pseudonym an die Forscher. Auch die Anfragen an das Bundeszentralregister werden von der treuhänderisch tätigen Person unter Angabe der identifizieren-

den Daten und des Pseudonyms durchgeführt, während die Registerauskünfte wiederum in pseudonymisierter Form an die Forscher erfolgen.

Die Zusammenarbeit bestätigte wieder einmal, dass sich Forschungsinteressen und Datenschutz in der Regel gut vereinbaren lassen.

8 Sozialwesen

8.1 ELENA-Verfahren gestoppt

„Das Projekt ELENA ist endgültig eingestellt worden, der Datenbankhauptschlüssel sowie alle weiteren Schlüssel sind Ende letzten Jahres gelöscht worden, auch die – nicht mehr zugänglichen – Daten wurden physikalisch gelöscht." Mit dieser Feststellung hat der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit Mitte des Jahres 2012 die Datenschutzbeauftragten der Länder darüber informiert, dass unter das seit Jahren äußerst umstrittene Gesetz über das Verfahren des elektronischen Entgeltnachweises (ELENA-Verfahrensgesetz) endlich ein Schlussstrich gezogen werden kann.

Seit 2010 bestand für alle Arbeitgeber die Verpflichtung, monatlich die Einkommensdaten ihrer Beschäftigten an eine Zentrale Datenbank zu übermitteln. Dort sollten die Daten ab 2012 zum Abruf durch Sozialbehörden bereit stehen, um Antragstellern einen elektronischen Einkommensnachweis zu ermöglichen.

Die Bundesregierung begründete die Einstellung des ELENA-Verfahrens mit der fehlenden Verbreitung der qualifizierten elektronischen Signatur. Umfassende Untersuchungen hätten gezeigt, dass sich dieser Sicherheitsstandard, der für das ELENA-Verfahren datenschutzrechtlich zwingend geboten war, trotz aller Bemühungen seitens der Wirtschaft und der Politik auch in absehbarer Zeit nicht flächendeckend verbreiten würde. Hiervon sei aber der Erfolg des ELENA-Verfahrens abhängig gewesen.

Die Datenschutzbeauftragten des Bundes und der Länder hatten zuvor wiederholt Kritik am ELENA-Verfahren geübt. In Stellungnahmen zu mehreren Verfassungsbeschwerden beim Bundesverfassungsgericht wurden unter meiner Federführung alle wesentlichen verfassungsrechtlichen und -politischen Einwände aus Datenschutzsicht gebündelt vorgetragen. Ein Kritikpunkt war dabei stets der Umstand, dass Einkommensdaten von allen Beschäftigten gespeichert werden, obwohl sie nur für die relativ wenigen Betroffenen benötigt werden, die bestimmte Sozialleistungen beantragt haben.

Mit der Einstellung des Verfahrens ist nun erfreulicher Weise der Gesetzgeber einer Forderung der Datenschutzbeauftragten des Bundes und der Länder nachgekommen, insbesondere im Zusammenhang mit umfangreichen zentralen Datensammlungen größere Zurückhaltung zu wahren. Das ELENA-Verfahren war ein klassisches Beispiel für die rechtsstaatlich bedenkliche Vorratsspeicherung von sensiblen Daten vieler Millionen Bundesbürgerinnen und Bundesbürger.

Ich hoffe, dass die Bundesregierung ihre Ankündigung, ein Konzept zu erarbeiten, wie die bereits bestehende Infrastruktur des ELENA-Verfahrens und das erworbene Know-how für ein einfacheres und unbürokratisches Meldeverfahren in der Sozialversicherung genutzt werden können, mit Augenmaß verfolgen wird, und damit nicht womöglich noch weniger datenschutzrechtliche Anforderungen erfüllt werden als beim ELENA-Verfahren. Ich mache mir deshalb zur Aufgabe, die Entwicklung künftiger ELENA-Nachfolgeprojekte – bekannt sind derzeit ein Projekt des Bundesministeriums für Arbeit und Soziales „Optimiertes Meldever-

fahren in der sozialen Sicherung (OMS)“ und das Projekt „BEA – Bescheinigungen elektronisch annehmen“ der Bundesagentur für Arbeit – auch weiterhin kritisch zu begleiten und insbesondere den Bundesbeauftragten für den Datenschutz und die Informationsfreiheit zu unterstützen.

8.2 Hausbesuch bei Neugeborenen

In meinem letzten Tätigkeitsbericht habe ich mich ausführlich mit Hausbesuchen bei Eltern Neugeborener auseinandergesetzt (siehe hierzu 24. Tätigkeitsbericht, Nr. 8.1). Dadurch sollen Eltern zielgerichtet Informationen bzw. Hilfsangebote insbesondere der Kinder- und Jugendhilfe erhalten. Ich habe die Auffassung vertreten, derartige Hausbesuche seien nur zulässig, wenn die Eltern nach ausreichender Information vor einem solchen Hausbesuch ausdrücklich **freiwillig** und schriftlich gegenüber dem Jugendamt einwilligen. Ein bloßes Schweigen der Eltern gegenüber dem Jugendamt reicht dafür nicht. Es genügt auch nicht, die Einwilligung an der Haustüre der Eltern einzuholen, weil hier nicht mehr in jedem Fall die Freiwilligkeit der Einwilligung unterstellt werden kann. Die Eltern müssen sich freiwillig für oder gegen einen Hausbesuch entscheiden können. Insbesondere darf eine Verweigerung eines Hausbesuchs nicht vermerkt werden oder andere Sanktionen zur Folge haben.

Aufgrund dieser Ansicht bin ich in der Vergangenheit vielfach mit dem Vorwurf konfrontiert worden, dass mit meiner geforderten „Zustimmungslösung“ aufgrund des geringen Rücklaufs seitens der Eltern Hausbesuche faktisch unmöglich würden. Ich weise allerdings darauf hin, dass die Zustimmung nicht zwangsläufig per Post erklärt werden muss. Vielmehr ist die Einholung einer Einwilligung auch auf anderem Wege (z.B. in der Geburtsklinik, durch eine Hebamme bzw. den Kinderarzt etc.) denkbar.

Am 01.01.2012 ist das Bundeskinderschutzgesetz in Kraft getreten. Meiner Einschätzung nach bestätigt die darin enthaltene Regelung des Gesetzes zur Kooperation und Information im Kinderschutz (KKG) jedenfalls im Grundsatz meine Auffassung.

§ 2 KKG Information der Eltern über Unterstützungsangebote in Fragen der Kindesentwicklung
(1) Eltern sowie werdende Mütter und Väter sollen über Leistungsangebote im örtlichen Einzugsbereich zur Beratung und Hilfe in Fragen der Schwangerschaft, Geburt und der Entwicklung des Kindes in den ersten Lebensjahren informiert werden.
(2) Zu diesem Zweck sind die nach Landesrecht für die Information der Eltern nach Absatz 1 zuständigen Stellen befugt, den Eltern ein persönliches Gespräch anzubieten. Dieses kann auf Wunsch der Eltern in ihrer Wohnung stattfinden. Sofern Landesrecht keine andere Regelung trifft, bezieht sich die in Satz 1 geregelte Befugnis auf die örtlichen Träger der Jugendhilfe.

§ 2 Abs. 2 S. 1 KKG enthält eine Befugnis der zuständigen Stellen, den Eltern ein persönliches Gespräch anzubieten. Dieses könne „auf Wunsch der Eltern“ in ihrer Wohnung stattfinden (§ 2 Abs. 2 S. 1 KKG). Meiner Einschätzung nach scheiden die bisher in der Praxis zum Teil praktizierten „Widerspruchslösungen“ zukünftig schon aufgrund des ausdrücklichen Wortlauts des KKG aus. Ich weise nochmals darauf hin, dass ein Schweigen grundsätzlich ein „rechtliches Nullum“ darstellt.

Diese Ansicht wird auch ganz überwiegend von den Datenschutzbeauftragten der anderen Bundesländer geteilt.

Inzwischen hat sich auch das Bayerische Staatsministerium für Arbeit und Sozialordnung, Familie und Frauen diese Rechtsansicht angeschlossen. Sie wurde bereits in einer neuen Publikation für die Jugendämter übernommen.

Ich begrüße es, dass nun die Gesetzeslage klargestellt ist. Schließlich werden wohl aufgrund einer weiteren gesetzlichen Änderung Hausbesuche bei Eltern mit neugeborenen Kindern zunehmen. Zum 01.05.2012 wurde mit dem neuen § 13 a Meldedatenverordnung (MeldDV) eine Regelung geschaffen, nach der die Meldebehörden monatlich den Jugendämtern die Daten der Neugeborenen bzw. von deren Eltern zu übermitteln haben. Diese Daten dürfen die Jugendämter nach dem ausdrücklichen Wortlaut der Vorschrift allerdings nur zum Zwecke der allgemeinen Förderung der Erziehung in der Familie (§ 16 SGB VIII) verwenden. Mit den gesetzlichen Neuregelungen wird die bereits vielfach bestehende Praxis auf eine sichere datenschutzrechtliche Grundlage gestellt.

§ 13 a MeldDV Datenübermittlungen an die Jugendämter
(1) Die Meldebehörden … übermitteln jeweils zum Ersten eines Monats dem örtlich zuständigen Jugendamt zur Erfüllung seiner Aufgaben nach § 16 Abs. 1 Satz 1 und Abs. 2 des Achten Buches Sozialgesetzbuch (SGB VIII) folgende Daten Neugeborener: …
(2) [1]Ändern sich die in Abs. 1 genannten Daten vor Vollendung des 14. Lebensjahres oder ziehen Kinder vor Vollendung des 14. Lebensjahres mit alleiniger Wohnung oder Hauptwohnung in den Freistaat Bayern oder aus diesem weg, teilen die Meldebehörden dies jeweils einmal monatlich unter Angabe der in Abs. 1 genannten Daten den örtlich zuständigen Jugendämtern mit. [2]In Sterbefällen erfolgt die Datenübermittlung unverzüglich.
(3) [1]Die Jugendämter dürfen die nach Abs. 1 und 2 übermittelten Daten nur verwenden, um den gesetzlichen Vertretern von Kindern Leistungen der allgemeinen Förderung der Erziehung in der Familie nach § 16 Abs. 1 Satz 1 und Abs. 2 SGB VIII anzubieten. [2]Die Daten sind nach Vollendung des 14. Lebensjahres oder bei einem Wegzug aus dem Freistaat Bayern unverzüglich zu löschen.

8.3 Elternbrief

Das Zentrum Bayern Familie und Soziales – Bayerisches Landesjugendamt hat mit finanzieller Unterstützung des Bayerischen Staatsministeriums für Arbeit und Sozialordnung, Familie und Frauen Elternbriefe erstellt. Diese sollen zukünftig alle Eltern in Bayern „just in time“ zum jeweiligen Entwicklungsstand des Kindes über erziehungsrelevante Themen informieren.

Dabei sind insbesondere zwei Verbreitungswege geplant:

a) Zum einen sollen Eltern ab dem 01.07.2012 über ein Online-Portal im Wege eines Downloads bzw. eines Newsletter-Abonnements in den Besitz der Elternbriefe gelangen können.

   Dabei war meiner Einschätzung nach insbesondere ein Aspekt datenschutzrechtlich problematisch: Das Erheben der E-Mail-Adresse der Eltern sowie das Geburtsdatum des Kindes ist nur zulässig, wenn ihre Kenntnis zur Erfüllung einer Aufgabe nach dem Sozialgesetzbuch erfor-

derlich ist (§ 67 a Abs. 1 Satz 1 SGB X). Einschlägige Aufgabe ist die Förderung der Erziehung in der Familie (§ 16 SGB VIII). Zuständig dafür sind allerdings die Jugendämter (§§ 85 Abs. 1, 69 Abs. 1 bzw. 3 SGB VIII i.V.m. Art. 15 f. AGSG) – und **nicht** das Bayerische Landesjugendamt, das dieses Portal betreibt.

Letztlich konnte recht schnell mit dem Bayerischen Landesjugendamt gemeinsam eine Lösung gefunden werden, die das Bayerische Staatsministerium für Arbeit und Sozialordnung, Familie und Frauen mittragen konnte: Das Online-Portal kann zumindest für eine Übergangszeit als Modellprojekt zur Weiterentwicklung der Jugendhilfe angesehen werden. Damit kann sich das Landesjugendamt zumindest vorübergehend auf eine Zuständigkeit berufen (§ 85 Abs. 2 Nr. 4 SGB VIII i.V.m. Art. 24 Satz 2 AGSG). Während dieser Zeit soll im Gesetz zur Ausführung der Sozialgesetzbücher (AGSG) eine klare gesetzliche Zuständigkeitsregelung geschaffen werden.

b) Der zweite Vertriebsweg – die Verschickung der Elternbriefe per Post ab dem 01.10.2012 – ist aufgrund der zum 01.05.2012 in Kraft getretenen Neuregelung des § 13 a Meldedatenverordnung (siehe Nr. 8.2) zumindest datenschutzrechtlich unproblematisch. Nach dieser Regelung haben die Meldebehörden monatlich den Jugendämtern die Daten der Neugeborenen bzw. von deren Eltern zu übermitteln.

8.4 Kindergärten, andere Kindertagseinrichtungen und Tagespflege (BayKiBiG)

Das Bayerische Staatsministerium für Arbeit und Sozialordnung, Familie und Frauen hat mir im Berichtszeitraum den Gesetzentwurf zur Änderung des bayerischen Gesetzes zur Bildung, Erziehung und Betreuung von Kindern in Kindergärten, anderen Kindertagseinrichtungen und in Tagespflege (BayKiBiG-ÄndG) zugeleitet. Ich habe die Gelegenheit wahrgenommen, datenschutzrechtlich zu diesem Gesetzentwurf Stellung zu nehmen. Meine Anmerkungen wurden dabei vollständig übernommen.

a) Ein wesentlicher Punkt aus datenschutzrechtlicher Sicht ist dabei die gesetzliche Einführung einer Pflicht der Eltern zur Vorlage einer Bestätigung über die Teilnahme des Kindes an der letzten fälligen Früherkennungsuntersuchung (Art. 9 a Abs. 2 BayKiBiG-E). Damit wurde eine jahrelang bereits bestehende Praxis auf eine klare gesetzliche Grundlage gestellt.

Art. 9 a Abs. 2 BayKiBiG-E Kinderschutz
(2) Bei der Anmeldung zum Besuch einer Kindertageseinrichtung oder bei Aufnahme eines Kindes in die Tagespflege haben die Eltern eine Bestätigung der Teilnahme des Kindes an der letzten fälligen altersentsprechenden Früherkennungsuntersuchung vorzulegen. Die Nichtvorlage einer Bestätigung ist für die Förderung nach diesem Gesetz unschädlich. Der Träger ist verpflichtet, schriftlich festzuhalten, ob vonseiten der Eltern ein derartiger Nachweis vorgelegt wurde. Der Vermerk ist spätestens einen Monat nach Beendigung des Betreuungsverhältnisses der Einrichtung mit dem Kind zu löschen.

Ich habe mich ausdrücklich **nicht** gegen diese Pflicht ausgesprochen; dasselbe gilt auch hinsichtlich einer entsprechenden Vorlagepflicht bei der Beantragung des Landeserziehungsgelds sowie bei der Schuleingangsuntersuchung. Schließlich konnte so – im Gegensatz zu anderen Bundesländern – ein aus datenschutzrechtlicher Sicht problematisches Verfahren zur lückenlosen Nachverfolgung verhindert werden. Ein solches „Trackingverfahren" sollte die in Bayern bestehende Pflicht zur Teilnahme an den Früherkennungsuntersuchungen (Art. 14 Abs. 1 GDVG) kontrollieren.

Ich habe es auch begrüßt, dass die Kindertageseinrichtung ausschließlich dazu verpflichtet ist, schriftlich festzuhalten, dass ein derartiger Nachweis vorgelegt wurde. Ebenso aus datenschutzrechtlicher Sicht positiv ist die Tatsache, dass der Vermerk spätestens einen Monat nach Beendigung des Betreuungsverhältnisses zu löschen ist.

b) Ein weiterer aus datenschutzrechtlicher Sicht erfreulicher Punkt war die Einführung einer bereichsspezifischen datenschutzrechtlichen Regelung im BayKiBiG.

Bisher war die datenschutzrechtliche Gesetzeslage beim Vollzug des BayKiBiG überaus kompliziert. Bei öffentlich-rechtlichen Stellen waren die Regelungen des BayDSG, bei nichtöffentlichen Stellen die des BDSG einschlägig.

Zukünftig enthält das BayKiBiG – schon aus Gründen der Transparenz, aber auch aufgrund der Sensibilität der Daten – nachfolgende bereichsspezifische datenschutzrechtliche Regelung:

Art. 28 a BayKiBiG-E 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.

Darüber hinaus gelten für Kindertageseinrichtungen weiterhin beim Vollzug des SGB VIII die datenschutzrechtlichen Regelungen des Sozialgesetzbuchs (§§ 61 ff. SGB VIII; 67 ff. SGB X), bei öffentlich-rechtlichen Stellen unmittelbar, bei freien Trägern mittelbar über die Gewährleistungsverpflichtung des Jugendamts (§ 61 Abs. 3 SGB VIII).

8.5 Verbundverfahren

Bereits in früheren Tätigkeitsberichten habe ich mich mit der Problematik von „Verbundverfahren" befasst (siehe hierzu 23. Tätigkeitsbericht, Nr. 3.14 und Nr. 14.1 und 24. Tätigkeitsbericht, Nr. 7.7). Der „Trend" zu Informationsverbunden ging auch im Berichtszeitraum weiter:

a) Durch den Gesetzentwurf zur Änderung des bayerischen Gesetzes zur Bildung, Erziehung und Betreuung von Kindern in Kindergärten, anderen Kindertagseinrichtungen und in Tagespflege (BayKiBiG-ÄndG) sind zu-

künftig verpflichtend Daten für die kindbezogene Förderung durch ein Computerprogramm (KiBiG.web) an das zuständige Rechenzentrum zu melden (siehe Nr. 8.4). Dieses Programm ist bereits seit Dezember 2010 im Einsatz.

Im Rahmen dieses „Verbundverfahrens" sollen verschiedene Stellen verschiedene Informationen erhalten; KiBiG.web soll dabei vier Zwecke erfüllen:

– Dokumentation innerhalb der Kindertageseinrichtung
– Abwicklung des Bewilligungsverfahrens im Rahmen des BayKiBiG
– Ermöglichung von Statistik bzw. Evaluation
– Planung von Kindertageseinrichtungen

Sowohl bei der Erfassung der Kinder als auch des Personals in diesem Programm ist eine Eingabe des Vor- und Nachnamens in das Pflichtfeld „Bezeichnung" möglich. Damit handelt es sich derzeit zumindest teilweise um ein Verfahren mit personenbezogenen Daten. Dadurch sind derzeit die erhöhten rechtlichen bzw. technischen und organisatorischen Anforderungen anzuwenden.

So bedarf bei öffentlichen Stellen (z.B. öffentlich-rechtliche Kindertageseinrichtungen, die Regierungen, das Staatsministerium für Arbeit und Sozialordnung, Familie und Frauen, das Rechenzentrum Nord) der erstmalige Einsatz von automatisierten Verfahren, mit denen personenbezogene Daten verarbeitet werden, der vorherigen schriftlichen Freigabe durch die das Verfahren einsetzende öffentliche Stelle (Art. 26 BayDSG). Allerdings könnte das Staatsministerium für Arbeit und Sozialordnung, Familie und Frauen oder die von ihm ermächtigte öffentliche Stelle das Verfahren für den landesweiten Einsatz datenschutzrechtlich freigeben.

Außerdem sind zwischen den Kindertageseinrichtungen, den Regierungen bzw. dem Staatsministerium für Arbeit und Sozialordnung, Familie und Frauen einerseits und andererseits dem Rechenzentrum Nord sowie einer externen Firma, die Wartungstätigkeiten durchführt und Berechtigungen vergeben kann, jeweils Verträge zur Auftragsdatenverarbeitung zu schließen. Zudem ist ein Sicherheits- und Datenschutzkonzept erforderlich.

Ich habe dem Staatsministerium für Arbeit und Sozialordnung, Familie und Frauen anheim gestellt, ob entweder KiBiG.web zukünftig auf personenbezogene Daten verzichtet mit der Folge, dass die o.g. datenschutzrechtlichen Regelungen nicht anwendbar sind oder zeitnah die erhöhten rechtlichen bzw. technischen und organisatorischen Anforderungen erfüllt werden. Das Staatsministerium möchte zukünftig auf personenbezogene Daten verzichten; allerdings ist noch ungeklärt, wie mit den personenbezogenen Daten umgegangen wird, die sich aktuell noch im System befinden.

b) Auch für den Bereich der „Jugendsozialarbeit an Schulen" ist ein Programm entwickelt worden, durch das – vergleichbar zu KiBiG.web – verschiedene Stellen verschiedene Informationen erhalten sollen. Es soll ebenfalls vier Zwecke erfüllen (Dokumentation; Abwicklung des Bewilligungsverfahrens; Ermöglichung von Statistik bzw. Evaluation; Planung).

Leider ist auch dieses Programm bereits seit März 2012 im Einsatz, ohne dass – vergleichbar zu KiBiG.web – die datenschutzrechtlichen Anforderungen (z.B. Freigabe, Verträge zur Auftragsdatenverarbeitung etc.) erfüllt wurden. Besonders problematisch empfinde ich in diesem Zusammenhang die Tatsache, dass ein Staatsministerium auch hier eine finanzielle Förderung von dem Einsatz eines Programms abhängig macht, das gegen datenschutzrechtliche Vorschriften verstößt. Unabhängig von diesen formalen Fragen besteht aus meiner Sicht auch in der Sache noch erheblicher Klärungs- bzw. Überarbeitungsbedarf.

c) Leider ist das Verfahren TIZIAN trotz Bestehens eines mit mir weitgehend abgestimmten Gesetzentwurfs, immer noch nicht gesetzlich legitimiert (siehe hierzu 23. Tätigkeitsbericht, Nr. 3.14 und Nr. 14.1 sowie 24. Tätigkeitsbericht, Nr. 2.2.6 und Nr. 7.7). Dies hat zur Folge, dass derzeit umfangreiche Datensammlungen von Verbraucherschutz-, Lebensmittel- und Veterinärbehörden ohne ausreichende Rechtsgrundlage genutzt werden. Ich habe mehrmals die Staatsregierung darauf hingewiesen und den Erlass entsprechender Vorschriften über die Erhebung, Verarbeitung und Nutzung von Daten in Verbundverfahren angemahnt. Ich wiederhole diesen Appell hier noch einmal dringend.

8.6 „Jugendamt“ und „Bezirkssozialarbeit“

Im Rahmen einer Eingabe bin ich mit der Frage befasst worden, inwiefern zur Erfüllung von Aufgaben der Kinder- und Jugendhilfe die Weitergabe von Daten vom „Jugendamt“ an die „Bezirkssozialarbeit“ zulässig sei. Bei der Bezirkssozialarbeit handelt es sich um eine dezentrale und wohnortnahe Betreuung und Hilfe, die einen ganzheitlichen Ansatz der sozialen Versorgung „aus einer Hand“ verfolgt. Dies bedeutet, dass in der Bezirkssozialarbeit Hilfen nach unterschiedlichen Teilen der Sozialgesetzbücher vermittelt werden bzw. hierzu beraten wird.

Bei der Bezirkssozialarbeit sollte es sich nach Auffassung der Petentin schon um unzuständige Behörden zur Erfüllung von Aufgaben der Kinder- und Jugendhilfe handeln – mit der Folge einer datenschutzrechtlichen Unzulässigkeit der Weitergabe. Sie verwies dabei auf die §§ 85 Abs. 1, 69 Abs. 3 SGB VIII i.V.m. Art. 16 Abs. 1 AGSG.

§ 69 SGB VIII Träger der öffentlichen Jugendhilfe, Jugendämter …
(1) Die Träger der öffentlichen Jugendhilfe werden durch Landesrecht bestimmt.
…
(3) Für die Wahrnehmung der Aufgaben nach diesem Buch errichtet jeder örtliche Träger ein Jugendamt, jeder überörtliche Träger ein Landesjugendamt. …

Für die Wahrnehmung der Aufgaben nach dem SGB VIII ist der **örtliche Träger** (also die Landkreise und kreisfreien Gemeinden, Art. 15 Abs. 1 AGSG) zuständig (§ 85 Abs. 1 SGB VIII). Dieser hat jeweils **ein** Jugendamt zu errichten (Art. 16 Abs. 1 AGSG).

Das Jugendamt muss deshalb – worauf die Petentin richtigerweise hinwies – als **selbständige Organisationseinheit** innerhalb der Kommunalverwaltung zur Erfüllung der Aufgaben der Jugendhilfe organisiert sein (so ausdrücklich Wiesner, SGB VIII, § 69 Rdnr. 34). Durch die Regelung des § 69 Abs. 3 SGB VIII bzw. Art. 16 Abs. 1 AGSG wird also klargestellt, dass „der Befehl, Jugendämter … ein-

zurichten, in untrennbarem Zusammenhang mit der Pflicht steht, die Aufgaben der Kinder- und Jugendhilfe dieser Organisationseinheit zuzuweisen“ (so ausdrücklich BT-Drs. 12/2866 S. 19 f.).

Im Übrigen bleibt aber die **Organisationshoheit der kommunalen Gebietskörperschaften** unberührt, insbesondere die Entscheidung, wie diese Organisationseinheit weiter zu gliedern ist. So verbleibt weiterhin die volle Gestaltungsfreiheit, nach welchen fachlichen oder räumlichen Kriterien die Wahrnehmung der Aufgaben organisiert wird und in welchem Verhältnis zueinander allgemeine und spezialisierte Dienste eingerichtet werden (so ausdrücklich Wiesner, SGB VIII, § 69 Rdnr. 35).

Diese Auffassung entspricht auch dem sog. **funktionalen Behördenbegriff** im Sozialdatenschutz (§ 67 Abs. 9 SGB X).

§ 67 Abs. 9 SGB X
(9) Verantwortliche Stelle ist jede Person oder Stelle, die Sozialdaten für sich selbst erhebt, verarbeitet oder nutzt oder dies durch andere im Auftrag vornehmen lässt. Werden Sozialdaten von einem Leistungsträger im Sinne von § 12 des Ersten Buches erhoben, verarbeitet oder genutzt, ist verantwortliche Stelle der Leistungsträger. Ist der Leistungsträger eine Gebietskörperschaft, so sind eine verantwortliche Stelle die Organisationseinheiten, die eine Aufgabe nach einem der besonderen Teile dieses Gesetzbuches funktional durchführen.

Ist der Leistungsträger wie hier eine Gebietskörperschaft, so sind eine verantwortliche Stelle die Organisationseinheiten, die eine Aufgabe nach dem Sozialgesetzbuch – wie hier die Kinder- und Jugendhilfe – funktional durchführen (§ 67 Abs. 9 S. 3 SGB X). Dies gilt bei verschiedenen Organisationseinheiten einer Gebietskörperschaft auch im Hinblick auf eine dezentrale Geschäftsstelle und einer Zentrale des gleichen Leistungsträgers (siehe BT-Drs. 12/5187, S. 36; so ausdrücklich auch von Wulffen/Bieresborn, SGB X, § 67 Rdnr. 32 mit dem Hinweis auf die „Bezirkssozialämter“ in Berlin). Damit sind alle an einer Entscheidung notwendigerweise beteiligten Stellen innerhalb der Behördenhierarchie ein Teil der verantwortlichen Stelle.

Die „Praxis, die den **allgemeinen Sozialdienst außerhalb des Jugendamtes** organisiert und diesem die Wahrnehmung einzelner Aufgaben der Kinder- und Jugendhilfe zuweist, (ist aber) nur dann im Einklang mit der Rechtslage …, wenn dem **Leiter des Jugendamts die Fachaufsicht** für die Wahrnehmung aller Aufgaben nach diesem Gesetz erhalten bleibt und die Beteiligung des Jugendhilfeausschusses in vollem Umfang gesichert ist“ (so ausdrücklich BT-Drs. 12/3711 S. 40 f.).

Die Gebietskörperschaft konnte darlegen, dass dem Leiter des Jugendamtes die Fachaufsicht für die Wahrnehmung aller Aufgaben nach dem SGB VIII erhalten bleibt und die Beteiligung des Jugendhilfeausschusses in vollem Umfang gesichert ist. Unter diesen Umständen war eine Auslagerung von Aufgaben des allgemeinen sozialen Dienstes aus dem Jugendamt und deren Wahrnehmung außerhalb des Jugendamtes grundsätzlich nicht unzulässig (§ 69 Abs. 3 SGB VIII bzw. Art. 16 AGSG).

Aus diesen Gründen war die Weitergabe von Daten vom „Jugendamt“ an die „Bezirkssozialarbeit“ datenschutzrechtlich zulässig.

8.7 Formulare in der Sozialhilfe

Im Rahmen einer Eingabe wurde gerügt, die Erklärung einer Stadt zum Bezug von Grundsicherungsleistungen im Alter und bei Erwerbsminderungen verstoße gegen datenschutzrechtliche Bestimmungen. Ich habe diese Petition zum Anlass genommen, diese Erklärung von Amts wegen unabhängig vom Einzelfall datenschutzrechtlich zu bewerten.

Das Formular enthielt eine Vielzahl von Punkten, die aus meiner Sicht datenschutzrechtlich unzulässig bzw. in hohem Maße missverständlich sind. Bedauernswert ist hier wie in vielen vergleichbaren Fällen, dass durch derartige Formulare ihr beabsichtigter Zweck nicht erreicht wird. Statt Transparenz für den Betroffenen zu schaffen, bewirken sie häufig genau das Gegenteil. Im konkreten Fall war sogar für mich als datenschutzrechtlichen „Profi" großenteils nicht erkennbar, was mit der Regelung bezweckt war. So sollten beispielsweise Erklärungen, die für mich Einwilligungen zur Erhebung von Daten darstellten nach der Absicht ihrer Verfasser Hinweise auf die Rechtslage bei der Übermittlung von Daten sein. Ebenso unterschieden die Hinweise nicht eindeutig zwischen den einzelnen im Rahmen dieses Verfahrens beteiligten Stellen.

So wurden in diesem Fall diverse rechtliche Hinweise mit datenschutzrechtlichen „Erklärungen" vermischt. Letztere wurden sogar mit datenschutzrechtlichen „Einwilligungen" kombiniert, ohne dass die Unterschiede auffallen. Dies verstößt nicht nur gegen das Gesetz (§ 67 b Abs. 2 SGB X), sondern verwirrt den Betroffenen noch mehr. Außerdem fehlen oft die rechtlich gebotenen Hinweise.

§ 67 b Abs. 2 SGB X Zulässigkeit der Datenverarbeitung und -nutzung
(2) Wird die Einwilligung bei dem Betroffenen eingeholt, ist er auf den Zweck der vorgesehenen Verarbeitung oder Nutzung sowie auf die Folgen der Verweigerung der Einwilligung hinzuweisen. Die Einwilligung des Betroffenen ist nur wirksam, wenn sie auf dessen freier Entscheidung beruht. Die Einwilligung und der Hinweis bedürfen der Schriftform, soweit nicht wegen besonderer Umstände eine andere Form angemessen ist. Soll die Einwilligung zusammen mit anderen Erklärungen schriftlich erteilt werden, ist die Einwilligungserklärung im äußeren Erscheinungsbild der Erklärung hervorzuheben.

Auch hier musste ich – was leider nicht selten vorkommt – auf den Grundsatz der Erhebung beim Betroffenen (§ 67 a Abs. 2 SGB X) hinweisen. Für viele Behörden scheint es angenehmer zu sein, grundsätzlich die erforderlichen Unterlagen bei Dritten anzufordern als sich unmittelbar mit dem Betroffenen auseinanderzusetzen.

Die Stadt hat zum Teil von Antragstellern Einwilligungen zu Datenübermittlungen erbeten, obwohl die Stadt diese Datenübermittlungen schon auf Grund gesetzlicher Bestimmungen vornehmen konnte (z.B. auf Grund von § 69 SGB X). Dies ist problematisch, denn damit wird eine zur Aufgabenerfüllung der Behörde notwendige und vom Gesetzgeber für zulässig erklärte Datenübermittlung von der ungewissen Abgabe einer Einwilligung abhängig gemacht. Ist eine Datenübermittlung zur Aufgabenerfüllung der Behörde tatsächlich erforderlich, sollte die Behörde von vornherein auf Grund der gesetzlichen Bestimmungen handeln. Falls allerdings die Stadt dennoch eine Einwilligung erbittet, muss die Einwilligung gemäß § 67 b Abs. 2 Satz 2 SGB X auf der freien Entscheidung des Betroffenen beruhen. Es wäre unzulässig, bei der Einholung der Einwilligung Druck auszuüben mit dem Hinweis auf die ohnehin vorhandene gesetzliche Bestim-

mung oder gar mit der Ankündigung, die Übermittlung auf Grund einer gesetzlichen Befugnis vorzunehmen, falls keine Einwilligung erfolgt.

Grundsätzlich positiv ist die Tatsache, dass die Stadt in ihrem EDV-System Formulare zur Verfügung stellt. Es spricht grundsätzlich auch nichts dagegen, diese Formulare im Einzelfall anzupassen, sofern das Formular im konkreten Fall nicht passt. Allerdings führte genau dieses Vorgehen in der Vergangenheit bei dieser Stadt vielfach zu Fehlern. Daher halte ich es für zielführender, für jede Konstellation ein rechtlich klares Formular zur Verfügung zu stellen. Aus diesem Grund habe ich die Stadt aufgefordert, alle im Intranet zur Verfügung gestellten datenschutzrechtlichen Formblätter im Bereich des SGB XII zu überprüfen und ggf. zu überarbeiten. Außerdem wird zukünftig bei der Erstellung bzw. Änderung derartiger Hinweise der städtische Datenschutzbeauftragte oder zumindest die Datenschutzbeauftragten der jeweiligen Ämter mit einbezogen werden.

8.8 Erweitertes Führungszeugnis

Im Berichtszeitraum bin ich um Stellungnahme gebeten worden, ob es datenschutzrechtlich zulässig ist, dass eine Geschäftsleitung bestimmte Beschäftigtengruppen mit beruflichem Kontakt zu Minderjähren aufgefordert hat, ein erweitertes Führungszeugnis zu beantragen und vorzulegen. Diese Fragestellung ist in allen Fallgestaltungen von Belang, in denen Beschäftigte Kontakt zu Minderjährigen haben. Ich habe daher diese Petition zum Anlass genommen, unabhängig vom Einzelfall von Amts wegen diese Frage datenschutzrechtlich zu klären.

a) Ausgangspunkt der rechtlichen Bewertung ist § 30 a Abs. 1 BZRG.

§ 30 a Abs. 1 BZRG Antrag auf ein erweitertes Führungszeugnis
(1) Einer Person wird auf Antrag ein erweitertes Führungszeugnis erteilt,
1. wenn die Erteilung in gesetzlichen Bestimmungen unter Bezugnahme auf diese Vorschrift vorgesehen ist oder
2. wenn dieses Führungszeugnis benötigt wird für
a) die Prüfung der persönlichen Eignung nach § 72 a des Achten Buches Sozialgesetzbuch – Kinder- und Jugendhilfe –,
b) eine sonstige berufliche oder ehrenamtliche Beaufsichtigung, Betreuung, Erziehung oder Ausbildung Minderjähriger oder
c) eine Tätigkeit, die in einer Buchstabe b) vergleichbaren Weise geeignet ist, Kontakt zu Minderjährigen aufzunehmen.

§ 30 a BZRG ist jedoch nur eine **Befugnisnorm für Datenübermittlungen, nicht für Datenerhebungen.** Aus dieser Vorschrift ist auch abzuleiten, dass die Erhebung eines erweiterten Führungszeugnisses nicht auf eine Einwilligung des Betroffenen gestützt werden kann; sonst würde die gesetzlich vorgesehene Zweckbindung bei Antragstellung leerlaufen.

b) Eine **ausdrückliche Rechtsgrundlage** für die Erhebung erweiterter Führungszeugnisse existiert mit dem zum 01.01.2012 geänderten § 72 a SGB VIII **nur für den Bereich der Kinder- und Jugendhilfe**.

§ 72 a SGB VIII Tätigkeitsausschluss einschlägig vorbestrafter Personen
(1) Die Träger der öffentlichen Jugendhilfe dürfen für die Wahrnehmung der Aufgaben in der Kinder- und Jugendhilfe keine Person beschäftigen

oder vermitteln, die rechtskräftig wegen einer Straftat nach den §§ 171, 174 bis 174 c, 176 bis 180 a, 181 a, 182 bis 184 f, 225, 232 bis 233 a, 234, 235 oder 236 des Strafgesetzbuchs verurteilt worden ist. Zu diesem Zweck sollen sie sich bei der Einstellung oder Vermittlung und in regelmäßigen Abständen von den betroffenen Personen ein Führungszeugnis nach § 30 Absatz 5 und § 30 a Absatz 1 des Bundeszentralregistergesetzes vorlegen lassen.
(2) Die Träger der öffentlichen Jugendhilfe sollen durch Vereinbarungen mit den Trägern der freien Jugendhilfe sicherstellen, dass diese keine Person, die wegen einer Straftat nach Absatz 1 Satz 1 rechtskräftig verurteilt worden ist, beschäftigen.
(3) Die Träger der öffentlichen Jugendhilfe sollen sicherstellen, dass unter ihrer Verantwortung keine neben- oder ehrenamtlich tätige Person, die wegen einer Straftat nach Absatz 1 Satz 1 rechtskräftig verurteilt worden ist, in Wahrnehmung von Aufgaben der Kinder- und Jugendhilfe Kinder oder Jugendliche beaufsichtigt, betreut, erzieht oder ausbildet oder einen vergleichbaren Kontakt hat. Hierzu sollen die Träger der öffentlichen Jugendhilfe über die Tätigkeiten entscheiden, die von den in Satz 1 genannten Personen auf Grund von Art, Intensität und Dauer des Kontakts dieser Personen mit Kindern und Jugendlichen nur nach Einsichtnahme in das Führungszeugnis nach Absatz 1 Satz 2 wahrgenommen werden dürfen.
(4) Die Träger der öffentlichen Jugendhilfe sollen durch Vereinbarungen mit den Trägern der freien Jugendhilfe sowie mit Vereinen im Sinne des § 54 sicherstellen, dass unter deren Verantwortung keine neben- oder ehrenamtlich tätige Person, die wegen einer Straftat nach Absatz 1 Satz 1 rechtskräftig verurteilt worden ist, in Wahrnehmung von Aufgaben der Kinder- und Jugendhilfe Kinder oder Jugendliche beaufsichtigt, betreut, erzieht oder ausbildet oder einen vergleichbaren Kontakt hat. Hierzu sollen die Träger der öffentlichen Jugendhilfe mit den Trägern der freien Jugendhilfe Vereinbarungen über die Tätigkeiten schließen, die von den in Satz 1 genannten Personen auf Grund von Art, Intensität und Dauer des Kontakts dieser Personen mit Kindern und Jugendlichen nur nach Einsichtnahme in das Führungszeugnis nach Absatz 1 Satz 2 wahrgenommen werden dürfen.
(5) Träger der öffentlichen und freien Jugendhilfe dürfen von den nach den Absätzen 3 und 4 eingesehenen Daten nur den Umstand, dass Einsicht in ein Führungszeugnis genommen wurde, das Datum des Führungszeugnisses und die Information erheben, ob die das Führungszeugnis betreffende Person wegen einer Straftat nach Absatz 1 Satz 1 rechtskräftig verurteilt worden ist. Die Träger der öffentlichen und freien Jugendhilfe dürfen diese erhobenen Daten nur speichern, verändern und nutzen, soweit dies zum Ausschluss der Personen von der Tätigkeit, die Anlass zu der Einsichtnahme in das Führungszeugnis gewesen ist, erforderlich ist. Die Daten sind vor dem Zugriff Unbefugter zu schützen. Sie sind unverzüglich zu löschen, wenn im Anschluss an die Einsichtnahme keine Tätigkeit nach Absatz 3 Satz 2 oder Absatz 4 Satz 2 wahrgenommen wird. Andernfalls sind die Daten spätestens drei Monate nach der Beendigung einer solchen Tätigkeit zu löschen.

c) Dementsprechend kann eine Datenerhebung **außerhalb der Kinder- und Jugendhilfe** gegenwärtig nur auf **allgemeine Erhebungsbefugnisse** gestützt werden (Art. 102 BayBG (analog) bzw. Art. 16 Abs. 1 BayDSG). Dies gilt allerdings nur dann, wenn ihre Kenntnis zur Erfüllung der in der Zuständigkeit der erhebenden Stelle liegenden Aufgaben **erforderlich** ist.

Das Bundeszentralregistergesetz begrenzt dabei die Zulässigkeit einer Datenerhebung von vorneherein auf Fälle der **Beaufsichtigung, Betreuung, Erziehung oder Ausbildung Minderjähriger** oder **Tätigkeiten mit vergleichbaren Kontakt zu Minderjährigen**(§ 30 a Abs. 1 Nr. 2 b) und c) BZRG). Dabei sind folgende Fallgestaltungen zu unterscheiden:

aa) Soll ein erweitertes Führungszeugnis **vor Einstellung** bzw. **erstmaliger Betrauung** einer Person mit Aufgaben erhoben werden, die einen Kontakt zu Minderjährigen begründen, ist die Beschaffung im erforderlichen Maß zulässig, soweit der Schutz von anvertrauten Minderjährigen zur Aufgabenstellung der öffentlichen Stelle gehört.

bb) Soll **einmalig** ein erweitertes Führungszeugnis **im Rahmen eines laufenden Kontaktverhältnisses** erhoben werden, ist die Beschaffung erweiterter Führungszeugnisse im erforderlichen Maß zulässig, soweit der Schutz von anvertrauten Minderjährigen zur Aufgabenstellung der öffentlichen Stelle gehört. Bei einer einmaligen **flächendeckenden verdachtsunabhängigen Erhebung** von erweiterten Führungszeugnissen von Beschäftigten mit Kontaktverhältnissen muss aber in jedem Fall die Erforderlichkeit einer solchen Maßnahme eingehend begründet werden, wenn keine Anhaltspunkte für eine konkrete Gefährdung von Minderjährigen bestehen.

cc) Eine Erforderlichkeit kann unter weiteren Voraussetzungen beispielsweise jedoch dann angenommen werden, wenn und soweit **eine betroffene Person** selbst einen **konkreten Anlass** für eine Überprüfung zu verantworten hat.

dd) Soll **in regelmäßigen zeitlichen Abständen** ein erweitertes Führungszeugnis **im Rahmen eines laufenden Kontaktverhältnisses** erhoben werden, ist zu berücksichtigen, dass die regelmäßige Einholung von erweiterten Führungszeugnissen einer Dauerkontrolle der hiervon betroffenen Person nahekommt. Sie stellt damit einen **gesteigerten** Eingriff in das Grundrecht auf informationelle Selbstbestimmung dar. Dafür ist eine bereichsspezifische, hinreichend normbestimmte Erhebungsvorschrift geboten, die auf die Vorschrift des § 30 a BZRG Bezug zu nehmen hat. Hierfür spricht zunächst der Umstand, dass der Bundesgesetzgeber für die regelmäßige Erhebung von erweiterten Führungszeugnissen die bereichsspezifische Vorschrift des § 72 a SGB VIII für geboten gehalten hat. Weiterhin sind die allgemeinen Bestimmungen **nicht** geeignet, eingriffsintensive Datenerhebungen zu rechtfertigen.

Ich habe meine Rechtsauffassung den Bayerischen Staatsministerien des Innern, für Umwelt und Gesundheit, für Arbeit und Sozialordnung, Familie und Frauen sowie der Bayerischen Krankenhausgesellschaft e.V. zur Kenntnis bzw. der Bitte um Weiterleitung und Beachtung gegeben.

8.9 Personalausweiskopie

Im Berichtszeitraum wurde die Frage an mich herangetragen, ob eine Behörde im Schwerbehindertenverfahren eine Kopie des Personalausweises anfertigen

und zur Akte nehmen darf. Ich habe hierzu die Auffassung vertreten, dass zur Identifizierung des Antragstellers das Erheben und Speichern von Name, Anschrift, Geburtsdatum und auch des Geburtsortes erforderlich ist, nicht jedoch die Kenntnis der Augenfarbe, der Körpergröße und des Lichtbildes. Um – bei Zweifeln an der Identität – überprüfen zu können, ob die vom Antragssteller gemachten Angaben der Richtigkeit entsprechen, ist hierfür lediglich die kurze Vorlage eines Ausweispapiers und ein Hinweis in der Akte, dass sich der Antragsteller durch ein Ausweispapier identifiziert hat, erforderlich, nicht jedoch das Anfertigen und Einheften einer Kopie.

In diesem Zusammenhang habe ich auch darauf hingewiesen, dass durch eine Änderung des Personalausweisgesetzes zum 01.11.2010 nach dessen § 1 Abs. 1 Satz 2 vom Ausweisinhaber nicht mehr verlangt werden darf, den Personalausweis zu hinterlegen oder in sonstiger Weise den Gewahrsam aufzugeben. Dies gilt nach mir vorliegenden Schreiben des Bundesministeriums des Innern, des Bayerischen Staatsministeriums des Innern und des Bayerischen Staatsministeriums für Arbeit und Sozialordnung, Familie und Frauen auch hinsichtlich von Ausweiskopien.

Ebenfalls um den Einbehalt eines kopierten Ausweisdokumentes ging es in einem weiteren, allerdings völlig anders gelagerten Fall, nämlich im Zusammenhang mit der sogenannten „erziehungsbeauftragten Person". Seit dem Inkrafttreten des Jugendschutzgesetzes am 01.04.2003 haben die Eltern die Möglichkeit, für die Begleitung ihres Kindes eine sog. erziehungsbeauftragte Person im Sinne von § 1 Abs. 1 Nr. 4 JuSchG zu benennen.

§ 1 Abs. 1 Nr. 4 JuSchG Begriffsbestimmungen
(1) Im Sinne dieses Gesetzes …
4. ist erziehungsbeauftragte Person, jede Person über 18 Jahren, soweit sie auf Dauer oder zeitweise aufgrund einer Vereinbarung mit der personensorgeberechtigten Person Erziehungsaufgaben wahrnimmt oder soweit sie ein Kind oder eine jugendliche Person im Rahmen der Ausbildung oder der Jugendhilfe betreut.

