**Bayerischer Landtag**

16. Wahlperiode

Drucksache 16/**2100**

01.12.2009

# 23. Tätigkeitsbericht des Landesbeauftragten für den Datenschutz

**(gem. Art. 30 Abs. 5 des Bayerischen Datenschutzgesetzes)**

**Berichtszeitraum 2007/2008**

**(Die erst im Jahr 2009 in Kraft getretenen Gesetzesänderungen, insbesondere im**

- **Polizeiaufgabengesetz**
  **(Änderung der Befugnis zur Online-Durchsuchung; Streichung der Befugnis zur heimlichen Wohnungsdurchsuchung; Regelung der Benachrichtigungspflicht bei der „polizeilichen Beobachtung“; Verkürzung der Speicherfrist für Videoaufzeichnungen)**

- **Bayerischen Verfassungsschutzgesetz**
  **(Änderungen der Befugnisse zur Wohnraumüberwachung und Online-Durchsuchung; Streichung der Befugnis zur heimlichen Wohnungsdurchsuchung)**

- **Bayerischen Datenschutzgesetz**
  **(Verkürzung der Speicherfrist für Videoaufzeichnungen)**

**sind in diesem Tätigkeitsbericht nicht berücksichtigt. Dies gilt auch für die zum Bayerischen Versammlungsgesetz ergangene Eilanordnung des Bundesverfassungsgerichts vom 17.02.2009.)**

# Der Bayerische Landesbeauftragte für den Datenschutz

Nr. DSB/510 - 24 München, 01.12.2009

An die
Präsidentin
des Bayerischen Landtags
Frau Barbara Stamm
Maximilianeum
81627 München

## 23. Bericht über die Tätigkeit des Landesbeauftragten für den Datenschutz

Sehr geehrte Frau Landtagspräsidentin,

in der Anlage übersende ich gem. Art. 30 Abs. 5 des Bayerischen Datenschutzgesetzes den 23. Bericht über die Tätigkeit des Landesbeauftragten für den Datenschutz.

Mit freundlichen Grüßen

**Dr. Thomas Petri**

# 1 Dank

Am 01.07.2009 habe ich mein Amt angetreten, nachdem mich der Bayerische Landtag am 27.05.2009 auf Vorschlag der Staatsregierung gewählt hat.

Mit diesem Tätigkeitsbericht gebe ich Rechenschaft für die vielfältigen Aktivitäten meiner Dienststelle in den Jahren 2007 - 2008, für einen Zeitraum also, in dem sie teilweise von Herrn Dr. Karlheinz Worzfeld kommissarisch geleitet wurde. Herr Dr. Worzfeld hat diesen in seinen wesentlichen Bestandteilen längst fertig gestellten Tätigkeitsbericht nicht selbst dem Bayerischen Landtag vorgelegt, weil die Vorlagepflicht den jeweiligen **Landesbeauftragten für den Datenschutz** trifft. Ich möchte ihm an dieser Stelle für seine hervorragende Arbeit danken.

# 2 Ein Überblick: Datenschutz heute

Der Datenschutz befindet sich in einer Umbruchsituation. Der Präsident des Bundesverfassungsgerichts, Prof. Dr. Dres. h.c. Hans-Jürgen Papier, hat diese Umbruchsituation dahingehend charakterisiert, die Privatisierung der Informationstechnologie habe im Zusammenwirken mit der Globalisierung die Zahl potentieller „Big Brother“ unübersichtlich werden lassen. Es seien aus datenschutzrechtlicher Sicht eher anarchische Zustände als ein totalitärer Überwachungsstaat zu befürchten (vgl. Papier in Bundesbeauftragter für den Datenschutz und die Informationsfreiheit, 25 Jahre Volkszählungsurteil Datenschutz - Durchstarten in die Zukunft! 2009, S. 15). Ich kann dieser Analyse nur zustimmen und sie dahingehend ergänzen, dass die Verarbeitung personenbezogener Daten durch öffentliche und private Stellen - beispielsweise bei der Videoüberwachung - zunehmend verschränkt wird.

Bezogen auf die Kontrolle des Datenschutzes erweist sich die derzeitige Aufspaltung der Datenschutzaufsicht über den nicht-öffentlichen Bereich und der Datenschutzkontrolle über den öffentlichen Bereich nicht mehr als stimmig. Jenseits von europa- und verfassungsrechtlichen Fragen der Unabhängigkeit der jeweiligen Kontrollbehörde ist es nur schwer verständlich, warum der Bürger sich in der Rechtsmaterie Datenschutz an verschiedene Datenschutzbehörden wenden soll, zumal diese Zuständigkeitsabgrenzung mit einem erheblichen Mehraufwand an Personal bezahlt wird.

Die derzeit bestehende Umbruchsituation im Datenschutz veranlasst mich, in diesem Vorwort hauptsächlich Ausführungen zu seinen Perspektiven zu machen.

## 2.1 Datenschutz - alter und neuer grundrechtlicher Persönlichkeitsschutz

Wie meine Vorgänger im Amt betone ich, dass **Datenschutz Grundrechtsschutz** ist (Besonders pointiert hat dies mein Vorvorgänger Reinhard Vetter anlässlich seines ersten Tätigkeitsberichts getan, vgl. 16. Tätigkeitsbericht, 1994, Nr. 1.2). Grundrechte sind im Kern Antworten unseres freiheitlich-demokratischen Rechtsstaats auf tatsächliche Freiheitsbedrohungen für den Einzelnen.

Der Staat gewährt seinen Bürgerinnen und Bürgern bestimmte Freiheitssphären. Im Zusammenhang mit dem Datenschutz tut er dies, weil er einen bestimmten Persönlichkeitsschutz für ein freiheitliches demokratisches Gemeinwesen als schlechthin konstitutiv ansieht. In geringfügiger Abwandlung einer Feststellung im berühmten Volkszählungsurteil des Bundesverfassungsgerichts kann man sagen: Effektiver Datenschutz ist eine elementare Funktionsbedingung eines auf Handlungsfähigkeit und Mitwirkungsfähigkeit seiner Bürger begründeten freiheitlichen demokratischen Gemeinwesens.

Der Staat gewährt diese Rechte bewusst **dem Einzelnen** - gegen den Staat und durchaus auch gegen gesellschaftliche Interessen. Nach meiner Erfahrung besteht oft kein Verständnis dafür, warum eine staatliche Datenerhebung zum Wohl der Gemeinschaft unzulässig ist, weil „nur“ eine einzige Person Einwände gegen sie erhoben hat. Beispielsweise musste der Bundesgerichtshof für Strafsachen (BGH) eine Entscheidung des Landgerichts Kempten aufheben, weil Ermittlungsbehörden mit unfairen Mitteln gegen einen Untersuchungshäftling vorgegangen waren. Das Landgericht hatte es gebilligt, dass die Strafverfolgungsbehörden Gespräche eines Beschuldigten mit seiner Ehefrau im Besuchsraum während der Untersuchungshaft heimlich abhörten. Dabei erweckten die Strafverfolgungsbehörden bei dem Angeklagten gezielt den unrichtigen Eindruck, er könne sich mit seiner Ehefrau ohne die Gefahr der Überwachung über die ihm zur Last gelegten Straftaten unterhalten. Mit überzeugenden Gründen stellte der BGH fest, dass eine solche Vorgehensweise gegen den Grundsatz des fairen Verfahrens verstößt (BGH, U.v. 29.04.2009 - 1 StR 701/08). Die Entscheidung unterstreicht, dass der rechtsstaatliche Grundsatz des fairen Verfahrens eine erhebliche Datenschutzrelevanz hat.

### 2.1.1 Klassisches Verständnis von Datenschutz

Erfahrungsgemäß wird Datenschutz als grundrechtliche Gewährleistung oft allein mit dem **Schutz der Privatsphäre** gleichgesetzt, die vor staatlicher Ausforschung bewahrt. Diese Charakterisierung be-

schreibt einen wichtigen Teil des Datenschutzes. Er ist Gegenstand einer Vielzahl von verfassungsgerichtlichen Entscheidungen vor dem Jahr 1983 gewesen und nach wie vor aktuell. Datenschutz darf aber nicht auf den Schutz der Privatsphäre vor staatlicher Ausforschung reduziert werden.

Nicht übergangen werden darf zunächst das verfassungsrechtlich verbürgte **Recht des Einzelnen**, im Grundsatz **an** ihn betreffenden **Datenverarbeitungsprozessen gestaltend mitzuwirken**. Vor über fünfundzwanzig Jahren hat das Bundesverfassungsgericht in seinem berühmten Volkszählungsurteil vom 15.12.1983 den Begriff der „informationellen Selbstbestimmung“ geprägt. Dieses Recht auf informationelle Selbstbestimmung wird aus dem allgemeinen Persönlichkeitsrecht aus Art. 2 Abs. 1 und Art. 1 Abs. 1 des Grundgesetzes abgeleitet. Es besagt sinngemäß, dass der Einzelne auch im Zeitalter der automatisierten Datenverarbeitung grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten bestimmen können soll. Beispielsweise ist die Datenverarbeitung möglichst transparent zu gestalten: Daten sind grundsätzlich vorrangig bei den Betroffenen zu beschaffen. Im Regelfall haben die Betroffenen einen Anspruch auf Auskunft über die über sie erfassten Daten. Die Rechte auf Berichtigung, Löschung oder Sperrung gehören ebenfalls zu den Mitwirkungsrechten der Betroffenen.

In neueren Entscheidungen hat das Bundesverfassungsgericht den Begriff des **Grundrechts auf informationelle Privatheit** geprägt und damit das allgemeine Persönlichkeitsrecht in seiner verfassungsrechtlichen Terminologie an internationale Standards angepasst.

Kann dieses Grundrecht auf Datenschutz einschränkt werden? Sicherlich ist das möglich. Und natürlich ist der Mensch ein kommunikatives Wesen und kann sich nicht generell seiner Einbindung in kommunikative Prozesse der Gesellschaft entziehen. Für eine Einschränkung des Grundrechts auf Datenschutz ist es aber erforderlich, dass die Einschränkung im überwiegenden Allgemeininteresse erfolgt und bestimmte verfassungsrechtliche Anforderungen beachtet werden. Hierzu zählen unter anderem der Bestimmtheitsgrundsatz sowie das Verhältnismäßigkeitsprinzip. Gemäß dem Bestimmtheitsgrundsatz darf eine Verarbeitung personenbezogener Daten nur zu gesetzlich bestimmten Zwecken erfolgen. Er beugt einer allseitigen Überwachung vor, die dadurch entsteht, dass jede öffentliche Stelle alle Daten erhalten und nach Belieben verwenden kann. Dieser Tätigkeitsbericht greift das Erfordernis von gesetzlichen Regelungen insbesondere in Bezug auf die inzwischen erfolgte Neuregelung der Videoüberwachung im Bayerischen Datenschutzgesetz (Nr. 9.2) und hinsichtlich der weiterhin bestehenden gravierenden Regelungsdefizite im Maßregelvollzug (Nrn. 3.6 und 6.1.7) auf.

### 2.1.2 Neue Freiheitsbedrohungen - neue Datenschutzrechte

Der „traditionelle“ Grundrechtsschutz genügt heute nicht mehr für einen effektiven Datenschutz. Er gibt keine befriedigenden Antworten auf die Freiheitsgefährdungen unserer Zeit.

Daher hat das Bundesverfassungsgericht in seiner Entscheidung vom 27.02.2008 zur so genannten Online-Durchsuchung eine erste Konsequenz gezogen und aus dem Recht auf Privatheit das **„Recht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme“** abgeleitet. Das Gericht hat bei dieser Neuschöpfung deutlich darauf hingewiesen: Gesetzgebung, Verwaltung und Rechtsprechung haben künftig stärker zu berücksichtigen, dass die Nutzung der Informationstechnik für die Persönlichkeit und die Entfaltung des Einzelnen eine früher nicht absehbare Bedeutung erlangt hat. Das neue **„IT-Grundrecht“** wie das Recht auf Gewährleistung der Vertraulichkeit und Integrität häufig auch genannt wird, schützt zunächst die **Vertraulichkeit** eines IT-Systems. Das heißt, dass nur berechtigte Personen auf die im System verfügbaren Informationen zugreifen können. Weiterhin soll aber auch die **Integrität von IT-Systemen** gewährleistet werden.

Nach den Feststellungen des Bundesverfassungsgerichts ist selbst dann ein Eingriff in den Schutzbereich des IT-Grundrechts anzunehmen, wenn zum Beispiel Sicherheitsbehörden ein informationstechnisches System infiltriert haben, ohne dabei schon personenbezogene Daten erhoben zu haben. Die Beeinträchtigung der Integrität eines IT-Systems kann für den betroffenen Nutzer unter Umständen viel weiter reichende Nachteile haben als der Angriff auf die Vertraulichkeit.

Die Entscheidung des Bundesverfassungsgerichts zum IT-Grundrecht ist zwar im Zusammenhang mit der Befugnis zur Online-Durchsuchung, also einer staatlichen Ermittlungsmaßnahme, ergangen. Dieses Grundrecht beinhaltet aber auch einen **Schutzauftrag an den Staat** und wirkt dadurch in den gesellschaftlichen Raum hinein. Zumindest solange Online-Durchsuchungen technisch aufwändig bleiben, werden diese im Polizeiaufgabengesetz (PAG) und im Bayerischen Verfassungsschutzgesetz (BayVSG) geregelten Maßnahmen lediglich in Einzelfällen zu erwarten sein. Weitaus bedrohlicher als die - zahlenmäßig wohl seltenen - polizeilichen Zugriffe sind die massenweisen Angriffe auf IT-Systeme durch private Angreifer. Sie gehen beispielsweise von „privat“ betriebenen Botnetzen aus. Bei Botnetzen werden Computerprogramme (Bots) ohne Wissen der Besitzer auf ihren Computern installiert, welche dann für Zwecke des jeweiligen Angreifers missbraucht werden. Die meisten Bots können vom Angreifer über einen Kommunikationskanal beeinflusst werden und Befehle empfangen. Auf diese Weise fügen Cyber-

kriminelle Rechner von Privatpersonen in das Botnetz ein und verwenden sie wahlweise für das Versenden von Spam oder für gezielte Angriffe auf Dienste im Netz. Gefährliche Botnetze sind sogar geeignet, die allgemeine IT-Sicherheitslage nachhaltig zu beeinflussen (vgl. z.B. zum Botnetz „Waledac" Bundesamt für Sicherheit in der Informationstechnik, Quartalsbericht 1/2009 zur IT-Sicherheit).

Die technische Entwicklung hat gerade im Bereich der automatisierten Datenverarbeitung in den vergangenen Jahren gewaltige Fortschritte erzielt. Im Wesentlichen kann man von vier Entwicklungslinien sprechen: Informationstechnologie findet heute zumeist vernetzt statt, ihre Verwendung ist ein Massenphänomen, ihre Leistungsfähigkeit ist genauso immens gestiegen, wie sich die Größe bestimmter IT-Systeme verkleinert hat. Stecknadelgroße Kameras sind heute längst ebenso Realität wie der Einsatz von Nanotechnologie in Kliniken oder Handys, die als PC verwendet werden können und selbstverständlich den Zugang ins Internet ermöglichen. Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat wiederholt auf die Risiken hingewiesen, die mit dieser technischen Entwicklung einhergehen (z.B. Entschließung vom 04.04.2008, Berliner Erklärung: Herausforderungen für den Datenschutz zu Beginn des 21. Jahrhunderts, Anlage 14 dieses Tätigkeitsberichts).

### 2.2 Datenschutz trotz informationeller Selbstentblößung?

Ein Blick auf unsere **gesellschaftliche** Realität zeigt zugleich, dass zahlreiche Internetnutzer wie selbstverständlich Webtagebücher (Blogs) führen, die weltweit lesbar sind. Auf Plattformen wie Facebook oder StudiVZ geben sie persönliche, manchmal intimste Informationen preis, ohne dass sie Kontrolle über die einmal veröffentlichten Informationen haben. Denn der Satz „Das Internet vergisst nichts" gilt auch und insbesondere für soziale Netzwerke: Es ist nahezu unmöglich, die hinterlassenen Datenspuren im weltweiten Netz zu tilgen, was besonders für Beschäftigte gefährlich sein kann.

Die Risiken der Nutzung des Internet liegen auf der Hand: Unrichtige Informationen können oft nicht mehr korrigiert werden und holen die Nutzer später an unerwarteter Stelle wieder ein. Kaum ein Personalchef (auch von öffentlichen Stellen) verzichtet beispielsweise heute darauf, sich vor der Stellenbesetzung im Internet über die aussichtsreichen Bewerber und Bewerberinnen kundig zu machen. Dem setzt das Recht allerdings Grenzen: Auch wenn die Erhebung von im Internet frei zugänglichen personenbezogenen Daten durch eine öffentliche Stelle nicht generell einen Grundrechtseingriff darstellt, dürfen Daten nicht weiterverarbeitet werden, wenn die mit der Datenverarbeitung verfolgten Zwecke nicht im Einklang mit den datenschutzrechtlichen Rahmenbedingungen stehen. Jeder Betroffene würde informationell zum Freiwild, wenn man frei zugängliche Daten als frei verfügbar ansehen würde.

Es wäre eine zu einfache „Lösung", im Zusammenhang mit der Nutzung der neuen Möglichkeiten des Internet allein auf die Mündigkeit der Nutzer zu verweisen. Der Schutzauftrag des Grundrechts auf Privatheit erfordert eine Reaktion des Staates, wenn seine Bürgerinnen und Bürger vermeintlich selbstbestimmt informationelle Rechte aufgeben, tatsächlich aber oft gar nicht die Folgewirkungen ihres Verhaltens abschätzen können.

Deshalb halte ich jede Initiative der Staatsregierung zur **Stärkung der Medienkompetenz** vor allem junger Menschen für notwendig, insbesondere wenn und soweit sie auch den Selbstdatenschutz fördert.

### 2.3 Förderung von Selbstdatenschutz und Datenschutzkompetenz

Ich möchte die praktischen Schwierigkeiten des Selbstdatenschutzes anhand des Beispiels der **vertraulichen E-Mail-Kommunikation** ansprechen. Der Inhalt unverschlüsselter E-Mails kann mit einem gewissen technischen Aufwand leicht Beute unbefugter Personen werden. Dies bestätigen Stellen des Bundes und des Freistaates Bayern, die deshalb die Verschlüsselung von E-Mails empfehlen (z.B. Bundesamt für Sicherheit in der Informationstechnik, vgl. www.bsi.de, mit kostenlosen Downloads, nützliche Informationen sind auch auf meiner Website www.datenschutz-bayern.de unter der Rubrik Technik zu finden). Der prozentuale Anteil der E-Mail-Nutzer, die dieser Empfehlung folgen, ist verschwindend gering.

Eine Ursache hierfür ist sicher, dass es nur wenige bekannte Stellen gibt, die bei ihrer Kommunikation mit den Bürgerinnen und Bürgern die Verschlüsselung von E-Mails anbieten. Ähnlich wie das Anlegen des Sicherheitsgurts im PKW nur allmählich selbstverständlich geworden ist, ist auch die Akzeptanz von technik-gestütztem Selbstdatenschutz (wie Verschlüsselungstechnologie) schlichtweg eine Sache der Übung. Deshalb kann ich die Forderung der Datenschutzbeauftragten des Bundes und der Länder anlässlich ihrer 77. Konferenz vom 26./27.03.2009 nur unterstreichen, den **Einsatz datenschutzfreundlicher Technik** voranzutreiben und rechtlich verpflichtend vorzuschreiben. Ich würde mir wünschen, dass der Freistaat Bayern in diesem Sinne eine Vorreiterrolle übernimmt.

### 2.4 Zeitgerechte Datenschutzkontrolle im öffentlichen Bereich

Wie das Volkszählungsurteil des Bundesverfassungsgerichts verdeutlicht, ist die automatisierte Verwendung personenbezogener Daten für den Bürger oft undurchsichtig. Die Verwendung personenbezogener Daten begründet deshalb ein grundrechtlich geschütztes Interesse an einem vorgezogenen Rechtsschutz. Die Beteiligung **unabhängiger Datenschutzbeauftragter** ist insoweit von erheblicher Bedeutung für einen effektiven Schutz des Rechts auf informationelle Selbstbestimmung. Mit diesen Feststellungen hat das Bundesverfassungsgericht die unabhängige Kontrolle von Datenschutzbeauftragten verfassungsrechtlich abgesichert. Die Verfassung des Freistaates Bayern legt hierzu in Art. 33 a Abs. 2 fest, dass der Landesbeauftragte für den Datenschutz nach Maßgabe des Gesetzes bei den öffentlichen Stellen die Einhaltung der Vorschriften über den Datenschutz kontrolliert. Er ist in Ausübung seines Amtes unabhängig und nur dem Gesetz unterworfen. Der Bürger muss sich auch im Hinblick auf die Organisation und des Status des Landesbeauftragten für den Datenschutz darauf verlassen können, dass dieser in der Lage ist, seinem Anliegen ernsthaft nachzugehen und die Sach- und Rechtslage objektiv zu prüfen.

Selbstverständlich sehe ich es deshalb als wesentliche Aufgabe an, Eingaben schwerpunktmäßig und vorrangig zu bearbeiten. Allerdings muss eine zeitgerechte Datenschutzkontrolle auch berücksichtigen, dass ein vorgezogener Rechtsschutz aufgrund tatsächlicher Gegebenheiten leerlaufen kann. So sehen Sicherheitsbehörden oft aus verschiedenen Gründen davon ab, Betroffene über verdeckte Ermittlungsmaßnahmen zu informieren. Auch können Betroffene aus Sorge vor ihrer Bloßstellung darauf verzichten, von ihrem Eingaberecht Gebrauch zu machen. Wichtig ist daher ein **präventiv wirkender Datenschutz,** der unabhängig von konkreten Persönlichkeitsverletzungen einsetzt. Anlassfreie Prüfungen gehören zum unverzichtbaren Instrumentarium der Datenschutzkontrolle, das ich auch künftig anzuwenden gedenke.

### 2.5 Beteiligung an Gesetzgebungsverfahren

Auch im Sinne eines präventiv wirkenden Datenschutzes hat meine Dienststelle im Berichtszeitraum teilweise bis an die Grenzen ihrer personellen Belastbarkeit mit unterschiedlichem Erfolg an zahlreichen Gesetzesvorhaben beratend mitgewirkt bzw. auf die Notwendigkeit gesetzgeberischer Tätigkeit hingewiesen. Ich verweise insoweit auf die einschlägigen Beiträge dieses Berichts (Nrn. 4.1, 4.2, 4.9, 4.14, 5.1, 6.1.6, 6.1.7, 6.1.8, 6.1.9, 9.2, 10.1, 12.1, 12.2, 14.1, 14.4, 16, 17.9, 21.1, 22.2, 23.1, 23.3, 24.2).

Insbesondere auch bayerische Sicherheitsgesetze sind in den vergangenen Jahren Gegenstand von Verfassungsbeschwerdeverfahren geworden, die für die Beschwerdeführer zumindest Teilerfolge erbracht haben. Damit möchte ich noch einmal auf das Engagement meiner Mitarbeiter hinweisen, die mit zahlreichen Stellungnahmen dem Bundesverfassungsgericht zugearbeitet haben. Dabei entsprachen diese Stellungnahmen meines Hauses im Wesentlichen den späteren verfassungsgerichtlichen Feststellungen. Hervorzuheben sind die Stellungnahmen zum Versammlungsgesetz und zum Erfordernis einer Regelung zur Videoüberwachung im Bayerischen Datenschutzgesetz.

Im Hinblick auf die **Videoüberwachung** sind die Feststellungen des Bundesverfassungsgerichts zur Verfassungsrechtslage inhaltlich nahezu deckungsgleich mit den Hinweisen meiner Dienststelle (vgl. dazu Nrn. 3.9 und 9.1). Hinsichtlich des Versammlungsgesetzes ist bislang zwar erst eine einstweilige Anordnung ergangen, die aber ebenfalls die gleichen Bedenken aufgegriffen hat, auf die meine Dienststelle bereits hingewiesen hatte (vgl. Nrn. 3.3 und 4.2.).

Ungeachtet dessen ist es wünschenswert, dass den Stellungnahmen und Hinweisen jedoch auch dann ein angemessenes Gewicht beigemessen wird, wenn sie nicht das verfassungsrechtliche Mindestmaß, sondern auch Empfehlungen für datenschutzfreundliche Regelungen enthalten. Erfreulicherweise werden bereits im Rahmen der Ressortabstimmung solche Anregungen immer wieder aufgegriffen.

### 2.6 Öffentlichkeitsarbeit

In der Durchführung von Prüfungen und der beratenden Begleitung von Gesetzgebungsverfahren darf sich eine zeitgemäße Datenschutzkontrolle nicht erschöpfen. Ein weiteres wesentliches Instrument ist die Öffentlichkeitsarbeit. „Allgemeine Öffentlichkeitsarbeit“ ist bereits Aufgabe aller öffentlichen Stellen. Sie erwächst aus dem letztlich im Demokratiegrundsatz fußenden Prinzip der Transparenz und Publizität des staatlichen Handelns (vgl. Niese in Wilde et al., Kommentar zum BayDSG, Art. 19 BayDSG, Rdnr. 10). Diese Überlegung findet sich auch in der Allgemeinen Geschäftsordnung der Staatsregierung für die Behörden des Freistaates Bayern. Meine Öffentlichkeitsarbeit dient insoweit dazu, die Bürgerinnen und Bürger zum **Selbstdatenschutz** zu bewegen. Zugleich trägt sie zu einer lebendigen **Datenschutzkultur** bei, die unverzichtbare Voraussetzung für einen effektiven Datenschutz ist.

## 2.7 Transparenz hoheitlicher Datenverarbeitung und Datenschutz

Im vergangenen Sommer verursachte die europarechtliche Verpflichtung zur **Veröffentlichung der Empfänger von EU-Agrarsubventionen** eine erhebliche Unruhe. Als Rechtsgrundlage für die Veröffentlichung erging ein Bundesgesetz „zur Veröffentlichung von Informationen über die Zahlung von Mitteln aus den Europäischen Fonds für Landwirtschaft und Fischerei (AFIG)". Gleichwohl bewerteten obergerichtliche Entscheidungen die datenschutzrechtliche Zulässigkeit der Veröffentlichung sehr unterschiedlich. Vor diesem Hintergrund vertrat die Bayerische Staatsregierung zunächst die Auffassung, eine Veröffentlichung der Subventionsempfänger sei datenschutzrechtswidrig. Nunmehr veröffentlicht Bayern neben den vom AFIG geforderten Daten auch den jeweiligen Zweck der EU-Subvention. Nach meinem Eindruck wird erst dadurch ein sinnvoller und nachvollziehbarer Informationsertrag erzielt (vgl. dazu Beitrag „Presseecho" vom 10.08.2009 auf www.datenschutz-bayern.de).

Zugleich verdeutlicht der Vorfall, dass das Verhältnis zwischen der Transparenz staatlicher Datenverarbeitung und dem Datenschutz komplex ist und erhebliche Unsicherheiten erzeugt. Der Präsident des Bundesverfassungsgerichts, Herr Prof. Dr. Dres. h.c. Hans-Jürgen Papier, hat mit überzeugenden Erwägungen auf den engen Zusammenhang zwischen dem **Regelungskonzept einer informierten Öffentlichkeit** und dem Datenschutz hingewiesen. Zugleich hat er auf die erforderliche Abgrenzung zwischen dem Informationszugangsrecht und dem Schutz personenbezogener Daten aufmerksam gemacht (vgl. Papier in Bundesbeauftragter für den Datenschutz und die Informationsfreiheit, 25 Jahre Volkszählungsurteil Datenschutz - Durchstarten in die Zukunft! 2009, S. 19 f.).

Ein wesentlicher Gesichtspunkt zu einer solchen Abgrenzung wäre der Grundsatz der Verhältnismäßigkeit. Im Fall der Empfänger von EU-Agrarsubventionen war etwa zu berücksichtigen, dass sie im Internet weltweit veröffentlicht werden. Der Grundgedanke der EU-Vorgaben, die Vergabe von EU-Subventionen für die Allgemeinheit nachvollziehbar zu machen, hätte auch realisiert werden können, wenn man nur Empfänger von erheblichen Summen personenbezogen benannt und die Empfänger von geringfügigen Beträgen zu Gruppen gebündelt hätte.

Die Frage der Transparenz von EU-Agrarsubventionen ist bereichsspezifisch gesetzlich geregelt. Um vergleichbare Fragestellungen allgemein zu erfassen, haben sich - neben dem Bund - bereits elf Bundesländer dazu entschlossen, **Informationsfreiheitsgesetze** zu erlassen. Dabei nehmen bislang der Bundesbeauftragte für den Datenschutz sowie neun Landesbeauftragte für den Datenschutz jeweils die Funktion des Beauftragten für Informationsfreiheit wahr. Das hat Vorteile, weil die Fragen nach den Grenzen des Zugangs zu staatlich erfassten personenbezogenen Informationen maßgeblich durch den Datenschutz bestimmt sind. Informationsfreiheitsgesetze, die keinen Informationsbeauftragten vorsehen, existieren (nur) in zwei Bundesländern. In der EU nehmen die Datenschutzinstitutionen zahlreicher Mitgliedstaaten - z.B. in Frankreich oder in Ungarn - vergleichbar dem Bundesbeauftragten für Datenschutz und Informationsfreiheit die Funktion des Beauftragten für Informationsfreiheit wahr.

Dieser Trend, legitimen Informationsbedarf der Öffentlichkeit durch Informationsfreiheitsgesetze zu regeln, wird durch Initiativen wie die unseres Ministerpräsidenten zu seiner Zeit als Bundesminister für Ernährung, Landwirtschaft und Verbraucherschutz zur Schaffung eines Verbraucherinformationsgesetzes oder seiner Nachfolgerin zur Kennzeichnung von gentechnikfreien Lebensmitteln verstärkt.

Ein Bayerisches Informationsfreiheitsgesetz würde insoweit also für deutlich mehr Rechtssicherheit sorgen. Die hiergegen immer wieder vorgebrachten Bedenken - insbesondere die Beeinträchtigung der Funktionstüchtigkeit der Bayerischen Verwaltung - sind zwar ernst zu nehmen. Letztlich werden diese Befürchtungen durch die Erfahrungen anderer Bundesländer mit Informationsfreiheitsgesetzen jedoch nicht bestätigt.

## 2.8 Schlussbemerkungen

Die Bayerische Staatsregierung hat in ihrer Regierungserklärung am 10.12.2008 mit deutlichen Worten den politischen Stellenwert des Datenschutzes in den kommenden Jahren hervorgehoben. Hieran knüpfe ich an. Der Tätigkeitsbericht selbst weist nachfolgend auf positive und negative Entwicklungen hin. Zugleich zeigt er, dass der Datenschutz als Recht auf Privatheit eine der wichtigsten Herausforderungen unserer Zeit ist.

Im Übrigen weise ich darauf hin, dass im nachfolgenden Tätigkeitsbericht durchgängig die zum Redaktionsschluss gültigen Ressortbezeichnungen verwendet werden.

# 3 Schwerpunkte im Berichtszeitraum - ein Überblick

## 3.1 Grundsatzentscheidungen des Bundesverfassungsgerichts zur Online-Durchsuchung, automatisierten Kennzeichenerfassung und Vorratsdatenspeicherung

Der Berichtszeitraum war gekennzeichnet durch mehrere, wegweisende Grundsatzentscheidungen des Bundesverfassungsgerichts zu Eingriffsmaßnahmen von Polizei und Verfassungsschutz.

So hat das Gericht in seinem Urteil vom 27.02.2008 zur sog. Online-Durchsuchung aus dem Grundgesetz erstmals ein „Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme“ (sog. IT-Grundrecht) hergeleitet. Eingriffe in dieses Grundrecht - z.B. durch eine „Online-Durchsuchung“ - sind nach der Entscheidung nur zulässig bei Anhaltspunkten für eine konkrete Gefahr für überragend wichtige Rechtsgüter (vgl. auch Nrn. 4.1.2 und 5.1.4). Dazu zählen Leib, Leben und Freiheit der Person oder solche Güter der Allgemeinheit, deren Bedrohung die Grundlagen oder den Bestand des Staates oder die Grundlagen der Existenz der Menschen berührt („existenzielle Bedrohungslage“).

Wenige Tage später, am 11.03.2008, nahm das Gericht grundlegend Stellung zur sog. automatisierten Kennzeichenerfassung durch die Polizei. In diesem Urteil hat das Bundesverfassungsgericht den besonderen Eingriffscharakter der automatisierten Kennzeichenerkennung hervorgehoben: Soll die Maßnahme dazu dienen, die gewonnenen Informationen für weitere Zwecke zu nutzen (z.B. zur Erstellung eines Bewegungsprofils), besitze sie eine „besondere Schlagkraft und Eingriffsintensität“. Gegenstand der Entscheidung des Gerichts waren zwar gesetzliche Regelungen in Hessen und Schleswig-Holstein. Allerdings habe ich in der Folge gesetzliche Änderungen auch für Bayern gefordert, die zu einem maßgeblichen Teil in das Polizeiaufgabengesetz eingeflossen sind (vgl. Nr. 4.9).

In seiner ebenfalls am 11.03.2008 erlassenen Eilanordnung zur sog. Vorratsdatenspeicherung hat das Bundesverfassungsgericht betont, dass ein Abruf der auf Vorrat gespeicherten sog. Telekommunikationsverkehrsdaten durch Staatsanwaltschaften und Polizei zum Zweck der Strafverfolgung einen schwerwiegenden und nicht mehr rückgängig zu machenden Grundrechtseingriff darstellt. Das Gericht hat deshalb den Ermittlungsbehörden einen Zugriff auf diese Daten zur Strafverfolgung einstweilen nur dann gestattet, wenn - wie bei schweren Straftaten - auch die Telekommunikationsinhalte selbst überwacht werden dürften. Darüber hinaus hat das Bundesverfassungsgericht am 28.10.2008 auch den Abruf von auf Vorrat gespeicherten Daten durch die Polizei zur Gefahrenabwehr und durch das Landesamt für Verfassungsschutz einstweilen beschränkt. Diese Eilanordnungen lassen auch für die abschließende Entscheidung des Bundesverfassungsgerichts Einschränkungen der von mir stets abgelehnten Vorratsdatenspeicherung erhoffen (vgl. Nrn. 5.1.2, 6.1.3 ff.).

Ich habe darauf hingewirkt, dass bei den zahlreichen Änderungen der Strafprozessordnung, des Polizeiaufgabengesetzes und des Bayerischen Verfassungsschutzgesetzes die durch das Bundesverfassungsgericht geschaffenen Vorgaben eingehalten werden (vgl. Nrn. 4.1, 5.1 und 6.1.3).

## 3.2 Heimliche polizeiliche Wohnungsdurchsuchung verfassungsrechtlich problematisch

Auch in diesem Berichtszeitraum hat sich die Tendenz fortgesetzt, durch Änderung des Polizeiaufgabengesetzes das polizeiliche Instrumentarium um heimliche, tief in das Persönlichkeitsrecht eingreifende und z.T. verfassungsrechtlich problematische Eingriffsmaßnahmen zu erweitern. So wurde nicht nur die Befugnis geschaffen, unter bestimmten Voraussetzungen Daten heimlich aus privaten Computern zu erheben, zu verändern oder zu löschen (sog. Online-Durchsuchung, vgl. Nr. 4.12). Darüber hinaus wird die Polizei sogar ermächtigt, zur Vorbereitung einer Online-Durchsuchung, einer Telekommunikationsüberwachung oder einer Wohnraumüberwachung die Wohnung des Betroffenen heimlich zu betreten und heimlich zu durchsuchen (vgl. dazu Nr. 4.1.3). Dagegen hatte ich mich - leider erfolglos - ausgesprochen.

## 3.3 Polizeiliche Übersichtsaufzeichnungen von Versammlungen

Das Bayerische Versammlungsgesetz (BayVersG) regelt erstmals sog. Übersichtsaufnahmen und -aufzeichnungen von Versammlungsteilnehmern durch die Polizei und ihre zeitlich unbefristete Speicherung und Nutzung zu Zwecken der polizeilichen Aus- und Fortbildung (Art. 9 Abs. 2 und 3 BayVersG). In der Vergangenheit habe ich bei der datenschutzrechtlichen Überprüfung solcher Aufzeichnungen festgestellt, dass Versammlungsteilnehmer zum Teil individuell erkennbar gefilmt wurden. Darüber hinaus ist es grundsätzlich möglich, zunächst nicht eindeutig erkennbare Personen durch technische Mittel nachträglich zu individualisieren (vgl. Nrn. 4.2.3 und 4.2.4). Ich stehe deshalb solchen Aufzeichnungen kritisch gegenüber. Versammlungsteilnehmer können grundsätzlich nicht erkennen, ob eine Videokamera außer Betrieb ist, mit ihr Über-

sichtsaufzeichnungen oder personenbezogene Aufzeichnungen angefertigt werden. Das Bundesverfassungsgericht befürchtet, dass potentielle Versammlungsteilnehmer auf eine Teilnahme gerade deshalb verzichten, weil sie nicht abschätzen können, ob personenbezogene Informationen dauerhaft gespeichert werden und ihnen daraus Risiken entstehen können. Im Hinblick darauf habe ich im Gesetzgebungsverfahren gefordert, sog. Übersichtsaufzeichnungen im Gesetz ausdrücklich als „nicht personenbezogene Aufnahmen“ zu definieren und möglichst kurze Löschungsfristen festzulegen. Besser wäre allerdings, auf solche Aufzeichnungen völlig zu verzichten. Leider hat keine der beiden Forderungen Eingang in das Gesetz gefunden (vgl. Nr. 4.2.4).

### 3.4 Videoüberwachung von Versammlungsteilnehmern durch stationäre polizeiliche Kameras

Nachdem ich in den letzten Jahren eine Vielzahl polizeilicher Videoaufzeichnungen von Versammlungen datenschutzrechtlich geprüft hatte, die die Polizei mit mobilen Kameras angefertigt hatte (vgl. 22. Tätigkeitsbericht unter Nr. 4.15.4), habe ich in diesem Berichtszeitraum Aufzeichnungen stationärer Polizeikameras kontrolliert, die zur Überwachung öffentlicher Straßen und Plätze installiert sind (vgl. Art. 32 Abs. 2 PAG).

Schon die Kenntnis von Versammlungsteilnehmern, dass die stationären polizeilichen Videokameras (z.B. am Hauptbahnhof und Stachus in München) während einer Versammlung eingeschaltet bleiben, könnte Auswirkungen auf die Unbefangenheit der Teilnehmer haben. Das Grundrecht auf Versammlungsfreiheit (Art. 8 Abs. 1 GG) garantiert aber die möglichst unbeeinflusste Teilnahme des Einzelnen vor und bei Versammlungen und schützt damit auch davor, das Grundrecht im Visier von Polizei oder Verfassungsschutz wahrnehmen zu müssen.

Bei der datenschutzrechtlichen Kontrolle der Videoaufzeichnungen zu einer Versammlung habe ich festgestellt, dass personenbezogene Aufzeichnungen von Teilnehmern gefertigt worden waren, ohne dass die versammlungsrechtlichen Voraussetzungen dafür erfüllt waren (vgl. Nr. 4.13.2).

### 3.5 Keine Online-Durchsuchung und keine heimliche Wohnungsdurchsuchung für den Verfassungsschutz

Am 03.03.2004 hat das Bundesverfassungsgericht in einem Grundsatzurteil verfassungsrechtliche Anforderungen an die Wohnraumüberwachung („Großer Lauschangriff“) gestellt. Zu meinem Bedauern hat es über vier Jahre gedauert, bis die Regelungen der Wohnraumüberwachung für das Landesamt für Verfassungsschutz an diese Vorgaben angepasst wurden (vgl. Nr. 5.1.1).

Dabei wurde - wie bei der Änderung des Polizeiaufgabengesetzes - die Gelegenheit genutzt, neue tiefgreifende und z.T. verfassungsrechtlich problematische Eingriffsbefugnisse für das Landesamt für Verfassungsschutz in das Bayerische Verfassungsschutzgesetz aufzunehmen. Meine Kritik richtet sich dabei insbesondere dagegen, dass dem Verfassungsschutz Online-Durchsuchungen (vgl. Nr. 5.1.4) und sogar heimliche Wohnungsdurchsuchungen (vgl. Nr. 5.1.5) gesetzlich gestattet wurden. Das Bundesverfassungsgericht hat die Online-Durchsuchung nur zur Abwehr konkreter Gefahren für überragend wichtige Rechtsgüter zugelassen. Das Landesamt für Verfassungsschutz hat als „Frühwarnsystem“ der Staatsregierung aber die Aufgabe, im Vorfeld konkreter Gefahren Entwicklungen und Bestrebungen zu beobachten. Die Gefahrenabwehr selbst obliegt den Sicherheitsbehörden. Die ebenfalls neu geschaffene Befugnis zur heimlichen Wohnungsdurchsuchung dürfte schwerlich mit dem Grundgesetz (vgl. Art. 13 GG) zu vereinbaren sein, weil Art. 13 GG nach meinem Verständnis nur offene Wohnungsdurchsuchungen zulässt. Ich habe deshalb im Gesetzgebungsverfahren gefordert, auf die Möglichkeit der Online-Durchsuchung und der heimlichen Wohnungsdurchsuchung für das Landesamt für Verfassungsschutz zu verzichten (vgl. Nr. 5.1.4 f.).

### 3.6 Grundrechtseingriffe im Maßregelvollzug ohne ausreichende Rechtsgrundlage

Für Eingriffe in das Grundrecht auf informationelle Selbstbestimmung, die im Rahmen des sog. Maßregelvollzugs (z.B. Unterbringung eines Straftäters in einem psychiatrischen Krankenhaus oder in einer Entziehungsanstalt) erfolgen, enthält das bayerische Landesrecht keine ausreichenden Eingriffsgrundlagen. So fehlen solche z.B. für die in der Praxis durchgeführte Durchsuchung von Patientenzimmern, die erkennungsdienstliche Behandlung und die Videoüberwachung von Krankenzimmern. Angesichts der massiven Grundrechtseingriffe im Rahmen des Maßregelvollzugs halte ich die Herstellung eines verfassungskonformen Zustands für dringend geboten. Ich habe mich deshalb an die zuständige Staatsministerin gewandt (vgl. dazu unter Nr. 6.1.7).

### 3.7 Richtervorbehalt beachten

In der Praxis ist die Tendenz zu beobachten, dass Entscheidungen, die grundsätzlich dem unabhängigen Richter vorbehalten sind, von Ermittlungsbehörden (Polizei, Staatsanwaltschaft) getroffen werden. Das Bundesverfassungsgericht hat in den letzten Jahren in

mehreren Entscheidungen die Voraussetzungen und Grenzen einer auf Gefahr im Verzug gestützten Durchsuchungsmaßnahme aufgezeigt. Dabei hat es insbesondere betont, dass die Wahrung der Regelzuständigkeit des Richters sicherzustellen sei. Die Anordnung der Wohnungsdurchsuchung - aber auch jeder anderen Eingriffsmaßnahme, die der Gesetzgeber unter Richtervorbehalt gestellt hat - durch die Staatsanwaltschaft oder ihre Ermittlungspersonen muss daher der Ausnahmefall bleiben. Bei mehreren datenschutzrechtlichen Prüfungen habe ich festgestellt, dass die Vorgaben des Bundesverfassungsgerichts von bayerischen Ermittlungsbehörden nicht konsequent umgesetzt werden. So wurden sogar in Großstädten Eilanordnungen mit der Unerreichbarkeit von Richtern außerhalb der üblichen Dienstzeiten begründet, obwohl das Bundesverfassungsgericht bereits mit seinem Beschluss vom 28.09.2006 - dessen Gegenstand eine bayerische Großstadt war - klargestellt hat, dass der Richtervorbehalt dazu führe, dass auch außerhalb der üblichen Dienstzeiten die Erreichbarkeit des Ermittlungsrichters gewährleistet sein müsse (vgl. Nr. 6.2.1).

Für die Entnahme von Blutproben muss sogar festgestellt werden, dass hier der Richtervorbehalt nahezu vollständig ins Leere läuft. Trotz entgegenstehender Entscheidungen des Bundesverfassungsgerichts und von Obergerichten, in denen klargestellt wird, dass es Fallkonstellationen gibt, in denen der Ermittlungserfolg durch die Einschaltung des Ermittlungsrichters nicht gefährdet wird und damit nicht entbehrlich ist, habe ich eine Änderung der polizeilichen Praxis, insbesondere bei Alkoholverstößen im Straßenverkehr die Einschaltung eines Ermittlungsrichters regelmäßig zu unterlassen, nicht feststellen können (vgl. Nr. 6.3.5).

### 3.8 Weitergabe von personenbezogenen Informationen an die Presse

Durch die Veröffentlichung vor allem von bedeutsamen Urteilen oberer Gerichte soll die Öffentlichkeit über Rechtsentwicklungen informiert werden. Dies sehe ich als ein berechtigtes Anliegen an. Erfolgt die Veröffentlichung aber personenbezogen, wird erheblich in das Grundrecht auf informationelle Selbstbestimmung der davon Betroffenen eingegriffen. Sowohl bei der Entscheidung über das „Ob“ als auch das „Wie“ der Veröffentlichung muss deshalb das Persönlichkeitsrecht der Betroffenen mit dem Informationsinteresse der Öffentlichkeit abgewogen werden. Die Veröffentlichung von Urteilen in nicht anonymisierter Form halte ich im Ergebnis grundsätzlich für unzulässig. Allerdings reicht allein das Schwärzen der Namen für eine Anonymisierung oft nicht aus, da auch andere Angaben - wie z.B. Wohnort, Beruf, Alter - die Identifizierung der Betroffenen zumindest für einen bestimmten Personenkreis ermöglichen können. Auf weitere datenschutzrechtliche Anforderungen für den Umgang mit der Presse habe ich den Präsidenten eines Gerichts hingewiesen und ihn um zukünftige Beachtung gebeten (vgl. dazu unter Nr. 6.2.3).

Bei Übermittlung von personenbezogenen Informationen aus einem laufenden Ermittlungsverfahren durch die Staatsanwaltschaft an die Presse ist darüber hinaus insbesondere die Unschuldsvermutung zu beachten. Diese gebietet Zurückhaltung bei der behördlichen Publikation strafrechtlicher Beschuldigungen. Vor diesem Hintergrund halte ich Äußerungen von Staatsanwaltschaften zu internen Zwischenergebnissen eines laufenden Ermittlungsverfahrens für problematisch. Ich habe den Leiter einer Staatsanwaltschaft aufgefordert, dafür Sorge zu tragen, dass bei zukünftigen Presseauskünften die datenschutzrechtlichen Grundsätze berücksichtigt werden (vgl. dazu unter Nr. 6.3.10).

### 3.9 Beschluss des Bundesverfassungsgerichts zur Videoüberwachung öffentlicher Orte und Einrichtungen

Auch in diesem Berichtszeitraum war ich mit Fragen zur Videoüberwachung öffentlicher Orte und Einrichtungen befasst. Dazu hat das Bundesverfassungsgericht nunmehr eine grundlegende Entscheidung getroffen (Beschluss vom 23.02.2007 - 1 BvR - 2368/06). Dieser liegt die Videoüberwachung eines öffentlichen Ortes durch eine bayerische Kommune zugrunde, die diese auf Bestimmungen des Bayerischen Datenschutzgesetzes gestützt hatte.

Das Bundesverfassungsgericht hat dazu in der Begründung seines o.b. Beschlusses zu einer Verfassungsbeschwerde gegen die Videoüberwachung ausgeführt, dass die allgemeinen Regelungen des Bayerischen Datenschutzgesetzes nicht ausreichen, um eine Videoaufzeichnung auf öffentlichen Plätzen mit der Möglichkeit der Personenidentifizierung durchzuführen, sondern dass es hierzu einer speziellen Rechtsgrundlage bedarf. Dies sei die Folge des Eingriffs in das durch Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG gewährleistete allgemeine Persönlichkeitsrecht in seiner Ausprägung als Recht auf informationelle Selbstbestimmung.

Für die Beurteilung der Intensität des Eingriffs stellt das Bundesverfassungsgericht auf den von der Überwachung erfassten Personenkreis ab. Es liegt danach ein Eingriff von erheblichem Gewicht in das informationelle Selbstbestimmungsrecht vor, wenn von der Videoüberwachung öffentlicher Orte mit Aufzeichnung des gewonnenen Bildmaterials überwiegend Personen erfasst werden, die in keiner Beziehung zu einem konkreten Fehlverhalten stehen und den Eingriff durch ihr Verhalten nicht veranlasst haben. Verdachtslose Eingriffe mit großer Streubreite bei denen zahlreiche Personen in den Wirkungsbereich

einer Maßnahme einbezogen werden, die in keiner Beziehung zu einem konkreten Fehlverhalten stehen und den Eingriff durch ihr Verhalten nicht veranlasst haben, würden grundsätzlich eine hohe Eingriffsintensität aufweisen.

Bemerkenswert sind auch die Aussagen des Bundesverfassungsgerichts zu den Auswirkungen einer derartigen Videoüberwachung. Diese beeinträchtige alle, die den betroffenen Raum betreten würden. Sie diene dazu, belastende hoheitliche Maßnahmen vorzubereiten und das Verhalten der den Raum nutzenden Personen zu lenken. Das Gewicht dieser Maßnahme werde dadurch erhöht, dass infolge der Aufzeichnung das gewonnene Bildmaterial in vielfältiger Weise ausgewertet, bearbeitet und mit anderen Informationen verknüpft werden könne. Von den betroffenen Personen dürfte nur eine Minderheit gegen rechtliche Bestimmungen verstoßen. Die Videoüberwachung und die Aufzeichnung des gewonnenen Bildmaterials würden daher - wie bei solchen Maßnahmen stets - überwiegend Personen erfassen, die selbst keinen Anlass schaffen, deswegen die Überwachung vorgenommen werde.

Das Bundesverfassungsgericht hat allerdings auch betont, dass die Videoüberwachung öffentlicher Einrichtungen mit Aufzeichnung des gewonnenen Bildmaterials auf der Grundlage einer hinreichend bestimmten und normenklaren Ermächtigungsgrundlage materiell verfassungsgemäß sein kann. Der bayerische Gesetzgeber hat inzwischen in das Bayerische Datenschutzgesetz mit Art. 21 a eine Vorschrift eingefügt, mit der die Videobeobachtung und Videoaufzeichnung durch bayerische öffentliche Stellen unter bestimmten Voraussetzungen erlaubt wird (vgl. dazu Nr. 9.1).

### 3.10 Datenschutz bei Bürgerbegehren

Zu Bürgerbegehren habe ich mich wiederholt in meinen Tätigkeitsberichten geäußert, zuletzt im 21. Tätigkeitsbericht unter den Nrn. 2.1.4 und 11.11. Die bei der Gemeinde abgegebenen Unterschriftenlisten dürfen dort nur hinsichtlich der Frage ausgewertet werden, ob das Bürgerbegehren von einer ausreichenden Zahl stimmberechtigter Gemeindebürger unterschrieben worden ist. Diese Zweckbindung wird nicht immer beachtet. So ist mir im Berichtszeitraum bekanntgeworden, dass in einem Fernsehbericht über ein Bürgerbegehren Unterschriften mit personenbezogenen Daten von Unterstützern des Bürgerbegehrens gezeigt worden waren. Zu erkennen waren Nachnamen und Geburtsdaten von Unterzeichnern der Listen sowie teilweise auch die Vornamen und die Straßenbezeichnungen. Ein Mitarbeiter des Fernsehsenders hatte die Unterschriftenlisten in der Gemeindeverwaltung durchblättert und der Kameramann diesen Vorgang gefilmt. Die verantwortliche Gemeinde hätte hier ein Durchblättern und Aufzeichnen der Listen durch die Mitarbeiter des Senders verhindern müssen. Der Fall zeigt exemplarisch, dass zur Vermeidung einer Beeinträchtigung des Rechts auf informationelle Selbstbestimmung der Betroffenen ein sorgfältiger Umfang mit den erhaltenen Unterschriftenlisten und eine strikte Beachtung der Zweckbindung unerlässlich sind (vgl. dazu im Einzelnen Nr. 9.5).

### 3.11 Ein bemerkenswerter Einzelfall

Wohin Übereifer und mangelndes Datenschutzbewußtsein führen können, zeigt der folgende Fall: Ein Mitarbeiter eines Verkehrsbetriebs hatte zur Beitreibung einer Forderung gegen einen säumigen und nicht erreichbaren Kunden die Adressdaten der vermeintlichen Mutter des Kunden in Erfahrung gebracht. Tatsächlich handelte es sich jedoch um eine völlig unbeteiligte Dritte; die Namensgleichheit war rein zufällig. Die Verkehrsbetriebe forderten in der Folge die völlig überraschte Bürgerin auf, die neue Anschrift ihres (vermeintlichen) Sohnes zu nennen, verbunden mit der Drohung, andernfalls Strafanzeige wegen Betrugs zu stellen.

Hier liegen gleich mehrere Datenschutzverstöße vor. Zu einem wäre die Erhebung der Daten der vermeintlichen Mutter durch die Verkehrsbetriebe nicht zulässig gewesen. Bei dem Kunden der Verkehrsbetriebe handelte es sich nämlich um eine volljährige, geschäftsfähige Person. Eltern volljähriger und geschäftsfähiger Kinder sind weder verpflichtet Auskünfte über ihre Kinder an deren Vertragspartner zu erteilen, geschweige denn evtl. Zahlungsverpflichtungen aus dem Vertragsverhältnis zu übernehmen. Unzulässig war auch die Übermittlung von zum Teil sensiblen personenbezogenen Daten des Kunden des Verkehrsbetriebs an die vermeintliche Mutter. Um solchen gravierenden Datenschutzverstößen vorzubeugen sollten die öffentlichen Stellen ihren Mitarbeitern regelmäßig in geeigneter Weise, z.B. durch Rundschreiben oder im Rahmen von Schulungen, die Beachtung des Datenschutzes in der täglichen Arbeit ins Gedächtnis rufen (vgl. dazu Nr. 9.10).

### 3.12 Elektronische Steuerverwaltung - aber nicht ohne Datenschutz!

Mit hohem Tempo treibt die Steuerverwaltung den Umbau zu einer elektronischen Verwaltung voran. Im Mittelpunkt steht dabei das eGovernment-Projekt KONSENS (Koordinierte neue Software-Entwicklung der Steuerverwaltung), mit dem die Finanzminister der Länder das Ziel verfolgen, gemeinsam länderübergreifend einheitliche Software für das Besteuerungsverfahren zu entwickeln, zu beschaffen und einzusetzen. Das Projekt KONSENS umfasst eine Vielzahl von steuerlichen Fachverfah-

ren; bekanntestes Einzelverfahren ist wohl das unter bayerischer Federführung entwickelte Projekt ELSTER (Elektronische Steuererklärung). Eng verknüpft mit der (Weiter-)Entwicklung einzelner KONSENS-Verfahren ist die im Berichtszeitraum begonnene Zuteilung eines dauerhaften Identifikationsmerkmals an jeden Steuerpflichtigen - die sog. Steueridentifikationsnummer. Auf diesem Wege entsteht erstmals in der Geschichte der Bundesrepublik Deutschland und dauerhaft eine zentrale Bevölkerungsdatei. Die Erfahrungen der Vergangenheit geben Anlass zur Sorge, dass ein derart umfassender Datenpool über kurz oder lang die Begehrlichkeiten anderer Verwaltungen wecken und damit der Weg zu einem verfassungsrechtlich unzulässigen Personenkennzeichen („gläserner Bürger“) beschritten wird. Zu den aktuellen Entwicklungen im Steuerbereich rund um KONSENS nehme ich unter Nr. 11.1 ausführlich Stellung.

Mit dem „Gesetz zur Förderung der Steuerehrlichkeit“ hat der Bundesgesetzgeber den Finanzbehörden die Befugnis eingeräumt, die von den Kreditinstituten ursprünglich zur Bekämpfung illegaler Finanztransaktionen im Bereich des Terrorismus und der organisierten Kriminalität vorzuhaltenden Kontenstammdaten auch „zur Festsetzung und Erhebung von Steuern“ automatisiert abzurufen. Das Bundesverfassungsgericht hat diese Zweckänderung zwar im Ergebnis gebilligt, aus Transparenz- und Rechtsschutzgründen aber insbesondere eine (zumindest nachträgliche) Information des Steuerpflichtigen über einen durchgeführten Kontenabruf sowie eine entsprechende Dokumentation in den Steuerakten für erforderlich gehalten. Vor allem unter diesen Gesichtspunkten habe ich im Berichtszeitraum erneut die praktische Umsetzung des automatisierten Kontenabrufverfahrens bei einem bayerischen Finanzamt geprüft und dabei leider noch einige Mängel feststellen müssen (Nr. 11.2).

Hilfreich war das Bundesverfassungsgericht auch bei der Klärung eines weiteren, langjährigen Streitpunkts zwischen den Datenschutzbeauftragten und der Finanzverwaltung. So hat es im März 2008 klargestellt, dass der datenschutzrechtliche Auskunftsanspruch eines Betroffenen auch gegenüber der Steuerverwaltung gilt. Der Argumentation der Steuerverwaltung, dass die „absichtsvolle Nicht-Regelung“ eines Auskunftsrechts in der Abgabenordnung das allgemeine Datenschutzrecht verdränge, hat das Bundesverfassungsgericht nunmehr endgültig eine klare Absage erteilt (Nr. 11.3).

Einzelfälle von grundsätzlicher Bedeutung aus dem alltäglichen Umgang zwischen Steuerbürger und Finanzamt beleuchten schließlich die Nr. 11.4 (Reichweite von finanzamtlichen Auskunftsersuchen) und Nr. 11.5 (Nachweis von Krankheitskosten als außergewöhnliche Belastung).

### 3.13 Note 1 - leider noch nicht für den Datenschutz an Schulen

Wiederum stark in Anspruch genommen hat mich im Berichtszeitraum das weite Feld des Datenschutzes an Schulen.

Dies betraf zum einen Vorhaben von bayernweiter Bedeutung, wie zum Beispiel das eGovernment-Projekt „Amtliche Schuldaten“ und die Evaluation an Schulen. Nicht nur bei Eltern und Schülern, sondern auch bei Lehrern führen derartige umfangreiche Vorhaben zu teilweise tiefgreifenden Verunsicherungen und Befürchtungen im Hinblick auf den Schutz ihrer personenbezogenen Daten vor Zweckentfremdung und Missbrauch. Neben einer frühzeitigen, umfassenden Aufklärung und Information der Betroffenen ist deshalb eine datenschutzgerechte Ausgestaltung unabdingbare Voraussetzung für das Gelingen solcher (Groß-)Projekte.

Das bereits im letzten Berichtszeitraum begonnene eGovernment-Projekt „Amtliche Schuldaten“ habe ich weiterhin kritisch begleitet und im Wege intensiver und langwieriger Verhandlungen mit dem Kultusministerium erhebliche datenschutzrechtliche Verbesserungen erreichen können. Meine grundsätzlichen datenschutzrechtlichen Bedenken (keine amtliche Statistik, Festhalten an Totalerhebungen) bestehen aber fort (Nr. 23.1). Dagegen habe ich im Verlauf einer längeren Diskussion mit dem Kultusministerium erfreulicherweise erreichen können, dass die interne und externe Evaluation an bayerischen Schulen nunmehr auf eine tragfähige, normenklare und bestimmte Rechtsgrundlage gestützt ist, die dem Grundrecht auf informationelle Selbstbestimmung der Lehrer, Schüler und Eltern im Ergebnis in angemessener Weise Rechnung trägt (Nr. 12.1).

Zum anderen sind aber auch die einzelnen Schulen aufgefordert, bei ihrer Arbeit vor Ort die datenschutzrechtlichen Vorgaben einzuhalten. Nur wenn die Schulen das Grundrecht auf informationelle Selbstbestimmung selbst ernst nehmen, können sie den Schülerinnen und Schülern glaubwürdig vermitteln, beispielsweise bei der Nutzung des Internets auf die Gefährdungen für ihre Persönlichkeitsrechte zu achten, und damit letztlich dem verfassungsrechtlichen Bildungs- und Erziehungsauftrag gerecht werden. Generelle datenschutzrechtliche Brennpunkte an den Schulen waren und sind insbesondere Notenverwaltungsprogramme (dazu Nr. 12.2), Videoüberwachung (Nr. 12.2), Internetauftritt (Nr. 12.2 und 12.4) und Schülerbefragungen (Nr. 12.3), in Einzelfällen aber beispielsweise auch Schulchroniken (Nr. 12.5), Gesundheitsdaten in Schulzeugnissen (Nr. 12.6) und die öffentliche Bekanntgabe von Erziehungsmaßnahmen (Nr. 12.7).

### 3.14 TIZIAN

In dem EDV-Verfahren TIZIAN (Nr. 14.1) können die 105 in Bayern zuständigen Behörden in der Gesundheitsverwaltung personen- und betriebsbezogene Daten in einer zentralen und einheitlichen Datenbank zur Lebensmittel-, Veterinär- und Futtermittelkontrolle einstellen, aber auch behördenübergreifend lesen und abrufen. Das Projekt TIZIAN verdeutlicht damit sehr anschaulich die bereits bestehenden Möglichkeiten zur Zusammenführung von Daten und Datenbeständen in einer Datenbank. Technisch ist die Errichtung von automatisierten Verbunddateien heutzutage wahrlich keine unlösbare Aufgabe mehr. Aus der Sicht der Behörden ist es verständlich, dass so viele Informationen wie möglich zur Verfügung stehen sollen, um den Überwachungs- und Kontrollaufgaben, aber auch den Informationspflichten vor allem gegenüber der Europäischen Union gerecht zu werden. Das gilt insbesondere für den sensiblen Bereich des Verbraucher- und Gesundheitsschutzes. Es liegt im wohl verstandenen Interesse eines wirksamen gesundheitlichen Verbraucherschutzes, z.B. die Verursacher von Gammelfleischskandalen rasch ausfindig zu machen und in diesen Fällen die Bürger und Behörden frühzeitig zu warnen, um Gesundheitsgefahren abwehren zu können. An dieser Zielsetzung gibt es nichts auszusetzen, deshalb habe ich auch keine grundsätzlichen Einwendungen gegen die Notwendigkeit der Errichtung einer solchen Datenbank erhoben.