Auf diese Weise können die nach dem Jugendschutzgesetz bestehenden zeitlichen Beschränkungen zum Beispiel für den Besuch von Gaststätten oder Diskotheken aufgehoben werden. Vom Gesetz wird zwar keine Schriftform für die Vereinbarung gefordert. Da nach § 2 Abs. 1 JuSchG die erziehungsbeauftragten Personen ihre Berechtigung auf Verlangen darzulegen und die Veranstalter und Gewerbetreibende in Zweifelsfällen deren Berechtigung zu überprüfen haben, ist eine schriftliche Beauftragung durchaus empfehlenswert und wird in der Praxis auch so vorgenommen. Die Jugendämter vieler kreisfreier Städte und Landkreise stellen hierfür eigens Formblattvorlagen zur Verfügung.

So war es auch in dem der Eingabe zugrunde liegenden Fall. Neben der schriftlichen Beauftragung hat der Beschwerdeführer der erziehungsbeauftragten Person eine Kopie seines Reisepasses zur Vorlage beim Veranstalter mitgegeben, um die Echtheit seiner Unterschrift nachweisen zu können. Der Sicherheitsdienst des Veranstalters berief sich allerdings darauf, die Ausweiskopie einziehen zu dürfen, und gab diese nicht mehr zurück.

Ich habe hierzu die Auffassung vertreten, dass der Veranstalter zwar die Befugnis hat, sich eine Ausweiskopie der Eltern vorlegen zu lassen, um überprüfen zu können, ob die Unterschrift auf der Bescheinigung mit der Unterschrift auf dem

Ausweisdokument übereinstimmt. Das Speichern, also das Aufbewahren der Ausweiskopie habe ich jedoch nicht für erforderlich gehalten. Das zunächst uneinsichtige Ordnungsamt einer Großen Kreisstadt hat sich nach einigem Schriftwechsel jedoch durch mich eines Besseren belehren lassen und die örtliche Diskothek und die in der Großen Kreisstadt tätigen Sicherheitsdienste darüber informiert, dass ein Einbehalten von Ausweiskopien nicht mehr zulässig ist.

Ergänzend möchte ich in diesem Zusammenhang darauf hinweisen, dass es aufgrund der oben bereits dargelegten Änderung des Personalausweisgesetzes ebenfalls nicht mehr zulässig ist, die Hinterlegung des Personalausweises der Minderjährigen oder dessen Kopie beim Gewerbetreibenden oder Veranstalter zu fordern.

8.10 Callcenter

Im Berichtszeitraum habe ich mich aufgrund einiger Eingaben mit verschiedenen Telefonaktionen befasst, die durch Callcenter im Auftrag von Krankenkassen bei Krankenversicherten durchgeführt wurden.

a) Zum einen will eine Krankenkasse auf diesem Wege Kundenzufriedenheitsanalysen durchführen. Diese sollen Teil einer Organisationsuntersuchung sein, die auf eine Serviceoptimierung ausgerichtet ist.

   aa) Ein solches Nutzen der Versichertendaten sollte nach Auffassung der Krankenkasse zur Erfüllung der gesetzlichen Aufgaben der Aufklärung, Beratung und Auskunft erforderlich sein. Meiner Einschätzung nach bezweckt die Telefonaktion aber vorrangig eine Organisationsuntersuchung bzw. die Werbung beim Kunden. Zum anderen lässt sich mittelbar nahezu jede Maßnahme auf die sozialrechtlichen Grundsätze der Aufklärung, Beratung und Auskunft beziehen; dadurch würde der Datenschutz der Kundschaft aber komplett ausgehöhlt.

   bb) Außerdem habe ich Zweifel daran, inwiefern diese Nutzung der Kundendaten erforderlich ist; in jedem Fall ist sie unverhältnismäßig. Selbst wenn Telefonbefragungen im Vergleich zu schriftlichen Befragungen besser geeignet sein sollten, stellen sie einen erheblich größeren Eingriff in die Privatsphäre der Betroffenen dar.

   cc) Ebenso kann meiner Einschätzung nach keine Maßnahme datenschutzrechtlich erforderlich sein, die wettbewerbsrechtlich unzulässig ist. Meiner Einschätzung nach liegt aufgrund des „Werbungscharakters“ der Anrufe ein Verstoß gegen § 7 Abs. 2 UWG vor.

   § 7 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 Einwilli-

gung oder gegenüber einem sonstigen Marktteilnehmer ohne dessen zumindest mutmaßliche Einwilligung …,

Ich erlaube mir, hier auszugsweise die Leitsätze von Entscheidungen des OLG Köln (Urteile vom 12.12.2008 – 6 U 41/08 OLG Köln bzw. vom 30.03.2012 6 U 191/11; WRP 2012, 725) zu zitieren:

„Wird ein Meinungsforschungsinstitut von einem Unternehmen mit einer Telefonumfrage gegenüber Verbrauchern beauftragt (hier: Kundenbefragung), liegt hierin jedenfalls dann eine unlautere Telefonwerbung und damit eine unzumutbare Belästigung im Sinne von § 7 Abs. 2 Nr. 2 UWG, wenn die Anrufe zumindest mittelbar der Absatzförderung des auftraggebenden Unternehmens dienen … Eine telefonische Umfrage, die die Zufriedenheit der Kunden mit den Dienstleistungen betrifft und das Ziel verfolgt, Service und Leistungen zu verbessern und so Kunden zu erhalten, stellt insoweit Werbung im Sinne von § 7 Abs. 2 Nr. 2 UWG dar. …"

„Lässt ein Unternehmer einen Kunden, der ihm zuvor als Geschäftsmann einen Dienstleistungsauftrag erteilt hatte … durch ein Meinungsforschungsinstitut anrufen und nach seiner Zufriedenheit befragen, ist dies als gem. § 7 Abs. 1 UWG unzumutbare Belästigung unzulässig, wenn nicht eine zumindest mutmaßliche Einwilligung des Kunden vorliegt."

Hauptargument gegen die Werbeabsicht ist nach Auffassung der Krankenkasse die Tatsache, dass die telefonische Befragung verdeckt durchgeführt wird, also der Auftraggeber nicht genannt wird. Meiner Einschätzung nach kann jedoch ein Verstoß gegen § 67 a Abs. 3 SGB X nicht als Argument für eine fehlende Werbeintention herangezogen werden.

§ 67 a Abs. 3 SGB X Datenerhebung
(3) Werden Sozialdaten beim Betroffenen erhoben, ist er, sofern er nicht bereits auf andere Weise Kenntnis erlangt hat, über die Zweckbestimmungen der Erhebung, Verarbeitung oder Nutzung und die Identität der verantwortlichen Stelle zu unterrichten.

dd) Auch das Erheben von Daten im Rahmen der Telefoninterviews ist aus meiner Sicht nicht erforderlich bzw. verhältnismäßig. Schließlich kann meiner Ansicht nach auch zumindest ein vergleichbarer Effekt durch Fragebögen erzielt werden, die anonym zurückgeschickt werden könnten. Keinesfalls anschließen konnte ich mich der Auffassung der Krankenkasse, dass bei den Telefoninterviews überhaupt keine personenbezogenen Daten erhoben werden. Schließlich kommt es beim Beschaffen von Daten gar nicht auf eine mögliche anonyme Erfassung bzw. Auswertung an.

b) Im zweiten Fall rügte ein Petent die telefonische Kontaktaufnahme durch ein Callcenter, das im Auftrag der Krankenkasse deren Programme bewarb.

aa) Schon die zugrundeliegende Auftragsdatenverarbeitung zwischen Krankenkasse und Callcenter war datenschutzrechtlich bedenklich.

Zum einen war der Datenschutzvertrag rechtlich auf dem Stand des Jahres 2003, zum anderen fand die letzte „regelmäßige Prüfung“ vor über fünf Jahren statt.

bb) In diesem Fall stützte die Krankenkasse überdies ihr Vorgehen – im Gegensatz zu den Kundenzufriedenheitsanalysen – auf eine Einwilligung. Grundsätzlich akzeptiere ich einen solchen Weg angesichts der bei den Kundenzufriedenheitsanalysen aufgezeigten Probleme. Allerdings erfüllte die Einwilligung nicht die gesetzlichen Anforderungen (§ 67 b Abs. 2 SGB X): So ist der Betroffene auf den Zweck hinzuweisen. Ebenso muss die Erklärung verdeutlichen, welche konkreten Daten zu welchem konkreten Zweck – hier also der Information über Gesundheitsangebote – genutzt werden dürfen. Eine Generaleinwilligung reicht nicht aus. Ich habe daher der Krankenkasse empfohlen, die Formulierungen in der Einwilligungserklärung („interne Zwecke“, „spätere Informations- und Beratungszwecke“, „schriftlicher und telefonischer Kontakt“) genauer zu fassen. Ebenso ist der Betroffene auf die Folgen der Verweigerung der Einwilligung hinzuweisen. Soll die Einwilligung – wie in dem problematisierten Formular – zusammen mit anderen Erklärungen schriftlich erteilt werden, ist die Einwilligungserklärung im äußeren Erscheinungsbild der Erklärung hervorzuheben. Leider lag hier genau der Fall vor, den das Gesetz verhindern will: Im „Kleingedruckten“ wird eine Einwilligung „versteckt“, so dass der Betroffene unterschreibt, ohne dass ihm ganz klar wird, dass es eine Einwilligung ist. Im übrigen habe ich darauf hingewiesen, dass die Möglichkeit des Streichens der Einwilligungserklärung als Annahme nicht ausreicht.

§ 67 b Abs. 2 SGB X Zulässigkeit der Datenverarbeitung und -nutzung
(2) Wird die Einwilligung bei dem Betroffenen eingeholt, ist er auf den Zweck der vorgesehenen Verarbeitung oder Nutzung sowie auf die Folgen der Verweigerung der Einwilligung hinzuweisen. Die Einwilligung des Betroffenen ist nur wirksam, wenn sie auf dessen freier Entscheidung beruht. Die Einwilligung und der Hinweis bedürfen der Schriftform, soweit nicht wegen besonderer Umstände eine andere Form angemessen ist. Soll die Einwilligung zusammen mit anderen Erklärungen schriftlich erteilt werden, ist die Einwilligungserklärung im äußeren Erscheinungsbild der Erklärung hervorzuheben.

Die Krankenkasse hat sich bereit erklärt, die Einwilligungserklärung zeitnah zu überarbeiten.

cc) Außerdem habe ich klargestellt, dass eine potentielle vom Kunden eingeräumte Einwilligung in eine telefonische Kontaktierung nicht auch gleichzeitig eine Befugnis zur Erhebung, Verarbeitung und Nutzung von Daten darstellt. Hier stellen sich dieselben Problematiken wie bei der Kundenzufriedenheitsanalyse.

8.11 Krankengeldfallmanagement

Im Berichtszeitraum habe ich mich aufgrund einiger Eingaben und der Prüfung einer Krankenkasse mit verschiedenen Problematiken des Krankengeldfallmanagements befasst. Beim Krankengeldfallmanagement handelt es sich um eine systematische und zielgerichtete Fallsteuerung bei den Krankenkassen; dadurch soll der Ablauf sowie die Schnittstellen, insbesondere zu anderen Sozialversicherungsträgern optimiert werden. Dies soll beim Versicherten zur Überwindung seiner Arbeitsunfähigkeit und zur Wiedereingliederung ins Arbeitsleben führen. Außerdem soll dadurch zum einen die Qualität erhöht, aber auch die Kosten minimiert werden.

Besonders strittig ist die Frage, inwiefern die Krankenkasse bei medizinischen Daten eine eigene Datenerhebungsbefugnis besitzt bzw. diese zur Kenntnis nehmen kann oder aber eine Kenntnisnahme derartiger Daten grundsätzlich ausschließlich dem Medizinischen Dienst der Krankenversicherung (MDK) zugewiesen ist. Ich habe bereits in meinem 17. Tätigkeitsbericht dargelegt, dass die für den MDK bestimmten Daten zwar auch über die Krankenkassen zugeleitet werden können; es muss dabei aber „ausgeschlossen" werden, dass die Krankenkasse vom Inhalt von Daten für den MDK Kenntnis nimmt (siehe hierzu 17. Tätigkeitsbericht, Nr 4.4.2). Daher sind die Unterlagen für den MDK in ein weiteres verschlossenes Kuvert für den MDK zu legen. Allerdings erheben auch weiterhin einige Krankenkassen eine Vielzahl von Daten, die für den MDK bestimmt sind, „offen".

a) So bieten Krankengeldfallmanager in der Regel bei Arbeitsunfähigkeit schriftlich ein persönliches Beratungsgespräch an. In diesem wird ein Selbstauskunftsbogen gemeinsam mit dem Versicherten ausgefüllt. Dabei werden die Arbeitsplatzsituation und der Krankheitszustand, z.T. auch die familiäre oder soziale Situation abgefragt. Zum Teil sind sogar Vermerke erstellt worden, die das Aussehen bzw. das Auftreten des Versicherten bewertet haben.

   Problematisch ist zum einen der fehlende Hinweis auf die Freiwilligkeit bzw. der pauschale Hinweis auf die Mitwirkungspflicht des Versicherten. Zum anderen werden durch den Selbstauskunftsbogen unter anderem auch medizinische Daten „offen" von der Krankenkasse erhoben. Hier sehe ich jeweils noch Gesprächsbedarf. Einen Erfolg konnte ich hinsichtlich der – aus meiner Sicht nicht erforderlichen, teilweise sogar diskriminierenden – Vermerke erzielen; deren Erstellung wurde letztendlich eingestellt.

b) Auskünfte werden unter anderem auch von Leistungserbringern (Ärzten, Krankenhäusern etc.) erbeten, zu denen die Leistungserbringer zum Teil gesetzlich (z.B. §§ 294 a, 301, 276 Abs. 2 Satz 1 Halbsatz 2 SGB V, § 100 Abs. 1 Satz 1 Nr. 1 SGB X) oder auf Grund von Einwilligungen der Betroffenen verpflichtet sind (§ 100 Abs. 1 Satz 1 Nr. 2 SGB X). In solchen Fällen ist die Krankenkasse verantwortliche Stelle, selbst wenn sie Daten für den MDK erhebt.

   Vielfach kamen bei derartigen Anforderungen auch Formulare mit fehlerhaften Datenschutzhinweisen zum Einsatz. Außerdem wurde überwiegend keine schriftliche Einwilligungserklärung bzw. Schweigepflichtsentbindung des Versicherten eingeholt. Außerdem war häufig fraglich, ob ei-

ne derartige Datenerhebung überhaupt erforderlich war. In diesen Punkten ist zwar ein deutliches Entgegenkommen der Krankenkassen erkennbar, aber auch hier muss die Praxis noch den datenschutzrechtlichen Anforderungen gerecht werden.

Grundsätzlich werden diese Daten bei den Leistungserbringern postalisch erhoben mit der Aufforderung, das beigefügte Kuvert für den MDK zu verwenden. In eilbedürftigen Fällen oder beim „Nachfassen" wurden diese medizinischen Daten aber zum Teil auch per Fax erhoben. In diesen Fällen erfolgt die Rücksendung in der Regel auch per Fax – allerdings nicht unter Verwendung eines Umschlags für den MDK.

Allerdings muss „ausgeschlossen" werden, dass die Krankenkasse vom Inhalt von Daten für den MDK Kenntnis nimmt. Dies ist beim „normalen" Faxen unzweifelhaft nicht der Fall. Zum einen ist aus meiner Sicht Faxen schon an sich datenschutzrechtlich problematisch. Zum anderen handelt es sich hier um sensible Gesundheitsdaten mit erhöhtem Schutzbedarf - „für den MDK" und nicht „für die Krankenkasse". Ein „normales" Faxen von Unterlagen für den MDK an die Krankenkasse hat daher zukünftig zu unterbleiben.

c) Datenschutzrechtlich eine besondere Herausforderung stellt die Tatsache dar, dass die sog. Sozialmedizinische Fallberatung mit dem MDK grundsätzlich in den Räumlichkeiten der Krankenkasse stattfindet. Ich habe damals gefordert, dass auf dem beigelegten Versandkuvert die Anschrift des MDK angegeben sein muss. Inzwischen habe ich meine Auffassung weiterentwickelt. Grundsätzlich kann der Umschlag auch an die Krankenkasse adressiert sein, sofern dieser mit der Aufschrift versehen ist „Nur vom MDK zu öffnen". Allerdings muss der Mitarbeiter des MDK Bayern in den Räumlichkeiten der Krankenkasse einen eigenen von den übrigen Mitarbeitern abgeschirmten Arbeitsplatz und abschließbare Schränke haben, die nur MDK-Gutachtern zugänglich sind. Nach der Bearbeitung müssen in jedem Fall die Akte und die Befunde vom MDK-Gutachter wieder getrennt und die medizinischen Unterlagen in dem nur den MDK-Gutachtern zugänglichen Schrank zur ggf. weiteren Bearbeitung abgelegt werden.

Datenschutzrechtlich bedenklich ist die Tatsache, dass der Krankengeldfallmanager dem MDK-Mitarbeiter am Schreibtisch unmittelbar gegenüber sitzt, um einzelne von ihm bearbeitete Fälle zu besprechen. Ich habe daher einen gewissen räumlich Abstand zum Arbeitsplatz des MDK-Mitarbeiters angeregt, damit eine Einsicht in die MDK-Unterlagen ausgeschlossen ist.

d) Nach Abschluss des Falls wird die Akte vielfach zusammengeführt und im Keller aufbewahrt, bevor die Unterlagen datenschutzkonform vernichtet werden. Es erscheint zumutbar, die Akten auch im Keller getrennt aufzubewahren und anschließend zu vernichten.

8.12 Arbeitsunfähigkeitsbescheinigung und Blutzuckertagebuch

Durch einen behandelnden Arzt bin ich darauf aufmerksam gemacht worden, dass das Zentrum Bayern Familie und Soziales (ZBFS) – Versorgungsamt in Verfahren zur Feststellung einer Behinderung und des Grades der Behinderung

(GdB) sowie von Merkzeichen nach § 69 Sozialgesetzbuch – Neuntes Buch (SGB IX) von Antragstellern insbesondere verlange, – bei insulinpflichtigem Diabetes – ein **Blutzuckertagebuch** sowie eine von ihrer gesetzlichen Krankenkasse ausgestellte **Arbeitsunfähigkeitsbescheinigung** mit medizinischen Diagnosen unter Verwendung des ICD-10-Schlüssels vorzulegen.

Das ZBFS hat sich für die Zulässigkeit der Erhebung von Daten im Feststellungsverfahren nach dem Schwerbehindertenrecht grundsätzlich auf § 67 a Abs. 1 Satz 1 SGB X i.V.m. § 69 SGB IX berufen. Die erforderlichen Daten würden teilweise bei den Antragstellern erhoben; dies sei allerdings nur in geringem Umfang möglich, da diesen die maßgeblichen Unterlagen (ärztliche Befundberichte, Krankenhausentlassungsberichte, MDK-Gutachten usw.) großenteils nicht vorlägen. Das ZBFS sei daher darauf angewiesen, dass sich der Antragsteller mit der Einholung dieser Unterlagen bei den entsprechenden Stellen einverstanden erkläre und die Ärzte insoweit von der Schweigepflicht entbinde. Im Antragsformular werde darauf hingewiesen, dass alle Angaben freiwillig sind. Die **Anforderung des Blutzuckertagebuches** sei sinnvoll und geschehe im Interesse des Antragstellers, weil es zur Feststellung eines höheren GdB führen könne. Das ZBFS hat jedoch auch eingeräumt, dass selbstverständlich die Antragsteller nicht zur Führung eines Blutzuckertagebuches verpflichtet seien und das ZBFS auch nicht über ein Einsichtsrecht in das Blutzuckertagebuch verfüge.

Auf meine Bitte hin hat sich das ZBFS bereit erklärt, den **Hinweis gemäß § 67 a Abs. 3 Satz 3 SGB X**, dass die Vorlage eines Blutzuckertagebuches durch den Antragsteller aufgrund **freiwilliger** Entscheidung ohne eine entsprechende Rechtspflicht erfolge, nicht nur in dem Formular, das der Antragsteller für seinen Antrag auf Feststellung der Behinderung vom ZBFS erhalte, sondern darüber hinaus auch ausdrücklich in den Anschreiben an die Antragsteller aufzunehmen.

Arbeitsunfähigkeitsbescheinigungen ziehe das ZBFS in aller Regel nicht bei. Sie trügen zur Sachverhaltsermittlung grundsätzlich nichts bei, weil sie keine Aussage zur funktionellen Beeinträchtigung enthalten. Diese Datenerhebung sei damit (grundsätzlich) nicht erforderlich i.S.d. § 67 a SGB X. Eine Ausnahme sei nur in seltenen, besonders gelagerten Einzelfällen denkbar. So könne eine Arbeitsunfähigkeitsbescheinigung in bestimmten Fällen mit widersprüchlicher Befundlage oder ohne sonstigen objektiven Nachweis einer Beeinträchtigung zur Klärung beitragen. Insbesondere seien hier Fälle von Migräne zu nennen. Hier richte sich der GdB nach Häufigkeit und Dauer der Anfälle. Für diese lägen oft keine objektiven Nachweise vor. In solchen Fällen könne die Beiziehung von Arbeitsunfähigkeitsbescheinigungen sinnvoll sein, weil sie Rückschlüsse auf den Schwergrad der Migräne ermöglichen.

In den Fällen, die ausnahmsweise eine Anforderung der Arbeitsunfähigkeitsbescheinigung rechtfertigen können, hat mir das ZBFS zugesichert, in den Anschreiben an die Antragsteller die Erforderlichkeit im Sinne des § 67 a Abs. 1 Satz 1 SGB X besonders zu begründen und auf die Freiwilligkeit der Vorlage gemäß § 67 a Abs. 3 Satz 3 SGB X ausdrücklich hinzuweisen.

8.13 Mitteilungspflichten des Medizinischen Dienstes der Krankenversicherung

Im Rahmen einer Eingabe war ich mit der Frage befasst, in welchem Umfang der Medizinische Dienst der Krankenversicherung in Bayern (MDK Bayern) sozialmedizinische Gutachten an die Krankenkasse weitergegeben kann.

Laut Gesetz hat sich die Mitteilung des MDK an die Krankenkasse auf das **„Ergebnis der Begutachtung“** und die **„erforderlichen Angaben über den Befund“** zu beschränken (§ 277 Abs. 1 SGB V). Bei letzterem handelt es sich um das Gutachten untermauernde medizinische Angaben mit Bedeutung für die Leistungsgewährung (Becker/Kingreen/Sichert, SGB V, § 277 Rdnr. 2).

§ 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 . . . .

Mit dieser Thematik habe ich mich bereits 1998 befasst (siehe hierzu 18. Tätigkeitsbericht, Nr. 4.8.1). Bereits damals war es mein Anliegen, dass der MDK an die Krankenkasse eine inhaltlich auf das gesetzlich vorgesehene Maß reduzierte Version des MDK-Gutachtens weiterleitet. Demgegenüber kann das zur Archivierung beim MDK vorgesehene Gutachtenexemplar im Hinblick auf eventuelle Folgebegutachtungen detaillierter gehalten werden. Unter anderem auf meine Bemühungen hin wurde das EDV-Verfahren (ISmed) dahingehend überarbeitet, dass MDK-Gutachten nunmehr je nach Verwendungszweck inhaltlich variiert werden können. Diese technische Verbesserung stellte einen bedeutenden Fortschritt zur datenschutzgerechten Handhabung der Mitteilungen an die Krankenkasse dar. Leider wurden meiner Einschätzung nach die technischen Möglichkeiten dieses Programms in der Vergangenheit vielfach **nicht** genutzt, so dass häufig das gesamte Gutachten an die Krankenkasse weitergegeben wurde.

Daher wurde im Rahmen einer Besprechung mit dem MDK Bayern nachfolgendes Verfahren zur Handhabung des EDV-Programms „ISmed 3“ festgelegt:

Die MDK-Gutachter sollen zukünftig das Ergebnis der Begutachtung in das Datenfeld „Ergebnis“ aufnehmen. Dieses kann dann grundsätzlich an die Krankenkassen weitergeleitet werden. Angaben über den Befund sind zukünftig im Textfeld „Befund“ einzugeben. Eine Übermittlung dieses Textfeldes an die Krankenkassen ist dann zulässig, wenn dies im jeweiligen Einzelfall erforderlich erscheint. Darüber hinausgehende Punkte, insbesondere bei denen eine Übermittlung an die Krankenkassen nicht erforderlich erscheint, sind zukünftig im Textfeld „Vorgeschichte“ einzutragen. Dieses Textfeld ist grundsätzlich **nicht** an die Krankenkassen weiterzuleiten.

Des Weiteren wird der MDK Bayern seine Gutachter auf das präzise und datenschutzgerechte Ausfüllen des EDV-Programms ISmed 3 hinweisen. Ebenso wird er seine Gutachter hinsichtlich der korrekten Handhabung dieses Programms schulen und für datenschutzrechtliche Belange sensibilisieren.

8.14 Übermittlung von Daten durch Beistand

Mit datenschutzrechtlichen Fragen der Beistandschaft (§§ 1712 ff. BGB) war ich in der Vergangenheit bereits mehrfach befasst (siehe hierzu 16. Tätigkeitsbericht, Nr. 3.4.1 und 17. Tätigkeitsbericht, Nr. 4.7.2). Im Rahmen verschiedener Eingaben war im Berichtszeitraum die Rechtsfrage zu klären, inwiefern eine unaufgeforderte bzw. angeforderte Übermittlung von Daten über die Einkommensverhältnisse des unterhaltspflichtigen Elternteils durch den Beistand des Kindes an den sorgeberechtigten Elternteil datenschutzrechtlich zulässig ist.

Einschlägige Rechtsnorm ist hier § 68 Abs. 1 SGB VIII:

§ 68 Abs. 1 SGB VIII Sozialdaten im Bereich der Beistandschaft …
Der Beamte oder Angestellte, dem die Ausübung der Beistandschaft … übertragen ist, darf Sozialdaten nur erheben und verwenden, soweit dies zur Erfüllung seiner Aufgaben erforderlich ist. … .

Entscheidend ist also, ob die Übermittlung von Daten im konkreten Fall für das Führen einer Beistandschaft erforderlich ist. Die Weitergabe von Daten über die Einkommensverhältnisse des unterhaltspflichtigen Elternteils durch den Beistand des Kindes an den sorgeberechtigten Elternteil ist also dann zulässig, wenn sie zur Wahrnehmung einer konkreten Aufgabe des Beistands – in diesem Fall der Geltendmachung von Unterhaltsansprüchen (§ 1712 Abs. 1 Nr. 2 BGB) – erforderlich ist.

Überzeugt hat mich insbesondere ein Argument des Bayerischen Staatsministeriums für Arbeit und Sozialordnung, Familie und Frauen. Dieses hat darauf hingewiesen, dass eine unzureichende Information des Elternteils durch den Beistand nach den Erfahrungen der Praxis in aller Regel zu dem Kindeswohl nicht dienlichen Konflikten und auch zur Beendigung der Beistandschaft führt. Diese Argumentation ist für mich nachvollziehbar.

Aus diesem Grunde halte ich es für vertretbar, die bereits beschriebene Übermittlung von Daten grundsätzlich für erforderlich anzusehen. Meiner Einschätzung nach ist allerdings lediglich das Recht, nicht jedoch die Pflicht zur Datenübermittlung erforderlich und damit zulässig. Im Gegensatz dazu hält das Staatsministerium der Justiz und für Verbraucherschutz eine Übermittlungspflicht für geboten.

Insbesondere ist also eine Datenübermittlung zulässig, wenn die vom Kindsvater dargestellten Einkommensverhältnisse zweifelhaft oder nicht glaubhaft sind. Hier ist es zur gesetzlichen Aufgabenerfüllung des Beistandes erforderlich, sich mit dem Kenntnisstand der Mutter bezüglich der Einkommensverhältnisse des Vaters abzugleichen.

8.15 Übermittlung von Daten durch Jugendgerichtshilfe

Im Rahmen einer Eingabe beklagten mehrere Petentinnen, dass die Jugendgerichtshilfe im Rahmen eines Strafverfahrens gegen ihren Sohn bzw. Bruder ihre Geburtsdaten, vollständige Adresse mit Angabe der Postleitzahl, Wohnort und Straße inklusive Hausnummer sowie exakte derzeitige Schul-, Berufs- und Studienausbildungsrichtung dargelegt habe.

Die Beschwerde war zu einem großen Teil gerechtfertigt; es lag ein Verstoß gegen das Sozialgeheimnis vor (§ 35 Abs. 1 SGB I). Grundsätzlich unterstützt die Jugendgerichtshilfe die beteiligten Behörden (Gerichte, Staatsanwaltschaft) durch Erforschung der Persönlichkeit, der Entwicklung und der Umwelt des Beschuldigten (§§ 52 SGB VIII, 38 Abs. 2 JGG).

Dabei wurde der Grundsatz, dass Sozialdaten bei den Betroffenen selbst zu erheben sind, nicht beachtet (§ 62 Abs. 2 SGB VIII). Die Daten wurden auf standardisierte Weise beim Beschuldigten erfragt.

Die Personendaten der Familienangehörigen sollen dazu dienen, das zuständige Gericht sowie die Staatsanwaltschaft über die Familiensituation des Angeklagten zu informieren. Da die Familiensituation als zentrale Komponente für die Biographie des Angeklagten zu sehen ist, wird es grundsätzlich als erforderlich gesehen, diese entsprechend darzulegen (§§ 69 Abs. 1 Nr. 1 SGB X, 52 SGB VIII, 38 Abs. 2 JGG). Allerdings ging in diesem Fall letztlich sogar die Jugendgerichtshilfe selbst davon aus, dass auf die ausdrückliche Angabe der Namen und Geburtsdaten sowie der genauen Adressen hätte verzichtet werden können, da deren konkrete Nennung für die Aufgabenerfüllung nicht erforderlich gewesen wäre. Die Nennung der jeweiligen Schul-, Berufs- und Studienausbildungsrichtung hingegen war zur Auftragserfüllung erforderlich, da diese Aufschluss darüber geben können, welche Chancen der beruflichen Integration der Beschuldigte im Familienverbund vorgelebt bekam, diese hätte ihm als „positives Modell“ dienen können.

Letztendlich habe ich im Rahmen meines pflichtgemäßen Ermessens trotz Vorliegen eines datenschutzrechtlichen Verstoßes von einer Beanstandung abgesehen (Art. 31 Abs. 3 BayDSG). Maßgeblich dafür war hauptsächlich, dass sich die Jugendgerichtshilfe bei ihrem Bericht an einer zumindest missverständlichen Publikation einer Landesbehörde orientiert hatte.

Nach meiner Rüge hat diese Landesbehörde die entsprechende fachliche Empfehlung vollständig überarbeitet.

8.16 Übermittlung von Versichertendaten durch Krankenkasse

Im Wege einer Eingabe erfuhr ich, dass eine Krankenkasse anlässlich eines Amtshilfeersuchens einer Stadt Verordnungen übersandt habe, die von einem Arzt ausgestellt worden seien. Die in Rede stehenden Verordnungen hätten die Namen von acht Versicherten enthalten, die sich zum Zeitpunkt der Rezeptausstellung in einer substitutionsgestützten Behandlung Opiatabhängiger befunden hätten. Schwärzungen seien insofern nicht vorgenommen worden.

Letztlich hat die Krankenkasse eingeräumt, dass die Übermittlung von Versichertendaten nicht durch eine gesetzliche Befugnisnorm im Sozialgesetzbuch gestattet war. Der Mitarbeiter der Krankenkasse habe die Zulässigkeit einer Datenübermittlung nach dem Sozialgesetzbuch nicht gesondert geprüft. Er habe die Übermittlungsbefugnis lediglich aus den nicht zutreffenden Angaben der auskunftsersuchenden Stelle abgeleitet und sich darauf verlassen.

Dadurch hat die Krankenkasse gegen das Sozialgeheimnis (§ 35 Abs. 1 SGB I) verstoßen. Ich habe dies **beanstandet**. Schließlich hätten sich die Mitarbeiter der Krankenkasse nicht auf die Angaben der Stadt verlassen dürfen bzw. zumindest prüfen oder nachfragen müssen. Außerdem sollte einem Mitarbeiter einer Kran-

kenkasse bekannt sein, dass es sich bei derartigen Versichertendaten um Sozialdaten handelt mit der Folge, dass die Vorschriften der Sozialgesetzbücher und nicht die des BayDSG einschlägig sind. Ebenso zu berücksichtigen war, dass es sich bei der Verordnung von Betäubungsmitteln um Daten von höchster Sensibilität handelt. Außerdem sind von dem Verstoß mehrere Personen betroffen. Im Übrigen hat der betroffene Mitarbeiter sogar entsprechende Daten für ein weiteres Quartal „angeboten". Des Weiteren sind in relativ kurzer Zeit zwei weitere vergleichbare Fälle aufgetreten. Letztlich hat die Krankenkasse auch nur nach längerer Bearbeitungszeit und nach nochmaligem Nachfassen den Datenschutzverstoß eingeräumt.

8.17 Übermittlung von Daten durch Unfallversicherungsträger

Im Rahmen einer Eingabe wurde mir folgender Sachverhalt vorgetragen: Ein Unfallversicherungsträger habe auf Nachfrage Gesundheitsdaten des Betroffenen an eine privaten Versicherung weitergegeben.

Ich habe diesen Verstoß im Rahmen meines pflichtgemäßen Ermessens **beanstandet** (Art. 31 Abs. 1 BayDSG). Der Unfallversicherungsträger ging zwar irrtümlicherweise von falschen Voraussetzungen aus, die eine Befugnisnorm begründet hätten. Allerdings liegt ein besonders schwerer Fall eines Datenschutzverstoßes vor: Nur auf nochmalige Nachfrage hat der Unfallversicherungsträger zur Aufklärung des Sachverhalts beigetragen und letztlich den Verstoß gegen das Sozialgeheimnis eingeräumt. Des Weiteren wurde gegen das Sozialgeheimnis verstoßen. Zum anderen betraf die Übermittlung Gesundheitsdaten, also besonders sensible Daten, die eines höheren Schutzniveaus bedürfen.

8.18 Übermittlung von Daten durch Bezirk

Bereits in meinem 23. Tätigkeitsbericht habe ich mich dazu geäußert, dass auch in der Überweisung der Miete von einer ARGE direkt an einen Vermieter eine Datenübermittlung liegt, die nur zulässig ist, wenn eine solche zur Aufgabenerfüllung der ARGE erforderlich ist oder der Betroffene eingewilligt hat (siehe hierzu 23. Tätigkeitsbericht, Nr. 17.6.1).

In einem ähnlich gelagerten Fall, in dem eine Vermieterin durch einen Bezirk darüber informiert wurde, dass der schwerbehinderte Bewohner der vermieteten Wohnung vom Bezirk Unterstützungsleistungen erhält, habe ich eine **Beanstandung** ausgesprochen. Der Beanstandung lag folgender Sachverhalt zu Grunde:

Der schwerbehinderte Sohn der Petentin, die sich an mich gewandt hatte, lebt im Rahmen des sog. betreuten Einzelwohnens in einem Appartement, das seine Mutter, die zugleich seine Betreuerin ist, für ihn angemietet hatte. Die Grundsicherung für ihren Sohn erhielt die Petentin direkt vom Bezirk ebenso wie eine einmalig angefallene Restzahlung der Nebenkosten, über deren Begleichung sie mit Schreiben des Bezirks informiert wurde. Dieses Schreiben wurde allerdings auch in Abdruck an die Vermieterin der Wohnung übersandt. Dadurch wurde dieser bekannt, dass der Sohn der Petentin unter ihrer Betreuung steht und vom Bezirk Unterstützungsleistungen erhält.

Da weder die Petentin noch ihr Sohn in diese Datenübermittlung eingewilligt haben und auch keine gesetzliche Befugnis für die Datenübermittlung ersichtlich

war, lag ein nicht unerheblicher Verstoß gegen datenschutzrechtliche Vorschriften vor. Angesichts des Verfahrensverlaufs war zudem nicht auszuschließen, dass der Verstoß zu nicht rückgängig zu machenden Nachteilen für den Sohn der Petentin führen würde. Deshalb war die Verletzung des Sozialgeheimnisses durch den Bezirk zu beanstanden.

9 Steuer- und Finanzverwaltung

9.1 ELStAM – Elektronische Lohnsteuerabzugsmerkmale

Schon im 23. Tätigkeitsbericht, Nr. 11.1.3, und im 24. Tätigkeitsbericht, Nr. 9.1.3, hatte ich eingehend über den durch das Jahressteuergesetz 2008 in das Einkommensteuergesetz neu eingefügten § 39 e EStG „Verfahren zur Bildung und Anwendung der elektronischen Lohnsteuerabzugsmerkmale“ berichtet. Als **Ersatz für die herkömmliche Papierlohnsteuerkarte** sollten die Elektronischen Lohnsteuerabzugsmerkmale (ELStAM) ursprünglich bereits ab dem Kalenderjahr 2011 in einer beim Bundeszentralamt für Steuern errichteten zentralen Datenbank für den automatisierten Abruf durch den Arbeitgeber bereitgestellt werden. Aufgrund mehrfacher Verzögerungen soll dies nunmehr erst ab dem 01.01.2013 erfolgen.

9.1.1 Bürger-Informationsschreiben nicht immer fehlerfrei

Im Berichtszeitraum haben die Finanzämter alle Steuerbürger über die beim Bundeszentralamt für Steuern erstmals elektronisch für den Lohnsteuerabzug gespeicherten Daten schriftlich informiert. Daraufhin haben sich zahlreiche Bürger mit Eingaben an mich gewandt und dabei eine völlige oder teilweise Unrichtigkeit der in diesen Informationsschreiben genannten Daten vorgebracht. Ich habe diese Eingaben zum Anlass genommen, das Staatsministerium der Finanzen um nähere Informationen zu ersuchen.

Nach Darstellung des Finanzministeriums hätten alle Meldebehörden in einer Initialdatenlieferung bis zum 01.11.2010 den bei ihnen vorliegenden, zum Aufbau der zentralen Datenbank über die elektronischen Lohnsteuerabzugsmerkmale erforderlichen Meldedatenbestand an das Bundeszentralamt für Steuern geliefert. In der Folgezeit sei zudem im Falle von Meldedatenänderungen eine tagesaktuelle Lieferung der berichtigten Daten erfolgt. Am 01.07.2011 habe das Bundeszentralamt für Steuern den Aufbau der zentralen Datenbank schließlich abgeschlossen.

Eine erste Auswertung der Informationsschreiben durch das Finanzministerium habe ergeben, dass von den in Bayern versandten rund 6 Millionen Mitteilungsschreiben nur eine relativ geringe Anzahl fehlerbehaftet gewesen sei. So sei beispielsweise in einigen Fällen der in der zentralen Datenbank zutreffend gespeicherte Pauschbetrag für behinderte Menschen nicht in das Mitteilungsschreiben übernommen worden. Dies sei auf einen – inzwischen behobenen – Softwarefehler zurückzuführen gewesen. In der Mehrzahl der nach Angabe der betroffenen Steuerbürger fehlerhaften Mitteilungen beruhten die dort nachgewiesenen Angaben allerdings auf den von den Meldebehörden gelieferten Daten. Da die Finanzbehörden aber keine Möglichkeit hätten, Daten der Meldebehörden selbst zu prüfen und zu berichtigen, könnten sie nur die entsprechenden Fehlermeldungen an die Meldebehörden vornehmen. Die Aufklärung des Fehlergrundes könne daher – abhängig von dem jeweils zugrunde liegenden Sachverhalt – in Einzelfällen einige Zeit in Anspruch nehmen.

Die Aussagen des Staatsministeriums der Finanzen erscheinen mir nachvollziehbar. Ich gehe aber davon aus, dass bis zu der nunmehr ab dem 01.01.2013 geplanten Bereitstellung der ELStAM zum automatisierten Abruf durch den Arbeitgeber diese Probleme gelöst sein werden.

9.1.2 Datensperrung zur Abwehr von „Neugierabfragen“

Aus datenschutzrechtlicher Sicht ist es von besonderer Bedeutung, unberechtigte Abfragen aus dem zentralen ELStAM-Datenbestand zuverlässig zu verhindern.

In diesem Zusammenhang mache ich auf die Vorschrift des § 52 b Abs. 8 EStG aufmerksam. Danach kann ein Steuerbürger über das Finanzamt die **Bereitstellung der ELStAM allgemein sperren lassen bzw. nur für bestimmte Arbeitgeber freigeben** (Positivliste) **oder für bestimmte Arbeitgeber sperren lassen** (Negativliste).

§ 52 Abs. 8 EStG Übergangsregelungen bis zur Anwendung der elektronischen Lohnsteuerabzugsmerkmale
(8) [1]Das Finanzamt teilt dem Steuerpflichtigen auf Anfrage die bereitgestellten ELStAM mit. [2]Der Steuerpflichtige kann über das Finanzamt die Bereitstellung der ELStAM allgemein sperren lassen. [3]Er kann die Bereitstellung für bestimmte Arbeitgeber freigeben (Positivliste) oder sie für bestimmte Arbeitgeber sperren lassen (Negativliste). [4]Der Arbeitgeber ist verpflichtet, dem Arbeitnehmer für Zwecke der Positivliste die Steuernummer der Betriebsstätte mitzuteilen oder des Teils des Betriebs des Arbeitgebers, in dem der für die Durchführung des Lohnsteuerabzugs maßgebende Arbeitslohn des Arbeitnehmers ermittelt wird. [5]Für Zwecke der Negativliste gilt dies nur für einen Arbeitgeber, bei dem der Arbeitnehmer ab dem Kalenderjahr 2011 beschäftigt ist. [6]Werden wegen einer Sperrung nach Satz 2 oder Satz 3 für einen abrufenden Arbeitgeber keine ELStAM bereitgestellt, so wird dem Arbeitgeber die Sperrung mitgeteilt und der Arbeitgeber hat die Lohnsteuer nach Steuerklasse VI zu ermitteln.

Die beim Umgang mit der herkömmlichen Papierlohnsteuerkarte einzuhaltenden Schutzvorschriften gelten für die Verwendung der ELStAM sinngemäß. Insbesondere stellt der vorsätzliche oder leichtfertige Abruf von ELStAM für andere Zwecke als für die Durchführung des Steuerabzugs – also etwa die **„Neugierabfrage“** – eine **bußgeldbewehrte Ordnungswidrigkeit** dar (§ 39 e Abs. 4 Satz 7 i.V.m. § 39 Abs. 8 und 9 EStG).

9.2 Outsourcing im Lohnsteuerverfahren

In der Vergangenheit war ich bereits mehrfach mit Fragen des Outsourcings im Lohnsteuerverfahren befasst. In diesem Zusammenhang möchte ich nur beispielhaft auf meinen Beitrag im 18. Tätigkeitsbericht, Nr. 11.1, hinweisen, in dem ich mich aus datenschutzrechtlicher Sicht zur Vergabe des Drucks und des Versands von Lohnsteuerkarten durch Kommunen an private Dienstleister geäußert habe.

9.2.1 Lohnsteuerkarten

Früher waren die **Gemeinden** insoweit, als sie Lohnsteuerkarten auszustellen sowie Eintragungen auf den Lohnsteuerkarten vorzunehmen und zu ändern hatten, **örtliche Landesfinanzbehörden** (§ 39 Abs. 6 EStG a.F.). Im Zusammenhang mit der **Vergabe des Drucks und des Versands von Lohnsteuerkarten durch Kommunen an private Dienstleister** vertrat das Staatsministerium der Finanzen folgerichtig die Auffassung, dass die im Rahmen dieser Auftragsdatenverarbeitung im Sinne des Art. 6 BayDSG tätigen privatwirtschaftlichen Beschäftigten nach dem Verpflichtungsgesetz förmlich zu verpflichten waren, um die **Wahrung des Steuergeheimnisses nach § 30 AO** sicherzustellen und insbesondere strafrechtliche Sanktionen bei einer unzulässigen Durchbrechung des Steuergeheimnisses ergreifen zu können. Darüber hinaus hielt es das Finanzministerium für erforderlich, dass der für die Einhaltung der datenschutzrechtlichen Bestimmungen weiterhin gem. Art. 6 Abs. 1 Satz 1 BayDSG verantwortliche kommunale Auftraggeber die Wahrung des Steuergeheimnisses auch faktisch sicherstellte. In einem Merkblatt zur Ausstellung der (Papier-)Lohnsteuerkarten wurden die Kommunen entsprechend unterrichtet.

9.2.2 Lohnsteuerbescheinigungen

Auch wenn – wie unter 9.1 dargestellt – die bisherige (Papier-)Lohnsteuerkarte ab dem 01.01.2013 durch Elektronische Lohnsteuerabzugsmerkmale (ELStAM) abgelöst werden soll, ist ein Outsourcing im Rahmen der Erfüllung von lohnsteuerlichen Pflichten durch kommunale Arbeitgeber nach wie vor denkbar. Allerdings handeln die **Kommunen** insoweit in keinem Fall mehr als örtliche Landesfinanzbehörden, sondern ausschließlich **in lohnsteuerlicher Arbeitgebereigenschaft.**

So sind beispielsweise auch die kommunalen Arbeitgeber gem. § 41 b EStG verpflichtet, bei Beendigung des Dienstverhältnisses bzw. am Ende des Kalenderjahres eine elektronische Lohnsteuerbescheinigung zu erstellen. Nach Auffassung des Staatsministeriums der Finanzen richtet sich die **Geheimhaltungspflicht des Arbeitgebers im Lohnsteuerabzugsverfahren ausschließlich nach § 39 Abs. 8 EStG**: danach darf der Arbeitgeber die Lohnsteuerabzugsmerkmale nur für die Einbehaltung der Lohn- und Kirchensteuer verwenden; er darf sie ohne Zustimmung des Arbeitnehmers nur offenbaren, soweit dies gesetzlich zugelassen ist.

§ 39 Abs. 8 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.

Nach Ansicht des Staatsministeriums der Finanzen ist bei einer **Vergabe des Drucks und des Versands der elektronischen Lohnsteuerbescheinigungen durch Kommunen an private Dienstleister** daher Folgendes zu beachten:

– Da der kommunale Auftraggeber nach Art. 6 Abs. 1 BayDSG für die Einhaltung der datenschutzrechtlichen Vorschriften verantwortlich bleibt, sind bei einem Outsourcing im Lohnsteuerverfahren die **Beschäftigten des privaten Auftragnehmers** – über die **Verpflichtung auf das Datenge-**

heimnis gem. § 5 BDSG hinaus – auch auf die Einhaltung des Offenbarungsverbots nach § 39 Abs. 8 EStG vertraglich zu verpflichten.

§ 5 BDSG Datengeheimnis
[1]Den bei der Datenverarbeitung beschäftigten Personen ist untersagt, personenbezogene Daten unbefugt zu erheben, zu verarbeiten oder zu nutzen (Datengeheimnis). [2]Diese Personen sind, soweit sie bei nichtöffentlichen Stellen beschäftigt werden, bei der Aufnahme ihrer Tätigkeit auf das Datengeheimnis zu verpflichten. [3]Das Datengeheimnis besteht auch nach Beendigung ihrer Tätigkeit fort.

– Darüber hinaus müssen die weiteren von Art. 6 BayDSG für die Auftragsdatenverarbeitung aufgestellten Vorgaben eingehalten werden. Insbesondere muss vertraglich festgelegt werden, dass ausschließlich die verpflichteten Personen tätig werden. Ein Tätigwerden von Subunternehmern und nicht verpflichtetem Personal ist durch Aufnahme entsprechender Bedingungen bei der Beauftragung des privaten Unternehmens auszuschließen.

– Nach Art. 6 Abs. 2 Satz 3 BayDSG hat sich der Auftraggeber – soweit erforderlich – von der Einhaltung der getroffenen technischen und organisatorischen Maßnahmen beim Auftragnehmer zu überzeugen. Vor diesem Hintergrund muss der Auftraggeber die Wahrung des Offenbarungsverbots auch faktisch sicherstellen. Die Übermittlung von Daten auf elektronischem Weg ist daher nur zulässig, wenn sichergestellt ist, dass ein unberechtigter Datenzugriff nicht erfolgen kann; elektronisch übermittelte Steuerdaten sind nach dem Stand der Technik zu verschlüsseln. Insoweit ist das beauftragte Unternehmen ausdrücklich auf § 39 Abs. 8 EStG hinzuweisen.

Aus datenschutzrechtlicher Sicht sehe ich keine Veranlassung, der Rechtsauffassung des Staatsministeriums der Finanzen entgegen zu treten. Ich würde es aber nach wie vor begrüßen, wenn sowohl der zulässige Umfang als auch die im Einzelnen zu beachtenden Maßgaben bei einem Outsourcing im Lohnsteuerverfahren gesetzlich festgelegt würden.

9.3 Datenschutzrechtliche Freigabe des Verfahrens ELSTER

Auch für kommunale Arbeitgeber besteht nach §§ 41 a, 41 b EStG die gesetzliche Verpflichtung, Lohnsteuer-Anmeldungen und Lohnsteuerbescheinigungsdaten elektronisch an die Steuerverwaltung zu übermitteln. In diesem Zusammenhang stellt sich die Frage, ob außerstaatliche bayerische öffentliche Stellen für die diesbezügliche Verwendung von Teilen des Verfahrens ELSTER ein eigenständiges datenschutzrechtliches Freigabeverfahren durchführen müssen.

Zwar kann im staatlichen Bereich ein fachlich zuständiges Staatsministerium im Einvernehmen mit den betroffenen Ressorts gem. Art. 26 Abs. 1 Satz 2 Halbsatz 2 BayDSG eine landesweite Freigabe für Verfahren erteilen, die auch in öffentlichen Stellen anderer Ressorts eingesetzt werden sollen. Bei unveränderter Übernahme dieser Verfahren sind dann weitere Freigaben durch die einsetzenden staatlichen bayerischen öffentlichen Stellen entbehrlich. Offen ist jedoch,

welche Folgen eine landesweite Freigabe für **außerstaatliche** bayerische öffentliche Stellen – wie hier bayerische Kommunen – hat.

Auf meine entsprechende Anfrage hin hat sich das im vorliegenden Zusammenhang zuständige **Staatsministerium der Finanzen** im Verlauf einer längeren Diskussion schließlich auf **folgenden Standpunkt** gestellt:

– Das eigentliche Verfahren ELSTER – bestehend aus einer Clientkomponente, einer Einsatzkomponente in den ELSTER-Clearingstellen und einer Komponente, die in den Rechenzentren der Länder-Finanzverwaltungen Verwendung findet – setzt frühestens beim Empfang der Daten in den Clearingstellen an. Das gilt in dem in Rede stehenden Zusammenhang beispielsweise auch bei der Verwendung des Verfahrens ELSTERLohn I, d.h. der elektronischen Übermittlung von Lohnsteuerbescheinigungsdaten über das Portal **ELSTEROnline**.

  Andere öffentliche Stellen außerhalb der Steuerverwaltung setzen diese Verfahren damit nach Auffassung des Finanzministeriums nicht selbst im Sinne des Art. 26 Abs. 1 BayDSG ein. Die Datenverarbeitung erfolgt ab Übergabe ausschließlich im Machtbereich der Steuerverwaltung mit der Folge, dass eine **datenschutzrechtliche Freigabe nur durch einen behördlichen Datenschutzbeauftragten der Steuerverwaltung** erfolgen kann und muss.

– Anders verhält es sich mit dem Verfahren **ELSTERFormular.** Mit diesem Freewareprogramm der Steuerverwaltung können Steuererklärungen und Steuervoranmeldungen am PC ausgefüllt und die Daten anschließend elektronisch an die Steuerverwaltung übermittelt werden. ELSTERFormular steht damit gleichwertig neben anderen (kommerziellen) Produkten privatwirtschaftlicher Anbieter und betrifft den Datenstrom vom Anwender bis zu den Clearingstellen.

  Verantwortlich für den Verfahrenseinsatz im datenschutzrechtlichen Sinne ist damit der jeweilige Anwender. Im vorliegenden Zusammenhang hat dies zur Folge, dass **außerstaatliche bayerische öffentliche Stellen den Einsatz von ELSTERFormular** oder eines entsprechenden Softwareprodukts nach Art. 26 Abs. 1 BayDSG **selbst datenschutzrechtlich freigeben** müssen.

Die Auffassung des Staatsministeriums der Finanzen erscheint mir nachvollziehbar. Der vom Finanzministerium dargestellten Rechtsansicht bin ich daher **nicht entgegen getreten.**

9.4 Erhebung der Kirchensteuer auf Kapitalerträge

Mit dem Unternehmensteuerreformgesetz 2008 hat der Bundesgesetzgeber eine **Abgeltungssteuer auf private Kapitalerträge** eingeführt. Seit dem 01.01.2009 werden diese Einkünfte einheitlich mit einem Steuersatz von 25 v.H. besteuert.

Zur Entrichtung der auf die Kapitalerträge anfallenden **Kirchensteuer** räumte das Gesetz den betroffenen Steuerbürgern ein **Wahlrecht** ein. Zum Einen bestand die Möglichkeit, von der auszahlenden Stelle – im Regelfall dem Kreditin-

stitut – auch die Kirchensteuer einbehalten zu lassen; dazu musste der Steuerpflichtige der auszahlenden Stelle seine Religionszugehörigkeit mitteilen (§ 51 a Abs. 2 c EStG a.F.). Zum Anderen hatten die betroffenen Steuerbürger die Möglichkeit, auf die Angabe der Religionszugehörigkeit gegenüber der auszahlenden Stelle zu verzichten, dann aber beim Finanzamt eine entsprechende Steuererklärung zur individuellen Kirchensteuerveranlagung abzugeben (§ 51 a Abs. 2 d EStG). Der Gesetzgeber bestimmte in § 51 a Abs. 2 e EStG a.F. weiterhin, dass die Auswirkungen der geschilderten Wahlmöglichkeit zu evaluieren seien und die Bundesregierung den Bundestag bis spätestens zum 30.06.2010 über das Ergebnis der Evaluierung zu unterrichten habe. In Anbetracht des bereits im Gesetzestext ausdrücklich vorgegebenen Ziels, auch bei der Erhebung der auf die Kapitalerträge anfallenden Kirchensteuer einen umfassenden verpflichtenden Quellensteuerabzug vorzunehmen, habe ich bereits in meinem 23. Tätigkeitsbericht, Nr. 11.1.3, eine ergebnisoffene Evaluierung für mehr als fraglich gehalten.

Den geforderten **Evaluationsbericht** hat die Bundesregierung am 01.09.2010 beschlossen und sodann dem Bundestag übermittelt. Wie zu erwarten war, wurde in dem Bericht ein umfassender Abzug der Kirchensteuer auf Kapitalerträge an der Quelle unter verpflichtender Bekanntgabe der Religionszugehörigkeit gegenüber der auszahlenden Stelle befürwortet. Die Ermittlung der Religionszugehörigkeit des jeweils betroffenen Steuerpflichtigen sollte dabei im Wege eines automatisierten Abrufs des entsprechenden Religionsschlüssels durch die auszahlende Stelle aus der beim Bundeszentralamt für Steuern geführten zentralen Steuerdatei erfolgen.

In langwierigen Verhandlungen konnten die Datenschutzbeauftragten des Bundes und der Länder allerdings erreichen, dass Steuerbürgern, die ein Bekanntwerden ihrer Religionszugehörigkeit bei der auszahlenden Stelle nicht wünschen, ein **Widerspruchsrecht** eingeräumt wird. Dazu bestimmt § 51 a Abs. 2 c Satz 1 Nr. 3 und Abs. 2 e EStG nunmehr, dass die auszahlende Stelle den Steuerbürger auf die bevorstehende Abfrage seiner Religionszugehörigkeit und das in diesem Zusammenhang bestehende Widerspruchsrecht gegenüber dem Bundeszentralamt für Steuern schriftlich oder in anderer geeigneter Form hinzuweisen hat. Der Hinweis hat dabei individuell zu erfolgen; ein bloßer Verweis – etwa auf Allgemeine Geschäftsbedingungen – ist nicht ausreichend. Gehört der betroffene Steuerbürger keiner Steuer erhebenden Religionsgemeinschaft an oder hat er dem Abruf von Daten zur Religionszugehörigkeit widersprochen (Sperrvermerk), so teilt das Bundeszentralamt für Steuern der anfragenden auszahlenden Stelle lediglich einen neutralen Wert (Nullwert) mit. Der auszahlenden Stelle wird damit nicht bekannt, ob der betroffene Steuerbürger überhaupt keiner Religionsgemeinschaft angehört oder ob er bloß die Bekanntgabe seiner gespeicherten Religionszugehörigkeit nicht wünscht. Mit diesem Verfahren wird insbesondere die Wahrung der verfassungsrechtlich in Art. 4 GG gewährleisteten sogenannten **„negativen Religionsfreiheit“** – also des Grundrechts auf Verschweigen der (Nicht-)Zugehörigkeit zu einer Religionsgemeinschaft – sichergestellt. Konsequenterweise verpflichtet die Eintragung eines Sperrvermerks den einer Steuer erhebenden Religionsgemeinschaft angehörigen Steuerbürger aber zur Abgabe einer Steuererklärung für die Kirchensteuerveranlagung. Vor diesem Hintergrund hat das Bundeszentralamt für Steuern das Bestehen eines Sperrvermerks dem für den Kirchensteuerpflichtigen zuständigen Wohnsitz-Finanzamt bzw. -Kirchensteueramt mitzuteilen, das diesen sodann zur Abgabe einer Steuererklärung auffordern muss. Dieses Verfahren ist erstmals auf nach dem 31.12.2013 zufließende Kapitalerträge anzuwenden.

Aus datenschutzrechtlicher Sicht wäre eine Weitergeltung des derzeit noch bestehenden Wahlverfahrens sicherlich vorzugswürdig gewesen. Das ab dem 31.12.2013 geltende Verfahren stellt aber einen **hinnehmbaren Kompromiss** dar.

9.5 Fahrtenbuchauflage bei Berufsgeheimnisträgern

Immer wieder stellen mir Berufsgeheimnisträger – vor allem Ärzte und Rechtsanwälte – die Frage, ob ihnen das Finanzamt zur ertragsteuerlichen Behandlung der Nutzung betrieblicher Kraftfahrzeuge für Privatfahrten die Auflage machen kann, ein Fahrtenbuch zu führen und **in diesem Fahrtenbuch die besuchten Patienten bzw. Mandanten namentlich zu benennen.** Die diesen Eingaben zugrunde liegende Problematik betrifft das Spannungsverhältnis zwischen dem Auskunftsverweigerungsrecht bestimmter Berufsgruppen im Sinne von § 102 AO und § 203 StGB einerseits und der Mitwirkungspflicht von Steuerpflichtigen im Besteuerungsverfahren gem. § 90 AO (allgemein) und gem. § 200 AO (bei Außenprüfungen) andererseits.

§ 90 Abs. 1 AO Mitwirkungspflichten der Beteiligten
(1) [1]Die Beteiligten sind zur Mitwirkung bei der Ermittlung des Sachverhalts verpflichtet. [2]Sie kommen der Mitwirkungspflicht insbesondere dadurch nach, dass sie die für die Besteuerung erheblichen Tatsachen vollständig und wahrheitsgemäß offenlegen und die ihnen bekannten Beweismittel angeben. [3]Der Umfang dieser Pflichten richtet sich nach den Umständen des Einzelfalls.

§ 200 Abs. 1 AO Mitwirkungspflichten des Steuerpflichtigen
(1) [1]Der Steuerpflichtige hat bei der Feststellung der Sachverhalte, die für die Besteuerung erheblich sein können, mitzuwirken. [2]Er hat insbesondere Auskünfte zu erteilen, Aufzeichnungen, Bücher, Geschäftspapiere und andere Urkunden zur Einsicht und Prüfung vorzulegen, die zum Verständnis der Aufzeichnungen erforderlichen Erläuterungen zu geben und die Finanzbehörde bei Ausübung ihrer Befugnisse nach § 147 Abs. 6 zu unterstützen. [3]Sind der Steuerpflichtige oder die von ihm benannten Personen nicht in der Lage, Auskünfte zu erteilen, oder sind die Auskünfte zur Klärung des Sachverhalts unzureichend oder versprechen Auskünfte des Steuerpflichtigen keinen Erfolg, so kann der Außenprüfer auch andere Betriebsangehörige um Auskunft ersuchen. [4]§ 93 Abs. 2 Satz 2 und § 97 Abs. 2 gelten nicht.

Zu dieser Problematik nehme ich aus datenschutzrechtlicher Sicht wie folgt Stellung:

– Mit der Frage des Auskunftsverweigerungsrechts der in § 102 AO genannten Berufsgeheimnisträger hat sich der **Bundesfinanzhof** bisher vor allem im Zusammenhang mit Außenprüfungen von Finanzämtern befasst. So ist nach ständiger Rechtsprechung des Bundesfinanzhofs auch bei Angehörigen eines Berufs, denen ein Auskunftsverweigerungsrecht als Berufsgeheimnisträger zusteht, eine **Betriebsprüfung zulässig** (vgl. beispielhaft das Urteil des Bundesfinanzhofs vom 08.04.2008, Az.: VIII R 61/06). Die grundsätzlichen Mitwirkungspflichten des Steuerpflichtigen bei einer Außenprüfung ergeben sich aus § 200 AO: danach sind u.a. Aufzeichnungen, Bücher, Geschäftspapiere und andere Urkunden zur Einsicht und Prüfung vorzulegen. Aus Gründen der Gleichbehandlung aller Steuerpflichtigen und der Gleichmäßigkeit der Besteuerung **ob-**

liegen diese Mitwirkungspflichten auch den Berufsgeheimnisträgern, denen ein Auskunftsverweigerungsrecht nach § 102 AO zusteht. Der Bundesfinanzhof führt in dem genannten Urteil insoweit aus: „Diese Handhabung wird nicht zuletzt durch das Gebot einer gleichmäßigen Besteuerung (§ 85 AO) gerechtfertigt, dessen Befolgung beeinträchtigt werden könnte, wenn sich Angehörige bestimmter Berufsgruppen unter Berufung auf eine bestehende Verschwiegenheitspflicht generell der Überprüfung ihrer im Besteuerungsverfahren gemachten Angaben entziehen könnten."

§ 102 AO Auskunftsverweigerungsrecht zum Schutz bestimmter Berufsgeheimnisse
(1) Die Auskunft können ferner verweigern:
1. Geistliche über das, was ihnen in ihrer Eigenschaft als Seelsorger anvertraut worden oder bekannt geworden ist,
2. Mitglieder des Bundestages, eines Landtages oder einer zweiten Kammer über Personen, die ihnen in ihrer Eigenschaft als Mitglieder dieser Organe oder denen sie in dieser Eigenschaft Tatsachen anvertraut haben, sowie über diese Tatsachen selbst,
3. a) Verteidiger,
b) Rechtsanwälte, Patentanwälte, Notare, Steuerberater, Wirtschaftsprüfer, Steuerbevollmächtigte, vereidigte Buchprüfer,
c) Ärzte, Zahnärzte, Psychologische Psychotherapeuten, Kinder- und Jugendlichenpsychotherapeuten, Apotheker und Hebammen,
über das, was ihnen in dieser Eigenschaft anvertraut worden oder bekannt geworden ist,
4. Personen, die bei der Vorbereitung, Herstellung oder Verbreitung von periodischen Druckwerken oder Rundfunksendungen berufsmäßig mitwirken oder mitgewirkt haben, über die Person des Verfassers, Einsenders oder Gewährsmanns von Beiträgen und Unterlagen sowie über die ihnen im Hinblick auf ihre Tätigkeit gemachten Mitteilungen, soweit es sich um Beiträge, Unterlagen und Mitteilungen für den redaktionellen Teil handelt; § 160 bleibt unberührt.

– Das in § 102 AO gesetzlich normierte **Auskunftsverweigerungsrecht** dient dem besonderen Schutz des Vertrauensverhältnisses zwischen dem Berufsgeheimnisträger und dem Patienten bzw. Mandanten. Es besteht unabhängig von der Verpflichtung der Finanzbeamten (z.B. Betriebsprüfer) zur Wahrung des Steuergeheimnisses gem. § 30 AO. Strafrechtlich geschützt wird das Auskunftsverweigerungsrecht durch § 203 StGB: danach ist ein unbefugtes Offenbaren von persönlichen Mandanten- bzw. Patientendaten durch einen Berufsgeheimnisträger unter Strafe gestellt. Die Ausübung des Auskunftsverweigerungsrechts **kann jedoch zu steuerlichen Nachteilen für den Berufsgeheimnisträger führen,** sei es dass Betriebsausgaben nicht steuermindernd anerkannt werden, sei es dass Betriebseinnahmen im Schätzungswege ermittelt werden.

– Auch nach Auffassung der Finanzverwaltung fallen etwa die durch einen Arzt festgestellten Diagnosen und Behandlungsmethoden unter § 102 AO, § 203 StGB. Grundsätzlich gilt dies ebenso für den **Namen und** die **Adresse des Patienten bzw. Mandanten.** Die **Rechtsprechung** ist in diesem Zusammenhang allerdings **nicht einheitlich:** Einerseits hat der Bun-

desfinanzhof in seinen Urteilen vom 14.05.2002 (Az.: IX R 31/00) und 28.10.2009 (Az.: VIII R 78/05) ausdrücklich festgestellt, dass sich das Zeugnisverweigerungsrecht nach § 102 AO auch auf die Identität des Mandanten bezieht. Andererseits hat der Bundesfinanzhof in seinem Urteil vom 26.02.2004 (Az.: IV R 50/01) zur steuerlichen Geltendmachung von Bewirtungsspesen durch einen Rechtsanwalt entschieden, dass von einer konkludenten Einwilligung des bewirteten Mandanten zur Offenbarung seiner für steuerliche Zwecke des Rechtsanwalts erforderlichen persönlichen Daten – vor allem also des Namens – gegenüber den Finanzbehörden auszugehen ist und damit kein unbefugtes Offenbaren im Sinne des § 203 StGB vorliegt. Entsprechend hat der Bundesfinanzhof in der bereits erwähnten Entscheidung vom 08.04.2008 darauf abgestellt, dass diejenigen Mandanten, die in ihrer Steuererklärung kenntlich gemacht haben, dass ein Angehöriger eines steuerberatenden Berufes an der Erstellung der Steuererklärung mitgewirkt hat, auf eine Geheimhaltung ihrer Identität verzichtet haben.

– Der Bundesfinanzhof hat in seinem bereits erwähnten Urteil vom 14.05.2002 aufgezeigt, dass ein Berufsgeheimnisträger gehalten sein kann, die Vollständigkeit und Richtigkeit der geführten Bücher und Steuerunterlagen bei **Abdecken, Schwärzen usw. der geheim zu haltenden Daten** nachzuweisen.

– Im Zusammenhang mit der Führung von Fahrtenbüchern durch Ärzte haben das Bundesministerium der Finanzen und der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit bereits im Jahre 1999 nach intensiven Verhandlungen eine **Kompromisslösung** vereinbart, die die gegenständliche Problematik zwar nicht endgültig lösen, jedoch deutlich entschärfen kann. Danach reicht **im Fahrtenbuch** zu Reisezweck, Reiseziel und Reiseroute neben der Angabe des Datums, des Kilometerstands und des Zielorts grundsätzlich die **Angabe „Patientenbesuch“** aus, wenn **Name und Adresse der Patienten** vom Arzt **in einem vom Fahrtenbuch getrennt zu führenden** – und nur in besonders gelagerten Ausnahmefällen dem Finanzamt vorzulegenden – **Verzeichnis** festgehalten werden. Nähere Einzelheiten können meinem 19. Tätigkeitsbericht, Nr. 11.5, entnommen werden.

Im Zusammenhang mit dem Auskunftsverweigerungsrecht bestimmter Berufsgeheimnisträger ist **erneut ein Verfahren beim Bundesfinanzhof anhängig** (Az.: VIII R 44/09). Es bleibt zu hoffen, dass die Problematik des Auskunftsverweigerungsrechts von Berufsgeheimnisträgern im Besteuerungsverfahren endlich höchstrichterlich einer abschließenden Klärung zugeführt wird.

9.6 Fehlzustellung von Steuerbelegen

Immer wieder tragen mir Bürger in Eingaben vor, dass ihnen vom Finanzamt Steuerbelege zugeschickt worden sind, die von anderen Steuerbürgern in Erfüllung steuerlicher Pflichten beim Finanzamt eingereicht worden sind.

Die irrigerweise übermittelten Belege weisen vielfach eine **erhebliche Sensibilität** auf. Neben Bankbelegen finden sich hier oftmals auch medizinische Unterlagen, die tiefgreifende Rückschlüsse auf den gesundheitlichen Zustand anderer ermöglichen.

Ich verkenne nicht, dass im „Massengeschäft“ der Steuerveranlagung Unachtsamkeiten auftreten können. Festzuhalten ist aber, dass Fehlzustellungen von Steuerbelegen im Regelfall eine nicht unerhebliche **Verletzung des in § 30 AO normierten Steuergeheimnisses** darstellen; sie müssen daher – nicht nur aus Datenschutzsicht – weitestgehend minimiert bzw. ausgeschlossen werden.

§ 30 Abs. 1 und 2 AO Steuergeheimnis
(1) Amtsträger haben das Steuergeheimnis zu wahren.
(2) Ein Amtsträger verletzt das Steuergeheimnis, wenn er
1. Verhältnisse eines anderen, die ihm
a) in einem Verwaltungsverfahren, einem Rechnungsprüfungsverfahren oder einem gerichtlichen Verfahren in Steuersachen,
b) in einem Strafverfahren wegen einer Steuerstraftat oder einem Bußgeldverfahren wegen einer Steuerordnungswidrigkeit,
c) aus anderem Anlass durch Mitteilung einer Finanzbehörde oder durch die gesetzlich vorgeschriebene Vorlage eines Steuerbescheids oder einer Bescheinigung über die bei der Besteuerung getroffenen Feststellungen
bekannt geworden sind, oder
2. ein fremdes Betriebs- oder Geschäftsgeheimnis, das ihm in einem der in Nummer 1 genannten Verfahren bekannt geworden ist,
unbefugt offenbart oder verwertet oder
3. nach Nummer 1 oder Nummer 2 geschützte Daten im automatisierten Verfahren unbefugt abruft, wenn sie für eines der in Nummer 1 genannten Verfahren in einer Datei gespeichert sind.

Mit dem Ziel, das im Falle der Belegrückgabe vom Finanzamtssachbearbeiter heranzuziehende finanzamtsinterne Datenverarbeitungsverfahren weniger fehleranfällig zu gestalten, habe ich mich deshalb an das Staatsministerium der Finanzen gewandt. Das Finanzministerium hat mir daraufhin eine **Verfahrensweise** zum Aufruf der Schreibprogrammvorlage „Belegrückgabe“ erläutert, die geeignet ist, die Problematik **künftig wesentlich zu entschärfen.** Meiner Bitte, die Sachbearbeiterinnen und Sachbearbeiter in allen bayerischen Finanzbehörden zeitnah auf diese Verfahrensweise hinzuweisen, ist das Landesamt für Steuern im Auftrag des Staatsministeriums der Finanzen unverzüglich nachgekommen.

Ich hoffe, dass die gefundene Lösung künftig die Anzahl der Fehlzustellungen von Steuerbelegen deutlich verringern wird.

9.7 Telefonische Auskunftserteilung in Steuerangelegenheiten

Nach § 30 Abs. 1 AO haben Amtsträger das Steuergeheimnis zu wahren. § 30 Abs. 4 AO regelt abschließend die zulässigen Offenbarungsgründe. Eine nicht zulässige Offenbarung und damit eine **Verletzung des Steuergeheimnisses ist gem. § 355 StGB strafbewehrt**. Die Vorschrift des § 30 AO gilt für alle Steuern im Sinne des § 1 AO; dazu zählen etwa die Einkommensteuer und die Umsatzsteuer, aber auch die von den Gemeinden erhobenen Realsteuern (Grundsteuer und Gewerbesteuer). Für die übrigen kommunalen Steuern erklärt Art. 13 Kommunalabgabengesetz die Vorschrift des § 30 AO grundsätzlich ebenfalls für anwendbar. Der Wahrung des Steuergeheimnisses kommt damit eine hohe Bedeutung zu.

§ 355 Abs. 1 StGB Verletzung des Steuergeheimnisses
(1) Wer unbefugt
1. Verhältnisse eines anderen, die ihm als Amtsträger
a) in einem Verwaltungsverfahren oder einem gerichtlichen Verfahren in Steuersachen,
b) in einem Strafverfahren wegen einer Steuerstraftat oder in einem Bußgeldverfahren wegen einer Steuerordnungswidrigkeit,
c) aus anderem Anlaß durch Mitteilung einer Finanzbehörde oder durch die gesetzlich vorgeschriebene Vorlage eines Steuerbescheids oder einer Bescheinigung über die bei der Besteuerung getroffenen Feststellungen
bekanntgeworden sind, oder
2. ein fremdes Betriebs- oder Geschäftsgeheimnis, das ihm als Amtsträger in einem der in Nummer 1 genannten Verfahren bekanntgeworden ist,
offenbart oder verwertet, wird mit Freiheitsstrafe bis zu zwei Jahren oder mit Geldstrafe bestraft.

Durch das Steuerverkürzungsbekämpfungsgesetz vom 19.12.2001 wurde ein leistender Unternehmer verpflichtet, in allen nach dem 30.06.2002 ausgestellten Rechnungen die ihm vom Finanzamt erteilte Steuernummer oder die ihm vom Bundeszentralamt für Steuern erteilte Umsatzsteuer-Identifikationsnummer anzugeben (§ 14 Abs. 4 Satz 1 Nr. 2 UStG). **Auch vor diesem Hintergrund rate ich allen bayerischen öffentlichen Stellen dringend davon ab, telefonische Auskünfte in Steuerangelegenheiten allein aufgrund der Angabe des Namens bzw. der Firma und der Steuernummer bzw. der Umsatzsteuer-Identifikationsnummer zu erteilen.** Vielmehr hat der Anrufer durch zusätzliche Angaben glaubhaft zu machen, dass er tatsächlich berechtigt ist, die telefonisch erbetene Auskunft zu erhalten. Dabei sollte es sich um Angaben handeln, die nur der Steuerpflichtige selbst oder sein steuerlicher Vertreter machen können. Welche Angaben zur Überprüfung der Befugnis zur Auskunftserteilung geeignet sind, richtet sich stets nach den Umständen des Einzelfalls. **In vielen Fällen kann auch ein Rückruf in Aussicht gestellt werden;** dann ist die angegebene Rufnummer mit der sich aus den Steuerakten bzw. aus dem Fernsprechverzeichnis ergebenden Rufnummer zu vergleichen. Insgesamt empfehle ich allen bayerischen öffentlichen Stellen, ihre mit steuerlichen Angelegenheiten betrauten Bediensteten eingehend – unter Umständen auch wiederkehrend – insoweit zu sensibilisieren. In Anbetracht der nicht unerheblichen Strafandrohung des § 355 StGB **rate ich im Hinblick auf eine telefonische Auskunftserteilung in Steuerangelegenheiten generell zur Zurückhaltung.**

Die für die telefonische Auskunftserteilung aufgezeigten Maßstäbe sind **entsprechend auch bei der Übermittlung von steuerlichen Kontoauszügen oder von Bescheidkopien zu beachten.**

9.8 Protokollierung des Abrufs von Steuerdaten

Der **unbefugte automatisierte Abruf von Steuerdaten** durch Bedienstete der Steuerverwaltung stellt eine **Verletzung des in § 30 AO gesetzlich verankerten Steuergeheimnisses** dar. Eine Befugnis zum Datenabruf ergibt sich in erster Linie aus dem finanzbehördeninternen Geschäftsverteilungsplan. Allerdings erweist sich in der Praxis eine passgenaue technische Beschränkung der Zugriffsrechte jedes Finanzamtsbediensteten auf die für den jeweiligen Aufgabenbereich erforderlichen Steuerdaten oftmals als schwierig: nur beispielhaft sei hier

auf die bei allen bayerischen Finanzämtern eingerichteten Servicezentren oder auf bestimmte Organisationseinheiten der Außenprüfungsdienste hingewiesen.

Vor diesem Hintergrund sieht § 6 Steuerdaten-Abrufverordnung (StDAV) eine **automatisierte Protokollierung** derartiger Abrufe vor. § 7 StDAV schreibt zudem eine – zumindest stichprobenartige – **Prüfung der Zulässigkeit der Datenabrufe** vor.

§ 6 StDAV Aufzeichnung der Abrufe
(1) [1]Abrufe und Abrufversuche sind zur Prüfung der Zulässigkeit der Abrufe automatisiert aufzuzeichnen. [2]Die Aufzeichnungen umfassen mindestens die Benutzerkennung, das Datum, die Uhrzeit sowie die sonstigen zur Prüfung der Zulässigkeit der Abrufe erforderlichen Daten.
(2) [1]Die Aufzeichnungspflicht entfällt, soweit die Abrufbefugnis durch technische Maßnahmen auf die Daten oder Arten von Daten beschränkt worden ist, die zur Erledigung der jeweiligen Aufgabe erforderlich sind. [2]Unbeschadet des Satzes 1 können Aufzeichnungen anlassbezogen durchgeführt werden.
(3) Die Aufzeichnungen dürfen nur zur Prüfung der Zulässigkeit der Abrufe verwendet werden.
(4) Die Aufzeichnungen sind zwei Jahre aufzubewahren und danach unverzüglich zu löschen.

§ 7 StDAV Prüfung der Zulässigkeit der Abrufe
[1]Anhand der Aufzeichnungen ist zeitnah und in angemessenem Umfang zu prüfen, ob der Abruf nach § 30 Abs. 6 Satz 1 der Abgabenordnung und nach dieser Verordnung zulässig war. [2]Unbeschadet des Satzes 1 können aufgezeichnete Abrufe anlassbezogen geprüft werden.

Um eine **effektive kontinuierliche Prüfung** der Zulässigkeit der automatisierten Steuerdatenabrufe vornehmen zu können, sollte der Auswahlabstand aus meiner Sicht so festgelegt werden, dass die Wahrung des Steuergeheimnisses mit akzeptablem Aufwand sichergestellt werden kann. Eine bloße Erhöhung der zu prüfenden Fallzahlen ist meiner Erfahrung nach nicht zwangsläufig Ziel führend, sondern bringt in Anbetracht der ohnehin schon hohen Arbeitsbelastung der zusätzlich mit der Prüfaufgabe betrauten Finanzbeamten oftmals Abstriche bei der Prüfungsintensität mit sich.

Bei meinen datenschutzrechtlichen Außenprüfungen von Organisationseinheiten bayerischer Finanzämter habe ich stets ein besonderes Augenmerk auf die Protokollierung und Auswertung der Steuerdatenabrufe gelegt. Nach meinem Eindruck wurden die Vorgaben der Steuerdaten-Abrufverordnung von den Finanzämtern im Allgemeinen angemessen umgesetzt. Als förderlich hat es sich dabei immer wieder erwiesen, wenn Amtsleitungen die **Protokollierung und Auswertung der Steuerdatenabrufe** – ggf. wiederkehrend – **zum Gegenstand von finanzamtsinternen Besprechungen** gemacht haben.

9.9 Elektronisches Abrufverfahren ZEUGE

Seit 2007 wird das von der Finanzverwaltung des Freistaates Sachsen entwickelte elektronische Abrufverfahren ZEUGE (ZStV/BZR-Ermittlungs-Unterstützung auf der Grundlage von EOSS) auch von bayerischen Finanzämtern eingesetzt. Durch dieses Verfahren werden die in steuerstrafrechtlichen Angelegenheiten den Staatsanwaltschaften bzw. der Polizei gleichgestellten finanzamtlichen Buß-

geld- und Strafsachenstellen bzw. Steuerfahndungsstellen an das Zentrale Staatsanwaltschaftliche Verfahrensregister (ZStV) und an das Bundeszentralregister (BZR) elektronisch angebunden. Das Verfahren bietet der Finanzverwaltung allerdings keinen Online-Zugriff auf die genannten bundesweiten Register, sondern eröffnet den Finanzämtern nur die Möglichkeit, elektronisch Auskunftsanfragen zu stellen, die dann elektronisch beantwortet werden. Umgekehrt kommen die Finanzämter über ZEUGE ihren Verpflichtungen aufgrund des Verbrechensbekämpfungsgesetzes nach, bestimmte Informationen über ihre steuerstrafrechtlichen Ermittlungen in das ZStV einzustellen. Das elektronische Abrufverfahren ZEUGE verfolgt somit nicht nur das **Ziel, die steuerstrafrechtlichen Ermittlungstätigkeiten der Finanzämter durch Nutzung des ZStV und des BZR zu verbessern,** sondern dient auch dazu, **den bundesweiten Datenbestand des ZStV um steuerstrafrechtlich relevante Informationen der Finanzämter zu erweitern.**

Im Berichtszeitraum habe ich den praktischen **Einsatz des Verfahrens ZEUGE bei einem bayerischen Finanzamt datenschutzrechtlich überprüft.** Gegenstand der Prüfung waren u.a. die Vergabe der Zugriffsberechtigungen, die Protokollierung der Anfragen und die Auswertung der Protokolle. Im Wesentlichen habe ich dabei Folgendes festgestellt:

– Im Rahmen des Verfahrens ZEUGE werden die **Zugriffsberechtigungen an die Bediensteten** über Einzelschlüssel vergeben. Zugriffe können hier lesend, verändernd oder ausführend erfolgen.

  Die Vergabe der Zugriffsberechtigungen habe ich stichprobenartig überprüft. Die dabei aufgetretenen Unklarheiten wurden mit dem betroffenen Finanzamt diskutiert und anschließend bereinigt. Grundlegende datenschutzrechtliche Bedenken ergaben sich allerdings nicht.

– Im Zusammenhang mit den dargestellten Zugriffsberechtigungen habe ich auch das Problem der etwaigen Vornahme sogenannter **„Neugierabfragen“** thematisiert. Vom geprüften Finanzamt wurde mir dargelegt, dass sämtliche Anfragen über das Verfahren ZEUGE automatisiert protokolliert werden. Daraufhin habe ich mir exemplarisch eine Liste mit **Protokolldaten getätigter Abrufe** vorlegen lassen.

  Aufgrund einer Verfügung des Landesamts für Steuern haben die Hauptsachgebietsleiter Bußgeld- und Strafsachenstelle sowie Steuerfahndungsstelle je für ihr Aufgabengebiet die Zulässigkeit der getätigten Abrufe stichprobenweise zu überprüfen. Die Mitarbeiter der betroffenen Organisationseinheiten sind über diese Kontrollmaßnahmen informiert.

  Größere Probleme haben sich nach Auskunft des Finanzamts in der Vergangenheit dabei nicht ergeben. Bei einer Durchsicht der vorgelegten Protokolldaten konnte ich ebenfalls keine Auffälligkeiten feststellen.

– Im Zuge der Prüfung stellte sich allerdings heraus, dass mittels des Verfahrens ZEUGE nicht nur Anfragen an das ZStV und das BZR, sondern auch an einen – vergleichsweise weniger Informationen enthaltenden – sogenannten **„Landesdatenbestand“** gerichtet werden. Bei der Prüfung konnte vor Ort jedoch nicht abschließend geklärt werden, warum innerhalb des Verfahrens ZEUGE parallel zum ZStV ein separater „Landesdatenbestand“ eingerichtet wurde.

Im Zuge meiner anschließenden Diskussion mit dem für das Verfahren ZEUGE innerhalb der bayerischen Finanzverwaltung federführenden Landesamt für Steuern ergab sich, dass der „Landesdatenbestand“ alle von den bayerischen Finanzämtern dem ZStV gemeldeten Fälle enthält. Die Einrichtung des „Landesdatenbestands“ war – so die Auskunft des Landesamts für Steuern – notwendig geworden, da das ZStV gegen gleiche oder ähnliche Personen bei der anfragenden „Behörde“ anhängige Verfahren nicht beauskunftet, der Begriff „Behörde“ nach der programmtechnischen Umsetzung des Verfahrens ZEUGE aber nicht nur das anfragende Finanzamt, sondern die gesamte Finanzverwaltung eines Landes umfasst.

Zudem stellte sich in datenschutzrechtlicher Hinsicht heraus, dass Anfragen an den „Landesdatenbestand“ nicht protokolliert und damit auch nicht ausgewertet werden. Des Weiteren ergab sich, dass die datenschutzrechtlich notwendigen Löschungen im „Landesdatenbestand“ nicht maschinell erfolgen, sondern vom jeweiligen Bearbeiter manuell angestoßen werden müssen.

Aus all diesen Gründen habe ich die vorgefundene Einrichtung des „Landesdatenbestands“ im Verfahren ZEUGE gegenüber dem Landesamt für Steuern kritisch bewertet.

Unter Einbeziehung des Programmierstandorts Sachsen konnte das Landesamt für Steuern in der Folge erreichen, dass ab April 2012 auch die eigenen Fälle der anfragenden „Behörde“ in die Auskunft des ZStV einbezogen werden. Der „Landesdatenbestand“ dient jetzt im Wesentlichen nurmehr dazu, dem jeweils berechtigten Finanzamtsbediensteten zur Erstellung von Folgemitteilungen an das ZStV den Zugriff auf die von ihm erstellten Erstmitteilungen zu ermöglichen. Damit kann der jeweilige Bearbeiter innerhalb des „Landesdatenbestandes“ nur noch auf die von ihm selbst erstellten Fälle zugreifen. Nach Auskunft des Landesamts für Steuern ist allerdings ein manuelles Löschen im „Landesdatenbestand“ auch weiterhin erforderlich.

Im Ergebnis konnten so aufgrund meiner Prüfung **wesentliche datenschutzrechtliche Verbesserungen – mit teilweise bundesweiter Auswirkung – im elektronischen Abrufverfahren ZEUGE erreicht** werden.

9.10 Erhebung der Kurtaxe in bayerischen Staatsbädern

Art. 24 Kostengesetz (KG) eröffnet die Möglichkeit, für die Bereitstellung von Kureinrichtungen eine Kurtaxe zugunsten der bayerischen Staatsbäder zu erheben. Von dieser Möglichkeit hat das Staatsministerium der Finanzen durch Erlass der „Verordnung über die Erhebung der Kurtaxe in den bayerischen Staatsbädern Bad Reichenhall, Bad Steben, Bad Kissingen, Bad Brückenau und Bad Bocklet (Kurtaxordnung für die bayerischen Staatsbäder)“ – im Folgenden Kurtaxordnung – Gebrauch gemacht. Bei der **Kurtaxe** handelt es sich um einen **öffentlich-rechtlichen Beitrag, der personenbezogen erhoben wird.** Kurtaxpflichtig ist, wer im Kurbezirk Unterkunft nimmt, ohne dort seine Wohnung oder seinen ständigen Aufenthalt zu haben. Die **Erhebungsberechtigung** kann **auf**

juristische Personen des Privatrechts übertragen werden; in der Kurtaxordnung ist dies für die meisten Staatsbäder vorgesehen.

Art. 24 Abs. 1 KG Kurtaxe
(1) [1]Für die Bereitstellung von Einrichtungen, die in den Staatsbädern festgesetzt und zu Kurzwecken unterhalten werden, kann auf Grund einer Kurtaxordnung eine Kurtaxe zugunsten der Staatsbäder erhoben werden. [2]Das Verfahren zur Festsetzung und Erhebung der Kurtaxe kann auf juristische Personen des Privatrechts übertragen werden. [3]Die Kurtaxen dürfen höchstens so bemessen sein, daß die einmaligen und laufenden Aufwendungen für die Einrichtungen gedeckt werden können. [4]Sind die Vorteile, die den Abgabeschuldnern aus den Einrichtungen erwachsen können, verschieden groß, so ist das durch entsprechende Abstufung der Abgabenhöhe zu berücksichtigen.

Im Berichtszeitraum war ich mit zahlreichen Problemen im Zusammenhang mit der Erhebung der Kurtaxe befasst, von denen ich nur folgende herausgreifen möchte:

9.10.1 Umfang der zu übermittelnden personenbezogenen Daten

Das Verfahren zur Erhebung der Kurtaxe ist im Einzelnen in der Kurtaxordnung geregelt. Danach ist jede kurtaxpflichtige Person verpflichtet, unverzüglich nach ihrem Eintreffen im Kurbezirk gegenüber dem Vermieter oder seinem Beauftragten bzw. der Erhebungsberechtigten alle Angaben zu machen, die zur Festsetzung und Erhebung der Kurtaxe erforderlich sind (§ 6 Satz 1 Kurtaxordnung). Der konkrete Umfang dieser Daten war bislang jedoch weder in der Kurtaxordnung noch im Kostengesetz bestimmt. Dies führte bei den Beherbergungsbetrieben zu Unsicherheiten darüber, welche Daten ihrer Gäste an die staatliche Kurverwaltung bzw. die entsprechende privatrechtliche Erhebungsberechtigte weitergegeben werden dürfen.

Diese rechtlichen Unsicherheiten wurden durch Einfügung eines neuen Art. 24 Abs. 2 Satz 2 KG im Zuge des Haushaltsgesetzes 2011/2012 mit Wirkung zum 01.05.2011 beseitigt. Danach hat der Schuldner der Kurtaxe den Vor- und Familiennamen, das Geburtsdatum und die Anschrift an die Erhebungsberechtigte mitzuteilen und sich auf Verlangen durch Personalausweis oder Pass auszuweisen; andere als die hier genannten Daten dürfen nicht erhoben werden. Ich begrüße, dass nunmehr eine sichere und abschließende gesetzliche Grundlage für die Erhebung personenbezogener Gästedaten durch die Erhebungsberechtigte geschaffen wurde.

Für Personen, die in Krankenhäusern und Rehabilitationskliniken aufgenommen sind, ist in der Kurtaxordnung keine Ausnahme von der Kurtaxpflicht vorgesehen. Die in Art. 25 MeldeG geregelte Ausnahme von der Meldepflicht dient lediglich melderechtlichen Zwecken und lässt die im Rahmen des Vollzugs der Kurtaxordnung vorgesehenen Meldepflichten unberührt. Auch für diese Personen müssen daher die in Art. 24 Abs. 2 Satz 2 KG genannten Daten an die Erhebungsberechtigten mitgeteilt werden. Die abschließende gesetzliche Aufzählung stellt jedoch sicher, dass in diesem Zusammenhang keinesfalls sensible Daten, insbesondere Gesundheitsdaten, erhoben werden dürfen.

Art. 24 Abs. 2 KG Kurtaxe
(2) [1]Schuldner der Kurtaxe ist, wer im Kurbezirk Unterkunft nimmt oder Kureinrichtungen oder -veranstaltungen der Staatsbäder in Anspruch nimmt, ohne dort seine Hauptwohnung im Sinn des Melderechts oder seinen ständigen Aufenthalt zu haben. [2]Er hat der Erhebungsberechtigten nach Abs. 1 Sätze 1 und 2 den Vor- und Familiennamen, das Geburtsdatum und die Anschrift mitzuteilen und sich auf Verlangen durch Personalausweis oder Pass auszuweisen. [3]Inhaber von Zweitwohnungen können verpflichtet werden, der Erhebungsberechtigten nach Abs. 1 Sätze 1 und 2 über die Benutzung der Zweitwohnung Auskunft zu geben. [4]Für die Inhaber von Zweitwohnungen kann in der Kurtaxordnung eine pauschale Abgeltung der Kurtaxe vorgeschrieben werden, die sich an der durchschnittlichen Aufenthaltsdauer der Zweitwohnungsinhaber im jeweiligen Staatsbad zu orientieren hat. [5]Die Pauschalierung entfällt, wenn der Zweitwohnungsinhaber nachweist, dass er sich im Abgeltungszeitraum nicht im Staatsbad aufgehalten hat.

9.10.2 Nutzungsbeschränkung der übermittelten personenbezogenen Daten

Beherbergungsbetriebe haben mir berichtet, dass die zur Erhebung der Kurtaxe übermittelten Daten von einem Staatsbad zu **Marketingzwecken** genutzt wurden. In Rundschreiben an die Kurgäste wurden dabei beispielsweise auch Informationen zu Konkurrenzangeboten übermittelt.