Allerdings ist es meine Aufgabe, auf vernünftige Regelungen für den Umgang mit einer solchen umfassenden Datenbank hinzuwirken, zumal damit ein erheblicher Eingriff in das informationelle Selbstbestimmungsrecht der Betroffenen verbunden ist. Eine meiner zentralen Forderungen besteht deshalb auch darin, die vielfältigen Datenerhebungen, -verarbeitungen und -nutzungen auf eine ausreichende gesetzliche Grundlage zu stellen, die den Anforderungen des Bundesverfassungsgerichts an eine klare und hinreichend bestimmte Rechtsgrundlage gerecht wird. Die bestehenden allgemeinen datenschutzrechtlichen Regelungen sind an diese Entwicklungen zur Vernetzung vorhandener Informationen durch alle beteiligten Behörden noch nicht angepasst und reichen für Verbunddateien dieses Ausmaßes nicht aus. Ich habe deshalb darauf gedrängt, dass solange keine Grundregeln für Verbunddateien bestehen, zumindest die wichtigsten datenschutzrechtlichen Anforderungen in speziellen Rechtsvorschriften festgelegt werden, insbesondere

- eine allgemeine Ermächtigung zur Errichtung einer Verbunddatei bzw. eines gemeinsamen und/oder verbundenen (automatisierten) Verfahrens

- der Zweck der Einrichtung einer Verbunddatei

- Angaben zum Inhalt und Umfang der Verbunddatei

- Angabe der öffentlichen Stellen, welche Daten in der Verbunddatei erheben, verarbeiten und nutzen

- Vorgaben z.B. zur Verantwortlichkeit, zu den Zugriffsberechtigungen, zu den Auskunftsregelungen, zur Protokollierung.

Eines möchte ich betonen: Auch wenn in diesem Fall die Errichtung einer Verbunddatei für die Aufgabenerfüllung der Gesundheitsbehörden sinnvoll sein kann, sollte von diesem Instrumentarium grundsätzlich nur sehr zurückhaltend Gebrauch gemacht werden. Eine Datensammlung dieses Ausmaßes sowie die umfangreichen Zugriffsmöglichkeiten darauf bergen immer die Gefahr einer missbräuchlichen Verwendung der Daten. Daran würde auch die Schaffung einer Rechtsgrundlage nichts ändern.

### 3.15 ELENA

Der Trend geht auch auf Bundesebene hin zu großen Datensammlungen in zentralen Datenbänken. Ein Beispiel dafür ist die Entwicklung des ELENA-Verfahrens, ehemals JobCard-Verfahren (Nr. 17.9). Mit diesem in der Öffentlichkeit bisher weitgehend unbeachteten Verfahren des elektronischen Entgeltnachweises wird eine der größten Datensammlungen mit personenbezogenen Daten in Deutschland geschaffen. Es werden Einkommensdaten von allen Beschäftigten, Beamten, Richtern und Soldaten gespeichert, ohne dass feststeht, ob die Daten im Einzelfall tatsächlich gebraucht werden. Die Nutzung dieser Daten ist bisher auf den Fall beschränkt, dass soziale Leistungen der Bundesagentur für Arbeit sowie der Elterngeld- und Wohngeldstellen beantragt werden. Es ist aber schon jetzt absehbar, dass die Nutzung der Daten künftig auch auf andere Sozialleistungsbereiche ausgeweitet werden soll.

Verfassungsrechtlich zulässig ist eine solche Datenbank nur, wenn zum Zeitpunkt der Speicherung deren Zweck bestimmt ist und wirksame technische, organisatorische und rechtliche Sicherungen gegen Zweckänderungen und Datenmissbrauch gewährleistet sind. Darauf hat die Konferenz der Datenschutzbeauftragten des Bundes und der Länder bereits wiederholt hingewiesen. Auf Initiative Bayerns hat die 76. Datenschutzkonferenz noch einmal eindringlich auf die verfassungsrechtlichen und technisch-organisatorischen Mängel des Verfahrens aufmerksam gemacht und eine Nachbesserung gefordert. Ich werde das Verfahren auch weiterhin kritisch verfolgen.

### 3.16 Hört und sieht der Chef denn alles? - Telekommunikation am Arbeitsplatz

Fast schon jahrzehntelanger Dauerbrenner in meiner täglichen Arbeit sind Anfragen von Bediensteten und Personalräten, aber auch von Mitarbeitern der Personalverwaltungen, ob und ggf. inwieweit am Arbeitsplatz eine Kontrolle von E-Mail und anderen Internetdiensten oder auch des klassischen Telefonverkehrs zulässig ist. In diesem Zusammenhang möchte ich zunächst darauf hinweisen, dass der Arbeitskreis Medien der Konferenz der Datenschutzbeauftragten des Bundes und der Länder unter meiner Mitwirkung seine „Orientierungshilfe zur datenschutzgerechten Nutzung von E-Mail und anderen Internetdiensten am Arbeitsplatz“ im Berichtszeitraum überarbeitet und aktualisiert hat (Nr. 22.1). Schließlich habe ich aber auch im Hinblick auf die „klassische Telefonie“ im Rahmen der Neufassung der Bekanntmachung über die „Einrichtung und Benutzung dienstlicher Telekommunikationsanlagen (TK-Bek)“ zahlreiche datenschutzrechtliche Verbesserungen erreichen können (Nr. 22.2). „Datenschutzskandale“ in diesem Bereich, wie bei der Deutschen Telekom oder der Deutschen Bahn, sind zumindest bislang in der bayerischen öffentlichen Verwaltung nicht bekannt geworden.

Von grundlegender Bedeutung in personaldatenschutzrechtlicher Hinsicht war im Übrigen die Neuordnung des Bayerischen Beihilferechts, mit der ich mich intensiv - und nicht ohne Erfolg - auseinander gesetzt habe (Nr. 21.1).

### 3.17 Die Volkszählung 2011 wirft ihre Schatten voraus …

Bereits in meinem letzten Tätigkeitsbericht hatte ich darauf aufmerksam gemacht, dass sich Deutschland an der kommenden Volkszählungsrunde der Europäischen Union im Jahr 2011 mit einem registergestützten Zensus beteiligen wird. Die letzte Volkszählung fand in den „alten“ Ländern im Jahr 1987, in den „neuen“ Ländern im Jahr 1981 statt.

Dem Zensus 1987 war eine breite und vielfach sehr emotionale Diskussion über die Reichweite des Rechts des Einzelnen vorausgegangen, über die Preisgabe und Verwendung seiner persönlichen Daten selbst bestimmen zu können. In deren Verlauf hatte das Bundesverfassungsgericht in seinem sogenannten „Volkszählungsurteil“ vom 15.12.1983 aus dem allgemeinen Persönlichkeitsrecht und der Menschenwürde das Grundrecht auf informationelle Selbstbestimmung gefolgert. Der kommende Zensus wird sich an diesem strengen Maßstab messen lassen müssen.

Der Zensus 2011 wird nach einem neuartigen, registergestützten Verfahren durchgeführt. Dabei werden in der Hauptsache Daten aus bestehenden Verwaltungsregistern zu einem bestimmten Stichtag bei den Statistischen Ämtern des Bundes und der Länder zusammengeführt. Ergänzt werden die aus den Registern gewonnenen Daten durch eine postalische Befragung der Eigentümer und Verwalter von Gebäuden und Wohnungen, durch eine 10%-ige Stichprobenerhebung zu erwerbs- und bildungsstatistischen Daten sowie durch Erhebungen in Gemeinschaftsunterkünften. Eine direkte Befragung aller Bundesbürger wird damit nicht stattfinden.

Nach dem Zensusvorbereitungsgesetz 2011 hat der Bundesgesetzgeber inzwischen auch das Zensusgesetz 2011 beschlossen. Ich war in beide Gesetzgebungsverfahren eingebunden und konnte gemeinsam mit meinen Kolleginnen und Kollegen in Bund und Ländern einige datenschutzrechtliche Verbesserungen erreichen. Aus datenschutzrechtlicher Sicht werde ich auch weiterhin die Vorbereitung und die Durchführung der Volkszählung 2011 kritisch begleiten (Nr. 23.3).

In den Zeiträumen zwischen den Volkszählungen dient der sogenannte „Mikrozensus“ dazu, die erhobenen Daten in kurzen Zeitabständen mit überschaubarem organisatorischem Aufwand zu überprüfen und gegebenenfalls zu korrigieren. An dieser amtlichen Repräsentativstatistik sind jährlich 1% aller Haushalte in Deutschland beteiligt („Kleine Volkszählung“). Insbesondere die im Mikrozensusgesetz angeordnete Auskunftspflicht führte auch im Berichtszeitraum wieder zu einer nicht unerheblichen Anzahl von Anfragen und Eingaben „ausgewählter“ Bürgerinnen und Bürger. Die „immerwährende“ Problematik des Mikrozensus gibt Anlass zu umfassenden und grundsätzlichen Ausführungen aus datenschutzrechtlicher Sicht (Nr. 23.2).

### 3.18 Datenschutz - auch bei Geodaten

Aktuell wird vor allem die bildmäßige Erfassung von Straßenzügen durch ein Privatunternehmen in der Öffentlichkeit kontrovers diskutiert („Google Street View“). Wenngleich sich auch meine auf bayerische öffentliche Stellen konzentrierte datenschutzrechtliche Kontrollkompetenz auf dieses Privatunternehmen nicht erstreckt, zeigt dieser Sachverhalt jedoch exemplarisch die stark zunehmende Bedeutung der - leider oftmals einseitig nur als „Ware“ angesehenen - Geodaten (Daten mit direktem oder indirektem Bezug zu einem bestimmten Standort oder geografischen Gebiet).

Aufgrund europarechtlicher Vorgaben sind die Mitgliedstaaten der Europäischen Union verpflichtet, eine Geodateninfrastruktur zu schaffen, um so den Zugang zu und die Nutzung von Geodaten für Bürger, Verwaltung und Wirtschaft europaweit zu vereinfachen. In Deutschland hat der Freistaat Bayern

als erstes Land ein Geodateninfrastrukturgesetz erlassen. Dem Gesetz liegen die „Musterempfehlungen für die Geodateninfrastrukturgesetzgebungen in den Ländern“ zugrunde, die von einer Länderarbeitsgruppe unter bayerischer Federführung erarbeitet wurden. Sowohl bei den „Musterempfehlungen“ als auch beim Bayerischen Geodateninfrastrukturgesetz habe ich mich für eine datenschutzgerechte Fassung eingesetzt. So konnte ich in intensiven Verhandlungen mit dem Staatsministerium der Finanzen an mehreren Stellen des Bayerischen Geodateninfrastrukturgesetzes Verweisungen auf das Bayerische Datenschutzgesetz erreichen, sodass im Ergebnis von einem „zweistufigen datenschutzrechtlichen Schutzkonzept“ gesprochen werden kann. Ich sehe darin einen großen Schritt zu einem angemessenen Ausgleich zwischen den berechtigten Interessen der Nutzer von Geodaten einerseits und den schutzwürdigen Belangen der Betroffenen andererseits (Nr. 24.2).

### 3.19 Der behördliche Datenschutzbeauftragte

Nach Art. 25 Abs. 2 Satz 1 BayDSG haben alle öffentlichen Stellen, die personenbezogene Daten mit Hilfe von automatisierten Verfahren verarbeiten oder nutzen, einen ihrer Beschäftigten zum behördlichen Datenschutzbeauftragten zu bestellen.

Nach wie vor besteht gelegentlich Unklarheit darüber, dass diese Vorschrift auch für Vereinigungen des privaten Rechts gilt, soweit sie Aufgaben der öffentlichen Verwaltung wahrnehmen (wie z.B. kommunale Krankenhäuser, Stadtwerke, Bäder und Verkehrswesen) und an denen eine oder mehrere juristische Personen des öffentlichen Rechts (wie z.B. ein Landratsamt oder eine Kommune) beteiligt sind.

Auch wenn gem. Art. 25 Abs. 2 Satz 2 BayDSG unter bestimmten Voraussetzungen für mehrere kleinere öffentliche Stellen die Möglichkeit besteht, einen gemeinsamen Datenschutzbeauftragten zu bestellen (vgl. 21. Tätigkeitsbericht Nr. 22.1.6), so ist doch festzuhalten, dass eine Aufgabenübertragung an externe Dritte grundsätzlich ausscheidet (vgl. Nr. 25.6.1).

Dem behördlichen Datenschutzbeauftragten kommt nach Art. 25 Abs. 4 BayDSG eine ganz wesentliche Rolle bei der Sicherstellung des Datenschutzes in der jeweiligen Behörde zu. Um dieser Aufgabe gerecht zu werden, hat der Gesetzgeber u.a. in Art. 26 Abs. 3 BayDSG bestimmt, dass dem behördlichen Datenschutzbeauftragte rechtzeitig vor dem Einsatz oder der wesentlichen Änderung eines automatisierten Verfahrens eine entsprechende Verfahrensbeschreibung zur Verfügung zu stellen ist. Diese benötigt er, um das Vorhaben nach datenschutzrelevanten Aspekten zu prüfen und zu bewerten.

Obwohl diese Vorschrift schon viele Jahre besteht, muss ich leider immer wieder feststellen, dass die Vorabbeteiligung und frühzeitige Einbindung des eigenen Datenschutzbeauftragten von öffentlichen Stellen in der Praxis nicht immer und nicht konsequent durchgeführt wird. Ohne eine eigene positive Bewertung des Vorhabens kann der behördliche Datenschutzbeauftragte keine datenschutzrechtliche Freigabe erteilen - erforderlichenfalls hat er nämlich auf Änderungen des Verfahrens zu drängen, die den Entwicklungsprozess nicht nur in zeitlicher sondern u.U. auch in finanzieller Hinsicht beeinflussen können. Eine fehlende datenschutzrechtliche Freigabe verbietet aber den Einsatz eines Verfahrens - dies muss bei der Projektplanung bereits berücksichtigt werden. Bei der datenschutzrechtlichen Freigabe durch den behördlichen Datenschutzbeauftragten handelt es sich also nicht lediglich um eine Formalie, sondern um einen wesentlichen und nicht entbehrlichen Teil eines IuK-Projektes. Der behördliche Datenschutzbeauftragte ist daher möglichst frühzeitig einzubinden, um unnötige Komplikationen und Zeitverzögerungen zu vermeiden (vgl. Nr. 25.4.6 und Nr. 25.5.5).

Um seine Überwachungsaufgaben wahrnehmen zu können, hat der Gesetzgeber dem behördlichen Datenschutzbeauftragten mit Art. 25 Abs. 4 Satz 2 BayDSG auch weitreichende Einsichtsrechte in Dateien und Akten zugewiesen. Abgesehen von den im Gesetz genannten Einschränkungen ist allgemein aber auch der Grundsatz der Erforderlichkeit des Zugriffs zu beachten. So ist es sicher nicht erforderlich, dass dem behördlichen Datenschutzbeauftragten ein genereller unmittelbarer Zugriff auf alle Dateien einer öffentlichen Stelle ermöglicht wird - sehr wohl aber ein Zugriff im konkreten Einzelfall (vgl. Nr. 25.4.5).

### 3.20 E-Mails und Fernmeldegeheimnis

In Nr. 23.3. des 22. Tätigkeitsberichts bin ich ausführlich auf Spam-Behandlung eingegangen. In diesem letzten Berichtszeitraum haben sich hingegen die Anfragen gehäuft, wie mit den elektronischen Postfächern ausgeschiedener/versetzter Mitarbeiter zu verfahren ist. Im Grundsatz sind darauf eingehende E-Mails dabei genauso zu behandeln, als wäre der betreffende Mitarbeiter noch aktiv im Dienst - Näheres hierzu unter Nr. 25.4.3.

### 3.21 IP-Protokollierung auf Webservern

Die Frage der Protokollierung der IP-Adressen von Besuchern eines Web-Servers bewegt - nicht zuletzt aufgrund entsprechender Urteile - unverändert die Gemüter. Grundsätzlich halte ich die Protokollierung personenbezogener Daten auf einem Webserver einer

bayerischen Behörde, insbesondere der IP-Adresse der Besucher von Webseiten, für nicht zulässig. Auf Sicherheitsinstanzen, wie z.B. einer vorgeschalteten Firewall, kann m.E. unter Beachtung einer strikten Zweckbindung aus Gründen der IT-Sicherheit eine Protokollierung von IP-Adressen für maximal sieben Tage erfolgen. Eine ausführliche Darstellung und Bewertung der Angelegenheit gebe ich in Nr. 25.2.

### 3.22 Datenschutzgerechte Entsorgung

Bereits im letzten Absatz der Nr. 3.19 meines 22. Tätigkeitsberichts hatte ich angemahnt, über die Einführung und datenschutzgerechte Nutzung der IuK-Technik nicht die „konventionelle“ Datenverarbeitung zu vergessen. Leider hat dies aber nicht in allen Fällen gefruchtet und so gab es auch in diesem Berichtszeitraum einige Anfragen und diesbezügliche Probleme. Eine umfassende Problemdarstellung mit entsprechenden Handlungshinweisen findet sich in Nr. 25.4.7.

## 4 Polizei

Meine Kontrolle im Polizeibereich umfasste nicht nur Speicherungen in Dateien, wie z.B. im Kriminalaktennachweis, der Staatsschutzdatei, der Antiterrordatei (ATD), der „Haft-Entlassenen-Auskunfts-Datei-Sexualstraftäter“ (HEADS), sowie in weiteren Dateien, insbesondere in regional geführten GAST-Dateien. Überprüft habe ich auch Datenerhebungsmaßnahmen wie beispielsweise Entnahmen von Speichelproben zum Zwecke der DNA-Analyse sowie Maßnahmen der präventiven Telekommunikationsüberwachung, soweit sie nicht bereits gerichtlich überprüft worden waren. Polizeiliche Datenerhebungen und -speicherungen im Zusammenhang mit der automatisierten Kennzeichenerkennung sowie der Videoüberwachung öffentlicher Straßen und Plätze und von Versammlungen waren weitere Prüfungsschwerpunkte.

Datenübermittlungen der Polizei, z.B. an die Presse, Abfragen im polizeilichen Informationssystem durch Polizeibedienstete sowie Auskünfte an Betroffene über polizeiliche Speicherungen zu ihrer Person habe ich ebenfalls überprüft. Daneben habe ich anlassabhängig aufgrund von Bürgereingaben, Pressemitteilungen oder sonstigen Hinweisen aber auch anlassunabhängig Prüfungen vor Ort beim Landeskriminalamt, bei zwei Präsidien und einer Polizeidirektion durchgeführt.

Darüber hinaus habe ich auf eine datenschutzkonforme Fassung von Gesetzen und Verwaltungsvorschriften hingewirkt, soweit sie Befugnisse zum Eingriff in das informationelle Selbstbestimmungsrecht durch die Polizei zum Gegenstand hatten. Schwerpunkte waren in diesem Zusammenhang Stellungnahmen zur Novellierung des Polizeiaufgabengesetzes (PAG), insbesondere zur vorgesehenen Befugnis der Durchsuchung von Wohnungen als „Begleitmaßname“ der „Online-Durchsuchung“, und zum Entwurf eines Bayerischen Versammlungsgesetzes. Ich habe mich dafür eingesetzt, dass die Gesetzentwürfe die verfassungsrechtlichen Vorgaben, insbesondere hinsichtlich Normenklarheit, Bestimmtheit und Verhältnismäßigkeit, beachten und ausreichende Schutzvorkehrungen für den Kernbereich privater Lebensgestaltung enthalten. Außerdem habe ich auch zahlreiche Errichtungsanordnungen, die die wesentlichen Festlegungen für polizeiliche Dateien enthalten, geprüft und an Prüfungen bundesweiter polizeilicher Dateien mitgewirkt.

Meine datenschutzrechtliche Beratung der Polizei umfasste auch Vorträge bei Aus- und Fortbildungsveranstaltungen.

Die nachfolgende Darstellung ist eine Auswahl meiner Feststellungen im Polizeibereich.

### 4.1 Gesetz zur Änderung des Polizeiaufgabengesetzes

In meinem letzten Tätigkeitsbericht (vgl. Nr. 4.8) habe ich auf die Notwendigkeit hingewiesen, die Befugnis zur präventiven Rasterfahndung (Art. 44 PAG) baldmöglichst an die Entscheidung des Bundesverfassungsgerichts zur präventiven Rasterfahndung vom 04.04.2006 anzupassen.

Die Feststellungen des Bundesverfassungsgerichts können aber auch Bedeutung für andere polizeiliche Eingriffsmaßnahmen haben, die - wie die Rasterfahndung - sowohl durch Verdachtslosigkeit als auch durch eine große Streubreite gekennzeichnet sind, bei denen also zahlreiche Personen in den Wirkungsbereich einer Maßnahme einbezogen werden, die in keiner Beziehung zu einem konkreten Fehlverhalten stehen und den Eingriff durch ihr Verhalten nicht veranlasst haben. Ich habe deshalb das Staatsministerium des Innern gebeten, im Polizeiaufgabengesetz über die Rasterfahndungsbefugnis hinaus weitere polizeiliche Eingriffsnormen (z.B. automatisierte Kennzeichenerfassung, Anfertigung von Bild- und Tonaufnahmen) datenschutzkonform auszugestalten. Darüber hinaus halte ich es für verfassungsrechtlich geboten, die von der „Polizeilichen Beobachtung“ betroffenen Personen grundsätzlich nach Abschluss der Maßnahme zu benachrichtigen (vgl. dazu Nr. 4.1.4).

Das Staatsministerium des Innern hat mir am 06.03.2007 einen Referentenentwurf zur Änderung des Polizeiaufgabengesetzes übersandt, der die Anpassung der Befugnis zur Rasterfahndung an die Vorgaben des Bundesverfassungsgerichts zum Ziel hatte. Ich bedaure, dass meine o.g. Forderungen, auch

andere polizeiliche Eingriffsmaßnahmen datenschutzkonform auszugestalten, nicht aufgegriffen wurden.

Die CSU-Fraktion hat im Rahmen des o.g. Gesetzgebungsverfahrens mehrere Änderungsanträge in den Landtag eingebracht. Damit sollten die Befugnis zur automatisierten Kennzeichenerfassung an die Anforderungen des Urteils des Bundesverfassungsgerichts vom 11.03.2008 angepasst (vgl. Nr. 4.1.1) und die Polizei mit neuen, tiefgreifenden und z.T. verfassungsrechtlich bedenklichen Befugnissen (Online-Durchsuchung, heimliche Wohnungsdurchsuchung, vgl. Nrn. 4.1.2 und 4.1.3) ausgestattet werden.

Zu dem Gesetzentwurf und den Änderungsanträgen habe ich gegenüber dem Staatsministerium des Innern und den zuständigen Ausschüssen des Landtags ausführlich Stellung genommen. Der Landtag hat das Gesetz am 03.07.2008 beschlossen. Es ist am 01.08.2008 in Kraft getreten.

### 4.1.1 Automatisierte Kennzeichenerkennung

Im Rahmen des Gesetzgebungsverfahrens zur Änderung der Befugnis zur polizeilichen Rasterfahndung (Art. 44 PAG) hat die CSU-Fraktion einen Änderungsantrag eingebracht mit dem Ziel, die Befugnis zur automatisierten Kennzeichenerfassung an das Urteil des Bundesverfassungsgerichts vom 11.03.2008 anzupassen. Zuvor hatte ich das Staatsministerium des Innern auf eine Reihe verfassungs- und datenschutzrechtlich problematischer Punkte der bisherigen Regelung hingewiesen (vgl. Nr. 4.1).

Die Neufassung der Befugnis berücksichtigt meine Forderungen zum Teil:

- Art. 33 Abs. 2 Satz 3 PAG enthält nunmehr eine nähere Bestimmung der polizeilichen Fahndungsbestände, mit denen ein Abgleich der erfassten Kennzeichen erfolgen darf.

- Die Befugnis, die erhobenen Daten zur Verfolgung von Ordnungswidrigkeiten zu verwenden, wurde in Art. 38 Abs. 3 Satz 2 PAG gestrichen.

Leider wurde die automatisierte Kennzeichenerfassung nicht ausdrücklich auf Stichprobenkontrollen beschränkt. Darüber hinaus ist nicht vorgesehen, dass Lageerkenntnisse, auf die sich die Maßnahme stützt, gemäß dem Urteil des Bundesverfassungsgerichts dokumentiert sein müssen. Im Gegensatz zur Begrenzung der Fahndungsbestände ist die Umschreibung der „anderen polizeilichen Dateien“, mit denen ein Abgleich der Kfz-Kennzeichen möglich ist, wenig präzise. Sie ermöglicht einen Abgleich mit nahezu allen polizeilichen Dateien.

### 4.1.2 Online-Durchsuchung

Das Bundesverfassungsgericht hat sich in seinem Urteil vom 27.02.2008 erstmals zur verfassungsrechtlichen Zulässigkeit der sog. Online-Durchsuchung und zu den Anforderungen an diese Maßnahme geäußert sowie deren Grenzen aufgezeigt. Das Gericht ist dabei davon ausgegangen, dass die Nutzung der Informationstechnik für die Persönlichkeit und die Entfaltung des Einzelnen eine früher nicht absehbare Bedeutung erlangt hat. Die moderne Informationstechnik eröffne dem Einzelnen neue Möglichkeiten, begründe aber auch neuartige Gefährdungen der Persönlichkeit.

Zum Schutz der Nutzer informationstechnischer Systeme vor diesen neuartigen Gefährdungen hat das Bundesverfassungsgericht aus dem Grundgesetz erstmals ein „Grundrecht auf Gewährleistung der Integrität und Vertraulichkeit informationstechnischer Systeme“ hergeleitet. Einen heimlichen Eingriff in dieses Grundrecht, wie er durch die sog. Online-Durchsuchung erfolgt, hat es nur unter besonderen, eng begrenzten Voraussetzungen zugelassen. Das Bundesverfassungsgericht hebt die besondere Schwere des Grundrechtseingriffs der Online-Durchsuchung hervor, die durch einen heimlichen Zugriff auf ein fremdes informationstechnisches System („technische Infiltration“) die längerfristige Überwachung der Nutzung des Systems und die laufende Erfassung der entsprechenden Daten ermöglicht.

Wegen der besonderen Schwere des Eingriffs fordert das Gericht tatsächliche Anhaltspunkte einer konkreten Gefahr für ein überragend wichtiges Rechtsgut. Überragend wichtig sind nach der Entscheidung Leib, Leben und Freiheit der Person oder solche Güter der Allgemeinheit, deren Bedrohung die Grundlagen oder den Bestand des Staates oder die Grundlagen der Existenz der Menschen berührt.

Es müssen bestimmte Tatsachen auf eine im Einzelfall durch bestimmte Personen drohende Gefahr für ein solch wichtiges Rechtsgut hinweisen. Die Tatsachen müssen dabei den Schluss auf ein wenigstens seiner Art nach konkretisiertes und zeitlich absehbares Geschehen zulassen. Der heimliche Zugriff auf informationstechnische Systeme muss grundsätzlich von einem Richter angeordnet werden.

Darüber hinaus fordert das Gericht, dass eine gesetzliche Regelung, die zur Online-Durchsuchung ermächtigt, den verfassungsrechtlich gebotenen Schutz des Kernbereichs privater Lebensgestaltung sicherstellen muss. Erforderlich sei ein zweistufiges Schutzkonzept, wonach in einer ersten Stufe die Erfassung kernbereichsrelevanter Daten soweit möglich unterbleibt. Ergibt die Durchsicht (Zweite Stufe), dass kernbereichsrelevante Daten erhoben wurden, sind diese unverzüglich zu löschen. Eine Weitergabe oder Verwertung ist auszuschließen.

Auf Anfrage hat mir der Staatsminister des Innern mit Schreiben vom 10.04.2007 mitgeteilt, dass weder die Polizei zur Gefahrenabwehr noch das Landesamt für Verfassungsschutz Online-Durchsuchungen in den drei vorangegangenen Jahren durchgeführt hätten. Für den Bereich der Strafverfolgung verweise ich auf meine Ausführungen unter Nr. 6.1.2.

Die Datenschutzbeauftragten des Bundes und der Länder begrüßen, dass das Bundesverfassungsgericht das neue Grundrecht mit besonders hohen verfassungsrechtlichen Hürden vor staatlichen Eingriffen schützt. Sie haben auf ihrer Konferenz am 03. und 04.04.2008 in Berlin die Gesetzgeber in Bund und Ländern aufgefordert, die Erforderlichkeit von Online-Durchsuchungen kritisch zu hinterfragen (vgl. die Entschließung der 75. Datenschutzkonferenz „Vorgaben des Bundesverfassungsgerichts bei der Online-Durchsuchung beachten“, Anlage Nr. 18).

Die CSU-Fraktion im Bayerischen Landtag hat am 02.04.2008 im Rahmen des Gesetzgebungsverfahrens zur Neufassung der Befugnis zur Rasterfahndung einen Änderungsantrag eingebracht. Ziel war insbesondere, in das Polizeiaufgabengesetz eine Befugnis zur „Online-Durchsuchung“ einzufügen. Diese gestattet der Polizei nicht nur, Daten aus informationstechnischen Systemen unter bestimmten Voraussetzungen zu erheben, sondern bei gegenwärtiger Gefahr für Leib, Leben oder Freiheit einer Person auch zu löschen oder zu verändern.

Die Schaffung einer Befugnis zur „Online-Durchsuchung“ setzt eine seit Jahren zu beobachtende Entwicklung fort, der Polizei immer wieder neue, zum Teil tiefgreifende Eingriffsbefugnisse einzuräumen, die das Recht auf informationelle Selbstbestimmung zunehmend einschränken. Von solchen Eingriffen sind nicht nur Verantwortliche oder Störer im Sinne des Polizeirechts betroffen, sondern im großen Umfang auch und gerade Nichtverantwortliche und Nichtstörer. So darf die Polizei auf informationstechnische Systeme von Nichtverantwortlichen und Nichtstörern zugreifen, soweit bestimmte Tatsachen die begründete Annahme rechtfertigen, dass Verantwortliche für eine Gefahr oder potentielle Straftäter diese Systeme benutzen oder benutzt haben (vgl. Art. 34 d Abs. 1 Satz 1 Nr. 3 Buchstabe b PAG n.F.).

In einer ausführlichen Stellungnahme habe ich die zuständigen Ausschüsse im Landtag auf meine zum Teil grundlegenden datenschutzrechtlichen Bedenken hingewiesen. Dadurch konnten erhebliche Verbesserungen erreicht werden. Die Aufzählung von Straftaten, zu deren Abwehr die Online-Durchsuchung zulässig ist („Anlasstatenkatalog“), wurde nahezu ausschließlich auf solche Straftatbestände beschränkt, die zum Schutz überragend wichtiger Rechtsgüter bestehen. Neben dem Schutz von Leib, Leben und Freiheit der Person fallen darunter nur Güter der Allgemeinheit, deren Bedrohung die Grundlagen oder den Bestand des Staates oder die Grundlagen der Existenz der Menschen berührt (existenzielle Bedrohungslage).

Nicht berücksichtigt wurden vor allem meine nachstehenden Forderungen:

- Streichung der Befugnis der Polizei, zur Durchführung einer Online-Durchsuchung auch die Wohnung heimlich zu durchsuchen. Eine solche Durchsuchung sieht das Grundgesetz nicht vor (vgl. dazu Nr. 4.1.3).

- Schutz des Zeugnisverweigerungsrechts engster Familienangehöriger (vgl. § 52 StPO). Aus einer Online-Durchsuchung gewonnene Erkenntnisse sollten nur verwertet werden dürfen, wenn dies unter Berücksichtigung der Bedeutung des zugrundeliegenden Vertrauensverhältnisses nicht außer Verhältnis zum Interesse an der Erforschung des Sachverhalts steht. Eine entsprechende Regelung ist bereits in der Strafprozessordnung für den „Großen Lauschangriff“ enthalten.

Der bayerische Gesetzgeber hat zum 01.08.2008 die Ermächtigung zur Online-Durchsuchung für die Polizei und - trotz meiner Bedenken - für das Landesamt für Verfassungsschutz (vgl. dazu Nr. 5.1.4) geschaffen. Zur Vorbereitung dieser Maßnahme sollen Polizei und Verfassungsschutz heimlich in Wohnungen eindringen und diese auch durchsuchen dürfen (vgl. dazu Nrn. 4.1.3 und 5.1.5).

### 4.1.3 Heimliche Wohnungsdurchsuchung

Die Gesetzesänderung enthält darüber hinaus - bundesweit erstmalig - die Befugnis für die Polizei, zur Durchführung einer Wohnraumüberwachung, einer Telekommunikationsüberwachung oder einer Online-Durchsuchung die Wohnung des Betroffenen heimlich zu betreten und zu durchsuchen.

Dies wirft erhebliche verfassungsrechtliche Bedenken auf. Art. 13 des Grundgesetzes garantiert die Unverletzlichkeit der Wohnung als räumliche Sphäre der Privatheit und als Mittelpunkt der menschlichen Existenz. In dieses Grundrecht kann zwar unter bestimmten Voraussetzungen eingegriffen werden; allerdings ist dem Wortlaut und der Systematik des Grundgesetzes zu entnehmen, dass nur offene Wohnungsdurchsuchungen auf Art. 13 GG gestützt werden können.

Meiner Forderung, auf die Befugnis zur heimlichen Wohnungsdurchsuchung zu verzichten, wurde leider nicht entsprochen.

### 4.1.4 Benachrichtigungspflicht bei der „Polizeilichen Beobachtung“

Leider wurde die Änderung des Polizeiaufgabengesetzes nicht auch dazu benutzt, Art. 36 PAG (Polizeiliche Beobachtung) verfassungskonform dahin gehend zu ergänzen, dass der Betroffene nach Abschluss der polizeilichen Beobachtung grundsätzlich zu benachrichtigen ist.

Das Bundesverfassungsgericht hat wiederholt die Bedeutung der Benachrichtigungspflicht bei heimlichen Eingriffsmaßnahmen hervorgehoben. So hat es z.B. in seiner Entscheidung zum Großen Lauschangriff vom 03.03.2004 Folgendes dazu ausgeführt:

„Bei nicht erkennbaren Eingriffen steht dem Grundsrechtsträger 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.“

Seit 01.01.2008 besteht bei der polizeilichen Beobachtung zum Zwecke der Strafverfolgung grundsätzlich die Pflicht zur Benachrichtigung der Zielperson und der Person, deren personenbezogene Daten erfasst worden sind. Der Gesetzesbegründung zufolge „erscheint“ eine Benachrichtigungspflicht „in Anbetracht der mit der Maßnahme im Einzelfall verbundenen Überwachungsintensität (Erstellung von Bewegungsprofilen) geboten“.

Ich habe das Staatsministerium des Innern bereits im Dezember 2006 auf die Notwendigkeit hingewiesen, die Benachrichtigung der Betroffenen grundsätzlich auch bei der polizeilichen Beobachtung zur Gefahrenabwehr vorzusehen. Da die Pflicht zur Benachrichtigung sich unmittelbar aus dem Grundgesetz ergibt, muss sie - trotz der derzeitigen fehlenden gesetzlichen Verpflichtung - bereits jetzt erfüllt werden. Ich halte es daher für notwendig, dass das Staatsministerium des Innern z.B. durch den Erlass entsprechender Verwaltungsvorschriften die verfassungsrechtlich gebotene Benachrichtigung sicherstellt. Das Staatsministerium des Innern hat mir mitgeteilt, dass die Regelung einer Benachrichtigungspflicht der Betroffenen geprüft werde.

### 4.1.5 Präventive Rasterfahndung

In meinem letzten Tätigkeitsbericht (vgl. Nr. 4.8) habe ich über den Beschluss des Bundesverfassungsgerichts zur präventiven Rasterfahndung vom 04.04.2006 berichtet und die wichtigsten Punkte aufgeführt, in denen die Befugnis zur präventiven Rasterfahndung (vgl. Art. 44 PAG) an die Vorgaben des Bundesverfassungsgerichts angepasst werden muss. Dies ist, nachdem ich das Staatsministerium des Innern auf die Notwendigkeit der Anpassung und die erforderlichen inhaltlichen Änderungen hingewiesen habe, mit dem In-Kraft-Treten der Gesetzesänderung am 01.08.2008 nach mehr als zwei Jahren geschehen.

Dabei wurde die Regelung der Rasterfahndung im Wesentlichen in folgenden Punkten geändert:

- Voraussetzung für den Einsatz der Maßnahme ist nunmehr das Vorliegen einer „konkreten“ Gefahr für hochrangige Rechtsgüter, wie den Bestand oder die Sicherheit des Bundes oder eines Landes oder für Leib, Leben oder Freiheit einer Person.

- Die Maßnahme darf nur durch den Richter angeordnet werden. Dabei muss die richterliche Anordnung den zur Datenübermittlung Verpflichteten bezeichnen.

- Präzise Bestimmung des Verwendungszwecks der durch die Maßnahme erlangten Daten und Einführung einer Kennzeichnungspflicht.

- Ausweitung der Pflicht zur Benachrichtigung von Personen, gegen die nach Abschluss der Rasterfahndung weitere Maßnahmen durchgeführt werden. Die Betroffenen müssen informiert werden, sobald dies ohne Gefährdung des Zwecks der Maßnahme, der eingesetzten nicht offen ermittelnden Beamten oder hochrangiger Rechtsgüter geschehen kann.

Mehr Klarheit hätte ich mir aber bei der Festlegung des Zeitpunkts der Löschung der Daten gewünscht. Der Neuregelung zufolge sollen die im Rahmen der Rasterfahndung übermittelten und im Zusammenhang mit der Maßnahme zusätzlich angefallenen Daten erst dann gelöscht werden, wenn der Zweck der Rasterfahndung erreicht ist oder sich zeigt, dass er nicht erreicht werden kann (vgl. Art. 44 Abs. 6 Satz 1 PAG n.F.). Es wird jedoch nicht deutlich, wann von einer „Zweckerreichung“ auszugehen ist. Auch bei den Rasterfahndungen im Jahr 2001 nach sog. Schläfern war nicht klar, ob Zweck der Maßnahme i.S.d. Art. 44 PAG der Erhalt der Rasterungsergebnisse, deren Auswertung oder die Ermittlung der sog. Schläfer war (vgl. dazu meine Ausführungen im 21. Tätigkeitsbericht unter Nr. 7.7 und im 20. Tätigkeitsbericht unter Nr. 6.11). Ich hatte deshalb eine Pflicht zur Löschung der übermittelten und im Zusammenhang mit der Rasterfahndung zusätzlich angefallenen Daten gefordert, sobald der Abgleich abgeschlossen ist und die Daten nicht für weitere polizeiliche Maßnahmen benötigt werden.

### 4.2 Bayerisches Versammlungsgesetz (BayVersG)

Das Versammlungsrecht war bisher durch das Versammlungsgesetz des Bundes geregelt. Durch die Föderalismusreform I ist die Gesetzgebungskompetenz für das Versammlungsrecht vom Bund auf die Länder übergegangen. Bayern hat mit dem Erlass eines Bayerischen Versammlungsgesetzes (BayVersG) von dieser Gesetzgebungskompetenz Gebrauch gemacht. Das BayVersG ist am 01.10.2008 in Kraft getreten.

Das BayVersG enthält insbesondere folgende datenschutzrechtlich relevanten Regelungen:

- Die Polizei erhält eine allgemeine Befugnis, unter bestimmten Voraussetzungen personenbezogene Daten von Versammlungsteilnehmern zu erheben (vgl. Nr. 4.2.1).

- Sog. Übersichtsaufnahmen und -aufzeichnungen, deren Speicherung und Nutzung durch die Polizei, sind - im Gegensatz zum Versammlungsgesetz des Bundes - grundsätzlich zugelassen (vgl. dazu Nr. 4.2.3 und 4.2.4).

- Der Veranstalter der Versammlung hat der zuständigen Behörde auf Anforderung bestimmte persönliche Daten des Leiters und der Ordner (z.B. Namen, Geburtsnamen, Geburtsdatum und Geburtsort) mitzuteilen.

Zu den Gesetzentwürfen hatte ich gegenüber dem Staatsministerium des Innern ausführlich Stellung genommen. Leider wurde eine Reihe meiner Änderungsvorschläge nicht berücksichtigt. Die wichtigsten datenschutzrechtlichen Problempunkte habe ich im Folgenden zusammengefasst.

#### 4.2.1 Allgemeine Befugnis zur Datenerhebung

Die Polizei darf bei oder im Zusammenhang mit Versammlungen personenbezogene Daten von Teilnehmern erheben, wenn tatsächliche Anhaltspunkte die Annahme rechtfertigen, dass von ihnen erhebliche Gefahren für die öffentliche Sicherheit oder Ordnung ausgehen (Art. 9 Abs. 1 Satz 1 BayVersG). Diese personenbezogenen Daten müssen grundsätzlich offen erhoben werden (Art. 9 Abs. 3 BayVersG i.V.m. Art. 30 Abs. 3 PAG).

Die allgemeine Befugnis, personenbezogene Daten zu erheben, begegnet im Hinblick auf den Grundsatz der Normenbestimmtheit und Normenklarheit datenschutzrechtlichen Bedenken. Das Bundesverfassungsgericht führt in seinem Beschluss vom 04.04.2006 zur präventiven Rasterfahndung aus, dass Ermächtigungen zu Grundrechtseingriffen einer gesetzlichen Grundlage bedürfen, die dem rechtsstaatlichen Gebot der Normenbestimmtheit und Normenklarheit entspricht. Zwar ist der Begriff der „personenbezogenen Daten“ in Art. 4 Abs. 1 BayDSG definiert als „Einzelangaben über persönliche oder sachliche Verhältnisse bestimmter oder bestimmbarer natürlicher Personen“. Die Art der möglichen Datenerhebungsmaßnahmen (z.B. offene oder verdeckte Maßnahmen) und deren Umfang (z.B. Erhebung auch der Religionszugehörigkeit) bleiben aber offen.

#### 4.2.2 Bild- und Tonaufnahmen oder -aufzeichnungen von Versammlungsteilnehmern

Die Anfertigung von Bild- und Tonaufnahmen oder -aufzeichnungen von Versammlungsteilnehmern ist nicht nur ein Eingriff in das Grundrecht auf informationelle Selbstbestimmung (Art. 1 Abs. 1 und Art. 2 Abs. 1 GG) der Betroffenen, sondern auch in das für eine Demokratie wesentliche Grundrecht der Versammlungsfreiheit (Art. 8 Abs. 1 GG).

Aus diesem Grund gestattet Art. 9 Abs. 1 Satz 1 BayVersG der Polizei - wie bisher das Versammlungsgesetz des Bundes - personenbezogene Bild- und Tonaufnahmen oder -aufzeichnungen von Versammlungsteilnehmern nur unter engen Voraussetzungen anzufertigen: Es müssen tatsächliche Anhaltspunkte die Annahme rechtfertigen, dass von den betroffenen Teilnehmern erhebliche Gefahren für die öffentliche Sicherheit oder Ordnung ausgehen. Datenschutzrechtliche Bedenken gegen diese Befugnis habe ich nicht, wenn im Einzelfall ihre Voraussetzungen beachtet werden.

Auf meine Forderung hin wurde in der Gesetzesbegründung klargestellt, dass die Anfertigung solcher Bild- und Tonaufnahmen oder -aufzeichnungen nur von solchen Personen zulässig ist, bei denen tatsächliche Anhaltspunkte dafür bestehen, dass gerade von ihnen erhebliche Gefahren für die öffentliche Sicherheit und Ordnung ausgehen.

#### 4.2.3 Übersichtsaufnahmen

Art. 9 Abs. 2 Satz 1 BayVersG gestattet der Polizei, Übersichtsaufnahmen von der Versammlung und ihrem Umfeld zur Lenkung und Leitung des Polizeieinsatzes anzufertigen. Die Erfahrungen aus der datenschutzrechtlichen Prüfungspraxis zeigen, dass bei Versammlungen lange Bildsequenzen von der Polizei aufgenommen werden, ohne dass zwischen Übersichtsaufnahmen und personenbezogenen Aufnahmen unterschieden wird (vgl. dazu 21. Tätigkeitsbericht 2004 unter Nr. 7.14). Häufig sind auch bei sog. Übersichtsaufnahmen die Betroffenen zum Teil individuell erkennbar. Im Übrigen ist es technisch grund-

sätzlich möglich, nicht personenbezogen erfasste Personen nachträglich zu individualisieren.

Versammlungsteilnehmer können grundsätzlich nicht erkennen, ob eine Videokamera außer Betrieb ist, mit ihr Übersichtsaufnahmen oder Übersichtsaufzeichnungen oder personenbezogene Aufnahmen/Aufzeichnungen angefertigt werden. Das Bundesverfassungsgericht befürchtet daher im sog. Volkszählungsurteil, dass potentielle Versammlungsteilnehmer auf eine Teilnahme an der Versammlung gerade deshalb verzichten, weil sie nicht abschätzen können, ob personenbezogene Informationen dauerhaft gespeichert werden und ihnen daraus Risiken entstehen können.

Um diesen Gefahren zu begegnen, habe ich gefordert, Übersichtsaufnahmen nur zuzulassen, soweit sie zur Lenkung und Leitung des Polizeieinsatzes „unbedingt erforderlich“ sind. Darüber hinaus habe ich - aus Gründen der verfassungsrechtlich gebotenen Bestimmtheit der Befugnis - gefordert, den Begriff „Übersichtsaufnahme“ im Gesetz dahin gehend zu definieren, dass „Übersichtaufnahmen“ nur solche Aufnahmen sind, die keinen Personenbezug erkennen lassen. Beide Vorschläge haben - ohne erkennbaren Grund - keinen Eingang in das Gesetz gefunden.

#### 4.2.4 Übersichtsaufzeichnungen

Sofern es zur Auswertung des polizeitaktischen Vorgehens erforderlich ist, darf die Polizei auch Übersichtsaufzeichnungen anfertigen. Diese dürfen auch zu Zwecken der polizeilichen Aus- und Fortbildung verwendet und dazu zeitlich unbegrenzt gespeichert werden (vgl. Art. 9 Abs. 2 BayVersG).

Übersichtsaufzeichnungen verlängern den durch Übersichtsaufnahmen erfolgten Grundrechtseingriff. Ich hätte es deshalb begrüßt, wenn auf Übersichtsaufzeichnungen vollständig verzichtet worden wäre.

Der mir vom Staatsministerium des Innern übersandte Gesetzentwurf hatte ursprünglich die unbefristete Speicherung von Übersichtsaufzeichnungen auch für den Fall vorgesehen, dass diese zur Auswertung des polizeitaktischen Vorgehens verwendet werden. Neben dem Verzicht auf Übersichtsaufzeichnungen habe ich hilfsweise gefordert, wenigstens kurze Löschungsfristen vorzusehen. Diese Forderung wurde im Gesetzgebungsverfahren insoweit berücksichtigt, als Übersichtsaufzeichnungen, soweit sie zur Auswertung des polizeitaktischen Vorgehens verwendet werden, spätestens nach einem Jahr seit ihrer Entstehung zu löschen sind.

Nicht berücksichtigt wurde meine Forderung, Übersichtsaufzeichnungen, die zu Zwecken der polizeilichen Aus- und Fortbildung verwendet werden, ebenfalls nach einer kurzen Frist zu löschen. Allerdings wurde im Gesetz die Möglichkeit der Polizei, auf solchen Aufzeichnungen abgebildete Personen nachträglich - z.B. durch Heranzoomen - zu individualisieren, in zeitlicher Hinsicht eingeschränkt. So ist die Identifizierung einer abgebildeten Person nach Ablauf von einem Jahr seit Entstehen der Aufzeichnungen nicht mehr zulässig.

### 4.3 Kriminalaktennachweis (KAN)

Speicherungen personenbezogener Daten im Kriminalaktennachweis der bayerischen Polizei (KAN) sind ein Schwerpunkt bei Bürgereingaben. Neben der anlassbezogenen Prüfung solcher Eingaben habe ich auch polizeiliche Speicherungen ohne konkreten Anlass im KAN geprüft. Dabei habe ich dieses Mal ein besonderes Augenmerk auf die Speicherung von Daten Jugendlicher und Kinder sowie die Einstufung von Anlasstaten als sog. Fälle geringerer Bedeutung gelegt. Für Kinder und Jugendliche sind nach dem Polizeiaufgabengesetz verkürzte Regelspeicherfristen vorgesehen. Nachdem in Fällen geringerer Bedeutung eine weitere Verkürzung der Speicherfristen geboten ist, habe ich bei der Neufassung der Richtlinien für die Führung polizeilicher personenbezogener Sammlungen (PpS-Richtlinien) auf die Aufnahme eines entsprechenden Hinweises gedrängt. Zudem sollen Fälle geringerer Bedeutung - soweit nicht weitere polizeiliche Erkenntnisse vorliegen - nur in der polizeilichen Vorgangsverwaltung (PSV) nachgewiesen werden. Unter diesen Gesichtspunkten habe ich bei einer Polizeidirektion Fälle geringerer Bedeutung, bei denen Kinder oder Jugendliche als Tatverdächtige gespeichert waren, geprüft.

Dabei habe ich nur in vier von 25 überprüften Fällen die festgelegte Speicherungsfrist für vertretbar gehalten. Bei 19 Speicherungen habe ich die Polizei zur Fristverkürzung aufgefordert, weil ich von Fällen geringerer Bedeutung ausgegangen bin. Die nachfolgenden Beispiele zeigen, dass hier bereits die Erfassung im KAN nicht erforderlich war:

Eine 13 Jahre alte österreichische Schülerin war zusammen mit ihrer Freundin bei einer Kontrolle im Bus nur mit einem Sonderfahrausweis festgestellt worden, welcher für die betreffende Fahrstrecke keine Gültigkeit besaß. Die Betroffene gab an, mit dem Ticket von Österreich nach Deutschland zu einer Haltestelle gefahren zu sein, wofür der Fahrschein galt. Sie habe gedacht, man könne das Ticket anschließend auch für die in der betreffenden Stadt eingesetzten Busse benutzen. Folglich eines polizeilichen Vermerks soll auf einen Strafantrag verzichtet worden sein, weil es sich um eine Ersttat gehandelt und das Fahrgeld nur 80 Cent betragen habe. Von der Einleitung eines Ermittlungsverfahrens wurde von der Staatsanwaltschaft nach § 152 Abs. 2 StPO abgesehen. Unter Berücksichtigung der Gesamtumstände, nicht zuletzt auch wegen des Alters des Kindes bin

ich von einem Fall geringerer Bedeutung ausgegangen.

In einem anderen Fall hatte ein Vater Anzeige bei der Polizei gegen einen 15-jährigen Jungen erstattet, weil dieser seinen zwölfjährigen Sohn im Schulbus so gegen eine Scheibe gestoßen hätte, dass dieser Kopfschmerzen bekommen habe. Im Laufe der Ermittlungen beschuldigte der Junge den Sohn des Anzeigeerstatters der Beleidigung, weil dieser ihm auf seine Aussage, er sei „rechteckig", entgegnet haben soll: „Das sieht man ja an deiner Fresse". Hinweise auf die Vorlage der Anzeige an die Staatsanwaltschaft und auf den Verfahrensausgang waren der Kriminalakte nicht zu entnehmen. Bei einem Privatklagedelikt nach § 185 StGB ist folglich der PpS-Richtlinien regelmäßig von einem Fall geringerer Bedeutung auszugehen. Ein solcher Fall lag hier vor.

Eine 14-Jährige hatte zusammen mit ihren beiden Freundinnen mit einem Edding-Stift einen Schriftzug an eine Kirchenmauer gemalt. Die Kirchenverwaltung hatte keinen Strafantrag gestellt, nachdem sich die Mädchen später freiwillig beim Pfarrer gemeldet und die Schmiererei beseitigt haben. Die Staatsanwaltschaft sah nach § 45 Abs. 2 JGG von der Verfolgung der Straftat ab. Bei einem Privatklagedelikt nach § 303 StGB ist in der Regel dann ein Fall geringerer Bedeutung anzunehmen, wenn die Tat nicht in der Öffentlichkeit begangen wurde und die Staatsanwaltschaft ein öffentliches Interesse nicht bejaht hat. Diese Voraussetzungen waren zwar wegen der Öffentlichkeit der Tat hier nicht vollständig erfüllt. Da die Betroffene aber gerade erst 14 Jahre alt geworden war, kein Strafantrag gestellt war, die Verschmutzung von ihr und ihren Freundinnen wieder behoben wurde und somit der durch die geringfügige Sachbeschädigung entstandene Schaden wieder beseitigt worden war, erschien mir die Annahme eines Falles geringerer Bedeutung angemessen.

Die Polizeidirektion hat alle meine Forderungen in diesen Fällen ausnahmslos erfüllt. Zudem hat mir der Behördenleiter mitgeteilt, dass das Prüfungsergebnis bei einer Besprechung den Dienststellenleitern vorgestellt und diese auf die Regelungen zur Einstufung von Vorgängen als Fälle geringerer Bedeutung hingewiesen wurden.

Im Rahmen der o.g. Prüfung ist mir auch aufgefallen, dass zu einigen Betroffenen Ordnungswidrigkeiten im KAN gespeichert waren. Die Ordnungswidrigkeit eines 15-Jährigen war wegen eines Verstoßes gegen das Bayerische Straßen- und Wegegesetz im KAN nachgewiesen worden. Der Junge war von einer Polizeistreife angetroffen worden, wie er auf einem Weihnachtsmarkt bettelte. Die Sicherheitsbehörde der Stadt verwarnte den Betroffenen wegen des Verstoßes schriftlich ohne Verwarnungsgeld. Ordnungswidrigkeiten sollen nur in bestimmten Ausnahmefällen im KAN gespeichert werden. Die Gründe für die Speicherung - die wegen der geringeren Bedeutung dieser Vorgänge zu verkürzen ist - sind grundsätzlich schriftlich zu dokumentieren. Ein solcher Ausnahmefall lag aber nicht vor, so dass die Speicherung auf mein Betreiben hin im KAN gelöscht wurde.

Ich habe in der Folge noch bei einer weiteren Polizeidienststelle die Speicherung von Ordnungswidrigkeiten im Kriminalaktennachweis auf die Einhaltung dieser Vorgaben hin überprüft. Dabei konnte ich feststellen, dass die datenschutzrechtlichen Anforderungen weitgehend erfüllt waren. Nur in wenigen Ausnahmefällen habe ich die Polizei aufgefordert, den Sachverhalt aus dem Kriminalaktennachweis zu löschen und lediglich in der Vorgangsverwaltung nachzuweisen.

So war ein Betroffener zusammen mit einer weiteren Person gespeichert worden, weil sie an einem Weiher Alkohol getrunken und die leeren Flaschen anschließend in den Weiher geworfen hatten. Vor der Polizei räumten beide ein, jeweils eine Flasche in den Weiher geworfen und damit eine Ordnungswidrigkeit nach dem Kreislaufwirtschafts- und Abfallgesetz begangen zu haben. Zwar können im KAN Ordnungswidrigkeiten mit besonderer sicherheitsrechtlicher Gefahrenneigung sowie solche, deren Speicherung im Einzelfall unter besonderer Berücksichtigung der Person des Betroffenen (Vorerkenntnisse) oder anderer nachvollziehbarer Umstände zur Gefahrenabwehr erforderlich sind, gespeichert werden. Der vorliegende Sachverhalt ließ aber nicht erkennen, wieso hier ein Nachweis der Ordnungswidrigkeiten im KAN erforderlich sein sollte. Die Polizei ist meiner Forderung nach Löschung dieser Speicherungen aus dem KAN nachgekommen.

Ordnungswidrigkeiten werden nach Art. 38 Abs. 1 PAG gespeichert. Sie unterliegen somit nicht der sog. Mitziehautomatik nach Art. 38 Abs. 2 Satz 6 PAG. Diese bewirkt eine Verlängerung der Speicherfrist im Falle der Hinzuspeicherung weiterer Erkenntnisse, für die die Löschungsfrist später endet. Ich habe deshalb das Innenministerium aufgefordert zu gewährleisten, dass die im bayerischen KAN nachgewiesenen Ordnungswidrigkeiten nicht der sog. Mitziehautomatik unterliegen. Meine Forderung wurde in einer der nächsten Programmversionen des elektronischen KAN umgesetzt.

Derzeit findet die Pilotierung für die sog. Elektronische Kriminalakten-Archivierung (EKAA) bei der Bayerischen Polizei statt. Dabei sollen alle bisher in Papierform vorliegenden Kriminal- und Vorgangsakten digitalisiert gespeichert und elektronisch abgerufen werden können. Das Innenministerium hat mir dazu das Berechtigungs- und Zugriffskonzept übermittelt. Wegen des bayernweiten Zugriffs auf Vorgangsverwaltungsdaten durch eine Vielzahl von Bediensteten verschiedenster Funktionen hatte ich bereits früher meine Bedenken gegenüber dem Innen-

ministerium geäußert (vgl. hierzu Nr. 4.2 des 22. Tätigkeitsberichts). Mit EKAA sollen nun Zugriffe der Polizeibeamten auf (digitalisierte) Kriminal- und Vorgangsakten grundsätzlich präsidiumsweit und für bestimmte Benutzer auch landesweit ermöglicht werden. Bisher war eine Sicht auf die Akten mit einem erhöhten Aufwand, nämlich der schriftlichen Anforderung oder einer direkten Einsichtnahme bei der Kriminalaktenstelle oder der den Vorgang führenden Dienststelle verbunden. Mit dem Zugriff auf elektronischem Wege können zukünftig die berechtigten Benutzer beispielsweise auch auf in diesen Akten enthaltene Beschuldigten- und Zeugenvernehmungen oder Gutachten zugreifen. Diese Leichtigkeit des Zugriffs und die fehlende Kontrolle durch die Kriminalaktenstelle erhöht die Gefahr einer unzulässigen Nutzung oder Weitergabe auch sensibler personenbezogener Daten, wie beispielsweise Niederschriften über die Vernehmung von Opfern von Sexualstraftaten oder psychologische Gutachten.

Ich habe deswegen gefordert, dass Benutzer außerhalb der sachbearbeitenden Dienststellen nur zu einer elektronischen Anforderung im Einzelfall oder temporär für die Ermittlungssachbearbeitung berechtigt werden sollen und gebeten, im Rahmen der Pilotierung ein solches Berechtigungskonzept zu prüfen.

Zudem ist es jedem Berechtigten möglich, recherchierte Vorgangs- und Kriminalakten oder Teile davon auszudrucken. Dies birgt wegen der Möglichkeit der Vervielfältigung die Gefahr, dass noch nach Vernichtung der Originalakten ausgedruckte Akten oder Aktenteile erhalten bleiben. Ich habe deshalb gebeten, die Druckfunktion im Rahmen des Berechtigungskonzeptes nur einem eingeschränkten Benutzerkreis zur Verfügung zu stellen und neben dem Lesezugriff auch den Ausdruck zu protokollieren.

Unabhängig davon werde ich mich über die EKAA vor dem flächendeckenden Einsatz bei einer der Pilotdienststellen vor Ort eingehend informieren.

### 4.4 Speicherungen in der Staatsschutzdatei

Immer wieder sind auch Speicherungen in der Staatsschutzdatei der Polizei (ISIS) Gegenstand meiner datenschutzrechtlichen Prüfungen. In meinem 22. Tätigkeitsbericht (vgl. hierzu Nr. 4.5) hatte ich in diesem Zusammenhang auch von meinen datenschutzrechtlichen Bedenken hinsichtlich der Speicherung von Betroffenen wegen des Verdachts der Beleidigung von Organen und Vertretern ausländischer Staaten berichtet, weil sie bei Demonstrationen gegen die Münchner Sicherheitskonferenz 2006 Plakate mit der Aufschrift „Rumsfeld Massenmörder“ trugen. Meiner Aufforderung, die Speicherungen derjenigen Personen in der Datei ISIS zu löschen, über die darüber hinaus keine staatsschutzrelevanten Erkenntnisse vorliegen, ist die Polizei nach kontroverser Auseinandersetzung schließlich nachgekommen.

Datenschutzrechtlich bedenklich waren auch Speicherungen, auf die ich durch die Presse und durch eine schriftliche Anfrage einer Abgeordneten des Landtags aufmerksam gemacht wurde. Anlass dieser Anfrage war eine Veranstaltung eines Kreisverbandes einer Partei, an der auch ein Regierungsmitglied teilnahm. Vor und während der Veranstaltung sollen personenbezogene Daten von Landwirten, Mitgliedern des „Bundes Naturschutz“ und weiteren Bürgern, die sich als Gegner der sog. „Grünen Gentechnik“ zu erkennen gaben, von Polizeibeamten erhoben und gespeichert worden sein. Der von mir zur datenschutzrechtlichen Prüfung der Speicherungen beigezogenen staatsanwaltschaftlichen Ermittlungsakte war im Wesentlichen zu entnehmen, dass die Betroffenen den Besuch der Veranstaltung auch nutzen wollten, um vor dem Veranstaltungsort ihre Meinung zur Gentechnik zum Ausdruck zu bringen. Dazu kamen sie mit Traktoren zum Veranstaltungsort, an denen u.a. Transparente angebracht waren. Auf einem Anhänger war ein überdimensionaler Maiskolben mitgeführt worden. Einer der Beschuldigten sagte aus, dass ihm nicht bewusst gewesen sei, dass die Aktion anmeldepflichtig war. Es habe auch keinen Koordinator der Aktion gegeben, der die Versammlung hätte anmelden können. Auch der polizeiliche Sachbearbeiter kam in seinen Ermittlungsvermerken zum Ergebnis, dass die Betroffenen, bei denen es sich ausschließlich um besorgte Landwirte handelte, keine Erfahrungen im Bereich des Versammlungsrechts hatten. Die zuständige Staatsanwaltschaft führte in ihrer Einstellungsverfügung aus, dass aufgrund der durchgeführten Ermittlungen nicht nachweisbar sei, dass es sich um einen von den Beschuldigten geplante bzw. initiierte Versammlung gehandelt habe. Es sei aber nicht auszuschließen, dass sämtliche Teilnehmer ohne vorherige Absprache zur Kundgabe Ihrer Einstellung gegen Gentechnik am Ort der Informationsveranstaltung erschienen seien.