Ich habe das betroffene Staatsbad darauf hingewiesen, dass diese Praxis ohne ausdrückliche Zustimmung sowohl des Kurgastes als auch des Beherbergungsbetriebs **nicht zulässig** ist. Es gibt **keine gesetzliche Erlaubnis**, die von den Kurgästen zur Festsetzung und Erhebung der Kurtaxe erhobenen Daten für Marketingzwecke zu verwenden. Art. 26 Abs. 1 MeldeG enthält eine **strenge Nutzungsbeschränkung** hinsichtlich der melderechtlichen Angaben, die von den Gästen der Beherbergungsbetriebe erhoben wurden. Nach Art. 26 Abs. 1 Satz 2 MeldeG dürfen diese Daten – abgesehen von den in Satz 1 vor allem geregelten Zwecken der Gefahrenabwehr und Strafverfolgung – nur zur Erhebung des Fremdenverkehrs- und Kurbeitrags gemäß Art. 6 und 7 Kommunalabgabengesetz (KAG), zur Erhebung der Kurtaxe gemäß Art. 24 KG und für Zwecke der Beherbergungs- und Fremdenverkehrsstatistiken ausgewertet und verarbeitet werden. Seit der Neufassung des Art. 24 Abs. 3 Satz 5 KG im Zuge des Haushaltsgesetzes 2011/2012 mit Wirkung zum 01.05.2011 sieht nunmehr auch das Kostengesetz eine klare Nutzungsbeschränkung vor: danach dürfen die Erhebungsberechtigten die übermittelten Daten nur zur Erhebung der Kurtaxe und zur Ahndung von entsprechenden Ordnungswidrigkeiten verwenden. Für eine anderweitige Verwendung dieser Gästedaten durch die Staatsbäder besteht keine gesetzliche Grundlage.

Kurtaxpflichtige Personen haben in der Regel ein schutzwürdiges Interesse daran, dass ihre zwangsweise erhobenen Daten von den Erhebungsberechtigten nur zu den gesetzlich vorgesehenen Zwecken – im Wesentlichen also zur Erhebung der Kurtaxe – verwendet werden und sie im Übrigen von unerwünschter personenbezogener Werbung verschont bleiben. Hieraus folgt, dass die Nutzung der Meldedaten durch die Staatsbäder für Werbezwecke **nur mit ausdrücklicher Einwilligung der betroffenen kurtaxpflichtigen Personen** zulässig ist (Art. 15 Abs. 1 Nr. 2 BayDSG). Bei den Adressdaten der Kurgäste handelt es sich aus meiner Sicht ferner um **Kundendaten** und damit um personenbezogene Daten des jeweiligen Beherbergungsunternehmers. Eine Nutzung der Adressdaten der

Kurgäste durch die Staatsbäder für Werbezwecke setzt daher **zusätzlich die Einwilligung der betroffenen Beherbergungsunternehmer** voraus.

Art. 26 Abs. 1 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.

Art. 24 Abs. 3 KG Kurtaxe
(3) [1]Die Kurtaxordnungen für die einzelnen Staatsbäder erlässt das Staatsministerium der Finanzen als Rechtsverordnungen. [2]Die Kurtaxordnungen haben insbesondere die Festlegung der Kurbezirke, die Höhe der Kurtaxen, den Kreis der Abgabenpflichtigen und das Entstehen der Abgabeschuld zu bestimmen. [3]Sie können auch nähere Bestimmungen über völlige oder teilweise Befreiungen von der Abgabepflicht aus sozialen oder sonstigen wichtigen Gründen und über die Erhebung und Verwendung der Kurtaxen sowie Durchführungsvorschriften enthalten. [4]Es kann ferner bestimmt werden, dass

a) die Vermieter von Unterkünften, Reiseunternehmer von Gesellschaftsreisen und Inhaber von Kurmittelanstalten zur Meldung von Kurgästen und zur Vereinnahmung und Abführung der Kurtaxe verpflichtet sind und neben dem Schuldner als Gesamtschuldner für die Zahlung der Kurtaxe haften;

b) für Meldeformulare, die in Zusammenhang mit der Kurtaxerhebung ausgegeben und nicht zurückgegeben wurden, ein pauschaler Ersatz zu leisten ist, der den Zwei-Monats-Betrag des jeweils geltenden Kurtaxsatzes nicht überschreiten darf; die Erhebung des pauschalen Ersatzes unterbleibt, soweit sie der Billigkeit widerspricht;

c) die Kurtax-Anmeldung nach amtlich vorgeschriebenem Datensatz durch Datenfernübertragung zu übermitteln ist.

[5]Die Erhebungsberechtigte nach Abs. 1 Sätze 1 und 2 kann die übermittelten Daten bis zum Eintritt der Verjährung zum Vollzug der Art. 24 und 26 sowie der Kurtaxordnung verwenden. [6]Die Verordnung über die elektronische Übermittlung von für das Besteuerungsverfahren erforderlichen Daten (Steuerdaten-Übermittlungsverordnung – StDÜV) vom 28. Januar 2003 (BGBl I S. 139) gilt in der jeweils geltenden Fassung sinngemäß.

9.10.3 Frist zur Aufbewahrung der Meldeunterlagen

Die Pflichten der Vermieter im Rahmen der Erhebung der Kurtaxe sind in § 7 Kurtaxordnung definiert. Die Vermieter müssen danach der Erhebungsberechtigten u.a. die Meldedaten spätestens am dritten Werktag nach dem Eintreffen der Kurgäste übermitteln und auf Verlangen über alle Tatsachen und Umstände, die zur Festsetzung der Kurtaxe erheblich sind, Auskunft erteilen sowie insbesondere die Meldeunterlagen zur Einsicht vorlegen.

Bislang war in § 7 Abs. 3 Satz 2 Kurtaxordnung geregelt, dass die Meldeunterlagen drei Jahre nach Vornahme der letzten Eintragung aufzubewahren sind. Dies stand in Widerspruch zu den melderechtlichen Regelungen, wonach die **besonderen Meldescheine für Beherbergungsstätten grundsätzlich ein Jahr aufzubewahren** sind (Art. 24 Abs. 4 MeldeG); diese Frist verlängert sich auf zwei Jahre, soweit die Stammgastregelung nach Art. 23 Abs. 2 Satz 5 MeldeG greift.

Auf diese Diskrepanz habe ich das Staatsministerium der Finanzen aufmerksam gemacht. Ich begrüße sehr, dass die Regelung des § 7 Abs. 3 Satz 2 Kurtaxordnung mittlerweile mit Wirkung zum 01.06.2011 aufgehoben wurde. Somit besteht nun Rechtssicherheit, dass die **Aufbewahrungsfristen des Meldegesetzes hinsichtlich der Meldescheine auch dann gelten, wenn diese Unterlagen der Erhebung der Kurtaxe dienen.**

Art. 24 Abs. 4 MeldeG
(4) Die Meldescheine sind von der Beherbergungsstätte ein Jahr aufzubewahren, für die Polizei und die Meldebehörde zur Einsichtnahme bereitzuhalten sowie ihnen auf Verlangen auszuhändigen, vor unbefugter Einsichtnahme zu sichern und nach Ablauf der Aufbewahrungsdauer binnen angemessener Frist zu vernichten, soweit sie nicht nach Art. 23 Abs. 2 Satz 5 oder Art. 26 Abs. 1 Satz 3 genutzt werden.

Von der Frage der die Vermieter treffenden Pflicht zur Aufbewahrung der Meldeunterlagen zu unterscheiden ist die Frage, wie lange die Erhebungsberechtigte die zur Festsetzung und Erhebung der Kurtaxe übermittelten Daten verwenden kann. Hierzu ist in Art. 24 Abs. 3 Satz 5 KG nunmehr klar gestellt, dass die **Erhebungsberechtigte die Daten äußerstenfalls bis zum Eintritt der Verjährung verwenden darf.** Maßgeblich sind insoweit die in der Abgabenordnung festgelegten Festsetzungs- und Verjährungsfristen (Art. 24 Abs. 6 Satz 1 KG i.V.m. Art. 13 Abs. 1 Nr. 4 Buchst. b) Doppelbuchst. bb) und Nr. 5 Buchst. a) KAG).

10 Schulen

10.1 Endlich: Datenschutzbeauftragte an staatlichen Schulen

In Folge der Einfügung des Art. 25 Abs. 2 BayDSG im Zuge der Novellierung des Bayerischen Datenschutzgesetzes sind seit dem 01.03.2001 **alle bayerischen öffentlichen Stellen,** die personenbezogene Daten mit Hilfe von automatisierten Verfahren verarbeiten oder nutzen, **gesetzlich verpflichtet, einen ihrer Beschäftigten zum behördlichen Datenschutzbeauftragten zu bestellen.** Als einziges Staatsministerium hatte jedoch das Staatsministerium für Unterricht und Kultus seinerzeit von der in Art. 28 Abs. 2 BayDSG eingeräumten Verordnungsermächtigung umgehend Gebrauch gemacht und in der „Verordnung zur Durchführung des Art. 28 Abs. 2 des Bayerischen Datenschutzgesetzes“ vom 23.03.2001 für die öffentlichen Schulen bestimmt, dass die Bestellung behördlicher Datenschutzbeauftragter, die datenschutzrechtliche Freigabe und die Führung eines Verfahrensverzeichnisses nicht erforderlich sind, wenn die Schulen ausschließlich automatisierte Verfahren, die durch das Staatsministerium für Unterricht und Kultus bereits generell freigegeben sind, in dem in den Anlagen der Verordnung aufgeführten Umfang einsetzen.

Aus Datenschutzsicht habe ich dieses Vorgehen des Kultusministeriums stets kritisch gesehen. In Anbetracht der an den Schulen tagtäglich erfolgenden umfangreichen Erhebungen, Verarbeitungen und Nutzungen von – überdies noch oftmals sehr sensiblen – Schüler-, Eltern- und Lehrerdaten habe ich das Staatsministerium für Unterricht und Kultus daher in den vergangenen Jahren immer wieder – und mit stetig zunehmendem Nachdruck – aufgefordert, auch an den staatlichen Schulen – ebenso wie an allen anderen bayerischen öffentlichen Stellen – endlich die Bestellung behördlicher Datenschutzbeauftragter vorzusehen.

Im Berichtszeitraum hat sich das Staatsministerium für Unterricht und Kultus im Rahmen der Einführung des Amtlichen Schulverwaltungsprogramms (ASV) – siehe hierzu ausführlich Nr. 10.2 – erfreulicherweise endlich meinen Argumenten gegenüber aufgeschlossen gezeigt und sich bereit erklärt, **an den staatlichen Schulen bzw. Schulämtern sukzessive behördliche Datenschutzbeauftragte einzurichten.** Dabei ist folgender Zeitplan vorgesehen:

– Schuljahr 2011/2012: Bestellung jeweils eines Datenschutzbeauftragten an 24 staatlichen Realschulen (Pilotschulen);

– Schuljahr 2012/2013: Bestellung jeweils eines Datenschutzbeauftragten an den rund 190 übrigen staatlichen Realschulen und den rund 310 staatlichen Gymnasien;

– Schuljahr 2013/2014: Bestellung jeweils eines Datenschutzbeauftragten an den 96 Schulämtern, der auch für die staatlichen Grund-, Haupt- und Mittelschulen sowie die staatlichen Volksschulen zur sonderpädagogischen Förderung des jeweiligen Schulamtsbezirks zuständig ist;

– Schuljahr 2014/2015: Bestellung jeweils eines Datenschutzbeauftragten an den rund 485 staatlichen beruflichen Schulen (einschließlich berufliche Schulen zur sonderpädagogischen Förderung und Wirtschaftsschulen).

In Anbetracht dieses herausragenden Erfolgs für den Schuldatenschutz in Bayern habe ich es mir nicht nehmen lassen, die an den 24 Pilotrealschulen neu bestellten behördlichen Datenschutzbeauftragten zu Beginn ihrer **Ausbildung an der Akademie für Lehrerfortbildung und Personalführung Dillingen** persönlich zu begrüßen, für aktuelle datenschutzrechtliche Fragestellungen im Schulbereich zu sensibilisieren und auf ihre neue Rolle als Ansprechpartner für die Schulleiter wie für die Schülerinnen, Schüler, Erziehungsberechtigten, Lehrerinnen und Lehrer einzustimmen.

Daneben habe ich das Staatsministerium für Unterricht und Kultus bei der Erarbeitung einer umfassenden, laufend aktualisierten **Handreichung für Datenschutzbeauftragte an bayerischen staatlichen Schulen** unterstützt. Die Handreichung ist von der Homepage des Kultusministeriums www.stmuk.bayern.de unter „Ministerium“ – „Recht“ – „Datenschutz“ allgemein abrufbar. Über die datenschutzrechtlichen Fachbegriffe und die für die Schulen bedeutsamen Datenschutzbestimmungen hinaus erläutert die Handreichung detailliert die Bestellung, Aufgaben und Rechte der schulischen Datenschutzbeauftragten und beantwortet ausführlich die an den Schulen hauptsächlich auftretenden Datenschutzfragen. Schließlich enthält die Handreichung neben den für die tägliche Arbeit der schulischen Datenschutzbeauftragten relevanten Vorlagenmustern auch Prüfungsschemata, in denen die Vorgehensweise bei der Prüfung der Rechtmäßigkeit von schulischen Datenerhebungen, -verarbeitungen und -nutzungen anhand von schulbezogenen Beispielen praxisnah erläutert wird. Ich hoffe, dass sich die Handreichung als ein verständliches, praxisgerechtes und insgesamt wertvolles Hilfsmittel für die tägliche Arbeit der schulischen Datenschutzbeauftragten erweisen wird.

Last but not least möchte ich darauf hinweisen, dass die Akademie für Lehrerfortbildung und Personalführung Dillingen in Zusammenarbeit mit der Behördlichen Datenschutzbeauftragten des Staatsministeriums für Unterricht und Kultus für Datenschutzbeauftragte an bayerischen Schulen einen umfangreichen, interaktiven **Onlinekurs zum Selbststudium** entwickelt hat.

Ich bin zuversichtlich, dass die bayernweite und schulartenübergreifende Einrichtung schulischer Datenschutzbeauftragter in den kommenden Jahren nicht nur zu einer flächendeckenden, sondern auch zu einer substantiellen Verbesserung des Datenschutzes an bayerischen staatlichen Schulen führen wird. Ich möchte es daher nicht versäumen, auch an dieser Stelle dem Staatsministerium für Unterricht und Kultus meine Anerkennung für diese wegweisende Entscheidung auszusprechen.

10.2 Amtliches Schulverwaltungsprogramm (ASV)

In meinem 24. Tätigkeitsbericht, Nr. 10.1, hatte ich zuletzt über das im Jahre 2005 gestartete eGovernment-Großprojekt **„Amtliche Schuldaten (ASD)“** des Staatsministeriums für Unterricht und Kultus ausführlich berichtet und dabei auch die von mir erreichten datenschutz- und statistikrechtlichen Verbesserungen geschildert. Gegenstand des Verfahrens ASD ist zum einen eine umfassende Restrukturierung der Geschäftsprozesse der Kultusverwaltung mit dem Ziel ei-

nes **effektiven, netzbasierten Schulverwaltungsverfahrens** und zum anderen eine **Neukonzeption der Schulstatistik,** die insbesondere durch die Ermöglichung von Bildungsverlaufsuntersuchungen die längerfristige Bildungsplanung verbessern soll. Am 19.05.2010 hat der Landtag schließlich die von mir stets nachdrücklich geforderte rechtssichere, normenklare und tragfähige gesetzliche Rechtsgrundlage für das Verfahren ASD beschlossen.

ASD setzt in seiner praktischen Anwendung den Einsatz eines vom Staatsministerium für Unterricht und Kultus bereitgestellten Schulverwaltungsprogramms an den einzelnen bayerischen Schulen voraus. Im Berichtszeitraum habe ich die Entwicklung dieses **„Amtlichen Schulverwaltungsprogramms (ASV)"** durch das Staatsministerium für Unterricht und Kultus von Anfang an aus Datenschutzsicht intensiv begleitet. Mit ASV sollen nicht nur **innerschulische Verwaltungsprozesse** – wie zum Beispiel die Anmeldung der Schüler, die Bildung der Klassen, die Erfassung der Leistungsdaten, die Erstellung der Zeugnisse, der Unterrichtseinsatz der Lehrkräfte oder die Organisation des Unterrichts – erleichtert werden. Vielmehr soll ASV auch – in dem nach Art. 85 Abs. 1 Satz 5, 85 a, 113 a und 113 b BayEUG gesetzlich zulässigen Umfang – den **zur Ausübung der Schulaufsicht erforderlichen Datentransfer** zwischen der Schule und den zuständigen Schulaufsichtsbehörden sowie die **Datenübermittlung zu statistischen Zwecken** von der Schule an das Landesamt für Statistik und Datenverarbeitung unterstützen.

Im Laufe einer lang andauernden, intensiven und kritischen Diskussion mit dem Staatsministerium für Unterricht und Kultus habe ich mir in Bezug auf die von ASV erfassten personenbezogenen Daten – vor allem von Schülerinnen und Schülern, Erziehungsberechtigten und Lehrkräften – jeweils detailliert erläutern lassen, warum die Speicherung jedes einzelnen Datums zur Aufgabenerfüllung der Schulen erforderlich ist. Ebenso eingehend habe ich mir den Umfang sowie die Empfänger der regelmäßigen Datenübermittlungen aus ASV, den Kreis der verarbeitungs- und nutzungsberechtigten Personengruppen und die vorgesehenen Löschfristen im Einzelnen darlegen lassen. Durch mein Tätigwerden **konnte ich so erhebliche datenschutzrechtliche Verbesserungen erreichen:** vom vollständigen Verzicht auf zahlreiche Datenspeicherungen über die Eindämmung datenschutzrechtlich stets bedenklicher Freitextfelder bis etwa zur Einschränkung der Nutzungsrechte oder zur Abkürzung der Löschfristen. Die konstruktive Atmosphäre bei allen meinen zahlreichen Besprechungen im Staatsministerium für Unterricht und Kultus möchte ich an dieser Stelle nicht unerwähnt lassen.

10.2.1 Landesweite datenschutzrechtliche Freigabe von ASV

Entgegen den ursprünglichen, auch von mir unterstützten Planungen hat das Staatsministerium für Unterricht und Kultus allerdings leider davon Abstand genommen, die Einführung von ASV durch eine Änderung der Verordnung zur Durchführung des Art. 28 Abs. 2 des Bayerischen Datenschutzgesetzes auf eine für alle bayerischen staatlichen, kommunalen und staatlich anerkannten Ersatzschulen geltende, passgenaue rechtliche Grundlage zu stellen. Stattdessen hat sich das Kultusministerium dafür entschieden, das Verfahren ASV **für den Einsatz an allen staatlichen Schulen** im Sinne des Art. 3 Abs. 1 Satz 2 BayEUG landesweit datenschutzrechtlich gem. Art. 26 Abs. 1 Satz 2 Halbsatz 2 BayDSG freizugeben. Diese Freigabe ist von der Homepage des Kultusministeriums www.stmuk.bayern.de unter „Ministerium" – „Recht" – „Datenschutz" allgemein abrufbar. Die für die staatlichen Schulen bestellten behördlichen Datenschutzbe-

auftragten müssen die Freigabe gem. Art. 27 Abs. 1 BayDSG nur noch in das jeweilige Verfahrensverzeichnis aufnehmen. Bei den **kommunalen und privaten Schulen** muss der Einsatz von ASV dagegen weiterhin durch den jeweils zuständigen Datenschutzbeauftragten **eigenständig datenschutzrechtlich freigegeben** werden, wobei selbstverständlich die landesweite Freigabe des Kultusministeriums entsprechend herangezogen werden kann.

Im Hinblick auf den äußerst umfangreichen Datenkranz unter Abschnitt 3 („Art der gespeicherten Daten") der landesweiten datenschutzrechtlichen Freigabe von ASV möchte ich bereits an dieser Stelle **festhalten, dass die Schulen weder verpflichtet sind, in jedem Falle alle Daten erheben zu müssen, noch insoweit umfassende Datenerhebungsbefugnisse für sich in Anspruch nehmen können:**

– Zum einen müssen **nicht alle** in der Freigabe aufgeführten **Daten an jeder Schule verpflichtend** gespeichert werden. Vielmehr handelt es sich hier **zum Teil** schulartübergreifend um **freiwillige** Angaben (wie z.B. die E-Mail-Adresse, die URL oder die Bankverbindung) oder **teilweise** um **schulartspezifische** Angaben (wie z.B. die Kammernummer).

– Zum anderen bildet die landesweite Freigabe nur den **weitestmöglichen Rahmen** aller in allen Schularten auf verpflichtender oder freiwilliger Basis möglichen Dateneingaben. Über die **Verpflichtung zur Erhebung und Angabe** des jeweiligen Datums entscheiden **allein die bestehenden** – ggf. schulartspezifischen – **schulrechtlichen Bestimmungen.**

10.2.2 Umfang des verpflichtenden Einsatzes von ASV

Zu meinem Bedauern hat das Staatsministerium für Unterricht und Kultus den staatlichen Schulen den Einsatz von ASV allerdings **nicht in allen Funktionalitäten, sondern nur** in dem in Art. 85 Abs. 1 Satz 5 BayEUG umrissenen **Mindestumfang** verpflichtend vorgeschrieben. Im Hinblick auf das in Art. 11 Abs. 2 Bayerische Verfassung garantierte kommunale Selbstverwaltungsrecht einerseits und die in Art. 134 Bayerische Verfassung gewährleistete Privatschulfreiheit andererseits kann ich zwar nachvollziehen, dass den kommunalen und privaten Schulen der Einsatz des vom Freistaat vorgegebenen Amtlichen Schulverwaltungsprogramms nur in dem für ASD zwingend notwendigen, in Art. 85 Abs. 1 Satz 5 BayEUG beschriebenen Umfang verpflichtend vorgeschrieben werden konnte. Dem Kultusministerium ist es aber aus verfassungsrechtlichen Gründen gerade nicht verwehrt, kraft seiner Weisungskompetenz als oberste Dienstbehörde den umfassenden Einsatz von ASV allen seinen nachgeordneten staatlichen Schulen verpflichtend vorzugeben.

Dies ist aus datenschutzrechtlicher Sicht auch geboten. Mit meiner intensiven Unterstützung konnte ASV nämlich in einem langwierigen Prozess im Grundsatz datenschutzgerecht ausgestaltet werden. **ASV ist daher in seiner Gesamtheit geeignet, zu einer substantiellen Verbesserung des Datenschutzes an allen bayerischen staatlichen Schulen entscheidend beizutragen.** Im Hinblick auf an staatlichen Schulen derzeit noch rechtmäßig eingesetzte, ganz oder teilweise vergleichbare EDV-Programme privater Anbieter können dabei selbstverständlich die im Einzelfall notwendigen Übergangsregelungen vorgesehen werden, worauf ich das Kultusministerium auch hingewiesen habe.

Im Zuge einer eingehenden und langwierigen Diskussion mit dem Kultusministerium konnte ich immerhin zwei datenschutzrechtlich wesentliche Punkte erreichen: Zum einen hat das **Kultusministerium** den staatlichen Schulen den – im Übrigen völlig kostenfreien – **Einsatz der weiteren**, über den in Art. 85 Abs. 1 Satz 5 BayEUG beschriebenen Mindestumfang hinausgehenden **Funktionalitäten von ASV ausdrücklich empfohlen.** Sollten die staatlichen Schulen stattdessen (weiterhin) andere (private und damit im Regelfall kostenpflichtige) EDV-Programme zur schulischen Datenverarbeitung einsetzen, hat das Kultusministerium zum anderen Folgendes zur **Sicherstellung des datenschutzkonformen Einsatzes dieser anderen Verfahren** bestimmt:

– Soweit mit dem Verfahren Daten verarbeitet werden, die in der landesweiten Freigabe von ASV genannt sind, gelten für die Löschung der Daten, die Zugriffsberechtigungen auf die Daten und die Datenübermittlung die Vorgaben der landesweiten Freigabe entsprechend.

– Sind andere Daten als die in der landesweiten Freigabe von ASV genannten betroffen, ist eine Freigabe für die Datengruppen „Ordnungsmaßnahmen", „Daten zum sozialen Hintergrund" und „sensible Daten im Sinne des Art. 15 Abs. 7 BayDSG" ausdrücklich untersagt.

10.2.3 Ausblick

Der Einsatz von ASV ist erst möglich, wenn für die Schule ein behördlicher Datenschutzbeauftragter bestellt ist (siehe hierzu Nr. 10.1). Der flächendeckende Rollout von ASV wird daher noch einige Zeit in Anspruch nehmen.

Ich werde die Entwicklung **in datenschutzrechtlicher Hinsicht weiterhin aufmerksam begleiten** und – soweit immer notwendig – erneut an das Staatsministerium für Unterricht und Kultus herantreten.

10.3 Veröffentlichung von personenbezogenen Daten durch Schulen

Im Rahmen ihrer Öffentlichkeitsarbeit wollen viele öffentliche Schulen über Ereignisse aus dem Schulleben auch einem breiteren Publikum – insbesondere auf der **Schulhomepage** – berichten und dabei u.a. auch personenbezogene Daten von Schulangehörigen verwenden. Datenschutzrechtlich bedarf es hierfür grundsätzlich einer **freiwilligen, informierten und schriftlichen Einwilligung der betroffenen Schülerinnen, Schüler, Eltern, Lehrerinnen und Lehrer** (siehe im Einzelnen Art. 15 Abs. 2 bis 4 und 7 BayDSG). Eine Ausnahme von diesem Einwilligungserfordernis besteht im Hinblick auf die Veröffentlichung dienstlicher Kommunikationsdaten der Schulleitung und von Lehrkräften, die an der Schule eine Funktion mit Außenwirkung wahrnehmen (vgl. etwa Nr. 3 der Anlage 9 „Internetauftritt von Schulen" der Verordnung des Staatsministeriums für Unterricht und Kultus zur Durchführung des Art. 28 Abs. 2 des Bayerischen Datenschutzgesetzes). Im **papiergebundenen Jahresbericht** ist zudem ohne Einwilligung die Veröffentlichung der in Art. 85 Abs. 3 BayEUG ausdrücklich genannten Daten zulässig. Insbesondere **(Schüler-, Lehrer- und Klassen-) Fotos** dürfen daher ohne datenschutzgerechte Einwilligung der betroffenen Schulangehörigen weder in den schulischen Jahresbericht aufgenommen noch in die Schulhomepage eingestellt noch in sonstiger Weise von der Schule veröffentlicht werden.

Art. 85 Abs. 3 BayEUG Erhebung, Verarbeitung und Nutzung von Daten
(3) Gibt eine Schule für die Schülerinnen und Schüler und Erziehungsberechtigten einen Jahresbericht heraus, so dürfen darin 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.

Mit diesem breitgefächerten Problemkreis, der mich bereits in den vergangenen Jahren wiederholt beschäftigt hat (siehe hierzu nur 24. Tätigkeitsbericht, Nr. 10.2, sowie 23. Tätigkeitsbericht, Nr. 12.2.3 und Nr. 12.4), war ich auch im aktuellen Berichtszeitraum wieder intensiv befasst

10.3.1 Muster-Einwilligungserklärungen

Aus datenschutzrechtlicher Sicht muss grundsätzlich für jede schulische Veröffentlichung eines personenbezogenen Datums eine gesonderte, datenschutzgerechte Einwilligung des jeweils Betroffenen vorliegen. Um den Schulen die Einholung rechtlich einwandfreier Einwilligungserklärungen zu ermöglichen und die praktische Arbeit zu erleichtern, habe ich in Abstimmung mit dem Staatsministerium für Unterricht und Kultus **vier Muster-Einwilligungserklärungen** entwickelt, die von meiner Homepage www.datenschutz-bayern.de unter der Rubrik „Themen", Unterrubrik „Schulen" abrufbar sind. Diese Muster basieren auf Vorarbeiten des Referats für Bildung und Sport der Landeshauptstadt München; auch insoweit weise ich auf meine Pressemitteilung „Schuldatenschutz verbessern: Datenschutzkonforme Einwilligungserklärungen verwenden!" vom 26.05.2011 sowie auf meinen 24. Tätigkeitsbericht, Nr. 10.2.3, hin.

Mit den Muster-Einwilligungserklärungen werden die Schulen in die Lage versetzt, die notwendigen Einwilligungen **für bestimmte, typische Veröffentlichungsformen** im Voraus einzuholen und damit Rechtssicherheit zu erlangen. Die Schulen haben dabei sicherzustellen, dass für jede Person, die **auf der Schulhomepage, im schulischen Jahresbericht oder in der Tagespresse** genannt oder abgebildet ist, die erforderliche Einwilligung vorliegt. Auf meine Bitte hin hat das Staatsministerium für Unterricht und Kultus mit KMS vom 27.05.2011 (Az.: I.5-5 L 0572.2/48/20) den **bayernweiten Einsatz** der Muster-Einwilligungserklärungen **allen staatlichen Schulen ab dem Schuljahr 2011/2012 verbindlich vorgegeben und allen kommunalen und staatlich anerkannten Schulen empfohlen.**

Die Muster-Einwilligungserklärungen **differenzieren nach vier Gruppen von Schulangehörigen** („Minderjährige Schülerinnen und Schüler", „Volljährige Schülerinnen und Schüler", „Mitglieder des Elternbeirats" sowie „Lehrkräfte, Verwaltungspersonal, externes Personal in Ganztagesangeboten"). Sie eröffnen den Betroffenen jeweils die Möglichkeit, einer Veröffentlichung ihrer personenbezogenen Daten im Jahresbericht der Schule (soweit nicht bereits gesetzlich nach Art. 85 Abs. 3 BayEUG zulässig), in der örtlichen Tagespresse und/oder im World Wide Web (Internet) auf der Schulhomepage zuzustimmen. Hintergrund für diese Differenzierung ist, dass aufgrund der jeweils unterschiedlichen Öffentlichkeitswirkung aus Datenschutzsicht insoweit auch ein unterschiedlicher Gefährdungsgrad besteht. Die Betroffenen sollen sich konkret Gedanken darüber machen, ob sie eine **Veröffentlichung ihrer personenbezogenen Daten in**

dem jeweiligen Medium mit dem jeweiligen Adressatenkreis – Jahresbericht: Schülerinnen, Schüler und Eltern; örtliche Tagespresse: Allgemeinheit am Schulort; World Wide Web: Allgemeinheit weltweit – wollen.

Ungeachtet der zur Verfügung gestellten Muster-Einwilligungserklärungen habe ich stets deutlich gemacht, dass mit jeder Veröffentlichung von personenbezogenen Daten einschließlich Fotos datenschutzrechtliche Risiken verbunden sind. Dies gilt insbesondere für Veröffentlichungen im Internet: die Daten können über Internet-Suchmaschinen aufgefunden und mit weiteren im Internet verfügbaren Daten verknüpft, verändert oder zu anderen Zwecken verwendet werden. **Daher empfehle ich allen öffentlichen Stellen und damit auch allen öffentlichen Schulen, bei der Veröffentlichung von personenbezogenen Daten grundsätzlich Zurückhaltung zu üben.** Auch vor diesem Hintergrund beziehen sich die Muster-Einwilligungserklärungen nur auf die Veröffentlichung von Fotos und Texten; die Veröffentlichung von – datenschutzrechtlich noch sensibleren – Ton-, Video- und Filmaufnahmen ist hiervon ausdrücklich nicht umfasst.

10.3.2 Einzelfragen zu den Muster-Einwilligungserklärungen

Die Auslegung und Handhabung der Muster war – wie einige Anfragen bei mir gezeigt haben – in der schulischen Praxis vereinzelt noch mit Unsicherheiten verbunden, insbesondere zu Beginn des Schuljahres 2011/2012. Meine wichtigsten Hinweise an die öffentlichen Schulen ebenso wie an die betroffenen Schulangehörigen möchte ich daher nachfolgend kurz zusammenfassen:

– Angesichts der Vielzahl der denkbaren Fallgestaltungen wurde bewusst darauf verzichtet, in den Mustern einzelne personenbezogene Daten aufzulisten und mit einer Wahlmöglichkeit zu versehen (eine im Hinblick auf Internetveröffentlichungen eingeschränkte Auswahloption gibt es insoweit nur in den Mustern für „Mitglieder des Elternbeirats“ und für „Lehrkräfte, Verwaltungspersonal, externes Personal in Ganztagesangeboten“). Die **Formulare** wären sonst nicht mehr handhabbar gewesen. Sie **beziehen sich** vielmehr – wie in den einleitenden Ausführungen der Muster klargestellt – in allgemeiner Form **nur auf diejenigen personenbezogenen Daten, die für die Öffentlichkeitsarbeit der Schulen erforderlich sind.** Dies sind etwa personenbezogene Informationen über Schulausflüge, Schülerfahrten, Schüleraustausche, (Sport-)Wettbewerbe, Unterrichtsprojekte oder den „Tag der Offenen Tür“. Damit sind gleichzeitig die Grenzen einer Veröffentlichung aufgezeigt: Daten, die für die schulische Öffentlichkeitsarbeit im dargestellten Umfang nicht erforderlich sind, sind von der Einwilligung nicht erfasst. Eine schrankenlose Veröffentlichung von Daten – also etwa eine Veröffentlichung von Schulnoten, Telefonnummern oder (E-Mail-) Adressen der Schülerinnen und Schüler, Eltern, Lehrerinnen und Lehrer – ist daher auch nach Unterzeichnung des Formulars nicht zulässig.

– Die ausdrückliche Aufnahme der Antwortoption „Nein“ in das Muster halte ich nicht für notwendig. Soweit und solange eine Einwilligung nicht vorliegt, darf die Schule keine personenbezogenen Daten veröffentlichen. Schweigen bedeutet datenschutzrechtlich „Nein“. **Schulangehörige, die einer Veröffentlichung von Daten nicht – auch nicht eingeschränkt – zustimmen wollen, müssen daher nichts tun.** Selbstverständlich ist es der Schule datenschutzrechtlich unbenommen, sich insoweit ggf. durch

Rückfragen zu vergewissern; dabei darf allerdings kein Druck ausgeübt werden. Die Entscheidung, ob und in welchem Umfang eine Einwilligungserklärung erteilt und das Formular dementsprechend ausgefüllt und an die Schule zurückgegeben wird, liegt allein bei den Schülerinnen, Schülern, Eltern, Lehrerinnen und Lehrern.

– Verantwortlich für die Einhaltung des Datenschutzes ist die **Schule**. Sie **muss in jedem Einzelfall dafür Sorge tragen, dass ohne hinreichende Einwilligungserklärung keine personenbezogenen Daten veröffentlicht werden.** Dies hat sie durch angemessene technische und organisatorische Maßnahmen sicherzustellen (vgl. Art. 7 Abs. 1 BayDSG). Diese datenschutzrechtliche Verantwortlichkeit kann die Schule – wie in einem mir bekannt gewordenen Fall zunächst beabsichtigt – nicht auf die Lehrerinnen und Lehrer, Eltern oder gar die Schülerinnen und Schüler „abwälzen". Die Schulangehörigen sind weder verpflichtet, eine Erklärung zur Übernahme der datenschutzrechtlichen Verantwortung zu unterschreiben, noch würde eine Unterschrift die Schule von ihrer Verantwortung entbinden.

– Die Muster-Einwilligungserklärungen sollen den Schulen eine Hilfe sein, den unterschiedlichen Vorstellungen der Schülerinnen und Schüler, Eltern, Lehrerinnen und Lehrer in der Praxis gerecht zu werden. Vor diesem Hintergrund ist es den Schulen verwehrt, im Falle nur eingeschränkt erteilter Einwilligungserklärungen (beispielsweise nur für den Jahresbericht und die Tagespresse, nicht jedoch für das Internet) unter Verweis auf einen etwaigen Mehraufwand generell auf jede Veröffentlichung von Daten des Betroffenen zu verzichten. Dies würde nicht nur dem ausdrücklichen Willen des Betroffenen widersprechen, sondern ihn auch in unzulässiger Weise unter Druck setzen, letztlich gegen seinen Willen einer schulischen Veröffentlichung in allen Medien zuzustimmen. Kein Betroffener ist aber verpflichtet, seine Einwilligung zu geben; **aus der Nichterteilung, der eingeschränkten Erteilung oder dem (Teil-) Widerruf der Einwilligung dürfen den Betroffenen** auch **keine Nachteile entstehen.**

10.4 Kein Einsatz von „Plagiatssoftware" an Schulen

Um den Schulen unkomplizierte und rechtssichere Vervielfältigungen aus urheberrechtlich geschützten Werken für den Unterrichts- und Prüfungsgebrauch zu ermöglichen, schlossen die Kultusministerien der Länder mit den Verwertungsgesellschaften und Schulbuchverlagen im Dezember 2010 einen „Gesamtvertrag zur Einräumung und Vergütung von Ansprüchen nach § 53 UrhG". Den **Schulen erlaubt werden** in dem dort näher bestimmten Umfang allerdings **nur papiergebundene, nicht aber digitale Kopien.** Um die Einhaltung dieser Vereinbarung sicherzustellen, sieht der Vertrag an jährlich mindestens einem Prozent der öffentlichen Schulen den Einsatz einer – von den Verlagen noch zu entwickelnden und sodann den Schul- und Sachaufwandsträgern zur Verfügung zu stellenden – sog. „Plagiatssoftware" vor, mit der die Schulrechner auf nicht erlaubte digitale Kopien überprüft werden sollen (§ 6 Abs. 4 des Gesamtvertrags).

Die vereinbarte Anwendung einer **Software zum Auffinden unzulässiger digitaler Kopien** wurde in Politik, Medien und Öffentlichkeit unter dem Schlagwort **„Schultrojaner"** sehr kritisch diskutiert. In diesem Zusammenhang haben mich zahlreiche Anfragen – insbesondere von Landtagsabgeordneten und von Lehre-

rinnen und Lehrern – erreicht. Auch der Bayerische Landtag hat sich u.a. im Rahmen von vier Dringlichkeitsanträgen eingehend mit dieser Problematik befasst (siehe Plenarprotokoll 16/87 vom 09.11.2011, S. 7829 ff.).

Von dem Vertrag und dem darin vorgesehenen Einsatz der „Plagiatssoftware" habe ich erst im Herbst 2011 aus der Presseberichterstattung erfahren. Aus Datenschutzsicht kann ich die Sorgen der Lehrerinnen und Lehrer sehr gut nachvollziehen. Ich habe mich daher unmittelbar nach Bekanntwerden der Vorgänge an das Staatsministerium für Unterricht und Kultus gewandt und um Aufklärung des Sachverhalts gebeten. Dabei habe ich bereits zu diesem Zeitpunkt deutlich gemacht, dass ich **zur Wahrung der Urheberrechte keine Notwendigkeit für eine personenbezogene Datenerhebung mittels der Software** sehe.

Das Staatsministerium für Unterricht und Kultus teilte mir daraufhin mit, dass die im Vertrag vorgesehene Software nicht der Feststellung dienen soll, welche Lehrkräfte digitale Kopien hergestellt haben. Nach **Darstellung des Kultusministeriums** ist eine **Erhebung personenbezogener Daten mithilfe der Software** vielmehr überhaupt **nicht beabsichtigt.** Den Verlagen sollen lediglich die Zahl etwaiger Plagiate sowie die Namen und der Umfang der betroffenen Werke mitgeteilt werden. Das Staatsministerium für Unterricht und Kultus sicherte mir darüber hinaus zu, dass die Länder den Einsatz der Software erst dann befürworten werden, wenn sie als datenschutzrechtlich und technisch unbedenklich angesehen werden kann.

Im Wege einer im Internet abrufbaren Pressemitteilung gab die Kultusministerkonferenz schließlich am 13.12.2011 bekannt, dass die „Plagiatssoftware" bis auf Weiteres – jedenfalls im Jahr 2012 – nicht zum Einsatz kommen wird; in Gesprächen der Vertragspartner sollten ferner mögliche Alternativen diskutiert werden.

Daraufhin habe ich das Staatsministerium für Unterricht und Kultus im Januar 2012 aufgefordert, auf den Einsatz der „Plagiatssoftware" vollständig zu verzichten und eine das informationelle Selbstbestimmungsrecht unberührt lassende Form der Kontrolle zu finden. Auch wenn die unmittelbare Erhebung personenbezogener Daten mittels der „Plagiatssoftware" nach Angaben des Kultusministeriums nicht beabsichtigt ist, können doch die erhobenen, auf den ersten Blick rein werkbezogenen Daten – je nach Art und Verbreitungsgrad des betroffenen Werks sowie den kopierten Stellen und dem Zeitpunkt der Speicherung – in vielen Fällen **mittelbar sehr wohl Rückschlüsse auf bestimmte Lehrerinnen und Lehrer zulassen.** In diesem Zusammenhang ist zu beachten, dass sich die Länder bei Bekanntwerden von Verstößen zur Einleitung disziplinarrechtlicher Maßnahmen gegen die betreffenden staatlichen Schulleiter und Lehrkräfte (§ 6 Abs. 7 des Gesamtvertrags) und zur Information der Rechteinhaber über die bei Rechtsverletzungen eingeleiteten Maßnahmen (§ 6 Abs. 3 Spiegelstrich 3 des Gesamtvertrags) im Gesamtvertrag verpflichtet haben. Unabhängig davon ist der Dienstvorgesetzte ohnehin nach Art. 19 Abs. 1 Satz 1 Bayerisches Disziplinargesetz – also bereits kraft Gesetzes – zur Einleitung eines Disziplinarverfahrens und zur Durchführung der erforderlichen Ermittlungen verpflichtet, wenn zureichende tatsächliche Anhaltspunkte vorliegen, die den Verdacht eines Dienstvergehens rechtfertigen. Vor diesem Hintergrund habe ich das Kultusministerium darauf aufmerksam gemacht, dass der **Einsatz einer „Plagiatssoftware" einer hinreichenden gesetzlichen Rechtsgrundlage bedarf** (Art. 15 Abs. 1 BayDSG), die schuldatenschutzrechtliche Befugnisnorm des Art. 85 Abs. 1 BayEUG insoweit aber wohl ausscheidet, da die Wahrung der Ur-

heberrechte nach meinem Kenntnisstand keine den Schulen durch Rechtsvorschriften zugewiesene Aufgabe darstellt.

Meine erneute Intervention beim Staatsministerium für Unterricht und Kultus und die öffentliche Kritik haben offensichtlich ihre Wirkung nicht verfehlt: Mit Pressemitteilung vom 04.05.2012 teilte das – innerhalb der Länder für die Verhandlungen mit den Schulbuchverlagen federführende – **Staatsministerium für Unterricht und Kultus** mit, dass nach neuerlichen Verhandlungen **bundesweit vom Einsatz einer „Plagiatssoftware" an den Schulen** im beiderseitigen Einvernehmen **abgesehen** wird. Das Kultusministerium kündigte zudem an, mit den Schulbuchverlagen eine gemeinsame Lösung zu erarbeiten, um den Lehrkräften **auch Möglichkeiten zur digitalen Nutzung von Unterrichtswerken und -materialien** an die Hand zu geben.

Ich werde die weitere Entwicklung genau verfolgen und mich auch künftig mit Nachdruck für die datenschutzrechtlichen Belange der Lehrerinnen und Lehrer einsetzen.

10.5 Videoüberwachung der Schultoilette

In kurzer Folge waren in der Knabentoilette einer staatlichen Schule mehrere, teils schwerwiegende Vorfälle von **Sachbeschädigungen** aufgetreten. So war u.a. eine Toilette mehrfach absichtlich mit Klopapierrollen verstopft, sodann benutzt und anschließend gespült worden. Um weitere Beschädigungen zu verhindern, ließ die Schulleitung in der Aula eine **Videokamera** anbringen, die auch den **Zugang zur Knabentoilette** erfasste. Die Schülerinnen und Schüler, die Lehrerinnen und Lehrer, der Personalrat und der Elternbeirat der Schule wurden allerdings erst nach der Installation der Videokamera informiert.

Über diesen Vorgang wurde ausführlich in der örtlichen Presse berichtet; dabei wurde auch darauf hingewiesen, dass **an weiteren Schulen im betroffenen Landkreis** eine **Videoüberwachung vorhanden** sei. Vor allem aufgrund dieser Berichterstattung gingen zahlreiche Eingaben bei mir ein, in denen (auch nicht unmittelbar betroffene) Bürgerinnen und Bürger ihre Besorgnis über derartige Überwachungsmethoden – gerade in Schulen – zum Ausdruck brachten.

Auf meine Bitte um Stellungnahme teilte mir die Schule zunächst mit, dass es sich bei der Videokamera lediglich um eine **Kameraattrappe** handelte. Aus datenschutzrechtlicher Sicht ist allerdings festzuhalten, dass auch eine Kameraattrappe bezweckt, das Verhalten der vermeintlich überwachten Personen in bestimmter Weise zu beeinflussen, und daher in ähnlicher Weise wie eine „echte" Videoüberwachung in das Persönlichkeitsrecht der Betroffenen eingreift. Aus diesem Grunde muss die datenschutzrechtliche Zulässigkeit einer Kameraattrappe **nach den für eine Videoüberwachung geltenden Grundsätzen des Art. 21 a BayDSG beurteilt** werden (siehe hierzu 24. Tätigkeitsbericht, Nr. 7.3 sowie Wilde/Ehmann/Niese/Knoblauch, Bayerisches Datenschutzgesetz, Kommentar, Art. 21 a BayDSG Anm. 9). Speziell für den Schulbereich enthält Anlage 8 „Videoaufzeichnung an Schulen" der vom Staatsministerium für Unterricht und Kultus erlassenen Verordnung zur Durchführung des Art. 28 Abs. 2 des Bayerischen Datenschutzgesetzes (im Folgenden: Durchführungsverordnung) weitere, detaillierte Vorgaben.