Wegen dieses Vorgangs waren zunächst personenbezogene Daten von vier Beschuldigten im Kriminalaktennachweis und der Staatsschutzdatei gespeichert. Nach der Einstellung des Ermittlungsverfahrens wurden drei Personen aus diesen Dateien gelöscht. Im Zuge meiner Überprüfung hat die Polizei auch die Daten der vierten Person gelöscht. Die Betroffenen waren aber noch in der Vorgangsverwaltung gespeichert, wobei drei von ihnen weiterhin als „Beschuldigte“ geführt wurden.

Ich hatte auf Grund des Sachverhalts erhebliche Zweifel, dass ein Tatverdacht von ausreichender Substanz, der eine Speicherung der drei Betroffenen als „Beschuldigte“ wegen eines Verstoßes gegen das Versammlungsrecht rechtfertigen könnte, gegeben war. Dies galt insbesondere deshalb, weil völlig offen war, wer ggf. als Versammlungsleiter angesehen

werden sollte. Meiner Aufforderung, die Betroffenen in der Vorgangsverwaltung mit der weniger belastenden Personenart „Betroffene einer polizeilichen Maßnahme“ zu speichern, ist die Polizei nachgekommen. Auch die Speicherung der Person, gegen die als Leiter/Veranstalter einer nicht angemeldeten Versammlung ein Verfahren wegen des Verdachts des Verstoßes gegen das Versammlungsgesetz geführt wurde, in der INPOL-Fall-Datei „Innere Sicherheit“ (IFIS) wurde nach einiger Verzögerung inzwischen gelöscht.

### 4.5 Polizeiliche Speicherungen in der Antiterrordatei

Über das zwischenzeitlich in Kraft getretene Gesetz zur Errichtung einer standardisierten zentralen Antiterrordatei von Polizeibehörden und Nachrichtendiensten von Bund und Länder (Antiterrordateigesetz - ATDG) und den damit zusammenhängenden datenschutzrechtlichen Problemen habe ich bereits in meinem letzten Tätigkeitsbericht (vgl. hierzu Nr. 5.4) berichtet. In diesem Berichtszeitraum habe ich Speicherungen in der Antiterrordatei sowohl bei der Bayerischen Polizei als auch beim Bayerischen Landesamt für Verfassungsschutz (vgl. hierzu Nr. 5.2 - Datenschutzrechtliche Prüfungen beim Verfassungsschutz) überprüft.

Die überprüfte Polizeidienststelle hatte dabei Daten von Personen aus etwa 20 umfangreichen Ermittlungsverfahren in der ATD gespeichert, die aus der Arbeitsdatei „AKIS“, dem Informationssystem zur Aufklärung krimineller islamistischer Strukturen, übernommen worden waren. Im Hinblick auf die Speicherfristen bestimmt § 11 Abs. 3 ATDG, dass personenbezogene Daten in der ATD zu löschen sind, wenn die zugehörigen Erkenntnisse nach den für die beteiligten Behörden jeweils geltenden Rechtsvorschriften zu löschen sind. Grundsätzlich ist deshalb in der ATD die Aussonderungsprüffrist festzusetzen, die für die korrespondierende Erkenntnis in AKIS maßgeblich ist. Nach Ablauf dieser Frist ist die Speicherung zu prüfen und ggf. zu löschen. Ich habe deshalb zu den zu prüfenden Speicherungen um einen AKIS-Auszug jedes Betroffenen sowie um Mitteilung der jeweiligen ATD-Speicherfristen gebeten. Die betreffende Dienststelle hat mir daraufhin mitgeteilt, dass bei der Überprüfung festgestellt worden sei, dass die Speicherfristen bei Kontaktpersonen nicht in allen Fällen korrekt festgesetzt waren. Sie habe dies zum Anlass genommen, die Speicherfristen für alle eingestellten Kontaktpersonen zu überprüfen und ggf. das nach der Errichtungsanordnung für AKIS vorgesehene Aussonderungsprüfdatum festzusetzen.

In Zukunft ist durch geeignete Maßnahmen sicherzustellen, dass bereits bei der Erfassung der Speicherungen die zutreffenden Speicherfristen in der ATD festgesetzt und die Speicherungen fristgerecht überprüft und gelöscht werden. Es darf nicht vorkommen, dass beispielsweise eine in der ATD gespeicherte Kontaktperson zehn Jahre gespeichert bleibt, nur weil eine (nicht ATD-relevante) Erkenntnis über den Betroffenen mit einer zehnjährigen Aussonderungsprüffrist in AKIS gespeichert ist.

In der ATD werden die Betroffenen nach bestimmten im Antiterrordateigesetz festgelegten Personenkategorien gespeichert: Angehörige oder Unterstützer einer terroristischen Vereinigung nach § 129 a/b StGB (§ 2 Nr. 1 ATDG), Gewaltbefürworter (§ 2 Nr. 2 ATDG) oder Kontakt- und Begleitpersonen (§ 2 Nr. 3 ATDG). Bei der Auswahl der zu prüfenden Speicherungen habe ich alle Personenkategorien berücksichtigt. In einigen Fällen habe ich die Polizei aufgefordert, die Personenkategorie, beispielsweise von „Gewaltbefürworter“ in „Kontaktperson“, mit entsprechender Korrektur der Aussonderungsprüffrist zu ändern. Bei einigen Betroffenen, die ausschließlich als Kontaktpersonen gespeichert waren, habe ich die Polizei zur Löschung aufgefordert, weil ich das Vorliegen der Vorraussetzungen für eine Speicherung in der ATD nicht gesehen habe. Als Kontaktpersonen nach § 2 Nr. 3 ATDG sollen Betroffene nämlich nur gespeichert werden, wenn tatsächliche Anhaltspunkte dafür vorliegen, dass sie mit einer in § 2 Nr. 1 oder Nr. 2 genannten Person (vgl. oben) nicht nur flüchtig oder in zufälligem Kontakt in Verbindung stehen, und durch sie weiterführende Hinweise für die Aufklärung oder Bekämpfung des internationalen Terrorismus zu erwarten sind.

So war z.B. eine Person gespeichert, weil sie während der Observation eines verdächtigten Unterstützers einer terroristischen Vereinigung erfolglos versucht habe, diesen zu erreichen, indem sie an dessen Eingangstüre geläutet hatte. Weitere Erkenntnisse zum Betroffenen waren nicht vorhanden. Lediglich das (einmalige) Läuten erschien mir für die Speicherung als Kontaktperson in der ATD zu weitgehend. Das gleiche galt für die Speicherung einer 21-Jährigen, die im Zusammenhang mit einem Ermittlungsverfahren als Inhaberin von zwei Telefonanschlüssen festgestellt worden war, von denen aus männliche Personen in afghanischer Sprache mit einem Informanten gesprochen haben sollen. Die Betroffene war in AKIS als „Tatverdächtige“ und in der ATD als Kontaktperson nachgewiesen. Auch hier habe ich die Löschung aus der ATD und eine Änderung der AKIS-Speicherung gefordert.

### 4.6 Öffentlich zugängliche Sexualstraftäterdatei

Aus der Presse habe ich erfahren, dass auch von bayerischen Sicherheitspolitikern Überlegungen angestellt werden, die personenbezogenen Daten polizeilich bekannter Sexualstraftäter zu veröffentlichen.

Eine solche allgemeine Bekanntgabe z.B. von Namen, Anschriften usw. polizeilich bekannter Sexualstraftäter an die Öffentlichkeit halte ich für unzulässig. Das Grundrecht auf informationelle Selbstbestimmung, das allgemeine Persönlichkeitsrecht aus Art. 2 Abs. 1 GG und das Recht auf Resozialisierung, wie es das Bundesverfassungsgericht in mehreren Entscheidungen ausgeführt hat (siehe BVerfGE 35, 202, 235; 45, 187, 238), lassen solche tiefgehenden Eingriffe mit Prangerwirkung nicht zu. Auch die 73. Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat sich in einer Entschließung gegen dieses Projekt gewandt (siehe Anlage Nr. 3). Die Konferenz betont zwar, dass an Kindern begangene Sexualstraftaten mit allen zur Verfügung stehenden rechtsstaatlichen Mitteln bekämpft werden müssen. Dies schließt jedoch die Anwendung eindeutig rechtsstaatswidriger Mittel aus. Eine solche Datei wäre lediglich dazu geeignet, Misstrauen und Selbstjustiz zu fördern.

### 4.7 Haft-Entlassenen-Auskunfts-Datei-Sexualstraftäter (HEADS)

In meinem letzten Tätigkeitsbericht hatte ich über die Konzeption des Staatsministeriums des Innern für eine „Haft-Entlassenen-Auskunfts-Datei-Sexualstraftäter“ (HEADS) berichtet (vgl. hierzu Nr. 4.6). Mit HEADS wird das Ziel verfolgt, das Risiko einer erneuten Begehung von Straftaten durch besonders rückfallgefährdete Sexualstraftäter zu minimieren und damit die Bevölkerung bestmöglich vor solchen Tätern zu schützen. Zielgruppe des Projekts HEADS sind Personen, die wegen Straftaten gegen die sexuelle Selbstbestimmung (§§ 174 ff. StGB) oder wegen Tötungsdelikten mit sexuellem Hintergrund oder unklarem Motiv verurteilt wurden oder sich wegen einer dieser Straftaten im Vollzug einer stationären Maßregel der Sicherung und Besserung befinden.

Nachdem es sich bei HEADS um die erstmalige zentrale Speicherung von Sexualstraftätern in einer besonderen Datei mit einer Vielzahl informationeller Eingriffsmöglichkeiten handelt, ist die Datei aus datenschutzrechtlicher Sicht von besonderer Bedeutung. In einigen Punkten der Konzeption, insbesondere bei der unmittelbaren Unterrichtung der Staatsanwaltschaft als Vollstreckungsbehörde durch Bewährungshelfer anstelle der Einschaltung des bewährungsaufsichtsführenden Gerichts, konnte ich keine Übereinstimmung mit dem Innen- bzw. dem Justizministerium erzielen. Ich sehe für eine unmittelbare Datenübermittlung vom Bewährungshelfer an die Staatsanwaltschaft keine ausreichende bereichsspezifische Rechtsgrundlage.

Nach der Aufnahme des Wirkbetriebs habe ich die Datei vor Ort bei einem Polizeipräsidium datenschutzrechtlich überprüft. Zunächst habe ich mir die grundsätzliche Verfahrensweise darlegen lassen. Danach wird in der Regel durch die Justizvollzugsanstalten (JVA) den zuständigen Staatsanwaltschaften mitgeteilt, dass ein Sexualstraftäter, der möglicherweise als Risikoproband einzustufen ist, in der nächsten Zeit entlassen wird. Zudem gibt es auch retrograde Erfassungen, d.h. von Personen, die bereits entlassen sind und unter Führungsaufsicht stehen. Die Staatsanwaltschaft entscheidet dann, ob der Betroffene als sog. HEADS-Risikoproband eingestuft werden soll und meldet diesen der HEADS-Zentralstelle der Polizei. Dort wird je nach Art und Schwere der begangenen Tat, der Persönlichkeit des Täters und seinem Verhalten nach der Tat eine Einteilung der Betroffenen in drei Kategorien und die Speicherung ihrer personenbezogenen Daten vorgenommen.

Für meine Prüfung habe ich von jeder Kategorie die Speicherungen von mindestens fünf Risikoprobanden ausgewählt. Ich habe festgestellt, dass nur in wenigen Fällen eine Entscheidung der Staatsanwaltschaft über die Einstufung als HEADS-Risikoproband dokumentiert war. Lediglich die Übermittlung der zur Beurteilung maßgeblichen Unterlagen aus den Strafverfahrensakten (z.B. Gerichtsurteile, Führungsaufsichtsbeschlüsse, Gutachten) an die Zentralstelle war festzustellen. Es war deshalb den Unterlagen nicht zu entnehmen, aufgrund welcher Gesichtspunkte die Staatsanwaltschaft zu dem Ergebnis gekommen war, dass die Personen als HEADS-Risikoprobanden einzustufen und die Daten der Polizei zu übermitteln sind. Ich habe deshalb das Staatsministerium der Justiz und für Verbraucherschutz um Mitteilung gebeten, nach welchen Kriterien bei der Staatsanwaltschaft eine Einstufung der Betroffenen als HEADS-Proband erfolgt und ob und ggf. auf welche Weise diese Entscheidung und deren Begründung dokumentiert werden.

Bei den überprüften Fällen hatte ich mit wenigen Ausnahmen keine datenschutzrechtlichen Bedenken gegen die Speicherung in HEADS. Bezüglich eines Betroffenen habe ich die Polizei gebeten, eine Löschung der Speicherung zu prüfen:

Der Betroffene wurde in HEADS als sog. Bewährungsfall eingestuft. Er war wegen sexuellen Missbrauchs von Kindern in Tateinheit mit sexuellem Missbrauch von Schutzbefohlenen zu einer Freiheitsstrafe von drei Jahren verurteilt worden. Mit Beschluss der Strafvollstreckungskammer des zuständigen Landgerichts wurde die Vollstreckung eines Restes der Gesamtfreiheitsstrafe für fünf Jahre zur Bewährung ausgesetzt, aber keine Führungsaufsicht angeordnet. Etwa eineinhalb Jahre nach der Entlassung informierte die Staatsanwaltschaft die HEADS-Zentralstelle über einen Vorfall, bei dem sich der Betroffene einem 17-Jährigen in sexueller Absicht genähert habe. Dies wurde von der Staatsanwaltschaft als Bewährungsversagen bewertet und der Betroffene als Risikoproband eingestuft.

Nachdem das Verfahren im Zusammenhang mit der Annäherung an den 17-Jährigen eingestellt worden war, weil durch die Annäherung kein Straftatbestand erfüllt war, gegen den Betroffenen keine Führungsaufsicht bestand, er sich einer sozialtherapeutischen Behandlung unterzogen und stets beanstandungsfrei verhalten hatte, habe ich dem Polizeipräsidium mitgeteilt, dass ich die Speicherung des Betroffenen in HEADS für problematisch halte. Das Staatsministerium habe ich, unabhängig von dem konkreten Einzelfall, gebeten, die Errichtungsanordnung für HEADS dahin gehend zu ändern, dass nach Ablauf der Führungsaufsicht in jedem Fall eine Prüfung der Erforderlichkeit der weiteren Speicherung in HEADS zu erfolgen hat.

### 4.8 Speicherungen in sonstigen Dateien

Gegenstand meiner Prüfungen bei verschiedenen Polizeidienststellen waren neben Speicherungen im Kriminalaktennachweis auch Speicherungen in deliktsspezifischen Dateien. Im Folgenden sind die wichtigsten Ergebnisse dieser Prüfungen zusammengefasst:

In meinem 21. Tätigkeitsbericht hatte ich meine Bedenken gegen die Speicherung aufgrund „polizeilichen Tatverdachts“ dargelegt (vgl. hierzu Nr. 7.6). Ich habe deshalb im zurückliegenden Berichtszeitraum insbesondere solche „Tatverdächtige“, die zum Tatzeitpunkt noch nicht volljährig waren, zu einem Schwerpunkt meiner datenschutzrechtlichen Prüfungen gemacht und dazu Arbeitsdateien der Bayerischen Polizei wie das „Rauschgift-Informationssystem“ (RGIS) und das „OK-Informationssystem“ (OKIS) herangezogen. Kinder und Jugendliche sind dort nur in einem geringen Umfang als „Tatverdächtige“ gespeichert. Bei einer Polizeidienststelle habe ich in zwei Fällen die Löschung der Speicherungen gefordert. So war ein 13-Jähriger als Tatverdächtiger länger als für die Regelspeicherfrist von 2 Jahren gespeichert. In einem anderen Fall war ein 8-jähriges Kind in OKIS als Tatverdächtiger gespeichert, weil es in einem Anwesen festgestellt wurde, in dem sich nach polizeilicher Annahme Personen - u.a. auch Prostituierte - aufhalten, die planmäßig aus Bulgarien eingeschleust wurden. In welchem Zusammenhang der Junge damit stand, ließ sich den Unterlagen nicht entnehmen. Auf meine Aufforderung hin wurden die beiden Speicherungen gelöscht.

Bei einem anderen Präsidium habe ich die Datei „Jugendliche Intensivtäter“ überprüft. Nach der Errichtungsanordnung sollen in dieser Datei Personen unter 21 Jahren gespeichert werden, die innerhalb eines nachvollziehbaren zeitlichen Zusammenhanges Delikte mit einer besonderen Schwere und/oder einer besonderen Häufigkeit begehen. Ihre Täterpersönlichkeit soll erkennen lassen, dass die Straffälligkeit nicht nur eine episodenhafte Lebensphase ist, sondern zum festen Bestandteil der Persönlichkeitsstruktur zu werden droht.

Nach Angabe des geprüften Polizeipräsidiums waren insgesamt 197 Jugendliche in der Datei erfasst. Bei den meisten der Betroffenen waren die Voraussetzungen für die Speicherung in der Datei gegeben. Zu ihrer Person waren regelmäßig eine Vielzahl von Delikten im KAN nachgewiesen, die auch hinsichtlich ihrer Schwere eine Einstufung als „Jugendliche Intensivtäter“ nachvollziehbar erschienen ließen.

### 4.9 Automatisierte Kennzeichenerkennung

Das Bundesverfassungsgericht hat sich in seinem Urteil vom 11.03.2008 grundlegend zur polizeilichen Maßnahme der „automatisierten Kennzeichenerfassung“ geäußert. Die bayerische gesetzliche Regelung zur automatisierten Kennzeichenerkennung war zwar nicht unmittelbar Gegenstand der verfassungsgerichtlichen Entscheidung. Diese hat aber auch für die bayerische Regelung und deren Vollzug erhebliche Bedeutung (vgl. hierzu Nr. 4.1.1).

Das Gericht stellt in der Entscheidung zunächst klar, dass die automatisierte Kennzeichenerfassung in das Grundrecht auf informationelle Selbstbestimmung dann nicht eingreift, wenn der Abgleich mit dem Fahndungsbestand unverzüglich vorgenommen wird und negativ ausfällt (sog. Nichttrefferfall) sowie rechtlich und technisch gesichert ist, dass die Daten anonym bleiben und sofort spurenlos gelöscht werden. Demgegenüber werde in das Grundrecht eingegriffen, wenn ein erfasstes Kennzeichen im Speicher festgehalten wird und - wie im sog. Trefferfall - ggf. Grundlage weiterer Maßnahmen werden kann. Das Gericht hebt in seiner Entscheidung den besonderen Eingriffscharakter der automatisierten Kennzeichenerfassung hervor: Die Möglichkeit einer seriellen Erfassung einer Vielzahl von Kennzeichen in kürzester Zeit verleihe der Maßnahme ein besonderes Gepräge. Soll die automatisierte Kennzeichenerfassung dazu dienen, die gewonnenen Informationen für weitere Zwecke zu nutzen (z.B. Zusammenstellung der Informationen über mehrere Einzelfahrten zu einem Bewegungsprofil), besitze diese Maßnahme eine „besondere Schlagkraft und Eingriffsintensität“.

Zum Schutz des Grundrechts auf informationelle Selbstbestimmung hat das Gericht insbesondere folgende Anforderungen an eine gesetzliche Eingriffsermächtigung gestellt:

- Die gesetzliche Regelung muss eine Umgrenzung des Anlasses der Maßnahme und auch des möglichen Verwendungszwecks der betroffenen Informationen sicherstellen (sog. Gebot der Normenbestimmtheit und Normenklarheit). Verdachtslose Massendatenabglei-

che sind als Grundrechtseingriffe „ins Blaue hinein“ verfassungsrechtlich unzulässig.

- Eine gesetzliche Regelung, die die Kennzeichenerfassung generell „zum Zwecke“ des Abgleichs mit dem „Fahndungsbestand“ gestattet, ist nicht hinreichend bereichsspezifisch und normenklar, weil sie weder den Anlass- noch den Ermittlungszweck benennt. Darüber hinaus ist der Begriff „Fahndungsbestand“ zu unbestimmt. Der Umfang der einbezogenen Datenbestände verändert sich laufend und in gegenwärtig nicht vorhersehbarer Weise (vgl. hierzu Nr. 4.1.4 des letzten Tätigkeitsberichts zur Übernahme der in der Datei „Gewalttäter Sport“ gespeicherten Personen in den Fahndungsbestand für die Zeit der Fußballweltmeisterschaft 2006). Die Bezugnahme auf den „Fahndungsbestand“ hat dem Bundesverfassungsgericht zufolge den „Charakter einer dynamischen Verweisung“. Nicht der Gesetzgeber, sondern die Verwaltung bestimmt Inhalt und Umfang des Datenbestandes, mit dem abgeglichen wird.

- Die automatisierte Erfassung von Kraftfahrzeugkennzeichen darf nicht anlasslos erfolgen oder flächendeckend durchgeführt werden.

- Der verfassungsrechtliche Grundsatz der Verhältnismäßigkeit ist nicht gewahrt, wenn die gesetzliche Ermächtigung die automatisierte Erfassung und Auswertung von Kennzeichen ermöglicht, ohne dass konkrete Gefahrenlagen oder allgemein gesteigerte Risiken von Rechtsgutgefährdungen oder -verletzungen einen Anlass zur Errichtung der Kennzeichenerfassung geben. Erforderlich ist dazu eine Begrenzung der Maßnahme auf Situationen, in denen Umstände der konkreten Örtlichkeit oder dokumentierte Lageerkenntnisse über Kriminalitätsschwerpunkte einen Anknüpfungspunkt geben, der auf diese Risiken und zugleich auf eine hinreichende Wahrscheinlichkeit hinweist, dass ihnen mit Hilfe der automatisierten Kennzeichenerfassung begegnet werden kann.

Im Hinblick auf die bayerische Regelung der Maßnahme (vgl. Art. 33 Abs. 2, 38 Abs. 3 PAG a.F.) hatte ich das Staatsministerium des Innern auf die Punkte hingewiesen, die vor dem Hintergrund des Urteils des Bundesverfassungsgerichts in der Gesamtschau verfassungs- und datenschutzrechtlich problematisch sind.

Ich hatte darüber hinaus das Staatsministerium des Innern gebeten, bis zu einer Anpassung der entsprechenden Vorschriften an die Vorgaben des Bundesverfassungsgerichts kurzfristig durch geeignete Vollzugshinweise für die Polizei eine verfassungskonforme Einschränkung der automatisierten Kennzeichenerfassung sicherzustellen. Mit Schreiben vom 11.03.2008, das ich trotz mehrfacher Erinnerung an meine datenschutzrechtlichen Forderungen erst nach über vier Monaten erhalten habe, wurde vom Innenministerium eine Reihe von Einschränkungen verfügt. Dies ist grundsätzlich zu begrüßen. Allerdings entsprachen die Regelungen den Anforderungen des Bundesverfassungsgerichts nicht in vollem Umfang:

- Die Maßnahme war nicht an *„konkrete Gefahrenlagen“* oder *„dokumentierte Lageerkenntnisse über Kriminalitätsschwerpunkte“* gekoppelt.

- Die Eingrenzung auf die Fahndungsbestände von INPOL und SIS war zu unbestimmt.

- Eine Einschränkung auf eine stichprobenartige Durchführung war nicht vorgesehen.

- Eine Verwendung der Daten zur Verfolgung von Ordnungswidrigkeiten wurde nicht ausgeschlossen.

Ich habe deshalb das Innenministerium gebeten, meine datenschutzrechtliche Beurteilung bei der evtl. weiteren Datenverarbeitung und -nutzung zu berücksichtigen. Bei einer früheren Unterrichtung durch das Innenministerium hätten die Vollzugshinweise allerdings rechtzeitig ergänzt werden können. Das Innenministerium sollte in Zukunft besser auf eine ausreichende Unterstützung des Landesbeauftragten für den Datenschutz achten.

In der Praxis habe ich insbesondere den Abgleich mit „anderen polizeilichen Dateien“ (Art. 33 Abs. 2 Satz 3 PAG) überprüft. Von dieser Möglichkeit wurde im Berichtszeitraum nach Mitteilung des Innenministeriums nur einmal Gebrauch gemacht. Dabei wurden im Rahmen einer Veranstaltung einer Gruppierung, die nach Darstellung der Polizei dem Bereich der Organisierten Kriminalität zuzurechnen ist, an drei Tagen Kennzeichen der Fahrzeuge der anreisenden Teilnehmer mit drei deliktsspezifischen polizeilichen Dateien abgeglichen. Sowohl die Notwendigkeit des Kennzeichenabgleichs als auch die Erforderlichkeit des Abgleichs mit den konkreten Dateien wurden von der Polizei nachvollziehbar begründet.

In meinem letzten Tätigkeitsbericht (vgl. hierzu Nr. 4.14) hatte ich von der temporären Übernahme (Zeitraum der Fußballweltmeisterschaft 2006) der Kennzeichen von Fahrzeugen der Personen in die Fahndungsdatei, die in der Datei „Gewalttäter Sport“ gespeichert waren, berichtet. Ich habe mich davon überzeugt, dass die eingestellten Kennzeichen wieder aus der Fahndungsdatei gelöscht wurden. Bei einem Betroffenen des Kennzeichenabgleichs habe ich festgestellt, dass Informationen über seine Kontrolle an die für die Ausschreibung in der Gewalttäterdatei

verantwortliche Polizeidienststelle übermittelt worden waren. Inhalt der Mitteilung war, dass sich der Betroffene auf dem Rückweg von einem Badesee befunden und alleine im Fahrzeug gesessen habe. Zweck der Datenübermittlung war nach Mitteilung der Polizei die „Pflege des Eintrags“ in der Gewalttäterdatei sowie eine mögliche Überprüfung durch die speichernde Stelle hinsichtlich der weiteren Notwendigkeit der Speicherung bzw. einer Verkürzung der Speicherungsdauer. Die Datenübermittlung nach einer polizeilichen Kontrolle ohne einen Bezug zu Sportveranstaltungen ist aber nicht zulässig, da sie für den Zweck der Datei, die Verhinderung gewalttätiger Auseinandersetzungen und sonstiger Straftaten im Zusammenhang mit Sportveranstaltungen, nicht erforderlich ist. Solche Datenübermittlungen bergen aber die Gefahr, dass Bewegungsprofile der Betroffenen erstellt werden, ohne dass die gesetzlichen Voraussetzungen dafür vorliegen. Ich habe deshalb die Polizei aufgefordert, zukünftig von Datenübermittlungen bei solchen „Trefferfällen“ abzusehen. Das Innenministerium hat mir daraufhin mitgeteilt, dass die Polizeipräsidien entsprechend angewiesen wurden.

## 4.10 Präventive Telekommunikationsüberwachung

Die Regelungen des Polizeiaufgabengesetzes zur präventiven Telekommunikationsüberwachung (vgl. Art. 34 a bis c PAG) ermächtigen die Polizei zu tiefgehenden Eingriffen in das Fernmeldegeheimnis. So bestehen nicht nur Befugnisse zur Überwachung und Aufzeichnung des Telekommunikationsinhalts, sondern z.B. auch zur Verpflichtung von Diensteanbietern, der Polizei die im Wege der „Vorratsdatenspeicherung“ (vgl. dazu Nr. 6.1.3) gespeicherten sog. Telekommunikationsverkehrsdaten (z.B. Standort, Beginn und Ende der Verbindung, anrufende und angerufene Rufnummer) zu übermitteln und zur Ermittlung des Standorts eines Mobilfunkgeräts. Diese Maßnahmen dürfen grundsätzlich nur durch den Richter angeordnet werden. Bei Gefahr im Verzug dürfen die Maßnahmen auch von der Polizei angeordnet werden; in diesem Fall ist nach dem Gesetz unverzüglich eine Bestätigung der Maßnahme durch den Richter einzuholen. Von der Telekommunikationsüberwachung sind die Beteiligten nachträglich grundsätzlich zu benachrichtigen.

Das Bundesverfassungsgericht hat in seiner Eilentscheidung zur „Vorratsdatenspeicherung“ vom 28.10.2008 ausgeführt, dass die Polizei durch die Verpflichtung des Dienstanbieters, Telekommunikationsverkehrsdaten zu übermitteln, neben der eigentlichen Zielperson möglicherweise auch Personen erfassen könnte, die in keiner Beziehung zu den den Datenabruf rechtfertigenden Gründen stehen und auch sonst keinen Anlass für den damit verbundenen Grundrechtseingriff gegeben hätten. Das Gericht erachtet für die Zeit bis zur Entscheidung über die Verfassungsbeschwerde eine Übermittlung dieser Daten durch den Anbieter an die Polizei nur dann für zulässig, wenn sie - zusätzlich zu den gesetzlichen Voraussetzungen - zur Abwehr einer dringenden Gefahr für Leib, Leben oder Freiheit einer Person, für den Bestand oder die Sicherheit des Bundes oder eines Landes oder zur Abwehr einer gemeinen Gefahr erforderlich ist. Ich werde prüfen, ob diese Vorgaben des Gerichts in der polizeilichen Praxis beachtet werden.

Wie in meinem letzten Tätigkeitsbericht (vgl. Nr. 4.13.3) angekündigt, habe ich die Entwicklung auf dem Gebiet der präventiven Telekommunikationsüberwachung weiter beobachtet. Ich habe dazu in vier Fällen Eingriffsmaßnahmen überprüft. Gegenstand meiner datenschutzrechtlichen Kontrolle waren insbesondere das Vorliegen einer richterlichen Anordnung und die Einhaltung des durch den Richter vorgegebenen Rahmens. Dabei habe ich in einem sog. Eilfall (Gefahr im Verzug) festgestellt, dass das zuständige Polizeipräsidium den Provider um Übermittlung der Standortdaten eines Handys ersucht hat, ohne dies - wie gesetzlich vorgesehen - schriftlich anzuordnen und die Bestätigung eines Richters einzuholen. Ich habe diesen Verstoß förmlich beanstandet. In den übrigen Fällen habe ich keine wesentlichen datenschutzrechtlichen Defizite festgestellt.

## 4.11 DNA-Maßnahmen zur vorbeugenden Verbrechensbekämpfung

### 4.11.1 DNA-Maßnahmen wegen mehrerer nicht-erheblicher Straftaten

Seit dem 01.11.2005 besteht die Möglichkeit, DNA-Maßnahmen bei Beschuldigten nicht nur bei Straftaten von erheblicher Bedeutung oder Sexualstraftaten durchzuführen, sondern auch bei der wiederholten Begehung sonstiger Straftaten, wenn diese im Unrechtsgehalt einer Straftat von erheblicher Bedeutung gleichstehen (§ 81 g Abs. 1 Satz 2 Strafprozessordnung - StPO). Gleiches gilt u.a. auch für verurteilte Straftäter, deren Eintragungen im Bundeszentralregister noch nicht gelöscht sind. Bei einem Polizeipräsidium habe ich die Durchführung solcher sog. retrograder DNA-Maßnahmen überprüft.

Bei DNA-Maßnahmen, die wegen der wiederholten Begehung nicht-erheblicher Straftaten angeordnet werden, müssen die betreffenden Straftaten einer Straftat von erheblicher Bedeutung gleichkommen, künftige Strafverfahren gegen den Betroffenen wegen einer Straftat von erheblicher Bedeutung zu erwarten und das erhobene DNA-Identifizierungsmuster für die künftige Sachaufklärung grundsätzlich dienlich sein. Soweit das Vorliegen dieser Voraussetzungen nicht vom Gericht geprüft und entschieden wird,

sondern die Maßnahme auf der Grundlage der Einwilligung des Betroffenen durchgeführt wird, ist dies von der Polizei zu prüfen.

Straftaten von erheblicher Bedeutung müssen nach der Rechtsprechung des Bundesverfassungsgerichts mindestens dem Bereich der mittleren Kriminalität zuzurechnen sein, den Rechtsfrieden empfindlich stören und dazu geeignet sein, das Gefühl der Rechtssicherheit der Bevölkerung erheblich zu stören. Eine solche Erheblichkeit kann bei Straftaten geringerer Bedeutung nicht schematisch angenommen werden, wenn ein Ersttäter erneut eine Straftat begeht. Ich habe deshalb das Präsidium darauf hingewiesen, dass bei der Prüfung der Erheblichkeit die vom Bundesverfassungsgericht aufgestellten Grundsätze zu beachten sind und nachvollziehbar zu dokumentieren ist, weshalb die begangenen Straftaten im Unrechtsgehalt einer Straftat von erheblicher Bedeutung gleichkommen.

Die Prognose künftiger Begehung einer Straftat von erheblicher Bedeutung durch den Betroffenen wurde aufgrund der beim Präsidium vorliegenden KAN-Unterlagen getroffen. Soweit für die Prognose auch KAN-Speicherungen als relevant angesehen wurden, bei denen keine Verurteilung erfolgt, sondern die Verfahren eingestellt worden waren, waren den Unterlagen in der überwiegenden Zahl der Fälle die Einstellungsbegründungen nicht zu entnehmen. Nach der Rechtsprechung des Bundesverfassungsgerichts setzt eine tragfähig begründete Entscheidung aber voraus, dass ihr eine zureichende Sachaufklärung, insbesondere durch Beiziehung u.a. der verfügbaren Straf- und Vollstreckungsakten vorausgegangen ist und in den Entscheidungsgründen die bedeutsamen Umstände abgewogen wurden. Diese Anforderungen, die für gerichtlich angeordnete DNA-Maßnahmen aufgestellt wurden, gelten nach meiner Auffassung in gleichem Maße für die Prognoseentscheidung der Polizei. Ich habe das Polizeipräsidium aufgefordert, diesen Anforderungen künftig Rechnung zu tragen.

Die Formblätter für die Prognoseentscheidung waren zum Teil nur formelhaft ausgefüllt. So war beispielsweise zur Art und Ausführung der Tat lediglich angemerkt: „A. entwendete eine Geldbörse“ oder „B. entwendete Waren im Wert von 9 Euro“. Zur Persönlichkeit des Täters waren teilweise nur stichpunktartig pauschale Aussagen getroffen wie „geringe Hemmschwelle“, „hohe kriminelle Energie“. Auch zur Begründung der in Zukunft zu erwartenden Straftat von erheblicher Bedeutung wurde häufig nur allgemein darauf hingewiesen, dass aufgrund der Anzahl der Straftaten eine hohe Wahrscheinlichkeit bestehe, dass der Betroffene wieder einschlägig strafrechtlich in Erscheinung treten werde. Nach der Rechtsprechung des Bundesverfassungsgerichts sind im Rahmen der Gefahrenprognose jedoch u.a. Rückfallgeschwindigkeit, Zeitablauf, Verhalten des Betroffenen in der Bewährungszeit oder nach einem Straferlass, Motivationslage bei der früheren Tatbegehung, Lebensumstände und Persönlichkeit zu berücksichtigen. Dabei ist stets eine auf den Einzelfall bezogene Beurteilung erforderlich. Die bloße Wiedergabe des Gesetzeswortlauts oder eine bloß formelhafte Begründung reicht nicht aus. Ich habe deshalb das Polizeipräsidium aufgefordert, künftig bei der Prognoseentscheidung die vom Bundesverfassungsgericht aufgestellten Grundsätze zu beachten und bei der schriftlichen Prognose nachvollziehbar darzulegen, aus welchen Gründen im konkreten Einzelfall zukünftig die Begehung einer Straftat von erheblicher Bedeutung durch den Betroffenen zu erwarten ist.

Unabhängig von den fehlenden Unterlagen und der häufig unzureichenden Begründungen, die - soweit möglich - nachzubessern sind, habe ich in einigen Fällen erhebliche Zweifel, ob die Voraussetzungen für die Durchführung von DNA-Maßnahmen vorliegen. Hier zwei Beispiele:

Über eine Betroffene waren zwei Eintragungen im BZR nachgewiesen, die für die Maßnahme ausschlaggebend gewesen sein sollen. Bei einem Diebstahl im Jahr 2001 soll sie als angestellte Kassiererin eines Einkaufsmarktes Beihilfe zum Diebstahl geleistet haben, indem sie zuließ, dass zwei ihr bekannte Frauen mit Waren im Wert von 545 DM (ca. 275 €) ihren Kassenbereich passieren konnten, ohne dafür zu bezahlen. Sie wurde zu 150 Tagessätzen zu je 15 Euro verurteilt. Bei einem weiteren Diebstahl im Jahr 2006 wurde sie zu 80 Tagessätzen zu je 20 € verurteilt. Ein Kaufhausdetektiv hatte die Betroffene angezeigt, nachdem sie eine Geldbörse im Warenwert von 25 Euro in ihre Einkaufstasche gesteckt hatte, ohne diese an der Kasse zu bezahlen.

Bei der Beurteilung, ob hier Straftaten vorliegen, die im Unrechtsgehalt einer Straftat von erheblicher Bedeutung gleichstehen, ist Folgendes zu berücksichtigen: Die Betroffene beging die erste Tat bereits im Jahr 2001. Erst fünf Jahre später erfolgte die nächste Tat. Im ersten Fall wurde sie zwar zu einer nicht geringen Strafe von immerhin 150 Tagessätzen verurteilt. Eine Straftat von erheblicher Bedeutung lag aber deshalb noch nicht vor. Trotz der Tatsache, dass sie Wiederholungstäterin war, erfolgte im zweiten Fall nur eine Verurteilung zu einer relativ geringen Strafe. In der Gesamtbetrachtung halte ich, insbesondere wegen des relativ geringen Gewichts der zweiten Tat und des zeitlichen Abstands zwischen den beiden Taten, die Annahme, dass die beiden Delikte zusammen im Unrechtsgehalt einer Straftat von erheblicher Bedeutung gleichstehen, nicht für vertretbar. Auch die Prognoseentscheidung war formelhaft und pauschal. Eine auf den Einzelfall bezogene Bewertung war nicht erkennbar. Wie ohne Beiziehung weiterer Unterlagen, insbesondere der entsprechenden Urteile, beurteilt werden konnte, dass die Täterin aufgrund ihrer Persönlichkeitsstruktur in der Zukunft Straftaten

von erheblicher Bedeutung begehen wird, war für mich nicht erkennbar. Ich habe deshalb die Polizei gebeten, die DNA-Speicherung zu löschen oder nachvollziehbar das Vorliegen der gesetzlichen Voraussetzungen für die Maßnahme zu begründen.

Gleiches habe ich auch im Hinblick auf einen Betroffenen gefordert, der im Jahr 2001 wegen Beleidigung und Bedrohung zu 60 Tagessätzen zu je 15 DM und 2006 wegen Diebstahls geringwertiger Sachen zu 20 Tagessätzen zu je 5 € verurteilt worden war. Im ersten Fall hatte er den Personalchef eines Amtes und dessen Mitarbeiterin beleidigt und bedroht, im zweiten Fall in einem Einkaufsmarkt eine Schachtel Zigaretten entwendet.

Der Prognoseentscheidung der Polizei war zu entnehmen, dass aufgrund der Persönlichkeitsstruktur des Täters von einer erheblichen Wiederholungsgefahr auszugehen sei. Eine Verurteilung aus dem Jahr 2000 habe ihn nicht gehindert, weitere Straftaten zu begehen. Als Grund für die Gefahr der erneuten Begehung von Straftaten wurde lediglich angeführt, dass er eine geringe Hemmschwelle besitze, ein aggressives Wesen habe, gewalttätig sei und insbesondere noch weitere Diebstähle vorliegen würden.

Das Vorliegen der Voraussetzungen für die DNA-Maßnahme sehe ich hier nicht: Der Betroffene war wegen der Straftaten, die im Abstand von sechs Jahren begangen wurden und unterschiedliche Deliktsbereiche betreffen, zum Teil erheblich unter 100 Tagessätzen verurteilt worden. Auch eine Staatsanwaltschaft ist in einem anderen (nicht geprüften) Fall bei Verurteilungen jeweils unter 100 Tagessätzen (Erwerb von Betäubungsmitteln, Nötigung mit Beleidigung) nicht von der Erheblichkeit der Straftaten ausgegangen. Darüber hinaus war die Prognoseentscheidung formelhaft und berief sich auf „mehrere Diebstähle“, obwohl diese trotz ihres angeblichen Zusammenhangs mit der ersten Tat neben der Verurteilung wegen Beleidigung und Bedrohung keinerlei Erwähnung in der gerichtlichen Entscheidung gefunden hatten.

### 4.11.2 Formblätter bei DNA-Maßnahmen

Das Staatsministerium des Innern hatte ich gebeten, die Formblätter, die zur Dokumentation der Einwilligung in molekulargenetische Untersuchungen von Körperzellen zu Vergleichszwecken (§ 81 e Abs. 1 StPO) und zur Identitätsfeststellung bei Beschuldigten und Verurteilten in künftigen Strafverfahren (§ 81 g StPO) verwendet werden sollen, entsprechend meinen Forderungen zu ändern (vgl. dazu Nr. 4.10 meines letzten Tätigkeitsberichts). Das Staatsministerium des Innern hat in der Folge einen Hinweis auf den Umfang der Untersuchungen aufgenommen und zwei getrennte Formblätter für Beschuldigte und Zeugen/Dritte eingeführt.

Nach wie vor fehlt aber

- ein Hinweis auf die erforderliche Einwilligung und Unterschrift auch des Erziehungsberechtigten, wenn Jugendliche von einer DNA-Maßnahme betroffen sind.

  Die Beurteilung, ob im jeweiligen Einzelfall der Jugendliche über eine genügende Verstandesreife verfügt, um die Tragweite seiner Entscheidung verstehen zu können, ist schwierig. Es besteht deshalb die Gefahr, dass die Einwilligung wegen des Fehlens der erforderlichen Verstandesreife unwirksam ist, weil auf die Einwilligung des Erziehungsberechtigten verzichtet wird. Diese Unsicherheit kann mit Hilfe der gemeinsamen Einwilligung von Betroffenem und Erziehungsberechtigtem ausgeräumt werden. Wie notwendig der von mir geforderte Hinweis ist, zeigen die Vorgaben des Staatsministeriums für Unterricht und Kultus zur Einwilligung in die - im Vergleich zu einer DNA-Maßnahme - weniger eingriffsintensive Speicherung von Schülerdaten in der „passwortgeschützten Lernplattform“: Dort müssen die Jugendlichen selbst und ihre Erziehungsberechtigten in die Speicherung einwilligen.

  Ich beabsichtige deshalb zu prüfen, ob das Vorliegen der genügenden Verstandesreife der betroffenen Jugendlichen ausreichend geprüft und aussagekräftig dokumentiert wird.

- eine Information über die regelmäßige Dauer der Speicherung des DNA-Identifizierungsmusters in der DNA-Analyse-Datei.

- ein Hinweis, dass der Betroffene seine Einwilligung widerrufen kann und Ausführungen über die Rechtsfolgen eines Widerrufs (zu Einzelheiten vgl. meinen letzten Tätigkeitsbericht unter Nr. 4.10).

Ich bedaure die ablehnende Haltung des Staatsministeriums des Innern gerade deshalb besonders, weil eine ausreichende Information eine wesentliche Voraussetzung für eine wirksame Einwilligung ist.

### 4.12 Erkennungsdienstliche Behandlung

Überprüft habe ich in diesem Berichtszeitraum auch erkennungsdienstliche Behandlungen, bei denen sich die Betroffenen an mich gewandt hatten, nachdem sie sich durch die Maßnahme in ihren Datenschutzrechten verletzt sahen. Einen Fall halte ich wegen der Unverhältnismäßigkeit der Mittel für besonders erwähnenswert:

Der Petent war bei einer Verkehrsordnungswidrigkeit festgestellt worden, weil er die zulässige Höchstge-

schwindigkeit um 8 km/h überschritten hatte. Der an ihn als Halter des betreffenden Fahrzeugs übersandte Anhörungsbogen kam u.a. mit der Bemerkung „Strohköpfe“ an die Polizei zurück. Wegen des Verdachts der Beleidigung wurde der Anhörungsbogen an die zuständige Kriminalpolizeiinspektion übersandt, wo Fingerspuren gesichert werden konnten. Der Petent wurde daraufhin als Beschuldigter vorgeladen und für einen möglichen Spurenvergleich erkennungsdienstlich behandelt. Ein Spurenvergleich mit den Fingerabdrücken des Petenten wurde beim Landeskriminalamt veranlasst. Das gegen ihn geführte Ermittlungsverfahren wurde - ohne dass das Ergebnis des Spurenabgleichs bei der Staatsanwaltschaft vorlag - nach § 153 a StPO eingestellt.

Gemäß § 81 b 1. Alternative StPO dürfen Lichtbilder und Fingerabdrücke des Beschuldigten auch gegen seinen Willen aufgenommen und Messungen an ihm vorgenommen werden, soweit es für die Zwecke der Durchführung des Strafverfahrens notwendig ist. Solche Maßnahmen dienen der Strafverfolgung (Identifizierung), wenn sie Schuld oder Unschuld des Beschuldigten in einem gegen ihn anhängigen Strafverfahren beweisen sollen, insbesondere, wenn die Identifizierung notwendig ist, weil seine Person unbekannt ist oder von Zeugen wiedererkannt werden soll oder wenn Fingerabdrücke mit Tatortspuren verglichen werden sollen. Dabei ist aber auch der Grundsatz der Verhältnismäßigkeit zu beachten. Demnach dürfen Maßnahmen nur getroffen werden, wenn sie zur Bedeutung der Sache nicht außer Verhältnis stehen.

Ich habe der Polizei mitgeteilt, dass ich unter Gesamtwürdigung des Sachverhalts erhebliche Bedenken habe, dass die Durchführung der erkennungsdienstlichen Behandlung in einem angemessenen Verhältnis zur Straftat gestanden hat. Zudem war für mich nicht erkennbar, wie die durch die Maßnahme erhobenen Fingerabdrücke, Lichtbilder und körperlichen Merkmale des Petenten zur Aufklärung der gegenständlichen Straftat beitragen hätten können.

Das für die betreffende Inspektion zuständige Polizeipräsidium hat meine Bedenken geteilt. Zwar müsse die Maßnahme im Zusammenhang mit dem zunehmenden Phänomen betrachtet werden, dass immer mehr Betroffene strafrechtlich relevante Kommentare schriftlich versenden und dann ihre Urheberschaft bestreiten. Der betreffende Beamte sei belehrt, die erkennungsdienstlichen Unterlagen seien vernichtet und die entsprechenden Speicherungen gelöscht worden. Der Vorgang werde nicht mehr im Kriminalaktennachweis, sondern nur noch in der polizeilichen Vorgangsverwaltung nachgewiesen.

## 4.13 Video- und Bildaufzeichnungen

### 4.13.1 Videoüberwachung in Innenstadtbereichen

Die bayerische Polizei nutzt die Möglichkeit der Videoüberwachung öffentlicher Straßen und Plätze auf der Grundlage von Art. 32 Abs. 2 PAG in den Städten München, Nürnberg, Regensburg, Schweinfurt, Ingolstadt und in Straubing während des Gäubodenvolksfestes. In München sind Kameras am Bahnhofsvorplatz, am Stachusrondell, am Orleansplatz, am Marienplatz zur Zeit des Christkindlmarkts und auf der Theresienwiese während der Zeit des Oktoberfestes installiert.

Der Orleansplatz wird seit April 2007 mit drei Kameras videoüberwacht. Die Polizei hat mir mit der Übermittlung der entsprechenden Konzeption und den festgestellten Kriminalitätsbelastungszahlen die Erforderlichkeit der Videoüberwachung dargelegt. Im Rahmen einer gemeinsamen Ortsbegehung wurden die Standorte der insgesamt 18 Hinweisschilder abgesprochen. Keine Übereinstimmung konnte hinsichtlich der Speicherungsdauer für die Aufzeichnungen erzielt werden. In der ursprünglichen Konzeption wollte die Polizei die gesetzliche Höchstfrist von zwei Monaten ausschöpfen. Auf meine Intervention hin hat sie die Speicherungsdauer auf 30 Tage beschränkt. Die von mir geforderte Verkürzung auf sieben Tage hält die Polizei nicht für ausreichend. Zur Begründung wurde vorgetragen, dass aufgrund einer Auswertung von Anzeigen nach Straftaten der Straßenkriminalität festgestellt wurde, dass nach mehr als 20 Tagen 13,3 % der Geschädigten noch keine Anzeige erstattet hatten.

Bei der Beurteilung der Erforderlichkeit der Speicherfrist kommt es jedoch nicht primär auf das Anzeigeverhalten der Geschädigten an, da die Videoüberwachung kriminalitätsbelasteter Orte eine Maßnahme der Gefahrenabwehr darstellt. Die Beobachtung der Videoübertragung sollte live durch Polizeibeamte erfolgen, damit unverzüglich auf Gefahren reagiert werden kann. Darüber hinaus ist die Vorsorge für die spätere Verfolgung von Straftaten dem „gerichtlichen Verfahren“ i.S.d. Art. 74 Abs. 1 Nr. 1 GG zuzuordnen, so dass dafür keine Gesetzgebungskompetenz des Landesgesetzgebers besteht. Das Bundesverfassungsgericht hat in seinem Urteil zum niedersächsischen Gesetz zur präventiven Telekommunikationsüberwachung vom 27.07.2005 ausgeführt, dass die Beweisbeschaffung zur Verwendung in künftigen Strafverfahren keine präventive Datenerhebung zur Verhütung von Straftaten darstellt und damit als Verfolgungsvorsorge in die Gesetzgebungskompetenz des Bundes fällt. Darüber hinaus hat das Bundesverfassungsgericht in seiner Entscheidung vom 23.02.2007 anlässlich einer geplanten kommunalen Videoüberwachung eines öffentlichen Kunst-

werks hervorgehoben, dass diese Maßnahme einen intensiven Eingriff in das allgemeine Persönlichkeitsrecht der den öffentlichen Raum nutzenden Personen darstellt. Das Gewicht dieser Maßnahme werde noch dadurch erhöht, dass infolge der Aufzeichnung das gewonnene Bildmaterial in vielfältiger Weise ausgewertet, bearbeitet und mit anderen Informationen verknüpft werden könne. Dabei würden durch die Videoüberwachung und die Aufzeichnung des gewonnenen Bildmaterials überwiegend Personen erfasst, die selbst keinen Anlass schaffen, dessentwegen die Überwachung vorgenommen wird. Das Bundesverfassungsgericht weist außerdem darauf hin, dass auch in zeitlicher Hinsicht (also hinsichtlich der Speicherungsdauer der Aufzeichnungen) das Übermaßverbot zu beachten ist.

Dies ist hier - trotz der von der Polizei angeführten Zahlen zum Anzeigeverhalten von Geschädigten - nicht in ausreichendem Maße geschehen. Im Umkehrschluss haben nämlich 86,7 % der Geschädigten und damit ein weit überwiegender Teil bereits innerhalb von 20 Tagen Strafanzeige erstattet. Der Rechercheliste der Polizei zur Videoüberwachung war über dies zu entnehmen, dass in keinem Fall ein Zugriff auf Aufzeichnungen erforderlich war, die älter als sieben Tage waren. Nur in einem Fall war die Auswertung genau sieben Tage nach dem Ereignis erfolgt. In allen anderen Fällen ist eine polizeiliche Recherche spätestens drei Tage nach dem Ereignis vorgenommen worden.

Bei der Planung der polizeilichen Videoüberwachung des Zentralen Omnibusbahnhofs (ZOB) in Ingolstadt hätte ich mir eine frühere Unterrichtung durch die Polizei gewünscht. Dies gerade deshalb, weil ich grundsätzliche datenschutzrechtliche Bedenken gegen den dortigen Einsatz der Videoüberwachung habe. Die Kriminalitätsbelastung am ZOB liegt im Vergleich zu entsprechenden polizeilich überwachten Plätzen in einem relativ niedrigen Bereich (73 Straftaten pro Jahr). So wurden beispielsweise in Nürnberg am Plärrer 133 Straftaten festgestellt. Selbst am Rossmarkt in Schweinfurt (etwa 55 000 Einwohner im Vergleich zu etwa 125 000 in Ingolstadt) wurden über 250 Straftaten (Ladendiebstähle nicht berücksichtigt) registriert. Hinzu kommt, dass in Ingolstadt bei den 73 Straftaten auch 17 Leistungserschleichungen mitgezählt sind, bei denen eine künftige Verhinderung durch die polizeiliche Videoüberwachung nicht zu erwarten ist.

Der Verwaltungsgerichtshof Baden-Württemberg hat in seinem Urteil vom 21.07.2003 ausgeführt, dass ein Kriminalitätsschwerpunkt, der die Videoüberwachung rechtfertigt, eine besondere Kriminalitätsbelastung aufweisen müsse. Eine solche besondere Kriminalitätsbelastung sehe ich aufgrund der mir übermittelten Kriminalitätszahlen nicht. Die Polizei hat diese Sichtweise leider nicht geteilt und die Videoüberwachung Anfang September 2007 gestartet. Zumindest hat die Polizei die Aufbewahrungsfrist für die Videoaufzeichnungen auf sieben Tage beschränkt und die Schilder, mit denen auf eine Videoüberwachung hingewiesen wird, auf meine Anregung hin auf DIN-A3-Format vergrößert.

Während des Gäubodenvolksfestes 2008 in Straubing hat die zuständige Polizeidienststelle erstmals einen Teil der Straubinger Innenstadt videoüberwacht. Betroffen waren die Bereiche Theresien-/Ludwigsplatz, April- und Steinergasse, Am Platzl und Rosengasse. Die Überwachung fand im Zeitraum vom 08.08. bis 18.08.2008, jeweils zwischen 22:00 Uhr und 06:00 Uhr statt. Es wurden nur Bildaufnahmen und -aufzeichnungen und keine Tonaufnahmen gefertigt.

Das Polizeipräsidium hat mich wenige Wochen vor Beginn der Videoüberwachung über das Vorhaben informiert. Es hat mir dazu eine nach einzelnen Straßen der Innenstadt aufgeschlüsselte Statistik vorgelegt über Delikte, die während des Gäubodenvolksfestes 2007 in der Zeit von 22:00 Uhr bis 06:00 Uhr begangen worden waren. Die Statistik weist für den videoüberwachten Bereich im Vergleich zu anderen Gebieten der Stadt eine deutlich höhere Kriminalität aus. Ich habe die zeitlich begrenzte Videoüberwachung deshalb für grundsätzlich vertretbar erachtet.

Allerdings waren insbesondere die Hinweise der Polizei auf die Videoüberwachung verbesserungsbedürftig. Nach Art. 32 Abs. 2 Satz 2 PAG soll der Bürger in geeigneter Weise auf die Bildaufnahmen hingewiesen werden. Dieser Hinweispflicht kann durch das Anbringen geeigneter Schilder nachgekommen werden, die auf die Überwachung in ausreichendem Maß aufmerksam machen. Dabei müssen die Schilder so angebracht werden, dass sie vor Eintritt in den Beobachtungsraum zur Kenntnis genommen werden können. Der mir übersandte Beschilderungsplan sah ursprünglich nur für einen Teil der Seitenstraßen zum überwachten Bereich Hinweisschilder vor. Ich habe deshalb das Polizeipräsidium gebeten, an allen Zugangswegen Hinweisschilder so anzubringen, dass die Passanten vor Eintritt in den Erfassungsbereich der Kamera entscheiden können, ob sie sich der Videoüberwachung aussetzen wollen. Das Polizeipräsidium hat mir mitgeteilt, dass es die Beschilderung entsprechend erweitert habe.

Die Videoaufnahmen sollen nach den Vorstellungen der Polizei für längstens zwei Monate gespeichert werden. Ich habe das Polizeipräsidium darauf hingewiesen, dass diese nach dem Polizeiaufgabengesetz vorgesehene Frist als Höchstfrist zu verstehen ist und nicht als Regelfrist missverstanden werden darf. Deshalb ist im konkreten Fall zu prüfen, welche Aufbewahrungsfrist für die Videoaufzeichnungen im Rahmen der Zweimonatsfrist erforderlich und verhältnismäßig ist. Das Polizeipräsidium hat eingewandt, dass das Gäubodenvolksfest als zweitgrößtes

Volksfest in Bayern auch von vielen auswärtigen Besuchern besucht werde; es sei daher vielfach mit einem zeitlich erheblich verzögerten Anzeigeverhalten auswärtiger Geschädigter zu rechnen. Inzwischen hat mir das zuständige Polizeipräsidium mitgeteilt, dass die Löschung der Videoaufzeichnungen am 15.09.2008 abgeschlossen war.

Ich habe aber für Zugriffe auf die gespeicherten Aufnahmen weitere datenschutzrechtliche Vorkehrungen gefordert: So sollten zumindest der Name der zugreifenden Person, ggf. der Name des Veranlassers, aussagekräftige Angaben zum Anlass des Zugriffs sowie Zeit und Umfang des Zugriffs protokolliert werden. Das Polizeipräsidium hat diese Forderungen berücksichtigt.

Datenschutzrechtlich bedeutsam für die polizeiliche Videoüberwachung ist auch ein Urteil des Verwaltungsgerichts Hamburg: Darin wird der Polizei untersagt, eine für den Bereich einer Privatwohnung installierte automatische Schwarzschaltung der polizeilichen Videokamera aufzuheben. Art. 13 Abs. 1 GG erfordere, dass eine Videoüberwachung der Wohnung der Klägerin zuverlässig und dauerhaft unterbleibe. Dies sei durch die Schwarzschaltung gewährleistet.

Im Rahmen der Prüfung einer Polizeidienststelle habe ich mir die Schwenkbereiche der dort nach Art. 32 Abs. 2 PAG angebrachten Videokameras angesehen. Dabei habe ich festgestellt, dass Fenster von Büroräumen, aber auch Fenster, bei denen nicht erkennbar war, ob es sich um Privat- oder Büroräume handelt, angezoomt werden konnten. In einem Fenster waren Personen zu sehen, die an einem Tisch saßen, ohne dass die Personen oder deren Verhalten wegen der bestehenden Lichtverhältnisse im Detail zu erkennen waren. Unter anderen Bedingungen (z.B. bei beleuchtetem Raum, bei offenem Fenster) oder bei entlaubten Bäumen besteht aber durchaus die Möglichkeit, mit den polizeilichen Videokameras in Räume Einsicht zu nehmen und personenbezogene Aufzeichnungen zu fertigen. Eine Rechtsgrundlage für diese Datenerhebung in dem durch das Grundgesetz besonders geschützten Bereich besteht nicht.

Ich habe deshalb das Staatsministerium des Innern um Prüfung gebeten, mit welchen Maßnahmen eine Einsichtnahme in diese Bereiche ausgeschlossen werden kann. Eine Überprüfung der Schwenkbereiche polizeilicher Videokameras unter diesem Gesichtspunkt halte ich auch bei anderen Dienststellen für notwendig.

### 4.13.2 Videoüberwachung von Versammlungsteilnehmern durch Überwachungskameras

In den letzten Jahren hatte ich eine Vielzahl von Videoaufnahmen datenschutzrechtlich geprüft, die Polizeibeamte von Versammlungsteilnehmern angefertigt hatten, wie zum Beispiel anlässlich der Sicherheitskonferenz 2005 oder der Gegendemonstration zur „Nazi-Mahnwache“ (vgl. hierzu Nr. 4.15.4, 22. Tätigkeitsbericht). In diesem Berichtszeitraum habe ich Videoaufzeichnungen von Versammlungen kontrolliert, die mit Kameras angefertigt wurden, die zur Überwachung öffentlicher Straßen und Plätzen nach Art. 32 Abs. 2 PAG fest installiert sind.

Ich hatte die Polizei bereits im Vorfeld darauf hingewiesen, dass dem Grundrecht auf Versammlungsfreiheit nach der Rechtsprechung des Bundesverfassungsgerichts (Beschluss vom 14.05.1985, Az. 1 BvR 233/81, 1 BvR 341/81) ein besonderer Rang gebührt, da es als Zeichen der Freiheit, Unabhängigkeit und Mündigkeit des selbstbewussten Bürgers in einem freiheitlichen Staatswesen anzusehen ist. Art. 8 Abs. 1 GG garantiert die möglichst unbeeinflusste Teilnahme des Einzelnen vor und bei Versammlungen und schützt damit auch davor, das Grundrecht im Visier von Polizei oder Verfassungsschutz wahrnehmen zu müssen.

Schon die Kenntnis von Versammlungsteilnehmern, dass die polizeilichen Videokameras, wie z.B. am Hauptbahnhof und Stachus in München oder am Plärrer in Nürnberg, während der Versammlung eingeschaltet bleiben, könnte Auswirkungen auf die Unbefangenheit der Teilnehmer haben und damit ihre grundrechtlich geschützten Rechte beeinträchtigen. Wer damit rechnen muss, dass seine Versammlungsteilnahme behördlich registriert wird und ihm dadurch Risiken entstehen können, wird möglicherweise auf die Ausübung der Versammlungsfreiheit verzichten, wodurch die individuellen Entfaltungschancen des Einzelnen beeinträchtigt werden. Ich halte es daher entgegen der Auffassung der Polizei für verfassungsrechtlich grundsätzlich geboten, die zur Überwachung von öffentlichen Straßen und Plätzen installierten polizeilichen Kameras während Versammlungen und Aufzügen entweder abzuschalten oder von der Versammlung wegzudrehen.

Für eine datenschutzrechtliche Prüfung habe ich Videoaufzeichnungen der Versammlung „Für das ganze Bleiberecht - dauerhaft und echt“ angefordert. Dabei habe ich festgestellt, dass auch Versammlungsteilnehmer gefilmt und teilweise sehr deutlich erkenn- und identifizierbar herangezoomt worden waren, ohne dass die Voraussetzungen der §§ 12 a, 19 a Versammlungsgesetz dafür vorlagen. Die Polizei hatte ausgeführt, dass der filmende Beamte zunächst keine Kenntnis von der Versammlung gehabt habe. Die Nahaufnahmen sollten dazu dienen, den Grund der Verkehrsstörung und die Schriftzüge auf den Transparenten zu erkennen. Dazu hätten aber Versammlungsteilnehmer nicht über einen längeren Zeitraum personenbezogen gefilmt werden müssen. Diese Bildaufnahmen waren deshalb unzulässig und sind zwischenzeitlich gelöscht worden. In einem weiteren

Fall waren nur sog. Übersichtsaufzeichnungen angefertigt worden.

Ich halte an meiner Auffassung fest, dass nur durch ein grundsätzliches Abschalten oder Wegschwenken der Kameras während Versammlungen ein ausreichender Schutz der Versammlungsteilnehmer gewährleistet ist. Das betreffende Polizeipräsidium hat mir zwar mitgeteilt, dass alle polizeilichen Monitorbeobachter über die besonderen gesetzlichen Voraussetzungen für Bildaufnahmen von Versammlungen hingewiesen worden seien, das bisherige Verfahren aber beibehalten werde. Sollte ich bei meinen Prüfungen in Zukunft wieder unzulässige Videoaufzeichnungen von Versammlungsteilnehmern feststellen, werde ich diese datenschutzrechtlichen Verstöße förmlich beanstanden und das Innenministerium um Abhilfe bitten.