Daher habe ich die Schule unter Verweis auf meine Ausführungen in meinem 23. Tätigkeitsbericht, Nr. 12.2.2, darauf hingewiesen, dass die Installation einer Videokamera(attrappe) **nur in engen Grenzen zulässig** ist. So darf – neben weiteren Einschränkungen – die (vermeintliche) Videoaufzeichnung beispielsweise nur Personen betreffen, die sich im Eingangsbereich der Schule aufhalten oder sich zwischen 22:00 Uhr und 6:30 Uhr außerhalb von schulischen oder sonstigen von der Schule zugelassenen Veranstaltungen auf dem Schulgelände befinden; darüber hinaus ist eine Aufzeichnung nur außerhalb von schulischen oder sonstigen von der Schule zugelassenen Veranstaltungen an Feiertagen, an Wochenenden oder in den Ferien auf dem Schulgelände zulässig (siehe Nr. 2.5 der Anlage 8 der Durchführungsverordnung). Selbst wenn diese örtlichen und zeitlichen Grenzen gewahrt werden, setzt eine Videoaufzeichnung oder die Anbringung einer Attrappe voraus, dass dies zum Schutz der in Art. 21 a Abs. 1 Satz 1 BayDSG genannten Rechtsgüter im Einzelfall erforderlich ist. Die Schule hat daher **sorgfältig zu prüfen, ob nicht andere Aufsichts- und Überwachungsmaßnahmen sowie sonstige – insbesondere pädagogische – Mittel ausreichen.** Zudem dürfen keine Anhaltspunkte dafür bestehen, dass durch die (vermeintliche) Videoüberwachung überwiegende schutzwürdige Interessen insbesondere der Schülerinnen und Schüler beeinträchtigt werden (Art. 21 a Abs. 1 Satz 2 BayDSG). Schließlich ist es aus Gründen der Transparenz und der Akzeptanz einer derart gravierenden Maßnahme ratsam, über die in der Regel nach Art. 75 a Abs. 1 Nr. 1 BayPVG notwendige vorherige Mitbestimmung des Personalrates hinaus auch den Elternbeirat zuvor in den Entscheidungsprozess einzubeziehen.

Art. 21 a Abs. 1 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.

Nicht zuletzt aufgrund meines Einschreitens wurde die **Kameraattrappe** schließlich **wieder entfernt.** Stattdessen will die Schule nun weitere Beschädigungen der Knabentoilette insbesondere durch organisatorische Vorkehrungen und pädagogische Maßnahmen – vor allem durch zusätzliche Aufsichten – verhindern.

Im Hinblick auf die oben skizzierte Presseberichterstattung habe ich das Staatsministerium für Unterricht und Kultus sodann gebeten, im Rahmen seiner datenschutzrechtlichen Gesamtverantwortung nach Art. 25 Abs. 1 BayDSG auf die **Einhaltung der datenschutzrechtlichen Vorgaben bei der Videoüberwachung an allen staatlichen Schulen im betroffenen Landkreis** hinzuwirken. **Das Staatsministerium für Unterricht und Kultus** hat daraufhin eine umfangreiche Überprüfung vorgenommen und mir alsdann **versichert,** dass nach der Behebung von Unregelmäßigkeiten mittlerweile keine unzulässigen Videoüberwachungen mehr erfolgen.

Abschließend möchte ich aus Datenschutzsicht noch einmal betonen, dass die **Installation von Kameras oder Kameraattrappen im Schulbereich** einen **intensiven Eingriff in das Persönlichkeitsrecht** insbesondere der Schülerinnen und Schüler sowie der Lehrerinnen und Lehrer bedeutet und ein **nicht unproblematisches Signal an die Schulgemeinschaft sowie die Öffentlichkeit** sendet. Die Schulen müssen daher bei der Beurteilung der Frage, ob die Anbringung einer Kamera oder Kameraattrappe im konkreten Fall tatsächlich notwendig und angemessen ist oder ob nicht andere – insbesondere pädagogische – Maßnahmen ausreichen, gerade **aufgrund ihrer pädagogischen Verantwortung** ein **hohes Maß an Sensibilität** zeigen.

10.6 Broschüre „Datenschutz in der Schule“

Bei meinem Amtsantritt hatte ich mir zum Ziel gesetzt, Bedeutung und Tragweite des mitunter etwas sperrigen Themas „Datenschutz“ einem breit gefächerten Adressatenkreis – in erster Linie natürlich den bayerischen Bürgerinnen und Bürgern – auf anschauliche, dennoch informative Art und Weise näher zu bringen. Ich habe daher bereits im Jahre 2010 damit begonnen, zu ausgewählten, nach meiner langjährigen Erfahrung die Allgemeinheit besonders interessierenden datenschutzrechtlichen Themenkomplexen eine **Reihe kompakter und allgemein verständlicher Broschüren** aufzubauen. So habe ich nach der im Jahre 2010 erschienenen Broschüre zum Thema „Datenschutz im Krankenhaus“ im Jahre 2011 die Broschüre „Datenschutz im Rathaus“ herausgebracht. Die Broschürenreihe ist insbesondere dadurch gekennzeichnet, dass anhand der Schilderung eines zwar fiktiven, in der Praxis aber regelmäßig so oder so ähnlich vorkommenden Geschehens **konkrete Lebenssituationen aus Sicht eines Betroffenen datenschutzrechtlich beleuchtet und erläutert** werden.

Diese erfolgreiche Reihe habe ich im Jahre 2012 mit der Veröffentlichung zweier weiterer Broschüren fortgesetzt. Zur Broschüre „Datenschutz bei der Polizei“ verweise ich im Einzelnen auf meine obigen Ausführungen (siehe Nr. 3.17). An dieser Stelle möchte ich über meine neue **Broschüre „Datenschutz in der Schule“** berichten, die pünktlich zu Beginn des Schuljahres 2012/2013 erschienen ist (siehe auch meine Pressemitteilung „Mit Datenschutz durchs neue Schuljahr“ vom 10.09.2012).

Mit dieser Broschüre möchte ich **alle am Schulleben Beteiligten** gleichermaßen ansprechen, also insbesondere die Schülerinnen und Schüler, ihre Erziehungsberechtigten und die Lehrkräfte. Anhand eines fiktiven Schülers, den ich gemeinsam mit dem Leser durch ein Schuljahr begleite, werden darin schlaglichtartig **einige zentrale Datenschutzvorgaben für öffentliche Schulen** erläutert: so werden insbesondere die Themen passwortgeschützte Lernplattformen, Schulhomepage, Videoaufzeichnung, Jahresbericht und Notenverwaltung, wie ich hoffe, für den Laien verständlich beleuchtet. Nicht zuletzt möchte ich mit dieser Broschüre auch die sukzessive an den staatlichen Schulen neu einzurichtenden schulischen Datenschutzbeauftragten (siehe dazu Nr. 10.1) in ihrer Aufgabenwahrnehmung unterstützen.

Um sicherzustellen, dass die Broschüre ihren breit gefächerten Adressatenkreis tatsächlich – möglichst zu Schuljahresbeginn 2012/2013 – erreicht, habe ich mich im Vorfeld an das **Staatsministerium für Unterricht und Kultus** mit der Bitte um Unterstützung gewandt. Das Kultusministerium hat die Broschüre voll-

umfänglich begrüßt und sich umgehend dazu bereit erklärt, sie **in elektronischer Form an die bayerischen öffentlichen Schulen zu verteilen** sowie insbesondere auf der Homepage des Kultusministeriums zu verlinken. Darüber hinaus hat mir das Kultusministerium angeboten, die bayerischen Lehrerinnen und Lehrer durch einen **Gastbeitrag in der Lehrerzeitschrift „Lehrerinfo"** in gleicher Weise wie die bayerischen Schülerinnen und Schüler und ihre Erziehungsberechtigten durch einen **Hinweis in der** – immerhin in einer Auflage von 1,34 Millionen Exemplaren bayernweit an jeden Schüler in Papierform verteilten – **Elternzeitschrift „Schule & Wir"** auf die Broschüre aufmerksam zu machen; dieses Angebot habe ich gerne angenommen.

Ebenso wie die übrigen bisher erschienenen Broschüren kann auch die Broschüre „Datenschutz in der Schule" in elektronischer Form **von meiner Homepage** www.datenschutz-bayern.de **unter der Rubrik „Veröffentlichungen" heruntergeladen oder in Papierform bei meiner Geschäftsstelle angefordert** werden.

11 Personalwesen

11.1 Neuerungen im Bayerischen Beihilferecht

In meinem 23. Tätigkeitsbericht, Nr. 21.1, hatte ich ausführlich über die im Jahre 2007 erfolgte umfassende Neuordnung des Bayerischen Beihilferechts berichtet. Seit der zwischenzeitlichen Neufassung des Bayerischen Beamtengesetzes sind die grundlegenden Fragen der Beihilfe nunmehr in Art. 96 BayBG geregelt. Im Berichtszeitraum war das Beihilferecht aus datenschutzrechtlicher Sicht vor allem durch zwei Neuerungen gekennzeichnet, über die ich im Folgenden berichten will:

11.1.1 Pseudonymisierung im Psychotherapie-Begutachtungsverfahren

Wie schon in meinem 23. Tätigkeitsbericht, Nr. 21.1.5, näher ausgeführt, sind bestimmte Aufwendungen für ambulante psychotherapeutische Behandlungen u.a. nur dann beihilfefähig, wenn die Festsetzungsstelle vor Beginn der Behandlung die Beihilfefähigkeit der Aufwendungen auf Grund eines vertrauensärztlichen Gutachtens zur Notwendigkeit und zu Art und Umfang der Behandlung anerkannt hat. Im Rahmen dieses sog. psychotherapeutischen Voranerkennungsverfahrens wurden dem Gutachter bislang auch Name und Vorname des Patienten mitgeteilt. Im Gegensatz dazu erfahren die vertrauensärztlichen Gutachter im Bereich der gesetzlichen Krankenversicherung die Identität des Patienten nicht, da Name und Vorname hier durch ein Pseudonym ersetzt werden.

Gegenüber dem für das Beihilferecht innerhalb der Staatsregierung federführenden Staatsministerium der Finanzen habe ich seit Jahren – auch unter Vorlage konkreter Formulierungsvorschläge – deutlich gemacht, dass ich allein die letztgenannte, zudem mit keinem besonderen Verwaltungsaufwand verbundene Vorgehensweise für datenschutzkonform halte. Denn bei den im psychotherapeutischen Voranerkennungsverfahren an den vertrauensärztlichen Gutachter übermittelten umfangreichen Patientendaten handelt es sich nicht nur um höchst sensible und intime Angaben über Gesundheitszustand, Leben und Persönlichkeit des Patienten, der Gutachter ist auch für die Erstellung seines Gutachtens auf das Wissen um die Identität des Patienten gar nicht angewiesen.

Erfreulicherweise haben meine langjährigen nachdrücklichen Bemühungen im Berichtszeitraum doch noch zum Erfolg geführt: Im Jahre 2011 hat das Staatsministerium der Finanzen die **Pseudonymisierung im psychotherapeutischen Voranerkennungsverfahren endlich beihilferechtlich fest verankert.** Im Hinblick auf das informationelle Selbstbestimmungsrecht der betroffenen Beihilfeberechtigten und der berücksichtigungsfähigen Angehörigen erschien es mir dabei allerdings – wie zunächst vom Finanzministerium beabsichtigt – nicht ausreichend, die Pseudonymisierung allein und erstmals in der Bekanntmachung zum Vollzug der Bayerischen Beihilfeverordnung zu regeln. Diese (versteckte) Regelungsweise hätte nämlich Betroffene davon abhalten können, sich in eine notwendige psychotherapeutische Behandlung zu begeben, und wäre deshalb in Anbetracht der dem Dienstherrn obliegenden Fürsorgepflicht problematisch gewesen.

Mit Wirkung zum 01.04.2011 hat das Staatsministerium der Finanzen nunmehr – unter vollständiger Übernahme meiner Formulierungsvorschläge – **in § 9 Abs. 2 Satz 1 Nr. 3 BayBhV ausdrücklich vorgeschrieben, dass die Anforderung des vertrauensärztlichen Gutachtens durch die Festsetzungsstelle pseudonymisiert erfolgen muss;** auf diese Vorschrift wird zudem in § 11 Abs. 7 Satz 5 und § 12 Abs. 2 Satz 3 BayBhV Bezug genommen. Sodann hat das Finanzministerium diese Vorgabe unter Zugrundelegung meiner Formulierungsvorschläge in den VV-BayBhV zu § 9 Abs. 2 BayBhV im Einzelnen näher ausgeführt; dabei wurden vor allem die einschlägigen Formblätter an das neue Pseudonymisierungsverfahren angepasst.

Damit hat der Freistaat Bayern – soweit ich das überblicke – als erstes deutsches Flächenland die Pseudonymisierung im Psychotherapie-Begutachtungsverfahren im Verordnungswege eingeführt.

§ 9 Abs. 2 BayBhV Allgemeine Abrechnungsgrundlagen für psychotherapeutische Leistungen
(2) [1]Aufwendungen für psychotherapeutische Behandlungen, die zu den wissenschaftlich anerkannten Verfahren gehören und nach den Abschnitten B und G der Anlage zur Gebührenordnung für Ärzte abgerechnet werden, sind beihilfefähig, wenn

1. *sie der Feststellung, Heilung oder Linderung von seelischen Krankheiten nach Abs. 1 dienen, bei denen Psychotherapie indiziert ist,*
2. *nach einer biographischen Analyse oder Verhaltensanalyse und gegebenenfalls nach höchstens fünf, bei analytischer Psychotherapie bis zu acht probatorischen Sitzungen die Voraussetzungen für einen Behandlungserfolg gegeben sind und*
3. *die Festsetzungsstelle vor Beginn bzw. Verlängerung der Behandlung die Beihilfefähigkeit der Aufwendungen auf Grund eines auf einem pseudonymisierten Bericht der Therapeutin bzw. des Therapeuten beruhenden vertrauensärztlichen Gutachtens zur Notwendigkeit und zu Art und Umfang der Behandlung anerkannt hat.*

[2]Satz 1 gilt nicht für psychotherapeutische Behandlungen im Rahmen von stationären Krankenhaus- oder Rehabilitationsbehandlungen. [3]Für das Erstellen von Gutachten nach Satz 1 Nr. 3 benennt das Staatsministerium der Finanzen geeignete Gutachterinnen und Gutachter und gibt diese durch Verwaltungsvorschrift bekannt.

11.1.2 Datenschutzkonforme Geltendmachung von Arzneimittelrabatten

Als Art. 11 a des vom Deutschen Bundestag Ende 2010 beschlossenen Arzneimittelmarktneuordnungsgesetzes ist das Gesetz über Rabatte für Arzneimittel (im Folgenden: AMRabG) am 01.01.2011 in Kraft getreten. Dieses Gesetz verpflichtet die pharmazeutischen Unternehmer, die den gesetzlichen Krankenkassen gewährten Rabatte auf verschreibungspflichtige Arzneimittel u.a. auch den Trägern der beamtenrechtlichen Beihilfe einzuräumen. Zur Überprüfung der von den Beihilfeträgern eingeforderten Rabatte sieht § 3 AMRabG vor, dass in begründeten Fällen sowie in Stichproben ein von den pharmazeutischen Unternehmern beauftragter Treuhänder die dafür erforderlichen personenbezogenen Daten aus den einschlägigen Arzneimittelverordnungen erhalten darf.

§ 3 AMRabG Prüfung durch Treuhänder
[1]Die pharmazeutischen Unternehmer können in begründeten Fällen sowie in Stichproben die Abrechnung der Abschläge durch einen Treuhänder überprüfen lassen. [2]Hierfür dürfen an den Treuhänder die für den Prüfungszweck erforderlichen personenbezogenen Daten übermittelt werden. [3]Zum Nachweis dürfen auch Reproduktionen von digitalisierten Verordnungsblättern vorgelegt werden. [4]Der Treuhänder darf die ihm übermittelten Daten nur zum Zwecke der Überprüfung der Abrechnung der Abschläge verarbeiten und nutzen. [5]Weitere Einzelheiten der Prüfung können in der Vereinbarung nach § 2 Satz 4 geregelt werden.

Im Zuge der Umsetzung dieser bundesrechtlichen Vorschrift im bayerischen Beihilferecht hat mir das Staatsministerium der Finanzen – wenn auch zwangsläufig sehr kurzfristig – Gelegenheit zur Stellungnahme gegeben.

– In diesem Rahmen habe ich das Finanzministerium zunächst darauf hingewiesen, dass die in § 3 Satz 2 AMRabG enthaltene bundesrechtliche Befugnis zur Übermittlung personenbezogener Daten an den Treuhänder schon mangels Gesetzgebungskompetenz des Bundes keine Rechtsgrundlage für eine Übermittlung von Personalaktendaten bayerischer Beamtinnen und Beamter darstellen kann. Art. 74 Abs. 1 Nr. 27 GG gesteht dem Bund nämlich in Bezug auf die Beamten der Länder, Gemeinden und anderen Körperschaften des öffentlichen Rechts sowie auf die Richter in den Ländern nur eine konkurrierende Gesetzgebungsbefugnis im Hinblick auf die Statusrechte und -pflichten zu und nimmt hiervon insbesondere die Bereiche Besoldung und Versorgung – zu denen auch die beamtenrechtliche Beihilfe zählt – ausdrücklich aus. Auch das Personalaktenrecht der bayerischen Beamten (§ 50 BeamtStG, Art. 102 ff. BayBG) enthält keine hinreichende Rechtsgrundlage für die beabsichtigte Personalaktendatenübermittlung an den Treuhänder.

  Vor diesem Hintergrund habe ich dem Finanzministerium mitgeteilt, dass für die zur Rabattgewährung notwendige Personalaktendatenübermittlung an den Treuhänder ohne Schaffung einer speziellen landesgesetzlichen Übermittlungsbefugnis in jedem Einzelfall die Einholung der Einwilligung des jeweils betroffenen Beamten bzw. berücksichtigungsfähigen Angehörigen notwendig wäre. Dies wäre allerdings kaum praktikabel und könnte sogar die Partizipation der bayerischen Beihilfeträger an der Rabattgewährung insgesamt in Frage stellen. Daher habe ich dem Staatsministerium der Finanzen vorgeschlagen, **in Art. 105 BayBG eine nach Umfang und Zweck stark eingeschränkte Übermittlungsbefugnis** aufzunehmen. Die Staatsregierung hat daraufhin den Landtag ersucht, in Art. 105 BayBG folgenden neuen Satz 5 einzufügen:

  „[5]Die erforderlichen personenbezogenen Daten aus Arzneimittelverordnungen im Sinn des § 1 des Gesetzes über Rabatte für Arzneimittel vom 22. Dezember 2010 (BGBl I S. 2262, 2275) dürfen an den Treuhänder ausschließlich zum Zweck der Prüfung gemäß § 3 des Gesetzes über Rabatte für Arzneimittel übermittelt werden.“

– Zudem habe ich das Staatsministerium der Finanzen darum gebeten, **in Art. 110 Abs. 2 BayBG klare Regelungen zum Umgang der Beihilfestellen mit den für die Prüfung durch den Treuhänder erforderlichen Unterlagen** vorzusehen, insbesondere im Hinblick auf die Vernichtung der zu Prüfungszwecken bei den Beihilfestellen verbleibenden und nicht an

die Beihilfeberechtigten zurückzugebenden einschlägigen Arzneimittelverordnungen. Meiner Bitte entsprechend hat die Staatsregierung daraufhin dem Landtag vorgeschlagen, Art. 110 Abs. 2 BayBG um folgenden neuen Satz 3 zu erweitern:

„[3]Arzneimittelverordnungen im Sinn des § 1 des Gesetzes über Rabatte für Arzneimittel sind zur Geltendmachung von Rabatten nach diesem Gesetz nicht zurückzugeben; die Vernichtung dieser Arzneimittelverordnungen erfolgt auf der Grundlage der nach § 3 Satz 5 des Gesetzes über Rabatte für Arzneimittel zu treffenden Vereinbarungen unverzüglich, sobald sie für die dort geregelten Zwecke nicht mehr benötigt werden."

Erfreulicherweise hat der Landtag die dargestellten Regelungen der Art. 105 Satz 5 und Art. 110 Abs. 2 Satz 3 BayBG als Art. 13 des Haushaltsgesetzes 2011/2012 beschlossen; sie sind mit Wirkung vom 01.01.2011 in Kraft getreten.

11.2 Datenschutz beim Betrieblichen Eingliederungsmanagement

Gemäß § 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 Abs. 2 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.

11.2.1 Datenschutzrechtliche Anforderungen

In datenschutzrechtlicher Hinsicht ist das BEM von großer Bedeutung, da hier mit besonders sensiblen Personalaktendaten im Sinne des § 50 Satz 2 BeamtStG wie auch Gesundheitsdaten im Sinne des Art. 15 Abs. 7 BayDSG umgegangen wird. Im Berichtszeitraum haben sich daher vor allem Behörden und Personalvertretungen mehrfach mit der Bitte um Beratung an mich gewandt. Diese habe ich insbesondere auf Folgendes hingewiesen:

– Eine datenschutzkonforme Durchführung des BEM erfordert zunächst, dass die **Dienststellenleitung** oder ein(e) von ihr bestimmte(r) Personalverantwortliche(r) **ohne Hinzuziehung/Information weiterer Personen** der/dem betroffenen Bediensteten das **Angebot, ein BEM durchzuführen,** unterbreitet. Dabei ist die/der Bedienstete umfassend über das BEM, seinen Grund und seine Zielsetzung, die Art und den Umfang der hierfür erhobenen und verwendeten Daten sowie über die mögliche Teilnahme weiterer Personen zu informieren.

– Sodann ist – noch vor dem Beginn des BEM – das **Einverständnis der/des Bediensteten oder ihre/seine Ablehnung** einzuholen. Dabei ist die/der Bedienstete darauf hinzuweisen, dass ein jederzeitiges Recht zum Widerruf des Einverständnisses besteht und eine Ablehnung des BEM keine dienst- oder arbeitsrechtlichen Konsequenzen hat.

– Im Falle des Einverständnisses hat die/der Bedienstete freiwillig ihre/seine **Zustimmung/Ablehnung hinsichtlich der Teilnahme weiterer, jeweils genau bezeichneter Einzelpersonen** (z.B. Personalratsmitglied, Schwerbehindertenbeauftragte(r), Gleichstellungsbeauftragte(r), Fachvorgesetzte(r)) zu erklären. Diese Erklärungen bedürfen der Schriftform und sind jederzeit widerruflich.

– Unter diesen Voraussetzungen kommt eine Teilnahme der **Betriebsärztin**/des **Betriebsarztes** am BEM gem. § 84 Abs. 2 Satz 2 SGB IX nur in Betracht, wenn dies im Einzelfall erforderlich ist. **Externe Stellen** – dazu zählen z.B. Krankenkassen, Rentenversicherungsträger, Unfallversicherungsträger, Integrationsämter oder Arbeitsagenturen – dürfen ebenfalls nur im Einzelfall und unter der zusätzlichen Maßgabe hinzugezogen werden, dass die Teilnahme am BEM Ziel führend erscheint. Dabei muss selbstverständlich auch die Verpflichtung der teilnehmenden externen Stellen zur Verschwiegenheit sichergestellt werden. In diesem Zusammenhang weise ich zudem darauf hin, dass der Beginn des BEM nicht von der Bereitschaft der/des Bediensteten abhängig gemacht werden darf, umfassende, von den Erfordernissen des Einzelfalls losgelöste Schweigepflichtentbindungserklärungen abzugeben.

– In die **Personalakte** zwingend aufzunehmen sind nur die BEM-Grunddaten, also das Angebot, ein BEM durchzuführen, das Einverständnis bzw. die Ablehnung der/des Bediensteten und gegebenenfalls – soweit es sich hierbei um Personalaktendaten im Sinne des § 50 Satz 2 BeamtStG handelt – die Maßnahmen, die aufgrund des BEM erfolgten. Jede weitere Dokumentation setzt die ausdrückliche schriftliche Zustimmung der/des Bediensteten voraus. Soweit es sich bei der anfallenden Dokumentation nicht um Personalaktendaten handelt, ist diese in einer vor unberechtigtem

Zugriff besonders zu schützenden und in jedem Fall in der Behörde verbleibenden **Sachakte** zu führen.

– Die **Entfernung der BEM-Unterlagen** aus der Personalakte erfolgt nach den strengen Aussonderungsvorschriften des Art. 109 Abs. 1 und Art. 110 Abs. 2 BayBG (bei Tarifbeschäftigten entsprechend). Die besonders gegen unbefugte Zugriffe zu schützende BEM-Sachakte ist zeitnah nach Beendigung des BEM zu vernichten.

Art. 109 BayBG Entfernung von Unterlagen aus Personalakten
(1) [1]Unterlagen über Beschwerden, Behauptungen und Bewertungen, auf die die Tilgungsvorschriften des Disziplinarrechts keine Anwendung finden, sind
1. falls sie sich als unbegründet oder falsch erwiesen haben, mit Zustimmung des Beamten oder der Beamtin unverzüglich aus der Personalakte zu entfernen und zu vernichten,
2. falls sie für Beamte und Beamtinnen ungünstig sind oder ihnen nachteilig werden können, auf Antrag nach zwei Jahren zu entfernen und zu vernichten; dies gilt nicht für dienstliche Beurteilungen.
[2]Die Frist nach Satz 1 Nr. 2 beginnt bei neuen Sachverhalten im Sinn dieser Vorschrift oder bei Einleitung eines Straf- oder Disziplinarverfahrens erneut. [3]Der Neubeginn der Verjährung tritt nicht ein, wenn sich der neue Vorwurf als unbegründet oder falsch herausstellt.

Art. 110 BayBG Aussonderung von Personalakten
(2) [1]Unterlagen über Beihilfen, Heilfürsorge, Heilverfahren, Unterstützungen, Erholungsurlaub, Erkrankungen sowie Umzugs- und Reisekosten sind fünf Jahre nach Ablauf des Jahres, in dem die Bearbeitung des einzelnen Vorgangs abgeschlossen wurde, aufzubewahren. [2]Unterlagen, aus denen die Art der Erkrankung ersichtlich ist, sind unverzüglich zurückzugeben oder zu vernichten, wenn sie für den Zweck, zu dem sie vorgelegt worden sind, nicht mehr benötigt werden. [3]Arzneimittelverordnungen im Sinn des § 1 des Gesetzes über Rabatte für Arzneimittel sind zur Geltendmachung von Rabatten nach diesem Gesetz nicht zurückzugeben; die Vernichtung dieser Arzneimittelverordnungen erfolgt auf der Grundlage der nach § 3 Satz 5 des Gesetzes über Rabatte für Arzneimittel zu treffenden Vereinbarungen unverzüglich, sobald sie für die dort geregelten Zwecke nicht mehr benötigt werden.

– Nach § 84 Abs. 2 Satz 7 SGB IX haben die **Personalvertretung** und bei Schwerbehinderten die **Schwerbehindertenvertretung** darüber zu wachen, dass der Arbeitgeber seine Pflicht zur Durchführung des BEM erfüllt. Der Personal- bzw. Schwerbehindertenvertretung ist daher regelmäßig (z.B. im Monatsgespräch gem. Art. 67 Abs. 1 BayPVG) zu berichten. Hierbei sollte – **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.

  Aus datenschutzrechtlicher Sicht dürfen dagegen **personenbezogene Gesundheitsdaten** von Beschäftigten an die Interessenvertretungen **nur** dann weitergegeben werden, wenn hierfür schriftliche **Einwilligungen der Betroffenen** vorliegen, die sich ausdrücklich auch auf Daten über die Gesundheit beziehen (vgl. Art. 15 Abs. 1 Nr. 2, Abs. 2 bis 4, Abs. 7 Satz 1 Nr. 2 BayDSG). Allerdings ist auch bei Vorliegen entsprechender Einwilligungen

darauf zu achten, dass an die Personalvertretungen nur die zur Aufgabenerfüllung erforderlichen Daten weitergeleitet werden.

In diesem Zusammenhang mache ich darauf aufmerksam, dass das **Bundesverwaltungsgericht** in seinem Beschluss vom 23.06.2010 (Az.: 6 P 8/09) die Rechtsfrage, ob die Personalvertretung einen Anspruch darauf hat, dass ihr die Dienststelle ohne Zustimmung der jeweils Betroffenen namentlich mitteilt, welche Beschäftigten innerhalb eines Jahres länger als sechs Wochen ununterbrochen oder wiederholt arbeitsunfähig waren, ausdrücklich nicht behandelt hat. Diesem Beschluss lag vielmehr ein besonderer, nicht verallgemeinerungsfähiger Sachverhalt zugrunde. Ausdrücklich befasst mit dieser Rechtsfrage hat sich allerdings der **Bayerische Verwaltungsgerichtshof** in seinem Beschluss vom 12.06.2012 (Az.: 17 P 11.1140): mit Blick auf das Grundrecht auf informationelle Selbstbestimmung der betroffenen Beschäftigten verleiht danach § 84 Abs. 2 Satz 7 SGB IX i.V.m. Art. 69 Abs. 2 Sätze 1 und 2 BayPVG der Personalvertretung kein Recht, vom Leiter einer Dienststelle ohne die Einwilligung der Betroffenen die Bekanntgabe der Namen der Personen verlangen zu können, denen ein Betriebliches Eingliederungsmanagement angeboten wurde. Die Rechtsprechung des Bayerischen Verwaltungsgerichtshofs ist für die Beurteilung der Reichweite des Informationsanspruchs bayerischer Personalvertretungen gem. Art. 81 Abs. 2 Satz 2 BayPVG **maßgeblich**; abweichende Entscheidungen von Verwaltungsgerichten anderer Länder oder von Gerichten anderer Gerichtszweige sind insoweit unerheblich.

11.2.2 BEM-Leitfaden und BEM-Informationsfaltblatt des Staatsministeriums der Finanzen

Als praktische Hilfestellung für die Umsetzung des Betrieblichen Eingliederungsmanagements hat das innerhalb der Staatsregierung für das Dienstrecht federführende Staatsministerium der Finanzen einen ausführlichen **„Leitfaden Betriebliches Eingliederungsmanagement § 84 Abs. 2 SGB IX“** erarbeitet, der auch mehrere **Musterformulare** – Musteranschreiben zum BEM-Erstkontakt, Einverständniserklärung, Ablehnung, Datenblatt – umfasst. Primär für die Beschäftigten hat das Staatsministerium der Finanzen darüber hinaus ein **Informationsfaltblatt „Das Betriebliche Eingliederungsmanagement“** erstellt. Diese Dokumente sind im Bayerischen Behördennetz von der Seite des Staatsministeriums der Finanzen unter http://www.stmf.bybn.de/default.asp?url=abt2%2Fpe%2Feingliederungsmanagement%2F&item=209 abrufbar.

Im Zuge einer längeren Diskussion mit dem Staatsministerium der Finanzen habe ich erreichen können, dass alle der oben dargestellten **datenschutzrechtlichen Anforderungen in diese Unterlagen Eingang gefunden** haben.

Ich **empfehle** daher **allen bayerischen öffentlichen Stellen,** die vom Staatsministerium der Finanzen zur Verfügung gestellten, mit mir abgestimmten Unterlagen (Leitfaden und Informationsfaltblatt) bei der Durchführung des Betrieblichen Eingliederungsmanagements zugrunde zu legen.

11.3 Nochmals: Geltendmachung von Regressansprüchen nach einem Dienstunfall

Dienstunfallunterlagen enthalten besonders sensible Gesundheitsdaten des verunfallten Beamten und stellen damit dem Personalaktengeheimnis unterliegende Personalaktendaten im Sinne der § 50 Satz 2 BeamtStG, Art. 102 ff. BayBG dar. Vor diesem Hintergrund hatte ich bereits in meinem 23. Tätigkeitsbericht, Nr. 21.2, die vom Dienstherrn **bei der Geltendmachung von Regressansprüchen nach einem Dienstunfall zu beachtenden datenschutzrechtlichen Vorgaben** im Einzelnen erläutert. Zusammengefasst hatte ich dabei festgestellt:

– Grundsätzlich hat der Dienstherr lediglich eine – weder eine Diagnose noch einen Befund des behandelnden Arztes enthaltende – **Arbeitsunfähigkeitsbescheinigung** an den Schadensersatzpflichtigen zu übersenden.

– Falls eine solche Arbeitsunfähigkeitsbescheinigung nicht vorliegt, ist sie beim betroffenen Beamten anzufordern und sodann an den Schadensersatzpflichtigen zu übersenden.

– Nur dann, wenn weder eine Arbeitsunfähigkeitsbescheinigung noch ein sonstiger geeigneter Beleg vom betroffenen Beamten vorgelegt werden kann, darf die **Übersendung des Befundberichts** aus der Dienstunfalluntersuchung an den Schadensersatzpflichtigen erfolgen, allerdings erst nach Unkenntlichmachung aller zum Nachweis der Unfallbedingtheit nicht erforderlichen persönlichen Daten.

– Gleiches gilt hinsichtlich der zum Nachweis der unfallbedingten Heilbehandlungskosten an den Schadensersatzpflichtigen übersandten **Rechnungen des behandelnden Arztes.** Auch diese dürfen erst nach Unkenntlichmachung aller zum Nachweis der Unfallbedingtheit nicht erforderlichen persönlichen Daten an den Schadensersatzpflichtigen übersandt werden.

Die zwischenzeitlich erfolgte Neufassung des Bayerischen Beamtengesetzes (siehe hierzu 24. Tätigkeitsbericht, Nr. 11.1.1) hat nicht zu Änderungen an diesen Vorgaben geführt. Auch künftig dürfen **Dienstunfallunterlagen nur insoweit an den Schadensersatzpflichtigen übermittelt werden, als dies zur Geltendmachung von Regressansprüchen unbedingt erforderlich ist.**

Im Berichtszeitraum habe ich davon Kenntnis erlangt, dass die datenschutzrechtlichen Vorgaben von den zuständigen Behörden immer noch nicht durchgängig eingehalten werden. Um – unter Umständen sogar schwerwiegende – Datenschutzverstöße schon im Ansatz zu vermeiden, habe ich daher in erster Linie die im staatlichen Bereich zentral zuständige Behörde gebeten, unter Beachtung meiner Vorgaben eine detaillierte **Dienstanweisung für die datenschutzkonforme Regelung des Regressverfahrens bei Dienst- und sonstigen Unfällen** zu erarbeiten. Die Behörde ist meiner Bitte gefolgt und hat in dieser Dienstanweisung insbesondere ausdrücklich klargestellt, dass

– **schon innerbehördlich** die Dienstunfallstelle an die für die Geltendmachung der Regressansprüche zuständige Stelle nur die dafür konkret erforderlichen personenbezogenen Daten und Unterlagen des Verunfallten weitergeben darf, nicht benötigte – insbesondere nicht dienstunfallbe-

dingte – Angaben aber schon in diesem vorbereitenden Verfahrensstadium unkenntlich zu machen hat,

– **von der Behörde** nur die unbedingt notwendigen personenbezogenen Daten und Unterlagen des Verunfallten **an den Schadensersatzpflichtigen** bzw. dessen Versicherung – ggf. in einem abgestuften Verfahren – übermittelt werden dürfen, nicht für die Anspruchsbegründung erforderliche Angaben aber unkenntlich zu machen sind,

– die **Privatadresse** des Verunfallten **keinesfalls** an den Schadensersatzpflichtigen bzw. dessen Versicherung übermittelt werden darf und

– Informationen, die die für die Geltendmachung der Regressansprüche zuständige Stelle erlangt hat, **an die Dienstunfallstelle** grundsätzlich nur mit Einwilligung des Verunfallten weitergegeben werden dürfen. Denn das Dienstunfallverfahren wird in erster Linie im Interesse des Verunfallten, das Regressverfahren aber in erster Linie im Interesse des Dienstherrn durchgeführt.

Ich hoffe, dass mit diesen Verfahrensvorgaben die datenschutzkonforme Geltendmachung von Regressansprüchen nach einem Dienstunfall künftig zumindest im staatlichen Bereich sichergestellt ist. Die kommunalen und die sonstigen der Aufsicht des Freistaates Bayern unterstehenden Dienstherrn rufe ich dazu auf, entsprechend diesen Vorgaben zu verfahren.

11.4 Akteneinsichtsrecht eines Beamten beim Gesundheitsamt

Im Berichtszeitraum wurde ich mehrfach mit der Frage befasst, ob ein Beamter das Recht hat, die beim Gesundheitsamt über die Überprüfung seiner Dienstfähigkeit geführten Akten einschließlich des Untersuchungsauftrags des Dienstvorgesetzten einzusehen.

Zu der mit dieser Frage aufgeworfenen Problematik des **Einsichtsrechts eines Beamten in amtsärztliche Unterlagen** nehme ich aus datenschutzrechtlicher Sicht wie folgt Stellung:

– Das Recht auf Akteneinsicht könnte sich schon aus **Art. 107 Abs. 1 BayBG** ergeben. Nach dieser Vorschrift hat der Beamte ein Recht auf Einsicht in seine vollständige Personalakte; Feststellungen über den Gesundheitszustand unterliegen allerdings dann nicht der Einsicht, wenn zu befürchten ist, dass der Beamte bei Kenntnis des Befundes weiteren Schaden an seiner Gesundheit nimmt.

  Dieses Einsichtsrecht bezieht sich auf die Personalakte im materiellen Sinn, d.h. der Beamte kann in Vorgänge, die zur Personalakte im materiellen Sinn gehören, auch dann Einsicht fordern, wenn die Vorgänge nicht in die Personalakte im formellen Sinn eingeordnet sind (Weiß/Niedermaier/Summer/Zängl, Bayerisches Beamtengesetz, Kommentar, München/Berlin, Stand: 2012, Art. 107 BayBG Rdnr. 4). Zur Personalakte im materiellen Sinn gehören gemäß § 50 Satz 2 BeamtStG alle Unterlagen einschließlich der in Dateien gespeicherten, die den Beamten betreffen, soweit sie mit seinem Dienstverhältnis in einem unmittelbaren inneren Zusammenhang stehen (Personalaktendaten).

Geht man davon aus, dass die von der Fragestellung umfassten Unterlagen in einem unmittelbaren inneren Zusammenhang mit dem Dienstverhältnis des Beamten stehen – diese Auffassung wird vertreten von Weiß/Niedermaier/Summer/Zängl, a.a.O., Art. 107 BayBG Rdnr. 6 und § 50 BeamtStG Rdnr. 48; anderer Ansicht ist Kathke, Personalaktenrecht, Heidelberg, 1994, Rdnr. 96 –, ergibt sich vorliegend das Akteneinsichtsrecht bereits aus Art. 107 Abs. 1 BayBG.

– Dieser Meinungsstreit muss hier allerdings nicht entschieden werden. Denn verneint man die Zugehörigkeit der Unterlagen zu den Personalaktendaten, ergibt sich das **Recht auf Akteneinsicht jedenfalls aus Art. 107 Abs. 2 BayBG.** Nach Satz 1 Halbsatz 1 dieser Vorschrift hat der Beamte ein Recht auf Einsicht auch in andere Akten, die personenbezogene Daten über ihn enthalten und für sein Dienstverhältnis verarbeitet oder genutzt werden, soweit gesetzlich nichts anderes bestimmt ist. Die Einschränkung des Akteneinsichtsrechts in Feststellungen über den Gesundheitszustand nach Art. 107 Abs. 1 Satz 2 BayBG findet dabei meiner Auffassung nach aus Gründen der beamtenrechtlichen Fürsorge entsprechende Anwendung.

  Art. 107 Abs. 2 BayBG enthält eine **über das eigentliche Personalaktenrecht hinausreichende Regelung über die Einsichtnahme in Sachakten, soweit dort personenbezogene Daten über den Beamten enthalten sind** (Weiß/Niedermaier/Summer/ Zängl, a.a.O., Art. 107 BayBG Rdnr. 53). Für das Akteneinsichtsrecht nach Art. 107 Abs. 2 BayBG ist kein unmittelbarer innerer Zusammenhang mit dem Dienstverhältnis des Beamten erforderlich; vielmehr reicht es aus, dass die Akten für das Dienstverhältnis des Beamten verarbeitet oder genutzt werden. Dies ist schon dann der Fall, wenn sie eine Grundlage für eine dienstrechtliche Entscheidung oder eine sonstige den Beamten in seiner dienstlichen Stellung betreffenden Amtshandlung bilden oder den Grund dafür, dass eine solche unterbleibt (Weiß/Niedermaier/Summer/Zängl, a.a.O., Art. 107 BayBG Rdnr. 54).

  Die von der Fragestellung umfassten Akten einschließlich des Untersuchungsauftrags des Dienstvorgesetzten dienen der Tätigkeit des Gesundheitsamtes als Gutachter für die Behörde des Dienstvorgesetzten und sind damit eine Grundlage für deren dienstrechtliche Entscheidung über die Dienstfähigkeit des Beamten. Diese Unterlagen werden demnach – sollten sie nicht sogar Personalaktendaten sein – zumindest für das Dienstverhältnis des Beamten verarbeitet und genutzt und damit vom Akteneinsichtsrecht nach Art. 107 Abs. 2 BayBG umfasst.

– Bei dieser Sachlage kommt es somit nicht mehr darauf an, ob dem Beamten bezüglich der von der Fragestellung betroffenen Unterlagen das Akteneinsichtsrecht nach Art. 29 BayVwVfG „in die einzelnen Teile der das Verfahren betreffenden Akten“ nicht zusteht, weil etwa das Gesundheitsamt in diesen Fällen kein eigenes Verwaltungsverfahren im Sinne des Art. 9 BayVwVfG betreibt, oder ob das Akteneinsichtsrecht nach Art. 29 BayVwVfG nicht nur die unmittelbar für ein Verfahren angelegten oder beigezogenen Akten oder sonstigen Unterlagen erfasst, sondern grundsätzlich alle Akten, die mit dem Gegenstand des Verfahrens im Zusammenhang stehen und für die Entscheidung von Bedeutung sein können

(so Weiß/Niedermaier/Summer/Zängl, a.a.O., Art. 107 BayBG Rdnr. 70 m.w.N.).

Im Ergebnis ist festzustellen, dass ein Beamter ein Recht auf Einsicht in die beim Gesundheitsamt über die Überprüfung seiner Dienstfähigkeit geführten Akten einschließlich des Untersuchungsauftrags des Dienstvorgesetzten hat. Dabei kann dahingestellt bleiben, ob sich das Akteneinsichtsrecht aus Art. 107 Abs. 1 oder Abs. 2 BayBG ergibt.

Art. 107 BayBG Einsichtnahme in Personalakten
(1) [1]Beamte und Beamtinnen haben, auch nach Beendigung des Beamtenverhältnisses, ein Recht auf Einsicht in ihre vollständige Personalakte. [2]Feststellungen über den Gesundheitszustand unterliegen dann nicht der Einsicht, wenn zu befürchten ist, dass der Beamte oder die Beamtin bei Kenntnis des Befunds weiteren Schaden an der Gesundheit nimmt.
(2) [1]Beamte und Beamtinnen haben ein Recht auf Einsicht auch in andere Akten, die personenbezogene Daten über sie enthalten und für ihr Dienstverhältnis verarbeitet oder genutzt werden, soweit gesetzlich nichts anderes bestimmt ist; dies gilt nicht für Sicherheitsakten. [2]Die Einsichtnahme ist unzulässig, wenn die Daten der Betroffenen mit Daten Dritter oder geheimhaltungsbedürftigen nichtpersonenbezogenen Daten derart verbunden sind, dass ihre Trennung nicht oder nur mit unverhältnismäßig großem Aufwand möglich ist. [3]In diesem Fall ist dem Beamten oder der Beamtin Auskunft zu erteilen.
(3) [1]Bevollmächtigten von Beamten und Beamtinnen ist Einsicht zu gewähren, soweit dienstliche Gründe nicht entgegenstehen. [2]Dies gilt auch für Hinterbliebene, wenn ein berechtigtes Interesse glaubhaft gemacht wird, und deren Bevollmächtigte. [3]Für Auskünfte aus der Personalakte gelten Sätze 1 und 2 entsprechend.
(4) [1]Die personalaktenführende Behörde bestimmt, wo die Einsicht gewährt wird. [2]Soweit dienstliche Gründe nicht entgegenstehen, können Auszüge, Abschriften, Ablichtungen oder Ausdrucke gefertigt werden; Beamten und Beamtinnen ist auf Verlangen ein Ausdruck der zu ihrer Person automatisiert gespeicherten Personalaktendaten zu überlassen.

11.5 Übermittlung von Personalratswahlergebnissen an Gewerkschaften

Im Mai 2011 fanden turnusmäßig die Neuwahlen der Personalvertretungen im gesamten Geltungsbereich des Bayerischen Personalvertretungsgesetzes statt. Unmittelbar nach den Wahlen erhielt ich davon Kenntnis, dass eine Gewerkschaft in einer bayerischen öffentlichen Stelle mittels eines „Berichtsbogens zur Personalratswahl 2011“ umfangreiche personenbezogene Daten der gewählten Personalratsmitglieder über die Wahlvorstände erheben lassen wollte. Zu jedem Personalratsmitglied sollten dabei auch die Privatanschrift und die (Nicht-)Zugehörigkeit zu einer Gewerkschaft gemeldet werden. Eine Einholung der Einwilligung der Betroffenen war nicht vorgesehen.

Zu der Frage, **in welchem Umfang die Personalräte/Wahlvorstände die Ergebnisse der Personalratswahlen an die in der Dienststelle vertretenen Gewerkschaften übermitteln dürfen**, nehme ich aus datenschutzrechtlicher Sicht wie folgt Stellung:

– Der Personalrat ist ebenso wie der Wahlvorstand zur Wahl des Personalrats Teil der jeweiligen bayerischen öffentlichen Stelle; die Gewerkschaf-

ten sind hingegen als „Dritte“ im Sinne des Art. 4 Abs. 10 Satz 1 BayDSG einzuordnen. Bei der Weitergabe von personenbezogenen Personalratswahlergebnissen an Gewerkschaften handelt es sich daher um eine Übermittlung im Sinne des Art. 4 Abs. 6 Satz 2 Nr. 3 BayDSG und damit um eine Verarbeitung personenbezogener Daten.

Nach Art. 15 Abs. 1 BayDSG sind die Erhebung, Verarbeitung und Nutzung personenbezogener Daten nur zulässig, wenn das Bayerische Datenschutzgesetz oder eine andere Rechtsvorschrift sie erlaubt oder anordnet (Nr. 1) oder der Betroffene eingewilligt hat (Nr. 2).

– Als spezialgesetzliche, die allgemeinen Verarbeitungstatbestände des Bayerischen Datenschutzgesetzes gem. Art. 2 Abs. 7 BayDSG verdrängende **Rechtsgrundlage für die Übermittlung von Personalratswahlergebnissen an Gewerkschaften** kommt hier **allein Art. 23 Abs. 2 Satz 2 BayPVG** in Betracht.