### 4.13.3 Auskunft der Polizei über Videoaufzeichnungen von Versammlungsteilnehmern

Ein Petent hat mir mitgeteilt, dass zwei Polizeibeamte eine angemeldete Versammlung von maximal sechs Teilnehmern vom Dach eines VW-Busses mit einer Videokamera durchgehend gefilmt hätten. Versammlungsteilnehmern, die sich kurzzeitig von der Versammlung entfernt hätten, sei gezielt „hinterher gefilmt“ worden. Der Bürger hat mich um datenschutzrechtliche Überprüfung gebeten.

Daraufhin habe ich das zuständige Polizeipräsidium zu diesem Sachverhalt um Stellungnahme und um Zusendung vorhandener Filme in Kopie gebeten. Das Polizeipräsidium hat mir geantwortet, dass der Versammlungsverlauf nicht „erforderte…, dass diese Beamten von der Versammlung Videoaufzeichnungen fertigten“. Die Beamten hätten das Objektiv „immer von der Versammlung weg gerichtet“.

Im Zusammenhang mit besagter Versammlung berichtete die Süddeutsche Zeitung (vgl. Ausgabe vom 29./30.03.2008, Seite 54), dass vom Polizeipräsidium im Zusammenhang mit der Versammlung die Durchsuchung von „Aktivisten“ und die Beschlagnahme von Flugblättern gefilmt worden seien. Dies sei dem Landesbeauftragten für den Datenschutz nicht mitgeteilt worden. Er „habe ja nur wissen wollen, ob man die Versammlung gefilmt habe“.

Daraufhin habe ich mich erneut an das Polizeipräsidium gewandt. Es hat mir in seiner Antwort mitgeteilt, es sei auf Grund des geschilderten Sachverhalts davon ausgegangen, dass lediglich zielgerichtete Videoaufnahmen der betreffenden Versammlung geprüft werden sollten. Es sei nicht davon ausgegangen, dass andere Geschehnisse, die „zwar in räumlicher und zeitlicher Nähe zu, jedoch außerhalb des … geschilderten Sachverhalts … [stattgefunden haben]“, von der Fragestellung umfasst waren. Weder Versammlung noch Versammlungsteilnehmer seien personenbezogen gefilmt worden. Es seien vielmehr polizeiliche Maßnahmen gegen zwei Beschuldigte aufgezeichnet worden. Die beiden hätten zum Aufnahmezeitpunkt nicht an der Versammlung teilgenommen. Dies hätten sie den Polizeibeamten auch erklärt.

Die Differenzierung des Polizeipräsidiums bezüglich meiner Anfrage danach, ob eine Person gerade zum Aufnahmezeitpunkt versammlungsrechtlich an der Versammlung „teilgenommen“ hat oder nicht, halte ich für nicht nachvollziehbar. Aus Sicht eines objektiven Empfängers konnte meine erste Anfrage an das Polizeipräsidium nur so verstanden werden, dass ich alle im räumlichen und zeitlichen Zusammenhang mit der Versammlung gefertigten Videoaufzeichnungen datenschutzrechtlich beurteilen wollte. Ob die abgebildeten Personen dabei „Versammlungsteilnehmer“ im Rechtssinne waren, war in diesem Zusammenhang deshalb nicht relevant. Ich hatte mich erkennbar auf einen bestimmten Lebenssachverhalt bezogen, ohne die Beantwortung meiner Anfrage von der Klärung versammlungsrechtlicher Statusfragen abhängig zu machen.

Die ursprüngliche Antwort des Polizeipräsidiums auf meine Anfrage ist deshalb unvollständig. Zumindest hätte es im Interesse meiner unfassenden datenschutzrechtlichen Prüfungsmöglichkeit auf die Existenz der Videoaufzeichnungen hinweisen müssen. Mit der unvollständigen Beantwortung meiner Anfrage hat es gegen die gesetzliche Pflicht, den Landesbeauftragten für den Datenschutz in der Erfüllung seiner Aufgaben zu unterstützen, verstoßen. Diesen Verstoß habe ich förmlich beanstandet.

### 4.13.4 Bildaufnahmen bei polizeilichen Gewahrsamnahmen

Bei der datenschutzrechtlichen Prüfung eines Polizeipräsidiums hatte ich festgestellt, dass Kriminalakten Polaroidfotos beigegeben waren, die die Betroffenen von Gewahrsamnahmen und den festnehmenden Polizeibeamten zeigen. Die Polizei hat zunächst als Rechtsgrundlage für das Anfertigen der Fotos Art. 19 Abs. 3 Satz 3 PAG angegeben, wonach der festgehaltenen Person nur solche Beschränkungen auferlegt werden dürfen, die der Zweck der Freiheitsentziehung oder die Ordnung im Gewahrsam erfordert. Die betreffenden Aufnahmen sollen nach Angaben der Polizei grundsätzlich nur im Zusammenhang mit sog. Massenfestnahmen angefertigt werden. Das jeweilige Foto diene dazu, die Gefahr von Verwechslungen auszuschließen, die schnelle Zuordnung des Festgehaltenen zum jeweiligen Vorgang zu ermöglichen, die Abwicklung des Verfahrens zu beschleunigen und somit einen ordnungsgemäßen Funktionsablauf zu gewährleisten. Darüber hinaus sei es den

festnehmenden Beamten dadurch möglich, zeitnah an den jeweiligen Einsatzort zurückzukehren und weitere Festnahmen zu tätigen.

Das Fertigen von Polaroidfotos der festgenommenen Personen im Rahmen der Gewahrsamsannahme stellt einen Eingriff in das Recht auf informationelle Selbstbestimmung dar. Sinn und Zweck des Art. 19 Abs. 3 Satz 3 PAG ist es, der Polizei, die auch für die Sicherheit im Gewahrsam zuständig ist, eine ordnungsgemäße Durchführung der Freiheitsentziehung zu ermöglichen. Die Vorschrift ist im Hinblick auf die Grundrechtsrelevanz der über die Freiheitsentziehung hinaus gehenden Eingriffe eng auszulegen. Nach Nr. 19.3 der Vollzugsbekanntmachung zum PAG sind Beschränkungen i.S.d. Art. 19 Abs. 3 Satz 3 PAG beispielsweise Fesselung, Verbot des Schreibens, Entzug mitgeführter Sachen. Zwar ist diese Aufzählung nur beispielhaft, jedoch stellt sie eine Auslegungshilfe dar, die zeigt, dass Maßnahmen, die über die Sicherung des Gewahrsams hinausgehen, nicht zulässig sind.

Polaroidfotos von Betroffenen und den festnehmenden Beamten dienen dagegen dazu, die Situation der Gewahrsamnahme festzuhalten. Sie werden zu Dokumentationszwecken gefertigt und nicht in erster Linie zu Zwecken, die die Freiheitsentziehung als solche oder die Ordnung im Gewahrsam erfordert.

Ich habe deshalb bei einem Polizeipräsidium eine datenschutzrechtliche Überprüfung der Praxis vorgenommen. Für die Bildaufnahmen von 18 betroffenen Personen wurde von der Polizei zusätzlich § 81 b 1. Alternative StPO als Rechtsgrundlage angeführt, wonach zum Zwecke der Durchführung des Strafverfahrens (z.B. Erleichterung der Identifizierung) auch Lichtbilder vom Beschuldigten angefertigt werden können. Im vorliegenden Fall war gegen alle 18 Betroffenen ein Ermittlungsverfahren eingeleitet worden und die Sachaufklärung erschien ohne Bildaufnahmen gefährdet. Die Lichtbilder wurden - nachdem sie nicht mehr als Beweismittel erforderlich waren - gelöscht.

Auch bei Massengewahrsamnahmen kommt die Anfertigung von Bildaufnahmen ausnahmsweise in Betracht, wenn die Ordnung im Gewahrsam (z.B. Zuordnung der Betroffenen zu einem bestimmten Vorgang) dies erfordert. Solche Aufnahmen dürfen jedoch nicht zum Standardinstrumentarium bei polizeilichen Festnahmen oder Gewahrsamnahmen werden.

### 4.13.5 Präventive Bildaufnahmen von Jugendlichen

Durch mehrere Bürgereingaben und durch Presseveröffentlichungen wurde ich darüber informiert, dass eine Polizeiinspektion in ihrem Zuständigkeitsbereich gezielt Bildaufnahmen von Kindern und Jugendlichen fertigt. Auf meine Nachfrage hin teilte mir die Polizei mit, dass in der betreffenden Gemeinde ein signifikanter Anstieg von Straftaten und Ordnungswidrigkeiten zu verzeichnen sei, der zum Teil auf Alkohol konsumierende Jugendliche und Heranwachsende zurückzuführen sei. Dadurch sei das Sicherheitsgefühl der Bevölkerung zunehmend beeinträchtigt worden. Die Polizeiinspektion habe deshalb ein Konzept zur Bekämpfung der Straßenkriminalität umgesetzt. Im Rahmen dieses Konzepts seien von potentiellen Störern offen Lichtbildaufnahmen gefertigt und die Identität der Betroffenen festgestellt worden. Dabei soll es sich nach Auffassung der Polizei aber nicht um eine erkennungsdienstliche Maßnahme gehandelt haben. Ziel der Maßnahmen sei eine präventivpolizeilich motivierte Verunsicherung und Abschreckung der erfassten Personen.

Nach dem Polizeiaufgabengesetz (vgl. Art. 32 Abs. 2 PAG) kann die Polizei unter den dort genannten Voraussetzungen offen Bildaufnahmen oder -aufzeichnungen von Personen anfertigen. In Betracht kommt die Bildaufzeichnung eines Geschehensablaufs, bei dem sich nach vorliegenden und dokumentierten polizeilichen Erkenntnissen und Erfahrungen mit hoher Wahrscheinlichkeit Sicherheitsstörungen im öffentlichen Bereich entwickeln können. Wenn es im weiteren Verlauf zu Sicherheitsstörungen kommen sollte, dienen die Aufzeichnungen als Beweismaterial zur Dokumentation der Situation und ermöglichen der Polizei, anhand der Aufnahmen Störer ausfindig zu machen und zu identifizieren.

Im vorliegenden Fall hatte die Polizei aber nicht eine gefahrenträchtige Situation in einem bestimmten öffentlichen Bereich gefilmt, sondern gezielt die Identität einzelner Personen ohne konkreten, durch Handlungen des Betroffenen begründeten Anlass festgestellt und diese fotografiert, um sie zu verunsichern und abzuschrecken. Bei dieser Sachlage können die Bildaufnahmen nicht auf Art. 32 Abs. 2 PAG gestützt werden, sondern sind als (teilweise) erkennungsdienstliche Behandlung zu bewerten. Die Rechtmäßigkeit der Maßnahme richtet sich daher nach § 81 b StPO. Nach den vorliegenden Erkenntnissen handelte es sich bei den Betroffenen zum Zeitpunkt der Maßnahme aber nicht um Beschuldigte, was eine erkennungsdienstliche Behandlung nach § 81 b StPO evtl. gerechtfertigt hätte.

Ich habe deshalb die Polizei aufgefordert, künftig von solchen Bildaufnahmen abzusehen und insbesondere die betreffende Dienststelle auf meine Rechtsauffassung hinzuweisen. Das zuständige Polizeipräsidium hat mir daraufhin mitgeteilt, dass die Bildaufzeichnungen gelöscht wurden und es die Angelegenheit - unabhängig der unterschiedlichen Rechtsauffassungen - zum Anlass genommen hat, die betroffene Polizeidienststelle hinsichtlich der Belange des Datenschutzes im Allgemeinen und der Bedeutung des

Grundsatzes der Verhältnismäßigkeit im Besonderen umfänglich zu sensibilisieren.

### 4.14 Akkreditierungsverfahren und Zuverlässigkeitsüberprüfungen

#### 4.14.1 Akkreditierungsverfahren bei Großereignissen

In meinem letzten Tätigkeitsbericht (Nr. 4.4.1) habe ich mich zu sog. Zuverlässigkeitsüberprüfungen unter Einbindung von Sicherheitsbehörden geäußert, die anlässlich der Fußballweltmeisterschaft 2006 und des Papstbesuchs in Bayern durchgeführt worden waren. Eine bereichsspezifische gesetzliche Grundlage für diese Überprüfungen bestand und besteht weiterhin nicht. Aufgrund der Sicherheitslage bei solchen Großereignissen, der besonderen Bedeutung der Veranstaltungen, ihrer Einmaligkeit für längere Zeit und der Einwilligung der Betroffenen habe ich gegen die mit der Durchführung des Akkreditierungsverfahrens verbundene Beteiligung des Landeskriminalamts und - anlässlich der Fußballweltmeisterschaft 2006 auch des Landesamts für Verfassungsschutz - keine grundsätzlichen Bedenken erhoben.

Allerdings halte ich eine Entscheidung des Gesetzgebers über das „Ob“ und das „Wie“ solcher Zuverlässigkeitsüberprüfungen für notwendig, falls das Verfahren auf Dauer angelegt sein sollte. Ich sehe mit Sorge, dass Zuverlässigkeitsüberprüfungen bei Großveranstaltungen auf der Grundlage „informierter Einwilligungen“ inzwischen offenbar als Regelverfahren durchgeführt werden. So wurden anlässlich des G 8-Gipfels 2007 sowie der EU-Ratspräsidentschaft der Bundesrepublik Deutschland im ersten Halbjahr 2007 im Rahmen eines bundesweiten Akkreditierungsverfahrens unter Einbindung von Polizei und Verfassungsschutz Überprüfungen von Personen vorgenommen, die Zutritt zu den jeweiligen Veranstaltungsorten erhalten wollten (z.B. Pressevertreter, Hotelmitarbeiter, Wachschutz, Fahrdienst).

Bürgereingaben im Zusammenhang mit den o.g. Zuverlässigkeitsüberprüfungen sind in meiner Geschäftsstelle nicht eingegangen. Das Landeskriminalamt und das Landesamt für Verfassungsschutz haben mir auf Anfrage mitgeteilt, dass alle im Rahmen dieser Akkreditierungsverfahren gespeicherten personenbezogenen Daten gelöscht wurden.

Zuverlässigkeitsüberprüfungen bei Großveranstaltungen führen aufgrund ihrer Bedeutung und ihres Umfangs zu schwerwiegenden Eingriffen in das Grundrecht auf informationelle Selbstbestimmung einer Vielzahl Betroffener. An der Freiwilligkeit einer Einwilligung in solche Eingriffe bestehen erhebliche Zweifel, weil Betroffene oft Nachteile befürchten müssen, wenn sie die Einwilligung verweigern. Darüber hinaus ist eine Einwilligung auch im Hinblick auf den Grundsatz des Vorbehalts des Gesetzes problematisch. Gemäß der vom Bundesverfassungsgericht entwickelten Wesentlichkeitslehre muss der Gesetzgeber „in grundlegenden normativen Bereichen, zumal im Bereich der Grundrechtsausübung … alle wesentlichen Entscheidungen selbst … treffen“ (BVerfGE 61, 260, 275; E 88, 103, 116). Dies gilt für die wesentlichen Entscheidungen über die Voraussetzungen, Umstände und Folgen von Eingriffen, die er nicht an die Verwaltung delegieren darf.

Die Datenschutzbeauftragten des Bundes und der Länder haben sich am 25./26.10.2007 in einer Entschließung gegen die bisherige Praxis ausgesprochen, umfassende Zuverlässigkeitsüberprüfungen vor Großveranstaltungen standardmäßig unter Einbeziehung der Datenbestände von Polizei und Verfassungsschutzbehörden nur auf der Grundlage einer Einwilligung der Betroffenen durchzuführen (vgl. Anlage Nr. 11). Wenn Akkreditierungsverfahren als Regelüberprüfungsverfahren institutionalisiert werden, reichen - wie die bereichsspezifischen Regelungen des Atomgesetzes und des Luftsicherheitsgesetzes zeigen - auch die gesetzlichen Vorschriften z.B. über Datenabgleich und Datenübermittlung nicht aus, um die Mitwirkung von Polizei und Verfassungsschutz an solchen Verfahren zu rechtfertigen. Solche Eingriffe sollten nur durchgeführt werden, wenn sie durch ein Gesetz, das den verfassungsrechtlichen Anforderungen - insbesondere den Grundsätzen der Normenklarheit und Verhältnismäßigkeit - genügt, erlaubt sind.

Das Staatsministerium des Innern, dem ich meine rechtliche Einschätzung zur Kenntnis gegeben habe, hat mir mitgeteilt, dass auch in Zukunft bei Großveranstaltungen mit einer entsprechend hohen Gefährdungseinschätzung Zuverlässigkeitsüberprüfungen (nur) auf die Einwilligung der Betroffenen gestützt werden. Ich bedaure, dass das Staatsministerium des Innern an diesem Verfahren festhalten will, ohne sich mit der verfassungsrechtlichen Problematik erkennbar auseinandergesetzt zu haben.

In einem Fall habe ich mich zusammen mit dem Bayerischen Journalisten-Verband e.V. gegen eine geplante Zuverlässigkeitsüberprüfung durch einen privaten Veranstalter - unter Beteiligung der Polizei - ausgesprochen und auf eine Änderung des Akkreditierungsverfahrens hingewirkt. Nach einer intensiven Überzeugungsarbeit hat der Veranstalter an der vorgesehenen Beteiligung der Polizei nicht mehr festgehalten. Statt dessen wurde ein Verfahren durchgeführt, in dessen Rahmen Journalisten lediglich ihren Personal- und Presseausweis vorlegen mussten.

### 4.14.2 Zuverlässigkeitsüberprüfungen durch Arbeitgeber und Polizei

Zuverlässigkeitsüberprüfungen auf der Grundlage von Einwilligungen unter Einbindung der Polizei werden nicht nur anlässlich von Großveranstaltungen durch öffentliche Stellen durchgeführt. Auch einzelne Arbeitgeber fordern Bewerber, Beschäftigte und Fremdpersonal (z.B. Reinigungskräfte) auf, in eine Anfrage des Arbeitgebers bei der Polizei zu etwaigen dort vorliegenden Erkenntnissen zu ihrer Person einzuwilligen. In anderen Fällen sollen die Betroffenen eine solche Auskunft („fremdbestimmte Selbstauskunft“) selbst einholen und ihrem Arbeitgeber vorlegen.

Die dem Arbeitgeber so zugänglich gemachten Informationen können über den zulässigen Inhalt eines „Führungszeugnisses“ hinausgehen. Die Polizei speichert - neben den in ein „Führungszeugnis“ aufzunehmenden Daten - auch personenbezogene Daten, die in das Bundeszentralregister gar nicht erst eingetragen werden, bereits getilgt sind oder Arbeitgebern in einem „Führungszeugnis“ nicht übermittelt werden dürfen.

Soweit die bestehenden Regelungen z.B. des Luftsicherheitsgesetzes und des Atomgesetzes auf diese Zuverlässigkeitsüberprüfungen nicht anwendbar sind, fehlt dafür eine bereichsspezifische gesetzliche Regelung. Aus datenschutzrechtlicher Sicht ist es höchst problematisch, die polizeiliche Datenübermittlung allein auf die Einwilligung des Betroffenen zu stützen. Bei Bewerbungen und Arbeitsverhältnissen ist die Freiwilligkeit der Einwilligung des Betroffenen zumindest zweifelhaft. Die Betroffenen sehen sich oftmals dem faktischen Druck des Wohlverhaltens im Hinblick auf den Erhalt oder die Sicherung des Arbeitsplatzes ausgesetzt (vgl. dazu Entschließung der Datenschutzbeauftragten des Bundes und der Länder vom 03./04.04.2008, Anlage Nr. 19).

Ich bin der Ansicht, dass derartige polizeiliche Auskünfte an Personen oder Stellen außerhalb des öffentlichen Bereichs grundsätzlich nur zur polizeilichen Gefahrenabwehr in Betracht kommen, da der Arbeitgeber mit Hilfe eines „Führungszeugnisses“ die „Zuverlässigkeit“ des Betroffenen überprüfen kann. Vom Staatsministerium des Innern wird diese Auffassung grundsätzlich geteilt. Bei der Prüfung, ob die Voraussetzungen für eine Datenübermittlung an Arbeitgeber vorliegen, komme der Art der künftigen Tätigkeit des Betroffenen und dem vorgesehenen Einsatzbereich im Unternehmen eine besondere Bedeutung zu. Das Staatsministerium des Innern hat angekündigt, die Polizei im Hinblick auf die bestehende Rechtslage zu sensibilisieren.

### 4.15 Datenabfragen und Datenübermittlungen

Auch in diesem Berichtszeitraum haben mich wieder Übermittlungen personenbezogener Daten durch die Polizei beschäftigt. Dabei habe ich erneut in einigen Fällen feststellen müssen, dass das Persönlichkeitsrecht der Betroffenen verletzt wurde. In einem gravierenden Fall habe ich die betreffende Polizeidienststelle förmlich beanstandet:

Während eines Urlaubsaufenthalts eines Petenten in einer Pension war es zu einem Vorfall gekommen, aufgrund dessen der Gastwirt zivilrechtliche Ansprüche gegenüber dem Betroffenen geltend machen wollte. In der Folge soll es zu Problemen bei der postalischen Zustellung von Schreiben an den außerhalb Bayerns wohnenden Petenten gekommen sein. Deswegen soll der dem Wirtsehepaar bekannte bayerische Polizeibeamte die von ihm mit Hilfe einer außerbayerischen Polizeidienststelle ermittelte Telefonnummer zum Zwecke der Kontaktaufnahme an den Gastwirt weitergegeben haben. Zur Ermittlung der Telefonnummer hatte der Polizeibeamte die außerbayerische Dienststelle um Vorsprache bei dem Petenten gebeten. Beim ersten Besuch sollen die uniformierten Polizeibeamten zwar festgestellt haben, dass der Petent tatsächlich unter der angegebenen Adresse wohnhaft war, die Telefonnummer konnten sie jedoch nicht in Erfahrung bringen. Dies war erst bei der zweiten Vorsprache der Polizei gelungen. Kurze Zeit später hat die Ehefrau des Gastwirts beim Petenten angerufen.

Die Polizei hat die Übermittlung der Telefonnummer an den Gastwirt zunächst auf Art. 41 Abs. 2 Nr. 2 PAG gestützt. Dies hätte allerdings vorausgesetzt, dass die Datenübermittlung offensichtlich im Interesse des Petenten lag. Ein solches Interesse war aber weder dargetan noch ersichtlich. Auch die Voraussetzungen des Art. 41 Abs. 2 Nr. 1 PAG waren nicht erfüllt, da neben der Kenntnis der Anschrift des Petenten ein rechtliches Interesse gerade an der Kenntnis der Telefonnummer nicht bestand. Vielmehr hatte er ein schutzwürdiges Interesse am Ausschluss der Übermittlung der Telefonnummer, zumal diese bewusst nicht in frei zugänglichen Verzeichnissen gespeichert war.

Die Polizei hat mir gegenüber weiter angeführt, dass der Vorgang wegen des Verdachts einer Straftat der Staatsanwaltschaft vorgelegt worden sei, nachdem aufgrund der Unzustellbarkeit des Forderungsschreibens der Gastwirtsfamilie von der Angabe einer falschen Adresse durch den Petenten ausgegangen worden sei. Gleichzeitig wurde aber auch eingeräumt, dass die Erhebung der Telefonnummer sowie deren Weitergabe an den Gastwirt nicht erforderlich waren, insbesondere nachdem die Staatsanwaltschaft die Anzeige nicht weiter verfolgt hatte.

Die Datenübermittlung war auch nicht zur Verfolgung von Straftaten oder Ordnungswidrigkeiten erforderlich. Sie diente offensichtlich der Möglichkeit der telefonischen Kontaktaufnahme des Wirtsehepaars mit dem Petenten, um damit den finanziellen Forderungen Nachdruck zu verleihen. Erschwerend kommt hinzu, dass der Polizeibeamte eine außerbayerische Polizeidienststelle veranlasst hatte, den Petenten deswegen zweimal aufzusuchen. Diesen Datenschutzverstoß habe ich nach Art. 31 Abs. 1 Satz 1 BayDSG förmlich beanstandet.

In einem weiteren Fall war es zwischen dem Hund des Petenten und dem Hund der Lebensgefährtin eines Polizeibeamten zu einer Beißerei gekommen. Dabei soll nach Darstellung der Polizei der nicht angeleinte Hund des Petenten zum zweiten Mal einen anderen Hund gebissen haben. Der Polizeibeamte habe den Petenten zur Rede gestellt und sich als Kriminalbeamter zu erkennen gegeben, da er eine Gefahr für die Allgemeinheit erkannt habe und die Umstände dem zuständigen Ordnungsamt mitteilen wollte. Um zu diesem Zweck die vollständigen Personalien des Hundehalters festzustellen, hat der Beamte eine Abfrage über das Einwohnermeldeverfahren (EWO) veranlasst. Systembedingt hat er dabei neben den Personalien auch Erkenntnis über die waffenrechtlichen Erlaubnisse des Petenten erlangt. Aufgrund der wiederholten Beißattacken des Hundes und des Verhaltens des Petenten hat der Polizeibeamte eine Anzeige an das Ordnungsamt mit dem Ziel übermittelt, die Zuverlässigkeit des Petenten bei der Hundehaltung überprüfen zu lassen sowie ggf. Gefahren abwehrende Maßnahmen (Leinenzwang) zu veranlassen.

Ich habe dem Polizeipräsidium mitgeteilt, dass die mir vorliegende Anzeige nicht als polizeiliche Anzeige, sondern im Hinblick auf die Gesamtumstände als Privatanzeige des Polizeibeamten anzusehen ist. Die Anzeige war nicht als polizeiliches Schreiben erkennbar. So war weder dienstliches Briefpapier verwendet worden, noch war als Absender eine Polizeidienststelle oder die Absicht des Anzeigeerstatters als Polizeibeamter handeln zu wollen, erkennbar. Auch lag kein entsprechender polizeilicher Anzeigenvorgang vor. Lediglich der von der Polizei mitgeteilte Hinweis des Polizeibeamten beim Ordnungsamt auf seine berufliche Tätigkeit lässt eine andere Beurteilung nicht zu. Eher ist davon auszugehen, dass er damit seiner privaten Anzeige Nachdruck verleihen wollte. Demnach hatte der Polizeibeamte die im Dienst erlangten Informationen - insbesondere die Kenntnis waffenrechtlicher Erlaubnisse - privat genutzt und an das Ordnungsamt übermittelt. Bereits die Datenabfrage wäre - unabhängig vom Tätigwerden des Beamten im eigenen sozialen Nahbereich - unzulässig gewesen, wenn sie zu diesem Zweck (private Nutzung) stattgefunden hätte.

Ein weiterer Bürger hatte sich mit der Bitte an mich gewandt, eine von der Polizei auf Verlangen einer Gemeinde durchgeführte Abfrage seiner Kfz-Halterdaten und die Übermittlung dieser Daten an die Gemeinde zu überprüfen. Hintergrund war eine Meinungsverschiedenheit zwischen dem Petenten und einem Gemeindebediensteten, ob der Petent ihn bei der Dienstausübung fotografiert habe. Der Gemeinde war zu diesem Zeitpunkt nur das Kennzeichen des von dem Petenten gefahrenen Kraftfahrzeugs bekannt. Die Gemeinde befürchtete eine Veröffentlichung der - streitigen - Fotografien und hat deshalb die Polizei gebeten, über das Kfz-Kennzeichen des Bürgers seinen Namen und seine Anschrift zu ermitteln (sog. Kfz-Halterabfrage) und ihr mitzuteilen. Der Dienstvorgesetzte des Gemeindebediensteten hat nach Erhalt dieser Daten die Telefonnummer des Bürgers aus dem Telefonbuch ermittelt und ihm telefonisch eine etwaige Veröffentlichung der streitigen Fotografien untersagt.

Ich halte die von der Gemeinde an die Polizei herangetragene Bitte, die Kfz-Halterdaten abzufragen und an sie zu übermitteln, für eine unzulässige Datenerhebung. Art. 16 BayDSG gestattet die Erhebung personenbezogener Daten nur unter der Voraussetzung, dass sie zur „Aufgabenerfüllung“ erforderlich ist.

Aufgabe einer Gemeinde ist u.a. die Abwehr von Gefahren z.B. durch die Verhütung von Straftaten (vgl. Art. 6 Landesstraf- und Verordnungsgesetz). Zwar ist die Veröffentlichung von Fotografien ohne Einwilligung der abgebildeten Person grundsätzlich strafbar gemäß § 33 Kunsturhebergesetz. Allerdings konnte ich im vorliegenden Fall keine sicherheitsrechtlich relevante Gefahr einer drohenden Veröffentlichung und damit einer Straftat erkennen. Der verwaltungsgerichtlichen Rechtsprechung zufolge existiert kein allgemeiner Erfahrungssatz, dass Personen, die im Verlauf eines Einsatzes (auch) Polizeibeamte fotografieren, die Aufnahme anschließend verbreiten oder öffentlich zur Schau stellen. Selbst bei Pressefotografen müsse im Hinblick auf die zivil- und strafrechtlichen Sanktionen einer unrechtmäßigen Veröffentlichung grundsätzlich von der Rechtstreue des Fotografen ausgegangen werden. Es dürfe nicht von vornherein und ohne weitere Anhaltspunkte zukünftiges rechtswidriges Verhalten unterstellt werden. Anhaltspunkte dafür, die Fotos könnten gegen den Willen des Abgebildeten veröffentlicht werden (insbesondere durch die Medien), bestanden vorliegend nicht.

Die von der Polizei durchgeführte Kfz-Halterdatenabfrage wäre nur zur Abwehr einer Gefahr zulässig gewesen. Ich halte sie aus den o.g. Gründen, wegen des Fehlens einer Gefahr, ebenfalls für rechtswidrig. Darüber hinaus waren die Datenübermittlung der Polizei an die Gemeinde und die anschließende Datenverwendung durch die Gemeinde

rechtswidrig, weil die Übermittlung und Verwendung rechtswidrig erhobener Daten datenschutzrechtlich nicht „erforderlich“ ist (vgl. Art. 40 Abs. 4 Nrn. 1 und 3 PAG, Art. 17 Abs. 1 Nrn. 1 und 2 BayDSG).

Ich habe deshalb die Gemeinde aufgefordert, künftig die Erhebung und Nutzung personenbezogener Daten ohne gesetzliche Grundlage zu unterlassen. Das Polizeipräsidium habe ich aufgefordert, durch geeignete Maßnahmen darauf hinzuwirken, dass künftig solche Kfz-Halterabfragen und Datenübermittlungen ohne gesetzliche Grundlage unterbleiben.

In den vorangegangenen Berichtszeiträumen hatte ich Datenabfragen aus dem polizeilichen Informationssystem im sozialen Nahfeld der abfragenden Polizeibeamten und die Protokollierung eines Abfragegrundes thematisiert. Auch in diesem Berichtszeitraum habe ich wieder in einigen Fällen feststellen müssen, dass sich die Abfragenden bei entsprechenden Nachfragen im Rahmen von Datenschutzkontrollen zum Teil nicht mehr an den Grund der Datenabfrage erinnern konnten. Dies zeigt deutlich die Berechtigung meiner Forderung nach Protokollierung des Abfragegrundes, wie sie beispielsweise im Zentralen Verkehrsinformationssystem (ZEVIS) vorgenommen wird. Ich habe eine solche Protokollierung erneut im Zusammenhang mit der Änderung der Errichtungsanordnung für die Protokolldatei gefordert. Leider lehnt das Staatsministerium des Innern die Umsetzung dieser Forderung aus nicht nachvollziehbaren Gründen nach wie vor ab.

### 4.16 Auskunftserteilung über polizeiliche Speicherungen

Auf der Grundlage des Art. 48 PAG geben bayerische Polizeidienststellen grundsätzlich Auskunft über die Speicherung personenbezogener Daten des Betroffenen im „Bayerischen Kriminalaktennachweis“ (KAN) und in der polizeilichen Vorgangsverwaltung. Eine Mitteilung, ob und ggf. welche Speicherungen nicht nur im Landes-KAN, sondern auch im Bundes-KAN gespeichert sind, ist damit nicht verbunden. Dadurch kann beim Empfänger der Auskunft der Eindruck entstehen, dass eine bundesweite Speicherung und damit die Möglichkeit einer bundesweiten Nutzung nicht gegeben ist. Nach § 12 Abs. 5 Satz 3 Bundeskriminalamtgesetz (BKAG) kann das Landeskriminalamt - sofern es aus seinem Landesbestand Auskunft erteilt - damit einen Hinweis auf einen von seinem Land im polizeilichen Informationssystem (INPOL-Bund) eingegebenen Datensatz verbinden. Ich habe deshalb das Innenministerium aufgefordert, von dieser Ermächtigung Gebrauch zu machen und Auskünfte aus dem Landes-KAN mit einem Hinweis auf Speicherungen bayerischer Daten im Bundes-KAN zu verbinden. Dadurch würde der Betroffene auch darüber informiert werden, welche Daten bundesweit verfügbar sind.

Das Innenministerium hat die Auffassung vertreten, dass das Bundeskriminalamt (BKA) speichernde Stelle für die im Bundes-KAN nachgewiesenen Daten sei und deshalb dem Betroffenen Auskünfte über solche Speicherungen nach § 12 Abs. 5 Satz 2 BKAG vom BKA erteilt werden sollten. Danach seien Auskünfte aus dem Bundes-KAN grundsätzlich vom BKA im Einvernehmen mit der Stelle zu erteilen, die die datenschutzrechtliche Verantwortung für die gespeicherten Daten trägt. Einen konkreten Hinweis auf die Speicherung bayerischer Datensätze im Bundes-KAN hält das Innenministerium nicht für erforderlich.

Eine Umfrage bei den Landesbeauftragten für den Datenschutz der anderen Bundesländer hat ergeben, dass in mindestens sieben Bundesländern ein entsprechender Hinweis erteilt wird. So werden beispielsweise in einem Bundesland Auskünfte über Speicherungen im Landes-KAN bezüglich der Speicherung eigener Daten im Bundes-KAN wie folgt ergänzt:

„Im Kriminalaktennachweis Bund, der allen Polizeidienststellen bundesweit auf Abruf zur Verfügung steht, sind folgende Informationen über Sie gespeichert:…“

Einen solchen ergänzenden Hinweis auf die bundesweite Speicherung polizeilicher Landes-KAN-Daten würde ich auch bei der Bayerischen Polizei begrüßen. Leider ist das Staatsministerium des Innern auch meiner erneuten Aufforderung zur Umsetzung einer bürger- und datenschutzfreundlichen Auskunftspraxis in diesem Punkt nicht gefolgt.

## 5 Verfassungsschutz

Beim Landesamt für Verfassungsschutz (LfV) habe ich im Berichtszeitraum wieder Überprüfungen von Datenerhebungen, -speicherungen und -übermittlungen sowie von Auskunftserteilungen bzw. -ablehnungen vorgenommen. Die Prüfungen erfolgten anlassunabhängig (zwei Prüfungen vor Ort) oder aufgrund von Bürgereingaben. Schwerpunkte waren Speicherungen in der Antiterrordatei, von Abgeordneten einer Partei und Speicherungen im Zusammenhang mit der Organisierten Kriminalität im Informationssystem IBA.

Im Bereich der bayerischen Gesetzgebung habe ich mich für die Berücksichtigung datenschutzrechtlicher Anforderungen bei der Änderung des Bayerischen Verfassungsschutzgesetzes (vgl. hierzu Nr. 5.1 - Änderung des Bayerischen Verfassungsschutzgesetzes) eingesetzt. Dabei waren die Anpassung der Befugnis zum „Großen Lauschangriff“ an die Vorgaben des Bundesverfassungsgerichts (vgl. hierzu Nr. 5.1.1), die Einführung einer Befugnis zur „Online-Durchsuchung“ (vgl. hierzu Nr. 5.1.4) und die Schaffung einer grundsätzlichen Auskunftspflicht des

Landesamts für Verfassungsschutz gegenüber Betroffenen von Datenspeicherungen (vgl. hierzu Nr. 5.1.6) von besonderer datenschutzrechtlicher Bedeutung.

## 5.1 Änderung des Bayerischen Verfassungsschutzgesetzes (BayVSG)

Ein wesentlicher Grund für die Änderung des Bayerischen Verfassungsschutzgesetzes lag in der Notwendigkeit, die Regelung zur Wohnraumüberwachung (sog. Großer Lauschangriff) an die Vorgaben des Bundesverfassungsgerichts in seinem Urteil vom 03.03.2004 zum „Großen Lauschangriff“ anzupassen. Bereits in meinem vorletzten Tätigkeitsbericht (vgl. Nr. 8.1, 21. Tätigkeitsbericht) habe ich darauf hingewiesen, dass die aus dem Urteil sich ergebenden Anforderungen im Gesetz umzusetzen sind. Durch die Anpassung der Befugnis zur Wohnraumüberwachung - die allerdings erst nach mehr als vier Jahren vorgenommen wurde - hat der Gesetzgeber insbesondere den Schutz des Kernbereichs privater Lebensgestaltung und von Berufsgeheimnissen gestärkt sowie Kennzeichnungspflichten bezüglich der erhobenen Daten und Benachrichtigungspflichten gegenüber Betroffenen geschaffen (vgl. dazu Nr. 5.1.1). Darüber hinaus wurden auf meine Anregung hin die Rechte der Bürger bei Auskunftsbegehren gestärkt, indem - statt der bisherigen Ermessensregelung - nunmehr grundsätzlich ein Anspruch auf Auskunft gegenüber dem Landesamt für Verfassungsschutz besteht (vgl. dazu Nr. 5.1.6).

Neben der Regelung der Wohnraumüberwachung hätte aber auch der Einsatz der sonstigen nachrichtendienstlichen Mittel zur Erhebung personenbezogener Daten an die Vorgaben des Bundesverfassungsgerichts angepasst werden müssen. Ich habe dabei insbesondere folgende Ergänzungen gefordert:

- Schaffung von Schutzvorschriften für den Kernbereich privater Lebensgestaltung

- Einführung einer grundsätzlichen Pflicht des Landesamts für Verfassungsschutz, Betroffene, in deren Grundrechte durch verdeckte Maßnahmen eingegriffen wurde, zu benachrichtigen.

Meine Forderungen wurden im Gesetz nur unzureichend umgesetzt (vgl. auch meine Ausführungen zum Abhören und Aufzeichnen des nicht-öffentlich gesprochenen Wortes unter Nr. 5.1.3 und zur Online-Durchsuchung unter Nr. 5.1.4). Es fehlt nicht nur an einer abschließenden gesetzlichen Aufzählung der zulässigen nachrichtendienstlichen Mittel des Verfassungsschutzes, sondern auch an einer umfassenden Regelung des Kernbereichsschutzes und der Benachrichtigungspflicht. Erheblich erweitert wurden aber die Eingriffsbefugnisse des Landesamts für Verfassungsschutz. Insbesondere folgende neue Befugnisse sind hervorzuheben:

- Befugnis, Auskünfte über Telekommunikationsverkehrsdaten einzuholen (vgl. dazu Nr. 5.1.2)
- Befugnis, das nicht-öffentlich gesprochene Wort außerhalb von Wohnungen abzuhören und aufzuzeichnen (vgl. Nr. 5.1.3)
- Befugnis zum verdeckten Zugriff auf informationstechnische Systeme („Online-Durchsuchung“, vgl. Nr. 5.1.4)
- Befugnis, eine heimliche Wohnungsdurchsuchung zur Vorbereitung der Telekommunikationsüberwachung, der Wohnraumüberwachung oder der Online-Durchsuchung durchzuführen (vgl. Nr. 5.1.5).

### 5.1.1 Wohnraumüberwachung („Großer Lauschangriff“)

Bereits nach der bis zum 31.07.2008 geltenden Fassung des Verfassungsschutzgesetzes war die Wohnraumüberwachung durch das Landesamt für Verfassungsschutz unter bestimmten Voraussetzungen zulässig (Art. 6 a BayVSG a.F.). Sie erlaubte dem Landesamt für Verfassungsschutz nicht nur die akustische, sondern auch die optische Überwachung auch der zu Wohnzwecken genutzten Räume. Aufgrund der Entscheidung des Bundesverfassungsgerichts zum „Großen Lauschangriff“ vom 03.03.2004 bestand erheblicher Änderungsbedarf, da die landesrechtliche Regelung an die vom Bundesverfassungsgericht zum Schutz des Kernbereichs der privaten Lebensgestaltung entwickelten Grundsätze angepasst werden musste. Mit der Anpassung wurden auch von mir erhobene datenschutzrechtliche Forderungen berücksichtigt:

- Bei den Straftaten, zu deren Abwehr der „Große Lauschangriff“ eingesetzt werden darf („Anlasstatenkatalog“), handelt es sich nahezu ausschließlich um besonders schwere Straftaten. Gemäß dem Urteil des Bundesverfassungsgerichts zum „Großen Lauschangriff“ ist dieser intensive Eingriff in das Grundrecht auf Unverletzlichkeit der Wohnung (Art. 13 Abs. 1 GG) nur bei einer besonderen Schwere der Straftat gerechtfertigt. Von einer solchen Schwere der Straftat ist nur auszugehen, wenn sie der Gesetzgeber mit einer höheren Höchststrafe als fünf Jahre Freiheitsstrafe bewehrt hat.

- Die zunächst vorgesehene Möglichkeit, die Wohnraumüberwachung auch bei einer gemeinen Gefahr für Sachen durchzuführen, wurde gestrichen.

Allerdings hätte ich es begrüßt, wenn auch die nachfolgenden Punkte berücksichtigt worden wären:

- Verzicht auf die nur automatische Aufzeichnung von Gesprächen. Dem Bundesverfassungsgericht zufolge (Urteil zum „Großen Lauschangriff“ vom 03.03.2004) kann es wegen der Unterbrechungspflicht bei Kernbereichsgesprächen notwendig sein, bei dem Abhören einer Privatwohnung auf eine nur automatische Aufzeichnung der abgehörten Gespräche zu verzichten, um jederzeit die Ermittlungsmaßnahme unterbrechen zu können.

- Schutz des Zeugnisverweigerungsrechts engster Familienangehöriger (vgl. § 52 StPO). Aus einer Wohnraumüberwachung gewonnene Erkenntnisse sollten nur verwertet werden dürfen, wenn dies unter Berücksichtigung der Bedeutung des zugrundeliegenden Vertrauensverhältnisses nicht außer Verhältnis zum Interesse an der Erforschung des Sachverhalts steht. Eine entsprechende Regelung hat der Bundesgesetzgeber bereits in § 100 c Abs. 6 Satz 2 StPO („Großer Lauschangriff“) vorgesehen.

- Ausweitung der Pflicht zur Benachrichtigung Betroffener. Nach dem Urteil des Bundesverfassungsgerichts vom 03.03.2004 besteht „eine Benachrichtigungspflicht … grundsätzlich auch gegenüber solchen Personen, die sich als Gast oder sonst zufällig in einer überwachten Wohnung aufgehalten haben und die in ihrem … Recht am gesprochenen Wort und in ihrem informationellen Selbstbestimmungsrecht betroffen sind“. Die im Gesetz enthaltene Beschränkung der Benachrichtigung auf zufällig mitbetroffene Personen, deren personenbezogene Daten auch verwendet wurden, erscheint im Hinblick auf die Ausführungen des Gerichts verfassungsrechtlich bedenklich.

Das Staatsministerium des Innern hat den Bayerischen Landtag darüber unterrichtet, dass das Landesamt für Verfassungsschutz im Jahr 2007 keine Wohnraumüberwachung durchgeführt hat. Zahlen für das Jahr 2008 liegen mir noch nicht vor.

### 5.1.2 Auskunft über Telekommunikationsverkehrsdaten

Das Landesamt für Verfassungsschutz kann Auskunft über Telekommunikationsverkehrsdaten von denjenigen verlangen, die geschäftsmäßig Telekommunikationsdienste erbringen, soweit dies zu seiner Aufgabenerfüllung erforderlich ist und tatsächliche Anhaltspunkte für eine schwerwiegende Gefahr für bestimmte Schutzgüter vorliegen. Zu diesen zählen z.B. die freiheitliche demokratische Grundordnung, die unbeeinträchtigte Amtsführung verfassungsmäßiger Organe des Bundes oder eines Landes oder ihrer Mitglieder und der Schutz vor innerstaatlichen Tätigkeiten ausländischer Geheimdienste (vgl. Art. 6 c Abs. 2 Satz 1 Nr. 4 BayVSG n.F.).

Das Bundesverfassungsgericht hat in seiner Eilentscheidung zur Vorratsdatenspeicherung vom 11.03.2008 festgestellt, dass in dem Verkehrsdatenabruf ein „schwerwiegender und nicht mehr rückgängig zu machender Eingriff in das Grundrecht aus Art. 10 Abs. 1 GG“ liege. „Ein solcher Datenabruf ermöglicht es, weitreichende Erkenntnisse über das Kommunikationsverhalten und die sozialen Kontakte des Betroffenen zu erlangen, ggf. sogar begrenzte Rückschlüsse auf die Gesprächsinhalte zu ziehen. Zudem weist ein Verkehrsdatenabruf eine erhebliche Streubreite auf, da er neben der Zielperson des Auskunftsersuchens notwendigerweise deren Kommunikationspartner erfasst, also vielfach Personen, die in keiner Beziehung zu dem Tatvorwurf stehen und den Eingriff durch ihr Verhalten nicht veranlasst haben.“

Wegen dieser hohen Eingriffsintensität habe ich gefordert, die Maßnahme nur zuzulassen, wenn auch die Telekommunikationsinhalte überwacht werden dürften, also bei der Gefahr der Planung oder Begehung schwerwiegender, enumerativ aufgezählter Straftaten. Dieser Forderung ist leider ebenso nicht entsprochen worden, wie meiner Forderung, den Verwendungszweck für die erhobenen Daten - wie bei der sog. Online-Durchsuchung - präzise gesetzlich zu regeln.

Wie berechtigt meine Forderung nach Einschränkung dieser Maßnahme war, zeigt die am 28.10.2008 ergangene Eilentscheidung des Bundesverfassungsgerichts. Auch das Gericht hält die o.g. Schutzgüter, deren Gefährdung den Abruf von Verkehrsdaten zulässt, für weit, offen, unscharf und konkretisierungsbedürftig. Zudem müsse die Gefahr für diese Schutzgüter nicht konkret sein. Das Bundesverfassungsgericht erachtet deshalb für die Zeit bis zum Urteil über die Verfassungsbeschwerde die Übermittlung von Telekommunikationsverkehrsdaten an die Verfassungsschutzbehörden des Bundes und der Länder nur dann für zulässig, wenn - wie von mir gefordert - auch die Telekommunikationsinhalte überwacht werden dürften.

### 5.1.3 Verdeckter Einsatz technischer Mittel zum Abhören und Aufzeichnen des nicht-öffentlich gesprochenen Wortes außerhalb von Wohnungen

Das Bayerische Verfassungsschutzgesetz sieht - nach entsprechender Ergänzung - für das Landesamt für Verfassungsschutz erstmals die Befugnis vor, das nicht-öffentlich gesprochene Wort durch den verdeckten Einsatz technischer Mittel außerhalb von

Wohnungen abzuhören und aufzuzeichnen. Auch wenn man eine solche Maßnahme unter engen Voraussetzungen als vertretbar ansieht, muss die gesetzliche Regelung den Anforderungen an den Schutz des Kernbereichs privater Lebensgestaltung und die Benachrichtigungspflicht genügen, die das Bundesverfassungsgericht in seinen Entscheidungen zum Großen Lauschangriff vom 03.03.2004 und zur Online-Durchsuchung vom 27.02.2008 aufgestellt hat. Unter diesem Gesichtspunkt erscheint die Regelung - worauf ich im Gesetzgebungsverfahren wiederholt hingewiesen habe - verfassungsrechtlich problematisch:

- Es fehlt ein zweistufiges Schutzkonzept für den Kernbereich privater Lebensgestaltung. Das Bundesverfassungsgericht fordert in seinem Urteil zur Online-Durchsuchung vom 27.02.2008, dass eine gesetzliche Regelung darauf hinwirken muss, dass die Erfassung kernbereichsrelevanter Daten soweit möglich unterbleibt (1. Stufe). Ergibt die Durchsicht (2. Stufe), dass kernbereichsrelevante Daten erhoben wurden, seien diese unverzüglich zu löschen. Eine Weitergabe oder Verwendung sei auszuschließen. Das Bayerische Verfassungsschutzgesetz sieht beim Abhören und Aufzeichnen des nicht-öffentlich gesprochenen Wortes einen Kernbereichsschutz in der Erhebungsphase nicht vor.

- Es fehlt - im Gegensatz zur Regelung des Bundesverfassungsschutzgesetzes, des Polizeiaufgabengesetzes und der Strafprozessordnung - eine Pflicht, die Betroffenen von der Maßnahme zu unterrichten, selbst für den Fall, dass die von ihnen erhobenen Daten verwendet wurden.

  Das Bundesverfassungsgericht führt in seiner Entscheidung zum Großen Lauschangriff zur Benachrichtigungspflicht Folgendes aus: „Die Benachrichtigungspflicht dient der Gewährleistung effektiven Schutzes der hier betroffenen Grundrechte. Demzufolge sind all diejenigen von der heimlichen Maßnahme zu unterrichten, in deren Grundrechte durch sie eingegriffen worden ist und denen somit Rechtschutzmöglichkeiten und Anhörungsrechte offenstehen müssen“.

### 5.1.4 Online-Durchsuchung

Die Anpassung des Bayerischen Verfassungsschutzgesetzes an die Vorgaben des Bundesverfassungsgerichts zum „Großen Lauschangriff“ wurde auch dazu benutzt, für das Landesamt für Verfassungsschutz erstmals eine Befugnis zur „Online-Durchsuchung“ (sog. verdeckte Online-Datenerhebung) zu schaffen. Das Bundesverfassungsgericht hat in seiner Entscheidung vom 27.02.2008 (vgl. dazu Nr. 4.1.2) hohe verfassungsrechtliche Anforderungen an die Zulässigkeit der Online-Durchsuchung gestellt. Sie sei nur zulässig bei tatsächlichen Anhaltspunkten für eine konkrete Gefahr für ein überragend wichtiges Rechtsgut. Eine solche Befugnis des Landesamts für Verfassungsschutz zur Abwehr konkreter Gefahren halte ich für systemwidrig:

Die Abwehr konkreter Gefahren ist typischerweise Aufgabe der Polizei und der Sicherheitsbehörden (vgl. Art. 6 Landesstraf- und Verordnungsgesetz). Das Landesamt für Verfassungsschutz hat hingegen als „Frühwarnsystem“ der Staatsregierung die Aufgabe, im Vorfeld konkreter Gefahren Entwicklungen und Bestrebungen zu beobachten. Hinzu kommt, dass auch für die Polizei eine Befugnis für Online-Durchsuchungen geschaffen worden ist (vgl. Art. 34 e PAG und Nr. 4.1.2). Es ist zu befürchten, dass eine solche parallele Zuständigkeit von Verfassungsschutz und Polizei ohne ausreichende Abgrenzung zu überlappenden und damit zusätzlichen Rechtseingriffen führt. Vor diesem Hintergrund hätte besser gänzlich auf die Befugnis zur Online-Durchsuchung für das Landesamt für Verfassungsschutz verzichtet werden sollen.

Unabhängig davon habe ich mich im Gesetzgebungsverfahren dafür eingesetzt, dass die Neuregelung die vom Bundesverfassungsgericht vorgegebenen engen Grenzen nicht überschreitet. So wurden meine datenschutzrechtlichen Forderungen zumindest zum Teil umgesetzt. Die Straftaten, zu deren Abwehr die Online-Durchsuchung zulässig ist („Anlasstatenkatalog“), wurden nahezu ausschließlich auf solche Straftatbestände beschränkt, die zum Schutz überragend wichtiger Rechtsgüter bestehen (vgl. dazu Nr. 4.1.2). Neben dem Schutz von Leib, Leben und Freiheit der Person fallen darunter nur Güter der Allgemeinheit, deren Bedrohung die Grundlagen oder den Bestand des Staates oder die Grundlagen der Existenz der Menschen berührt (existenzielle Bedrohungslage).

Ich hätte es begrüßt, wenn auch meine Forderungen zum Schutz des Vertrauensverhältnisses mit engsten Familienangehörigen (vgl. § 52 StPO) und zur Benachrichtigungspflicht Betroffener übernommen worden wären (vgl. dazu meine Ausführungen zur Wohnraumüberwachung unter Nr. 4.1.1).

### 5.1.5 Heimliche Wohnungsdurchsuchung

Die Gesetzesänderung enthält darüber hinaus - bundesweit einmalig - die Befugnis, zur Durchführung einer Wohnraumüberwachung, einer Beschränkung der Telekommunikation und einer Online-Durchsuchung die Wohnung des Betroffenen heimlich zu betreten und zu durchsuchen. Zur verfassungsrechtlichen Problematik verweise ich auf meine Ausführun-

gen unter Nr. 4.1.3 zur heimlichen Wohnungsdurchsuchung nach dem Polizeiaufgabengesetz.

Meiner Forderung, auf die Befugnis zur heimlichen Wohnungsdurchsuchung zu verzichten, wurde - trotz meiner massiven verfassungsrechtlichen Bedenken - leider nicht entsprochen.

### 5.1.6 Auskunftsanspruch über die beim Landesamt für Verfassungsschutz gespeicherten Informationen

Zur Notwendigkeit, dem Betroffenen gegenüber dem Landesamt für Verfassungsschutz einen grundsätzlichen Anspruch auf Auskunft über die zu seiner Person in Dateien oder Akten gespeicherten personenbezogenen Daten einzuräumen, habe ich in verfassungsrechtlicher und datenschutzrechtlicher Hinsicht in meinem letzten Tätigkeitsbericht (Nr. 5.2) Stellung genommen. Das Staatsministerium des Innern habe ich gebeten, im Rahmen der Novellierung des Verfassungsschutzgesetzes einen solchen Anspruch vorzusehen. Dem hat das Staatsministerium des Innern entsprochen.

Art. 11 Abs. 1 BayVSG n.F. sieht nun vor, dass das Landesamt für Verfassungsschutz dem Betroffenen auf Antrag kostenfrei Auskunft über die zu seiner Person in Dateien oder Akten gespeicherten Daten erteilen muss. Der Betroffene hat allerdings - wie bisher - ein „besonderes Interesse“ an der Auskunft darzulegen. Dies kann hingenommen werden. So hat das Bundesverwaltungsgericht in seinem Urteil zum Auskunftsersuchen eines Journalisten gegenüber dem Bundesnachrichtendienst vom 28.11.2007 entschieden, dass eine Verletzung des Grundrechts auf informationelle Selbstbestimmung nicht vorliegt, wenn der Auskunftsanspruch eingebettet ist in eine Abwägung zwischen dem Auskunftsinteresse und dem Geheimhaltungsbedürfnis.

## 5.2 Datenschutzrechtliche Prüfungen beim Verfassungsschutz

Das Gesetz zur Errichtung einer standardisierten zentralen Antiterrordatei von Polizeibehörden und Nachrichtendiensten von Bund und Länder (Antiterrordateigesetz - ATDG) ist am 31.12.2006 in Kraft getreten. Über die datenschutzrechtlichen Probleme einer solchen Datei hatte ich bereits in meinem letzten Tätigkeitsbericht (vgl. hierzu Nr. 5.4) berichtet. Ein Schwerpunkt meiner Prüfungen beim LfV waren deshalb Speicherungen in der Antiterrordatei (ATD). Neben den Speicherungen dort habe ich auch polizeiliche Speicherungen in der ATD überprüft (vgl. hierzu Nr. 4.5 - Polizeiliche Speicherungen in der Antiterrordatei).

Beim LfV habe ich festgestellt, dass die Speicherungen in der Mehrzahl gesetzeskonform vorgenommen wurden. Bei einigen Speicherungen habe ich das LfV aufgefordert, mir das Vorliegen der gesetzlichen Voraussetzungen für die Speicherungen im Einzelnen darzulegen oder die Speicherungen zu löschen. Bei anderen Speicherungen habe ich das LfV zur Löschung aufgefordert. Dies betraf - anders als bei der Polizei, wo ich überwiegend die Löschung der Speicherung von „Kontaktpersonen“ gefordert habe - die Speicherungen von „Gewaltbefürwortern“. Als solche können nach dem Gesetz Personen gespeichert werden, wenn tatsächliche Anhaltspunkte dafür vorliegen, dass sie rechtswidrig Gewalt als Mittel zur Durchsetzung international ausgerichteter politischer oder religiöser Belange anwenden oder eine solche Gewaltanwendung unterstützen, vorbereiten, befürworten oder durch ihre Tätigkeiten vorsätzlich hervorrufen. In zwei Fällen habe ich eine solche Gewaltbefürwortung nicht erkennen können.

Im Hinblick auf ein Urteil des Verwaltungsgerichts Köln habe ich die pauschale und unterschiedslose Speicherung einfacher Mitglieder einer Partei im Informationssystem IBA problematisiert. In diesem Urteil wurden Speicherungen zur Person eines Abgeordneten der „Linken“ durch das Bundesamt für Verfassungsschutz (BfV) nicht für verhältnismäßig angesehen. Die Ausführungen des Verwaltungsgerichts in diesem Urteil stützen wegen seiner Bezugnahme auf den Grundsatz der Verhältnismäßigkeit auch meine grundsätzlichen datenschutzrechtlichen Bedenken gegen die Speicherung von einfachen Mitgliedern solcher Beobachtungsobjekte (vgl. hierzu Nr. 8.3, 21. Tätigkeitsbericht).

Das Verwaltungsgericht hatte zunächst festgestellt, dass das BfV das Erfordernis einer Informationssammlung über den Kläger darauf gestützt hat, „dass der Kläger führender Funktionär zunächst der PDS, später „Linkspartei.PDS“ bzw. jetzt „Die Linke“ war und ist und die Partei Bestrebungen gegen die freiheitlich demokratische Grundordnung verfolge. Demgegenüber hat das BfV nicht geltend gemacht, dass der Kläger **selbst** ansonsten durch eigene schriftliche oder mündliche Äußerungen oder sonstige politische Aktivitäten derartige Bestrebungen verfolgt“. In der Folge kommt das Gericht zu dem Ergebnis, dass es hinsichtlich der Datenerhebung und -sammlung über den Kläger nicht ausreichend sei, sich weitestgehend darauf zu berufen, dass es sich bei ihm um einen herausgehobenen Funktionär der Linkspartei.PDS handele. Der Kläger sei „nicht Angehöriger einer der Linkspartei.PDS angehörenden linksextremistischen bzw. orthodox-kommunistischen Strömungen oder Flügel, noch ist er als Förderer entsprechender Bestrebungen hervorgetreten“. Nach alledem kommt die Kammer zu dem Ergebnis, dass bereits die Beobachtung des Klägers im Hinblick auf seine Funktion als Abgeordneter in der bisher erfolgten Form nicht verhältnismäßig ist.

Dies zeigt, dass dem Grundsatz der Verhältnismäßigkeit bei der Entscheidung über die Speicherung personenbezogener Daten in Dateien des Verfassungsschutzes besondere Bedeutung zukommt. Im konkreten Fall hatte dies die Rechtswidrigkeit der Sammlung personenbezogener Informationen über den in herausgehobener Funktion auch für die frühere PDS tätigen Kläger wegen des Fehlens individueller verfassungsfeindlicher Bestrebungen und Aktivitäten zur Folge. Das Fehlen dieser individuellen Merkmale muss auch Bedeutung für die Speicherung von einfachen Mitgliedern einer Partei haben. Im konkreten Fall habe ich das LfV um Löschung der Daten der von mir überprüften Mitglieder gebeten, soweit über sie keine weiteren relevanten Erkenntnisse vorliegen.

Hinsichtlich der Speicherung von Abgeordneten habe ich im Hinblick auf die noch ausstehende Berufungsentscheidung des Verwaltungsgerichts Nordrhein-Westfalen meine abschließende Meinungsbildung zurückgestellt.

Speicherungen von Personen im Zusammenhang mit der Beobachtung von Bestrebungen und Tätigkeiten der Organisierten Kriminalität waren ebenfalls Gegenstand meiner datenschutzrechtlichen Prüfungen. Meiner Forderung nach Löschung oder Fristverkürzung von Speicherungen in einzelnen Fällen ist das LfV nachgekommen.

Darüber hinaus habe ich auch Datenabfragen aus dem Dokumentenmanagementsystem DOMEA geprüft. Dort sollte bei personenbezogenen Suchanfragen ein vom Sachbearbeiter anzugebender Abfragegrund mit protokolliert werden, um eine spätere Nachvollziehbarkeit für datenschutzrechtliche Überprüfungen zu erleichtern.

Vernichtet wurden endlich die Bildaufnahmen von Versammlungsteilnehmern (vgl. hierzu Nr. 5.3, 22. Tätigkeitsbericht), bei denen ich die Voraussetzungen für die Erhebung und Speicherung durch das LfV nicht hatte erkennen können.

# 6 Justiz

Im Berichtszeitraum habe ich anlassunabhängig bei zwei Staatsanwaltschaften und einer Justizvollzugsanstalt vor Ort eine datenschutzrechtliche Prüfung durchgeführt. Ferner habe ich anhand entsprechender Protokollierungen Abrufe von Staatsanwaltschaften und Justizvollzugsanstalten aus der Zentralen Vollzugsdatei Bayern und Abrufe von bayerischen Notaren im Online-Abrufverfahren für das automatisierte Grundbuch auf ihre Zulässigkeit hin überprüft. Neben diesen anlassunabhängigen Prüfungen habe ich anlassbezogen aufgrund von Bürgereingaben auch Prüfungen konkreter Einzelfälle vorgenommen. Bei Gesetzentwürfen, Verwaltungsvorschriften im Rahmen der Einführung von Formblättern für die Praxis und beim Verwaltungsvollzug habe ich auf die Umsetzung datenschutzrechtlicher Anforderungen unter Berücksichtigung der Rechtsprechung des Bundesverfassungsgerichts hingewirkt.