Art. 23 Abs. 2 BayPVG
(2) [1]Unverzüglich nach Abschluß der Wahl nimmt der Wahlvorstand öffentlich die Auszählung der Stimmen vor, stellt deren Ergebnis in einer Niederschrift fest und gibt es den Angehörigen der Dienststelle durch Aushang bekannt. [2]Dem Dienststellenleiter und den in der Dienststelle vertretenen Gewerkschaften ist eine Abschrift der Niederschrift zu übersenden.

Nach Art. 23 Abs. 2 Satz 2 BayPVG hat der Wahlvorstand auch den in der Dienststelle vertretenen Gewerkschaften eine Abschrift der Niederschrift über das Ergebnis der öffentlichen Auszählung der Stimmen zu übersenden. Den genauen Inhalt dieser Wahlniederschrift hat die Staatsregierung in § 21 Abs. 1 Satz 2 Buchst. a) bis f) und Abs. 2 Wahlordnung zum Bayerischen Personalvertretungsgesetz (WO-BayPVG) im Einzelnen festgelegt. Über die **Zahl der auf sie entfallenen gültigen Stimmen** gem. § 21 Abs. 1 Satz 2 Buchst. e) WO-BayPVG hinaus sind im Hinblick auf die gewählten Bewerber in der Wahlniederschrift gem. § 21 Abs. 1 Satz 2 Buchst. f) WO-BayPVG nur die **Namen** festzuhalten, nicht dagegen etwa die Privatanschrift und die Gewerkschaftszugehörigkeit. Schon vom Wortlaut her handelt es sich bei den letztgenannten Daten auch nicht um „besondere Vorkommnisse“ im Sinne des § 21 Abs. 2 WO-BayPVG.

§ 21 WO-BayPVG Wahlniederschrift
(1) [1]Über das Wahlergebnis fertigt der Wahlvorstand eine Niederschrift, die von sämtlichen Mitgliedern des Wahlvorstands zu unterzeichnen ist. [2]Die Niederschrift muß enthalten
a) bei Gruppenwahl die Summe der von jeder Gruppe abgegebenen Stimmzettel und Stimmen, bei gemeinsamer Wahl die Summe aller abgegebenen Stimmzettel und Stimmen,
b) bei Gruppenwahl die Summe der von jeder Gruppe abgegebenen gültigen Stimmzettel und Stimmen, bei gemeinsamer Wahl die Summe aller abgegebenen gültigen Stimmzettel und Stimmen,
c) die Zahl der ungültigen Stimmzettel,
d) die für die Gültigkeit oder Ungültigkeit zweifelhafter Stimmzettel maßgebenden Gründe,
e) im Fall der Verhältniswahl die Zahl der auf sämtliche Bewerber einer jeden Vorschlagsliste sowie die auf die einzelnen Bewerber inner-

halb der Vorschlagsliste entfallenen gültigen Stimmen, die Errechnung der Höchstzahlen und ihre Verteilung auf die Vorschlagslisten, im Fall der Personenwahl die Zahl der auf jeden Bewerber entfallenen gültigen Stimmen,

f) die Namen der gewählten Bewerber.

(2) Besondere Vorkommnisse bei der Wahlhandlung oder der Feststellung des Wahlergebnisses sind in der Niederschrift zu vermerken.

(3) Dem Dienststellenleiter und den in der Dienststelle vertretenen Gewerkschaften übersendet der Wahlvorstand eine Abschrift der Niederschrift.

Im Ergebnis haben daher die in der Dienststelle vertretenen Gewerkschaften gegenüber dem Wahlvorstand nur einen Anspruch auf Übersendung einer Abschrift der Wahlniederschrift gem. Art. 23 Abs. 2 Satz 2 BayPVG mit dem in § 21 Abs. 1 Satz 2 und Abs. 2 WO-BayPVG festgelegten Umfang. Demzufolge dürfen die in der Dienststelle vertretenen Gewerkschaften in gewerkschaftseigenen Formularen auch nur diese Daten von den Wahlvorständen abfragen.

– Insbesondere das gesetzliche Zusammenarbeitsgebot des **Art. 2 Abs. 1 BayPVG** stellt dagegen **keine normenklare und bestimmte Rechtsgrundlage** für Eingriffe in das Grundrecht auf informationelle Selbstbestimmung dar. Im Übrigen gilt dieses Zusammenarbeitsgebot schon dem Wortlaut des Art. 2 Abs. 1 BayPVG nach selbstverständlich nur „im Rahmen der Gesetze“ und damit auch nur im Rahmen des Art. 23 Abs. 2 Satz 2 BayPVG i.V.m. § 21 Abs. 1 Satz 2 und Abs. 2 WO-BayPVG.

– Andere, über den in Art. 23 Abs. 2 Satz 2 BayPVG i.V.m. § 21 Abs. 1 Satz 2 und Abs. 2 WO-BayPVG festgelegten Umfang hinausgehende personenbezogene Daten – insbesondere der gewählten Personalratsmitglieder – dürfen die Wahlvorstände mangels gesetzlicher Rechtsgrundlage nur auf der Grundlage einer datenschutzgerechten, d.h. freiwilligen, informierten und grundsätzlich schriftlichen **Einwilligung der Betroffenen** im Sinne des Art. 15 Abs. 2 bis 4 und 7 BayDSG an die in der Dienststelle vertretenen Gewerkschaften übermitteln. Hierzu zählen insbesondere die **Privatanschrift und** die **Gewerkschaftszugehörigkeit** der gewählten Personalratsmitglieder.

11.6 Weitergabe einer Schwerbehindertenliste an den Personalrat

Im Berichtszeitraum wandte sich ein Personalratsmitglied mit der Frage an mich, ob der Personalrat zum Zwecke der Durchführung der Wahl der Schwerbehindertenvertretung von der Dienststelle die **Herausgabe einer Namensliste der schwerbehinderten Beschäftigten (Schwerbehindertenliste)** verlangen kann.

Aus datenschutzrechtlicher Sicht nehme ich zu dieser Problematik wie folgt Stellung:

– Nach allgemeinen Grundsätzen hat der Personalrat ohne Einwilligung der Betroffenen nur dann Zugang zu den in der Behörde vorhandenen personenbezogenen Daten der Beschäftigten, wenn dies durch eine Rechtsvorschrift erlaubt ist (Art. 15 Abs. 1 Nr. 1 BayDSG). Konkrete Regelungen hierzu sind in Art. 69 Abs. 2 Satz 1 BayPVG getroffen, wonach der **Perso-**

nalrat zur Durchführung seiner Aufgaben rechtzeitig und umfassend zu unterrichten ist. Ihm sind auch die hierfür erforderlichen Unterlagen zur Verfügung zu stellen (Art. 69 Abs. 2 Satz 2 BayPVG). Da der Personalrat kein allgemeines Kontrollorgan der Dienststelle ist, besteht der Informationsanspruch allerdings nur insoweit, als dies aufgrund eines bestimmten Anlasses für die Erfüllung einer konkreten Aufgabe des Personalrats erforderlich ist (zu den Informations- und Einsichtsrechten der Personalvertretung siehe eingehend meinen 20. Tätigkeitsbericht, Nr. 13.4).

– Zu den **Aufgaben des Personalrats** gehört es, **auf die Wahl der Schwerbehindertenvertretung hinzuwirken** (§ 93 Satz 2 Halbsatz 2 SGB IX). Ist in einer Dienststelle eine Schwerbehindertenvertretung nicht vorhanden, kann daher bei Vorliegen der gesetzlichen Voraussetzungen auch der Personalrat zu der für die Wahl notwendigen Versammlung einladen (siehe § 1 Abs. 2 Satz 2, § 19 Abs. 2 Wahlordnung Schwerbehindertenvertretungen – SchwbVWO).

  Die weiteren Schritte zur Durchführung der Wahl obliegen dann allerdings der Versammlung der Schwerbehinderten bzw. der Wahlversammlung und dem zu wählenden Wahlvorstand bzw. Wahlleiter; der Personalrat hat insoweit keine weiteren Mitwirkungsrechte.

  § 93 SGB IX Aufgaben des Betriebs-, Personal-, Richter-, Staatsanwalts- und Präsidialrates
  [1]Betriebs-, Personal-, Richter-, Staatsanwalts- und Präsidialrat fördern die Eingliederung schwerbehinderter Menschen. [2]Sie achten insbesondere darauf, dass die dem Arbeitgeber nach den §§ 71, 72 und 81 bis 84 obliegenden Verpflichtungen erfüllt werden; sie wirken auf die Wahl der Schwerbehindertenvertretung hin.

– Zur **Einberufung einer solchen Versammlung** ist es aus meiner Sicht nicht zwingend erforderlich, jeden einzelnen schwerbehinderten Beschäftigten persönlich zu kontaktieren. Vielmehr kann dies ohne persönliche Adressierung etwa **durch Aushang am „Schwarzen Brett" oder auf anderem geeigneten Wege** geschehen; dies ist so in der Wahlordnung Schwerbehindertenvertretungen ausdrücklich vorgesehen (siehe § 19 Abs. 1 SchwbVWO). Dementsprechend sind auch im Internet verfügbare Mustereinladungen formuliert; nur beispielhaft verweise ich hier auf die Broschüre des Zentrums Bayern Familie und Soziales zur Wahl der Schwerbehindertenvertretung (S. 54 bzw. S. 76), die von der Webseite www.zbfs.bayern.de/publikationen unter dem Link „Menschen mit Behinderung, Integrationsamt" abrufbar ist.

  Die Einberufung einer Versammlung zur Bestellung des Wahlvorstands bzw. zur Wahl der Schwerbehindertenvertretung kann daher aus Datenschutzsicht die **Nennung der Namen der schwerbehinderten Beschäftigten durch die Dienststelle an den Personalrat ohne deren Einwilligung nicht rechtfertigen.**

  § 1 Abs. 2 SchwbVWO Bestellung des Wahlvorstandes
  (2) [1]Ist in dem Betrieb oder der Dienststelle eine Schwerbehindertenvertretung nicht vorhanden, werden der Wahlvorstand und dessen Vorsitzender oder Vorsitzende in einer Versammlung der schwerbehinderten und

diesen gleichgestellten behinderten Menschen (Wahlberechtigte) gewählt. [2]Zu dieser Versammlung können drei Wahlberechtigte oder der Betriebs- oder Personalrat einladen. [3]Das Recht des Integrationsamtes, zu einer solchen Versammlung einzuladen (§ 94 Abs. 6 Satz 4 des Neunten Buches Sozialgesetzbuch), bleibt unberührt.

§ 19 SchwbVWO Vorbereitung der Wahl
(1) Spätestens drei Wochen vor Ablauf ihrer Amtszeit lädt die Schwerbehindertenvertretung die Wahlberechtigten durch Aushang oder sonst in geeigneter Weise zur Wahlversammlung ein.
(2) Ist in dem Betrieb oder der Dienststelle eine Schwerbehindertenvertretung nicht vorhanden, können drei Wahlberechtigte, der Betriebs- oder Personalrat oder das Integrationsamt zur Wahlversammlung einladen.

11.7 Speicherung von Beschäftigtendaten beim Personalrat

Vor allem Personalräte, aber auch mit Personalangelegenheiten befasste Organisationseinheiten bayerischer öffentlicher Stellen konfrontieren mich immer wieder mit der Problematik, ob, inwieweit und wie lange der Personalrat personenbezogene Daten der Beschäftigten speichern darf, die er im Rahmen von Mitbestimmungsverfahren ohne Einwilligung der Betroffenen berechtigterweise erhalten hat. Aus datenschutzrechtlicher Sicht ist die Zulässigkeit in jedem Einzelfall daran zu messen, ob die Speicherung der Beschäftigtendaten **zur Aufgabenerfüllung des Personalrats erforderlich** ist.

– Diesem Prinzip folgt letztlich **auch das Bundesverwaltungsgericht** in seinem Beschluss vom 04.09.1990, Az.: 6 P 28/87. Es legt dabei die Überlegung zugrunde, aus den differenzierten Vorschriften des Personalvertretungsrechts über die interne Weitergabe personenbezogener Beschäftigtendaten an den Personalrat seien auch Grundsätze für die Speicherung personenbezogener Beschäftigtendaten beim Personalrat ableitbar (BVerwG, a.a.O., juris Rdnr. 26 bis 28).

  Im Ergebnis nichts grundlegend anderes ergibt sich, wenn man – von der Systematik des Datenschutzrechts her meines Erachtens überzeugender – für die Frage der Speicherung Art. 17 BayDSG und für die Frage der Löschung bzw. Sperrung Art. 12 BayDSG anwendet.

– Welche konkreten Schlussfolgerungen sich aus diesem **Maßstab der Erforderlichkeit** für die Speicherung personenbezogener Beschäftigtendaten durch den Personalrat und deren Löschung bzw. Sperrung ableiten lassen, bleibt allerdings immer eine **Frage des Einzelfalls**.

  Auch das Bundesverwaltungsgericht hat sich in dem genannten Beschluss auf die Entscheidung des Einzelfalls beschränkt und festgestellt, dass im konkreten Fall einer „kleineren, überschaubaren Dienststelle von der Größenordnung einer Hundertschaft“ der Personalrat diejenigen Beschäftigtendaten, die er durch die Dienststelle anlässlich konkreter beteiligungspflichtiger Angelegenheiten erfahren hat, in der Regel „nicht darüber hinaus im automatisierten Verfahren in einer Datei“ gesondert speichern darf (BVerwG, a.a.O., juris Rdnr. 27).

– Im Grundsatz wird man festhalten können, dass regelmäßig dann Anlass zu datenschutzrechtlichen **Bedenken** besteht, wenn ein Personalrat die Erkenntnisse über Beschäftigte aus Mitbestimmungsverfahren in einer gesonderten, automatisierten Datei zusammenfasst, die **erweiterte Auswertungsmöglichkeiten** bietet.

  Auch darf es nicht dazu kommen, dass der Personalrat mit Hilfe der ihm im Rahmen des Mitbestimmungsverfahrens überlassenen Unterlagen quasi jeweils eine **zweite (automatisierte) Personalakte** aufbaut.

– Hingegen wird man es meiner Auffassung nach dem Personalrat nicht verwehren können, dass er Unterlagen, die er im Zusammenhang mit einem Mitbestimmungsverfahren erhalten hat, für eine gewisse Zeit aufbewahrt, selbst wenn diese einige personenbezogene Beschäftigtendaten enthalten sollten. Insbesondere wird der Personalrat z.B. das Anschreiben der Dienststelle in einem Mitbestimmungsverfahren anlässlich der Beförderung eines Beschäftigten und sein Antwortschreiben an die Dienststellenleitung zu seinen Akten nehmen dürfen, selbst wenn in diesen Schriftstücken die neue Besoldungs- bzw. Entgeltgruppe des Beschäftigten und ggf. sogar das Ergebnis der letzten Beurteilung enthalten ist. Denn wie bei allen anderen (Verwaltungs-)Vorgängen auch, ist dies allein schon deshalb erforderlich, um die ordnungsgemäße Abwicklung eines Verfahrens nachweisen zu können.

  Sind entgegen diesem allgemeinen Grundsatz ausnahmsweise Unterlagen unverzüglich zurückzugeben oder zu vernichten, ist eine dies anordnende gesetzliche Regelung zu erwarten (siehe etwa im Beihilfebereich Art. 110 Abs. 2 Satz 2 BayBG; eine vergleichbare Bestimmung enthält das BayPVG nicht).

  Zu berücksichtigen ist ferner, dass der Personalrat ohnehin über jede Sitzung eine Niederschrift aufzunehmen hat, die u.a. mindestens den Wortlaut der Beschlüsse zu enthalten hat (Art. 41 Abs. 1 Satz 1 BayPVG). Auch insoweit ist die **nicht nur vorübergehende Speicherung einzelner Beschäftigtendaten,** die der Personalrat im Rahmen eines Mitbestimmungsverfahrens erfahren hat, zur Aufgabenerfüllung erforderlich und damit **datenschutzrechtlich zulässig.**

11.8 Erkenntnisse aus Prüfungen städtischer Personalämter

Im Berichtszeitraum habe ich verstärkt bei städtischen Personalämtern die Einhaltung datenschutzrechtlicher Vorschriften vor Ort überprüft. Bei meinen bayernweiten Außenprüfungen konnte ich zwar regelmäßig ein ernsthaftes Bemühen um datenschutzgerechtes Verwaltungshandeln feststellen, musste aber dennoch eine nicht unerhebliche Anzahl von **Prüfungsfeststellungen** aussprechen. Diese betrafen im Wesentlichen folgende Punkte:

11.8.1 Stellung des behördlichen Datenschutzbeauftragten

Nach Art. 25 Abs. 3 Satz 1 BayDSG sind die behördlichen Datenschutzbeauftragten in dieser Eigenschaft der Leitung der öffentlichen Stelle oder deren ständigen Vertretung unmittelbar zu unterstellen; in Gemeinden können sie auch ei-

nem berufsmäßigen Gemeinderatsmitglied unterstellt werden. Gemäß Art. 25 Abs. 3 Satz 5 BayDSG sind die behördlichen Datenschutzbeauftragten zudem im erforderlichen Umfang von der Erfüllung sonstiger dienstlicher Aufgaben freizustellen. Bei den geprüften Personalämtern wurde weder dieser **Freistellungspflicht** stets ausreichend Rechnung getragen noch die **unmittelbare Zuordnung** des behördlichen Datenschutzbeauftragten **zur Behördenleitung** immer hinreichend transparent gemacht.

11.8.2 Aufbewahrung von Bewerbungsunterlagen

Bewerbungsunterlagen unterlegener Bewerberinnen und Bewerber dürfen selbstverständlich nicht im Personalakt der erfolgreichen Bewerberin oder des erfolgreichen Bewerbers aufbewahrt werden. Soweit sie nicht – was aus Datenschutzsicht ohnehin vorzugswürdig ist – an die betroffenen Bewerberinnen und Bewerber zurückgegeben werden, dürfen sie allenfalls in einem gesonderten, gegen unberechtigte Zugriffe besonders geschützten Stellenbesetzungs-Sachakt aufbewahrt werden – dies aber nur so lange, wie mit rechtlichen Maßnahmen unterlegener Bewerberinnen oder Bewerber gerechnet werden muss. In Anbetracht der in § 15 Abs. 4 Allgemeines Gleichbehandlungsgesetz vorgesehenen Frist, innerhalb der eine unzulässige Benachteiligung geltend gemacht werden muss, dürfen personenbezogene Daten unterlegener Bewerberinnen und Bewerber **regelmäßig allenfalls sechs Monate** nach Abschluss des Bewerbungsverfahrens aufbewahrt werden. Eine längere Aufbewahrung personenbezogener Bewerbungsunterlagen – insbesondere mit der mir oftmals genannten Zielsetzung, einen Bewerberpool für kurzfristig erforderliche Nach- oder Neubesetzungen vorzuhalten –, ist grundsätzlich nur mit schriftlicher Einwilligung der Betroffenen zulässig. Diese rechtlichen Vorgaben wurden von den geprüften Personalämtern nicht immer vollständig beachtet.

11.8.3 Umgang mit (elektronischen) Zeiterfassungsdaten

Zeiterfassungsdaten stellen grundsätzlich Personalaktendaten im Sinne des § 50 Satz 2 BeamtStG dar und unterliegen damit dem Gebot der doppelten Zugangsbeschränkung des Art. 103 BayBG: Zugang zu Zeiterfassungsdaten dürfen danach nur Beschäftigte haben, die im Rahmen der Personalverwaltung mit der Bearbeitung von Personalangelegenheiten beauftragt sind, und nur soweit dies zu Zwecken der Personalverwaltung oder der Personalwirtschaft erforderlich ist. Daher ist für die Überwachung der Arbeitszeiterfassung idealerweise **ein zentraler Arbeitszeitbeauftragter** durch den Dienstherrn zu bestellen. Aus datenschutzrechtlicher Sicht zwar nicht unbedingt wünschenswert, aber möglich und zulässig ist es auch, für die einzelnen Verwaltungsbereiche jeweils einen Vorgesetzten ausdrücklich zum (Teil-)Arbeitszeitbeauftragten zu bestellen und ihm für seinen Bereich die Aufgabe der Kontrolle der Arbeitszeiterfassung zu übertragen. Dieser darf dann aber auch nur auf die Zeiterfassungsdaten der Mitarbeiterinnen und Mitarbeiter seines Bereichs zugreifen (siehe hierzu 22. Tätigkeitsbericht, Nr. 19.3). In der Praxis wurde diesen strengen rechtlichen Vorgaben regelmäßig nicht umfassend Rechnung getragen.

11.8.4 Beachtung der Mitbestimmungsrechte des Personalrats

Bei meinen Prüfungen musste ich immer wieder feststellen, dass den Personalämtern die dem Personalrat nach dem Bayerischen Personalvertretungsgesetz zustehenden Beteiligungsrechte zwar durchwegs bekannt sind, deren verfahrensfehlerfreie Beachtung jedoch nicht immer sichergestellt ist. Gerade bei den Mitbestimmungsrechten gem. Art. 75 und Art. 75 a BayPVG handelt es sich jedoch im Grundsatz um **Rechtmäßigkeitsvoraussetzungen** für den Umgang mit personenbezogenen Beschäftigtendaten.

11.8.5 Personalaktenführung

Als allgemein gültige **Schutzprinzipien für alle öffentlichen Bediensteten** sind die detaillierten Regelungen des Personalaktenrechts der bayerischen Beamten (§ 50 BeamtStG und Art. 102 ff. BayBG) meiner Auffassung nach grundsätzlich auch auf die nicht-verbeamteten Beschäftigten des bayerischen öffentlichen Dienstes entsprechend anzuwenden. Leider musste ich jedoch immer wieder feststellen, dass – auch im Beamtenbereich! – den allgemeinen Geboten der § 50 BeamtStG, Art. 102 ff. BayBG nicht ausreichend Rechnung getragen wurde. Dabei möchte ich nur folgende Punkte herausgreifen:

– Entgegen Art. 104 Abs. 1 Satz 4 BayBG wurde regelmäßig in der Personalgrundakte kein vollständiges **Verzeichnis aller Teil- und Nebenakten** aufgenommen. Der vom bayerischen Gesetzgeber mit dieser Vorschrift beabsichtigte rasche und zuverlässige Überblick über den vollständigen Inhalt der Personalakte war den Betroffenen damit nicht möglich.

– Entgegen Art. 104 Abs. 2 Satz 1 BayBG wurde die **Kindergeldakte** teilweise nicht als – grundsätzlich von der Personalakte zu trennende – Sachakte geführt. Damit wurde nicht hinreichend sichergestellt, dass diese Daten – so der Wille des Gesetzgebers – nicht für allgemeine Zwecke der Personalführung und Personalplanung zur Verfügung stehen.

– Entgegen Art. 110 Abs. 4 BayBG wurden vom zuständigen öffentlichen Archiv nicht übernommene Personalakten nach Ablauf der Aufbewahrungsfrist oftmals nicht **vernichtet**, sondern nur in die Registratur oder in einen Keller verbracht.

11.8.6 Umgang mit Beihilfeunterlagen

Unterlagen über Beihilfen enthalten besonders vertraulich zu behandelnde sensible Gesundheitsdaten im Sinne des Art. 15 Abs. 7 BayDSG. Der Gesetzgeber hat daher in Art. 105 Satz 4 BayBG Beihilfeunterlagen einer strikten Zweckbindung unterworfen. Zur Absicherung hat der Gesetzgeber in Art. 105 Sätze 1 bis 3 BayBG angeordnet, dass Beihilfeunterlagen in einer von der übrigen Personalakte getrennt aufzubewahrenden Teilakte zu führen sind und in einer von der übrigen Personalverwaltung getrennten Organisationseinheit bearbeitet werden sollen (siehe hierzu 17. Tätigkeitsbericht, Nr. 12.2). Bei meinen Prüfungen habe ich jedoch festgestellt, dass die danach notwendige **Eigenständigkeit der Beihilfestelle** – von der Sachbearbeitung bis hin zur verantwortlichen Schlusszeichnung – nicht immer durchgehend gewahrt und auch – etwa anhand von Organigramm oder Türschildern – nicht stets erkennbar war. Zudem war im Verfahren

der Beihilfeantragstellung eine Kenntnisnahme von Dritten nicht immer hinreichend sicher ausgeschlossen. Insoweit habe ich u.a. die Weitergabe von Beihilfeunterlagen von Hand zu Hand oder in einem verschlossenen Umschlag mit dem Vermerk „Vertrauliche Beihilfeunterlagen“ empfohlen.

11.8.7 Veröffentlichung personenbezogener Beschäftigtendaten im Internet

Zu einer sach- und zeitgerechten behördlichen Aufgabenerfüllung gehört auch die Information der Öffentlichkeit über die zuständigen Ansprechpartner. Eine auf die Öffentlichkeit bezogene Aufgabenstellung kommt allerdings nur **Bediensteten** zu, die **Funktionen mit „Außenwirkung“** wahrnehmen; diese müssen es hinnehmen, dass ihre dienstlichen Kommunikationsdaten wie etwa Name, Amts- und Dienstbezeichnung, Tätigkeitsbereich, Funktion, dienstliche Anschrift, Telefonnummer und E-Mail-Adresse im Internet veröffentlicht werden. Bei städtischen Personalämtern wird eine solche Außenwirkung regelmäßig bei Dezernent(inn)en sowie Amts- und Abteilungsleiter(inne)n gegeben sein. Personenbezogene Daten von sonstigen Beschäftigten dürfen dagegen regelmäßig erst nach vorheriger Einholung von datenschutzgerechten Einwilligungen veröffentlicht werden; aufgrund der damit verbundenen Gefahren für das informationelle Selbstbestimmungsrecht der Beschäftigten rate ich jedoch grundsätzlich hiervon ab (siehe hierzu zuletzt meinen 23. Tätigkeitsbericht, Nr. 21.4).

11.8.8 Weitergabe von Bewerberdaten an kommunale Entscheidungsgremien

Ab einer bestimmten Stelleneinstufung wird in allen geprüften Städten die konkrete Einstellungsentscheidung nicht mehr vom städtischen Personalamt selbst, sondern von einem kommunalen Gremium – Stadtrat oder Personalausschuss – getroffen. Bei der Behandlung von Personalentscheidungen in einem kommunalen Gremium ist ein angemessener Ausgleich zu finden zwischen dem berechtigten Informationsbedürfnis der Gremiumsmitglieder einerseits und dem Recht auf informationelle Selbstbestimmung der Stellenbewerber andererseits. Daher dürfen dem Gremium personenbezogene Daten von Stellenbewerbern **nur** in dem Umfang mitgeteilt werden, der **zur Beschlussfassung erforderlich** ist. Dies wird regelmäßig nicht bei den vollständigen Bewerbungsunterlagen, sondern nur bei den darin enthaltenen Grunddaten der Fall sein.

11.8.9 Ausblick

Ich hoffe, dass diese Kurzübersicht schon jetzt dazu beiträgt, das Bewusstsein für wesentliche personaldatenschutzrechtliche Anforderungen bei den bayerischen Personalverwaltungen zu schärfen.

Jedenfalls meine Prüfungen städtischer Personalämter werde ich auch in Zukunft fortsetzen.

12 Spezielle datenschutzrechtliche Themen

12.1 Gesetz zur Optimierung der Geldwäscheprävention

Der Bundestag hat Ende 2011 das Gesetz zur Optimierung der Geldwäscheprävention verabschiedet.

Ein erster Gesetzesentwurf sah zunächst vor, dass bereits beim Erwerb von E-Geld-Kleinstbeträgen umfangreiche Kundendaten zu erheben seien. Dies hätte eine verdachtsunabhängige, undifferenzierte und schrankenlose Datenerfassung zur Folge gehabt.

Aus diesem Grund befassten sich die Datenschutzbeauftragten des Bundes und der Länder auf ihrer 82. Konferenz im Herbst 2011 in München mit dem Thema und verabschiedeten die Entschließung „Anonymes elektronisches Bezahlen muss möglich bleiben!".

Entschließung der 82. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 28./29.09.2011
„Anonymes elektronisches Bezahlen muss möglich bleiben!"

Die Datenschutzbeauftragten des Bundes und der Länder fordern den Bundesgesetzgeber auf, bei der Bekämpfung von Geldwäsche auf umfassende und generelle Identifizierungspflichten beim Erwerb von elektronischem Geld zu verzichten. Ein aktueller Gesetzentwurf der Bundesregierung zum Geldwäschegesetz (BT-Drs. 17/6804) sieht vor, über bereits bestehende – allerdings nicht umgesetzte – gesetzliche Verpflichtungen hinaus umfangreiche Daten über sämtliche Erwerber elektronischen Geldes zu registrieren. Der anonyme Erwerb von E-Geld würde damit generell abgeschafft.

Dies ist besonders kritisch, da umfangreiche Kundinnen- und Kundendaten unabhängig vom Wert des E-Geldes erhoben werden müssen. Beispielsweise ist eine Tankstelle bereits beim Verkauf einer E-Geld Karte im Wert von fünf Euro verpflichtet, den Namen, das Geburtsdatum und die Anschrift der Kundinnen und Kunden zu erheben und für mindestens fünf Jahre aufzubewahren.

Eine generelle Identifizierungspflicht würde außerdem dazu führen, dass anonymes Einkaufen und Bezahlen im Internet selbst bei Bagatellbeträgen praktisch ausgeschlossen werden. Anonyme Bezahlsysteme im Internet bieten ihren Nutzern jedoch Möglichkeiten, die Risiken eines Missbrauchs ihrer Finanzdaten beispielsweise durch Hackerangriffe zu minimieren. Sie sind zugleich ein wichtiger Baustein, um die Möglichkeit zum anonymen Medienkonsum zu erhalten, da Online-Medien zunehmend gegen Bezahlung angeboten werden. Auf jeden Fall muss verhindert werden, dass personenbeziehbare Nutzungsdaten über jeden einzelnen Artikel in Online-Zeitungen oder einzelne Sendungen im Internet-TV schon immer dann entstehen, wenn eine Nutzung gebührenpflichtig ist.

Nach den vorgesehenen Regelungen würden noch mehr personenbezogene Daten unbescholtener Bürgerinnen und Bürger erfasst und ganz überwiegend anlasslos gespeichert. Dies steht in Widerspruch zur Rechtsprechung des Bundesverfassungsgerichts. In seinem Urteil zur Vorratsdatenspeicherung von Telekommunikationsdaten vom 02.03.2010 (1 BvR 256/08) hatte das Gericht gemahnt, dass Gesetze, die auf eine möglichst flächendeckende vorsorgliche Speicherung aller für die Strafverfolgung oder Gefahrenprävention nützlichen Daten zielen, mit der Verfassung unvereinbar sind.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder lehnt die vorgesehene verdachtsunabhängige, undifferenzierte und schrankenlose Datenerfassung ab, die auch europarechtlich nicht geboten ist. Die dritte Geldwäscherichtlinie (2005/60/EG) erlaubt den Mitgliedstaaten, von Identifizierungspflichten abzusehen, wenn der Wert des erworbenen elektronischen Guthabens 150 Euro nicht übersteigt. Der Bundesgesetzgeber sollte durch Einführung eines entsprechenden Schwellenwerts diesem risikoorientierten Ansatz folgen.

Die von der Konferenz geäußerten Bedenken wurden im Gesetzgebungsverfahren zumindest teilweise aufgegriffen. Das Gesetz sieht nunmehr eine Identifizierungspflicht erst ab einem Schwellenwert von 100 Euro pro Monat vor.

12.2 Verlängerung von Ausschreibungen im Schengener Informationssystem

Auch im Berichtszeitraum habe ich wieder Datenspeicherungen zu Drittausländern, die nach Art. 96 Abs. 3 des Schengener Durchführungsübereinkommens (SDÜ) zur Einreiseverweigerung im Schengener Informationssystem (SIS) ausgeschrieben wurden, auf ihre Rechtmäßigkeit hin überprüft. Die Datenerfassung im SIS ist zunächst auf drei Jahre befristet, kann jedoch gemäß Art. 112 Abs. 1 und 2 SDÜ verlängert werden (vgl. Nr. 5.5.4.2.3 der Allgemeinen Verwaltungsvorschrift zum Aufenthaltsgesetz). Im Rahmen meiner Prüfungen habe ich wiederholt festgestellt, dass Ausländerbehörden SIS-Ausschreibungen nach Ablauf dieser drei Jahre automatisch verlängerten, ohne dass geprüft wurde, ob eine Verlängerung der SIS-Ausschreibung für den der Ausschreibung zugrunde liegenden Zweck erforderlich war.

Auf meine Bitte hin hat das Bayerische Staatsministerium des Innern die nachgeordneten Behörden darauf hingewiesen, dass die Erforderlichkeit der weiteren Ausschreibung schon bei der erstmaligen Verlängerung zu überprüfen ist (Art. 112 Abs. 1 Satz 2 SDÜ). Als Ergebnis der Prüfung kann die Ausländerbehörde beschließen, die Ausschreibung noch beizubehalten, wenn dies für den zugrundeliegenden Zweck weiter erforderlich ist (Art. 112 Abs. 4 Satz 1 SDÜ). Dies setzt – wie bereits die Erstausschreibung – eine individuelle Prüfung und Entscheidung voraus, ob und wie lange eine weitere Ausschreibung erfolgen soll. Die Entscheidung und ihre Gründe sind im Akt zu dokumentieren. Falls nach der Prüfung keine Notwendigkeit einer weiteren Speicherung gesehen wird, ist die Löschung zu veranlassen.

Artikel 112 Abs. 1 und 4 SDÜ
(1) Die zur Personenfahndung in dem Schengener Informationssystem aufgenommenen personenbezogenen Daten werden nicht länger als für den verfolgten Zweck erforderlich gespeichert. Spätestens drei Jahre nach ihrer Einspeicherung ist die Erforderlichkeit der weiteren Speicherung von der ausschreibenden Ver-

tragspartei zu prüfen. Für die Ausschreibung gemäß Artikel 99 beträgt diese Frist ein Jahr.
(4) Die ausschreibende Vertragspartei kann innerhalb der Prüffrist beschließen, die Ausschreibung noch beizubehalten, wenn dies für den der Ausschreibung zugrunde liegenden Zweck erforderlich ist. Eine Verlängerung der Ausschreibung ist in die technische Unterstützungseinheit einzugeben. Absatz 1 gilt entsprechend.

12.3 Nochmals: Einheitlicher Ansprechpartner nach der EU-Dienstleistungsrichtlinie

Wie schon in meinem letzten Tätigkeitsbericht eingehend erläutert, ist die im Anwendungsbereich der Richtlinie 2006/123/EG über Dienstleistungen im Binnenmarkt geforderte und mit dem Gesetz über die Zuständigkeit für die Aufgaben des Einheitlichen Ansprechpartners im Freistaat Bayern vom 22.12.2009 umgesetzte Schaffung sogenannter Einheitlicher Ansprechpartner datenschutzrelevant, da neben der eigentlichen Genehmigungsbehörde eine neue zusätzliche Stelle in das Genehmigungsverfahren eingeführt wird, welche eine Vielzahl personenbezogener Daten erhebt und verarbeitet (siehe hierzu 24. Tätigkeitsbericht, Nr. 12.2). Aus datenschutzrechtlicher Sicht war es insbesondere wichtig, den Umgang mit dem beim Einheitlichen Ansprechpartner entstehenden Datenpool klar zu regeln. Insoweit habe ich erreicht, dass in § 5 Abs. 1 der Verordnung zur Ausführung des Gesetzes über die Zuständigkeit für die Aufgaben des Einheitlichen Ansprechpartners im Freistaat Bayern vom 28.04.2010 (AVBayEAG) ausdrücklich klargestellt wurde, dass der Einheitliche Ansprechpartner personenbezogene Daten getrennt von anderen Verfahren/Aufgaben verarbeiten muss.

§ 5 AVBayEAG
(1)[1] Personenbezogene Daten aus sachlich nicht zusammengehörenden Verwaltungsvorgängen sind getrennt voneinander zu verarbeiten. [2] Handelt es sich beim Einheitlichen Ansprechpartner zugleich um die für die Antragsbearbeitung zuständige Behörde, müssen auch bei sachlich zusammengehörenden Verwaltungsvorgängen personenbezogene Daten getrennt nach dem jeweiligen Aufgabenbereich verarbeitet werden.

Dieses Gebot der **getrennten Datenverarbeitung** ist vornehmlich dann von besonderer Bedeutung, wenn Einheitlicher Ansprechpartner und für die eigentliche Antragsbearbeitung zuständige Behörde identisch sind. In diesen Fällen darf kein einheitlicher zentraler Datenbestand gebildet werden, sondern entsprechend allgemeiner datenschutzrechtlicher Grundsätze darf ein Zugriff auf personenbezogene Daten immer nur im Rahmen des für die konkrete Aufgabenerfüllung Erforderlichen möglich sein. Vor diesem Hintergrund weise ich insoweit aus aktuellem Anlass ergänzend auf Folgendes hin:

– Nach dem in Bayern seit jeher vertretenen organisatorischen Behördenbegriff (vgl. Wilde/Ehmann/Niese/Knoblauch, Bayerisches Datenschutzgesetz, Art. 2 Rdnr. 8 ff.) stellt auch eine solche Behörde mit Doppelfunktion als Einheitlicher Ansprechpartner (EA) und Zuständige Stelle (ZS) eine **einheitliche öffentliche Stelle** im Sinne des Art. 4 Abs. 2 Satz 1 BayDSG dar.

– Das Speichern personenbezogener Daten stellt eine Datenverarbeitung im Sinne des Art. 4 Abs. 6 Satz 2 Nr. 1 BayDSG dar, weswegen in der öffentlichen Stelle EA-Daten und ZS-Daten **getrennt gespeichert** werden müssen.

– Erkanntermaßen irrtümlich an die öffentliche Stelle in ihrer EA-Funktion gerichtete – personenbezogene Daten enthaltende – Anfragen (Pseudo-EA-Fälle) dürfen nicht weiterhin im EA-Teil der Datenbank gespeichert werden.

– Ist jedoch in einem solchen **Pseudo-EA-Fall** eine ZS-Zuständigkeit der öffentlichen Stelle gegeben, so müssen die irrtümlich im EA-Teil der Datenbank gespeicherten Daten nicht sofort gemäß Art. 12 Abs. 1 Nr. 2 BayDSG gelöscht werden, da deren Kenntnis noch für die Erfüllung der ZS-Aufgaben der einheitlichen öffentlichen Stelle erforderlich sein kann.

– Bevor die Daten jedoch in dieser Funktion verarbeitet werden dürfen, müssen sie in **den ZS-Teil der Datenbank übertragen werden**. Datenschutzrechtlich handelt es sich insoweit um eine Datennutzung im Sinne des Art. 4 Abs. 7 BayDSG innerhalb einer einheitlichen öffentlichen Stelle.

– Diese Datennutzung wird in aller Regel nicht auf Art. 17 Abs. 1 BayDSG gestützt werden können, da die Daten nicht für die ZS-Funktion, sondern für die EA-Funktion erhoben wurden, womit eine der Datennutzung grundsätzlich schädliche Zweckänderung im Sinne des Art. 17 Abs. 1 Nr. 2 BayDSG vorliegt. Damit wird im Ergebnis wohl regelmäßig nur die Einholung von **Einwilligungen** im Sinne des Art. 17 Abs. 2 Nr. 2 i.V.m. Art. 15 Abs. 1 Nr. 2 BayDSG der Betroffenen die **Übertragung der Daten vom EA-Teil der Datenbank in dessen ZS-Teil rechtfertigen können**.

12.4 Volkszählung 2011

Bereits seit Jahren bin ich mit der Volkszählung 2011 intensiv befasst. In früheren Berichtszeiträumen habe ich vor allem über die gesetzgeberischen Vorarbeiten auf Bundes- und Landesebene berichtet, die ich aus datenschutzrechtlicher Sicht eingehend begleitet habe (siehe hierzu 24. Tätigkeitsbericht, Nr. 12.1, 23. Tätigkeitsbericht, Nr. 23.3, und 22. Tätigkeitsbericht, Nr. 21.5).

Im aktuellen Berichtszeitraum fanden nunmehr die **Erhebungen zum Stichtag 09.05.2011** statt. Die Bürgerinnen und Bürger sind damit unmittelbar mit dem Zensus in Berührung gekommen. **Schwerpunkt meiner Tätigkeit war es, die Einhaltung der datenschutzrechtlichen Vorgaben bei den Befragungen und bei der Bearbeitung der gesammelten Daten zu überwachen.** Dabei stand ich in laufendem und engem Kontakt mit dem Landesamt für Statistik und Datenverarbeitung. Zudem habe ich in einer Arbeitsgruppe der Datenschutzbeauftragten des Bundes und der Länder mitgewirkt, um die bei der Durchführung des Zensus 2011 auftretenden datenschutzrechtlichen Fragen auch bundesweit einer Lösung zuzuführen.

Die **rechtlichen Grundlagen des Zensus 2011** wurden vor allem im „Gesetz über den registergestützten Zensus im Jahre 2011 (Zensusgesetz 2011)“, im „Gesetz zur Vorbereitung eines registergestützten Zensus einschließlich einer Gebäude- und Wohnungszählung 2011 (Zensusvorbereitungsgesetz 2011)“

sowie in Abschnitt V des Bayerischen Statistikgesetzes (BayStatG) geschaffen. Das **Bundesverfassungsgericht** hat Ende 2010 mehrere gegen das Zensusgesetz 2011 gerichtete Verfassungsbeschwerden nicht zur Entscheidung angenommen und damit das Zensusgesetz 2011 **nicht für verfassungswidrig erklärt** (siehe nur Beschluss vom 21.09.2010, Az.: 1 BvR 1865/10).

12.4.1 Keine grundlegenden datenschutzrechtlichen Mängel

Im Ergebnis konnte ich in Bayern **bislang keine gravierenden datenschutzrechtlichen Mängel** feststellen. Das Landesamt für Statistik und Datenverarbeitung zeigte erfreulicherweise ein hohes Maß an Sensibilität für die Belange des Datenschutzes. Auch die Arbeit der örtlichen Erhebungsstellen gab keinen Anlass zu grundlegenden Bedenken. Kleinere Unregelmäßigkeiten – wie etwa der mehrmalige oder unberechtigte Versand von Fragebögen, Erinnerungsschreiben oder Mahnungen – sind bei einem Projekt dieser Größenordnung praktisch nicht vermeidbar und wurden auf meine Nachfrage hin jeweils umgehend aufgeklärt und bereinigt.

Wie zu erwarten war, hat mich eine **Vielzahl von Anfragen besorgter Bürgerinnen und Bürger** erreicht. Gleichwohl bleibt festzuhalten, dass diese Anfragen – weder von der Anzahl noch von der Gewichtigkeit her – bei weitem nicht jenen Umfang angenommen haben, der im Zusammenhang mit der Volkszählung 1987 zu beobachten war.

12.4.2 Statistikgeheimnis und Rückspielverbot

Die Volkszählung 2011 wird von den statistischen Ämtern des Bundes und der Länder einheitlich durchgeführt. Sie ist – anders als die Volkszählung 1987 – nicht als Totalerhebung durch Befragung jedes einzelnen Bürgers, sondern als sog. **„registergestützter Zensus"** ausgestaltet. Dies bedeutet, dass die notwendigen Basisinformationen zunächst den bei der Verwaltung vorhandenen Registern entnommen werden: in erster Linie den Melderegistern der Kommunen, den Datensätzen der Bundesagentur für Arbeit über die sozialversicherungspflichtig beschäftigten Erwerbstätigen und den Datensätzen der öffentlichen Dienstherren über ihre Bediensteten. Ergänzt werden diese Daten durch eine schriftliche Befragung aller Gebäude- und Wohnungseigentümer, durch Erhebungen in sog. „Sonderbereichen" (vor allem Heime und Anstalten) und durch eine Stichprobenbefragung von etwas weniger als 10 % der Bevölkerung.

In diesem Zusammenhang wurden zahlreiche, **teilweise sehr sensible personenbezogene Daten erhoben.** Bei allen Befragungen bestand – außer bei der Frage nach dem Merkmal „Bekenntnis zu einer Religion, Glaubensrichtung oder Weltanschauung" im Rahmen der Stichprobenbefragung – eine Auskunftspflicht (§ 18 Zensusgesetz 2011). Die erhobenen Daten unterliegen einem umfassenden gesetzlichen Schutz. Wie bei allen amtlichen Statistiken in Deutschland und in Bayern sind die personenbezogenen Zensuseinzeldaten **gemäß dem in § 16 BStatG und Art. 17 BayStatG verankerten Statistikgeheimnis geheim zu halten.** Sie dürfen nach den dort aufgestellten Maßgaben nur für statistische Zwecke verwendet und weder an die Polizei noch an das Finanzamt oder sonst eine Vollzugsbehörde weitergegeben werden. Dieses **Gebot der strikten Trennung von Statistik und Verwaltungsvollzug** (sog. „Rückspielverbot") war eine der Kernforderungen des Bundesverfassungsgerichts im sog. „Volkszählungsurteil"

aus dem Jahre 1983. Eine Weitergabe der personenbezogenen Daten an privatwirtschaftliche Unternehmen ist nach den genannten Vorschriften ebenfalls untersagt. Verstöße gegen die statistische Geheimhaltung werden strafrechtlich verfolgt (§ 203 StGB).

Im Rahmen meiner Kontrollen beim Landesamt für Statistik und Datenverarbeitung sowie bei acht örtlichen Erhebungsstellen konnte ich mich davon überzeugen, dass die **notwendigen technischen und organisatorischen Vorkehrungen zur Einhaltung des Statistikgeheimnisses getroffen** wurden. Größere Probleme sind mir nicht bekannt geworden.