Die nachfolgenden Darstellungen sind eine Auswahl meiner Feststellungen im Justizbereich.

## 6.1 Gesetzgebung

### 6.1.1 Datenschutz in der Dritten Säule der Europäischen Union

Auf Ebene der EU werden immer mehr Rechtsakte geschaffen, die zu Eingriffen in die Privatsphäre auch vieler unverdächtiger Bürger führen. Dazu zählen z.B. die Richtlinie zur Einführung der Vorratsdatenspeicherung und der Rahmenbeschluss über die Vereinfachung des Austauschs von Informationen und Erkenntnissen zwischen den Strafverfolgungsbehörden der Mitgliedstaaten vom 18.12.2006 (sog. Schwedische Initiative). Diese sieht vor, die polizeiliche und justizielle Zusammenarbeit in Strafsachen (sog. Dritte Säule) durch die Vereinfachung des Datenaustausches zu erleichtern. Die Mitgliedstaaten sind verpflichtet, diesen Rahmenbeschluss in nationales Recht umzusetzen (vgl. im Einzelnen Entschließung „Besserer Datenschutz bei der Umsetzung der „Schwedischen Initiative“ zur Vereinfachung des polizeilichen Datenaustausches zwischen den EU-Mitgliedstaaten geboten“ vom November 2008, Anlage Nr. 26). Darüber hinaus bestehen bilaterale Abkommen, die den Datenaustausch zwischen EU-Mitgliedstaaten und Drittstaaten vereinfachen sollen.

Der Ausbau der grenzüberschreitenden Datenübermittlung und der Aufbau zentraler Datenbestände greifen erheblich in das Grundrecht auf informationelle Selbstbestimmung ein. Ein EU-weiter hoher und einheitlicher Datenschutz, wie ihn die Datenschutzbeauftragten des Bundes und der Länder bereits im März 2006 gefordert haben (vgl. dazu Nr. 6.1.5, 22. Tätigkeitsbericht), besteht im Rahmen der polizeilichen und justiziellen Zusammenarbeit auch weiterhin nicht. Die Datenschutzbeauftragten des Bundes und der Länder warnen daher in ihrer Entschließung „Angemessener Datenschutz bei der polizeilichen und justiziellen Zusammenarbeit in der EU dringend erforderlich“ vom November 2008 (vgl. Anlage Nr. 25) vor dadurch verursachten Gefahren für jeden Einzelnen, die durch eine Verknüpfbarkeit der Datenbanken noch gesteigert werden.

Zwar hat die EU am 27.11.2008 einen Rahmenbeschluss zum Schutz personenbezogener Daten verabschiedet, die im Rahmen der polizeilichen und justiziellen Zusammenarbeit verarbeitet werden. Der Rahmenbeschluss ist aber nur auf die grenzüberschreitende Datenverarbeitung und nicht auch auf die

innerstaatliche Datenverarbeitung durch Polizei und Strafverfolgungsbehörden anwendbar. Dies wäre aber erforderlich, um einen einheitlichen Datenschutzstandard in den EU-Mitgliedstaaten zu gewährleisten. Darüber hinaus wurde die mit dem Rahmenbeschluss eröffnete Möglichkeit nicht genutzt, ein unabhängiges Datenschutzgremium einzurichten, das die Kommission, den Rat und das Europäische Parlament im Bereich der polizeilichen und justiziellen Zusammenarbeit berät.

### 6.1.2 Heimliche Online-Durchsuchung zur Strafverfolgung

Mit Beschluss vom 31.01.2007 hat der Bundesgerichtshof entschieden, dass die verdeckte repressive Online-Durchsuchung von informationstechnischen Systemen mangels einer Rechtsgrundlage in der Strafprozessordnung unzulässig ist. Diese Entscheidung begrüße ich. Von der Einführung einer solchen Rechtsgrundlage sollte im Hinblick auf die mit der Online-Durchsuchung verbundenen Grundrechtseingriffe abgesehen werden.

Bei dem verdeckten Zugriff auf informationstechnische Systeme geht es nicht nur um „Online-Durchsicht“ als einmalige Durchsuchung und Übertragung von Festplatteninhalten an die Strafverfolgungsbehörden, sondern auch um die anhaltende Überwachung, um das Ausspähen von Passworten und die Protokollierung aller elektronischen Aktivitäten. Auch sollen alle anderen Kommunikations- und Datenverarbeitungssysteme, wie lokale Netzwerke, Mobiltelefone, PDAs usw. in die heimliche Durchsuchung einbezogen werden. Dabei ist die Gefahr groß, dass von einer solchen Maßnahme auch unverdächtige Nutzerinnen und Nutzer dieser Systeme betroffen sein würden. Der unantastbare Kernbereich privater Lebensgestaltung lässt sich bei Online-Durchsuchungen auf der Stufe der Datenerhebung durch technische Mittel nicht schützen. Ein automatisierter Kernbereichsschutz ist nicht realisierbar. Die Erforderlichkeit der Online-Durchsuchung zur Strafverfolgung ist nicht dargetan. Die Eignung ist im Hinblick auf die vielfältigen Absicherungsmaßnahmen gegen das Eindringen sog. Spionagesoftware mehr als zweifelhaft. Sicher ist aber, dass die Online-Durchsuchung zu einer weiteren Einschränkung der Freiheit führen würde.

Bereits die 73. und 74. Konferenz der Datenschutzbeauftragten des Bundes und der Länder haben darauf hingewiesen, dass der Computer im täglichen Leben der meisten Menschen eine zentrale Bedeutung für die Aufbewahrung und Gestaltung privatester Informationen, wie Fotografien, Reiseberichte, Tagebuchaufzeichnungen, persönliche Briefe, Eindrücke, Vorstellungen und Gefühle hat. Die heimliche Online-Durchsuchung führt deshalb zu erheblichen Eingriffen in Grundrechte wie das informationelle Selbstbestimmungsrecht, die Unverletzlichkeit der Wohnung und das Telekommunikationsgeheimnis (siehe Anlagen Nr. 2 und Nr. 9).

Mit Urteil vom 27.02.2008 hat das Bundesverfassungsgericht die Vorschriften zur Online-Durchsuchung sowie zur Aufklärung des Internets im Verfassungsschutzgesetz Nordrhein-Westfalens für nichtig erklärt (Az. 1 BvR 370/07; 1 BvR 595/07). Besonders hervorzuheben ist in dieser Entscheidung die Feststellung des Gerichts, dass das allgemeine Persönlichkeitsrecht auch das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme umfasst. Damit hat es den Datenschutz weiter gestärkt und ihn an die Herausforderungen des elektronischen Zeitalters angepasst. Das Bundesverfassungsgericht hat außerdem verfassungsrechtliche Mindeststandards für den Fall aufgestellt, dass Online-Durchsuchungen gesetzlich zugelassen werden sollten (siehe hierzu auch Nr. 4.1.2). Die 75. Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat mit ihrer Entschließung „Vorgaben des Bundesverfassungsgerichts bei der Online-Durchsuchung beachten“ (siehe Anlage Nr. 18) die Gesetzgeber in Bund und Ländern aufgefordert, diese Eingriffsvoraussetzungen zu respektieren.

In Bayern ist inzwischen die verdeckte Online-Durchsuchung in das Polizeiaufgabengesetz und das Verfassungsschutzgesetz aufgenommen worden (siehe hierzu auch Nr. 4.1.2 und Nr. 5.1.4).

Die Bayerische Staatsregierung hat außerdem eine Initiative in den Bundesrat eingebracht (vgl. BR-Drs. 365/08), mit der durch einen § 100 k der Strafprozessordnung der verdeckte Zugriff auf informationstechnische Systeme mit Hilfe der Online-Durchsuchung zugelassen werden sollte. Dabei war auch vorgesehen, zur Durchführung einer solchen Maßnahme das heimliche Betreten und Durchsuchen von Wohnungen zu erlauben.

Eine solche neue strafprozessuale Ermittlungsmaßnahme wirft erhebliche verfassungsrechtliche Bedenken im Hinblick auf das Grundrecht der Unverletztlichkeit der Wohnung auf. Art. 13 GG erlaubt nur offene Wohnungsdurchsuchungen; heimliche Durchsuchungen halte ich ohne eine Änderung des Grundgesetzes nicht für zulässig. Die Bundesregierung hat daher aus gutem Grund bei der Änderung des Bundeskriminalamtsgesetzes von der Aufnahme einer Befugnis zur heimlichen Durchsuchung Abstand genommen.

Die Zusicherung gegenüber der Öffentlichkeit, dass die Online-Durchsuchung nur in wenigen Fällen schwerster Kriminalität in Betracht kommt, wird bereits durch die Vielzahl der über 50 Straftatbestände widerlegt, bei denen die Maßnahme zulässig sein soll. Die von Bayern genannten Straftatbestände

beschränken sich auch nicht auf schwerste Kriminalität wie z.B. terroristische Gewalttaten. Es besteht deshalb die Gefahr, dass Online-Durchsuchung in der Praxis als Standardmaßnahme auch in Fällen minder schwerer Kriminalität eingesetzt würde.

Der Bundesrat hat zwischenzeitlich die Einbringung des Gesetzentwurfs in den Bundestag abgelehnt.

### 6.1.3 Gesetz zur Neuregelung der Telekommunikationsüberwachung und anderer verdeckter Ermittlungsmaßnahmen sowie zur Umsetzung der Richtlinie 2006/24/EG

Am 01.01.2008 sind die Neuordnung der verdeckten Ermittlungsmaßnahmen in der Strafprozessordnung (insbesondere Eingriffsbefugnisse der Telekommunikationsüberwachung) sowie die Regelung der Vorratsspeicherung von Telekommunikationsverkehrsdaten in Kraft getreten. Ziel war eine Überarbeitung der Strafprozessordnung im Sinne einer harmonischen Gesamtregelung der strafprozessualen heimlichen Ermittlungsmaßnahmen (vgl. hierzu Nr. 6.1.3, 22. Tätigkeitsbericht). Bei den in Kraft getretenen Regelungen besteht aber in wesentlichen Punkten noch erheblicher Verbesserungsbedarf:

- Der Umfang der Straftaten, die Voraussetzung für die Anordnung einer Telekommunikationsüberwachung sind, wurde nicht im Hinblick auf Art und Schwere der Straftaten begrenzt. Vielmehr wurden zusätzliche Straftaten aufgenommen.

- Der Schutz des Kernbereichs privater Lebensgestaltung genügt nicht den Vorgaben des Bundesverfassungsgerichts. Die Neuregelung nimmt in Kauf, dass regelmäßig auch kernbereichsrelevante Informationen erfasst werden, für die grundsätzlich ein Erhebungsverbot gelten sollte.

- Für die Kommunikation mit Berufsgeheimnisträgerinnen und Berufsgeheimnisträgern muss ein absolutes Erhebungs- und Verwertungsverbot geschaffen werden, das dem jeweiligen Zeugnisverweigerungsrecht entspricht (vgl. Entschließung der 73. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 08./09.03.2007, Anlage Nr. 4). Für Angehörige ist zum Schutz der besonderen verwandtschaftlichen Vertrauensverhältnisse ein Erhebungs- und Verwertungsverbot für die Fälle vorzusehen, in denen das öffentliche Interesse an der Strafverfolgung nicht überwiegt.

- Eine ausdrückliche Regelung, dass Daten, die aufgrund von Eilanordnungen durch die Staatsanwaltschaft erhoben wurden, dann nicht verwertbar sind, wenn die Anordnung nicht richterlich bestätigt wird, ist zum Schutz der Grundrechte der Bürger und zur Schaffung von Rechtssicherheit geboten.

- Die Benachrichtigungspflichten sind nun in einer Vorschrift für alle verdeckten Ermittlungsmaßnahmen zusammengefasst. Eine Benachrichtigung kann allerdings dann unterbleiben, wenn eine Person von der Maßnahme nur unerheblich betroffen wurde und anzunehmen ist, dass sie kein Interesse an einer Benachrichtigung hat. Den Verfolgungsbehörden wird mit der Neuregelung sogar die Möglichkeit gegeben, endgültig von einer Benachrichtigung abzusehen, wenn die Voraussetzungen für eine Benachrichtigung mit an Sicherheit grenzender Wahrscheinlichkeit auch in Zukunft nicht eintreten werden.

- Durch die Vorratsspeicherung von Telekommunikationsverkehrsdaten für sechs Monate wird, worauf die Datenschutzbeauftragten des Bundes und der Länder bereits in ihrer Entschließung vom 08.06.2007 hingewiesen haben (vgl. Anlage Nr. 7), tief in die Privatsphäre und das Kommunikationsverhalten der gesamten Bevölkerung eingegriffen und dieses pauschal und anlasslos erfasst. Auch eine Erhebung von Standortdaten in Echtzeit ist zulässig. Der Erhebungs- und Verwendungszweck für die auf Vorrat gespeicherten Daten wurde über die europarechtlichen Vorgaben hinaus auch auf die Verfolgung mittels Telekommunikation begangener leichter Straftaten, die Gefahrenabwehr und sogar auf die Aufgaben der Nachrichtendienste erstreckt. Auch das Bundesverfassungsgericht hat in seiner Eilentscheidung zur Vorratsdatenspeicherung erhebliche Bedenken gegen diese Regelungen geäußert (s. hierzu auch Nr. 6.1.5).

### 6.1.4 Gutachten des Max-Planck-Instituts zur „Rechtswirklichkeit der Auskunftserteilung über Telekommunikationsverbindungsdaten nach §§ 100 g, 100 h StPO

Der Bundestag hatte am 21.10.2004 mit einem Entschließungsantrag die Bundesregierung aufgefordert, ihm bis zum 30.06.2007 einen Erfahrungsbericht über die praktische Umsetzung der §§ 100 g, 100 h StPO (alte Fassung) vorzulegen. Dazu hat das Max-Planck-Institut für ausländisches und internationales Strafrecht in Freiburg im Auftrag des Bundesministeriums der Justiz die Nutzung von Telekommunikationsverkehrsdaten für Zwecke der Strafverfolgung evaluiert. Das Bundesministerium der Justiz hat die Studie erst im Februar 2008 und somit nach Abschluss des Gesetzgebungsverfahrens zur „Neuregelung der Telekommunikationsüberwachung und anderer verdeckter

Ermittlungsmaßnahmen sowie zur Umsetzung der Richtlinie zur Vorratsdatenspeicherung“ veröffentlicht. Das Gutachten liefert Erkenntnisse, deren Berücksichtigung bereits bei der Neufassung des § 100 g StPO durch das Gesetz vom 21.12.2007 erforderlich gewesen wäre (vgl. hierzu Nr. 6.1.3, 22. Tätigkeitsbericht).

Das Gutachten geht zu Recht davon aus, dass Verkehrsdaten ein hohes Überwachungspotential in sich tragen und besser als andere Daten dazu geeignet sind, soziale Netzwerke nachzuweisen, Beziehungen zu identifizieren und Informationen über Individuen zu generieren. Auch die quantitative Bedeutung der Verkehrsdatenabfrage ist nach den Feststellungen der Studie erheblich. So lag die Zahl der Verkehrsdatenabfragen im Jahr 2005 bereits bei etwa 40.000 (ohne Abfragen zu dynamischen IP-Adressen). Schon von 2002 (10.200) bis 2004 (22.600) war sie stark und kontinuierlich angestiegen. Die Zahl der Beschlüsse, die eine Abfrage zu einer IMEI-Nummer (elektronische Gerätekennung) beinhalten, stieg in diesem Zeitraum etwa um das Vierfache. Die angeordneten Zielwahlsuchen verdreifachten sich. Etwa 70 % der unmittelbar betroffenen und identifizierten Anschlussinhaber waren Nichtbeschuldigte.

Vor diesem Hintergrund fordern die Datenschutzbeauftragten des Bundes und der Länder den Gesetzgeber sowie die Strafverfolgungsbehörden und Gerichte auf, aus den Erkenntnissen des Gutachtens die erforderlichen Konsequenzen zu ziehen (siehe Anlage Nr. 20):

- Die Verkehrsdatenabfrage erfasst ein weites Spektrum von Anlassstraftaten. Insbesondere im Hinblick auf die inzwischen eingeführte Vorratsdatenspeicherung sollte die Straftatenschwelle auf schwere Straftaten angehoben werden.

- Die Dauer der Maßnahme lag schwerpunktmäßig beim gesetzlichen Maximum von drei Monaten. Eine gesetzliche Befristung auf zwei Monate dürfte nach dem Gutachten die praktischen Bedürfnisse der Strafverfolgungsbehörden abdecken.

- Bei den Begründungen gerichtlicher Anordnungen fällt insbesondere die lediglich formelhafte Wiedergabe des Gesetzestextes sowie die häufig wörtliche Übernahme der staatsanwaltschaftlichen Anträge auf. Um die Begründungsqualität zu verbessern, sollten (nach dem Vorbild der Regelungen für die akustische Wohnraumüberwachung) auch für die Verkehrsdatenabfrage qualifizierte Begründungspflichten in der Strafprozessordnung vorgesehen werden. Auch sollten die Rechtsfolgen für erhebliche Verstöße gegen die Begründungsanforderungen gesetzlich geregelt werden (z.B. Beweisverwertungsverbote).

- Das Gutachten enthält Hinweise darauf, dass der Verhältnismäßigkeitsgrundsatz und die gesetzlichen Subsidiaritätsklauseln in der Praxis nicht hinreichend beachtet werden. In den Begründungen von Polizei, Staatsanwaltschaft und Gericht, weshalb keine anderen Maßnahmen alternativ in Betracht kommen, wurde häufig ohne weitere Ausführungen lediglich der Gesetzeswortlaut wiedergegeben. Auf die Prüfung von Subsidiarität und Angemessenheit der Maßnahme ist in der Praxis daher besonderes Augenmerk zu richten.

- Der Richtervorbehalt erfüllt seine Funktion nicht in ausreichendem Maße. Als ein Grund hierfür wird auf die Arbeitsbelastung der Ermittlungsrichter und deren Prioritätensetzung verwiesen. Es ist daher in der Praxis darauf hinzuwirken, dass der Richtervorbehalt - nicht zuletzt durch ausreichende personelle Ressourcen bei den Ermittlungsrichtern - seine grundrechtssichernde Funktion effizient erfüllen kann.

- Bei den Telekommunikationsunternehmen besteht Unsicherheit, inwieweit sie zur Herausgabe der Verbindungsdaten verpflichtet sind bzw. ihnen eine eigene Prüfungskompetenz zusteht, wenn eine staatsanwaltschaftliche Eilanordnung nicht innerhalb der gesetzlichen Frist richterlich bestätigt wird. Zur Vermeidung von Rechtsunsicherheit sowie zur Stärkung des Richtervorbehalts sollte in den Fällen staatsanwaltschaftlicher Eilanordnung die Verwertbarkeit der erlangten Daten davon abhängig gemacht werden, dass ein Gericht rückwirkend die formelle und materielle Rechtmäßigkeit der Maßnahme feststellt.

- In 87 % der Fälle konnte den Akten kein Hinweis auf die Benachrichtigung der Betroffenen entnommen werden. Die Strafverfolgungsbehörden müssen daher angehalten werden, den gesetzlich festgeschriebenen Benachrichtigungspflichten nachzukommen.

- Nur in 3 % der ausgewerteten Verfahren konnte den Akten entnommen werden, dass die Verkehrsdaten nach Abschluss des Verfahrens vernichtet wurden. Auch die Experteninterviews ergaben, dass die Vernichtung der Daten offensichtlich nicht die Regel ist. Es ist daher in der Praxis darauf hinzuwirken, dass die gesetzliche Löschungs- und Dokumentationspflicht eingehalten wird.

- Im Hinblick auf die Vorratsdatenspeicherung bemerkenswert ist die Feststellung der Studie,

dass im Untersuchungszeitraum (also noch vor Einführung der sechsmonatigen Speicherungspflicht) nur etwa 2 % der Abfragen ins Leere gingen, weil die Verkehrsdaten bei den TK-Unternehmen bereits gelöscht waren. Diese Zahl bestätigt die erheblichen Zweifel am tatsächlichen Nutzen der Vorratsdatenspeicherung für die Strafverfolgung.

Eine Fortführung der wissenschaftlichen Evaluation der Verkehrsdatenabfrage unter den neuen rechtlichen Rahmenbedingungen ist - auch aufgrund der Weiterentwicklung der Technik - unerlässlich.

### 6.1.5 Eilanordnung des Bundesverfassungsgerichts zur Vorratsdatenspeicherung

Durch das Gesetz zur Neuregelung der Telekommunikationsüberwachung und anderer verdeckter Ermittlungsmaßnahmen sowie zur Umsetzung der Richtlinie 2006/24/EG, das am 01.01.2008 in Kraft getreten ist, wurde die EU-Richtlinie zur Vorratsdatenspeicherung in deutsches Recht umgesetzt. Die Anbieter von Internetzugangsdiensten, Diensten der elektronischen Post oder Internettelefondiensten haben die sie treffenden Anordnungen spätestens ab dem 01.01.2009 zu erfüllen. Die Speicherdauer für Telekommunikationsverkehrsdaten wurde auf die europarechtlich verpflichtende Mindestfrist von sechs Monaten festgesetzt. Nach Art. 1 Abs. 1 der Richtlinie sollen damit die Vorschriften der Mitgliedstaaten über die Vorratsspeicherung „harmonisiert werden, um sicherzustellen, dass die Daten zum Zwecke der Ermittlung, Feststellung und Verfolgung von „schweren“ Straftaten, wie sie von jedem Mitgliedstaat in seinem nationalen Recht bestimmt werden, zur Verfügung stehen“ (vgl. hierzu auch Nr. 6.1.3).

Entgegen diesem ausdrücklichen Wortlaut der Richtlinie hat der deutsche Gesetzgeber die Möglichkeit der Erhebung dieser Vorratsdaten zu Strafverfolgungszwecken in § 100 g StPO erweitert. Sie ist nach der gesetzlichen Regelung nicht auf die Ermittlung, Aufdeckung und Verfolgung schwerer Straftaten beschränkt, sondern erfasst auch Straftaten von nur „erheblicher Bedeutung“ und solche, die mittels Telekommunikation begangen worden sind. Diese Ausweitung ist im Hinblick auf den damit verbundenen Eingriff in die Grundrechte der Telekommunikationsteilnehmer problematisch und steht im Widerspruch zu der europarechtlich vorgeschriebenen Beschränkung auf schwere Straftaten.

Gespeichert werden aufgrund der Vorratsdatenspeicherung Telekommunikationsverkehrsdaten, aber keine Telekommunikationsinhalte. Zu den Telekommunikationsverkehrsdaten zählen z.B. Rufnummern des anrufenden oder angerufenen Anschlusses, Datum, Uhrzeit und Dauer der Verbindung. Darüber hinaus wird bei der Mobilfunktelefonie der Standort (angewählte Funkzelle) bei Beginn der Mobilfunkverbindung gespeichert. Dadurch wird die Erstellung von Bewegungsbildern möglich.

Das Bundesverfassungsgericht hat einem Eilantrag zur Vorratsdatenspeicherung teilweise stattgegeben und die Regelungen zur Verwendung der auf Vorrat gespeicherten Daten zu Strafverfolgungszwecken eingeschränkt (Eilentscheidung vom 11.03.2008, Az. 1 BvR 256/08). Über das Hauptsacheverfahren wird später entschieden werden. Das Bundesverfassungsgericht hat zwar nicht die Speicherung der Verkehrsdaten bis zur Entscheidung in der Hauptsache ausgesetzt, es bleibt insoweit bei der gesetzlichen Verpflichtung. Es hat aber die Verwendung der gespeicherten Daten zum Zweck der Strafverfolgung bis zur Entscheidung in der Hauptsache modifiziert: Die von den Telekommunikationsdiensteanbietern zu speichernden Verkehrsdaten sind nur dann an die Strafverfolgungsbehörden zu übermitteln, wenn Gegenstand des Ermittlungsverfahrens eine schwere Straftat i.S.v. § 100 a Abs. 2 StPO ist, die auch im Einzelfall schwer wiegt, der Verdacht durch bestimmte Tatsachen begründet ist und die Erforschung des Sachverhalts auf andere Weise wesentlich erschwert oder aussichtslos wäre. In den übrigen Fällen ist von einer Übermittlung der Daten einstweilen abzusehen. Zugleich wurde der Bundesregierung aufgegeben, dem Bundesverfassungsgericht bis zum 01.09.2008 über die praktischen Auswirkungen der Datenspeicherungen und der vorliegenden einstweiligen Anordnung zu berichten.

Im Rahmen seiner Abwägung hat das Bundesverfassungsgericht deutlich gemacht, dass der Verkehrsdatenabruf einen schwerwiegenden und nicht mehr rückgängig zu machenden Eingriff in das Fernmeldegeheimnis aus Art. 10 Grundgesetz darstellt. Es hat darüber hinaus betont, dass bereits durch die sechs Monate andauernde Möglichkeit des Zugriffs auf sämtliche durch eine Inanspruchnahme von Telekommunikationsdiensten entstandenen Verkehrsdaten eine erhebliche Gefährdung des in dem Grundrecht des Fernmeldegeheimnisses verankerten Persönlichkeitsschutzes zu sehen ist. Diese durch die anlasslose Speicherung hervorgerufene Gefährdung trifft annähernd jeden Bürger bei jeder Nutzung von Telekommunikationsanlagen. Darauf hatte auch die Konferenz der Datenschutzbeauftragten des Bundes und der Länder in ihren Entschließungen vom 26./27.10.2006 (Anlage Nr. 18 meines 22. TB) und vom 08./09.03.2007 hingewiesen (Anlage Nr. 4).

Das Bundesverfassungsgericht hat mit dieser Entscheidung einen weiteren wichtigen Meilenstein für den Datenschutz gesetzt. Die Entscheidung lässt auch für das noch ausstehende Hauptsacheverfahren hoffen, dass das Bundesverfassungsgericht die Vorratsdatenspeicherung zumindest erheblich einschränken wird.

### 6.1.6 Gesetz über den Vollzug der Freiheitsstrafe, der Jugendstrafe und der Sicherungsverwahrung (Bayerisches Strafvollzugsgesetz)

Aufgrund der Föderalismusreform ist die Gesetzgebungskompetenz für den Strafvollzug auf die Bundesländer übergegangen (vgl. 22. Tätigkeitsbericht Nr. 6.4). In Bayern ist am 01.01.2008 das bayerische Gesetz über den Vollzug der Freiheitsstrafe, der Jugendstrafe und der Sicherungsverwahrung in Kraft getreten. Ich habe zum Entwurf dieses Gesetzes insbesondere darauf hingewiesen, dass die Aufbewahrung der von Gefangenen gefertigten erkennungsdienstlichen Unterlagen einschließlich der Lichtbilder weit über die Dauer der Strafhaft hinaus bis zum Ablauf der für die sonstigen über sie gespeicherten personenbezogenen Daten geltenden Aufbewahrungsfrist unverhältnismäßig ist. Die im Strafvollzugsgesetz des Bundes für die Gefangenen vorgesehene Möglichkeit, nach der Entlassung aus dem Vollzug die Vernichtung erkennungsdienstlicher Unterlagen zu verlangen, hätte aus meiner Sicht beibehalten und auf die Vernichtung von Lichtbildern ausgedehnt werden sollen.

Bei der Neuregelung des Strafvollzugs hätte außerdem die Chance ergriffen werden sollen, den Schutz besonderer Daten stärker zu betonen. Nach dem Bayerischen Strafvollzugsgesetz (Art. 200 Abs. 2) haben sich die in § 203 Abs. 1 Nrn. 2 und 5 des Strafgesetzbuchs genannten Personen, nämlich Berufspsychologen und Sozialarbeiter, gegenüber dem Anstaltsleiter schon immer dann zu offenbaren, wenn und soweit dies für die Aufgabenerfüllung der Vollzugsbehörde erforderlich ist. Dies bedeutet, dass z.B. Erkenntnisse aus der psychologischen Betreuung unmittelbare Auswirkungen auf Vollzugsentscheidungen haben können. Eine Befugnisregelung ohne Offenbarungsverpflichtung wäre aus meiner Sicht ausreichend gewesen. Zumindest sollte den Psychologen und Sozialarbeitern eine Abwägungsbefugnis eingeräumt werden, ob Zwecke des Vollzugs die jeweils konkrete Durchbrechung ihrer Schweigepflicht rechtfertigen.

Änderungsbedarf habe ich auch gesehen im Hinblick auf die Regelung zur Überwachung von Besuchen, insbesondere der Dauer der Aufbewahrung entsprechender Videoaufzeichnungen sowie die Überwachung des Schriftwechsels, die ich nur in begründeten Einzelfällen als zulässig erachte. Zum Schutz der in Gefangenenpersonalakten und Dateien enthaltenen sensiblen Daten habe ich eine Protokollierung und Dokumentation auch des lesenden Zugriffs auf diese Unterlagen gefordert, der leider nahezu uneingeschränkt möglich ist. Zu den Löschungsfristen für Gefangenenpersonalakten habe ich gefordert, dass - jedenfalls in der Begründung des Gesetzes - aufgenommen wird, dass es sich insoweit um Höchstfristen und nicht um Mindestfristen handelt. Die Notwendigkeit einer Prüfung, ob eine Aussonderung vorher möglich ist, sollte dadurch verdeutlicht werden.

Ich werde die praktische Handhabung der Regelungen des Gesetzes einer fortlaufenden datenschutzrechtlichen Prüfung unterziehen.

### 6.1.7 Grundrechtseingriffe im Maßregelvollzug ohne Rechtsgrundlage

Anlässlich des zwischenzeitlich in Kraft getretenen Bayerischen Strafvollzugsgesetzes, das aufgrund der Föderalismusreform notwendig geworden war, habe ich das zuständige Staatsministerium für Arbeit und Sozialordnung, Familie und Frauen bereits am 22.03.2007 darauf hingewiesen, dass Eingriffe in das Recht auf informationelle Selbstbestimmung auch im Rahmen des Maßregelvollzugs einer ausreichend bestimmten gesetzlichen Grundlage bedürfen. Die bestehenden Regelungen im Unterbringungsgesetz (UnterbrG) erfüllen diese Voraussetzungen nicht.

Das Bundesverfassungsgericht hat bereits in seiner Entscheidung vom 14.03.1972 (Az. 2 BvR 41/71) ausgeführt, dass in Art. 1 Abs. 3 GG die Grundrechte für Gesetzgebung, vollziehende Gewalt und Rechtsprechung für unmittelbar verbindlich erklärt werden. Dieser umfassenden Bindung der staatlichen Gewalt widerspreche es, wenn im Strafvollzug die Grundrechte beliebig oder nach Ermessen eingeschränkt werden könnten. Eine Einschränkung komme nur dann in Betracht, wenn sie zur Erreichung eines von der Werteordnung des Grundgesetzes gedeckten gemeinschaftsbezogenen Zwecks unerlässlich ist und in den dafür verfassungsrechtlich vorgesehenen Formen geschieht. Die Grundrechte von Strafgefangenen können also nur durch oder aufgrund eines Gesetzes eingeschränkt werden. Auch in seiner Entscheidung vom 31.05.2006 zur verfassungsrechtlichen Notwendigkeit einer gesetzlichen Regelung für Maßnahmen im Jugendstrafvollzug, die in Grundrechte des Gefangenen eingreifen, hat das Bundesverfassungsgericht festgestellt, dass solche Eingriffe, die über den Freiheitsentzug als solchen hinausgehen, unabhängig von den guten oder sogar zwingenden sachlichen Gründen, die für sie sprechen mögen, einer eigenen gesetzlichen Grundlage bedürfen, die die Eingriffsvoraussetzungen in hinreichend bestimmter Weise normiert. Für Maßnahmen, die in Grundrechte des Gefangenen eingreifen, ist deshalb auch im Jugendstrafvollzug eine gesetzliche Grundlage erforderlich.

Diese Ausführungen des Bundesverfassungsgerichts zur Notwendigkeit einer gesetzlichen Regelung für Eingriffe in Grundrechte Gefangener sind auf im Maßregelvollzug Untergebrachte ebenfalls anwendbar. Auch hier handelt es sich um Personen, denen aufgrund richterlicher Entscheidung die Freiheit entzogen wurde. Das Bayerische Unterbringungsgesetz (vgl. Art. 28, 12 - 21 UnterbrG) und das Bayeri-

sche Strafvollzugsgesetz (Art. 208 BayStVollzG i.V.m. §§ 136 - 138 StVollzG) enthalten hierfür keine ausreichenden Eingriffsgrundlagen. Es fehlen beispielsweise Regelungen zur Durchsuchung von Patientenzimmern, für erkennungsdienstliche Behandlungen und Videoüberwachungen von Krankenzimmern, welche, wie mir aus meiner Prüfung bei einem Bezirkskrankenhaus bekannt ist, durchgeführt werden (vgl. hierzu Nr. 6.4.2, 22. Tätigkeitsbericht).

Das zuständige Staatsministerium hat mir auf entsprechende Vorhalte mitgeteilt, dass der Ministerrat in seiner Sitzung am 20.03.2007 beschlossen habe, es mit der Erarbeitung entsprechender landesrechtlicher Vorschriften für den Maßregelvollzug und anschließender Vorlage an den Ministerrat zur Beschlussfassung zu beauftragen. In diesem Zusammenhang sei beabsichtigt, auch die von mir angesprochenen Problempunkte zu regeln. Es sei geplant, die entsprechenden Regelungen für den Maßregelvollzug in ein reformiertes Unterbringungsgesetz zu integrieren.

Im Hinblick auf den bisherigen Zeitablauf habe ich mich mit dem Ziel einer zügigen Umsetzung des Ministerratsbeschlusses an die zuständige Staatsministerin gewandt. Angesichts der massiven Grundrechtseingriffe im Rahmen des Maßregelvollzugs halte ich es für dringend erforderlich, ohne zeitliche Verzögerung endlich eine normenklare und verhältnismäßige Rechtsgrundlage für die Gestaltung des Maßregelvollzugs zu schaffen.

### 6.1.8 Entwurf eines Gesetzes zur Aufbewahrung des Schriftguts der Justiz

In meinem 22. Tätigkeitsbericht (Nr. 6.1.6) hatte ich berichtet, dass mir das Justizministerium des Landes Nordrhein-Westfalen einen ersten Entwurf für ein Aktenaufbewahrungsgesetz zugeleitet hat, der unter Federführung einer durch die Justizministerkonferenz eingesetzten länderoffenen Arbeitsgruppe erarbeitet worden war.

Im April 2008 hat mir das Staatsministerium der Justiz und für Verbraucherschutz einen bayerischen Entwurf zur gesetzlichen Regelung der Aufbewahrung von Schriftgut zur Stellungnahme übersandt. Der Entwurf lehnt sich zum Teil an das Schriftgutaufbewahrungsgesetz des Bundes, das am 01.04.2006 in Kraft getreten ist, an. In meiner Stellungnahme dazu habe ich darauf hingewiesen, dass ich es aus Gründen der Normenbestimmtheit und Normenklarheit für vorzugswürdig hielte, im Gesetz selbst klarzustellen, dass die in der ergänzenden Rechtsverordnung festgelegten Fristen nicht lediglich Mindest- sondern Höchstfristen sind. Außerdem habe ich angeregt, dass in das Gesetz zur Aktenaufbewahrung die Verpflichtung zur Aufnahme von zusätzlichen Prüffristen, unabhängig von bereits bestehenden bundesgesetzlichen Prüffristen, soweit aus Gründen der Verhältnismäßigkeit geboten, aufgenommen wird. Darüber hinaus halte ich eine Überprüfung der vorgesehenen Aufbewahrungsfristen im Hinblick auf den Erforderlichkeitsgrundsatz mit dem Ziel einer Verkürzung für notwendig.

Das Staatsministerium hat meinen Vorschlägen leider nicht Rechnung getragen.

### 6.1.9 Bundesratsinitiative Bayerns zur Stärkung der Aussagekraft von Führungszeugnissen

Bayern hat am 15.02.2008 im Bundesrat eine Initiative eingebracht, um Kinder und Jugendliche durch aussagekräftigere Führungszeugnisse besser vor Sexualstraftätern zu schützen. Danach sollen Verurteilungen wegen des Erwerbs oder des Besitzes kinderpornografischer Schriften, wegen Verletzung der Fürsorge- oder Erziehungspflicht oder wegen der Misshandlung von Schutzbefohlenen künftig unabhängig von der Strafe zwingend in das Führungszeugnis aufgenommen werden.

Zur Begründung wird ausgeführt, dass ein privater Arbeitgeber in einem von dem Betroffenen vorzulegenden Führungszeugnis bzw. ein öffentlicher Arbeitgeber im Rahmen eines Behördenführungszeugnisses von derartigen Verurteilungen Kenntnis erlangen müsse, um etwaige Gefährdungen von Personen im beruflichen Umfeld des Betroffenen vermeiden zu können. Bislang können allein die obersten Landesbehörden, z.B. die Kultusministerien, bei der Entscheidung über die Einstellung aufgrund einer unbeschränkten Auskunft nach § 41 Abs. 1 Nr. 2 Bundeszentralregistergesetz (BZRG) auch solche Verurteilungen berücksichtigen.

Ich habe gegenüber dem Staatsministerium der Justiz und für Verbraucherschutz verfassungsrechtliche Bedenken gegen diese Initiative geäußert. Durch eine solche gesetzliche Regelung würde der Resozialisierungsgedanke des BZRG stark aufgeweicht. Es wären immer mehr Straftaten auch unterhalb einer besonderen Erheblichkeitsschwelle in ein Führungszeugnis einzutragen. Ich habe insoweit erhebliche Zweifel an der Verhältnismäßigkeit einer solchen Regelung und der Vereinbarkeit mit dem verfassungsrechtlich verankerten Grundsatz der Resozialisierung. Dies insbesondere im Hinblick darauf, dass Straftaten gegen die sexuelle Selbstbestimmung nicht bei jeder Art von Arbeitnehmerinnen und Arbeitnehmern Bedeutung zukommt, sondern lediglich dann, wenn ein Bezug zur konkreten Tätigkeit gegeben ist. Bei allen Änderungen des BZRG ist ein gerechter Ausgleich zu schaffen zwischen der Schutzfunktion des Registers einerseits und dem Ziel der Resozialisierung der Straffälligen andererseits. Ich halte daher eine Regelung für ein sog. erweitertes Führungszeugnis für besondere Berufsgruppen für vorzugswürdig. Die

Bundesregierung hat einen Gesetzentwurf auf den Weg gebracht, der in diese Richtung geht.

### 6.1.10 Unterstützungspflicht öffentlicher Stellen

Nach dem Bayerischen Datenschutzgesetz sind mir alle zur Erfüllung meiner Aufgaben notwendigen Auskünfte zu geben und auf Anforderung alle Unterlagen über die Erhebung, Verarbeitung oder Nutzung personenbezogener Daten zur Einsicht vorzulegen. Die Staatskanzlei und die Staatsministerien haben mich außerdem rechtzeitig über Entwürfe von Rechts- und Verwaltungsvorschriften des Freistaates Bayern sowie über Planungen bedeutender Automationsvorhaben, sofern sie die Erhebung, Verarbeitung oder Nutzung personenbezogener Daten betreffen, zu unterrichten.

Dieser gesetzlichen Regelung trägt auch die Geschäftsordnung der Bayerischen Staatsregierung Rechnung: Bevor ein Staatsministerium der Staatsregierung eine Vorlage zur Beschlussfassung unterbreitet, gibt es der Staatskanzlei und den Staatsministerien Gelegenheit, hierzu innerhalb einer angemessenen Frist Stellung zu nehmen. Ausnahmen sind nur bei besonderer Dringlichkeit zulässig. Dies gilt entsprechend für die Beteiligung des Landesbeauftragten für den Datenschutz.

Im Berichtszeitraum gab es bedauerlicherweise Vorgänge, bei denen ich mir eine - rechtzeitige - Beteiligung meiner Behörde gewünscht hätte oder eine zureichende Stellungnahme auf meine Anfragen unterblieben ist. Dies gilt beispielsweise für die Bundesratsinitiativen Bayerns zur Änderung des Bundeszentralregistergesetzes (siehe auch Nr. 6.1.9) und zur Ergänzung der Strafprozessordnung um eine Rechtsgrundlage für die sog. heimliche Online-Durchsuchung (siehe auch Nr. 6.1.2), von der ich erstmals durch die Presse Kenntnis erlangt habe. Anlässlich einer datenschutzrechtlichen Prüfung, die ich bei einer Staatsanwaltschaft durchgeführt habe, musste ich trotz wiederholter Erinnerungen fast ein Jahr auf eine Antwort zu meinem Prüfbericht warten. Erst nach Einschaltung des Amtschefs des Staatsministeriums der Justiz und für Verbraucherschutz ist eine Stellungnahme erfolgt. Eine Antwort des Staatsministeriums auf meine Stellungnahme zu einem automatisierten Vorgangsverwaltungsverfahren bei den Gerichten hat immerhin 13 Monate gedauert.

Die Erfüllung meiner Aufgaben ist mir aber nur dann möglich, wenn mich die öffentlichen Stellen den Vorgaben des Bayerischen Datenschutzgesetzes entsprechend unterstützen.

## 6.2 Gerichtlicher Bereich

### 6.2.1 Wohnungsdurchsuchungen bei Gefahr im Verzug - richterlicher Bereitschaftsdienst

Das Bundesverfassungsgericht hat in den letzten Jahren in mehreren Entscheidungen die Voraussetzungen und Grenzen einer auf Gefahr im Verzug gestützten Durchsuchungsmaßnahme aufgezeigt (siehe auch Nr. 6.3.6 und 21. Tätigkeitsbericht, Nr. 9.3.3). Dabei hat es insbesondere betont, dass die Wahrung der Regelzuständigkeit des Richters sicherzustellen sei. Die Bedeutung und Tragweite der betroffenen Grundrechte der Unverletzlichkeit der Wohnung und der informationellen Selbstbestimmung verlangen grundsätzlich, dass bei Eingriffen in den Schutzbereich dieser Grundrechte der Richtervorbehalt zur Grundrechtssicherung praktisch wirksam wird. Der Richtervorbehalt zielt auf eine vorbeugende Kontrolle der Maßnahme durch eine unabhängige und neutrale Instanz ab. Das Bundesverfassungsgericht hat hierzu ausgeführt, dass der persönlich und sachlich unabhängige, strikt dem Gesetz unterworfene Richter die Rechte der Betroffenen im Einzelfall am besten und sichersten wahren könne (vgl. BVerfGE 103, 142, 151).

Die Anordnung einer Wohnungsdurchsuchung - aber auch jeder anderen Eingriffsmaßnahme, die der Gesetzgeber unter Richtervorbehalt gestellt hat - durch die Staatsanwaltschaft oder ihre Ermittlungspersonen muss daher der Ausnahmefall bleiben. In der Vergangenheit habe ich jedoch bei mehreren datenschutzrechtlichen Prüfungen festgestellt, dass in zahlreichen Fällen Eilanordnungen durch die Staatsanwaltschaft oder Polizei nicht damit begründet wurden, dass jede weitere zeitliche Verzögerung den Ermittlungserfolg behindert hätte, sondern mit der Unerreichbarkeit von Richtern außerhalb der üblichen Dienstzeiten.

Das Bundesverfassungsgericht hat in seinem Beschluss vom 28.09.2006 (Az. 2 BvR 876/06) im Rahmen seiner Entscheidung über eine auf Gefahr im Verzug gestützte Wohnungsdurchsuchung in einer bayerischen Großstadt festgestellt, dass es von Verfassungs wegen zu beanstanden sei, wenn Gefahr im Verzug nur deshalb angenommen werde, weil in einer Stadt dieser Größe am frühen Abend gegen 18 Uhr ein richterlicher Durchsuchungsbeschluss nicht mehr zu erwirken sei. Die Strafverfolgungsbehörden müssten regelmäßig versuchen, eine Anordnung des instanziell und funktionell zuständigen Richters zu erlangen, bevor sie eine Durchsuchung beginnen. Die Annahme von Gefahr im Verzug könne nicht allein mit dem abstrakten Hinweis begründet werden, eine richterliche Entscheidung sei in einer Großstadt gewöhnlicherweise am späten Nachmittag oder am frühen Abend nicht mehr zu erlangen. Damit

korrespondiere die verfassungsrechtliche Verpflichtung der Gerichte, die Erreichbarkeit eines Ermittlungsrichters auch durch die Einrichtung eines Eil- oder Notdienstes zu sichern. Bei Tage müsse die Regelzuständigkeit des Ermittlungsrichters uneingeschränkt gewährleistet sein. Deshalb verpflichte der Richtervorbehalt die Länder dazu, sowohl innerhalb als auch außerhalb der üblichen Dienstzeiten für die Erreichbarkeit des Ermittlungsrichters bei Tage Sorge zu tragen. Gleichzeitig müssten dem Richter die notwendigen Hilfsmittel für eine sachangemessene Wahrnehmung seiner richterlichen Aufgaben zur Verfügung gestellt werden.

Ich habe mich unter Hinweis auf die oben genannte Entscheidung des Bundesverfassungsgerichts an das Staatsministerium der Justiz und für Verbraucherschutz gewandt und darauf hingewiesen, dass die bestehende Bereitschaftsdienstregelung einer Überprüfung bedarf. Das Ministerium hat unter Beteiligung der gerichtlichen Praxis die Anordnung über den Bereitschaftsdienst bei Gerichten und Staatsanwaltschaften daraufhin dahingehend geändert, dass eine Erreichbarkeit bei den Amtsgerichten von 6 bis 21 Uhr zu gewährleisten ist. Regelungen für einen Bereitschaftsdienst während der Nachtzeit finden sich nicht.

Das Bundesverfassungsgericht hat aber in seinem Beschluss vom 04.02.2005 (Az. 2 BvR 308/04) auch ausgeführt, dass die Landesjustiz- und Gerichtsverwaltungen und die Ermittlungsrichter die Voraussetzungen für eine tatsächlich wirksame präventive richterliche Kontrolle der Wohnungsdurchsuchungen schaffen müssen. Dazu gehöre neben der Erreichbarkeit eines Ermittlungsrichters bei Tage auch außerhalb der üblichen Dienststunden auch seine Erreichbarkeit während der Nachtzeit (§ 104 Abs. 3 StPO), jedenfalls bei einem praktischen, nicht auf Ausnahmefälle beschränkten Bedarf.

Ein Bedürfnis für eine generelle Ausweitung des Bereitschaftsdienstes, auch für die Nachtzeit, sieht das Staatsministerium der Justiz und für Verbraucherschutz nicht. Dies schließe nicht aus, dass - soweit nach den örtlichen Gegebenheiten hierfür Bedarf bestehe - die zuständigen Präsidien den Bereitschaftsdienst in zeitlicher Hinsicht über die bestehende Rahmenregelung hinaus ausdehnen. Ein solcher Bedarf wird offensichtlich derzeit nicht gesehen.

Ich habe mich deshalb an das Ministerium mit der Bitte gewandt, mir für meine datenschutzrechtliche Kontrolle die Erkenntnisse - insbesondere die sachlichen Grundlagen für die Bedarfsbeurteilung - mitzuteilen, die den Präsidien vor Ort vorliegen.

Eine Antwort steht noch aus.

### 6.2.2 Zuverlässigkeitsüberprüfung nach dem Rechtsberatungsgesetz

Aufgrund einer Eingabe war ich mit folgendem Sachverhalt befasst: Im Rahmen eines Erlaubnisverfahrens nach dem Rechtsberatungsgesetz (a.F.) sind Zuverlässigkeit, Eignung und Sachkunde des Antragstellers zu prüfen. Im konkreten Fall handelte es sich um die Frage, welche Anforderungen insoweit an die Zuverlässigkeit eines Rentenberaters zu stellen sind. Zu diesem Zweck wurde dem Petenten vom zuständigen Amtsgerichtspräsidenten ein Fragebogen zugesandt, mit dem eine Vielzahl von Daten erhoben wurde. Für die Fragen zum Beruf des Vaters, Alter des Ehegatten und Beruf der Kinder habe ich keine Erforderlichkeit gesehen. Die Frage „Besitzt Ihr Ehegatte Vermögen?“ halte ich, abgesehen von der fehlenden Bestimmtheit, angesichts des damit verbundenen Eingriffs in das informationelle Selbstbestimmungsrecht des am Verfahren unbeteiligten Ehegatten für höchst problematisch. Auch nach dem Bayerisches Datenschutzgesetz sind personenbezogene Daten, die nicht aus allgemein zugänglichen Quellen entnommen werden, beim Betroffenen mit seiner Kenntnis zu erheben.

Dies habe ich dem zuständigen Präsidenten des Amtsgerichts sowie dem Staatsministerium der Justiz und für Verbraucherschutz mit der Aufforderung mitgeteilt, in zukünftigen Verfahren diese Daten zumindest nur mit Einwilligung des Ehegatten zu erheben oder gänzlich darauf zu verzichten. Der Fragebogen sollte entsprechend geändert werden.

Das Staatsministerium und der Präsident des betroffenen Amtsgerichts haben mir daraufhin mitgeteilt, dass die Abfrage des Berufs des Vaters, Alters des Ehegatten sowie Berufs der Kinder zukünftig unterbleiben werde, da insoweit ebenfalls keine Erforderlichkeit für die Datenerhebung gesehen werde. Die Erhebung der Vermögens- und Einkommenssituation des Ehegatten werde aber auch zukünftig erfolgen, da diese für die Beurteilung der Zuverlässigkeit bei Tätigkeiten nach dem Rechtsberatungsgesetz sachlich erforderlich und der Ehegatte - dessen Einkommen erhoben werde - nur mittelbar betroffen sei.

Diese Argumentation überzeugt mich nicht. Ich habe daher das Staatsministerium der Justiz und für Verbraucherschutz und den zuständigen Amtsgerichtspräsidenten nochmals darauf hingewiesen, dass ich es nach wie vor für geboten halte, dass der jeweilige Ehepartner, dessen Einkommens- und Vermögensverhältnisse erhoben werden sollen, bei dieser Erhebung beteiligt wird. Dies kann dadurch geschehen, dass die Informationen zum Ehepartner mit einem gesonderten Blatt und Unterschriftenfeldern für beide Eheleute erhoben werden.

Sollte ich davon Kenntnis erlangen, dass der bisherige Fragebogen zukünftig weiter verwendet wird, werde ich eine förmliche Beanstandung prüfen.

### 6.2.3 Veröffentlichung von Gerichtsurteilen

Bei der Entscheidung über das Ob und Wie einer Veröffentlichung von Gerichtsurteilen ist das Persönlichkeitsrecht der Personen, deren Daten veröffentlicht werden sollen, mit dem Informationsinteresse der Öffentlichkeit abzuwägen.

Gerade die Veröffentlichung von bedeutsamen Urteilen der Obergerichte dient der Information und Fortbildung der Rechtsöffentlichkeit und der einheitlichen Rechtsprechung und damit auch der Rechtsklarheit. Grundsätzlich ist deshalb ein berechtigtes Interesse an der Veröffentlichung bedeutsamer Gerichtsurteile anzuerkennen. Andererseits wird durch eine Veröffentlichung erheblich in das Grundrecht auf informationelle Selbstbestimmung eingegriffen, wenn die Veröffentlichung personenbezogen erfolgt. Die Veröffentlichung von Gerichtsurteilen in nicht anonymisierter Form halte ich jedoch grundsätzlich nicht für erforderlich und damit auch nicht für zulässig. Der Zweck der Veröffentlichung kann auch durch anonymisierte Entscheidungen erreicht werden. Der mit einer Anonymisierung verbundene Aufwand ist als eher gering einzuschätzen. Die Namen von Prozessbeteiligten, Sachverständigen und Zeugen lassen sich ohne weiteres mit einer Suchroutine finden und ersetzen. Zu beachten ist jedoch, dass das bloße Weglassen des Namens für eine Anonymisierung oft nicht ausreichend ist, da auch andere Angaben ggf. im Zusammenwirken mit weiteren Informationen (z.B. Wohnort, Alter, Beruf, Arbeitsstelle, Staatsangehörigkeit oder familiäre Verhältnisse) geeignet sein können, die Identifizierung von Betroffenen - zumindest für einen bestimmten Personenkreis - zu ermöglichen. Zusätzliche Bedeutung kommt der Veröffentlichung einer Gerichtsentscheidung im Internet zu, da sie dort weltweit abrufbar ist. Der Verbreitungsgrad der Informationen wird hierdurch ganz erheblich gesteigert, die Gefahr einer Identifizierung der Betroffenen nimmt zu.

Im Berichtszeitraum habe ich aufgrund mehrerer Eingaben die Zulässigkeit von Veröffentlichungen von Gerichtsurteilen überprüft. In einem Fall waren in der veröffentlichten Gerichtsentscheidung umfangreiche Gesundheitsdaten enthalten. Diese Daten sind besonders sensibel und sind deshalb besonders zu schützen, so dass besonders hohe Anforderungen an eine ausreichende Anonymisierung zu stellen sind. In dem von mir überprüften Fall war eine Veröffentlichung dieser Daten vertretbar, da sie für das Verständnis der Entscheidung von Bedeutung waren und der Persönlichkeitsschutz des Betroffenen durch eine noch ausreichende Anonymisierung gewahrt war. Wäre ein solcher Schutz nicht möglich gewesen, hätte die Veröffentlichung dieser (bedeutsamen) Entscheidung in Frage gestellt werden müssen.

In einem anderen Fall hat das Gericht einer juristischen Fachzeitschrift, die unter Nennung des Namens der Parteien angefragt hatte, eine Urteilsabschrift übersandt, in der der Name der Parteien geschwärzt war. Aufgrund der Vorkenntnis des Adressaten war diesem - für das Gericht erkennbar - die Identität des Betroffenen trotz der Schwärzung bekannt.

Ich halte zwar die Übersendung einer anonymisierten Urteilsabschrift an die Presse auch in einem solchen Fall nicht grundsätzlich für ausgeschlossen. Notwendig ist aber ein besonders hohes schutzwürdiges Interesse der Öffentlichkeit an der Information durch die Gerichtsentscheidung, das das schutzwürdige Interesse des Betroffenen an der Nichtveröffentlichung überwiegt. Dabei ist auch darauf zu achten, dass die Übermittlung auf die für die Öffentlichkeit rechtlich bedeutsamen Ausführungen des Gerichts beschränkt wird, um überschießende Informationen zu vermeiden. So hätte im geprüften Fall das für die rechtliche Entscheidung nicht erhebliche Einkommen der Parteien geschwärzt werden müssen. Diese Angaben sind durch das Grundrecht auf informationelle Selbstbestimmung geschützt, das die Befugnis des Einzelnen gewährleistet, grundsätzlich selbst über die Preisgabe und Verwendung persönlicher Daten zu bestimmen, also selbst zu entscheiden, wann und innerhalb welcher Grenzen persönliche Lebenssachverhalte offenbart werden (vgl. auch BVerfGE 77, 121, 125). Die Übermittlung der Urteilsgründe ohne Schwärzung der Einkommensangaben war daher im vorliegenden Fall nicht zulässig, da überwiegend schutzwürdige Interessen entgegenstanden. Ich habe dies dem Präsidenten des betroffenen Gerichts mitgeteilt und ihn aufgefordert sicherzustellen, dass die datenschutzrechtlichen Anforderungen für den Umgang mit der Presse in Zukunft beachtet werden. Der Präsident hat mir daraufhin mitgeteilt, dass zukünftig in derartigen Fällen neben den Namen der Betroffenen auch weitere personenbezogene Angaben, die für das rechtliche Verständnis der Entscheidung nicht erforderlich sind, geschwärzt werden.

### 6.2.4 Automatisiertes Grundbuchabrufverfahren bei Notaren

In meinem 22. Tätigkeitsbericht (Nr. 6.2.1) hatte ich von meiner anlassunabhängigen Überprüfung der Rechtmäßigkeit von automatisierten Abrufen aus dem Grundbuch durch stichprobenartige Auswertung der Protokolldatei von zehn bayerischen öffentlichen Stellen berichtet.

In der Folge habe ich beim Präsidenten des Oberlandesgerichts München, Zentrale Grundbuchspeicherstelle für Bayern, um eine Auswertung der Protokolldateien nach aktuellen Abfragen durch bayerische

Notare gebeten. Aus den mir übersandten Protokolldaten habe ich zehn bayerische Notare ausgewählt und diese um Mitteilung des Anlasses, des berechtigten Interesses im Sinne von § 12 Grundbuchordnung und eventueller weiterer Rechtsgrundlagen für die Datenabfragen gebeten.

Die Prüfung der Zulässigkeit der Abfragen durch die Notare hat zwar keine datenschutzrechtlichen Verstöße ergeben, in einzelnen Fällen hatten mir aber Notare unter Berufung auf ihre Verschwiegenheitspflicht eine detaillierte Auskunftserteilung zunächst verweigert.

Die Kontrollkompetenz des Bayerischen Landesbeauftragten für den Datenschutz besteht nach dem Bayerischen Datenschutzgesetz (BayDSG) aber auch für Notare. Als sog. Beliehene gehören auch die bayerischen Notare zu den Adressaten dieses Gesetzes. Der Kontrolle durch den Landesbeauftragten für den Datenschutz unterliegen die Notare auch in Bezug auf Daten, die durch das bundesrechtlich geregelte Notargeheimnis besonders geschützt sind. In Art. 30 Abs. 2 Satz 1 BayDSG ist ausdrücklich festgelegt, dass sich die Kontrolle durch den Landesbeauftragten für den Datenschutz auch auf personenbezogene Daten erstreckt, die einem Berufs- oder besonderen Amtsgeheimnis unterliegen, insbesondere dem Steuergeheimnis nach § 30 der Abgabenordnung. Notare haben deshalb dem Landesbeauftragten für den Datenschutz wie alle öffentlichen Stellen in der Erfüllung seiner Aufgaben zu unterstützen, ihm die notwendigen Auskünfte zu geben und auf Anforderung Unterlagen zu übersenden (Art. 32 BayDSG).

Dies ist sei langem mit dem Staatsministerium der Justiz und für Verbraucherschutz und der Landesnotarkammer Bayern geklärt und konnte auch - nach entsprechenden Hinweisen - im Rahmen der Prüfung umgesetzt werden.

## 6.3 Strafverfolgung

### 6.3.1 Beteiligung von Sachverständigen an Strafermittlungen - Besorgnis der Befangenheit

Ein Petent hat sich an mich gewandt, weil eine Kriminalpolizeiinspektion eine private Gesellschaft im Rahmen eines gegen ihn geführten strafrechtlichen Ermittlungsverfahrens um Prüfung gebeten hatte, ob die auf seinem Computer gespeicherten Dateien einen strafrechtlich (urheberrechtlich) relevanten Inhalt haben. Dazu wurden die von der Polizei sichergestellten Computer unter Angabe der vollständigen Personalien des Petenten an die Gesellschaft übersandt. Eigentliche Aufgabe der Gesellschaft ist es, die Interessen ihrer Mitglieder zu vertreten, die in den entsprechenden Ermittlungsverfahren als Geschädigte eines evtl. Verstoßes gegen das Urhebergesetz in Betracht kommen.

In der Bitte der Polizei um Auswertung der Computerspeicherungen im Hinblick auf strafrechtlich relevante Inhalte sehe ich einen Sachverständigenauftrag, da die erbetenen Feststellungen, Sachkunde im Umgang mit Computern voraussetzen. Die Person des Sachverständigen muss aber Gewähr dafür bieten, dass er geeignet ist, zur Verfügung steht und kein Ablehnungsgrund vorliegt. Die Übermittlung personenbezogener Daten an einen Sachverständigen, bei dem die Besorgnis der Befangenheit besteht, halte ich deshalb für unzulässig. Dies gilt unabhängig von der Frage, ob der Sachverständige auf Antrag der Staatsanwaltschaft oder des Angeklagten in der Hauptverhandlung vom Gericht tatsächlich abgelehnt wird.

Im konkreten Fall war aus meiner Sicht die Besorgnis der Befangenheit gegeben, da die mit der Erstellung eines Sachverständigengutachtens beauftragte Gesellschaft gleichzeitig die Interessen der potentiell Geschädigten vertrat. Die fehlende Neutralität der Gesellschaft zeigte sich gerade dadurch, dass sie in dem Schreiben, mit dem sie der auftraggebenden Polizeidienststelle das Ergebnis der Auswertung mitteilte, zugleich die Vertretung der Geschädigten anzeigte und in deren Namen Strafantrag gegen den Petenten stellte. Unabhängig davon war die Übermittlung der personenbezogenen Daten des Petenten für die ordnungsgemäße Erfüllung des Sachverständigenauftrags auch nicht erforderlich und damit unzulässig. Dies habe ich dem Staatsministerium der Justiz und für Verbraucherschutz und der die Ermittlungen leitenden Staatsanwaltschaft mitgeteilt, und sie um künftige Beachtung in vergleichbaren Fällen gebeten.

Das Staatsministerium der Justiz und für Verbraucherschutz hat in einer Dienstbesprechung mit den Leitern der bayerischen Staatsanwaltschaften meine Bedenken gegen die Übermittlung personenbezogener Daten dargelegt und darauf hingewiesen, dass unabhängig von der Frage der Geeignetheit des beauftragten Gutachters die Akteneinsicht des Sachverständigen nach § 80 Abs. 2 StPO beschränkt werden könne und eine solche Beschränkung grundsätzlich in Betracht zu ziehen sei, soweit die Kenntnis personenbezogener Daten zur Erstellung des Gutachtens nicht erforderlich sei. Wenn zudem - wie in dem zugrunde liegenden Ermittlungsverfahren - eine private, nicht der Schweigepflicht unterliegende Interessenvertreterin um Sachverständigenauskunft gebeten werde, erscheine eine Übermittlung der Personalien des Beschuldigten nicht gerechtfertigt.

Außerdem hat das Staatsministerium der Justiz und für Verbraucherschutz die bayerischen Staatsanwaltschaften nach Erörterung dieser Thematik in einer Sitzung des Strafrechtsausschusses der Justizministerkonferenz insbesondere auf Folgendes hingewiesen:

- Bei einer Beiziehung von Mitarbeitern einer privaten Gesellschaft mit besonderem Fachwissen zu Durchsuchungen sei der Grundsatz der Verhältnismäßigkeit besonders zu beachten. Unzulässig sei es, solchen Mitarbeitern eigenständige Ermittlungshandlungen zu übertragen.