12.4.3 Informationsfaltblatt „Zensus 2011“ des Landesbeauftragten

Sowohl für die Akzeptanz als auch für das Vertrauen in das Bestehen hinreichender rechtlicher, technischer und organisatorischer Datenschutzregelungen – einschließlich einer effektiven Datenschutzkontrolle – ist es von entscheidender Bedeutung, dass die Bürgerinnen und Bürger möglichst umfassend und in verständlicher Form über den Zensus 2011 informiert werden. Im Vorfeld der Haushaltebefragung habe ich daher ein vierseitiges **Informationsfaltblatt „Zensus 2011“** erarbeitet, in dem ich die **für die Bürgerinnen und Bürger wichtigsten Fragen allgemein beantwortet** habe. Hier habe ich insbesondere den Ablauf des registergestützten Verfahrens, den Umfang der Auskunftsverpflichtung und die datenschutzrechtlichen Schutzregelungen knapp und übersichtlich erläutert. Das Papier wurde in einer **Auflage von 40.000 Stück** vervielfältigt und insbesondere **allen etwa 16.000 in Bayern eingesetzten Erhebungsbeauftragten persönlich zur Information und auch zur Weitergabe zur Verfügung gestellt.** Das Informationsfaltblatt ist selbstverständlich auch jetzt noch von meiner Homepage www.datenschutz-bayern.de unter der Rubrik „Themen“ – „Statistik“ abrufbar.

12.4.4 Erhebungsstellen und Erhebungsbeauftragte

Wie bei flächendeckenden Großzählungen üblich, wurden die Befragungen vor Ort von Erhebungsstellen durchgeführt, die bei den kreisfreien Städten und den Landkreisen eingerichtet wurden. Diese örtlichen Erhebungsstellen setzten hierzu ehrenamtliche Erhebungsbeauftragte ein. Insgesamt waren **in Bayern 92 örtliche Erhebungsstellen und etwa 16.000 Erhebungsbeauftragte** im Einsatz, die ab dem Stichtag 09.05.2011 **knapp 1,2 Millionen bayerische Bürgerinnen und Bürger befragt** haben. Die rechtlichen Grundlagen der örtlichen Erhebungsstellen und Erhebungsbeauftragten sind in §§ 10, 11 Zensusgesetz 2011 und in Art. 27 bis 30 BayStatG enthalten.

Die Anforderungen der statistischen Geheimhaltung sind selbstverständlich auch von den örtlichen Erhebungsstellen und Erhebungsbeauftragten einzuhalten. Dies bedeutet insbesondere, dass die **Erhebungsstellen räumlich, organisatorisch, technisch und personell von den anderen Bereichen der öffentlichen Verwaltung getrennt eingerichtet** werden mussten. Die Erhebungsbeauftragten waren, soweit sie nicht bereits Amtsträger sind, auf die Wahrung des Statistikgeheimnisses nach § 16 BStatG und Art. 17 BayStatG zu verpflichten, um die Strafbewehrung nach § 203 StGB sicherzustellen.

In diesem Zusammenhang hat das Landesamt für Statistik und Datenverarbeitung den kreisfreien Städten und Landkreisen konkrete **Hinweise zur Einrichtung und insbesondere zur Abschottung der Erhebungsstellen vom Verwaltungsvollzug sowie zur Auswahl der Erhebungsbeauftragten** an die Hand gegeben. Die Hinweise wurden mit mir abgestimmt. Danach sollte bei der Bestellung öffentlich Bediensteter zu Erhebungsbeauftragten insbesondere auf die **Vermeidung von Interessenkonflikten** geachtet werden (beispielhaft wurden die Bereiche Einwohnermeldeamt, Steueramt, Ausländeramt, Sozialamt und Polizei genannt). Bei Bewerbern außerhalb des öffentlichen Dienstes sollten Kollisionen mit potentiellen kommerziellen Interessen (so z.B. bei Versicherungsvertretern) schon im Ansatz ausgeschlossen werden. In diesem Zusammenhang wurde ein Musterschreiben („Teilnahmeerklärung für eine Interviewertätigkeit") entwickelt, in dem die Bewerber auch Fragen zur ausgeübten Berufstätigkeit zu beantworten hatten. Des Weiteren sollten die **Erhebungsbeauftragten nicht in unmittelbarer Nähe ihrer Wohnung eingesetzt** werden. Für Bürgerinnen und Bürger, die gleichwohl eine Kenntnisnahme der Daten durch die Erhebungsbeauftragten vermeiden wollten, bestand die Möglichkeit, die Auskünfte im Wesentlichen schriftlich (per Brief oder durch Übergabe im verschlossenen Umschlag an die Erhebungsbeauftragten) oder im Rahmen eines elektronischen Übertragungsverfahrens zu erteilen (§ 18 Abs. 4 Zensusgesetz 2011).

Die Tätigkeit der Erhebungsstellen und Erhebungsbeauftragten war Gegenstand eines Großteils der bei mir eingegangenen Anfragen und Beschwerden. Dabei habe ich in jedem Einzelfall das Landesamt für Statistik und Datenverarbeitung oder die betroffene örtliche Erhebungsstelle um Aufklärung gebeten. Im Ergebnis konnte ich keine diesen Stellen zurechenbare wesentliche Verstöße gegen gesetzliche Vorgaben feststellen. In einem Fall hat ein Erhebungsbeauftragter das im Rahmen des Zensus erlangte Wissen zwar für eigene privatwirtschaftliche Zwecke genutzt; allerdings ergaben meine Untersuchungen hier keine Anhaltspunkte für ein Auswahlverschulden der Erhebungsstelle.

Einige Eingaben hatten auch das den Auskunftspflichtigen vom Landesamt für Statistik und Datenverarbeitung alternativ zur Verfügung gestellte **elektronische Auskunftserteilungsverfahren** gem. § 18 Abs. 4 Zensusgesetz 2011 zum Gegenstand. So beschwerten sich mehrere Bürgerinnen und Bürger bei mir darüber, dass sie vom Landesamt für Statistik und Datenverarbeitung zur Rücksendung ihrer Fragebögen aufgefordert wurden, obwohl sie bereits online Auskunft erteilt hätten. Nach genauer Überprüfung durch das von mir um Stellungnahme gebetene Landesamt für Statistik und Datenverarbeitung stellte sich aber jeweils heraus, dass die Betroffenen nach Ausfüllen des Fragebogens irrtümlich bereits die sogenannte „Druckansicht" als Quittung für eine Datenübermittlung angesehen hatten und daher nicht den „Sende"-Knopf betätigt hatten. Somit hatten sie ihre Daten letztlich nicht an das Landesamt für Statistik und Datenverarbeitung übermittelt. Meine eigenen weiteren Nachprüfungen haben diese Darstellung bestätigt.

12.4.5 Vernichtung der Erhebungsbögen und Löschung der Hilfsmerkmale

Die **Erhebungsbögen** wurden vom Landesamt für Statistik und Datenverarbeitung bei den örtlichen Erhebungsstellen abgeholt und bayernweit zentral in Fürth ausgewertet.

Um einen Personenbezug auf das Nötigste zu beschränken, ist es aus datenschutzrechtlicher Sicht besonders wichtig, dass die Namen und Adressen – die sog. „Hilfsmerkmale" – zum frühestmöglichen Zeitpunkt von den eigentlichen, dauerhaft gespeicherten statistischen Daten – den sog. „Erhebungsmerkmalen" – getrennt und gelöscht werden. Die **Löschung der Hilfsmerkmale** ist **gesetzlich** in § 19 Zensusgesetz 2011 **bis spätestens vier Jahre nach dem Berichtszeitpunkt 09.05.2011 vorgegeben.** Zentrale Frage ist dabei, ab wann die Hilfsmerkmale für die Durchführung und Kontrolle der Erhebungen nicht mehr erforderlich sind. Ich habe daher **vom Landesamt für Statistik und Datenverarbeitung die Vorlage eines Löschkonzepts gefordert,** um Klarheit über das Verfahren zur Löschung der Hilfsmerkmale zu erhalten. Leider gibt es ein derartiges Konzept bislang nicht. Ich werde diese Problematik aber sehr genau im Auge behalten.

§ 19 Zensusgesetz 2011 Löschung
(1) [1]Die Hilfsmerkmale sind von den Erhebungsmerkmalen zum frühestmöglichen Zeitpunkt zu trennen und gesondert aufzubewahren. [2]Sie sind, soweit sich nicht aus § 22 Absatz 2 und § 23 etwas anderes ergibt, zu löschen, sobald bei den statistischen Ämtern die Überprüfung der Erhebungs- und Hilfsmerkmale auf ihre Schlüssigkeit und Vollständigkeit abgeschlossen ist. [3]Sie sind spätestens vier Jahre nach dem Berichtszeitpunkt zu löschen.
(2) Die Erhebungsunterlagen sind nach Abschluss der Aufbereitung des Zensus, spätestens vier Jahre nach dem Berichtszeitpunkt zu vernichten.

12.4.6 Ausblick

Die ersten Ergebnisse des Zensus 2011 werden bundesweit voraussichtlich im Frühjahr 2013 veröffentlicht. Das endgültige Ergebnis wird nach derzeitigem Stand frühestens im Herbst 2013 erwartet.

Die Zensusarbeiten werde ich aus datenschutzrechtlicher Sicht auch weiterhin aufmerksam beobachten. Die datenschutzrechtlichen Erfahrungen aus dem Zensus 2011 werden im Übrigen auf Bund- und Länderebene gesammelt; hieran bin ich im Rahmen der Arbeitsgruppe der Datenschutzbeauftragten des Bundes und der Länder beteiligt.

12.5 Statistische Erhebungen und informationelle Selbstbestimmung

Wie schon in den vorangegangenen Berichtszeiträumen erreichten mich auch im aktuellen Berichtszeitraum wieder zahlreiche Eingaben, in denen Bürgerinnen und Bürger durch eine **gesetzlich angeordnete Auskunftspflicht bei statistischen Erhebungen** ihr Grundrecht auf informationelle Selbstbestimmung als verletzt ansahen.

Aus Datenschutzsicht habe ich die Betroffenen auf Folgendes hingewiesen:

Das Bundesverfassungsgericht hat in seinem so genannten „Volkszählungsurteil" vom 15.12.1983 (Az.: 1 BvR 209, 269, 362, 420, 440, 484/83) ausgeführt, dass das Grundrecht auf informationelle Selbstbestimmung nicht schrankenlos gewährleistet ist. Der Einzelne muss vielmehr Einschränkungen seines Rechts auf informationelle Selbstbestimmung im überwiegenden Allgemeininteresse hinnehmen. Voraussetzungen für eine derartige Einschränkung sind allerdings das

Vorliegen einer normenklaren gesetzlichen Rechtsgrundlage und die Beachtung des Grundsatzes der Verhältnismäßigkeit.

Bis zu einer verfassungsgerichtlichen Verwerfung ist davon auszugehen, dass statistikrechtliche Auskunftspflichten in gesetzlich angeordneten amtlichen Statistiken den verfassungsrechtlichen Vorgaben genügen. Im Hinblick auf Stichprobenbefragungen hat das Bundesverfassungsgericht dabei ausdrücklich darauf hingewiesen, dass bereits eine Verweigerung der Angaben durch wenige Befragte das Ergebnis der gesamten Repräsentativumfrage in Frage stellen könnte.

Einer weit gehenden statistikrechtlichen Auskunftspflicht müssen jedoch – gleichsam als „Gegengewicht" – entsprechende **Sicherungsvorkehrungen** gegenüber stehen. So betrachtet das Bundesverfassungsgericht den Grundsatz, die zu statistischen Zwecken erhobenen Einzelangaben strikt geheim zu halten, als unverzichtbar.

Der Gesetzgeber hat dem durch Schaffung restriktiver Geheimhaltungsvorschriften in § 16 Bundesstatistikgesetz (BStatG) und Art. 17 Bayerisches Statistikgesetz (BayStatG) Rechnung getragen (sog. **Statistikgeheimnis**). So sind personenbezogene oder -beziehbare Einzelangaben grundsätzlich geheim zu halten. Eine Weitergabe ist in der Regel nur in Zusammenfassung mit den Angaben anderer Befragter zulässig. Bei diesem Nachweis von statistischen Ergebnissen ist sicherzustellen, dass ein Rückschluss auf den einzelnen Betroffenen nicht möglich ist.

§ 16 Abs. 1 BStatG Geheimhaltung
(1) [1]Einzelangaben über persönliche und sachliche Verhältnisse, die für eine Bundesstatistik gemacht werden, sind von den Amtsträgern und für den öffentlichen Dienst besonders Verpflichteten, die mit der Durchführung von Bundesstatistiken betraut sind, geheimzuhalten, soweit durch besondere Rechtsvorschrift nichts anderes bestimmt ist. [2]Dies gilt nicht für

1. *Einzelangaben, in deren Übermittlung oder Veröffentlichung der Befragte schriftlich eingewilligt hat,*
2. *Einzelangaben aus allgemein zugänglichen Quellen, wenn sie sich auf die in § 15 Abs. 1 genannten öffentlichen Stellen beziehen, auch soweit eine Auskunftspflicht aufgrund einer eine Bundesstatistik anordnenden Rechtsvorschrift besteht,*
3. *Einzelangaben, die vom Statistischen Bundesamt oder den statistischen Ämtern der Länder mit den Einzelangaben anderer Befragter zusammengefaßt und in statistischen Ergebnissen dargestellt sind,*
4. *Einzelangaben, wenn sie dem Befragten oder Betroffenen nicht zuzuordnen sind.*

[3]Die §§ 93, 97, 105 Abs. 1, § 111 Abs. 5 in Verbindung mit § 105 Abs. 1 sowie § 116 Abs. 1 der Abgabenordnung vom 16. März 1976 (BGBl. I S. 613; 1977 I S. 269), zuletzt geändert durch Artikel 1 des Gesetzes vom 19. Dezember 1985 (BGBl. I S. 2436), gelten nicht für Personen und Stellen, soweit sie mit der Durchführung von Bundes-, Landes- oder Kommunalstatistiken betraut sind.

Art. 17 BayStatG Geheimhaltung
(1) [1] Einzelangaben sind von den mit der Durchführung der Statistik betrauten Stellen und Personen geheimzuhalten. [2] Dies gilt nicht für

1. *Einzelangaben, in deren Übermittlung oder Veröffentlichung die Auskunftgebenden oder die betroffenen Personen schriftlich eingewilligt haben;*

2. Einzelangaben, soweit deren Übermittlung oder Veröffentlichung durch Art. 18 oder durch besondere Rechtsvorschrift zugelassen ist;
3. Einzelangaben aus allgemein zugänglichen Quellen;
4. Einzelangaben, die ausschließlich einer öffentlichen Stelle, die nicht am wirtschaftlichen Wettbewerb teilnimmt, zugeordnet werden können;
5. Einzelangaben, die keiner befragten oder betroffenen Person zuzuordnen sind, insbesondere, wenn sie mit den Einzelangaben anderer zusammengefaßt und in statistischen Ergebnissen dargestellt sind.

[3] Die Pflicht zur Geheimhaltung besteht auch für Personen, die Empfänger von Einzelangaben nach Art. 18 oder auf Grund einer besonderen Rechtsvorschrift sind.

(2) Sonstige Vorschriften über die Geheimhaltung und Verschwiegenheit bleiben unberührt.

12.6 Namensangabe auf dem bayerischen Parkausweis für Schwerbehinderte

Bereits im 18. Tätigkeitsbericht habe ich mich mit personenbezogenen Angaben auf Parkausweisen für Schwerbehinderte befasst (siehe hierzu 18. Tätigkeitsbericht, Nr. 16.1). Seither haben sich bezüglich der Ausgestaltung der einzelnen Muster der Parkausweise Änderungen ergeben. So sieht der neue (seit 2001 gültige) EU-einheitliche Parkausweis für Schwerbehinderte die Namensangabe nur mehr auf der Ausweisrückseite vor, auf dem 2009 eingeführten bundesweit gültigen (orangefarbenen) Ausweis sind keine personenbezogenen Angaben zulässig. Auf dem (dunkelblauen) Parkausweis für den Personenkreis „nur Bayern" ist dagegen weiterhin der Name des Berechtigten auf der Vorderseite einzutragen. Beim Ausstellen der Ausweise werden zum Teil doppelseitige Vordrucke verwendet, bei denen auf der Vorderseite das blaue Ausweismuster „nur Bayern" und auf der Rückseite das orangene Ausweismuster abgebildet ist. Damit soll den Berechtigten das Mitführen dieser beiden Parkausweise erleichtert werden. Der jeweilige Parkausweis ist dabei beim Parken auf Behinderten-Parkplätzen bzw. um Parkerleichterungen in Anspruch nehmen zu dürfen gut lesbar im Fahrzeug auszulegen.

Aufgrund einer auf die Namensangabe im bayerischen Parkausweis bezogenen Beschwerde eines Bürgers habe ich dem Bayerischen Staatsministerium des Innern mitgeteilt, dass ich eine Namensangabe auf dem Parkausweis „nur Bayern" deutlich sichtbar auf der Ausweisvorderseite für nicht erforderlich halte. Soweit auf den Namenseintrag zu Kontrollzwecken nicht verzichtet werden kann, habe ich vorgeschlagen, den Namen auf der Ausweisrückseite einzutragen bzw. das Abdecken des Namensfeldes auf der Vorderseite des Ausweismusters „nur Bayern" zuzulassen, wenn das kombinierte doppelseitige Ausweismuster Verwendung findet (und damit ein Eintrag des Namens auf der Rückseite des Ausweises nicht mehr möglich ist).

Das Bayerische Staatsministerium des Innern hat meine Anregung in der Neufassung der Anwendungshinweise zum Vollzug der Straßenverkehrs-Ordnung (Betreff: Parkerleichterungen für behinderte Menschen) zum 01.03.2011 berücksichtigt und ausgeführt, dass keine Bedenken bestehen, wenn das Namensfeld auf dem Ausweis „nur Bayern" vom Berechtigten so abgedeckt wird, dass die Abdeckung zu Kontrollzwecken jederzeit leicht entfernt werden kann.

12.7 Datenweitergabe von der Fahrerlaubnisbehörde an die Waffenbehörde

Im Berichtszeitraum war ich mit der Anfrage eines Landratsamtes befasst, unter welchen Voraussetzungen die Fahrerlaubnisbehörde personenbezogene Daten über eine (mögliche) Alkohol- oder Rauschmittelabhängigkeit an die Waffenbehörde weitergeben darf.

Dazu vertritt das Bayerische Staatsministerium des Innern die Auffassung, dass eine Mitteilung über eignungsrelevante Vorfälle, z.B. im Zusammenhang mit einer Alkohol- oder Drogenproblematik, von der Fahrerlaubnisbehörde an die Waffenbehörde nach Art. 17 Abs. 2 Nr. 9 BayDSG zulässig ist, sofern der Fahrerlaubnisbehörde bekannt ist, dass der Betroffene Inhaber einer waffenrechtlichen Erlaubnis ist. Diese Einschätzung teile ich grundsätzlich. Aus datenschutzrechtlicher Sicht habe ich dazu ergänzend auf Folgendes hingewiesen:

– Die in § 60 Abs. 1 Satz 1 des Straßenverkehrsgesetzes (StVG) geregelte Übermittlungsbefugnis bezieht sich aufgrund des Wortlauts nur auf die Daten aus den Fahrerlaubnisregistern. Soweit für die sonstigen bei den Fahrerlaubnisbehörden gespeicherten Unterlagen (wie z.B. Gutachten oder polizeiliche Mitteilungen) keine spezialgesetzlichen Übermittlungsbefugnisse existieren, finden die allgemeinen Vorschriften des BayDSG Anwendung.

– Wegen des Grundsatzes der Zweckbindung dürfen personenbezogene Daten nur für den Zweck genutzt werden, für den sie erhoben bzw. gespeichert worden sind (Art. 17 Abs. 1 Nr. 2 BayDSG). Dabei umfasst der Begriff der Nutzung auch die Weitergabe der Daten innerhalb der speichernden Stelle, hier innerhalb des Landratsamtes (vgl. Art. 4 Abs. 7 BayDSG).

  Abweichend von Art. 17 Abs. 1 Nr. 2 BayDSG kommt eine Datenweitergabe nach Art. 17 Abs. 2 Nr. 9 BayDSG in Betracht, wenn es zur Abwehr erheblicher Nachteile für das Gemeinwohl oder von Gefahren für die öffentliche Sicherheit oder Ordnung oder zur Abwehr einer schwerwiegenden Beeinträchtigung der Rechte einer anderen Person erforderlich ist. Die Auslegung des Begriffs „erforderlich“ führt dazu, dass eine automatische Mitteilung an die Waffenbehörde im Sinne einer Datenweitergabe „auf Vorrat“ unzulässig ist (vgl. Wilde/Ehmann/Niese/Knoblauch, Bayerisches Datenschutzgesetz, Art. 16 Rdnrn. 9 - 14).

– Gleichzeitig muss der Fahrerlaubnisbehörde bekannt sein, dass der Betroffene Inhaber einer waffenrechtlichen Erlaubnis ist. Sie kann dies insbesondere nicht durch Nachfrage bei der Waffenbehörde in Erfahrung bringen, da sie hierfür – mangels Erforderlichkeit zur eigenen Aufgabenerfüllung – keine eigene Datenerhebungsbefugnis besitzt.

– Sofern unter den o.g. Voraussetzungen eine Datenweitergabe im Einzelfall möglich ist, kommt es maßgeblich auf den zulässigen Umfang der Datenweitergabe an. Personenbezogene Daten dürfen dabei nur weitergegeben werden, soweit es zur Aufgabenerfüllung der Waffenbehörde bzw. für deren waffenrechtliche Prüfung erforderlich ist. Dies ist jedoch in erster Linie eine fachliche Frage im Vollzug des Waffenrechts, die seitens der Fahrerlaubnisbehörde nicht in jedem Fall sicher beantwortet werden kann. So werden z.B. der Fahrerlaubnisbehörde vorliegende Erkenntnisse im

Zusammenhang mit einer Alkohol- oder Drogenproblematik nicht in jedem Fall bereits die Annahme rechtfertigen, dass die betreffende Person abhängig von Alkohol oder anderen berauschenden Mitteln im Sinne des § 6 Abs. 1 Nr. 2 Waffengesetz (WaffG) ist. Z.B. dürfte dies nicht bereits dann der Fall sein, wenn die Fahrerlaubnis aufgrund einer wiederholten Fahrt unter Alkoholeinfluss im Ordnungswidrigkeitenbereich entzogen wird, weil der Betroffene ein nach der Fahrerlaubnisverordnung gefordertes medizinisch-psychologisches Gutachten nicht beigebracht hat.

Tatsachen, die die Annahme einer Alkoholabhängigkeit begründen, könnten sich jedoch z.B. aus einer Trunkenheitsfahrt mit über 1,6 ‰ (was für eine weit überdurchschnittliche Alkoholgewöhnung spricht und regelmäßig zum Entzug der Fahrerlaubnis führt) ergeben oder aus einem der Fahrerlaubnisbehörde vorliegenden (fachärztlichen, medizinisch-psychologischen) Gutachten, das die Alkoholabhängigkeit attestiert.

Folglich müsste in jedem Einzelfall seitens der Fahrerlaubnisbehörde eine Vorprüfung erfolgen, ob tatsächlich Tatsachen im Sinne des § 6 Abs. 1 Nr. 2 WaffG vorliegen, die z.B. die Annahme einer Alkoholabhängigkeit begründen. Falls dahingehende Zweifel bestehen, habe ich keine Bedenken, wenn die Fahrerlaubnisbehörde die ihr vorliegenden Erkenntnisse zunächst in anonymisierter Form bei der Waffenbehörde vorträgt und anfragt, ob dies für eine waffenrechtliche Überprüfung als auch im Hinblick auf Art. 17 Abs. 2 Nr. 9 BayDSG tatsächlich für erforderlich gehalten wird. Sofern die Waffenbehörde dies bejaht, ist die Weitergabe der personenbezogenen Daten zu deren Aufgabenerfüllung zulässig.

Im Hinblick auf den Grundsatz der Datenerhebung beim Betroffenen (Art. 16 Abs. 2 Satz 1 BayDSG) hat sich die Datenweitergabe auf die hierfür erforderlichen Angaben zu beschränken, d.h. es dürften zunächst nur die für die Einleitung einer Überprüfung durch die Waffenbehörde notwendigen Daten weitergegeben werden. Dabei müssen die betreffenden Aktenbestandteile durch Schwärzen, Kürzen etc. entsprechend bereinigt werden, so dass sie nurmehr die relevanten Informationen enthalten.

Das Bayerische Staatsministerium des Innern hat die nachgeordneten Behörden in einem Rundschreiben entsprechend informiert.

§ 6 Abs. 1 Nr. 2 WaffG
(1) [1]Die erforderliche persönliche Eignung besitzen Personen nicht, wenn Tatsachen die Annahme rechtfertigen, dass sie
1. …
2. abhängig von Alkohol oder anderen berauschenden Mitteln, psychisch krank oder debil sind oder
3. …

12.8 Übermittlung von Fahrzeug- und Halterdaten an einen Rechtsanwalt

Bereits in meinem letzten Tätigkeitsbericht habe ich über eine unzulässige Weitergabe von Fahrzeug- und Halterdaten durch eine Kfz-Zulassungsstelle berichtet (siehe hierzu 24. Tätigkeitsbericht, Nr. 12.7). Auch im Berichtszeitraum war ich wieder mit der Prüfung eines ähnlichen Sachverhalts befasst. Im zugrundeliegenden Fall war einem Rechtsanwalt aus dem örtlichen Fahrzeugregister eine

Auskunft zu Fahrzeug- und Halterdaten des Beschwerdeführers erteilt worden, ohne dass dieser – wie in § 39 Abs. 1 StVG vorausgesetzt – dargelegt hatte, dass er die Daten für einen mit der Teilnahme am Straßenverkehr im Zusammenhang stehenden Rechtsanspruch oder zur Erhebung einer Privatklage wegen im Straßenverkehr begangener Verstöße benötigt. Der Anwalt hatte gegenüber dem betreffenden Landratsamt lediglich angegeben, die Daten in einer zivilrechtlichen Angelegenheit zu benötigen. Das Landratsamt erläuterte in seiner Stellungnahme, die Auskunftsanfrage habe darauf abgezielt, eine dauerhafte unentgeltliche Gebrauchsmöglichkeit des angefragten Kraftfahrzeugs durch die vom Mandanten des Rechtsanwalts getrennt lebende Ehefrau, die am Steuer dieses Wagens gesehen worden sei, zu ermitteln, was wiederum Ansprüche im Rahmen des Getrenntlebensunterhalts begründen könnte. Da es in diesem Zusammenhang möglicherweise auch auf die Eigenbeteiligung bzw. Freistellung von Versicherungsbeiträgen ankommen könne, seien auch Versicherungsdaten des Kraftfahrzeughalters übermittelt worden.

Im vorliegenden Fall war die Auskunftserteilung danach bereits deswegen unzulässig, weil der vorgetragene Rechtsanspruch in keinem Zusammenhang mit der Teilnahme am Straßenverkehr stand. Hierfür genügt es zwar schon, dass der Anspruch einen Bezug zum straßenverkehrlichen Geschehen hat. Ein solcher ist aber dann nicht gegeben, wenn ein Kraftfahrzeug wie im vorliegenden Fall lediglich als Vermögensgegenstand betrachtet wird. Dieser Sachverhalt ist vergleichbar mit der Vollstreckung in das Vermögen eines Schuldners, in welchem sich auch ein Kraftfahrzeug befindet. Auch hier ist ein Zusammenhang mit der Teilnahme am Straßenverkehr zu verneinen.

Mit der erteilten Versicherungsauskunft wurden hier außerdem auch noch personenbezogene Daten übermittelt, die ohne Grund über das Auskunftsersuchen, welches sich nur auf den Namen und die Anschrift des Kraftfahrzeughalters bezog, hinausgingen. Die unzulässige Datenübermittlung habe ich beanstandet.

§ 39 Abs. 1 StVG
Von den nach § 33 Abs. 1 gespeicherten Fahrzeugdaten und Halterdaten sind
1. Familienname (bei juristischen Personen, Behörden oder Vereinigungen: Name oder Bezeichnung),
2. Vornamen,
3. Ordens- und Künstlername,
4. Anschrift,
5. Art, Hersteller und Typ des Fahrzeugs,
6. Name und Anschrift des Versicherers,
7. Nummer des Versicherungsscheins, oder, falls diese noch nicht gespeichert ist, Nummer der Versicherungsbestätigung,
8. gegebenenfalls Zeitpunkt der Beendigung des Versicherungsverhältnisses,
9. gegebenenfalls Befreiung von der gesetzlichen Versicherungspflicht,
10. Zeitpunkt der Zuteilung oder Ausgabe des Kennzeichens für den Halter sowie
11. Kraftfahrzeugkennzeichen
durch die Zulassungsbehörde oder durch das Kraftfahrt-Bundesamt zu übermitteln, wenn der Empfänger unter Angabe des betreffenden Kennzeichens oder der betreffenden Fahrzeug-Identifizierungsnummer darlegt, dass er die Daten zur Geltendmachung, Sicherung oder Vollstreckung oder zur Befriedigung oder Abwehr von Rechtsansprüchen im Zusammenhang mit der Teilnahme am Straßen-

verkehr oder zur Erhebung einer Privatklage wegen im Straßenverkehr begangener Verstöße benötigt (einfache Registerauskunft).

12.9 Datenschutzrechtliche Unterschiede zwischen Veröffentlichungen in Planfeststellungsverfahren und der öffentlichen Bekanntmachung von Enteignungsverfahren nach dem Bayerischen Gesetz über die entschädigungspflichtige Enteignung

Im Berichtszeitraum an mich gerichtete Eingaben haben gezeigt, dass hinsichtlich der datenschutzrechtlichen Unterschiede zwischen Veröffentlichungen in Planfeststellungsverfahren einerseits und der öffentlichen Bekanntmachung von Enteignungsverfahren nach dem Bayerischen Gesetz über die entschädigungspflichtige Enteignung (BayEG) andererseits noch immer Unklarheiten bestehen. Dies nehme ich zum Anlass, erneut auf Folgendes hinzuweisen:

12.9.1 Veröffentlichungen in Planfeststellungsverfahren

Wie bereits in meinem 17. Tätigkeitsbericht im Einzelnen erläutert, ist es im Hinblick auf die Beschlüsse des Bundesverfassungsgerichts vom 14.10.1987 (BVerfGE 77, 121) und 24.07.1990 (Az.: 1 BvR 1244/87) datenschutzrechtswidrig, Namen und Anschriften von betroffenen Grundstückseigentümern bzw. Einwendern in die öffentlich ausgelegten Planunterlagen bzw. den Planfeststellungsbeschluss aufzunehmen (siehe hierzu 17. Tätigkeitsbericht, Nr. 8.14). Stattdessen sind im Planfeststellungsbeschluss den betroffenen Grundstückseigentümern bzw. Einwendern (Betriebs-) Nummern zuzuteilen und nur diese in der entsprechenden Passage der Begründung des Planfeststellungsbeschlusses aufzuführen. Gegen die – hierbei bzw. bei der öffentlichen Auslegung der Planunterlagen erfolgende – Nennung der Flurstücksnummern der betroffenen Grundstücke erhebe ich aus datenschutzrechtlicher Sicht keine Einwände.

Zwar kann es auch bei einer Vergabe von Betriebsnummern aufgrund der gebotenen umfassenden Begründung der in einem Planfeststellungsbeschluss getroffenen Abwägungsentscheidungen dazu kommen, dass einige „Insider“ aus den Angaben im Planfeststellungsbeschluss zum jeweiligen Betrieb auf die konkrete Person des Betriebsinhabers rückschließen können, doch handelt es sich hierbei um ein nicht auszuschließendes und aus datenschutzrechtlicher Sicht damit hinzunehmendes Restrisiko.

12.9.2 Öffentliche Bekanntmachung von Enteignungsverfahren nach dem BayEG

Die öffentliche Bekanntmachung von Enteignungsverfahren nach dem BayEG ist in Art. 26 Abs. 7 BayEG – spezialgesetzlich im Sinne des Art. 2 Abs. 7 BayDSG – geregelt. Für den Inhalt dieser öffentlichen Bekanntmachung wird in Art. 26 Abs. 7 Satz 2 BayEG sinngemäß auf Art. 26 Abs. 5 BayEG verwiesen.

Art. 26 Abs. 5 BayEG
(5)[1] Die Ladung muss enthalten
1. die Bezeichnung des Antragstellers und des Enteignungsgegenstands,
2. den wesentlichen Inhalt des Enteignungsantrags mit dem Hinweis, dass der Antrag mit den ihm beigefügten Unterlagen bei der Enteignungsbehörde oder einer von ihr bestimmten Stelle eingesehen werden kann,

3. die Aufforderung, etwaige Einwendungen gegen den Enteignungsantrag möglichst vor der mündlichen Verhandlung bei der Enteignungsbehörde schriftlich einzureichen oder zur Niederschrift zu erklären und etwaige Rechte spätestens in der mündlichen Verhandlung wahrzunehmen, und

4. den Hinweis, dass auch bei Nichterscheinen über den Enteignungsantrag und andere im Verfahren zu erledigende Anträge entschieden werden kann.

[2]Sie soll einen Hinweis auf die Verfügungs- und Veränderungssperre (Art. 27) und ein etwaiges Planfeststellungsverfahren enthalten.

Insbesondere die Bezeichnung des Enteignungsgegenstands in der öffentlichen Bekanntmachung nach Art. 26 Abs. 7 Satz 2 i.V.m. Abs. 5 Satz 1 Nr. 1 BayEG muss derart beschaffen sein, dass nicht ermittelte Beteiligte und die in Art. 22 Abs. 1 Nr. 3 BayEG aufgezählten Inhaber nicht im Grundbuch oder Wasserbuch eingetragener Rechte erkennen können, ob sie von dem Enteignungsverfahren betroffen sein können (vgl. Molodovsky/Bernstorff, Enteignungsrecht in Bayern, Art. 26 BayEG, Erl. 7.6.2.3). Dies erfordert in gewissem Umfang auch die Bekanntgabe personenbezogener Daten.

Bei der konkreten Bestimmung des hierbei zulässigen Umfangs einer Bekanntgabe personenbezogener Daten ist zu beachten, dass der Gesetzgeber in den Art. 26 Abs. 7 Satz 2 i.V.m. Abs. 5 BayEG nur den Mindestinhalt der öffentlichen Bekanntmachung geregelt hat. Ein darüber hinausgehender Ladungsinhalt ist daher nicht von vornherein ausgeschlossen. Angaben über wirtschaftliche Verhältnisse von Betroffenen, die deren Recht auf informationelle Selbstbestimmung verletzen, sind aber nicht zulässig (vgl. Molodovsky/Bernstorff, a.a.O., Art. 26 BayEG, Erl. 7.1, 7.6.1, 7.6.5 und 8.1.1).

Daher dürfen beispielsweise bei Grundstücken, die von einem Enteignungsverfahren nach dem BayEG betroffen sind, regelmäßig Flurstücksnummer, Grundbuchblatt und Hausnummer bzw. Lage an einer Straße öffentlich bekannt gemacht werden. Daneben wird die Angabe des Eigentümers grundsätzlich zur Konkretisierung des Enteignungsgegenstands erforderlich sein (vgl. Molodovsky/Bernstorff, a.a.O., Art. 26 BayEG, Erl. 7.6.2.3). Auch die öffentliche Bekanntmachung von auf dem Enteignungsgegenstand lastenden Grundschulden wird aufgrund der aus § 1192 Abs. 1 BGB folgenden Unabhängigkeit der Grundschuld von einer zugrundeliegenden schuldrechtlichen Forderung regelmäßig zulässig sein, da dies keinen Rückschluss aus der Bekanntmachung auf die Höhe der tatsächlich auf dem Enteignungsgegenstand lastenden Verbindlichkeiten bzw. die wirtschaftliche Situation des Eigentümers zulässt.

12.10 Information der Betroffenen über eine mit Mitteln des Verwaltungszwangs erfolgte Öffnung ihrer Wohnungstür

Ein Landratsamt hat in einem Mehrfamilienhaus eine verschlossene Wohnungstür während der Abwesenheit der Wohnungsinhaberin berechtigtermaßen mit Mitteln des Verwaltungszwangs fachmännisch öffnen und – nach Einbau eines neuen Türschlosses – wieder verschließen lassen. Die Wohnungsinhaberin wurde sodann vom Landratsamt mit einem offen vor ihrer Wohnungstür abgelegten und für alle Benutzer des Hausgangs gut sichtbaren Zettel darüber informiert, wo sie ihren neuen Wohnungsschlüssel abholen könne.

In datenschutzrechtlicher Hinsicht habe ich diesen Vorgang wie folgt bewertet:

Auch die Tatsache, dass die Betroffene einen neuen Wohnungsschlüssel hat und wo dieser zur damaligen Zeit verwahrt wurde, stellt ein personenbezogenes Datum im Sinne des Art. 4 Abs. 1 BayDSG dar. Da diese Information auf einem offen vor der Wohnungstür abgelegten Zettel für jedermann im Hausgang unschwer wahrnehmbar war, liegt eine Datenübermittlung gemäß Art. 4 Abs. 6 Satz 2 Nr. 3 a BayDSG an Dritte vor. Da es sich hierbei um private Dritte, mithin nichtöffentliche Stellen gehandelt hat, bemisst sich die Rechtmäßigkeit dieser Datenübermittlung – mangels Vorliegen einer Einwilligung der Betroffenen gemäß Art. 15 Abs. 1 Nr. 2 BayDSG – anhand des Art. 19 BayDSG. Die Voraussetzungen des Art. 19 Abs. 1 BayDSG waren insoweit jedoch nicht erfüllt. Weder war es zur Aufgabenerfüllung des Landratsamtes gemäß Art. 19 Abs. 1 Nr. 1 BayDSG erforderlich, die anderen Hausbewohner darüber zu informieren, dass die Betroffene einen neuen Wohnungsschlüssel hat und wo sie diesen abholen kann noch war ein schutzwürdiges Interesse der Wohnungsinhaberin an einem Ausschluss der Übermittlung gemäß Art. 19 Abs. 1 Nr. 2 BayDSG auszuschließen. Insoweit hätte es beispielsweise vollkommen ausgereicht, die **Benachrichtigung in einem verschlossenen (idealerweise gesiegelten) und an die Wohnungsinhaberin persönlich adressierten Umschlag vor deren Wohnungstür zu legen**. Auf diese Weise wäre hinreichend sichergestellt gewesen, dass die Betroffene sofort nach dem Bemerken, dass ihr alter Wohnungsschlüssel nicht mehr sperrt, den Aufbewahrungsort des neuen Schlüssels in Erfahrung bringen kann. Nicht ausreichend wäre es dagegen gewesen, den Zettel in ihren Briefkasten zu werfen, denn, dass ein Wohnungsinhaber stets auch seinen Briefkastenschlüssel bei sich hat, kann nicht unterstellt werden.

Das betroffene Landratsamt hat mir zugesichert, in zukünftigen vergleichbaren Fällen für eine datenschutzgerechte Information der betroffenen Wohnungsinhaber zu sorgen.

12.11 Veröffentlichungen von Agrarsubventionen

Die Veröffentlichung von Informationen über die Zahlung von Mitteln aus den Europäischen Fonds für Landwirtschaft und Fischerei ist vor dem Hintergrund der sog. „Europäischen Transparenzinitiative“ zu sehen. Ziel dieser Initiative ist es, die Verwaltungs- und Entscheidungsprozesse auf EU-Ebene durchsichtiger zu machen und das Vertrauen der Öffentlichkeit in die Europäische Union zu verbessern.

Rechtliche Grundlage für die Veröffentlichung der Empfänger von Zahlungen aus den EU-Agrarfonds waren die Verordnung (EG) Nr. 1290/2005 des Rates über die Finanzierung der Gemeinsamen Agrarpolitik und die Verordnung (EG) Nr. 259/2008 der Kommission mit Durchführungsbestimmungen hinsichtlich der Veröffentlichung von Informationen über die Empfänger von Mitteln aus dem Europäischen Garantiefonds für die Landwirtschaft (EGFL) und dem Europäischen Landwirtschaftsfonds für die Entwicklung des ländlichen Raums. Mit dem „Gesetz zur Veröffentlichung von Informationen über die Zahlung von Mitteln aus dem Europäischen Fonds für Landwirtschaft und Fischerei (AFIG)“ und der dazu erlassenen Durchführungsverordnung sind diese EU-Vorschriften in Deutschland umgesetzt worden.

Auf der Grundlage dieser gesetzlichen Vorschriften wurden auf der Internetseite der Deutschen Bundesanstalt für Landwirtschaft und Ernährung insbesondere in

Bezug auf natürliche Personen als Zahlungsempfänger der Name, Vorname, Wohnort mit Postleitzahl und die Höhe der Jahresbeträge veröffentlicht. Nicht der Veröffentlichungspflicht unterworfen waren dagegen z.B. Straße und Hausnummer des Empfängers.

Im Rahmen meiner Beteiligung im Vorfeld des Gesetzgebungsverfahrens hatte ich mich leider vergeblich für die bloße Veröffentlichung statistisch aufbereiteter und damit in der Regel wohl aggregierter Daten eingesetzt, zumindest aber für die Einführung von Bagatellgrenzen, oberhalb derer erst eine Veröffentlichungspflicht gelten sollte, ausgesprochen (siehe hierzu 23. Tätigkeitsbericht, Nr. 2.7).

Nachdem zwischenzeitlich der Europäische Gerichtshof (EuGH) in Luxemburg mit Urteil vom 09.11.2010 (Az.: C-92/09 und C-93/09) entschieden hat, dass bei natürlichen Personen die Namen der Empfänger von EU-Landwirtschaftsbeihilfen nicht länger in der bisherigen Form veröffentlicht werden dürfen (zwar sei das Ziel, Transparenz über die Verwendung von EU-Mitteln sicherzustellen, legitim, die Veröffentlichung der personenbezogenen Daten der Subventionsempfänger in der bisherigen Form sei aber, in Abwägung mit dem Recht auf Datenschutz, unverhältnismäßig. Unverhältnismäßig sei vor allem, dass in den Veröffentlichungen nicht nach Bezugsdauer, Häufigkeit, Art und Umfang der erhaltenen Beihilfen unterschieden werde), wurde in Deutschland, wie auch in anderen EU-Mitgliedstaaten, die Veröffentlichung sämtlicher Daten vorerst gestoppt. Nachdem die Europäische Kommission zwischenzeitlich durch Erlass der Durchführungsverordnung (EU) Nr. 410/211 vom 27.04.2011 (umgesetzt in Deutschland durch Änderung des AFIG) auf das Urteil des EuGH reagiert hat, sind die Daten von juristischen Personen als Zahlungsempfänger von EU-Agrarbeihilfen auf der Internetseite www.agrar-fischerei-zahlungen.de der Bundesanstalt für Landwirtschaft und Ernährung wieder einsehbar. Die Daten von natürlichen Personen bleiben dagegen weiter gesperrt, bis über einen noch von der EU-Kommission vorzulegenden Vorschlag über eine Neuregelung für die 27 Mitgliedstaaten entschieden ist.

13 Datenschutzkommission

Der Datenschutzkommission beim Bayerischen Landtag gehörten in den vergangenen zwei Jahren folgende Mitglieder bzw. stellvertretende Mitglieder an:

Für den Landtag:

Mitglieder:

Eberhard Rotter, CSU
Walter Taubeneder, CSU
Prof. Dr. Winfried Bausback, CSU
Dr. Florian Herrmann, CSU
Florian Ritter, SPD
Florian Streibl, Freie Wähler — bis zum 14.03.2012
Alexander Muthmann, Freie Wähler — ab dem 15.03.2012
Christine Kamm, BÜNDNIS 90/DIE GRÜNEN
Dr. Andreas Fischer, FDP

stellvertretende Mitglieder:

Peter Schmid, CSU
Christian Meißner, CSU — bis zum 12.12.2011
Alexander König, CSU — ab dem 13.12.2011
Manfred Ländner, CSU
Dr. Franz Rieger, CSU
Horst Arnold, SPD
Alexander Muthmann, Freie Wähler — bis zum 14.03.2012
Mannfred Pointner, Freie Wähler — ab dem 15.03.2012
Susanna Tausendfreund, BÜNDNIS 90/DIE GRÜNEN
Karsten Klein, FDP

Auf Vorschlag der Staatsregierung:

Mitglied:

Christian Peter Wilde, Ltd. Ministerialrat a.D. im Bayerischen Staatsministerium des Innern

stellvertretendes Mitglied:

Armin Schwimmbeck, Ministerialrat im Bayerischen Staatsministerium für Wirtschaft, Infrastruktur, Verkehr und Technologie

Auf Vorschlag der kommunalen Spitzenverbände in Bayern:

Mitglied:

Rudolf Schleyer, Mitglied des Vorstands der AKDB

stellvertretendes Mitglied:

Mario Pohl, früherer Abteilungsleiter bei der AKDB **bis zum 22.05.2012**
Doris Kirmeyer, Datenschutzbeauftragte bei der AKDB **ab dem 23.05.2012**

Auf Vorschlag des Staatsministeriums für Arbeit und Sozialordnung, Familie und Frauen 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

stellvertretendes Mitglied:

Dr. Janusz Rat, Vorsitzender des Vorstands 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 sieben Mal. Dabei befasste sie sich u.a. mit folgenden Themen:

- Vorberatung des 25. Tätigkeitsberichts
- Berichte über Beanstandungen
- Berichte von Datenschutzkonferenzen
- Berichte vom Europäischen Datenschutztag
- Berichte vom Nationalen IT-Gipfel
- Zensus 2011
- Pläne der Europäischen Kommission zur Reform des europäischen Datenschutzrechts
- Einführung der elektronischen Aufenthaltsüberwachung in der Führungsaufsicht
- Einsatz von Überwachungssoftware zur Quellen-Telekommunikationsüberwachung
- Nutzung von Sozialen Netzwerken durch öffentliche Stellen

Anlage 1:
Entschließung der 81. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 16./17.03.2011
Beschäftigtendatenschutz stärken statt abbauen

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder bekräftigt die Notwendigkeit, durch umfassende allgemein gültige Regelungen für den Datenschutz am Arbeitsplatz mehr Rechtssicherheit zu erreichen und bestehende Schutzlücken zu schließen. Dieser Ansatz erfordert klare gesetzliche Begrenzungen der Erhebung, Verarbeitung und Nutzung von Beschäftigtendaten. Die Bundesregierung und die Bundestagsfraktionen der SPD und von BÜNDNIS 90/DIE GRÜNEN haben hierzu Gesetzentwürfe vorgelegt.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder appelliert an den Deutschen Bundestag, bei den Beratungen über Regelungen des Beschäftigtendatenschutzes insbesondere folgende notwendige Anforderungen sicherzustellen:

- Im Bewerbungsverfahren und im Beschäftigungsverhältnis
  - ist die Erforderlichkeit von Eignungstests und medizinischen Untersuchungen vor der Durchführung der jeweiligen Maßnahme zu dokumentieren,
  - sind Datenerhebungen nur zulässig, wenn und soweit diese Daten wegen der Art und der Ausübung der Tätigkeit oder der Bedingung ihrer Ausübung unabdingbar sind und entscheidende berufliche Anforderungen oder Hindernisse darstellen,
  - sind Eignungstests ausschließlich zulässig, wenn sie auf einer wissenschaftlichen Methode beruhen.
- Arbeitgeber müssen verpflichtet werden, Bewerber so früh wie möglich umfassend über die Datenerhebung aus allgemein zugänglichen Quellen (z.B. im Internet) und bei Dritten zu unterrichten.
- Zur Aufdeckung von Straftaten und ähnlich schwerwiegenden Pflichtverletzungen dürfen Beschäftigtendaten nur oberhalb normenklarer und verhältnismäßiger Einschreitschwellen erhoben und verwendet werden. Arbeitgeber dürfen dabei – insbesondere verdeckte – Überwachungsmaßnahmen nur ergreifen, wenn zu dokumentierende Tatsachen vorliegen. Mit Blick auf rechtsstaatliche Anforderungen ist die Grenze zwischen eigenverantwortlichen Recherchen des Arbeitgebers und der den Strafverfolgungsbehörden vorbehaltenen Aufgaben eindeutig zu bestimmen. Aus präventiven Gründen ist eine verdeckte Datenerhebung unzulässig.
- Insbesondere bezüglich der Durchführung von Screening-Verfahren sind klare materielle Kriterien – z.B. Prüfung der Verhältnismäßigkeit, Vorliegen von tatsächlichen Hinweisen auf Unregelmäßigkeiten – erforderlich. Zudem sollten Arbeitgeber verpflichtet sein, die näheren Umstände, die den Abgleich veranlassen, vorab zu dokumentieren.
- Die an verschiedenen Stellen im Gesetzentwurf der Bundesregierung vorgesehenen Regelungen zur Verhaltens- und Leistungskontrolle sind nach wie vor zu weitgehend. Der Gesetzgeber muss hier strenge Voraussetzungen vorgeben. Die Konferenz weist auf die gefestigte verfassungsrechtliche Rechtsprechung zum unzumutbaren Überwachungsdruck hin.