- Regelmäßig komme es nicht in Betracht, komplette Festplatten oder sonstige Datenträger, die auch nicht verfahrensrelevante Daten enthalten, der Gesellschaft zu übersenden.

Durch diese Hinweise wird das Bewusstsein der sachbearbeitenden Staatsanwältinnen und Staatsanwälte für die Belange des Datenschutzes geschärft.

### 6.3.2 Anfragen der Staatsanwaltschaften bei Sozialbehörden

Im Rahmen einer Eingabe war ich mit einer Auskunftserteilung durch eine Sozialbehörde an die Staatsanwaltschaft befasst. Ein Petent hat mir mitgeteilt, dass die für ihn zuständige Gemeinde auf Anfrage einer Staatsanwaltschaft, bei der gegen ihn ein Vollstreckungsverfahren wegen der Einziehung angefallener Gerichtskosten anhängig war, die Auskunft gegeben habe, dass er weder durch das Amt für soziale Leistungen noch durch die Agentur für Arbeit Leistungsbezüge erhalten habe. Vorausgegangen war dieser Datenübermittlung ein Schriftwechsel der Staatsanwaltschaft mit dem Petenten. Dieser hatte der Staatsanwaltschaft mitgeteilt, dass ihm das Arbeitslosengeld gestrichen worden sei. Der Aufforderung der Staatsanwaltschaft, die bezogene Arbeitslosenunterstützung durch die Übersendung eines entsprechenden Bescheides nachzureichen, war der Petent nicht nachgekommen. Daher hatte die Staatsanwaltschaft im Wege der Amtshilfe angefragt, ob und ggf. für welchen Zeitraum Unterstützung gewährt worden war.

Ich habe diese Anfrage überprüft und bin zu folgendem Ergebnis erlangt:

Mit der erbetenen Auskunft, dass kein Leistungsbezug erfolgt sei, werden Sozialdaten übermittelt. Diese sind besonders geschützt. Ihre Übermittlung ist - ohne Einwilligung des Betroffenen - nur zulässig, soweit eine gesetzliche Übermittlungsbefugnis nach den §§ 68 bis 77 SGB X oder nach einer anderen Rechtsvorschrift im Sozialgesetzbuch es erlauben oder anordnen. Für eine Datenübermittlung zur Vollstreckung von Gerichtskosten ist keine Rechtsgrundlage zu finden. Die Datenübermittlung war daher rechtswidrig. Die zuständige Stadt hat diese Auffassung geteilt. Sie sei fälschlicherweise davon ausgegangen, dass Auskünfte gegenüber der Staatsanwaltschaft in einem größeren Umfang zulässig seien und habe auf die Zulässigkeit der Anfrage einer Staatsanwaltschaft vertraut.

Ich habe daraufhin den Leiter der Staatsanwaltschaft auf die Unzulässigkeit der Datenerhebung hingewiesen und aufgefordert, die Mitarbeiter der Behörde entsprechend zu informieren, damit zukünftig solche auf staatsanwaltschaftlicher Anforderung beruhende rechtswidrigen Datenübermittlungen besonders geschützter Sozialdaten vermieden werden.

### 6.3.3 Gewährung von Akteneinsicht durch die Staatsanwaltschaft - Anhörung der Betroffenen

In seiner Entscheidung vom 26.10.2006 (Az. 2 BvR 67/06) hat das Bundesverfassungsgericht Stellung bezogen zur Frage des Umfangs der Erteilung von Auskünften aus Verfahrensakten und der Gewährung von Akteneinsicht an Privatpersonen oder sonstige Stellen (§ 475 StPO).

Es hat festgestellt, dass die auskunftserteilende oder akteneinsichtgewährende Stelle die schutzwürdigen Interessen solcher Personen, deren Daten auf diese Weise zugänglich gemacht werden, gegen das Informationsinteresse des Auskunft- oder Einsichtsbegehrenden abzuwägen und den Zugang zu den Daten ggf. angemessen zu beschränken hat. Werde durch die Gewährung der Akteneinsicht tief in Grundrechte Betroffener eingegriffen, so seien diese in der Regel zuvor anzuhören. Dies erfordere die Bedeutung und Reichweite des Rechts auf informationelle Selbstbestimmung der Betroffenen.

Nachdem nach meiner Kenntnis die Staatsanwaltschaften vor Gewährung von Akteneinsicht oder Erteilung von Auskünften aus Akten auch dann, wenn besonders sensible personenbezogene Daten übermittelt werden, bisher keine Anhörung der davon Betroffenen vorgesehen hatten, habe ich das Staatsministerium der Justiz und für Verbraucherschutz auf diese Entscheidung des Bundesverfassungsgerichts und die dort dargelegten Grundsätze hingewiesen. Das Ministerium hat diese daraufhin zum Gegenstand einer Dienstbesprechung mit den Leitern der bayerischen Staatsanwaltschaften gemacht und mir zugesichert, dass im Falle eines Akteneinsichts- oder Auskunftsgesuchs, mit dem tiefgreifende Grundrechtseingriffe einhergehen, eine vorherige Anhörung des Betroffenen erfolgen werde. Die Einhaltung der Grundsätze des Bundesverfassungsgerichts werde ich überprüfen.

### 6.3.4 Kontenabfragen durch die Staatsanwaltschaften

Nach dem Gesetz über das Kreditwesen erteilt die Bundesanstalt für Finanzdienstleistungsaufsicht auf Ersuchen Auskunft über Kontendaten an die für die Verfolgung und Ahndung von Straftaten zuständigen Behörden, soweit dies für die Erfüllung ihrer gesetzlichen Aufgaben erforderlich ist (§ 24 c Abs. 3 Nr. 2 KWG). Die Abrufe aus der entsprechenden Datei werden protokolliert.

Ich habe mir zur datenschutzrechtlichen Kontrolle der Rechtmäßigkeit von Auskunftsersuchen von der Bundesanstalt eine Übersicht der Gesamtzahl der Ersuchen der bayerischen Staatsanwaltschaften im Jahr 2005 erstellen lassen. Aus dieser Übersicht habe ich die Protokolldaten der Abrufe einer Staatsanwaltschaft in der Zeit vom 01.06. bis 31.12.2005 ausgewählt. Bei 18 bereits abgeschlossenen Verfahren habe ich eine datenschutzrechtliche Prüfung vor Ort durchgeführt. Die Prüfung hat gezeigt, dass bei bestimmten Deliktsarten, wie z.B. Betrug und Unterschlagung regelmäßig bereits nach Anzeigeerstattung eine Kontenabfrage erfolgt. Diese wurde in der Regel zu einem Zeitpunkt veranlasst, zu dem noch keine Beschuldigtenvernehmung oder weitere Ermittlungen stattgefunden hatten. Eine solche routinemäßige Kontenabfrage ohne ausreichende Anhaltspunkte für die Erforderlichkeit entspricht nicht den gesetzlichen Voraussetzungen.

Das Bundesverfassungsgericht hat in seiner Entscheidung vom 13.06.2007 zwar festgestellt, dass die Regelung zur Kontenabfrage den verfassungsrechtlichen Anforderungen genügt. Andererseits weist es aber auch ausdrücklich darauf hin, dass die Staatsanwaltschaften bei Anwendung dieser Norm Schranken unterworfen sind, die durch eine verfassungskonforme Auslegung der Norm und Anwendung der Verfahrensvorschriften zu wahren sind. Staatsanwaltschaften sollten deshalb grundsätzlich zunächst - auch unter Inkaufnahme gewisser zeitlicher Verzögerungen - über die Deliktsart hinaus ausreichende Anhaltspunkte für die Erforderlichkeit einer Kontenabfrage ermitteln, bevor ein entsprechendes Ersuchen gestellt wird. Dies habe ich gegenüber dem Leiter der überprüften Staatsanwaltschaft sowie dem Staatsministerium der Justiz und für Verbraucherschutz deutlich gemacht.

### 6.3.5 Anordnung von Blutentnahmen bei Gefahr im Verzug

In seinem Beschluss vom 12.02.2007 (Az. 2 BvR 273/06) hat das Bundesverfassungsgericht ausdrücklich darauf hingewiesen, dass die Anordnung einer Blutentnahme nach § 81 a Strafprozessordnung (StPO) grundsätzlich dem Richter zustehe. Der Richtervorbehalt ziele auf eine vorbeugende Kontrolle der Maßnahme durch eine unabhängige und neutrale Instanz. Nur bei einer Gefährdung des Untersuchungserfolgs durch die mit der Einholung einer richterlichen Entscheidung einhergehende Verzögerung bestehe auch eine Anordnungskompetenz der Staatsanwaltschaft und nachrangig ihrer Ermittlungspersonen. Die Strafverfolgungsbehörden müssen daher regelmäßig versuchen, eine Anordnung des zuständigen Richters zu erlangen, bevor sie selbst eine Blutentnahme anordnen. Die Gefährdung des Untersuchungserfolgs müsse mit Tatsachen begründet werden, die auf den Einzelfall bezogen und in den Ermittlungsakten zu dokumentieren sind, sofern die Dringlichkeit nicht evident sei. Die Gefährdung des Untersuchungserfolgs begründende einzelfallbezogene Tatsachen seien von den Staatsanwaltschaften in den Ermittlungsakten zu vermerken.

Ich habe das Staatsministerium der Justiz und für Verbraucherschutz auf diese Entscheidung hingewiesen und nachgefragt, wie bei den bayerischen Staatsanwaltschaften regelmäßig verfahren werde, insbesondere, ob im Regelfall für Anordnungen von Blutentnahmen ein richterlicher Beschluss beantragt werde.

Das Staatsministerium hat sich in seiner Antwort auf den Standpunkt gestellt, dass bei Blutprobenentnahmen wegen Alkoholgenusses im Hinblick auf den schnellen Abbau des Alkohols immer Gefahr im Verzug bestehe, da eine richterliche Entscheidung nur mit Verzögerung und daher nicht rechtzeitig erreicht werden könne. Es drohe insoweit ein Beweismittelverlust. Typischerweise handele es sich bei den den Blutprobenentnahmen zugrundeliegenden Sachverhalten um Vergehen im Zusammenhang mit Trunkenheit im Straßenverkehr bzw. entsprechende Ordnungswidrigkeiten.

Diese Verfahrensweise wird m.E. den Anforderungen des Bundesverfassungsgerichts nicht gerecht. Das Gesetz geht davon aus, dass der Regelfall die richterliche Anordnung ist (vgl. hierzu auch Nr. 3.2.1). Den Ausnahmefall bildet die Anordnungskompetenz der Staatsanwaltschaft bzw. ihrer Ermittlungspersonen. Etwaige Beweisschwierigkeiten in Grenzfällen dürfen nicht dazu führen, dass die gesetzliche Vorgabe systematisch ignoriert wird. Ich meine vielmehr, dass insbesondere in Fällen, in denen aufgrund der Umstände - etwa des Ergebnisses der Atemalkoholmessung - eine klar über den Grenzwerten liegende Blutalkoholkonzentration zu erwarten ist, eine eventuelle Unschärfe des Ergebnisses durch Rückrechnung in Kauf genommen werden muss, um dem gesetzlich normierten und grundgesetzlich gebotenen Richtervorbehalt - etwa durch den Versuch, eine mündliche Entscheidung des Richters einzuholen - Rechnung zu tragen.

Mein Schriftwechsel mit dem Staatsministerium der Justiz und für Verbraucherschutz dauert noch an.

### 6.3.6 Dokumentationspflicht bei Gefahr im Verzug

Wie ich bereits in meinem 21. Tätigkeitsbericht (Nr. 9.3.3) aufgezeigt habe, hat das Bundesverfassungsgericht schon im Jahr 2001 klargestellt, dass die staatsanwaltschaftliche Eilanordnung von Wohnungsdurchsuchungen der Ausnahmefall sein muss (siehe auch Nr. 6.2.1). Zur Wahrung der Grundrechte hat es deshalb u.a. gefordert, dass bei fehlender richterlicher Anordnung vor oder jedenfalls unmittelbar nach der Durchsuchung die Voraussetzungen der Maßnahme in der Ermittlungsakte dokumentiert werden, um eine spätere gerichtliche Nachprüfung zu ermöglichen. Insbesondere muss dokumentiert werden, warum ein Aufschieben der Wohnungsdurchsuchung nicht möglich und ob versucht worden war, den zuständigen Ermittlungsrichter zu erreichen.

Die praktische Umsetzung dieser Vorgaben des Bundesverfassungsgerichts habe ich erneut bei einer Staatsanwaltschaft geprüft. Dabei zeigte sich, dass das bei den bayerischen Staatsanwaltschaften in der Regel verwendete Formblatt für eine ordnungsgemäße Dokumentation der Voraussetzungen von „Gefahr im Verzug“ und der Erforderlichkeit einer Wohnungsdurchsuchung grundsätzlich ausreicht. Ich habe aber angeregt, zusätzlich auch die Uhrzeit der Versuche, den zuständigen Richter telefonisch zu erreichen, zu vermerken, weil dies im Einzelfall für die Beurteilung der Rechtmäßigkeit der Maßnahme von Bedeutung sein kann. Der Leiter der von mir geprüften Staatsanwaltschaft hat dies zum Anlass genommen, seine Behördenleiterverfügung betreffend „Durchsuchung wegen Gefahr im Verzug“ dahingehend zu ergänzen. Alle Abteilungsleiter und Referenten hat er auf diese Änderung hingewiesen und um zukünftige Beachtung gebeten.

Das Staatsministerium der Justiz und für Verbraucherschutz habe ich aufgefordert, auch bei den übrigen bayerischen Staatsanwaltschaften auf eine entsprechende datenschutzfreundliche Verfahrensweise hinzuwirken.

### 6.3.7 Benachrichtigung bei Maßnahmen der Telekommunikationsüberwachung

Nach der Strafprozessordnung sind die von der Telekommunikationsüberwachung Betroffenen (Beteiligte des überwachten Fernmeldeverkehrs) grundsätzlich zu benachrichtigen. Die Benachrichtigung hat zu erfolgen, sobald dies ohne Gefährdung des Untersuchungszwecks, des Lebens, der körperlichen Unversehrtheit und der persönlichen Freiheit einer Person und von bedeutenden Vermögenswerten geschehen kann. Diese Benachrichtigungspflicht besteht unabhängig vom Zeitpunkt der Anklageerhebung oder des rechtskräftigen Abschlusses des Verfahrens. Diese Verpflichtung wird häufig nicht oder nur unzureichend erfüllt. So wird im Gutachten des Max-Planck-Instituts über Rechtswirklichkeit und Effizienz der Telekommunikationsüberwachung festgestellt, dass in den überprüften Verfahren fast drei Viertel der betroffenen Anschlussinhaber nicht über die Maßnahme unterrichtet worden waren (siehe auch Nr. 9.3.6., 21. Tätigkeitsbericht).

Anlässlich der Prüfung einer Staatsanwaltschaft im Berichtszeitraum habe ich erneut festgestellt, dass der Pflicht zur Benachrichtigung des Beschuldigten und des Anschlussinhabers wie auch anderer Gesprächsteilnehmer wiederholt nicht nachgekommen wurde (siehe auch Nr. 7.2.4.3, 19. Tätigkeitsbericht). In vielen Fällen erfolgte die Benachrichtigung verspätet, erst nach rechtskräftigem Abschluss des Strafverfahrens. Unzutreffend ist auch die Annahme, die bloße Gewährung von Akteneinsicht an einen Verteidiger sei für die Erfüllung der Benachrichtigungspflicht ausreichend. Dieser muss, wenn schon keine gesonderte Benachrichtigung erfolgt, wenigstens im Rahmen der Akteneinsicht ausdrücklich von der Staatsanwaltschaft auf die erfolgte Telekommunikationsüberwachung hingewiesen werden.

Ich habe den Leiter der Staatsanwaltschaft gebeten, dafür Sorge zu tragen, dass zukünftig in seiner Behörde den gesetzlichen Benachrichtigungspflichten nachgekommen wird. Das Staatsministerium der Justiz und für Verbraucherschutz habe ich aufgefordert, auch bei den übrigen bayerischen Staatsanwaltschaften auf eine Beachtung dieser Grundsätze hinzuwirken.

Im Hinblick auf die Benachrichtigung von Verteidigern durch die Gewährung von Akteneinsicht habe ich erreicht, dass die Formblätter der Staatsanwaltschaften für die Gewährung von Akteneinsicht mit dem ergänzenden optional zu verwendenden ausdrücklichen Hinweis auf eine erfolgte Telekommunikationsüberwachung versehen werden.

### 6.3.8 Umfang der Akteneinsicht und Aktenführung bei besonders sensiblen Daten

Da die Frage der Akteneinsichtsgewährung nicht immer für die Gesamtheit der Verfahrensakten einheitlich beantwortet werden kann, regelt Nr. 186 Abs. 2 der Richtlinien für das Straf- und Bußgeldverfahren (RiStBV), dass Aktenteile, die erkennbar sensible persönliche Informationen enthalten, gesondert geheftet und hinsichtlich der Einsichtsgewährung einer besonderen Prüfung unterzogen werden. Zu den gesondert zu heftenden Aktenteilen zählen regelmäßig medizinische und psychologische Gutachten

sowie Berichte der Gerichts- und Bewährungshilfe sowie anderer sozialer Dienste und Niederschriften über besonders eingriffsintensive Ermittlungsmaßnahmen, wie beispielsweise die Telekommunikationsüberwachung. Nr. 220 RiStBV sieht ergänzend vor, dass Lichtbilder von Verletzten, die sie ganz oder teilweise unbekleidet zeigen, in einem verschlossenen Umschlag oder gesondert geheftet zu den Akten zu nehmen sind und bei der Gewährung von Akteneinsicht - soweit sie nicht für die verletzte Person selbst erfolgt - vorübergehend aus den Akten zu entfernen sind. Der Verteidigung ist insoweit Akteneinsicht auf der Geschäftsstelle zu gewähren.

Ich habe die Einhaltung dieser Grundsätze, die bei derart sensiblen Daten wegen der besonderen Schwere des Eingriffs in das informationelle Selbstbestimmungsrecht verfassungsrechtlich geboten sind, bei einer Staatsanwaltschaft überprüft. Dort habe ich festgestellt, dass in vielen Fällen sensible Aktenteile nicht in Sonderheften verwahrt waren. Zum Teil waren Aktenteile lediglich durch ein Trennblatt gesondert innerhalb der Akte geführt. Die bloße Trennung eines medizinischen Gutachtens vom restlichen Aktenteil durch ein Einlageblatt wird aber dem angestrebten Persönlichkeitsschutz nicht gerecht. Es soll verhindert werden, dass Dritte in sensible Aktenteile Einsicht erlangen, obwohl überwiegende schutzwürdige Interessen der Betroffenen entgegenstehen. Die Unterteilung einer umfangreichen Ermittlungsakte allein durch Trennblätter dient vielleicht der Übersichtlichkeit der Akte, ist aber nicht geeignet, einen Aktenteil mit sensiblen Daten ausreichend zu schützen.

Erkennbar sensible Akteninhalte sind daher stets in entsprechenden Sonderheften aufzubewahren. Der Leiter der von mir geprüften Staatsanwaltschaft hat die Staatsanwälte seiner Behörde auf die Einhaltung dieser Vorschriften nochmals hingewiesen.

Ich habe das Staatsministerium der Justiz und für Verbraucherschutz aufgefordert, auch bei den anderen bayerischen Staatsanwaltschaften auf die Einhaltung dieser Grundsätze hinzuwirken.

### 6.3.9 Abfragen aus der Zentralen Vollzugsdatei

Wie ich berichtet habe, ist die Zentrale Vollzugsdatei durch das Staatsministerium der Justiz und für Verbraucherschutz freigegeben worden (vgl. 22. Tätigkeitsbericht, Nr. 6.4.1). Bedienstete von Gerichten, Staatsanwaltschaften und Justizvollzugsanstalten dürfen zur Erfüllung ihrer dienstlichen Aufgaben auf die dort gespeicherten Informationen über Gefangene in den bayerischen Justizvollzugsanstalten zugreifen.

Die Möglichkeit und der Umfang des Zugriffs auf personenbezogene Daten wurden für die verschiedenen Benutzergruppen unter Berücksichtigung der jeweiligen Dienstaufgaben unterschiedlich geregelt. Die zum Abruf berechtigten Bediensteten werden nach Mitteilung des Staatsministeriums der Justiz und für Verbraucherschutz ausdrücklich darauf hingewiesen, dass der Abruf von Daten nur für die im Bayerischen Strafvollzugsgesetz genannten Zwecke zulässig ist, die Zugangsdaten vertraulich zu behandeln sind und im Falle eines möglichen Missbrauchs der zum Zugang berechtigenden Daten die Gemeinsame IT-Stelle der bayerischen Justiz unverzüglich und unmittelbar zu informieren ist, damit die notwendigen Sicherheitsvorkehrungen getroffen werden können. Darüber hinaus wird jeder Zugriff auf die Zentrale Vollzugsdatei unter Angabe von Zeitpunkt, Buchnummer des Gefangenen, Benutzerkennung und Aktenzeichen protokolliert. Jeder Nutzer wird aufgefordert, bei dem Zugriff ein Aktenzeichen anzugeben, auf das sich der Zugriff bezieht.

Ich habe die Gemeinsame IT-Stelle der bayerischen Justiz beim Oberlandesgericht München gebeten, mir zum Zweck einer anlassunabhängigen Prüfung von Zugriffen auf die Zentrale Vollzugsdatei Bayern die Protokolldaten zu den letzten 100 Anfragen der bayerischen Staatsanwaltschaften und Justizvollzugsanstalten zu überlassen. Die Auswertung der Protokolllisten hat ergeben, dass die Eingabe des Aktenzeichens nicht immer ordnungsgemäß erfolgt, so dass nicht in allen Fällen der Abfragegrund festgestellt werden konnte.

Das Staatsministerium der Justiz und für Verbraucherschutz hat deshalb die Leiterinnen und Leiter der Justizvollzugsanstalten dringend angehalten, bei Anfragen an die Zentrale Vollzugsdatei das vollständige der Anfrage zugrunde liegende Aktenzeichen anzugeben. In Fällen, in denen kein Aktenzeichen vorliegt (z.B. Vorbereitung einer beabsichtigten Verlegung), soll zur Nachprüfbarkeit ein aussagekräftiger und nachprüfbarer Vermerk - z.B. „Sicherheitsverlegung geplant“ - angebracht werden. Aus dem Bereich der Gerichte und Staatsanwaltschaften wurden die zugriffsberechtigten Anwender ebenfalls sensibilisiert.

Das Staatsministerium der Justiz und für Verbraucherschutz hat außerdem angekündigt, dass es selbst Stichproben veranlassen und überprüfen werde, ob die Hinweise Beachtung gefunden haben.

### 6.3.10 Datenübermittlung an die Presse

Über die Neufassung der Richtlinie für die Zusammenarbeit der bayerischen Justiz mit der Presse habe ich bereits in meinem 19. Tätigkeitsbericht (Nr. 7.3.3) berichtet. Dort ist zur Datenübermittlung in Strafsachen ausgeführt, dass personenbezogene

Daten an die Presse nur dann weiter gegeben werden dürfen, wenn die Beteiligten eingewilligt haben oder das Verfahren gerade im Hinblick auf die Person des Betroffenen oder die besonderen Umstände der Tat für die Öffentlichkeit von überwiegendem Interesse ist.

Ich habe im Berichtszeitraum die Zusammenarbeit der Staatsanwaltschaften mit der Presse durch Auswertung der Presseberichterstattung beobachtet. Dabei habe ich mehrere Presseveröffentlichungen zum Anlass genommen, die Leiter der Staatsanwaltschaften auf die folgenden zu beachtenden datenschutzrechtlichen Grundsätze hinzuweisen:

- Bei der Entscheidung, ob und in welchem Umfang personenbezogene Daten an die Presse übermittelt werden, sind die schutzwürdigen Belange der Betroffenen unter Berücksichtigung des Grundsatzes der Unschuldsvermutung gegen das Informationsinteresse der Öffentlichkeit abzuwägen. Zwar ist durch Art. 4 Bayerisches Pressegesetz (BayPrG) das Auskunftsrecht der Presse gegenüber Behörden festgelegt. Dieses Recht ist Ausfluss der Pressefreiheit, die durch Art. 5 Grundgesetz geschützt ist und den Staat verpflichtet, die ungehinderte Betätigung der Presseangehörigen von der Beschaffung der Informationen bis zur Verbreitung der Nachrichten zu ermöglichen. Art. 4 BayPrG stellt aber keine hinreichend normenklare bereichsspezifische Regelung für die Übermittlung personenbezogener Daten dar. Diese richtet sich, sofern keine spezialgesetzliche Regelung existiert, nach Art. 19 Bayerisches Datenschutzgesetz. Dort ist die materiell-rechtliche Zulässigkeit der Übermittlung personenbezogener Daten an private Dritte festgelegt. Danach ist die Übermittlung personenbezogener Daten an nichtöffentliche Stellen zulässig, wenn die nichtöffentliche Stelle ein berechtigtes Interesse an der Kenntnis der zu übermittelnden Daten glaubhaft darlegt und der Betroffene kein schutzwürdiges Interesse an dem Ausschluss der Übermittlung hat. Die Verantwortung für die Zulässigkeit der Datenübermittlung trägt die übermittelnde Stelle. In welcher Form, mit welchem Inhalt und zu welchem Zeitpunkt die Behörde dem Auskunftsersuchen der Presse nachkommt, unterliegt jedoch keinen starren Regeln, sondern bestimmt sich nach den Anforderungen, die für die Erfüllung der öffentlichen Aufgabe der Presse, den Schutz des Persönlichkeitsrechts des Betroffenen und einer effektiven staatlichen Aufgabenerfüllung im Einzelfall notwendig sind.

- Die Gefahr eines Rückschlusses auf die Person eines Betroffenen für einen - mit Zusatzwissen ausgestatteten - Personenkreis (z.B. Personen des sozialen Umfelds) ist zu berücksichtigen.

- Auch die (amtliche) Bestätigung personenbezogener Informationen gegenüber der Presse auf Nachfrage stellt eine Datenübermittlung an private Dritte dar. Durch eine solche Bestätigung der Staatsanwaltschaft verdichtet sich der Wahrheitsgehalt der Informationen, auch wenn sie bereits in der Öffentlichkeit bekannt sind. Auf solche Bestätigungen sind daher die Maßstäbe, die in der Richtlinie für die Zusammenarbeit der bayerischen Justiz mit der Presse aufgeführt sind, anzuwenden.

In einem Fall hatte sich die Staatsanwaltschaft zu internen Zwischenergebnissen eines laufenden Ermittlungsverfahrens gegenüber der Presse geäußert, obwohl, wie die Staatsanwaltschaft wusste, der Presse die Person des Beschuldigten aufgrund seiner eindeutigen Berufsbezeichnung bereits bekannt war. Eine solche Äußerung halte ich im Hinblick auf die Unschuldsvermutung (Art. 6 Abs. 2 Europäische Menschenrechtskonvention) grundsätzlich für bedenklich. Die Unschuldsvermutung gebietet Zurückhaltung bei behördlicher Publikation einer strafrechtlichen Beschuldigung. Ich habe den Leiter der Staatsanwaltschaft gebeten, dafür Sorge zu tragen, dass bei zukünftigen Presseauskünften die dargestellten Grundsätze berücksichtigt und die Mitarbeiter entsprechend sensibilisiert werden.

## 6.4 Justizvollzug

### 6.4.1 Verwaltungsvorschriften zum Bayerischen Strafvollzugsgesetz

Das Staatsministerium der Justiz und für Verbraucherschutz hat, da mit der Föderalismusreform I die Regelungskompetenz für den Strafvollzug auf die Bundesländer übergegangen ist, auch Verwaltungsvorschriften zum Bayerischen Strafvollzugsgesetz erlassen. Folgende datenschutzrechtliche Forderungen wurden dabei berücksichtigt:

- Beim Aufnahmeverfahren darf nur mit Einverständnis des Gefangenen ausnahmsweise die Hilfe eines sorgfältig ausgewählten Mitgefangenen in Anspruch genommen werden.

- Bei Überstellungen in eine andere Justizvollzugsanstalt darf nur in besonderen Fällen ein Begleitbericht beigefügt werden. Besondere Fälle liegen vor, wenn allein aufgrund eines besonderen Vermerks auf dem Transportschein eine sachgerechte Unterbringung oder Behandlung des Gefangenen in der aufnehmenden Anstalt nicht gewährleistet ist. Der Begleitbericht ist zum Schutz sensibler Daten

in einem verschlossenen Umschlag mitzugeben.

- Für besondere Sicherungsmaßnahmen (z.B. ständige Beobachtung, Fesselung), deren Notwendigkeit und Umfang in angemessenen Abständen zu überprüfen ist, sind neben dem Ergebnis der Überprüfung auch die Gründe für die erstmalige Anordnung der Sicherungsmaßnahme zu dokumentieren.

- Bei Besuchen und Besichtigungen der Justizvollzugsanstalt durch anstaltsfremde Personen, Vertreter von Publikationsorganen sowie Film- und Fernsehteams ist das informationelle Selbstbestimmungsrecht der Gefangenen zu wahren. Eine Besichtigung des Haftraums gegen den Willen des Gefangenen unterbleibt.

Eine ausreichende Klarstellung des Umfangs der ärztlichen Schweigepflicht bei Geheimnissen, die dem Arzt im Rahmen der allgemeinen Gesundheitsfürsorge bekannt wurden, ist trotz meiner Forderung nicht erfolgt.

### 6.4.2 Videoüberwachung des Besucherverkehrs

Art. 30 BayStVollzG sieht vor, dass Besuche aus Gründen der Behandlung oder der Sicherheit oder Ordnung der Anstalt überwacht werden dürfen, es sei denn, es liegen im Einzelfall Erkenntnisse dafür vor, dass es der Überwachung nicht bedarf. Die Überwachung und Aufzeichnung mit technischen Mitteln ist zulässig, wenn die Besucher und die Gefangenen vor dem Besuch darauf hingewiesen werden.

Anlässlich der Prüfung einer Justizvollzugsanstalt habe ich festgestellt, dass in den Warteräumen für die Besucher auf die Videoüberwachung schriftlich mittels eines Papierschilds in deutscher Sprache hingewiesen wird. Ich halte dies nicht für ausreichend, da auch Personen, die nicht des Lesens oder der deutschen Sprache mächtig sind, Besucher einer Justizvollzugsanstalt sein können. Deshalb sind Hinweisschilder mit einem Piktogramm in ausreichender Größe und Zahl an geeigneten Stellen anzubringen. Der Leiter der Justizvollzugsanstalt hat noch am Tag der Prüfung solche Hinweisschilder in Auftrag gegeben. Das Staatsministerium der Justiz und für Verbraucherschutz hat mir zwischenzeitlich mitgeteilt, dass dies für alle bayerischen Justizvollzugsanstalten veranlasst wurde.

Die Videobänder mit den Aufzeichnungen der Besuchsüberwachung sind nach Art. 30 Abs. 1 Satz 2 BayStVollzG spätestens mit Ablauf eines Monats zu löschen. Diese Frist ist eine Höchstfrist, so dass eine Aufbewahrung nur solange zulässig ist, wie sie auch erforderlich ist. Die Bänder sind deshalb - auch vor Ablauf der Monatsfrist - zu löschen, sobald sie zum Zwecke der Besuchsüberwachung nicht mehr benötigt werden. Eine regelmäßige Ausschöpfung der gesetzlichen Höchstfrist in bayerischen Justizvollzugsanstalten ist damit nicht vereinbar. Eine Justizvollzugsanstalt hat auf meinen Hinweis hin eine generelle Speicherungsdauer von 16 Tagen für ausreichend erachtet.

### 6.4.3 Überwachung von Telefonaten

Gefangenen kann in dringenden Fällen gestattet werden, Ferngespräche zu führen (Art. 35 Abs. 1 BayStVollzG). Die Genehmigung von Telefonaten stellt eine Ermessensentscheidung der Justizvollzugsanstalt dar. Sie dürfen aus Gründen der Behandlung oder der Sicherheit oder Ordnung in der Anstalt überwacht werden, es sei denn, es liegen im Einzelfall Erkenntnisse dafür vor, dass es der Überwachung nicht bedarf.

Anlässlich einer Überprüfung einer Justizvollzugsanstalt hat mir deren Leiter mitgeteilt, dass die Entscheidung über Anträge auf Telefonate den Abteilungsleitern übertragen ist. Den Entscheidungen lägen Einzelfallprüfungen zugrunde, bei denen auch die Frage der Notwendigkeit einer Gesprächsüberwachung geprüft werde. Falls aus Sicht der Anstalt erforderlich, würden - nach entsprechender vorheriger Mitteilung an den Gesprächsteilnehmer - auch Gespräche mit Verteidigern überwacht. Ich habe darauf hingewiesen, dass jedenfalls Gespräche von Gefangenen mit den Verteidigern - auch mit Einwilligung der Betroffenen - nicht überwacht werden dürfen. Dies ergibt sich - abgesehen von Zweifeln an der Freiwilligkeit der Einwilligung - aus der eindeutigen Regelung des Bayerischen Strafvollzugsgesetzes (Art. 30 Abs. 5 i.V.m. Art. 35 Abs. 1 Satz 2 BayStVollzG).

### 6.4.4 Anfertigung von Briefkopien - Unterrichtung des betroffenen Gefangenen

Im Rahmen einer Eingabe hatte ich die datenschutzrechtlichen Voraussetzungen für die Anfertigung einer Kopie eines an einen Gefangenen gerichteten Briefs und deren Beinahme zu der Gefangenenpersonalakte durch eine Justizvollzugsanstalt zu prüfen.

Das Anhalten eines Briefes in einer Justizvollzugsanstalt ist unter den Voraussetzungen des Art. 34 BayStVollzG grundsätzlich zulässig. Die Anhaltung ist dem Gefangenen mitzuteilen (Art. 34 Abs. 3 BayStVollzG). Entsprechendes muss gelten, wenn ein Brief zuvor nicht im Original angehalten, aber kopiert und die Kopie zur Akte des Gefangenen genommen wird. Eine Pflicht zur Unterrichtung des Gefangenen und bei eingehenden Briefen auch des

Absenders ergibt sich aus Art. 196 Abs. 4 Satz 1 BayStVollzG. Dort ist geregelt, dass die Betroffenen über eine ohne ihre Kenntnis vorgenommene Erhebung personenbezogener Daten unterrichtet werden, wenn dadurch nicht die Erfüllung der Aufgaben der Justizvollzugsanstalt gefährdet wird. Dabei ist in jedem Einzelfall das Grundrecht des Briefgeheimnisses aus Art. 10 Abs. 1 GG gegen die von der Justizvollzugsanstalt wahrzunehmenden Aufgaben abzuwägen.

Dies habe ich der Justizvollzugsanstalt mitgeteilt. Sie hat mir daraufhin zugesichert, dass zukünftig bei der Erhebung, Verarbeitung und Nutzung von personenbezogenen Informationen aus dem Schriftwechsel der Gefangenen entsprechend verfahren wird. Der besonderen Vertraulichkeit und Schutzbedürftigkeit brieflicher Außenkontakte werde Rechnung getragen. Sofern Kopien von Schreiben gefertigt und zu den Akten genommen würden, würden die Betroffenen hierüber informiert werden.

### 6.4.5 Notwendigkeit einer förmlichen Verpflichtung ehrenamtlicher Mitarbeiter

Im Rahmen mehrerer Prüfungen bei bayerischen Justizvollzugsanstalten habe ich festgestellt, dass dort in zahlreichen Fällen ehrenamtliche Mitarbeiter für die Einzelbetreuung von Gefangenen, Gruppenarbeit, Hilfe für Familienangehörige u.a. eingesetzt werden. Bei Aufnahme ihrer Tätigkeit werden diese durch die Leiter der jeweiligen Justizvollzugsanstalten regelmäßig zwar über ihre Aufgaben und Pflichten, die einschlägigen Vollzugsvorschriften und Strafvorschriften zum Schutz der Sicherheit und Ordnung in der Anstalt belehrt. Eine förmliche Verpflichtung zur Verschwiegenheit i.S.v. § 1 Verpflichtungsgesetz erfolgt jedoch nicht.

Ich halte dieses Verfahren aus datenschutzrechtlicher Sicht für unzureichend. Eine förmliche Verpflichtung zur Verschwiegenheit von anstaltsfremden Personen, die durch ihre Tätigkeit in der Justizvollzugsanstalt personenbezogene Daten von Gefangenen zur Kenntnis nehmen, ist dringend notwendig. Nur durch eine solche Verpflichtung ist der Schutz der Vertraulichkeit durch die bei Bruch der Verschwiegenheitspflicht bestehende Strafbarkeit nach § 203 StGB in ausreichendem Maß gewährleistet. Dies gilt auch für den Einsatz ehrenamtlicher Mitarbeiter.

Das Staatsministerium der Justiz und für Verbraucherschutz lehnt eine solche förmliche Verpflichtung von ehrenamtlichen Mitarbeitern ab, weil diese aus eigenem Antrieb eine humanitäre Aufgabe mit Einwilligung der Gefangenen erfüllten. Eine förmliche Verpflichtung könnte als Ausdruck ungerechtfertigten Misstrauens gegenüber der persönlichen Integrität des Betroffenen verstanden werden.

Diese Auffassung halte ich nicht für zutreffend. Der Gesetzgeber hat das Instrument der förmlichen Verpflichtung gerade gewählt, um die Geheimhaltung der Daten durch die Strafandrohung sicherzustellen. Im Bereich des öffentlichen Dienstes ist es eine Selbstverständlichkeit, dass Personen, die nicht Amtsträger sind, aber Zugriff auf sensible personenbezogene Daten haben, zuvor förmlich zur Verschwiegenheit verpflichtet werden. Dies ist nicht ehrenrührig, sondern aus datenschutzrechtlicher Sicht geboten.

## 7 Vermessungsverwaltung

### 7.1 Daten des Liegenschaftskatasters für Landkreise

Im Jahr 2005 wurde für die Benutzung der Daten des Liegenschaftskatasters ein automatisiertes Abrufverfahren eingeführt. In der Zwischenzeit wurde seitens der Landkreise der Wunsch geäußert, Daten aus dem Liegenschaftskataster nicht nur im Einzelfall bei Vorliegen eines berechtigten Interesses automatisiert abrufen zu können, sondern den Gesamtbestand der Daten bezogen auf das Gebiet des jeweiligen Landkreises in eigenen Datenbeständen vorhalten zu dürfen. Dies hätte den Vorteil, dass die Daten jederzeit verfügbar wären, wie es zum Beispiel im Katastrophenfall notwendig sei.

Weder die Vorschriften des Vermessungs- und Katastergesetzes (VermKatG) noch die Verordnung über den automatisierten Abruf von personenbezogenen Daten aus dem Liegenschaftskataster (ALBV) boten dafür aber eine Rechtsgrundlage. Darauf habe ich hingewiesen. Ich habe aber - bei bestehender Notwendigkeit der Vorhaltung des Gesamtbestands - eine Änderung des VermKatG als die einzig praktikable Lösung angesehen.

Nach fachlicher Prüfung und Bejahung dieser Vorfrage durch das Staatsministerium der Finanzen wurde Art. 11 VermKatG dahingehend geändert, dass die Landkreise zur Erfüllung ihrer Aufgaben auf Antrag die personenbezogenen Daten des Liegenschaftskatasters flächendeckend für ihr Gebiet erhalten.

Ich habe mich dafür eingesetzt, dass für die Verarbeitung und Nutzung der zur Verfügung gestellten Daten sowie für die Protokollierung der Abrufe datenschutzrechtliche Grundsätze Beachtung finden. So darf ein Abruf nur erfolgen, soweit ein berechtigtes Interesse vorliegt. Die abgerufenen Daten dürfen nur für Aufgaben genutzt und verarbeitet werden, zu deren Erfüllung sie abgerufen wurden. Die Daten dürfen nicht an Dritte weitergegeben werden, auch nicht in veränderter Form. Abgerufene und gespeicherte Daten sind zu löschen, wenn der Abruf unzulässig war, wenn eine weitere Speicherung der Daten unzulässig ist oder sobald ihre Kenntnis für die abru-

fende Stelle zur Aufgabenerfüllung nicht mehr erforderlich ist. Es ist sicherzustellen, dass Abrufe nur durch hierzu berechtigte Mitarbeiter unter Verwendung einer Benutzerkennung, eines Passworts sowie des Geschäfts- oder Aktenzeichens des dem Abruf zugrunde liegenden Vorgangs vorgenommen werden. Die Abrufe sind zu protokollieren, so dass eine Rechtmäßigkeitskontrolle und die Sicherstellung der ordnungsgemäßen Datenverarbeitung erfolgen können. Das Staatsministerium der Finanzen hat mir entsprechende Regelungen in der ALBV zugesichert.

# 8 Ordnungswidrigkeitenverfahren

## 8.1 Umfang der Datenerhebung in Verkehrsordnungswidrigkeitenverfahren

Im Berichtszeitraum war ich mit mehreren Eingaben befasst, die sich gegen den Umfang der abgefragten Daten in Anhörungsbögen kommunaler Verkehrsüberwachungsbehörden wandten. So sollte insbesondere die Telefonnummer, die mit dem Hinweis auf die Sanktionierung nach § 111 Ordnungswidrigkeitengesetz (OWiG) als Pflichtangabe bezeichnet war, erhoben werden. In einem Fall war mit dem gleichen Hinweis nach dem „Wohnungsgeber“ gefragt worden.

Nach § 111 OWiG handelt ordnungswidrig, wer einer zuständigen Behörde über seinen Vor-, Familien- oder Geburtsnamen, den Ort oder Tag seiner Geburt, seinen Familienstand, seinen Beruf, seinen Wohnort, seine Wohnung oder seine Staatsangehörigkeit eine unrichtige Angabe macht oder die Angabe verweigert. Nicht aufgeführt in diesem Katalog sind die Telefonnummer sowie der Wohnungsgeber.

Auf den von mir überprüften Anhörungsbögen fehlte nicht nur der Hinweis auf die Freiwilligkeit dieser Angaben. Im Gegenteil wurde durch den Hinweis auf § 111 OWiG gerade der Eindruck erweckt, dass die Verweigerung auch dieser Angaben bußgeldbewehrt sei. Ich habe mich deshalb sowie mit der Anregung, den missverständlichen Begriff „Wohnungsgeber“ durch „Angabe des Hauptmieters“ zu ersetzen, an die betreffenden kommunalen Verkehrsordnungswidrigkeitenbehörden gewandt.

Diese haben daraufhin die Angaben zu den Personalien auf den Anhörungsbögen neu gestaltet. Dabei wurden entsprechend meiner Anregung die Angabenblöcke „Pflichtangaben“ und „freiwillige Angaben“ geschaffen, räumlich getrennt und die Angabe „Telefonnummer“ entsprechend korrekt zugeordnet. Der unklare Begriff „Wohnungsgeber“ wurde durch „evtl. Hauptmieter“ ersetzt.

## 8.2 Anhörung wegen Verkehrsordnungswidrigkeit

Bürger hatten sich beschwert, dass sie als Halter eines Kraftfahrzeugs von kommunalen Verkehrsüberwachungsbehörden einen Anhörungsbogen als Betroffene einer Verkehrsordnungswidrigkeit erhalten hatten, obwohl von Anfang an feststellbar gewesen wäre, dass die Betroffenen nicht die Fahrer des Kraftfahrzeugs gewesen sein konnten.

Auf Nachfrage wurde mir von den Behörden mitgeteilt, dass im Rahmen eines automatisierten Verfahrens aufgrund des Kraftfahrzeugkennzeichens der Fahrzeughalter festgestellt werde. Ebenfalls automatisiert werde die Anhörung an den Fahrzeughalter als Betroffener einer Ordnungswidrigkeit versandt. Eine manuelle Kontrolle eventueller Messfotos auf Übereinstimmung von Alter und/oder Geschlecht des Halters erfolge zu diesem Zeitpunkt aufgrund der hohen Anzahl der zu bearbeitenden Fälle nicht. Erst im weiteren Verlauf der Ermittlungen, spätestens aber vor Erlass eines Bußgeldbescheids werde das Messfoto als Entscheidungshilfe mit herangezogen.

Neben der Polizei können in Bayern auch die Gemeinden Ordnungswidrigkeiten nach § 24 Straßenverkehrsgesetz, die im ruhenden Verkehr begangen wurden, oder Verstöße gegen die Vorschriften über die zulässige Geschwindigkeit von Kraftfahrzeugen verfolgen und ahnden. Aus datenschutzrechtlicher Sicht ist aber die ungeprüfte Versendung des Anhörungsbogens an den Fahrzeughalter nicht akzeptabel. Dieses Verfahren führt dazu, dass selbst dann, wenn bei einem Abgleich mit dem Messfotos eindeutig erkennbar wäre, dass der Fahrzeughalter als Fahrer nicht in Betracht kommt, dieser mit dem Status eines Betroffenen bei den Ordnungswidrigkeitenbehörden - jedenfalls vorübergehend - gespeichert und durch die Versendung des Anhörungsbogens auch entsprechend behandelt wird.

Ich habe diese Vorgänge zum Anlass genommen, das Staatsministerium des Innern dazu um Stellungnahme zu bitten. Dieses teilte mir mit, dass die bayerische Polizei vor Versendung des Anhörungsbogens durch Bildabgleich überprüfe, ob der Fahrzeughalter als Fahrer in Betracht komme. Sei dies nicht der Fall, weil z.B. der Fahrzeughalter männlich und der augenscheinliche Fahrzeugführer weiblich oder der Halter eine juristische Person sei, versende die Zentrale Bußgeldstelle an den Halter automatisiert nur einen Zeugenbefragungsbogen und keinen Anhörungsbogen für Betroffene. Das Staatsministerium des Innern stimmt mit mir darin überein, dass eine solche Vorgehensweise nicht nur möglich und vorzugswürdig, sondern geboten ist.

Dies habe ich den betreffenden kommunalen Verkehrsordnungswidrigkeitenbehörden mitgeteilt. Diese haben daraufhin das dort praktizierte Verfahren dahin

gehend geändert, dass sie neben Anhörungsbögen für Betroffene auch solche für Zeugen erstellen und entsprechend der Vorgaben des Staatsministeriums des Innern festlegen, welche Anhörungsbögen in welchen Fällen versendet werden. Außerdem wurde veranlasst, die EDV-technischen Abläufe im automatisierten Verfahren entsprechend anzupassen.

# 9 Gemeinden, Städte und Landkreise

## 9.1 Beschluss des Bundesverfassungsgerichts zur Videoüberwachung öffentlicher Orte und Einrichtungen

Das Bundesverfassungsgericht (BVerfG) hat mit Beschluss vom 23.02.2007 - 1 BvR 2368/06 - festgestellt, dass eine Videoüberwachung öffentlicher Orte und Einrichtungen mit Aufzeichnung des gewonnenen Bildmaterials, bei der überwiegend Personen erfasst werden, die in keiner Beziehung zu einem konkreten Fehlverhalten stehen und den Eingriff durch ihr Verhalten nicht veranlasst haben, angesichts des erheblichen Gewichts der Grundrechtsbeeinträchtigung nicht auf Art. 16 Abs. 1 und Art. 17 Abs. 1 Bayerisches Datenschutzgesetz (BayDSG) gestützt werden kann. Der Entscheidung liegt folgender Sachverhalt zugrunde:

Die Stadt R. ließ im Jahre 2005 über den Resten einer ehemaligen mittelalterlichen jüdischen Synagoge durch einen israelischen Künstler auf einem städtischen Platz ein Bodenrelief herstellen, das als Begegnungsstätte gedacht ist. Nachdem es im Bereich des Kunstwerks zu mehreren Vorfällen gekommen war, beabsichtigte die Stadt, den Ort auf der Grundlage des Bayerischen Datenschutzgesetzes mit Kameras zu überwachen. Dagegen erhob ein Bürger erfolglos Klage. Gegen die Entscheidung des Verwaltungsgerichts eingelegte Rechtsmittel blieben vor dem Bayerischen Verwaltungsgerichtshof ebenfalls ohne Erfolg. Auf die vom Beschwerdeführer dagegen erhobene Verfassungsbeschwerde hob das BVerfG die angegriffenen Entscheidungen mit der Begründung auf, für die geplante Videoüberwachung mit Aufzeichnung des gewonnenen Bildmaterials fehle es an einer hinreichenden gesetzlichen Ermächtigung. Die Entscheidung des BVerfG enthält im Wesentlichen folgende Aussagen:

- Eine Videoüberwachung öffentlicher Orte mit Aufzeichnung des gewonnenen Bildmaterials, bei der überwiegend Personen erfasst werden, die in keiner Beziehung zu einem konkreten Fehlverhalten stehen und den Eingriff durch ihr Verhalten nicht veranlasst haben, stellt einen Eingriff von erheblichem Gewicht in das informationelle Selbstbestimmungsrecht dar.

  Maßgebend für die rechtliche Beurteilung der Intensität eines Eingriffs in das Recht auf informationelle Selbstbestimmung ist die Art der Beeinträchtigung. Insofern kann auch von Belang sein, ob die betroffenen Personen für die Maßnahme einen Anlass geben und wie dieser beschaffen ist. Verdachtslose Eingriffe mit großer Streubreite, bei denen zahlreiche Personen in den Wirkungsbereich einer Maßnahme einbezogen werden, die in keiner Beziehung zu einem konkreten Fehlverhalten stehen und den Eingriff durch ihr Verhalten nicht veranlasst haben, weisen grundsätzlich eine hohe Eingriffsintensität auf.

  Die geplante Videoüberwachung ist ein intensiver Eingriff. Sie beeinträchtigt alle, die den betroffenen Raum betreten. Sie dient dazu, belastende hoheitliche Maßnahmen vorzubereiten und das Verhalten der den Raum nutzenden Personen zu lenken. Das Gewicht dieser Maßnahme wird dadurch erhöht, dass in Folge der Aufzeichnung das gewonnene Bildmaterial in vielfältiger Weise ausgewertet, bearbeitet und mit anderen Informationen verknüpft werden kann. Von den Personen, die die Begegnungsstätte betreten, dürfte nur eine Minderheit gegen die Benutzungssatzung oder andere rechtliche Vorgaben, die sich aus der allgemeinen Rechtsordnung für die Benutzung der Begegnungsstätte ergeben würden, verstoßen. Die Videoüberwachung und die Aufzeichnung des gewonnenen Bildmaterials erfassen daher - wie bei solchen Maßnahmen stets - überwiegend Personen, die selbst keinen Anlass schaffen, dessentwegen die Überwachung vorgenommen wird.

- Angesichts des erheblichen Gewichts der Grundrechtsbeeinträchtigung kann eine derartige Videoüberwachung nicht auf die allgemeinen Vorschriften des Art. 16 Abs. 1 und Art. 17 Abs. 1 BayDSG gestützt werden. Diese Ermächtigungsgrundlage enthält keine hinreichenden Vorgaben für eine Videoüberwachung öffentlicher Plätze.

  Im Beschluss des BVerfG heißt es dazu, Art. 16 Abs. 1 BayDSG normiere eine allgemeine Regelung für Datenerhebungen durch staatliche Stellen. Diese Norm knüpfe lediglich an die Zuständigkeit der jeweils handelnden Behörde an und begrenze die Datenerhebung lediglich durch das Gebot der Erforderlichkeit. Aufgaben- oder bereichsspezifische Voraussetzungen der Datenerhebung würden fehlen. Das in Art. 16 Abs. 1 BayDSG enthaltene Gebot der Erforderlichkeit könne die behördliche Praxis nicht hinreichend anleiten oder Kontrollmaßstäbe bereit stellen, wenn es

nicht auf ein näher beschriebenes Normziel ausgerichtet werde. Die Norm biete daher keine hinreichenden Maßstäbe für die Beurteilung der Rechtmäßigkeit einer Videoüberwachung. Auch könne der Einzelne auf dieser Grundlage nicht vorher sehen, bei welcher Gelegenheit, zu welchem Zweck und auf welche Weise Informationen über ihn erhoben werden dürfen.

Art. 17 Abs. 1 BayDSG, der die Speicherung, Veränderung und Nutzung der erhobenen Daten regle, enthalte gleichfalls keine hinreichenden Vorgaben für Anlass und Grenzen der erfassten datenbezogenen Maßnahmen, um als Ermächtigungsgrundlage für den beabsichtigten Grundrechtseingriff in Betracht zu kommen. Neben dem Gebot der Erforderlichkeit werde zwar auch der Erhebungszweck als Grenze der Datenverwendung genannt. Da jedoch Art. 16 Abs. 1 BayDSG den Erhebungszweck nicht näher umschreibe, verweise Art. 17 Abs. 1 BayDSG für Daten, die nach dieser Norm erhoben worden seien, gleichfalls lediglich auf die Zuständigkeitsordnung.

- Eine Videoüberwachung öffentlicher Einrichtungen mit Aufzeichnung des gewonnenen Bildmaterials kann auf der Grundlage einer hinreichend bestimmten und normenklaren Ermächtigungsgrundlage verfassungsgemäß sein.

  Das BVerfG führt dazu aus, es sei nicht ausgeschlossen, dass eine Videoüberwachung öffentlicher Einrichtungen mit Aufzeichnung des gewonnenen Bildmaterials auf der Grundlage einer hinreichend bestimmten und normenklaren Ermächtigungsgrundlage materiell verfassungsgemäß sein könne, wenn für sie ein hinreichender Anlass bestehe und Überwachung sowie Aufzeichnung insbesondere in räumlicher und zeitlicher Hinsicht und im Hinblick auf die Möglichkeit der Auswertung der Daten das Übermaßverbot wahren würden.

Aus der Entscheidung des BVerfG lassen sich insbesondere folgende Erkenntnisse ziehen:

- Der Beschluss des BVerfG hat den Blickwinkel vom Objekt, das videografiert werden soll, zum einzelnen sich korrekt verhaltenden und daher „unschuldigen“ Bürger verlagert. Der Beschluss entspricht damit dem Gedankengang der Rasterfahndungsentscheidung des BVerfG; auch hier ist die Tatsache der Einbeziehung einer Vielzahl unschuldiger Bürger maßgeblich für die Bewertung des Eingriffs in das informationelle Selbstbestimmungsrecht. Insoweit wird mit dem aktuellen Beschluss des BVerfG das Koordinatensystem grundsätzlich verändert, als nun gefragt werden muss: welchen hinreichenden Grund oder Anlass habe ich, den unschuldigen bzw. unverdächtigen Bürger hier zu videografieren?

- Der Beschluss des BVerfG hat erhebliche Auswirkungen weit über den entschiedenen Einzelfall hinaus. Eine Videoüberwachung im öffentlichen Raum mit Aufzeichnung des gewonnenen Bildmaterials ist künftig nur noch auf einer bereichsspezifischen Rechtsgrundlage, die den Anforderungen des BVerfG entspricht, zulässig.

### 9.2 Regelung der Videoüberwachung im Bayerischen Datenschutzgesetz

In Bayern konnte sich in der Vergangenheit lediglich die Polizei auf bereichsspezifische Vorschriften zur Videoüberwachung stützen (Art. 32 Abs. 2 Polizeiaufgabengesetz sowie §§ 12 a und 19 a Versammlungsgesetz). Die Videoüberwachung durch andere bayerische öffentliche Stellen wurde auf die allgemeinen datenschutzrechtlichen Vorschriften der Art. 16 Abs. 1 und 2 Satz 1 und Art. 17 Abs. 1 und 2 Nr. 10 Bayerisches Datenschutzgesetz bzw. bei Schulen auf Art. 85 Abs. 1 Bayerisches Gesetz über das Erziehungs- und Unterrichtswesen gestützt. Das Bundesverfassungsgericht hat in seinem Beschluss vom 23.02.2007 - 1 BvR 2368/06 - allerdings festgestellt, dass eine Videoüberwachung öffentlicher Orte und Einrichtungen mit Aufzeichnung des gewonnenen Bildmaterials, bei der überwiegend Personen erfasst werden, die in keiner Beziehung zu einem konkreten Fehlverhalten stehen, nicht auf Art. 16 Abs. 1 und Art. 17 Abs. 1 Bayerisches Datenschutzgesetz (BayDSG) gestützt werden kann. Es sei jedoch nicht ausgeschlossen, dass eine derartige Videoüberwachung auf der Grundlage einer hinreichend bestimmten und normenklaren Ermächtigungsgrundlage materiell verfassungsgemäß sein könne. Als Reaktion auf den Beschluss des Bundesverfassungsgerichts hat Bayern die Videoüberwachung durch bayerische öffentliche Stellen inzwischen bereichsspezifisch in einem neuen Art. 21 a im Bayerischen Datenschutzgesetz geregelt. Auf die Polizei findet diese neue Vorschrift nur in Ausübung des Hausrechts Anwendung.

Absatz 1 Satz 1 der Vorschrift enthält die tatbestandlichen Voraussetzungen für eine Videoüberwachung. Danach ist die Erhebung (Videobeobachtung) und Speicherung (Videoaufzeichnung) personenbezogener Daten mit Hilfe von optisch-elektronischen Einrichtungen zulässig, wenn dies im Rahmen der Erfüllung öffentlicher Aufgaben oder in Ausübung des Hausrechts zum Schutz wichtiger Rechtsgüter oder zum Schutz von Kulturgütern, öffentlichen Einrichtungen, öffentlichen Verkehrsmitteln, Dienstgebäu-

den und sonstigen baulichen Anlagen öffentlicher Stellen erforderlich ist.

Erforderlich bedeutet, dass die Kenntnis der Daten zur Erreichung des Zwecks objektiv geeignet ist und im Verhältnis zu dem angestrebten Zweck auch angemessen erscheint. In der Gesetzesbegründung wird ausdrücklich darauf hingewiesen, dass mit der Einführung des Art. 21 a BayDSG keine Ausweitung der Videoüberwachung durch bayerische öffentliche Stellen beabsichtigt ist und eine flächendeckende Videoüberwachung auch weiterhin unzulässig bleibt. Eine solche ist weder erforderlich noch verhältnismäßig. Die Maßnahmen dürfen stets nur zum Schutz der genannten Güter und Orte erfolgen. In der Gesetzesbegründung wird ausdrücklich darauf hingewiesen, dass sich die Erforderlichkeitsprüfung gerade auf den Einsatz der Videotechnik beziehen muss. Es ist daher in jedem Einzelfall zu prüfen, ob es überhaupt erforderlich ist, personenbezogene Daten zu erheben und ggf. zu speichern und ob es erforderlich ist, dies mittels Videotechnik zu tun. Weiterhin sind der Anlass, der räumliche Überwachungsbereich (etwa Eingangsbereiche von öffentlichen Gebäuden, Bereiche, in denen aufgrund von Erfahrungen in der Vergangenheit auch künftig z.B. mit erheblichen Sachbeschädigungen zu rechnen ist) und der Zeitraum der Überwachung (z.B. Aufzeichnung nur während bestimmter sensibler Tages- bzw. Nachtzeiten) zu prüfen. Auch ist jeweils zu erwägen, welche Art der Videoüberwachung (Videobeobachtung, Videoaufzeichnung) zur Erreichung des Zwecks erforderlich ist.

In jedem Fall ist die Videoüberwachung in räumlicher und zeitlicher Hinsicht auf das zur Erreichung des mit der Überwachung verfolgten Zwecks notwendige Maß zu beschränken.

Nach Absatz 2 sind die Videoüberwachungen und die erhebende Stelle durch geeignete Maßnahmen erkennbar zu machen. Die Regelung ist Ausfluss des Transparenzgebots und trägt der Feststellung des Bundesverfassungsgerichts im Volkszählungsurteil Rechnung, wonach der Einzelne über die Preisgabe und Verwendung seiner Daten grundsätzlich selbst bestimmen kann.

Die Vorschrift enthält außerdem Regelungen zur Zweckbindung, zur Benachrichtigung betroffener Personen, zur Löschung gespeicherter Daten, zur datenschutzrechtlichen Freigabe sowie dem Verfahrensverzeichnis und der Einbindung des behördlichen Datenschutzbeauftragten.

In dem Gesetzgebungsverfahren bin ich von Anfang an beteiligt worden. Dabei konnte ich u.a. erreichen, dass in Absatz 1 Satz 2 ausdrücklich geregelt wird, dass eine Videoüberwachung nur zulässig ist, wenn keine Anhaltspunkte dafür bestehen, dass überwiegende schutzwürdige Interessen der Betroffenen beeinträchtigt werden. Die schutzwürdigen Interessen der von einer Videoüberwachung betroffenen Personen sind zwar schon in die Prüfung der Erforderlichkeit der Maßnahme einzubeziehen. Da die personenbezogene Videoüberwachung jedoch einen erheblichen Grundrechtseingriff darstellt, sollen die schutzwürdigen Interessen der Betroffenen im Gesetzestext besonders hervorgehoben werden. In der Gesetzesbegründung wurde außerdem ausdrücklich klargestellt, dass die Videoüberwachung in räumlicher und zeitlicher Hinsicht auf das zur Erreichung des mit der Überwachung verfolgten Zwecks notwendige Maß zu beschränken ist.

### 9.3 Erhebung des Fingerabdrucks als Nachweis der Zutrittsberechtigung zu Schwimmbädern

Im Berichtszeitraum war ich mit der Erhebung von Fingerabdrücken durch bayerische öffentliche Stellen als Betreiber von Schwimmbädern befasst. Dazu wird aus dem Fingerabdruck von Dauerkarteninhabern ein individueller Zahlencode generiert und gespeichert. Bei Betreten des Schwimmbads legt der Kunde seinen Finger auf einen Zugangsautomaten und weist damit seine Zutrittsberechtigung nach. Nach Auskunft der Schwimmbadbetreiber soll mit der Einführung des Fingerprintsystems der Missbrauch von personengebundenen Saison- und Jahreskarten unterbunden werden. Außerdem müsse sich der Karteninhaber nicht mehr an der Kasse anstellen. Über das Verfahren wurde im Herbst vergangenen Jahres in der Presse umfassend berichtet. Ich halte die Erhebung eines Fingerabdrucks als Nachweis der Zutrittsberechtigung unter folgenden Voraussetzungen für zulässig:

- Die Betroffenen sind über das Verfahren aufgeklärt worden und haben in die Erhebung des Fingerabdrucks eingewilligt (vgl. Art. 15 Abs. 1 Nr. 2 Bayerisches Datenschutzgesetz - BayDSG). Die Einwilligung bedarf grds. der Schriftform (Art. 15 Abs. 3 Satz 1 BayDSG).

  Die Einwilligung muss freiwillig sein. Freiwilligkeit ist nur dann gegeben, wenn die Saison- bzw. Jahreskarten auch ohne Fingerabdruck und zum selben Preis erworben werden können. Der Bürger muss also eine echte Wahlmöglichkeit haben.

- Die gespeicherten Daten unterliegen einer strikten Zweckbindung, d.h. sie dürfen nur als Nachweis der Zutrittsberechtigung genutzt werden.

- Nur berechtigte Bedienstete haben Zugriff auf die Daten.

- Die Daten werden unverzüglich nach Ablauf bzw. Rückgabe der Saison- bzw. Jahreskarte gelöscht.

Ungeachtet der grundsätzlichen Zulässigkeit der Erhebung des Fingerabdrucks mit informierter Einwilligung der Betroffenen zu Zwecken der Einlasskontrolle dürfen die dadurch entstehenden Gefahren, z.B. einer zweckändernden Nutzung, einer Einstellung in zentrale Dateien und ein Unterlassen der fristgerechten Löschung des Fingerabdrucks nicht außer Acht gelassen werden. Die Bürger sollten deshalb sorgfältig überlegen, ob ihnen ein erleichterter Zugang zum Schwimmbad die Erhebung und Speicherung ihres Fingerabdrucks wert ist.

## 9.4 Inanspruchnahme privater Inkassounternehmen durch Kommunen in Verwaltungsvollstreckungsverfahren

Erneut war ich mit Fällen befasst, in denen Kommunen private Inkassounternehmen in Verwaltungsvollstreckungsverfahren eingeschaltet hatten. Ich vertrete dazu aus datenschutzrechtlicher Sicht folgende Auffassung:

Es gehört zu den Aufgaben der Kommunen, ihre öffentlich-rechtlichen und privatrechtlichen Forderungen beizutreiben. Der Gesetzgeber hat ihnen dazu das erforderliche rechtliche Instrumentarium zur Verfügung gestellt. Die Art. 18 ff. des Bayerischen Verwaltungszustellungs- und Vollstreckungsgesetzes (VwZVG) ermöglichen ihnen die Vollstreckung ihrer Verwaltungsakte. Die Beitreibung der Abgaben ist nach Maßgabe der Art. 18 ff. VwZVG Sache des Kassenverwalters (Widtmann/Grasser, Bayerische Gemeindeordnung, Exkurs zu Art. 22 Rdnr. 13). Die Durchführung der Vollstreckung der Geldforderungen der Gemeinden und Gemeindeverbände ist in Art. 26 VwZVG geregelt (siehe dazu auch Bauer/Böhle/Ecker, Bayerische Kommunalgesetze, Art. 22 Rdnr. 99). Das Gesetz sieht dabei für das umfassend und bereichsspezifisch geregelte Verfahren der Durchsetzung hoheitlicher Akte im Zwangswege die Möglichkeit der Forderungsbeitreibung durch Private nicht vor.

Soweit in diesem Zusammenhang Art. 101 der Gemeindeordnung, der die Besorgungen von Kassen- und Rechnungsgeschäften durch eine Stelle außerhalb der Gemeindeverwaltung zulässt, zitiert wird, ist darauf hinzuweisen, dass der Gesetzgeber bei dieser Regelung speziell an die Möglichkeit gedacht hat, dass einzelne Gemeinden die Kassen- und Rechnungsgeschäfte durch eine größere Nachbargemeinde, die über eine entsprechende Anlage verfügt, erledigen können (siehe Widtmann/Grasser, a.a.O., Art. 101 Rdnr. 1). Eine Übertragung von Befugnissen, welche Eingriffe in Rechte Dritter ermöglichen, lässt diese Vorschrift nicht zu (siehe Bauer/Böhle/Ecker, a.a.O., Art. 101 Rdnr. 4 sowie Widtmann/Grasser, a.a.O., Art. 101 Rdnr. 5).

Eine Aufgabenübertragung auf Dritte zur Forderungsbeitreibung wäre danach unzulässig. Zulässig ist lediglich eine Übertragung von Hilfstätigkeiten im Rahmen einer Auftragsdatenverarbeitung nach Art. 6 BayDSG. Eine Auftragsdatenverarbeitung liegt vor, wenn

- dem Auftragnehmer die Entscheidungsbefugnis über die Daten fehlt und er bei der Verarbeitung unselbstständig tätig und den Weisungen des Auftraggebers unterworfen ist;

- der Auftragnehmer in vollständiger Abhängigkeit hinsichtlich der Art und des Umgangs und nach den Vorgaben des Auftraggebers die Daten erhebt und/oder verwendet, gleichsam als „verlängerter Arm“ für den Auftraggeber mit den Daten umgeht, nur Hilfs- bzw. Unterstützungsfunktionen ausübt;

- sich der Auftragsschwerpunkt in erster Linie auf die technische Durchführung der Datenverarbeitung richtet.

Unzulässig wäre danach eine Übertragung von Tätigkeiten, bei der das Inkassounternehmen im jeweiligen Einzelfall über das Vorgehen gegen den Schuldner und die Art und konkrete Ausgestaltung der dabei zu treffenden Maßnahmen entscheiden würde.

Das Bayerische Staatsministerium des Innern, das ich in der Angelegenheit um Stellungnahme gebeten habe, weist aus vollstreckungsrechtlicher Sicht auf Folgendes hin:

Für die Einbeziehung von Inkassounternehmen in die Verwaltungsvollstreckung wäre eine ausdrückliche gesetzliche Regelung erforderlich. Die allgemeine Regelung des Art. 101 GO, wonach Kassengeschäfte auf Dritte übertragen werden können, reiche insoweit nicht aus, wenngleich gemäß § 42 Abs. 2 KommHV-Kameralistik, bzw. § 38 Abs. 2 KommHV-Doppik die Vollsteckung zu den Kassengeschäften gehöre.

Bei der Beitreibung von Geldforderungen im Verwaltungszwangsverfahren als Teil der Eingriffsverwaltung verlange der Grundsatz des Vorbehalts des Gesetzes für staatliche Maßnahmen eine gesetzliche Grundlage. Das Bayerische Verwaltungszustellungs- und Vollstreckungsgesetz regle demgemäß die Voraussetzungen der Vollstreckung, die Zuständigkeiten der Vollstreckungsbehörden, die zur Vornahme von Vollstreckungsmaßnahmen ermächtigten Personen, Eingriffsbefugnisse sowie das Verfahren. Eine Übertragung von hoheitlichen Vollstreckungsmaßnahmen oder Teilaufgaben hiervon auf Private sei dabei nicht vorgesehen.

Erst die besondere behördliche Bindung der Exekutive an Recht und Gesetz, insbesondere die Grundrechte, zusammen mit den besonderen Regelungen zu Verfahren und ermächtigten Vollstreckungspersonen würden den Verzicht auf einen gerichtlichen Titel als Voraussetzung für die Vollstreckung der Forderung legitimieren. Die Regelungen des VwZVG seien vor diesem Hintergrund als abschließend anzusehen. Einer Beauftragung von Privaten mit (Teil-)Aufgaben der Vollstreckung würden daher Vorrang und Vorbehalt des Gesetzes entgegenstehen.

Nach alledem würden vollstreckungsrechtlich als Tätigkeiten, die auf private Inkassobüros übertragen werden könnten, nur Hilfstätigkeiten verbleiben. Um solche handle es sich, wenn jeder einzelne Schritt von der Kommune vorgegeben werde und diese jede einzelne Entscheidung selbst treffe. Die im IMS vom 03.01.1994 genannte Adressermittlung oder Mahnabteilung könne im Einzelfall eine solche Tätigkeit sein. Werde dagegen die konkrete Vorgehensweise gegenüber dem Schuldner von Inkassounternehmen bestimmt, z.B. durch die ausschließliche Wahrnehmung von Korrespondenz und Kontakten mit dem Schuldner, die Sammlung von Informationen über dessen Vermögenslage oder durch den Abschluss von Ratenzahlungsvereinbarungen, so sei die Grenze zulässiger Aufgabenübertragung in aller Regel überschritten.

Auch wenn danach im Ergebnis eine Übertragung von reinen Hilfstätigkeiten auf Inkassounternehmen im Rahmen einer Auftragsdatenverarbeitung nach Art. 6 BayDSG grundsätzlich zulässig ist, ist doch zu berücksichtigen, dass hier in aller Regel sensible Bereiche betroffen sind und dem Inkassounternehmen schutzwürdige personenbezogene Daten des Schuldners (wie z.B. die Tatsache der Zahlungsunfähigkeit) bekannt werden können. Ein Outsourcing kann deshalb aus datenschutzrechtlicher Sicht generell nicht befürwortet werden.

### 9.5 Datenschutz bei Bürgerbegehren

Auch in den vergangenen beiden Jahren haben mich Betroffene um die Überprüfung von Bürgerbegehren gebeten, an denen sie sich mit der Eintragung in Unterschriftenlisten beteiligt hatten. In einem Fall nahmen Mitarbeiter einer Rundfunkanstalt einen Bericht zu einem Bürgerbegehren in der Gemeinde auf, der am Abend des gleichen Tages im Fernsehen ausgestrahlt wurde. In dem gesendeten Fernsehbericht wurden Unterschriftenlisten mit personenbezogenen Daten von Unterstützern des Bürgerbegehrens gezeigt. Zu erkennen waren - auch ohne Einstellung des Standbildes - Nachnamen und Geburtsdaten von Unterzeichnern der Listen sowie teilweise auch die Vornamen und Straßenbezeichnungen. Nach Mitteilung der betroffenen Kommune hatte ein Mitarbeiter des Rundfunks die Unterschriftenlisten in der Gemeindeverwaltung durchgeblättert und der Kameramann hatte diesen Vorgang gefilmt.

Diesen Sachverhalt habe ich aus datenschutzrechtlicher Sicht wie folgt bewertet:

Art. 18 a GO enthält keine Regelung über das Sammeln der Unterschriften für ein Bürgerbegehren. Dieses erfolgt nach der gängigen Praxis im Privatbereich. Sobald die Unterschriftenlisten allerdings bei der Gemeinde abgegeben worden sind, unterliegen sie den einschlägigen gesetzlichen Bestimmungen. Sie dürfen daher nur unter den Voraussetzungen der Art. 15 ff. BayDSG verarbeitet oder genutzt werden. Eine Auswertung der Unterschriftenlisten ist danach nur hinsichtlich der Frage zulässig, ob das Bürgerbegehren von einer ausreichenden Zahl unterschriftsberechtigter Gemeindebürger unterschrieben worden ist (Art. 18 a Abs. 5 und 6 GO). Eine Einsichtnahme in die Listen durch den Gemeinderat bzw. ein von diesem beauftragtes Gemeinderatsmitglied kommt nur im Rahmen des Vollzugs des Art. 30 Abs. 3 GO in nicht-öffentlicher Sitzung oder in den Amtsräumen in Betracht. Eine Bekanntgabe der Unterschriften an Dritte oder an die Öffentlichkeit wäre unzulässig. Die betroffenen Bürger müssen darauf vertrauen können, dass ihre Daten entsprechend den einschlägigen gesetzlichen Bestimmungen vertraulich behandelt werden und im Bereich der Verwaltung und des zuständigen Entscheidungsgremiums verbleiben.

Im vorliegenden Fall stellte das Überlassen personenbezogener Unterschriftenlisten des Bürgerbegehrens an Mitarbeiter der Rundfunkanstalt eine unzulässige Datenübermittlung dar. Die Gemeinde war für die Einhaltung der datenschutzrechtlichen Bestimmungen im Umgang mit den in ihrer Obhut befindlichen Unterschriftenlisten verantwortlich und hätte ein Durchblättern und Aufzeichnen der Listen durch Mitarbeiter des Rundfunks verhindern müssen. Zulässig wäre lediglich eine Übersichtsaufnahme der Unterschriftenlisten ohne die Möglichkeit der Identifizierung einzelner Unterzeichner gewesen.

Den Datenschutzverstoß habe ich nach Art. 31 Abs. 1 BayDSG beanstandet. Ein Absehen von der Beanstandung kam nicht in Betracht, weil die Fernsehaufzeichnung der personenbezogenen Daten der Unterzeichner des Bürgerbegehrens keinen unerheblichen Datenschutzverstoß darstellte und ein derartiger Vorgang geeignet ist, auf Unterzeichner des Bürgerbegehrens eine abschreckende Wirkung auszuüben und sie davon abzuhalten, sich künftig nochmals an dem gesetzlich ausdrücklich vorgesehenen Rechtsinstitut des Bürgerbegehrens zu beteiligen.

### 9.6 Weitergabe von Unterschriftenlisten innerhalb der Stadtverwaltung und an einen privaten Dritten

Bürger haben sich bei mir darüber beschwert, dass der Oberbürgermeister einer Stadt einen Bürgerantrag einschließlich der dazu eingereichten Unterschriftenlisten an alle Amtsleiter der Stadt und an ein privates Planungsbüro weitergeleitet hat.

Wie bei Bürgerbegehren nach Art. 18 a GO unterliegen die Unterschriftenlisten für Bürgeranträge nach Art. 18 b GO den einschlägigen gesetzlichen Bestimmungen, sobald sie bei der Gemeinde abgegeben worden sind. Sie dürfen daher ebenfalls nur unter den Voraussetzungen der Art. 15 ff. BayDSG verarbeitet oder genutzt werden. Eine Auswertung der Unterschriftenlisten ist nur hinsichtlich der Frage zulässig, ob der Bürgerantrag von einer ausreichenden Zahl unterschriftsberechtigter Gemeindebürger unterschrieben worden ist (Art. 18 b Abs. 3 GO).

Im vorliegenden Fall wäre es zur Bearbeitung des Bürgerantrags ausreichend gewesen, diesen mit der entsprechenden Begründung, aber ohne die Unterschriftenlisten an die zuständigen Stellen weiterzuleiten. Die Weiterleitung der Unterschriftenlisten an die Amtsleiter und an das Planungsbüro war daher unzulässig und wurde von mir beanstandet.

### 9.7 Behandlung sensibler personenbezogener Daten in öffentlicher Gemeinderatssitzung

Ein Bürger hat sich bei mir darüber beschwert, dass die Herzkrankheit seines Vaters in öffentlicher Gemeinderatssitzung bekannt gemacht wurde. Der Bürger hatte bei der Gemeinde einen Antrag auf Aufnahme seiner Anliegerstraße in den Räum- und Streuplan der Kommune gestellt und zur Begründung insbesondere auf die Herzkrankheit seines Vaters hingewiesen. Die von mir befragte Gemeinde teilte dazu mit, der Antrag auf Durchführung des regelmäßigen Winterdienstes in der Anliegerstraße des Petenten sei wegen des öffentlichen Interesses in öffentlicher Gemeinderatssitzung behandelt worden. Dabei seien auch die Antragsgründe öffentlich dargelegt worden. In der Presseberichterstattung über die Gemeinderatssitzung wurde die Öffentlichkeit auch über den Antrag des Petenten unter Nennung seines Namens und einem Hinweis auf die Herzkrankheit seines Vaters informiert. Ich habe den Vorgang aus datenschutzrechtlicher Sicht wie folgt bewertet:

Nach Art. 52 Abs. 2 Satz 1 der Gemeindeordnung (GO) sind Sitzungen des Gemeinderats öffentlich, soweit nicht Rücksichten auf das Wohl der Allgemeinheit oder auf berechtigte Ansprüche Einzelner entgegenstehen. Berechtigte Ansprüche Einzelner sind nicht erst Ansprüche im Rechtssinn, sondern auch rechtlich geschützte oder anerkannte Interessen einzelner Personen oder Personengesellschaften, z.B. die Vermeidung des Bekanntwerdens persönlicher oder wirtschaftlicher Verhältnisse, an deren öffentlicher Erörterung die Allgemeinheit kein Interesse hat und deren Bekanntgabe für den Einzelnen nachteilig sein kann. Es genügt die Möglichkeit ihrer Beeinträchtigung (Bauer/Böhle/Ecker, Bayerische Kommunalgesetze, Art. 52 GO Rdnr. 12).

Im vorliegenden Fall hatte insbesondere der Vater des Petenten ein schutzwürdiges Interesse daran, dass sein Gesundheitszustand und seine persönlichen Lebensumstände weder der Allgemeinheit bekannt gegeben noch öffentlich erörtert werden. Die Angelegenheit hätte daher nicht in öffentlicher Sitzung der Gemeinde behandelt werden dürfen.

Darüber hinaus verstieß die Bekanntgabe der Herzkrankheit des Vaters des Petenten in öffentlicher Gemeinderatssitzung auch gegen Art. 15 Abs. 7 Satz 1 BayDSG. Nach dieser Vorschrift ist die Erhebung, Verarbeitung und Nutzung besonders sensibler personenbezogener Daten, zu denen auch Daten über die Gesundheit gehören, über die allgemeinen Zulässigkeitsvoraussetzungen des Dritten Abschnitts des Bayerischen Datenschutzgesetzes hinaus nur unter den in den Nummern 1 bis 9 dieser Vorschrift genannten Voraussetzungen zulässig. Im vorliegenden Fall war keine dieser Voraussetzungen gegeben.

Den Datenschutzverstoß habe ich nach Art. 31 Abs. 1 BayDSG beanstandet.

### 9.8 Weitergabe von Adressdaten an den Feuerwehrverein

Ein kommunales Versorgungswerk, das insbesondere Aufgaben im Rahmen der Daseinsvorsorge wahrnimmt, hat auf Anfrage dem örtlichen Feuerwehrverein die Adressen von Zweitwohnungsbesitzern übermittelt. Die Namen und Anschriften der Zweitwohnungsbesitzer hatte das Versorgungswerk zur Erfüllung seiner Aufgabe der kommunalen Daseinsvorsorge erhalten. Der Feuerwehrverein nutzte die erhaltenen Daten für persönlich adressierte Werbeschreiben an die Zweitwohnungsbesitzer. Diese wurden in den Schreiben gebeten, förderndes Mitglied der Freiwilligen Feuerwehr e.V. zu werden bzw. eine Spende zu leisten. Betroffene Zweitwohnungsbesitzer beschwerten sich darauf hin bei mir über die Weitergabe ihrer Adressdaten von dem Versorgungswerk an den Feuerwehrverein.

Die Datenübermittlung vom Versorgungswerk, einem Eigenbetrieb der Kommune, an den Feuerwehrverein als nicht-öffentliche Stelle beurteilte sich nach Art. 19 Abs. 1 BayDSG. Art. 19 Abs. 1 Nr. 1 BayDSG schied als Rechtsgrundlage aus, weil die

Weitergabe der personenbezogenen Daten der Zweitwohnungsbesitzer keine Maßnahme im Rahmen der kommunalen Daseinsvorsorge war, zur Aufgabenerfüllung des kommunalen Versorgungswerks somit nicht erforderlich war und auch nicht zu diesem Zweck erfolgte. Die Datenübermittlung war auch nicht nach Art. 19 Abs. 1 Nr. 2 BayDSG zulässig. Nach dieser Vorschrift ist die Übermittlung personenbezogener Daten an nicht-öffentliche Stellen zulässig, wenn die nicht-öffentliche Stelle ein berechtigtes Interesse an der Kenntnis der zu übermittelnden Daten glaubhaft darlegt und der Betroffene kein schutzwürdiges Interesse an dem Ausschluss der Übermittlung hat. Im vorliegenden Fall hatten die Zweitwohnungsbesitzer ein schutzwürdiges Interesse daran, dass das Versorgungswerk die Tatsache, dass sie Haus- und Grundbesitz in der Gemeinde haben, nicht ohne ihre Einwilligung dem Feuerwehrverein übermittelt und dass sie von persönlich adressierten Werbebriefen des Feuerwehrvereins verschont bleiben. Bei einer Abwägung der Interessen des Feuerwehrvereins an der Mitglieder- und Spendengewinnung mit den schutzwürdigen Belangen der Inhaber von Zweitwohnungen, keine Beeinträchtigung ihrer Privatsphäre durch Werbebriefe hinnehmen zu müssen, überwiegen die schutzwürdigen Belange der Inhaber von Zweitwohnungen. Abgesehen davon bestehen für die Gewinnung von Mitgliedern und Spenden auch andere Möglichkeiten (z.B. Zeitungsanzeigen, Postwurfsendungen, Informationsveranstaltungen etc.).

Von einer Beanstandung des Datenschutzverstoßes habe ich ausnahmsweise nur deshalb abgesehen, weil der erste Bürgermeister die Datenübermittlung sofort schriftlich gerügt hat und der Feuerwehrverein die erhaltenen Daten auf Aufforderung der Gemeinde unverzüglich gelöscht hat.

### 9.9 Bekanntgabe von Bauvorhaben

Nach § 1 Nr. 56 des Gesetzes zur Änderung der Bayerischen Bauordnung (BayBO) und Änderungsgesetz vom 24.07.2007 ist u.a. Art. 84 BayBO 1998 aufgehoben worden. Nach dieser Vorschrift durften die Gemeinden und die Bauaufsichtsbehörden Ort und Straße der Baustelle, Art und Größe des Bauvorhabens sowie Namen und Anschrift des Bauherrn und des Entwurfsverfassers veröffentlichen oder an Dritte zum Zwecke der Veröffentlichung übermitteln, es sei denn, der Bauherr und der Entwurfsverfasser haben der Veröffentlichung der sie betreffenden Daten widersprochen.

Art. 84 BayBO a.F. diente allein den Interessen der für die Baubranche tätigen Werbewirtschaft. Die Vorschrift wurde aufgehoben, weil sie Gemeinden und untere Bauaufsichtsbehörden mit Auskunftsbegehren belastete und die Förderung der Werbewirtschaft nicht Sache des Bauordnungsrechts ist (siehe LT-Drs. 15/7161). Eine Veröffentlichung der Daten des Bauherrn und des Entwurfsverfassers oder ihre Weitergabe an Dritte zum Zwecke der Veröffentlichung ist künftig nur noch mit Einwilligung der Betroffenen zulässig (Art. 15 Abs. 1 Nr. 2 BayDSG).

Die Aufhebung des Art. 84 BayBO a.F. ist aus datenschutzrechtlicher Sicht zu begrüßen. In der Vergangenheit erhielt ich immer wieder Anfragen von Betroffenen, die den datenschutzrechtlichen Hinweis in den amtlichen Vordrucken übersehen hatten und sich über unerwünschte Werbung ärgerten.

### 9.10 Der übereifrige Mitarbeiter

Die Verkehrsbetriebe einer Stadt hatten mit einem Bürger einen Vertrag über Jahreskarten für den öffentlichen Personennahverkehr abgeschlossen und ihm die Karten ausgehändigt. Der Bürger bezahlte die Jahreskarten jedoch nicht und war für die Verkehrsbetriebe auch nicht über die angegebene Adresse erreichbar. Der zuständige Sachbearbeiter der Verkehrsbetriebe versuchte daraufhin, den Aufenthalt des Schuldners ausfindig zu machen. Bei seinen Nachforschungen stieß er auf eine Frau gleichen Namens mit dem des Schuldners, die er irrtümlich für dessen Mutter hielt. In Wirklichkeit hatte die Frau mit dem Schuldner der Verkehrsbetriebe nichts zu tun; die Namensgleichheit war rein zufällig. Die Verkehrsbetriebe forderten in der Folge die völlig überraschte Bürgerin auf, die neue Anschrift ihres (vermeintlichen) Sohnes zu nennen, verbunden mit der Drohung, andernfalls Strafanzeige wegen Betrugs zu stellen. Die betroffene Bürgerin wandte sich daraufhin an mich.

Die Beschaffung der Adressdaten der in der Sache völlig unbeteiligten Petentin habe ich beanstandet. Aber selbst wenn es sich bei ihr um die Mutter des zahlungssäumigen Vertragspartners der Verkehrsbetriebe gehandelt hätte, wäre die Erhebung ihrer Daten durch die Verkehrsbetriebe nicht zulässig gewesen. Bei dem Käufer der Jahreskarten handelte es sich um eine volljährige, geschäftsfähige Person. Abgesehen von seltenen unterhaltsrechtlichen Sondersituationen sind Eltern volljähriger und geschäftsfähiger Kinder nicht verpflichtet, Auskünfte über ihre Kinder an deren Vertragspartner zu erteilen, geschweige denn eventuelle Zahlungsverpflichtungen aus deren Vertragsverhältnis zu übernehmen.

Ein weiterer Datenschutzverstoß, denn ich ebenfalls beanstandet habe, lag in der Übermittlung personenbezogener Daten des Vertragspartners der Verkehrsbetriebe an die Petentin. Dieser wurde in dem Schreiben der Verkehrsbetriebe, in dem sie aufgefordert wurde, die neue Anschrift ihres vermeintlichen Sohnes mitzuteilen, unzulässigerweise offenbart, dass ihr angeblicher Sohn einen Vertrag über Jahreskarten mit den Verkehrsbetrieben abgeschlossen hatte, ihm die

Karten ausgehändigt wurden, in welcher Straße er bisher gewohnt hatte und dass die Verkehrsbetriebe erwägten, einen Strafantrag wegen Betrugs zu stellen.

# 10 Einwohnermeldewesen

## 10.1 Neuordnung des Meldewesens

Im Zuge der Föderalismusreform wurde das Meldewesen zum 01.09.2006 in die ausschließliche Gesetzgebungskompetenz des Bundes überführt. Nach den Plänen des federführenden Bundesministeriums des Innern sollen die Regelungen des Melderechtsrahmengesetzes und der Meldegesetze der Länder zusammengeführt und in Ergänzung der bisherigen kommunalen Melderegister ein Bundesmelderegister aufgebaut werden.

Die Neuordnung des Melderechts darf nicht zu einer Verringerung des bestehenden Datenschutzniveaus führen. Es sollte damit vielmehr eine Verbesserung des Datenschutzes erreicht werden. Aus datenschutzrechtlicher Sicht sind daher an ein Bundesmeldegesetz insbesondere folgende Forderungen zu stellen:

- Für die Errichtung eines zentralen Bundesmelderegisters besteht keine Notwendigkeit. Die Modernisierung des Meldewesens kann auch durch eine Vernetzung der vorhandenen Melderegister erreicht werden.

- Ein Bundesmeldegesetz müsste zudem dem verfassungsrechtlichen Verbot eines einheitlichen und verwaltungsübergreifenden Identifikationsmerkmals genügen. In diesem Zusammenhang sollte auf die Speicherung fremder bereichsspezifischer Identifikationsmerkmale, wie z.B. die Steueridentifikationsnummer, verzichtet werden.

- Bei einer Reform des Melderechts sollte weiter der Umfang der gespeicherten Daten auf das erforderliche Maß beschränkt werden. Auf die Speicherung von Daten, die dem originären Zweck der Melderegister, Identität und Wohnsitz der Einwohner festzustellen und zu registrieren, widersprechen (z.B. Waffenerlaubnis, Sprengstofferlaubnis), sollte deshalb verzichtet werden.

- Die Neuordnung des Meldewesens sollte außerdem zum Anlass genommen werden, die Rechte der Bürger zu stärken. Dazu sollten bestehende Widerspruchsregelungen (z.B. bei Melderegisterauskünften an Parteien zu Wahlwerbezwecken) durch Einwilligungslösungen ersetzt und das Auskunftsrecht der Betroffenen verbessert werden.

Das Gesetzgebungsverfahren wird von einer Arbeitsgruppe der Datenschutzbeauftragten des Bundes und der Länder begleitet.

## 10.2 Erlass einer Meldedatenverordnung

Im Gesetz über das Meldewesen (MeldeG) vom 08.12.2006 (GVBl S. 990) wurden bundesrechtliche Vorgaben des Melderechtsrahmengesetzes in Landesrecht umgesetzt. Ich habe mich dazu im 22. Tätigkeitsbericht 2006 unter der Nr. 9.1 geäußert. Als nächsten Schritt hat das Bayerische Staatsministerium des Innern die Verordnung zur Übermittlung von Meldedaten (Meldedatenverordnung - MeldDV) vom 14.03.2007 erlassen (GVBl S. 244), die inzwischen durch die Verordnung zur Änderung der Meldedatenverordnung zum 18.08.2007 (GVBl S. 628) geändert wurde. Im Verfahren zum Erlass der Meldedatenverordnung wurde ich beteiligt.

Die Meldedatenverordnung ersetzt die bisherige Bayerische Meldedaten-Übermittlungsverordnung (BayMeldeDÜV). Sie enthält u.a. folgende wichtige Regelungen:

- In den §§ 2 und 3 der Verordnung werden die Einzelheiten der elektronischen Rückmeldung zwischen bayerischen Meldebehörden geregelt. Nach Art. 27 Abs. 1 i.V.m. Art. 39 MeldeG dürfen Rückmeldungen seit dem 01.01.2007 nur noch elektronisch erfolgen. Dies setzt in allen Ländern gleiche Melderegisterinhalte und eine standardisierte elektronische Kommunikation voraus. Art. 27 Abs. 4 MeldeG ermächtigt das Staatsministerium des Innern insoweit, das Nähere über das Verfahren, insbesondere die Art und Form der zu übermittelnden Daten, durch Verordnung zu regeln.

- In § 5 wird die bayerische Vermittlungsstelle für elektronische Rückmeldungen von bzw. an bayerische Meldebehörden, die nicht in der erforderlichen Form und mit der nötigen Datensicherheit elektronisch kommunizieren können, bestimmt.

- Die Verordnung trägt dem Bedürfnis vieler Behörden und sonstiger öffentlicher Stellen nach einem Abgleich mit den Melderegisterdaten eines Einwohners, sei es durch Datenübermittlung der Meldebehörden oder durch Abrufe aus dem Melderegister, durch entsprechende Regelungen Rechnung. Auch das Nähere zur Erteilung elektronischer Melderegisterauskünfte wird in der Verordnung geregelt. Um den Eingriff in die bestehenden Strukturen im Meldewesen in Bayern im Rahmen der Umsetzung der Föderalismusreform möglichst gering zu halten, wurde der bei der Anstalt für

Kommunale Datenverarbeitung in Bayern (AKDB) vorhandene Teildatenbestand erweitert. Nach § 6 MeldDV mussten dazu die bayerischen Meldebehörden ihren Melderegisterdatenbestand erstmals bis 30.06.2007 und seither Änderungen tagesaktuell und elektronisch an die AKDB übermitteln. Aus diesem Datenbestand können die bayerischen öffentlichen Stellen Adressdaten einzelner Personen unter den in § 7 MeldDV geregelten Voraussetzungen automatisiert abrufen (allgemeines Behördeninformationssystem). Welche Daten darüber hinaus von welchen Behörden zu welchen Zwecken abgerufen werden können bzw. welche Datenübermittlungen die Meldebehörden vornehmen müssen, ist in den §§ 8 bis 31 MeldDV geregelt. In § 33 MeldDV wird festgelegt, unter welchen Voraussetzungen aus dem bei der AKDB geschaffenen Datenbestand einfache Melderegisterauskünfte im elektronischen Verfahren an private Dritte zulässig sind.

- §§ 34 und 35 MeldDV enthalten Regelungen zu Beschränkungen von regelmäßigen Datenübermittlungen wegen Auskunftssperren und zu Sicherungsmaßnahmen.

### 10.3 Melderegisterauskünfte für Wahlwerbezwecke

Vor den Gemeinde- und Landkreiswahlen am 02.03.2008 und der Wahl zum Bayerischen Landtag und den Bezirkstagen am 28.09.2008 haben mich wieder zahlreiche Anfragen und Beschwerden von Bürgern erreicht, die von Parteien persönlich adressierte Wahlwerbung erhalten hatten und wissen wollten, wie die Parteien an ihre Adressdaten gekommen sind. Dazu musste ich die betroffenen Bürger auf die besondere Regelung des Art. 32 Abs. 1 des Meldegesetzes hinweisen. Nach dieser Vorschrift 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 Familienname, Doktorgrad und Anschriften von Gruppen von Wahlberechtigten erteilen, für deren Zusammensetzung das Lebensalter der Betroffenen bestimmend ist, es sei denn, die Betroffenen haben dieser Weitergabe ihrer Daten widersprochen. Hierauf sind sie bei der Anmeldung und spätestens acht Monate vor den Wahlen durch öffentliche Bekanntmachung hinzuweisen.

Wie die Erfahrung gezeigt hat, erreicht die Information über die Widerspruchsmöglichkeit die Bürger häufig nicht. Sie sollte deshalb im Interesse einer konsequenten Umsetzung des Grundrechts auf informationelle Selbstbestimmung zum Schutz der Betroffenen im neuen Bundesmeldegesetz durch eine Einwilligungslösung ersetzt werden.

### 10.4 Übermittlung von Melderegisterdaten an den Bayerischen Rundfunk bzw. die GEZ

Ein „Dauerbrenner“ sind auch Beschwerden von verärgerten Bürgern, die Post von der Gebühreneinzugszentrale der öffentlich-rechtlichen Rundfunkanstalten (GEZ) erhalten haben und wissen wollen, wie die GEZ an ihre Daten gekommen ist. Dafür kommen mehrere Möglichkeiten in Betracht.

Zum einen beschafft sich die GEZ Daten beim kommerziellen Adresshandel. Für diese Datenübermittlung und für die Datenerhebung durch die GEZ habe ich allerdings keine Prüfungskompetenz. Diese beschränkt sich auf die Kontrolle der Datenübermittlung durch bayerische öffentliche Stellen, hier insbesondere durch die Meldebehörden, an die GEZ. Die Kontrolle der Datenerhebung, -verarbeitung und -nutzung durch die GEZ und durch den Bayerischen Rundfunk wird durch eigene unabhängige Datenschutzbeauftragte des Rundfunks ausgeübt. In Bayern können sich die Bürger dazu an die Datenschutzbeauftragte des Bayerischen Rundfunks wenden.

Neben dem Adresshandel und Datenerhebungen durch Mitarbeiter der Rundfunkanstalten (sogenannte Rundfunkgebührenbeauftragte) kommen insbesondere Datenübermittlungen nach melderechtlichen Vorschriften in Betracht. Datenübermittlungen zu einer bestimmten Person (z.B. Mitteilung der neuen Adresse eines Rundfunkteilnehmers) aber auch Gruppenauskünfte sind unter den in Art. 28 Abs. 1 Satz 1 bzw. Art. 28 Abs. 1 Satz 3 MeldeG genannten Voraussetzungen zulässig.

Den größten Teil der Datenübermittlungen nach melderechtlichen Vorschriften an die GEZ stellen wohl Datenübermittlungen nach § 31 der Meldedatenverordnung dar. Danach darf die Meldebehörde dem Bayerischen Rundfunk oder der GEZ zum Zweck der Erhebung und des Einzugs der Rundfunkgebühren im Fall der An- bzw. Abmeldung oder des Todes u.a. die Anschriften volljähriger Einwohner übermitteln.

Die vielen Beschwerden über die GEZ sowie regelmäßige Anfragen von Gemeinden, die sich mit Auskunftsersuchen des Bayerischen Rundfunks bzw. deren Rundfunkgebührenbeauftragten konfrontiert sehen, veranlassen mich, meine Forderung aus dem 22. Tätigkeitsbericht 2006 unter der Nr. 3.15 nach einer Gebührenstruktur, die mit weniger Datenerhebungen und einer geringeren Kontrolltätigkeit der GEZ verbunden ist, erneut zu stellen.

### 10.5 Die Stadt ist kein Adresshändler!

Zur Durchführung einer gemeinsamen Mailing-Aktion hatte eine Stadt mit einem Hotel vereinbart, dass das Hotel von der Stadt sowohl Adressen von Verbänden und Vereinen als auch von Personen erhält, die im Gästeamt der Stadt einen Gästeprospekt angefordert hatten. In der Folgezeit wurden dann von der Stadt an das Hotel aber nicht nur Daten von Personen, die vom städtischen Gästeamt Prospektmaterial angefordert hatten, sondern auch Namen und Anschriften aus den besonderen Meldescheinen für Beherbergungsstätten, die die Stadt zur Berechnung des Kurbeitrags von den Beherbergungsbetrieben erhalten hatte, übermittelt. Das Hotel nutzte die erhaltenen Adressen für eine hoteleigene Werbeaktion. Über die Weitergabe der Adressdaten von der Kommune an das Hotel haben sich darauf hin bei mir andere Beherbergungsbetriebe, die von ihren Gästen auf die Werbeaktion aufmerksam gemacht wurden, beschwert.

Den Vorgang habe ich aus datenschutzrechtlicher Sicht wie folgt bewertet:

- Art. 26 MeldeG enthält Nutzungsbeschränkungen für die besonderen Meldescheine für Beherbergungsstätten nach Art. 24 Abs. 2 MeldeG. Die Daten dürfen danach u.a. zur Erhebung des Fremdenverkehrsbeitrags, des Kurbeitrags sowie für Zwecke der Beherbergungs- und Fremdenverkehrsstatistiken ausgewertet und verarbeitet werden. Die Weitergabe der Meldedaten, die die Stadt zur Berechnung des Kurbeitrags von den Beherbergungsbetrieben erhalten hatte, an das Hotel widersprach der Regelung in Art. 26 MeldeG und war deshalb rechtswidrig.

- Die Weitergabe der Namen und Anschriften von Bürgern, die von der Kommune Prospektmaterial angefordert hatten, an das Hotel, war eine Übermittlung personenbezogener Daten an eine nicht-öffentliche Stelle. Als Rechtsgrundlage für die Datenweitergabe kommt Art. 19 Abs. 1 Nr. 2 BayDSG in Betracht. Die Übermittlung personenbezogener Daten an nicht-öffentliche Stellen ist danach zulässig, wenn die nicht-öffentliche Stelle ein berechtigtes Interesse an der Kenntnis der zu übermittelnden Daten glaubhaft darlegt und der Betroffene kein schutzwürdiges Interesse an dem Ausschluss der Übermittlung hat.

  Dem berechtigten Interesse der Vermieter, in Frage kommende Personen anzusprechen und für einen Aufenthalt in ihrem Haus zu gewinnen, steht das überwiegende schutzwürdige Interesse der Personen, die zentral vom Gästeamt einer Kommune Material anfordern, gegenüber, von unaufgefordert zugesandter und personenbezogener Direktwerbung verschont zu bleiben. Derjenige, der vom Gästeamt Prospektmaterial anfordert, will sich in der Regel zunächst informieren, um selbst zu entscheiden, mit welchem Vermieter er ggf. Kontakt aufnehmen möchte. Außerdem wäre es möglich, dass das Gästeamt von interessierten Vermietern zur Verfügung gestellte Hausprospekte versendet.

  Hinzu kommt, dass es sich bei der Weitergabe der Namen und Anschriften um eine Auskunft über mehrere im Auskunftsersuchen nicht namentlich bezeichnete Personen (Gruppenauskunft) handelte, die im Regelfall nach Art. 19 Abs. 1 Nr. 2 BayDSG nur erteilt werden soll, wenn sie gleichzeitig auch im öffentlichen Interesse liegt (Nr. 2 der Vollzugsbekanntmachung zum Bayerischen Datenschutzgesetz). Rein oder vorwiegend kommerzielle Interessen des Auskunftsbegehrenden, wie im vorliegenden Fall die Werbung für Leistungen des Hotels, rechtfertigen demgegenüber die Annahme eines öffentlichen Interesses nicht (siehe Wilde/Ehmann/Niese/Knoblauch, Bayerisches Datenschutzgesetz, Art. 19 Rdnr. 27).

Im Ergebnis ist somit festzuhalten, dass sowohl die Weitergabe von Daten aus den Gästemeldescheinen wie auch die Namen und Anschriften von Personen, die Prospektmaterial angefordert hatten, von der Stadt an das Hotel unzulässig war.

Da mit der Übermittlung der Adressdaten der Personen, die Prospekte angefordert hatten, keine Kundendaten von Beherbergungsbetrieben an ein Konkurrenzunternehmen weitergegeben wurden und den betroffenen Personen über die Zusendung personenbezogener Werbematerials durch das Hotel hinaus offenkundig kein weiterer Nachteil entstanden ist, habe ich für dieses Mal im Rahmen meines Ermessens nach Art. 31 Abs. 3 BayDSG insoweit von einer Beanstandung abgesehen.

Kein Absehen von einer Beanstandung war mir hingegen bei der Übermittlung der Daten aus den Gästemeldescheinen möglich, da hier gegen eine gesetzlich geregelte Nutzungsbeschränkung verstoßen wurde und außerdem nicht nur die Gäste, deren Namen weitergegeben wurden, sondern auch Beherbergungsbetriebe, deren Kundendaten an ein Konkurrenzunternehmen übermittelt wurden, betroffen waren. Diese Datenübermittlung habe ich daher nach Art. 31 Abs. 1 BayDSG beanstandet.

# 11 Steuer- und Finanzverwaltung

## 11.1 eGovernment-Projekt KONSENS

Bereits im Jahr 1989 hatten die Steuerverwaltungen der Länder mit dem Gemeinschaftsprojekt FISCUS den Versuch unternommen, das gesamte automatisierte Besteuerungsverfahren neu zu konzipieren, zu vereinheitlichen und arbeitsteilig zu realisieren. Aufgrund von nicht überwindbaren Problemen musste das Projekt jedoch nach einigen Jahren eingestellt werden. Am 09.07.2004 haben die Finanzminister der Länder eine neue Vorgehensweise beschlossen. Im Rahmen des eGovernment-Projekts KONSENS (Ko ordinierte neue Software-Entwicklung der Steuerverwaltung) soll nun gemeinsam länderübergreifend einheitliche Software für das Besteuerungsverfahren entwickelt, beschafft und eingesetzt werden. Die Finanzminister der Länder und des Bundes haben im Jahr 2006 ein entsprechendes Verwaltungsabkommen geschlossen, das am 01.01.2007 in Kraft getreten ist.

Das Projekt KONSENS umfasst eine Vielzahl von steuerlichen Fachverfahren. Auch bereits bestehende eGovernment-Anwendungen wie das Verfahren ELSTER (Elektronische Steuererklärung; siehe zuletzt Nr. 10.1 und Nr. 10.2 meines 22. Tätigkeitsberichts 2006) werden unter KONSENS weiterentwickelt. Die Entwicklung der einzelnen Fachverfahren erfolgt dabei nach dem „Prinzip des Auftrag nehmenden Landes“ („Einer für Alle“). Im Namen der Steuerverwaltungen hat deshalb das Staatsministerium der Finanzen den Wunsch an mich herangetragen, die mit dem jeweiligen Fachverfahren im Zusammenhang stehenden datenschutzrechtlichen Belange ebenfalls nur mit einem Landesdatenschutzbeauftragten abzustimmen. Diesem Wunsch hat die 74. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 25./26.10.2007 in Saalfeld jedoch mehrheitlich nicht entsprochen.

Mit der (Weiter-)Entwicklung einzelner KONSENS-Verfahren eng verknüpft sind auch einige gesetzgeberische Aktivitäten im Berichtszeitraum. Auf diese sowie auf einige ausgewählte KONSENS-Verfahren unter bayerischer Beteiligung möchte ich nachfolgend eingehen:

### 11.1.1 Steueridentifikationsnummer

Bereits durch das Steueränderungsgesetz 2003 hat der Bundestag die rechtlichen Grundlagen für ein an jeden Steuerpflichtigen dauerhaft zu vergebendes Identifikationsmerkmal geschaffen (§§ 139 a bis d AO). Um die Steueridentifikationsnummer zuteilen zu können, haben alle deutschen Meldebehörden die in § 139 b AO aufgeführten Melderegisterdaten dem Bundeszentralamt für Steuern übermittelt. Nach der ursprünglichen Planung sollte die Vergabe der Steueridentifikationsnummern durch das Bundeszentralamt für Steuern bis zum 01.01.2008 an alle Steuerpflichtigen erfolgt sein. Wohl aufgrund der stark unterschätzten praktischen Schwierigkeiten konnte die Zuteilung jedoch bis heute nicht abgeschlossen werden.

Auf diesem Wege entsteht erstmals in der Geschichte der Bundesrepublik Deutschland und dauerhaft eine zentrale Bevölkerungsdatei. Die Verwendung der beim Bundeszentralamt für Steuern gespeicherten Daten ist derzeit zwar in § 139 b AO gesetzlich strikt auf steuerliche Zwecke beschränkt. Die Erfahrungen der Vergangenheit lassen aber befürchten, dass ein derart umfassender Datenpool über kurz oder lang auch die Begehrlichkeiten anderer Verwaltungen wecken wird und damit der Weg zu einem verfassungsrechtlich unzulässigen Personenkennzeichen („gläserner Bürger“) beschritten wird. In diesem Zusammenhang darf ich auch auf die Entschließung der 75. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 03./04.04.2008 in Berlin „Datenschutzförderndes Identitätsmanagement statt Personenkennzeichen“ hinweisen (Anlage Nr. 15).

### 11.1.2 Projekt OpenELSTER

Eine erste Bestätigung dieser Befürchtung haben die Planungen für das Projekt OpenELSTER erbracht. Grundlegende Überlegung ist dabei, über das ELSTEROnline-Portal ein kostenloses Zertifikat für elektronische Behördengänge zur Verfügung zu stellen. Diese im Hinblick auf die Steigerung der Akzeptanz von eGovernment-Anwendungen an sich durchaus begrüßenswerte Überlegung wurde jedoch konterkariert durch die in einer ersten Planungsphase angedachte Übermittlung der Steueridentifikationsnummer an die beteiligten Verwaltungen zur Überprüfung der verwendeten Zertifikate. Ich musste das Staatsministerium der Finanzen darauf hinweisen, dass eine derartige Übermittlung gegen die in § 139 b AO gesetzlich festgelegte Zweckbindung des Identifikationsmerkmals ausschließlich für steuerliche Zwecke verstoßen würde.

Nach meinem derzeitigen Kenntnisstand wird die bei der Bundesregierung gebildete „eGovernment-Staatssekretärsrunde“ über eine Weiterverfolgung des Vorhabens entscheiden. Ebenso wie meine Kolleginnen und Kollegen werde ich das Vorhaben sehr kritisch weiter beobachten.

### 11.1.3 Projekt ELSTERLohn II

Mit dem Jahressteuergesetz 2008 hat der Bundestag einen neuen § 39 e EStG „Elektronische Lohnsteuerabzugsmerkmale“ beschlossen. In die bereits erwähnte zentrale Steuerdatei sollen für jeden Steuerpflichti-

gen weitere, zum Teil sensible Merkmale wie Religionszugehörigkeit (auch des Ehegatten), Steuerklasse und Freibeträge hinzugespeichert werden. Damit soll zum einen die Ablösung der bisher bekannten (Papier-) Lohnsteuerkarte durch ein elektronisches Abrufverfahren ab 2011 ermöglicht werden (Projekt ELSTERLohn II). Zum anderen soll aber auch den Kreditinstituten die Einbehaltung der Kirchensteuer auf Kapitalerträge im Rahmen der sogenannten Abgeltungssteuer erleichtert werden. Die während des Gesetzgebungsverfahrens gefasste Entschließung der 74. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 25./26.10.2007 in Saalfeld „Zentrale Steuerdatei droht zum Datenmoloch zu werden“ (Anlage Nr. 10) hat im Ergebnis keinen Niederschlag gefunden.

Bei dem künftigen elektronischen Lohnsteuerabzugsverfahren werden die Lohnsteuerabzugsmerkmale in der zentralen Datei zum automatisierten Abruf durch den Arbeitgeber bereitgehalten. Hier stellt sich insbesondere die Problematik der zuverlässigen Vermeidung von sogenannten Neugierabfragen. Es erscheint fraglich, ob die in § 39 e Abs. 4 EStG vorgesehenen Regeln für den Abruf durch den Arbeitgeber (Authentifizierung des Arbeitgebers, Angabe seiner Wirtschafts-Identifikationsnummer sowie Angabe der Steueridentifikationsnummer und des Geburtstages des jeweiligen Arbeitnehmers) unberechtigte Abrufe werden gänzlich verhindern können.

Eine vergleichbare Problematik sehe ich bei eventuellen künftigen Abrufen von Kreditinstituten zwecks Einbehaltung der Kirchensteuer auf Kapitalerträge im Rahmen der sogenannten Abgeltungssteuer. Zwar sieht § 51 a Abs. 2 e EStG vor, dass bis zum 30.06.2010 zu prüfen ist, ob die Kirchensteuer ab 2011 ausschließlich im Abzugsverfahren an der Quelle (Finanzinstitut) erhoben werden soll - hierfür benötigen die Kreditinstitute die Möglichkeit eines Abrufs der Religionszugehörigkeit ihrer Kunden aus der zentralen Steuerdatei - oder aber weiterhin nur nach Mitteilung der Religionszugehörigkeit an die Bank durch den Steuerpflichtigen bzw. im Rahmen der Einkommen- und Kirchensteuerveranlagung erhoben werden kann. Eine ergebnisoffene Evaluierung halte ich indessen für mehr als fraglich.

### 11.1.4 ELSTER-Clearingstellen

Die Problematik der in Bayern und Nordrhein-Westfalen eingerichteten Clearingstellen - als zentrale Annahme- und Verteilstellen für die im Rahmen von ELSTER eingehenden elektronischen Steuerdaten - habe ich bereits mehrfach thematisiert (siehe zuletzt Nr. 10.2 meines 22. Tätigkeitsberichts 2006). Ich habe in diesem Zusammenhang insbesondere eine Klärung der rechtlichen Stellung dieser Clearingstellen - und damit einhergehend auch der datenschutzrechtlichen Verantwortlichkeit - gefordert. Das Staatsministerium der Finanzen hat mir mitgeteilt, dass zwar - unter der Annahme, dass die Clearingstellen Datenverarbeitung im Auftrag vornähmen - das jeweils Auftrag gebende Land bzw. der Bund für die Einhaltung des Datenschutzes verantwortlich bliebe. Damit komme es eigentlich - je nach Einzelfall - zur Anwendung des jeweiligen Landesdatenschutzgesetzes bzw. des Bundesdatenschutzgesetzes. Da dies jedoch aus Sicht der Steuerverwaltung nicht praktikabel sei, sei auf Ebene der Referatsleiter Abgabenordnung des Bundes und der Länder vereinbart worden, dass für die Clearingstelle München datenschutzrechtlich der Freistaat Bayern und für die Clearingstelle Düsseldorf datenschutzrechtlich das Land Nordrhein-Westfalen zuständig sei.

Ich gehe davon aus, dass daraus auch die Anwendung der Landesdatenschutzgesetze der beiden genannten Länder folgen soll. Eine derartige Festlegung auf Verwaltungsebene vermag aber schon aus verfassungsrechtlichen Gründen die gesetzlichen Vorgaben der Datenschutzgesetze nicht auszuhebeln.

## 11.2 Automatisierte Kontenabfrage im Besteuerungsverfahren

Bereits im Jahr 2005 hatte ich die praktische Umsetzung des automatisierten Kontenabrufverfahrens bei einem bayerischen Finanzamt aus datenschutzrechtlicher Sicht geprüft. Zum damaligen Zeitpunkt war die Zahl der durchgeführten Kontenabrufe noch sehr gering. Nachdem sich das automatisierte Kontenabrufverfahren für Finanzbehörden mittlerweile etabliert hat, habe ich im Jahr 2008 erneut eine datenschutzrechtliche Prüfung bei einem bayerischen Finanzamt vorgenommen.

### 11.2.1 Rechtslage

Hinsichtlich der automatisierten Kontenabfrage im Besteuerungsverfahren stellt sich die datenschutzrechtlich relevante Rechtslage wie folgt dar:

- Zur Bekämpfung illegaler Finanztransaktionen im Bereich des Terrorismus und der organisierten Kriminalität (Geldwäsche) haben alle Kreditinstitute gem. § 24 c Kreditwesengesetz seit dem 01.04.2003 Dateien mit Kontenstammdaten (u.a. Kontonummer, Name und Geburtstag des Kontoinhabers, nicht aber: Kontostände und -bewegungen) ständig aktualisiert vorzuhalten. Auf diese Dateien kann die Bundesanstalt für Finanzdienstleistungsaufsicht automatisiert zugreifen, ggf. auf Ersuchen von Polizeien, Staatsanwaltschaften, Gerichten, Steuerfahndungs- und Zollbehörden.

Mit Wirkung vom 01.04.2005 wurden durch das „Gesetz zur Förderung der Steuerehrlichkeit“ vom 21.12.2003 in die Abgabenordnung die Bestimmungen des § 93 Abs. 7 AO und des § 93 b AO eingefügt. Seitdem ist es auch den Finanzbehörden gestattet, „zur Festsetzung oder Erhebung von Steuern“ die nach § 24 c KWG von den Kreditinstituten vorzuhaltenden Kontenstammdaten (mittelbar) über das Bundeszentralamt für Steuern und die Bundesanstalt für Finanzdienstleistungsaufsicht automatisiert abzurufen.

- Bereits mit Schreiben des Bundesministeriums der Finanzen vom 10.03.2005 wurde der Anwendungserlass zur Abgabenordnung (AEAO) um Regelungen zum automatisierten Kontenabruf ergänzt. Dabei wurde in Nummer 2.7 AEAO zu § 93 AO bestimmt: „Hat sich durch einen Kontenabruf herausgestellt, dass Konten oder Depots vorhanden sind, die der Beteiligte auf Nachfrage … nicht angegeben hat, ist er über das Ergebnis des Kontenabrufs zu informieren …. Würde durch eine vorhergehende Information des Beteiligten der Ermittlungszweck gefährdet …, kann sich die Finanzbehörde nach § 93 Abs. 1 Satz 1 unmittelbar an die betreffenden Kreditinstitute wenden …. In diesen Fällen ist der Beteiligte nachträglich über die Durchführung des Kontenabrufs zu informieren.“ In Nummer 2.8 AEAO zu § 93 AO heißt es: „Wurden die Angaben des Beteiligten durch einen Kontenabruf bestätigt, ist der Beteiligte gleichwohl über die Durchführung des Kontenabrufs zu informieren, z.B. durch eine Erläuterung im Steuerbescheid: „Es wurde ein Kontenabruf nach § 93 Abs. 7 AO durchgeführt.“

- Das Bundesverfassungsgericht hat in seinem Beschluss vom 13.06.2007 (Az. 1 BvR 1550/03) die Verfassungsbeschwerden gegen § 93 Abs. 7 AO i.V.m. § 93 b AO zwar im Ergebnis verworfen. Bereits in dem vorausgehenden Verfahren über den Antrag auf Erlass einer einstweiligen Anordnung hatte das Bundesverfassungsgericht aber aus Transparenz- und Rechtsschutzgründen eine zumindest nachträgliche, zeitnahe Information des Steuerpflichtigen über einen durchgeführten Kontenabruf für erforderlich gehalten (vgl. Rdnr. 60 ff. des Beschlusses vom 22.03.2005; Az. 1 BvR 2357/04). Zudem folgen nach Ansicht des Bundesverfassungsgerichts aus dem Anspruch des Bürgers auf effektiven Rechtsschutz auch entsprechende Dokumentationserfordernisse der Steuerverwaltung.

- Der Gesetzgeber hat den Anforderungen des Bundesverfassungsgerichts durch Anfügung von § 93 Abs. 9 und Abs. 10 AO im Rahmen des „Unternehmensteuerreformgesetzes 2008“ vom 14.08.2007 Rechnung getragen. Danach ist ein Betroffener vor einem Abrufersuchen auf die Möglichkeit eines Kontenabrufs hinzuweisen. Nach der Durchführung ist ein Betroffener zu benachrichtigen. Der Hinweis und die Benachrichtigung können allerdings im Wesentlichen in jenen Fällen unterbleiben, in denen sie die ordnungsgemäße Erfüllung der in der Zuständigkeit des Ersuchenden liegenden Aufgaben gefährden würden (§ 93 Abs. 9 AO). Weiterhin sind das Abrufersuchen und dessen Ergebnis vom Ersuchenden zu dokumentieren (§ 93 Abs. 10 AO). Die genannten Änderungen sind am 18.08.2007 in Kraft getreten.

- Bereits im Vorgriff auf die gesetzliche Regelung des § 93 Abs. 10 AO hat das Staatsministerium der Finanzen den nachgeordneten Finanzbehörden das Formular „Aktenvermerk zum Kontenabrufersuchen nach § 93 Abs. 7 i.V.m. § 93 b AO“ zur Verfügung gestellt. In dem Formular sind vom Ersuchenden der Abfragegrund und die bisherigen Ermittlungsmaßnahmen darzulegen. Das Formular ist dem Hauptsachgebietsleiter Abgabenordnung zur Prüfung und Unterschrift vorzulegen. Es liegt dem Leiter des Finanzamts auch bei dessen endgültiger Zeichnung des eigentlichen Kontenabfragevordrucks für das Bundeszentralamt für Steuern vor.

### 11.2.2 Praktische Umsetzung

Die praktische Durchführung der Kontenabfrage habe ich im Berichtszeitraum vor Ort bei einem bayerischen Finanzamt in Form einer detaillierten Einzelfallprüfung unter Hinzuziehung von Aktenunterlagen geprüft. Die Prüfung erbrachte folgende Ergebnisse:

- Zum Zeitpunkt der Prüfung bestand im Hinblick auf die Kontenabfragen keinerlei maschinelle Unterstützung. Die Kontenabfragen wurden nahezu ausschließlich von Außenprüfungsbeamten angestoßen. Das geprüfte Finanzamt verwendete für Dokumentationszwecke den erwähnten Vordruck des Staatsministeriums der Finanzen. Die Aufbewahrung einer Kopie des an das Bundeszentralamt für Steuern gesandten, jeweils vom Leiter des Finanzamts unterzeichneten Anfrageformulars und des Originals des dokumentierenden Vordrucks erfolgte nicht zentral, beispielsweise beim Hauptsachgebietsleiter Abgabenordnung, sondern in den jeweiligen Aktenunterlagen des Einzelfalls, bei den erwähnten Abfragen der Außenprüfungsbeamten in deren Handakten.

- Eine Einzeldurchsicht der dokumentierenden Vordrucke ergab im Ergebnis keine zu beanstandenden Mängel. Die Begründungen für die gewünschten Kontenabfragen waren durchweg individuell, ausführlich und nachvollziehbar. Die Frage der vorherigen Anhörung wurde jeweils erörtert; diese ist in einigen Fällen erfolgt, in den meisten Fällen wurde allerdings - mit entsprechender Begründung - von einer vorherigen Unterrichtung abgesehen.

- In den Fällen, in denen die durchgeführte Kontenabfrage zu Informationen über bisher nicht bekannte Konten führte, wurde der Steuerpflichtige in der Regel schriftlich um nähere Angaben zu den aufgedeckten Konten gebeten.

- In jenen Fällen, in denen die durchgeführte Kontenabfrage zu keinen neuen Erkenntnissen führte, erfolgte überwiegend die im Gesetz bzw. im Anwendungserlass vorgesehene Unterrichtung des Steuerpflichtigen durch ein gesondertes Schreiben oder eine entsprechende Formulierung in dem dem Steuerpflichtigen übermittelten Prüfungsbericht. Gegen diese Verfahrensweise bestehen aus datenschutzrechtlicher Sicht keine Einwendungen.

- In einer Anzahl von Fällen, nämlich in

  1 Fall von im Jahr 2005 insgesamt 12 getätigten Abfragen,

  10 Fällen von im Jahr 2006 insgesamt 38 getätigten Abfragen,

  1 Fall von im Jahr 2007 insgesamt 29 getätigten Abfragen

  ergab sich allerdings, dass durch den durchgeführten Kontenabruf keine neuen Konten ermittelt worden waren, die Unterrichtung des Betroffenen laut Aktenlage aber unterblieben ist. Dies widerspricht den bereits erwähnten Vorgaben und ist aus datenschutzrechtlicher Sicht im Hinblick auf die Transparenz staatlichen Handelns und unter dem Gesichtspunkt des Rechtsschutzgedankens nicht hinnehmbar.

  In oben genannten Fallzahlen nicht enthalten sind zwei telefonische Unterrichtungen der Betroffenen, die sich aus handschriftlichen Aufzeichnungen der Außenprüfer ergeben. Aus datenschutzrechtlicher Sicht sehe ich diese Art der Benachrichtigung sehr kritisch; hier ist aus Dokumentationszwecken zumindest die Fertigung eines Aktenvermerks notwendig.

- Die Problematik der Unterrichtung des Betroffenen war bereits in der Vergangenheit Gegenstand eines Schriftwechsels mit dem Staatsministerium der Finanzen. Sie resultiert aus einer vor allem in der vorliegenden Fallkonstellation (Auseinanderfallen von abrufender und veranlagender Stelle) nicht ausreichend klaren Aufgabenzuweisung und insbesondere aus dem Fehlen von Kontrollmechanismen.

  Zur Lösung bietet es sich an, die abfragende Stelle (Person) verpflichtend mit der Unterrichtung zu beauftragen und dies durch eine entsprechend gestaltete Verfügungszeile in dem verwendeten Vordruck sicherzustellen. Im Sinne des Vier-Augen-Prinzips erscheint darüber hinaus eine Kontrolle durch den verantwortlichen Hauptsachgebietsleiter notwendig.

- Bei Abgleich der vorgelegten Aktenunterlagen über die durchgeführten Kontenabfragen mit den vom Staatsministerium der Finanzen zur Verfügung gestellten statistischen Anschreibungen je Finanzamt ergaben sich Abweichungen. Die Zahlen konnten zwar letztlich konsolidiert werden; es bleibt aber festzuhalten, dass bei Abfragen von Konten bei Ehegatten oder bei Abfragen von Konten im Rahmen der Prüfung von Gesellschaften unter späterer Einbeziehung der Verhältnisse der Gesellschafter Zweifelsfragen in der Zählweise bestehen. Hier erscheint eine klare und verbindliche - zumindest bayernweite - Vorgabe wünschenswert.

Ich habe das Staatsministerium der Finanzen in dem genannten Zusammenhang um entsprechende Maßnahmen gebeten.

Zudem habe ich das geprüfte Finanzamt aufgefordert, die bisher unterbliebene Unterrichtung der von einem Kontenabruf betroffenen Steuerpflichtigen zeitnah nachzuholen.

### 11.3 Auskunftsanspruch in der Abgabenordnung

In der Vergangenheit habe ich schon mehrfach von den Bemühungen der Datenschutzbeauftragten des Bundes und der Länder berichtet, einen Auskunftsanspruch für Steuerpflichtige in der Abgabenordnung zu verankern (vgl. zuletzt Nr. 12.1 meines 20. Tätigkeitsberichts 2002). Diese Versuche sind bisher stets am Widerstand der Steuerverwaltung gescheitert.