- Die Konferenz der Datenschutzbeauftragten fordert, die offene Videoüberwachung stärker zu begrenzen und insbesondere
  - zu verbieten, die z.B. bei der Qualitätskontrolle anfallenden Daten zur Verhaltens- und Leistungskontrolle zu nutzen.
  - für Bereiche zu untersagen, die nicht nur „überwiegend", sondern auch der privaten Nutzung dienen.
- Das Petitionsrecht darf nicht beschränkt werden. Beschäftigte müssen sich jederzeit an die zuständige Datenschutzaufsichtsbehörde wenden können, ohne deswegen benachteiligt oder gemaßregelt zu werden.
- In gesetzliche Regelungen zum Beschäftigtendatenschutz sind darüber hinaus Bestimmungen aufzunehmen
  - zur Personalaktenführung – einschließlich der automatisierten Personalaktenführung,
  - zur privaten Nutzung von Telekommunikationsdiensten,
  - zum Thema Whistleblowing,
  - zum Bereich der Videoüberwachung im öffentlich zugänglichen Bereich, bei denen Beschäftigtendaten mit anfallen,
  - zum Beweisverwertungsverbot bei unzulässiger Datenerhebung und -verwendung,
  - zum Konzerndatenschutz unter Berücksichtigung des internationalen Datenverkehrs.

Anlage 2:
Entschließung der 81. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 16./17.03.2011 Keine Vorratsspeicherung und Rasterung von Flugpassagierdaten!

Die EU-Kommission hat am 02.02.2011 einen neuen Entwurf für eine Richtlinie zur Nutzung von EU-Flugpassagierdaten zur Gefahrenabwehr und Strafverfolgung vorgestellt.

Zentraler Gegenstand des Entwurfs ist die systematische Erfassung der Daten aller Fluggäste, die EU-Außengrenzen überqueren. Diese Daten aus den Buchungssystemen der Fluggesellschaften sollen anlass- und verdachtsunabhängig an eine nationale Zentralstelle der Sicherheitsbehörden übermittelt und regelmäßig für fünf Jahre gespeichert werden. Ziel soll es sein, damit Personen ausfindig zu machen, die in Terrorismus oder schwere Kriminalität verwickelt sein könnten.

Auch der neue Entwurf bleibt konkrete Beweise dafür schuldig, dass die anlassfreie automatisierte Auswertung und Analyse von Flugpassagierdaten geeignet und erforderlich ist, um dieses Ziel zu fördern. Ein solches Zusammenspiel von Vorratsspeicherung und Rasterung von Passagierdaten ist weder mit der EU-Grundrechtecharta noch mit dem grundgesetzlich garantierten Recht auf informationelle Selbstbestimmung vereinbar. Dies gilt insbesondere im Hinblick auf die Rechtsprechung des Bundesverfassungsgerichts, das in seinem Urteil vom 02.03.2010 (1 BvR 256/08) zur Vorratsdatenspeicherung von Telekommunikationsverkehrsdaten gemahnt hat: Zur verfassungsrechtlichen Identität der Bundesrepublik Deutschland gehört es, dass die Freiheitswahrnehmung der Bürgerinnen und Bürger nicht total erfasst und registriert werden darf. Hierfür hat sich

die Bundesrepublik auch auf europäischer und internationaler Ebene einzusetzen.

Ein solches System würde noch weiter reichende Eingriffe in die Bürgerrechte ermöglichen, wenn sogar Vorschläge zur Speicherung der Fluggastdaten bei Flügen innerhalb der Europäischen Union und von Daten der Bahn- und Schiffsreisenden Eingang in diese Richtlinie finden würden.

Dieser Entwurf verdeutlicht erneut, dass ein schlüssiges Gesamtkonzept auf europäischer Ebene zur Datenverarbeitung im Bereich der inneren Sicherheit fehlt, welches die Grundrechte der Betroffenen hinreichend gewährleistet.

Die Konferenz fordert daher die Bundesregierung und den Bundesrat auf, sich dafür einzusetzen, dass der Vorschlag der EU-Kommission für eine Richtlinie über die Verwendung von Passagierdaten nicht realisiert wird.

Anlage 3:
Beschluss der 81. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 16./17.03.2011
Datenschutzkonforme Gestaltung und Nutzung von Krankenhausinformationssystemen

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat im Oktober 2009 auf die Notwendigkeit einer datenschutzkonformen Gestaltung und Nutzung von Informationstechnik in Krankenhäusern hingewiesen.

Es besteht das dringende Bedürfnis, hierbei zu einem bundesweit und trägerübergreifend einheitlichen Verständnis der datenschutzrechtlichen Anforderungen zu gelangen, zumindest soweit dies Divergenzen in der Landeskrankenhausgesetzgebung erlauben. Zu diesem Zweck hat eine Unterarbeitsgruppe der Arbeitskreise „Gesundheit und Soziales“ und „Technik“ unter Mitarbeit von Datenschutzbeauftragten der Evangelischen Kirche in Deutschland und der Katholischen Kirche eine Orientierungshilfe erarbeitet. Im Rahmen eines Kommentierungsverfahrens und bei Expertenanhörungen wurden Hersteller von Krankenhausinformationssystemen, Betreiber und Datenschutzbeauftragte von Krankenhäusern einbezogen. Die genannten Arbeitskreise haben die Orientierungshilfe verabschiedet.

Sie konkretisiert in ihrem ersten Teil die Anforderungen, die sich aus den datenschutzrechtlichen Regelungen sowie den Vorgaben zur ärztlichen Schweigepflicht für den Krankenhausbetrieb und den Einsatz von Informationssystemen in Krankenhäusern ergeben. In Teil 2 werden Maßnahmen zu deren technischer Umsetzung beschrieben. Für die Hersteller von Krankenhausinformationssystemen, die diese nutzenden Krankenhäuser und die internen Datenschutzbeauftragten von Krankenhäusern liegt damit erstmals ein Orientierungsrahmen für eine datenschutzkonforme Gestaltung und einen datenschutzgerechten Betrieb entsprechender Verfahren vor.

Für die Datenschutzbehörden wird das vorliegende Dokument als Maßstab bei der künftigen Bewertung konkreter Verfahren im Rahmen ihrer Kontroll- und Beratungstätigkeit dienen. Dabei ist zu berücksichtigen, dass ein Teil der am Markt

angebotenen Lösungen nach den Erkenntnissen der Datenschutzbehörden in technischer Hinsicht gegenwärtig noch hinter den darin enthaltenen Anforderungen zurückbleibt. Es ist daher von der Notwendigkeit einer angemessenen Übergangsfrist für erforderliche Anpassungen durch die Hersteller auszugehen.

Stellen die Datenschutzbehörden im Zuge ihrer Kontrolltätigkeit Defizite im Vergleich zu den dargelegten Maßstäben fest, so werden sie auf die Krankenhäuser einwirken und sie dabei unterstützen, in einem geordneten Prozess unter Wahrung der Patientensicherheit Wege zur Behebung der Defizite zu finden und zu begehen. Die Deutsche Krankenhausgesellschaft und die jeweiligen Landeskrankenhausgesellschaften werden dabei einbezogen.

Die Erfahrungen der Prüftätigkeit sollen in eine regelmäßige Überarbeitung und Aktualisierung der Orientierungshilfe unter Berücksichtigung der technischen Weiterentwicklung einfließen. Die Arbeitskreise sind aufgefordert, diesen Revisionsprozess zu koordinieren und das Ergebnis spätestens im Frühjahr 2012 der Konferenz vorzulegen.

Die Konferenz nimmt die Orientierungshilfe zustimmend zur Kenntnis.

Anlage 4:
Entschließung der 81. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 16./17.03.2011 Gravierende Defizite bei der Umsetzung des SWIFT-Abkommens – dringender Handlungsbedarf auf nationaler und europäischer Ebene

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder missbilligt, dass – wie eine Prüfung der Gemeinsamen Kontrollinstanz von Europol ergeben hat[1] – EU-Zahlungsdaten auf der Grundlage viel zu abstrakter Anfragen von US-Seite umfassend in die USA übermittelt wurden. Im Ergebnis wurden damit nicht einmal die im Abkommen festgelegten unzureichenden Datenschutzregeln beachtet. Das europäische Polizeiamt Europol hat jedem US-Ersuchen zugestimmt, obwohl aufgrund der Abstraktheit der schriftlichen Ersuchen mit nur mündlicher Begründung eine abkommenskonforme Erforderlichkeitsprüfung durch Europol nicht möglich war. Die angeforderten Daten wurden stets ohne Abstriche in die USA übermittelt. Diese Vorgehensweise ist mit dem SWIFT-Abkommen und der Europol darin zugewiesenen datenschutzrechtlichen Wächterfunktion nicht vereinbar.

Nach dem SWIFT-Abkommen muss Europol im Interesse der EU-Bürgerinnen und Bürger gewährleisten, dass die Beschränkungen und Verfahrensvorgaben des Abkommens strikt beachtet werden. Europol ist demnach verpflichtet, alle US-Ersuchen auf die Beachtung dieser Beschränkungen und damit auf die Erforderlichkeit der Datenübermittlung zu überprüfen. Ohne die Zustimmung von Europol darf SWIFT keine EU-Zahlungsdaten an die USA übermitteln.

Die jetzt festgestellten Mängel bestätigen die bereits im Vorfeld des Abkommens von der Konferenz geäußerte Befürchtung, dass Europol seine Kontrollaufgabe bei SWIFT nicht angemessen wahrnimmt. Offenkundig werden die Voraussetzungen, unter denen das Europäische Parlament dem SWIFT-Abkommen zuge-

stimmt hat, nicht eingehalten. Inakzeptabel ist auch, dass die festgestellten Details von Europol pauschal als geheim klassifiziert wurden und dem Europäischen Parlament nicht mitgeteilt werden sollen. Auch die Öffentlichkeit hat ein Recht darauf zu erfahren, in welchem Umfang Daten aufgrund des Abkommens in die USA übermittelt wurden.

Die Konferenz fordert die politisch Verantwortlichen auf europäischer und nationaler Ebene auf, die Mängel umgehend zu beseitigen. Das Abkommen und seine Umsetzungspraxis gehören dringend auf den Prüfstand. Ein transparentes Verfahren und die Beteiligung der Öffentlichkeit sind unabdingbar. Die gravierenden Mängel erfordern zudem einen sofortigen Stopp der Entwicklung eines vergleichbaren EU-Systems.

[1]Der von der Gemeinsamen Kontrollinstanz von Europol vor wenigen Tagen veröffentlichte öffentliche Teil des Kontrollberichts zur Umsetzung des SWIFT-Abkommens ist auf der Homepage der GKI (http://europoljsb.consilium.europa.eu/about.aspx) abrufbar.

Anlage 5:
Entschließung der 82. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 28./29.09.2011
Datenschutz als Bildungsaufgabe

Ein großer Teil der wirtschaftlichen, gesellschaftlichen und persönlichen Aktivitäten findet mittlerweile im Internet statt. Millionen von Bürgerinnen und Bürgern nutzen seine Möglichkeiten und gehen dabei auch besondere Risiken ein, ohne dass ihnen dies immer bewusst wäre. Dies gilt insbesondere für Kinder und Jugendliche, aber auch erwachsene Internetnutzerinnen und -nutzer werden von der digitalen Welt zunehmend überfordert.

Vielen sind die Grundlagen, Funktionsbedingungen und wirtschaftlichen Spielregeln des Internet nicht oder nur zum Teil bekannt. Die meisten Internetnutzerinnen und -nutzer haben außerdem den Überblick darüber verloren, wer wann und zu welchem Zweck welche Daten von ihnen speichert, sie mit anderen Datensätzen verknüpft und ggf. auch an Dritte weitergibt. Wer aber nicht weiß, was mit seinen Daten geschieht oder geschehen kann, kann auch das informationelle Selbstbestimmungsrecht nicht effektiv ausüben.

Um dieser Entwicklung entgegenzuwirken, muss der Datenschutz auch als Bildungsaufgabe verstanden und praktiziert werden. Es genügt nicht, allein auf rechtliche Regelungen sowie auf datenschutzfreundliche technische Voreinstellungen und Anwendungen zu setzen. Die digitale Aufklärung ist unverzichtbar als Teil einer Datenschutzkultur des 21. Jahrhunderts. Sie beinhaltet zum einen die Vermittlung von Wissen und zum anderen die Entwicklung eines wachen, wertebezogenen Datenschutzbewusstseins.

So wie Bildung eine gesamtgesellschaftliche Aufgabe ist, so ist auch die Bildung im Hinblick auf die Datenschutzfragen unserer Zeit eine Aufgabe, die nicht nur dem Staat, sondern ebenso der Wirtschaft und der Zivilgesellschaft wie auch den Eltern im Verhältnis zu ihren Kindern obliegt.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder begrüßt deshalb und unterstützt vielfältige Überlegungen und Aktivitäten, die sich stärker als bisher um eine größere Datenschutzkompetenz der Internetnutzenden bemühen.

Die Datenschutzkonferenz hält die bisherigen Bemühungen allerdings noch nicht für ausreichend. Will man die Internetnutzerinnen und -nutzer dazu befähigen, Vorteile und Gefahren von Internetangeboten abzuwägen und selbstverantwortlich zu entscheiden, in welchem Umfange sie am digitalen Leben teilhaben wollen, sind weitergehende und nachhaltige Anstrengungen notwendig. Vor allem ist sicherzustellen, dass

- dabei viel intensiver als bisher die Möglichkeiten des Selbstdatenschutzes, der verantwortungsvolle Umgang mit den Daten anderer und die individuellen und gesellschaftlichen Auswirkungen einer leichtfertigen Nutzung des Internets thematisiert werden,
- sich die schulischen und außerschulischen Programme und Projekte zur Förderung von Medienkompetenz nicht auf Fragen des Jugendmedienschutzes und des Urheberrechts beschränken, sondern den Datenschutz als wesentlichen Bestandteil mit einbeziehen,
- Medien- und Datenschutzkompetenz entweder in einem eigenständigen Schulfach oder in einem Fächerspektrum mit Leitfächern verpflichtend zu verankern ist,
- die Vermittlung von Datenschutz als integraler Bestandteil von Medienkompetenz ausdrücklich in den Bildungsstandards und Lehrplänen verankert wird und dass die entsprechenden Anforderungen bewertungs- bzw. prüfungsrelevant ausgestaltet werden und
- Medien- und Datenschutzkompetenz und insbesondere die digitale Aufklärung zum verbindlichen Gegenstand der Lehrerausbildung gemacht werden.

Digitale Aufklärung und Erziehung zum Datenschutz bestimmen letztlich auch über den Stellenwert, den Privatsphäre und Persönlichkeitsrecht und damit Menschenwürde und Demokratie künftig in der internetgeprägten Gesellschaft insgesamt haben werden.

Anlage 6:
Entschließung der 82. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 28./29.09.2011 Vorbeugender Grundrechtsschutz ist Aufgabe der Datenschutzbeauftragten!

Der Sächsische Datenschutzbeauftragte hat mit einem Bericht zu den nicht individualisierten Funkzellenabfragen und anderen Maßnahmen der Telekommunikationsüberwachung im Februar 2011 durch die Polizei und die Staatsanwaltschaft Dresden Stellung genommen (Landtags-Drucksache 5/6787). In nicht nachvollziehbarer Weise ist die Kompetenz des Sächsischen Datenschutzbeauftragten zur Kontrolle von Verfahrensweisen von Polizei und Staatsanwaltschaften im Vorfeld einer bzw. nach einer richterlichen Anordnung in Frage gestellt worden.

Die Konferenz ist der Auffassung, dass derartige Äußerungen von der gebotenen inhaltlichen Aufarbeitung der Dresdener Funkzellenabfragen ablenken. Die gesetzliche Befugnis des Sächsischen Datenschutzbeauftragten zur Kontrolle aller polizeilichen und staatsanwaltschaftlichen Maßnahmen der Datenverarbeitung steht außer Frage. Es ist auch im Bereich der Strafverfolgung eine verfassungsrechtlich begründete Kernaufgabe der unabhängigen Datenschutzbeauftragten, einen vorgezogenen Rechtsschutz dort zu gewährleisten, wo Einzelne aufgrund der verdeckten Datenverarbeitung des Staates nicht oder nicht ausreichend früh anderweitigen Rechtsschutz erlangen können. Der Sächsische Datenschutzbeauftragte hat die polizeiliche Anregung bzw. staatsanwaltschaftliche Beantragung der konkreten Funkzellenabfragen als unverhältnismäßig und die besonderen Rechte von Abgeordneten, Verteidigerinnen und Verteidigern nicht wahrend beanstandet. Es kann dahinstehen, ob die funktional als Ausübung vollziehender Gewalt (vgl. BVerfGE 107, 395, 406) zu qualifizierende richterliche Anordnung solcher Maßnahmen von Landesdatenschutzbeauftragten kontrolliert werden kann, da die jeweiligen richterlichen Anordnungen in den konkreten Fällen nicht beanstandet wurden.

Anlage 7:
Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 25.05.2012
Patientenrechte müssen umfassend gestärkt werden
Datenschutzkonferenz fordert die Bundesregierung zur Überarbeitung des vorgelegten Gesetzentwurfs auf!

Mit dem im Januar 2012 der Öffentlichkeit vorgestellten und nun dem Bundeskabinett zugeleiteten Entwurf eines Gesetzes zur Verbesserung der Rechte von Patientinnen und Patienten (Patientenrechtegesetz) sollen insbesondere die bislang von den Gerichten entwickelten Grundsätze des Arzthaftungs- und Behandlungsrechts zusammengeführt und transparent für alle an einer Behandlung Beteiligten geregelt werden.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder teilt das Anliegen der Bundesregierung, die Rechte von Patientinnen und Patienten zu stärken.

Die Datenschutzkonferenz hält allerdings die vorgelegten Regelungen in dem Entwurf eines Patientenrechtegesetzes für nicht ausreichend. Sie fordert die Bundesregierung nachdrücklich auf, den Gesetzentwurf zu überarbeiten und dabei die folgenden Aspekte zu berücksichtigen:

– Die vertraglichen Offenbarungsobliegenheiten der Patientinnen und Patienten gegenüber den Behandelnden dürfen nicht ausgeweitet werden. Die Patientinnen und Patienten dürfen nicht zur Offenlegung von Angaben über ihre körperliche Verfassung verpflichtet werden, die keinen Behandlungsbezug haben.
– Die Patientinnen und Patienten müssen in jedem Fall und nicht erst auf Nachfrage über erlittene Behandlungsfehler informiert werden.
– Der Gesetzentwurf sollte im Zusammenhang mit der Behandlungsdokumentation um verlässliche Vorgaben zur Absicherung des Auskunfts-

rechts der Patientinnen und Patienten sowie zur Archivierung und Löschung ergänzt werden.
- Der Zugang der Patientinnen und Patienten zu der sie betreffenden Behandlungsdokumentation darf nur in besonderen Ausnahmefällen eingeschränkt werden. Die in dem Entwurf vorgesehenen Beschränkungen sind zu weitgehend und unpräzise. Zudem sollte klargestellt werden, dass auch berechtigte eigene Interessen der Angehörigen einen Auskunftsanspruch begründen können.
- Der Gesetzentwurf ist um Regelungen zur Einbeziehung Dritter im Rahmen eines Behandlungsvertrages (Auftragsdatenverarbeitung) zu ergänzen.
- Regelungsbedürftig ist ferner der Umgang mit der Behandlungsdokumentation beispielsweise im Falle eines vorübergehenden Ausfalls, des Todes oder der Insolvenz des Behandelnden. Im Bereich der Heilberufe fehlt es – anders als z.B. bei den Rechtsanwälten – an einem bundesweit einheitlichen Rechtsrahmen.

Anlage 8:
Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 27.06.2012
Orientierungshilfe zum datenschutzgerechten Smart Metering

Intelligente Energienetze und -zähler sind ein zentraler Baustein zur Sicherstellung einer nachhaltigen Energieversorgung im Sinne einer ressourcenschonenden, umweltfreundlichen und effizienten Produktion, Verteilung und Nutzung von Energie. Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat eine Orientierungshilfe beschlossen, die Empfehlungen zur datenschutzgerechten Konzeption von technischen Systemen für das Smart Metering enthält. Kernstück der Orientierungshilfe ist die Beschreibung und datenschutzrechtliche Bewertung sog. Use Cases, d.h. Anwendungsfälle, für die einzelnen Datenverarbeitungsprozesse beim Smart Metering unter Berücksichtigung des jeweiligen Schutzbedarfs der Daten.

Die Datenschutzbeauftragten des Bundes und der Länder halten es für erforderlich, dass insbesondere folgende Punkte beachtet werden:

- Eine Verarbeitung der Smart Meter Daten darf nur erfolgen, soweit es für die im Energiewirtschaftsgesetz aufgezählten Zwecke erforderlich ist.
- Die Ableseintervalle müssen so groß sein, dass aus dem Verbrauch keine Rückschlüsse auf das Verhalten der Nutzer gezogen werden können.
- Smart Meter Daten sollen möglichst nur anonymisiert, pseudonymisiert oder aggregiert übermittelt werden.
- Es muss möglich sein, hoch aufgelöste Daten lokal beim Letztverbraucher abzurufen, ohne dass dieser auf eine externe Verarbeitung der Daten angewiesen ist.
- Die Daten sollen an möglichst wenige Stellen übermittelt werden.
- Es sind angemessene Löschfristen für die Daten festzulegen, um eine Vorratsdatenspeicherung zu vermeiden.
- Die Kommunikations- und Verarbeitungsschritte von Smart Metering müssen zu jeder Zeit für den Letztverbraucher sichtbar und nachweisbar

sein. Er muss Zugriffe auf den Smart Meter erkennen und dies im Zweifel unterbinden können.

– Zusätzlich bedarf es durchsetzbarer Ansprüche der Betroffenen auf Löschung, Berichtigung und Widerspruch.
– Der Letztverbraucher muss die Möglichkeit haben, einen Tarif zu wählen, bei dem möglichst wenig über seinen Lebensstil offenbart wird, ohne dass dies für seine Energieversorgung nachteilig ist.
– Smart Meter dürfen von außen nicht frei zugänglich sein. Es müssen eindeutige Profile für den berechtigten Zugang zu den Daten definiert werden. Anhaltspunkte hierfür bieten die Vorgaben im Schutzprofil und in der Technischen Richtlinie des BSI.
– Schon bei der Konzeption und Gestaltung der technischen Systeme muss die Gewährleistung des Datenschutzes berücksichtigt werden (Privacy by Design). Der Letztverbraucher muss mit Hilfe der Technik alle notwendigen Informationen, Optionen und Kontrollmöglichkeiten erhalten, die ihm die Kontrolle seines Energieverbrauchs und die Gestaltung seiner Privatsphäre ermöglichen, wobei der Stand der Technik nicht unterschritten werden darf. Insbesondere müssen rechtlich verbindliche Vorgaben für die Konzeption der Geräte, Verfahren und Infrastrukturen sowie für deren Einsatz geschaffen werden.

Anlage 9:
Entschließung der 84. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 07./08.11.2012 Europäische Datenschutzreform konstruktiv und zügig voranbringen!

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder unterstützt die Absicht der Europäischen Kommission, den Datenschutz in Europa auf hohem Niveau zu harmonisieren. Sie hat dies bereits in ihrer Entschließung vom 21./22.03.2012 verdeutlicht. In zwei umfassenden Stellungnahmen vom 11.06.2012 haben die Datenschutzbeauftragten des Bundes und der Länder eine Vielzahl einzelner Aspekte der Datenschutzreform bewertet und Empfehlungen für den weiteren Rechtssetzungsprozess gegeben.

Angesichts der aktuellen Diskussionen in Deutschland und im Rat der Europäischen Union sowie entsprechender Äußerungen aus der Bundesregierung im Rahmen des Reformprozesses betont die Konferenz folgende Punkte:

– Im Hinblick auf geforderte Ausnahmen für die Wirtschaft ist es für die Datenschutzbeauftragten des Bundes und der Länder unabdingbar, in der Datenschutz-Grundverordnung an der bisherigen Systematik des Datenschutzrechts festzuhalten. Personenbezogene Daten dürfen nur dann verarbeitet werden, wenn dies durch eine gesetzliche Grundlage oder die Einwilligung des Betroffenen legitimiert ist. Die hier für die Wirtschaft geforderten Ausnahmen lehnt die Konferenz ab. Wollte man in Zukunft nur noch eine besonders risikobehaftete Datenverarbeitung im Einzelfall regeln und die so genannte alltägliche Datenverarbeitung weitgehend ungeregelt lassen, würde dies zu einer massiven Einschränkung des Datenschutzes führen und die Rechte der Betroffenen deutlich beschneiden.

Jede Verarbeitung scheinbar „belangloser“ Daten kann für den Einzelnen schwerwiegende Folgen haben, wie das Bundesverfassungsgericht bereits 1983 ausdrücklich klargestellt hat. Diese Aussage gilt heute mehr denn je. Deshalb lehnt es die Konferenz ab, angeblich „belanglose“ Daten von einer Regelung auszunehmen.

Soweit die Datenschutz-Grundverordnung eine Datenverarbeitung erlaubt, enthält der Reformvorschlag der Kommission bereits jetzt Ansätze für am Risiko der Datenverarbeitung ausgerichtete Differenzierungen. Diese sollten dort, wo ein risikobezogener Ansatz angemessen ist, weiter ausgebaut werden.

– Die Konferenz spricht sich nachdrücklich dafür aus, das bewährte Konzept eines grundsätzlich einheitlichen Datenschutzrechts sowohl für den öffentlichen als auch für den nichtöffentlichen Bereich beizubehalten und insbesondere für die Datenverarbeitung im öffentlichen Bereich die Möglichkeit eines höheren Schutzniveaus durch einzelstaatliches Recht zu belassen.

– Sie hält es für sinnvoll, für den Beschäftigtendatenschutz in der Datenschutz-Grundverordnung selbst qualifizierte Mindestanforderungen festzulegen und klarzustellen, dass die Mitgliedstaaten über diese zugunsten des Datenschutzes hinausgehen, sie aber nicht unterschreiten dürfen.

– Mit Blick auf die **Richtlinie im Bereich der polizeilichen und justiziellen Zusammenarbeit in Strafsachen** bekräftigt die Konferenz nochmals die Bedeutung eines hohen und gleichwertigen Datenschutzniveaus auch in diesem Bereich und damit die Wichtigkeit der Verabschiedung einer entsprechenden Regelung.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder fordert die Bundesregierung auf, sich im Sinne dieser Positionen im Rat der Europäischen Union für die Belange eines harmonisierten Datenschutzrechts auf einem hohen Niveau einzusetzen.

Anlage 10:
Entschließung der 84. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 07./08.11.2012 Übermittlung von Meldedaten an öffentlich-rechtliche Religionsgemeinschaften und die GEZ rechtskonform gestalten

Die Meldebehörden sind verpflichtet, regelmäßig Meldedaten an öffentlich-rechtliche Religionsgemeinschaften und an die Gebühreneinzugszentrale (GEZ) zu übermitteln. Die zu übermittelnden Daten beinhalten u.a. Angaben über die Religionszugehörigkeit aber auch Meldedaten, für die eine Auskunfts- und Übermittlungssperre (beispielsweise wegen Gefahr für Leib und Leben oder einer Inkognito-Adoption) im Meldedatensatz eingetragen ist. Sie sind daher besonders schutzbedürftig.

Die datenschutzrechtliche Verantwortung für den rechtmäßigen Umgang mit Meldedaten tragen allein die Meldebehörden. Eine Übermittlung in elektronischer Form ist nur dann zulässig, wenn die Identitäten von Absender und Empfänger zweifelsfrei feststehen und wenn die Daten vor dem Transport verschlüsselt werden. Diese Anforderungen werden jedoch häufig missachtet.

Die Datenschutzbeauftragten des Bundes und der Länder fordern, für die elektronische Übertragung von Meldedaten elektronische Signaturen und geeignete Verschlüsselungsverfahren mit öffentlichen Schlüsseln zu verwenden, die der jeweils aktuellen Richtlinie des Bundesamtes für die Sicherheit in der Informationstechnik entnommen sind. Durch Zertifizierung oder Beglaubigung der eingesetzten Schlüssel lassen sich auch bei der Nutzung öffentlicher Netze Absender und Empfänger eindeutig und zuverlässig identifizieren.

Mit dem Online Services Computer Interface (OSCI) steht eine bewährte Infrastruktur für E-Government-Anwendungen zur Verfügung. Die Meldeämter setzen das Verfahren entsprechend der Bundesmeldedatenübermittlungsverordnung u.a. für den Datenabgleich zwischen Meldebehörden verschiedener Länder ein. Wird ein auch nach heutigem Kenntnisstand sicheres Verschlüsselungsverfahren eingesetzt, ist die OSCI-Infrastruktur geeignet, die Sicherheit der Meldedatenübertragung auch an GEZ und öffentlich-rechtliche Religionsgemeinschaften zu gewährleisten. Wie jedes kryptographische Verfahren ist auch das Verfahren OSCI-Transport regelmäßig einer Revision zu unterziehen und weiter zu entwickeln.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder empfiehlt dem Bundesministerium des Innern, die Verwendung von OSCI-Transport für die Übermittlungen an GEZ und die öffentlich-rechtlichen Religionsgemeinschaften vorzuschreiben und fordert die Kommunen und die Innenressorts der Länder auf, unverzüglich die gesetzlichen Vorgaben bei Datenübermittlungen an die GEZ und öffentlich-rechtliche Religionsgemeinschaften umzusetzen.

Anlage 11:
Entschließung der 84. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 07./08.11.2012 Einführung von IPv6 – Hinweise für Provider im Privatkundengeschäft und Hersteller

Viele Provider werden demnächst in ihren Netzwerken die neue Version 6 des Internet-Protokolls (IPv6) einführen. Größere Unternehmen und Verwaltungen werden ihre Netze meist schrittweise an das neue Protokoll anpassen. Privatkunden werden von dieser Umstellung zuerst betroffen sein.

Für einen datenschutzgerechten Einsatz von IPv6 empfehlen die Datenschutzbeauftragten insbesondere:

– Um das zielgerichtete Verfolgen von Nutzeraktivitäten (Tracking) zu vermeiden, müssen Adresspräfixe grundsätzlich dynamisch an Endkunden vergeben werden. Auch eine Vergabe mehrerer statischer und dynamischer Adresspräfixe kann datenschutzfreundlich sein, wenn Betriebssys-

tem und Anwendungen den Nutzer dabei unterstützen, Adressen gezielt nach der erforderlichen Lebensdauer auszuwählen.

– Entscheidet sich ein Provider für die Vergabe statischer Präfixe an Endkunden, müssen diese Präfixe auf Wunsch des Kunden gewechselt werden können. Hierzu müssen dem Kunden einfache Bedienmöglichkeiten am Router oder am Endgerät zur Verfügung gestellt werden.

– Privacy Extensions müssen auf Endgeräten implementiert und sollten standardmäßig eingeschaltet sein. Ist dies nicht möglich, muss eine benutzerfreundliche manuelle Wechselmöglichkeit für den Interface Identifier bestehen.

– Zusätzlich sollten die Betriebssystem-Hersteller benutzerfreundliche Konfigurationsmöglichkeiten bereitstellen, mit denen Kunden die Wechselfrequenz des Interface Identifiers auf kurze Werte festlegen können bzw. einen Wechsel zu bestimmten Ereignissen anstoßen lassen können, z.B. beim Start des Browsers oder beim Start oder Aufwachen des Rechners.

– Interface Identifier und Präfix sollten synchron gewechselt werden.

– Um den Ortsbezug von Adressen zu verringern, sollten Provider die Adressen für Einwahl-Knoten und sonstige Infrastrukturkomponenten zufällig aus dem ganzen ihnen zur Verfügung stehenden Pool auswählen und regelmäßig innerhalb des Pools wechseln.

– Damit eine sichere und vertrauenswürdige Ende-zu-Ende-Kommunikation mit IPv6 unter Nutzung des Sicherheitsprotokolls IPsec möglich ist, müssen Hersteller von Betriebssystemen starke Verschlüsselungsalgorithmen im TCP/IP-Protokollstack implementieren.

– Die Endgerätehersteller sollten ihre Produkte mit korrekt und sinnvoll vorkonfigurierten IPv6-fähigen Paketfiltern ausstatten und diese über eine leicht zu bedienende Oberfläche zugänglich machen. Bei der Aktivierung der IPv6-Unterstützung im Router sollte die Aktivierung des Paketfilters automatisch stattfinden, dem Nutzer aber zumindest empfohlen werden.

– Hersteller von nicht IPv6-fähigen Firewalls (Firmware und Systemsoftware) sollten entsprechende Updates anbieten. Hersteller von IPv6-fähigen Firewalls sollten den Reifegrad ihrer Produkte regelmäßig prüfen und soweit erforderlich verbessern.

– IPv6-Adressen sind ebenso wie IPv4-Adressen personenbezogene Daten. Sofern eine Speicherung der Adressen über das Ende der Erbringung des Dienstes hinaus unzulässig ist, dürfen Provider und Diensteanbieter IPv6-Adressen allenfalls nach einer Anonymisierung speichern und verarbeiten. Ebenso ist die Ermittlung des ungefähren Standorts eines Endgerätes anhand der IPv6-Adresse für Provider und Diensteanbieter nur nach Anonymisierung der Adresse zulässig. Zur wirkungsvollen Anonymisierung der IPv6-Adressen sollten nach derzeitigem Kenntnisstand mindestens die unteren 88 Bit jeder Adresse gelöscht werden, d.h. der gesamte Interface Identifier sowie 24 Bit des Präfix.

– Der gemeinsame Betrieb von IPv6 und IPv4 auf einem Gerät (Dual-Stack-Betrieb) führt zu erhöhtem Gefahrenpotenzial und sollte daher vermieden werden. Dies gilt auch für die als Übergangslösung gedachten Tunnelprotokolle.

– Bestimmte Arten von Anonymisierungsdiensten sind dazu geeignet, die IP-Adressen von Nutzern wirksam zu verbergen. Auch Peer-to-Peer-Anwendungen können zu einem robusten und datenschutzfreundlichen, weil nicht an einzelnen Punkten stör- und überwachbaren Internet beitragen. Netzbetreiber können die Forschung auf diesem Gebiet unterstützen und selbst Anonymisierungsdienste anbieten. Die Verwendung von Anonymisierungsdiensten und Peer-to-Peer-Anwendungen darf durch Netzbetreiber nicht blockiert werden.

Mit der Orientierungshilfe „Datenschutz bei IPv6 - Hinweise für Hersteller und Provider im Privatkundengeschäft“ präzisieren die Datenschutzbeauftragten des Bundes und der Länder ihre Hinweise vom September 2011.

Abkürzungsverzeichnis

a.a.O.	am angegebenen Ort
a.D.	außer Dienst
a.F.	alte Fassung
Abs.	Absatz
AD	Active Directory
AFIG	Agrar- und Fischereifonds-Informationen-Gesetz
AKDB	Anstalt für Kommunale Datenverarbeitung in Bayern
AMRabG	Gesetz über Rabatte für Arzneimittel
AO	Abgabenordnung
App	Application, Anwendungsprogramm auf Smartphone
ARGE	Arbeitsgemeinschaft nach § 44 b SGB II
Art.	Artikel
ASV	Amtliches Schulverwaltungsprogramm
AVBayEAG	Ausführungsverordnung Einheitlicher Ansprechpartner
Az.	Aktenzeichen
BayArchivG	Bayerisches Archivgesetz
BayBG	Bayerisches Beamtengesetz
BayBhV	Bayerische Beihilfeverordnung
BayDSG	Bayerisches Datenschutzgesetz
BayEAG	Gesetz über die Zuständigkeit für die Aufgaben des Einheitlichen Ansprechpartners im Freistaat Bayern
BayEG	Bayerisches Gesetz über die entschädigungspflichtige Enteignung
BayEUG	Bayerisches Gesetz über das Erziehungs- und Unterrichtswesen
BayKrG	Bayerisches Krankenhausgesetz
BayKRG	Bayerisches Krebsregistergesetz
BayPrG	Bayerisches Pressegesetz
BayPVG	Bayerisches Personalvertretungsgesetz
BaySchwBerG	Gesetz über die Schwangerenberatung
BayStatG	Bayerisches Statistikgesetz
BayStVollzG	Bayerisches Strafvollzugsgesetz
BayVersG	Bayerisches Versammlungsgesetz
BayVGH	Bayerischer Verwaltungsgerichtshof
BayVSG	Bayerisches Verfassungsschutzgesetz
BayVwVfG	Bayerisches Verwaltungsverfahrensgesetz
BDSG	Bundesdatenschutzgesetz
BeamtStG	Beamtenstatusgesetz
BekV	Bekanntmachungsverordnung
BEM	Betriebliches Eingliederungsmanagement
BGB	Bürgerliches Gesetzbuch
BGBl.	Bundesgesetzblatt
BLKA	Bayerisches Landeskriminalamt
Bluetooth	Industriestandard für Datenübertragung über kurze Distanz per Funktechnik
BMG	Bundesministerium für Gesundheit
BSI	Bundesamt für Sicherheit in der Informationstechnik
BStatG	Bundesstatistikgesetz
Buchst.	Buchstabe
BV	Verfassung des Freistaates Bayern
BVerfG	Bundesverfassungsgericht

BVerfGE	Entscheidungen des Bundesverfassungsgerichts (zitiert nach Band und Seite)
BVerwG	Bundesverwaltungsgericht
BYOD	Bring Your Own Device
bzgl.	bezüglich
BZR	Bundeszentralregister
BZRG	Bundeszentralregistergesetz
bzw.	beziehungsweise
ca.	circa
CIO	Chief Information Officer
CSU	Christlich-Soziale Union in Bayern
d.h.	das heißt
DICOM	Digital Imaging and Communications in Medicine
DMS	Dokumentenmanagementsystem
DNA	Desoxyribonuclein Acid, Träger der Erbinformation
DNA-Analyse	Molekulargenetische Untersuchung
Doppelbuchst.	Doppelbuchstabe
e.V.	eingetragener Verein
EA	Einheitlicher Ansprechpartner
EDV	Elektronische Datenverarbeitung
eFA	elektronische Fallakte
EG	Europäische Gemeinschaft
ELENA	Elektronischer Entgeltnachweis
ELStAM	Elektronische Lohnsteuerabzugsmerkmale
ELSTER	Elektronische Steuererklärung
E-Mail	Elektronische Post
EOSS	Evolutionär Orientierte Steuer-Software
Erl.	Erläuterung(en)
EStG	Einkommensteuergesetz
etc.	et cetera
EU	Europäische Union
EuGH	Europäischer Gerichtshof
evtl.	eventuell
EWR	Europäischer Wirtschaftsraum
f.	folgende
FDP	Freie Demokratische Partei
ff.	fortfolgende
GBO	Grundbuchordnung
GdB	Grad der Behinderung
GDVG	Gesundheitsdienst- und Verbraucherschutzgesetz
gem.	gemäß
GEZ	Gebühreneinzugszentrale der öffentlich-rechtlichen Rundfunkanstalten
GG	Grundgesetz
ggf.	gegebenenfalls
GLKrWG	Gemeinde- und Landkreiswahlgesetz
GLKrWO	Gemeinde- und Landkreiswahlordnung
GmbH	Gesellschaft mit beschränkter Haftung
GO	Gemeindeordnung
GÜL	Gemeinsame elektronische Überwachungsstelle der Länder
i.S.d.	im Sinne des
i.V.m.	in Verbindung mit
IBA	Informationssystem für die Beschaffung und Auswertung

ICD	International Statistical Classification of Diseases and Related Health Problems
IfSG	Infektionsschutzgesetz
IGVP	Integrationsverfahren der Bayerischen Polizei
IKT	Informations- und Kommunikationstechnik
iMVS	integriertes Migrantenverwaltungssystem
INPOL	Informationssystem der Polizei (bundesweit)
IP	Internet Protocol
IPv4	Internet Protocol Version 4
IPv6	Internet Protocol Version 6
ISIS	Staatsschutz-Arbeitsdatei der Bayerischen Polizei
ISmed	Informationssystem der Medizinischen Dienste
IT	Informationstechnik
IuK	Informations- und Kommunikationstechnik
JGG	Jugendgerichtsgesetz
JuSchG	Jugendschutzgesetz
KAG	Kommunalabgabengesetz
KAN	Kriminalaktennachweis
KBV	Kassenärztliche Bundesvereinigung
Kfz	Kraftfahrzeug
KG	Kostengesetz
KIS	Krankenhausinformationssystem
KKG	Gesetz zur Kooperation und Information im Kinderschutz
KMS	Schreiben des Staatsministeriums für Unterricht und Kultus
KommZG	Gesetz über die kommunale Zusammenarbeit
KVB	Kassenärztliche Vereinigung Bayerns
KV-Nummer	Krankenversichertennummer
LfStaD	Landesamt für Statistik und Datenverarbeitung
LfV	Landesamt für Verfassungsschutz
Ltd.	Leitende(r)
m.E.	meines Erachtens
m.w.N.	mit weiteren Nachweisen
MAC	Media Access Control
MDK	Medizinischer Dienst der Krankenkassen
MdL	Mitglied des Landtages
MedHygV	Verordnung zur Hygiene und Infektionsprävention in medizinischen Einrichtungen
MeldDV	Meldedatenverordnung
MeldeG	Gesetz über das Meldewesen
NADIS	Nachrichtendienstliches Informationssystem
Nr.	Nummer
o.g.	oben genannt
OSCI	Online Services Computer Interface
OWA	Outlook Web Access / Outlook Web App
PAG	Polizeiaufgabengesetz
PC	Personalcomputer
PIN	Personell Identification Number
PsychThG	Gesetz über die Berufe des Psychologischen Psychotherapeuten und des Kinder- und Jugendlichenpsychotherapeuten
PVA	Polizeiverwaltungsamt
Rdnr.	Randnummer
RiStBV	Richtlinien für das Straf- und Bußgeldverfahren
RSA	Public-Key-Verschlüsselungsverfahren
S.	Seite

SchuFV	Schuldnerverzeichnisführungsverordnung
SchwbVWO	Wahlordnung Schwerbehindertenvertretungen
SDÜ	Schengener Durchführungsübereinkommen
SGB IX	Sozialgesetzbuch Neuntes Buch – Rehabilitation und Teilhabe behinderter Menschen
SGB V	Sozialgesetzbuch Fünftes Buch – Gesetzliche Krankenversicherung
SGB X	Sozialgesetzbuch Zehntes Buch – Sozialverwaltungsverfahren und Sozialdatenschutz
SGB	Sozialgesetzbuch
SIS	Schengener Informationssystem
sog.	sogenannt
SPD	Sozialdemokratische Partei Deutschlands
StDAV	Steuerdaten-Abrufverordnung
StGB	Strafgesetzbuch
StPO	Strafprozessordnung
StVG	Straßenverkehrsgesetz
TIZIAN	Gemeinsame EDV für den Gesundheitlichen Verbraucherschutz
TKÜ	Telekommunikationsüberwachung
TMG	Telemediengesetz
u.ä.	und ähnliches
u.a.	unter anderem
u.U.	unter Umständen
UrhG	Urheberrechtsgesetz
URL	Uniform Resource Locator
USB	Universal Serial Bus
UStG	Umsatzsteuergesetz
v.H.	von Hundert
vgl.	vergleiche
VollzBekMeldeG	Vollzugsbekanntmachung zum Meldegesetz
VPN	Virtuelles Privates Netz
VV	Verwaltungsvorschriften
WaffG	Waffengesetz
WO-BayPVG	Wahlordnung zum Bayerischen Personalvertretungsgesetz
z.B.	zum Beispiel
z.T.	zum Teil
ZBFS	Zentrum Bayern Familie und Soziales
ZEUGE	ZStV/BZR-Ermittlungs-Unterstützung auf der Grundlage von EOSS
ZEVIS	Zentrales Verkehrsinformationssystem
ZStV	Zentrales Staatsanwaltschaftliches Verfahrensregister

Stichwortverzeichnis