Erfreulicherweise hat das Bundesverfassungsgericht in seiner Entscheidung vom 10.03.2008 (1 BvR 2388/03) nunmehr klar gestellt, dass § 19 BDSG, der den Auskunftsanspruch eines Betroffenen

im Geltungsbereich des Bundesdatenschutzgesetzes regelt, auch gegenüber der Steuerverwaltung gilt.

In dem seiner Entscheidung zugrunde liegenden Fall hat das Bundesverfassungsgericht allerdings auch die Ablehnung der Auskunft im Hinblick auf die in § 19 Abs. 4 BDSG genannten Ablehnungstatbestände für verfassungskonform erachtet. Selbst wenn aber künftige Auskunftsersuchen in nicht unerheblichem Umfang unter Hinweis auf die Ausnahmetatbestände des § 19 Abs. 4 BDSG abgelehnt werden sollten, ist das Urteil des Bundesverfassungsgerichts aus datenschutzrechtlicher Sicht zu begrüßen: Die Steuerverwaltung hatte nämlich gegenüber der Datenschutzseite in der Vergangenheit stets argumentiert, dass die Frage eines Auskunftsrechts in der Abgabenordnung bewusst nicht geregelt worden sei, weshalb diese „absichtsvolle Nichtregelung“ das allgemeine Datenschutzrecht verdränge. Dieser Rechtsauffassung hat das Bundesverfassungsgericht nunmehr endgültig eine klare Absage erteilt.

### 11.4 Auskunftsersuchen der Finanzämter über Teilnehmer von Fortbildungsveranstaltungen

Immer wieder erreichen mich Eingaben im Zusammenhang mit Auskunftsersuchen der Finanzverwaltung über Teilnehmer an Fortbildungsveranstaltungen. Im Berichtszeitraum war die Eingabe einer staatlich anerkannten Heimvolkshochschule von besonderem datenschutzrechtlichem Interesse.

Diese Institution führte unter anderem Fortbildungsveranstaltungen für homosexuelle Lehrkräfte durch. Im Zuge der einkommensteuerlichen Geltendmachung der angefallenen Kosten als Werbungskosten durch einen der Teilnehmer wandte sich das für diesen zuständige Finanzamt an die Fortbildungsstätte mit der Bitte, die Teilnehmerliste der betreffenden Fortbildungsveranstaltung zu übermitteln. In diesem Zusammenhang ist zu bemerken, dass für die steuerliche Anerkennung von Fortbildungskosten ein Kriterium - unter mehreren - das Vorliegen eines homogenen Teilnehmerkreises sein kann. Das Finanzamt stützte das Auskunftsverlangen auf § 93 AO.

Die Finanzbehörden können sich zur Sachaufklärung der Beweismittel bedienen, die sie nach pflichtgemäßem Ermessen zur Ermittlung des Sachverhalts für erforderlich halten. Dieses Ermessen hat sich aber an den allgemein gültigen Grenzen der Erforderlichkeit, Verhältnismäßigkeit, Erfüllbarkeit und Zumutbarkeit zu orientieren. Bei Auskunftsersuchen wird dem Verhältnismäßigkeitsgrundsatz unter anderem durch eine im Gesetz vorgesehene Beweismittelreihenfolge Rechnung getragen. So sollen nach § 93 Abs. 1 Satz 3 AO andere Personen - dabei kann es sich auch um Behörden handeln, was dann zu einer Überschneidung der Auskunftspflicht mit der Amtshilfepflicht nach § 111 AO führt; siehe insoweit Nr. 15.2 meines 21. Tätigkeitsberichts 2004 - als die Beteiligten erst dann zur Auskunft angehalten werden, wenn die Sachverhaltsaufklärung durch die Beteiligten nicht zum Ziel führt oder keinen Erfolg verspricht. Der Begriff „sollen“ bedeutet dabei, dass die Finanzbehörden im Regelfall nach der gesetzlich vorgesehenen Beweismittelreihenfolge verfahren müssen und nur in besonders gelagerten, atypischen Fällen davon abweichen dürfen.

Aus dem mir zur Verfügung gestellten Schreiben des anfragenden Finanzamts ergab sich nun, dass die Sachverhaltsaufklärung durch den Steuerpflichtigen nicht zum Ziel geführt hatte. In einem solchen Fall bleibt es der Finanzbehörde unbenommen, im Hinblick auf die mangelnde Mitwirkung des Steuerpflichtigen bei der Sachverhaltsaufklärung den geltend gemachten Werbungskostenabzug steuerlich nicht anzuerkennen. Anders als beispielsweise bei gegenüber den Finanzbehörden verschwiegenen Einkünften kann hier auf ein Auskunftsersuchen gegenüber Dritten ohne die Gefahr staatlicher Einnahmeverluste verzichtet werden. In der vorliegenden, besonders sensiblen Fallgestaltung war zudem davon auszugehen, dass die Vorlage einer Teilnehmerliste das Vertrauensverhältnis zwischen der Fortbildungsstätte und den Teilnehmern der Fortbildungsveranstaltung in nicht unerheblichem Umfang beeinträchtigt hätte.

Meine Rechtsauffassung wird durch die finanzgerichtliche Rechtsprechung gestützt. So hat das Finanzgericht Düsseldorf mit Urteil vom 15.01.1997 (EFG 1997, 582) ein finanzamtliches Auskunftsersuchen gegenüber einer als Reiseveranstalter auftretenden Industrie- und Handelskammer (IHK) ebenfalls als nicht zulässig erachtet. Im Falle der Erteilung der begehrten Auskunft hält das Gericht das Vertrauensverhältnis zwischen dem Reiseveranstalter - der IHK - und den Reiseteilnehmern - den von der IHK betreuten Unternehmern - für so stark berührt, dass die künftige Aufgabenwahrnehmung der IHK ernstlich gefährdet würde. Diese Argumentation muss umso mehr bei der von mir geschilderten, weitaus sensibleren Fallgestaltung Platz greifen.

Schließlich möchte ich noch Folgendes bemerken: Ziel von finanzamtlichen Auskunftsersuchen, die auf die Übermittlung der Teilnehmerlisten von Fortbildungsveranstaltungen gerichtet sind, dürfte oftmals nicht allein die Prüfung der Abzugsfähigkeit der Aufwendungen in einem steuerlichen Einzelfall sein. Bei Versagung des Werbungskostenabzugs soll vielmehr auch im Hinblick auf die Aufgabe der Finanzverwaltung, die Gleichmäßigkeit der Besteuerung sicherzustellen, der Versand von Kontrollmitteilungen an die Wohnsitzfinanzämter der anderen Teilnehmer ermöglicht werden. Zur Erreichung dieses Ziels stehen der Finanzverwaltung allerdings mildere Mittel zur Verfügung. Beispielsweise könnten über

das Landesamt für Steuern in Bezug auf bestimmte (Reihen von) Fortbildungsveranstaltungen Kontrollhinweise an die bayerischen Finanzämter mit der Anweisung übermittelt werden, diesbezüglich geltend gemachte Aufwendungen nicht als Betriebsausgaben oder Werbungskosten steuerlich anzuerkennen.

### 11.5 Nachweis von Krankheitskosten als außergewöhnliche Belastung

Von Versicherungen nicht erstattete Krankheitskosten können im Rahmen der Veranlagung zur Einkommensteuer nach Abzug einer zumutbaren Eigenbelastung gemäß § 33 EStG als außergewöhnliche Belastung steuermindernd geltend gemacht werden.

In diesem Zusammenhang wandte sich ein Arzt mit folgender Sachverhaltsschilderung an mich:

Seine Ehefrau, mit der er einkommensteuerrechtlich zusammenveranlagt werde, habe eine medizinische Heilmaßnahme in einer Spezialklinik durchführen lassen. Allerdings seien die dafür angefallenen Kosten nicht von der Krankenversicherung übernommen worden. Deshalb seien diese im Rahmen der Einkommensteuerveranlagung als außergewöhnliche Belastung geltend gemacht worden. Im Zuge der Bearbeitung des Steuerfalls habe das Finanzamt zunächst darum gebeten, die medizinische Notwendigkeit der Heilmaßnahme durch ein vor der Durchführung der Heilmaßnahme ausgestelltes ärztliches Gutachten nachzuweisen. Der Eingabeführer habe daraufhin eine von ihm selbst ausgestellte Bestätigung der medizinischen Notwendigkeit beim Finanzamt eingereicht. Im weiteren Verlauf habe das Finanzamt jedoch eine steuerliche Berücksichtigung davon abhängig gemacht, dass dargelegt werde, „zum Zwecke der Heilung welcher Krankheit“ die Heilmaßnahme durchgeführt worden sei.

Der Eingabeführer sah die Forderung des Finanzamts nach Angabe der medizinischen Diagnose nicht durch die entsprechenden Bestimmungen des Steuerrechts gedeckt.

In Anbetracht der grundlegenden Bedeutung dieser Problematik habe ich mich daraufhin unmittelbar an das Staatsministerium der Finanzen gewandt. Dabei habe ich nicht bestritten, dass es dem Finanzamt in besonders gelagerten Einzelfällen möglich sein muss, sich die Zwangsläufigkeit, Notwendigkeit und Angemessenheit von geltend gemachten Krankheitskosten nachweisen zu lassen. Auch habe ich nicht in Zweifel gezogen, dass bei einer entscheidungserheblichen Beteiligung von nahen Angehörigen an die in § 90 AO normierten Mitwirkungspflichten der Beteiligten bei der Ermittlung eines steuerlichen Sachverhalts erhöhte Anforderungen zu stellen sind. Ich habe jedoch deutlich gemacht, dass selbst bei Vorliegen dieser besonderen Umstände Auskunftsersuchen an den allgemein gültigen Schranken der Verhältnismäßigkeit, Erfüllbarkeit und Zumutbarkeit zu messen sind. Insbesondere habe ich darauf hingewiesen, dass die Finanzverwaltung - auch und gerade im Rahmen der steuerlichen Veranlagung der Angehörigen der Heilberufe - bisher nie in Zweifel gezogen hat, dass die durch einen Arzt festgestellten Diagnosen und Behandlungsmethoden sowohl unter das Auskunftsverweigerungsrecht des § 102 AO als auch unter das in § 203 StGB normierte Arztgeheimnis fallen.

Die Forderung nach Angabe der medizinischen Diagnosen war daher bei dem in Rede stehenden Sachverhalt nicht zulässig. Das Finanzamt war vielmehr gehalten, dem Eingabeführer und seiner Ehefrau eine andere Nachweismöglichkeit vorzugeben.

Das Staatsministerium der Finanzen hat sich meiner Rechtsauffassung angeschlossen und ausdrücklich festgestellt, dass es nicht zulässig ist, zur Beurteilung der Frage, ob Krankheitskosten als außergewöhnliche Belastung anerkannt werden können, die Angabe von Diagnosen zu fordern. Daher hat das Finanzministerium das Landesamt für Steuern aufgefordert, neben dem konkret betroffenen auch alle anderen bayerischen Finanzämter auf die gegenständliche Problematik aufmerksam zu machen und die Einhaltung von § 102 AO und § 203 StGB zu gewährleisten.

## 12 Schulen

### 12.1 Evaluation an Schulen

Zur Qualitätssicherung und -verbesserung sollen die bayerischen Schulen nach den Vorstellungen des Staatsministeriums für Unterricht und Kultus entweder intern - d.h. durch die Schulen selbst - oder extern - d.h. durch die Schulaufsichtsbehörden im Zusammenwirken mit der Qualitätsagentur im Staatsinstitut für Schulqualität und Bildungsforschung - evaluiert werden. Als von datenschutzrechtlich besonderer Relevanz erweist sich dabei die externe Evaluation.

Nach der mir vorgelegten Konzeption des Staatsministeriums für Unterricht und Kultus für die „Externe Evaluation an Bayerns Schulen“ soll bezüglich jedes einzelnen Betroffenen eine Vielzahl von personenbezogenen Daten an den Schulen erhoben und verarbeitet, insbesondere gespeichert und übermittelt werden. Potentiell betroffen sind dabei nicht nur einzelne am Schulleben beteiligte Personen, sondern jeweils alle Schulleiter, sonstigen Lehrkräfte, Schüler und Eltern sowie ggf. auch betriebliche Ausbilder. Besonders problematisch ist zum einen, dass an der externen Evaluation gemäß der Konzeption des Kultusministeriums auch Vertreter der Eltern oder der Wirtschaft - also private Dritte - beteiligt sein sollen. Überdies sollen die - letztlich oft personenbeziehbaren - Evaluationsergebnisse in der Schulöffentlichkeit diskutiert werden. So haben Lehrkräfte in Eingaben mir gegen-

über ihrer Befürchtung Ausdruck verliehen, im Rahmen der Evaluation auch vor Außenstehenden an den „Pranger“ gestellt zu werden - mit unmittelbaren Folgen für das berufliche Fortkommen.

Im Zuge einer längeren Diskussion konnte ich das Staatsministerium für Unterricht und Kultus davon überzeugen, dass bereits die interne, vor allem aber die externe Evaluation wegen der vielfachen Eingriffe in das Grundrecht auf informationelle Selbstbestimmung der Lehrer, Schüler, Eltern und Ausbilder einer gesetzlichen Grundlage bedarf, die den verfassungsrechtlichen Geboten der Normenklarheit, Normenbestimmtheit und Verhältnismäßigkeit genügen muss. Insbesondere geht die externe Evaluation als - so das Kultusministerium - „Weiterentwicklung der Schulaufsicht“ über das bislang nach allgemeiner Auffassung unter Schulaufsicht zu Verstehende weit hinaus und kann daher nicht auf die allgemeine Aufgabenzuweisungsnorm für die staatliche Schulaufsicht in Art. 111 Abs. 1 BayEUG und die generalklauselartige Befugnisnorm des Art. 113 Abs. 1 BayEUG gestützt werden. Weder für die Verwaltung noch für die Gerichte und erst Recht nicht für die betroffenen Bürger ist erkennbar, dass der bayerische Gesetzgeber mit diesen allgemeinen schulaufsichtlichen Bestimmungen eine Rechtsgrundlage für die externe Evaluation schaffen wollte. In diesem Zusammenhang habe ich das Kultusministerium darauf aufmerksam gemacht, dass die schulische Evaluation auch in den anderen Bundesländern nahezu durchgängig auf eine spezielle gesetzliche Rechtsgrundlage gestützt wird. Zudem bestehen in Bayern bereits für die Evaluation im Hochschulbereich in Art. 10 Bayerisches Hochschulgesetz gesetzliche Vorgaben (vgl. dazu Nr. 12.1 meines 22. Tätigkeitsberichts 2006).

Im Sommer 2008 hat der Landtag mit Wirkung zum 01.08.2008 schließlich die Vorschrift des Art. 113 a „Evaluation“ in das BayEUG neu eingefügt. Die Bestimmungen des Art. 113 a BayEUG gehen dabei auf einen vom Staatsministerium für Unterricht und Kultus erarbeiteten Gesetzentwurf der Staatsregierung zurück, der wiederum in seinen datenschutzrechtlich relevanten Teilen im Wesentlichen einem Formulierungsvorschlag meines Hauses entspricht.

Nachfolgende Regelungen des neuen Art. 113 a BayEUG sind in datenschutzrechtlicher Hinsicht besonders bedeutsam:

- Bei der externen Evaluation gestattet es Art. 113 a Abs. 2 Satz 3 Halbsatz 1 BayEUG den Schulaufsichtsbehörden, an den Evaluationsgruppen private Dritte - also Vertreter der Eltern und der Wirtschaft - zu beteiligen. Diese Regelung halte ich aus vorbeschriebenen Gründen für problematisch. Ich würde es daher begrüßen, wenn die Schulaufsichtsbehörden in der Praxis von der Möglichkeit der Einschaltung privater Dritter Abstand nähmen. Die Problematik wird auch dadurch nicht wesentlich entschärft, dass die privaten Dritten nach den gesetzlichen Vorgaben über die erforderliche Eignung und Fachkunde verfügen müssen. Immerhin habe ich erreichen können, dass nach Art. 113 a Abs. 2 Satz 3 Halbsatz 2 BayBG die Zuerkennung der Eignung nunmehr gesetzlich voraussetzt, dass die mit der Evaluation betrauten Personen nach dem Verpflichtungsgesetz förmlich verpflichtet werden.

- Art. 113 a Abs. 3 Satz 2 BayEUG schränkt die Befugnis zur Datenerhebung, -verarbeitung und -nutzung im Rahmen der internen und externen Evaluation stark ein: hiernach dürfen nur soweit personenbezogene Daten der Betroffenen erhoben, verarbeitet und genutzt werden, als das öffentliche Interesse die schutzwürdigen Belange der Betroffenen erheblich überwiegt und der Zweck der Evaluation auf andere Weise nicht oder nur mit unverhältnismäßigem Aufwand erreicht werden kann.

- Die Regelung des Art. 113 a Abs. 3 Satz 3 BayEUG enthält ein gesetzliches Verwertungsverbot zu anderen Zwecken: die bei der Evaluation erhobenen personenbezogenen Daten dürfen nur für den Zweck der Evaluation selbst verwendet werden. Eine Verarbeitung oder Nutzung für andere Zwecke - also insbesondere für die dienstliche Beurteilung der Lehrkräfte - ist bereits von Gesetzes wegen unzulässig.

- Art. 113 Abs. 3 Satz 4 BayEUG stellt sicher, dass die Betroffenen - insbesondere Schulleitung, Lehrkräfte, Schüler und Erziehungsberechtigte - vor der Durchführung einer Evaluation über das Ziel des Vorhabens, die Art ihrer Beteiligung an der Untersuchung, die Verarbeitung und Nutzung ihrer Daten sowie über die zur Einsichtnahme in die personenbezogenen Daten Berechtigten schriftlich informiert werden. Diese Vorschrift dient ganz wesentlich der Transparenz.

- Die Regelungen in Art. 113 a Abs. 3 Sätze 5 bis 7 BayEUG entsprechen den für Forschungseinrichtungen geltenden Bestimmungen in Art. 23 Abs. 3 BayDSG. Die personenbezogenen Daten sind zu anonymisieren, sobald dies nach dem Zweck der Evaluation möglich ist. Im Stadium vor der Anonymisierung sind die Sachmerkmale von den Identifikationsmerkmalen getrennt zu speichern. Die Merkmale dürfen nur dann zusammengeführt werden, wenn dies für die Durchführung der Evaluation wirklich notwendig ist. Auf diese

Weise wird schon vor der Anonymisierung die Herstellung eines Personenbezugs erschwert.

- Art. 113 a Abs. 3 Satz 8 BayEUG untersagt die Veröffentlichung der Evaluationsergebnisse in personenbezogener Form. Denn Zweck der internen und externen Evaluation ist die Bewertung der Schule, um die Qualität schulischer Arbeit zu sichern und zu verbessern, nicht hingegen die Bewertung einzelner Personen. Soweit Ergebnisse für Teile der Schule veröffentlicht werden sollen (z.B. für einen bestimmten Fachbereich oder für die Schulleitung), ist im Gesetzesvollzug darauf zu achten, dass die betroffene Personengruppe groß genug ist, damit ein Rückschluss auf personenbezogene Daten einer bestimmten oder bestimmbaren Person sicher ausgeschlossen ist. Davon ist in aller Regel erst dann auszugehen, wenn die evaluierte Gruppe mehr als drei Personen umfasst. In Einzelfällen kann die Bildung auch größerer Gruppen jedoch geboten sein.

- Art. 113 a Abs. 3 Satz 9 BayEUG bestimmt, dass personenbezogene Daten spätestens ein Jahr nach ihrer Erhebung gelöscht und die entsprechenden Unterlagen nach dieser Frist vernichtet werden.

Insgesamt betrachtet habe ich durch meine Bemühungen erreichen können, dass die interne und externe Evaluation an bayerischen Schulen nunmehr auf eine tragfähige, normenklare und bestimmte Rechtsgrundlage gestützt ist, die dem Grundrecht auf informationelle Selbstbestimmung der Lehrer, Schüler und Eltern sowie ggf. Ausbilder in angemessener Weise Rechnung trägt.

## 12.2 Datenschutz in der Schule - Änderung der Durchführungsverordnung zu Art. 28 Abs. 2 BayDSG

Als bisher einziges Staatsministerium hatte das Staatsministerium für Unterricht und Kultus bereits am 23.03.2001 durch Erlass der „Verordnung zur Durchführung des Art. 28 Abs. 2 des Bayerischen Datenschutzgesetzes“ (im Folgenden: Durchführungsverordnung) von der in Art. 28 Abs. 2 BayDSG eingeräumten Verordnungsermächtigung Gebrauch gemacht. In dieser Verordnung hatte das Kultusministerium insbesondere 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 zur Durchführungsverordnung aufgeführten Umfang (Verfahren der Lehrerdatei, Schülerdatei, Kollegstufendatei, Stundenplanprogramm, Vertretungsplanprogramm, Externes Zeugnisprogramm, Buchausleiheprogramm) einsetzen.

Im Berichtszeitraum hat mir das Staatsministerium für Unterricht und Kultus nunmehr den Entwurf einer Verordnung zur Änderung und Ergänzung der Durchführungsverordnung vorgelegt, mit dem weitere, für den Datenschutz in der Schule bedeutsame Themenfelder allgemein geregelt werden sollten. In der anschließenden, intensiven Diskussion mit dem Kultusministerium konnte ich zahlreiche datenschutzrechtliche Verbesserungen erreichen. Die Änderungsverordnung ist am 01.09.2008 in Kraft getreten.

Aus datenschutzrechtlicher Sicht erscheinen mir folgende Punkte von besonderer Relevanz:

### 12.2.1 Verfahren Notenverwaltungsprogramm

Das in Anlage 6 zur Durchführungsverordnung bislang beschriebene „Verfahren Externes Zeugnisprogramm“ wurde durch ein allgemeines „Verfahren Notenverwaltungsprogramm“ ersetzt.

Im ursprünglichen Entwurf der Änderungsverordnung war noch vorgesehen, dass alle Lehrkräfte während des gesamten Schuljahres ohne besonderen Anlass fächerübergreifend sämtliche Daten der von ihnen unterrichteten Schülerinnen und Schüler einsehen können, insbesondere die Noten der einzelnen Leistungsnachweise in allen Fächern. Zur Begründung dieser umfassenden Leseberechtigungen hatte das Staatsministerium für Unterricht und Kultus ausgeführt, dass die Kenntnis der fächerübergreifenden Leistungen während des Schuljahres unerlässlich sei, damit jede Lehrkraft rechtzeitig schulische oder häusliche Probleme erkennen könne, die sich oftmals durch einen plötzlichen Leistungsabfall in mehreren Fächern gleichzeitig bemerkbar machten. Darüber hinaus sei die Kenntnis der fächerübergreifenden Einzelleistungen insofern notwendig, als alle Lehrkräfte einer Klasse im Rahmen der Klassenkonferenz beispielsweise über das Vorrücken zu entscheiden hätten.

In meiner Stellungnahme habe ich darauf hingewiesen, dass es aus datenschutzrechtlicher Sicht nicht zulässig ist, allen Lehrkräften zu jeder Zeit einen solch unbeschränkten Einblick in die Leistungen ihrer Schülerinnen und Schüler in allen Fächern einzuräumen. Der mit diesem weit reichenden Zugriff auf personenbezogene Daten verbundene Eingriff in das Grundrecht auf informationelle Selbstbestimmung kann nämlich nur dann als gerechtfertigt angesehen werden, wenn er zur Aufgabenerfüllung der Schule tatsächlich erforderlich ist. Dabei ist im Rahmen der Prüfung der Erforderlichkeit abzuwägen zwischen dem Informationsinteresse der Schule bzw. der Lehr-

kräfte einerseits und dem Persönlichkeitsschutz der Schülerinnen und Schüler andererseits. Diese haben Anspruch darauf, nicht befürchten zu müssen, dass schlechte Zensuren einer Lehrkraft in einem Fach bei den übrigen Lehrkräften - ohne böse Absicht, sondern in der Regel unbewusst - zu einem negativen Eindruck führen. Aus diesem Grund kann das Informationsinteresse der Schule nicht unbeschränkte Geltung beanspruchen; vielmehr muss es zumindest partiell hinter dem Persönlichkeitsrecht der Schülerinnen und Schüler zurücktreten.

Daran gemessen habe ich es für akzeptabel gehalten, wenn Lehrkräfte zur Erfüllung ihrer Aufgaben als Mitglieder der Klassenkonferenz (insbesondere Zeugniserstellung, Entscheidung über das Vorrücken, Empfehlung an die Lehrerkonferenz im Fall des Vorrückens auf Probe) Kenntnis der fächerübergreifenden Einzelleistungen ihrer Schülerinnen und Schüler erhalten. Für diesen Zweck ist es aber nicht erforderlich, dass Lehrkräfte ohne besonderen Anlass während des gesamten Schuljahrs mittels eines automatisierten Notenverwaltungsprogramms Zugriff auf die fächerübergreifenden Leistungen sämtlicher von ihnen unterrichteter Schülerinnen und Schülern haben. Vielmehr genügt es, wenn den betroffenen Lehrkräften zur Vorbereitung auf die Klassenkonferenz für einen begrenzten Zeitraum die Einzelleistungen der jeweils betroffenen Schülerinnen und Schüler zugänglich gemacht werden.

Nicht überzeugt hat mich die Argumentation des Kultusministeriums, die Kenntnis der fächerübergreifenden Leistungen während des Schuljahres sei unerlässlich, damit jede Lehrkraft rechtzeitig schulische oder häusliche Probleme erkennen könne. Denn die Förderlichkeit der Datenkenntnis in einigen konkreten Einzelfällen kann nicht den vorsorglichen Zugriff jeder Lehrkraft auf die Einzelleistungen aller von ihr unterrichteten Schülerinnen und Schüler während des gesamten Schuljahres rechtfertigen. Allenfalls kann der jeweiligen Klassenleitung ein fächerübergreifender Zugriff auf die im automatisierten Notenverwaltungsprogramm gespeicherten Einzelleistungen der Schülerinnen und Schüler ihrer Klasse gewährt werden.

Erfreulicherweise hat sich das Staatsministerium für Unterricht und Kultus meinen Argumenten nicht verschlossen gezeigt, so dass für die Regelungen zum „Verfahren Notenverwaltungsprogramm“ in Anlage 6 zur Durchführungsverordnung letztlich ein akzeptabler Kompromiss gefunden werden konnte:

- In der Durchführungsverordnung ist nun ausdrücklich klargestellt, dass das Notenverwaltungsprogramm nur soweit und solange der Information der Lehrkräfte über das fächerübergreifende Notenbild der von ihnen unterrichteten Schülerinnen und Schüler dient, als dies im Einzelfall zur Erfüllung der Aufgaben der Schule erforderlich ist.

- Lehrkräfte dürfen fächerübergreifenden Zugriff auf die Leistungsdaten der jeweils von ihnen unterrichteten Schülerinnen und Schüler nur im konkreten Einzelfall erhalten, insbesondere für den Zeitraum, für den dies zur Erfüllung ihrer Aufgaben als Mitglied der Klassenkonferenz erforderlich ist.

- Nur die Klassenleitungen dürfen darüber hinaus fächerübergreifenden Zugriff auf die Leistungsdaten der Schülerinnen und Schüler ihrer Klasse erhalten, um schulische oder häusliche Probleme erkennen zu können, die sich durch einen plötzlichen Leistungsabfall in mehreren Fächern gleichzeitig bemerkbar machen, sowie für die Zeugnisvorbereitung und -erstellung.

- Wegen der dort bestehenden schulorganisatorischen und didaktischen Besonderheiten dürfen Lehrkräfte an Berufsschulen fächerübergreifenden Zugriff auf die Leistungsdaten der jeweils von ihnen unterrichteten Schülerinnen und Schüler während des gesamten Schuljahres erhalten.

- Im Übrigen dürfen Lehrkräfte nur auf die Leistungsdaten der von ihnen unterrichteten Schülerinnen und Schüler in den von ihnen jeweils unterrichteten Fächern Zugriff erhalten.

Darüber hinaus konnte ich erreichen, dass die im Notenverwaltungsprogramm gespeicherten Daten jeweils spätestens am Ende des laufenden Schuljahres gelöscht werden. Im ursprünglichen Entwurf war noch eine Speicherung bis zum Ende des nachfolgenden Schuljahres vorgesehen; hierfür hatte ich keine Notwendigkeit gesehen.

### 12.2.2 Videoaufzeichnung an Schulen

Als Anlage 8 neu in die Durchführungsverordnung zu Art. 28 Abs. 2 BayDSG aufgenommen wurde die „Videoaufzeichnung an Schulen“.

Rechtsgrundlage für die Videoaufzeichnung ist die mit Wirkung zum 01.07.2008 neu in das Bayerische Datenschutzgesetz aufgenommene Bestimmung des Art. 21 a BayDSG (siehe dazu eingehend Nr. 9.2 dieses Tätigkeitsberichts). Gemäß Anlage 8 zur Durchführungsverordnung darf die Videoaufzeichnung an Schulen allein zum Schutz von Leben, Gesundheit, Freiheit und Eigentum der Personen, die sich im Bereich der Schule oder in deren unmittelbarer Nähe aufhalten, und zum Schutz der schulischen Einrichtung vor Sachbeschädigung und Diebstahl

eingesetzt werden. Von der Videoaufzeichnung betroffen dürfen dabei nur Personen sein, die sich im Eingangsbereich der Schule aufhalten oder die sich außerhalb von schulischen oder sonstigen von der Schule zugelassenen Veranstaltungen zwischen 22:00 Uhr und 6:30 Uhr auf dem Schulgelände befinden; über diese enge zeitliche Begrenzung hinaus ist eine Aufzeichnung nur an Feiertagen, an Wochenenden und in den Ferien zulässig. Weiter ist in der Durchführungsverordnung festgelegt, dass die gespeicherten Daten spätestens einen Monat nach der Aufzeichnung gelöscht werden müssen, soweit sie nicht zur Verfolgung von Ordnungswidrigkeiten von erheblicher Bedeutung oder von Straftaten oder zur Geltendmachung von Rechtsansprüchen benötigt werden. Darüber hinaus dürfen nur die von der Schulleitung beauftragten Angehörigen des Lehr- oder Verwaltungspersonals die Videoaufzeichnungen einsehen.

Bedauerlicherweise hat das Staatsministerium für Unterricht und Kultus meiner Anregung nicht entsprochen, eine kürzere Regelfrist für die Löschung der Videoaufzeichnungen vorzusehen. Allerdings weise ich darauf hin, dass bei einer Videoaufzeichnung an Schulen über die Regelungen in der Durchführungsverordnung hinaus selbstverständlich auch die gesetzlichen Vorgaben des Art. 21 a BayDSG zu beachten sind. Demnach muss die Videoüberwachung im konkreten Einzelfall zum Schutz der oben genannten Rechtsgüter erforderlich, also geeignet und verhältnismäßig sein (Art. 21 a Abs. 1 Satz 1 BayDSG). Davon wird in der Regel nur auszugehen sein, wenn bereits in der Vergangenheit Vorfälle aufgetreten sind, die eine Videoüberwachung rechtfertigen können. Zudem dürfen insbesondere im konkreten Einzelfall keine Anhaltspunkte dafür bestehen, dass durch die Videoüberwachung überwiegende schutzwürdige Interessen der Betroffenen beeinträchtigt werden (Art. 21 a Abs. 1 Satz 2 BayDSG). Ferner sind die Videoüberwachung und die erhebende Stelle durch geeignete Maßnahmen erkennbar zu machen (Art. 21 a Abs. 2 BayDSG). Werden durch Videoüberwachung erhobene Daten einer bestimmten Person zugeordnet, ist diese über die Tatsache der Speicherung entsprechend Art. 10 Abs. 8 BayDSG zu benachrichtigen (Art. 21 a Abs. 4 BayDSG).

Zur Vermeidung von Missverständnissen und Fehlinterpretationen möchte ich schließlich ausdrücklich auf Folgendes hinweisen: Mit der Aufnahme in die Durchführungsverordnung ist die „Videoaufzeichnung an Schulen“ selbstverständlich keinesfalls verpflichtend vorgeschrieben. Ein wie auch immer gearteter „Zwang“ zur Videoaufzeichnung besteht also gerade nicht. Vielmehr kommt es jeweils entscheidend darauf an, ob die Videoaufzeichnung im konkreten Einzelfall tatsächlich zum Schutz der genannten Rechtsgüter erforderlich ist oder ob nicht andere Aufsichts- und Überwachungsmaßnahmen sowie sonstige - insbesondere pädagogische - Mittel ausreichen. Zudem ist festzustellen, dass die Durchführungsverordnung nur die äußersten Grenzen der Videoaufzeichnung festlegt, die von den Schulen zwar nicht überschritten, aber selbstverständlich unterschritten werden dürfen und ggf. sogar unterschritten werden müssen. So dürfte beispielsweise die generelle Überwachung des Eingangsbereichs der Schule häufig nicht notwendig und damit unzulässig sein. Ebenso sind z.B. kürzere Löschungsfristen aus datenschutzrechtlicher Sicht wünschenswert.

Ich habe das Staatsministerium für Unterricht und Kultus gebeten, alle bayerischen Schulen auf die Rechtslage unter Berücksichtigung meiner Rechtsauffassung in einem Rundschreiben hinzuweisen. Dieser Bitte hat das Kultusministerium mit Rundschreiben vom 25.09.2008 (Az. I.5-5 L 0572-1.93780) entsprochen.

### 12.2.3 Internetauftritt von Schulen

Der Europäische Gerichtshof (EuGH) hatte bereits am 06.11.2003 entschieden, „dass die Handlung, die darin besteht, auf einer Internetseite auf verschiedene Personen hinzuweisen und diese entweder durch ihren Namen oder auf andere Weise, etwa durch Angabe ihrer Telefonnummer oder durch Informationen über ihr Arbeitsverhältnis oder ihre Freizeitbeschäftigungen, erkennbar zu machen, eine ganz oder teilweise automatisierte Verarbeitung personenbezogener Daten im Sinne von Art. 3 Abs. 1 der EG-Datenschutzrichtlinie darstellt.“ Aufgrund dieser Entscheidung haben bayerische öffentliche Stellen, die personenbezogene Daten in dem vom EuGH beschriebenen Umfang auf ihre Homepage einstellen, allein schon deswegen einen behördlichen Datenschutzbeauftragten zu bestellen (Art. 25 Abs. 2 Satz 1 BayDSG); zudem bedarf ein derartiger Internetauftritt gem. Art. 26 BayDSG der Freigabe durch den behördlichen Datenschutzbeauftragten (vgl. hierzu ausführlich Nr. 4.1 meines 21. Tätigkeitsberichts 2004). Vor diesem Hintergrund ist es aus datenschutzrechtlicher Sicht zu begrüßen, dass das Staatsministerium für Unterricht und Kultus nunmehr Regelungen über den „Internetauftritt von Schulen“ als neue Anlage 9 in die Durchführungsverordnung aufgenommen hat.

Im Rahmen meiner Beteiligung habe ich nicht kritisiert, dass laut Anlage 9 Name, Namensbestandteile, Vorname(n), Funktion, Amtsbezeichnung, Lehrbefähigung, dienstliche Anschrift, dienstliche Telefonnummer sowie dienstliche E-Mail-Adresse der Schulleitung und von Lehrkräften, die an der Schule eine Funktion mit Außenwirkung wahrnehmen, auch ohne deren Einwilligung in den Internetauftritt der Schule eingestellt werden können. Auch im Bereich der Schulen halte ich die Veröffentlichung dieser personenbezogenen Daten - im Gegensatz beispielsweise

zu Fotos - dieses Personenkreises ohne Einwilligung im Regelfall für akzeptabel (siehe hierzu ausführlich Nr. 12.3 meines 18. Tätigkeitsberichts 1998).

Hingegen konnte ich keine Rechtsgrundlage dafür erkennen, dass - wie im ursprünglichen Entwurf noch vorgesehen - Name, Namensbestandteile, Vorname(n), Funktion und Schuladresse von Erziehungsberechtigten sowie von Schülerinnen und Schülern, die an der Schule eine Funktion mit Außenwirkung wahrnehmen - insbesondere Elternbeiratsvorsitzende, Schülersprecherinnen und Schülersprecher -, ohne Einwilligung der Betroffenen auf Schulhomepages bekanntgegeben werden können. Denn eine Veröffentlichung personenbezogener Daten von Schülerinnen und Schülern sowie Erziehungsberechtigten im Internet ist auch dann nicht im Sinne des Art. 85 Abs. 1 BayEUG zur Aufgabenerfüllung der Schulen erforderlich, wenn diese als Schülersprecherinnen und Schülersprecher oder Elternbeiratsvorsitzende fungieren. Zwar ist es richtig, dass dieser Personenkreis zu den Funktionsträgern der Schule und die Öffentlichkeitsarbeit zu den Aufgaben der Schule gehört. Jedoch nimmt dieser Personenkreis seine schulischen Aufgaben ehrenamtlich war; es handelt sich gerade nicht um Angehörige des öffentlichen Dienstes, die aufgrund dieses Dienstverhältnisses gewisse Einschränkungen ihres Rechts auf informationelle Selbstbestimmung hinnehmen müssen. Auch ist das Informationsinteresse der Öffentlichkeit hinsichtlich Schülersprecherinnen und Schülersprechern sowie Elternbeiratsvorsitzenden im Vergleich zur Schulleitung nicht gewichtig genug, dass diese trotz der engen lokalen Begrenzung des Aufgaben- und Wirkungsbereichs der einzelnen Schule eine Einschränkung ihres Persönlichkeitsrechts durch eine weltweite Veröffentlichung ihrer Daten im Internet hinnehmen müssen. Schließlich untersagt Art. 85 Abs. 2 Satz 1 BayEUG ausdrücklich die Weitergabe von Daten über Schülerinnen und Schüler und Erziehungsberechtigte an außerschulische Stellen, wenn dies - wie vorliegend - nicht der Erfüllung der Aufgaben der Schule dient und auch kein rechtlicher Anspruch auf die Herausgabe der Daten nachgewiesen ist.

Im Ergebnis ist deshalb festzustellen, dass die Veröffentlichung jedweder personenbezogener Daten von Schülerinnen und Schülern sowie von Erziehungsberechtigten auf der Internetseite der Schule eine schriftliche, informierte und freiwillige Einwilligung voraussetzt (vgl. hierzu Nr. 15.1 meines 18. Tätigkeitsberichts 1998 und Nr. 15.1 meines 19. Tätigkeitsberichts 2000). Entsprechendes gilt für Lehrkräfte, die an der Schule keine Funktion mit Außenwirkung wahrnehmen, und sonstige Personen wie z.B. Hausmeister und Sekretärinnen. Erfreulicherweise hat sich das Staatsministerium für Unterricht und Kultus meiner Rechtsauffassung angeschlossen und Anlage 9 zur Durchführungsverordnung entsprechend angepasst.

Hinsichtlich der Einwilligung von Schülerinnen und Schülern war darüber hinaus problematisch, dass es nach dem ursprünglichen Entwurf des Staatsministeriums für Unterricht und Kultus bei allen minderjährigen Schülerinnen und Schülern auf eine wirksame Einwilligung nur der Erziehungsberechtigten ankommen sollte.

Bereits vor einigen Jahren hatte ich mit dem Kultusministerium kontrovers über die Frage diskutiert, ob und ggf. unter welchen Voraussetzungen minderjährige Schülerinnen und Schüler selbst datenschutzrechtlich einwilligen können oder ob bis zur Volljährigkeit eine Einwilligung der Erziehungsberechtigten erforderlich ist. Ich hatte dabei die Auffassung vertreten, dass es darauf ankommt, ob der/die Minderjährige über die Einsichtsfähigkeit in die Tragweite seiner/ihrer Entscheidung verfügt. Da sich die Einwilligung auf tatsächliche Handlungen - nämlich den Eingriff in das Persönlichkeitsrecht - bezieht und keinen rechtsgeschäftlichen Charakter besitzt, ist die Geschäftsfähigkeit des Betroffenen nicht erforderlich. Daraus folgt, dass Jugendliche ab einem bestimmten Alter die datenschutzrechtliche Einsichtsfähigkeit besitzen und dann nur sie - nicht dagegen ihre Erziehungsberechtigten - wirksam in die Verarbeitung ihrer personenbezogenen Daten einwilligen können und müssen. Ab welchem Alter diese Einsichtsfähigkeit vorliegt, kann nur für jede Schülerin und jeden Schüler individuell beurteilt werden; in der Regel dürfte sie ab einem Alter von 14 bis 15 Jahren gegeben sein. Eine von mir vor einigen Jahren initiierte Umfrage bei den Datenschutzbeauftragten des Bundes und der Länder hatte ergeben, dass diese meine Auffassung im Wesentlichen teilen. In einigen Ländern ist sogar gesetzlich klargestellt, dass minderjährige Schülerinnen und Schüler einwilligungsfähig sind, wenn sie die Bedeutung und Tragweite der Einwilligung und ihre rechtlichen Folgen erfassen können und ihren Willen hiernach zu bestimmen vermögen (vgl. § 120 Abs. 2 Satz 3 Schulgesetz für das Land Nordrhein-Westfalen, § 70 Abs. 2 Satz 5 Schulgesetz für das Land Mecklenburg-Vorpommern). Freilich ist auch der vom Staatsministerium für Unterricht und Kultus in der damaligen Diskussion vorgebrachte Hinweis auf die Probleme, die bei einer individuellen Beurteilung der Einsichtsfähigkeit im Schulalltag entstehen könnten, nicht ganz von der Hand zu weisen.

Vor diesem Hintergrund habe ich in meiner Stellungnahme zu dem Verordnungsentwurf als Kompromiss vorgeschlagen, dass die Schule bei minderjährigen Schülerinnen und Schülern, die das 14. Lebensjahr vollendet haben, Einwilligungen sowohl der Schüler(innen) als auch der Erziehungsberechtigten einholt. Auf diese Weise kann verhindert werden, dass sich die Schulen einen Datenschutzverstoß vorwerfen lassen müssen, weil sie die Einwilligung eines/einer einsichtsfähigen Minderjährigen nicht eingeholt haben, obwohl dies nach überwiegender Auffassung

datenschutzrechtlich erforderlich ist. Außerdem wird so vermieden, dass z.B. das Foto eines Minderjährigen mit Einwilligung der Erziehungsberechtigten im Internet veröffentlicht wird, obwohl der Minderjährige selbst dies ablehnt. Zugleich können die Schulen sicher sein, dass sie das Elternrecht beachtet haben, da sie in jedem Fall zusätzlich die Einwilligung der Erziehungsberechtigten einholen. Die festgelegte Altersgrenze von 14 Jahren vermeidet in der Praxis schwierige Einzelfallentscheidungen und stellt sicher, dass alle datenschutzrechtlich notwendigen Einwilligungen vorliegen.

Das Staatsministerium für Unterricht und Kultus hat meinen Vorschlag dankenswerterweise aufgegriffen und in Anlage 9 zur Durchführungsverordnung u.a. bestimmt, dass bei Minderjährigen ab Vollendung des 14. Lebensjahres diese selbst und die Erziehungsberechtigten wirksam einzuwilligen haben.

Schließlich habe ich in meiner Stellungnahme kritisiert, dass der ursprüngliche Entwurf vorsah, die Daten von Personen, die auf Grund der Wahrnehmung einer Funktion mit Außenwirkung ohne Einwilligung veröffentlicht werden können, jeweils erst spätestens am Ende des nachfolgenden Schuljahres zu löschen, in dem die Person die Funktion mit Außenwirkung aufgegeben hat. Ich konnte nicht erkennen, wieso es für die Aufgabenerfüllung der Schule erforderlich sein sollte, diese Daten noch so lange nach Aufgabe dieser Funktion auf den Internetseiten der Schule vorzuhalten. Erfreulicherweise hat sich das Staatsministerium für Unterricht und Kultus auch insoweit meiner Meinung angeschlossen: die in Kraft getretene Fassung der Anlage 9 sieht nunmehr vor, dass die betroffenen Daten jeweils gelöscht werden, sobald die Person die Funktion mit Außenwirkung aufgegeben hat.

### 12.2.4 Passwortgeschützte Lernplattform

Bei den in Anlage 10 zur Durchführungsverordnung beschriebenen Lernplattformen handelt es sich laut Verordnungsbegründung „um in Computernetzwerken bereitgestellte Dienste, die Lerninhalte über das Internet vermitteln und schulische Lernprozesse orts- und zeitungebunden unterstützen." Die Spannweite der Einsatzmöglichkeit einer Lernplattform soll von Aufgaben der Schulorganisation über die Kommunikation im Kollegium bis hin zur eigentlichen pädagogischen Arbeit in virtuellen Klassenräumen reichen. Als Funktionsbereiche sind insbesondere vorgesehen: Präsentation von Lerninhalten und Verwaltung von Dokumenten, Instrumente zur Erstellung sowie Durchführung von Übungen, Kursen und Workshops sowie Kommunikations- und Kooperationswerkzeuge, insbesondere Foren.

Soweit die Teilnahme an der Lernplattform freiwillig ist, erfordert die Speicherung von personenbezogenen Lehrer- und Schülerdaten eine wirksame Einwilligung der Betroffenen. Für eine wirksame Einwilligung muss insbesondere deren Freiwilligkeit gewährleistet sein. Bei der Ausgestaltung des Verfahrens ist deshalb besonders darauf zu achten, dass sich Lehrer und Schüler (bzw. ggf. deren Erziehungsberechtigte) tatsächlich ohne Nachteile frei entscheiden können, ob sie sich an der Lernplattform beteiligen möchten oder nicht.

### 12.3 Einwilligung bei Schülerbefragungen

In den letzten Jahren hat die Zahl der wissenschaftlichen Erhebungen an bayerischen Schulen ständig zugenommen. Hierunter fallen nicht nur so bekannte internationale Schulleistungsstudien wie etwa PISA (Programme for International Student Assessment), DESI (Deutsch Englisch Schülerleistungen International), IGLU (Internationale Grundschul-Lese-Untersuchung) oder TIMSS (Trends in Mathematics and Science Study). Vielmehr wenden sich zunehmend Wissenschaftler an die Schulverwaltung auch mit der Bitte um Genehmigung von Schülerbefragungen mit bundesweiter, bayernweiter oder nur lokal begrenzter Bedeutung.

Bei Leistungsvergleichen, die Zwecken der Qualitätssicherung und -steigerung dienen, kann das zuständige Staatsministerium mit der Genehmigung Schülerinnen, Schüler und Lehrkräfte gem. Art. 111 Abs. 4 BayEUG zur Teilnahme verpflichten (vgl. dazu kritisch Nr. 11.2 meines 22. Tätigkeitsberichts 2006). (Die Teile der) Schülerbefragungen, die über bloße Leistungsvergleiche hinausgehen, dürfen dagegen erst nach vorheriger, datenschutzkonformer Einwilligung der betroffenen Schüler (bzw. ihrer Erziehungsberechtigten), Eltern und Lehrer durchgeführt werden. Einer Einwilligung bedarf es nur dann nicht, wenn die Schülerbefragung so anonymisiert ist, dass die erhobenen Daten nicht mehr auf Personen bezogen werden können. Die datenschutzrechtlichen Anforderungen an eine Anonymisierung personenbezogener Daten und an eine rechtswirksame Einwilligungserklärung habe ich bereits in Nr. 20.2.2 meines 21. Tätigkeitsberichts 2004 exemplarisch dargestellt.

Die Abgrenzung zwischen Personenbeziehbarkeit und Anonymität der erhobenen Daten ist für die Anwendbarkeit des Bayerischen Datenschutzgesetzes und damit - außerhalb des Geltungsbereichs des Art. 111 Abs. 4 BayEUG - für die Frage der Einholung einer Einwilligung der von der Schülerbefragung Betroffenen von ausschlaggebender Bedeutung. Zu dieser Problematik nehme ich wie folgt Stellung:

- Nach der gesetzlichen Begriffsbestimmung des Art. 4 Abs. 1 BayDSG sind personenbezogene Daten Einzelangaben über persönliche oder sachliche Verhältnisse bestimmter oder bestimmbarer natürlicher Personen. Daten

sind also bereits dann personenbezogen, wenn die Person zwar nicht durch die Daten allein (eindeutig) identifiziert wird, jedoch mit Hilfe anderer Informationen festgestellt werden kann.

Nicht personenbezogen im Sinne des Bayerischen Datenschutzgesetzes sind Daten nur dann, wenn sie anonymisiert sind. Nach Art. 4 Abs. 8 BayDSG ist Anonymisieren das Verändern personenbezogener Daten derart, dass die Einzelangaben über persönliche oder sachliche Verhältnisse nicht mehr oder nur mit einem unverhältnismäßig großen Aufwand an Zeit, Kosten und Arbeitskraft einer bestimmten oder bestimmbaren natürlichen Person zugeordnet werden können.

- Von einer Personenbeziehbarkeit und damit einem Personenbezug im Sinne des Art. 4 Abs. 1 BayDSG ist somit schon dann auszugehen, wenn die erhobenen Daten

  - zum einen mittels mathematisch-statistischer Methoden - hier bieten informationstechnische Auswertungs- und Analyseprogramme vielfältige Möglichkeiten u.a. zur Bildung von Merkmalskombinationen - und

  - zum anderen durch zugängliches Zusatzwissen

  auf bestimmte Personen bezogen werden können.

  In diesem Zusammenhang genügt es bereits, dass das zur Re-Individualisierung benötigte fachliche Know-How und die wissenschaftlich-technischen Hilfsmittel am Markt zu haben sind. Auch kommt es nicht darauf an, ob im konkreten Fall die erhebende und speichernde Stelle die Absicht hat, sich etwaiges Zusatzwissen zu besorgen. Vielmehr ist bereits die Möglichkeit der Beschaffung von Zusatzwissen ausreichend, dessen legales Bekanntwerden nach sozialüblichen Maßstäben nicht ausgeschlossen werden kann.

- Gerade im Falle eines Verzichts auf die Erhebung eindeutig identifizierender Daten wie Name oder Adresse dürfte es nach meiner Einschätzung den mit der Genehmigung von Schülerbefragungen befassten öffentlichen Stellen zumeist nicht möglich sein, die mit dem Einsatz von - informationstechnisch überdies zunehmend ausgefeilteren - mathematisch-statistischen Methoden einhergehenden Möglichkeiten einer Re-Individualisierung zuverlässig abzuschätzen. Zudem ist es nach meinen Erfahrungen in der Praxis für die schul- und datenschutzrechtlich verantwortliche Stelle häufig unmöglich, zutreffend zu beurteilen, ob zur Identifikation geeignetes Zusatzwissen existiert und ob es zugänglich ist.

  Vor diesem Hintergrund rate ich dringend dazu, im Zweifel vom Vorliegen einer Personenbeziehbarkeit und damit eines Personenbezugs der erhobenen Daten im Sinne des Art. 4 Abs. 1 BayDSG auszugehen und eine Einwilligung im Sinne des Art. 15 BayDSG bei den Betroffenen einzuholen. Anderenfalls könnte der verantwortlichen Stelle im Falle einer späteren Identifikation - wenn auch nur eines Betroffenen - eine Amtspflichtverletzung vorgeworfen werden. Bei unzutreffender Annahme einer Anonymisierung der erhobenen Daten erfolgt die Schülerbefragung nämlich ohne Rechtsgrundlage (Einwilligung) und damit rechtswidrig, was zudem auch die Notwendigkeit der Vernichtung der Befragungsunterlagen zur Folge hat.

Unabhängig davon empfehle ich grundsätzlich, bei Schülerbefragungen eine datenschutzgerechte Einwilligung der Schüler (bzw. ihrer Erziehungsberechtigten) einzuholen. So ist dann nicht nur in jedem Falle eine tragfähige Rechtsgrundlage für die zum Teil überaus umfangreichen Befragungen gegeben (siehe Art. 15 Abs. 1 Nr. 2 BayDSG). Vielmehr kann meines Erachtens nur durch eine Einwilligung dem (informationellen) Selbstbestimmungsrecht der Schüler (bzw. ihrer Erziehungsberechtigten) in angemessener Weise Rechnung getragen werden - und damit letztlich auch dem schulischen Bildungs- und Erziehungsauftrag, siehe Art. 131 Bayerische Verfassung und vor allem Art. 2 Abs. 1 Satz 1 Unterabsatz 2 BayEUG: „Befähigung zu selbständigem Urteil und eigenverantwortlichem Handeln“. Nicht zuletzt dient die Einholung einer Einwilligung auch der rechtlichen Absicherung der datenschutzrechtlich verantwortlichen öffentlichen Stelle.

Ich habe das Staatsministerium für Unterricht und Kultus daher darum gebeten, seine nachgeordneten Dienststellen darauf hinzuweisen, bei Schülerbefragungen - außer in den Fällen des Art. 111 Abs. 4 BayEUG - immer eine Einwilligung der betroffenen Schüler (bzw. ihrer Erziehungsberechtigten) einzuholen.

### 12.4 Vertretungsplan auf der Schulhomepage

Eine Schule fragte bei mir an, ob es datenschutzrechtlich zulässig ist, den Vertretungsplan täglich aktualisiert auf die Schulhomepage zu stellen. Dieses Vor-

haben habe ich datenschutzrechtlich wie folgt bewertet:

Im Zuge der Erstellung des Vertretungsplans werden die dazu erforderlichen Personalaktendaten der Lehrkräfte zu Sachaktendaten, auf die die allgemeinen Datenschutzvorschriften des Bayerischen Datenschutzgesetzes Anwendung finden. Ebenso wie der Aushang des Vertretungsplans im Schulgebäude stellt die Einstellung des Vertretungsplans auf die Schulhomepage in datenschutzrechtlicher Hinsicht eine Datenverarbeitung in Form der Datenübermittlung dar (siehe Art. 4 Abs. 6 BayDSG). Nach Art. 15 Abs. 1 BayDSG ist die Übermittlung personenbezogener Daten allerdings nur dann datenschutzrechtlich zulässig, wenn eine Rechtsvorschrift sie gestattet (Nr. 1) oder die Betroffenen wirksam eingewilligt haben (Nr. 2).

- Als Rechtsvorschrift für die Übermittlung der im Vertretungsplan enthaltenen personenbezogenen Daten der Lehrkräfte an die Nutzer der Schulhomepage kommt allein Art. 85 Abs. 1 Satz 1 BayEUG in Betracht. Für die datenschutzrechtliche Zulässigkeit ist danach entscheidend, ob die Veröffentlichung des Vertretungsplans im Internet zur ordnungsgemäßen Aufgabenerfüllung der Schule erforderlich ist.

  In Bezug auf schulische Veröffentlichungen im Internet führen die mit mir abgestimmten und für die Schulen verbindlichen „Erläuternden Hinweise für die Schulen zum Vollzug des Bayerischen Datenschutzgesetzes“ (Bekanntmachung des Bayerischen Staatsministeriums für Unterricht und Kultus und Wissenschaft, Forschung und Kunst vom 19.04.2001, KWMBl I S. 112, geändert durch Bekanntmachung vom 10.10.2002, KWMBl I S. 354; abrufbar von meiner Homepage www.datenschutz-bayern.de unter der Rubrik „Recht und Normen“ - „Schul- und Hochschulrecht“) unter Nr. 4.4 Buchstabe e) wörtlich aus:

  „Bei Veröffentlichungen der Schule (beispielsweise in Form einer Homepage im Internet) ist zu beachten, dass in Hinblick auf die enge lokale Begrenzung des Aufgaben- und Wirkungsbereichs von Schulen das Persönlichkeitsrecht der Schüler, Eltern, Lehrer und des sonstigen Schulpersonals Vorrang vor dem Informationsinteresse einer breiteren Öffentlichkeit hat. … Vor der Einstellung personenbezogener Daten ins Internet (…) ist daher die Einwilligung der Betroffenen einzuholen (…).“

  Darüber hinaus ist auch zu bedenken, dass mit der Online-Veröffentlichung der in einem Vertretungsplan enthaltenen personenbezogenen Lehrerdaten besondere Risiken verbunden sind, vor allem im Hinblick auf eine kommerzielle Nutzung - in diesem Zusammenhang erinnere ich nur an die umfangreichen Möglichkeiten des Data- bzw. Web-Mining. Zudem besteht bei der Einstellung eines täglich aktualisierten Vertretungsplans ins Internet die Gefahr, dass aus den Angaben über einen längeren Zeitraum Verhaltensprofile einzelner Lehrkräfte erstellt werden können - also etwa über krankheitsbedingte Fehlzeiten oder regelmäßige, funktionsbedingte Abwesenheiten.

  Schließlich ist es zur ordnungsgemäßen Aufgabenerfüllung der Schule im Rahmen der Erstellung eines Vertretungsplans nur erforderlich, dass die von einem konkreten Unterrichtsausfall betroffenen Personen Kenntnis davon erlangen, welche Lehrkraft in welcher Unterrichtsstunde vertreten wird. Über dieses Erfordernis geht eine letztlich weltweite Veröffentlichung des Vertretungsplans durch Einstellung ins Internet jedenfalls weit hinaus. Art. 85 Abs. 1 Satz 1 BayEUG scheidet somit als Rechtsgrundlage aus.

- Damit ist die Veröffentlichung des Vertretungsplans auf der Schulhomepage gem. Art. 15 Abs. 1 Nr. 2 BayDSG nur mit ausdrücklicher Einwilligung der betroffenen Lehrkräfte zulässig.

  Bei der Einholung einer Einwilligung sind allerdings die vom Gesetzgeber in Art. 15 Abs. 2 bis 4 BayDSG aufgestellten, strengen Anforderungen einzuhalten. Danach stellt eine Einwilligung nur dann eine tragfähige Rechtsgrundlage dar, wenn sie freiwillig, informiert und grundsätzlich schriftlich erfolgt. Dies hat u.a. zur Folge, dass die Lehrkräfte von der Schule umfassend über die mit der Einstellung ihrer personenbezogenen Daten ins Internet verbundenen Gefahren und möglichen nachteiligen Auswirkungen aufgeklärt werden müssen.

Im Ergebnis dürfte somit eine datenschutz- und rechtskonforme Einstellung des Vertretungsplans auf die Schulhomepage - wenn überhaupt - nur sehr schwer zu verwirklichen sein. Angesichts der mit einer Einstellung des Vertretungsplans ins Internet verbundenen Gefahren für das Persönlichkeitsrecht der Lehrkräfte rate ich jedenfalls dringend davon ab.

### 12.5 Datenschutz bei Schulchroniken

Im Berichtszeitraum machte mich ein betroffener Bürger auf folgenden Sachverhalt aufmerksam: Anlässlich des 40-jährigen Schuljubiläums der örtlichen

Grundschule planten Elternbeirat und Schulleitung, eine umfangreiche, frei verkäufliche Schulchronik zu erstellen. In dieser Schulchronik sollten u.a. Klassenfotos und Namenslisten der Schülerinnen und Schüler aller bisherigen 40 Jahrgänge abgedruckt werden.

Nicht nur Schülernamenslisten, sondern auch Klassenfotos enthalten personenbezogene Daten im Sinne des Art. 4 Abs. 1 BayDSG. Die Veröffentlichung einer derartige Daten umfassenden Schulchronik stellt in datenschutzrechtlicher Hinsicht eine Datenübermittlung an nicht-öffentliche Stellen dar. Die Übermittlung von Schülerdaten ist in der Spezialbestimmung des Art. 85 BayEUG geregelt. Nach Art. 85 Abs. 2 Satz 1 BayEUG ist die Weitergabe von Daten und Unterlagen über Schülerinnen und Schüler an außerschulische Stellen durch die Schule in der Regel untersagt.

Als Ausnahme von diesem grundsätzlichen Übermittlungsverbot ist der Schule in Art. 85 Abs. 3 BayEUG die Herausgabe eines Jahresberichts in Papierform erlaubt, der allerdings im Wesentlichen nur Name, Geburtsdatum, Jahrgangsstufe und Klasse der Schülerinnen und Schüler enthalten darf. Die Veröffentlichung von Schülerfotos in Jahresberichten ist demzufolge nur mit Einwilligung der Betroffenen zulässig. Zu datenschutzrechtlichen Fragen im Zusammenhang mit schulischen Jahresberichten habe ich mich bereits in Nr. 15.1 meines 19. Tätigkeitsberichts 2000 sowie in Nr. 20.1.3 meines 21. Tätigkeitsberichts 2004 eingehend geäußert.

Eine die Veröffentlichung einer Schulchronik gestattende Ausnahmebestimmung enthält Art. 85 BayEUG dagegen nicht. Auch ist die die Herausgabe eines Jahresberichts erlaubende Vorschrift des Art. 85 Abs. 3 BayEUG mangels Vergleichbarkeit nicht entsprechend auf eine Schulchronik anwendbar. Der Jahresbericht dient vor allem dazu, den Schülerinnen und Schülern zur Erinnerung Informationen über das aktuelle Schuljahr zukommen zu lassen. So soll beispielsweise die Organisation von (zukünftigen) Klassentreffen erleichtert werden. Zu diesem Zweck werden die Schülerdaten durch den Jahresbericht in der Regel nur den Schülern und Erziehungsberechtigten des aktuellen Jahrgangs zugänglich gemacht. Im Unterschied dazu sollte die Schulchronik in dem von mir zu beurteilenden Fall Klassenfotos und Namenslisten der Schülerinnen und Schüler aus 40 Jahrgängen enthalten und darüber hinaus auch an andere Personen als die aktuellen Schüler und Erziehungsberechtigten verkauft werden.

Ebenso wie generell die Veröffentlichung von Klassenfotos ist deshalb auch die Veröffentlichung von Schülernamenslisten in einer Schulchronik nur mit ausdrücklicher und informierter Einwilligung der Betroffenen (volljährige Schüler / Erziehungsberechtigte bei minderjährigen Schülern) im Sinne des Art. 15 Abs. 1 Nr. 2 BayDSG zulässig. Für eine rechtswirksame Einwilligung hat dabei die Schule die vom Gesetzgeber in Art. 15 Abs. 2 bis 4 BayDSG aufgestellten strengen Anforderungen (Hinweispflichten, Schriftform etc.) einzuhalten.

### 12.6 Gesundheitsdaten in Schulzeugnissen

Mehrfach habe ich mich im Berichtszeitraum mit der Problematik befasst, ob und ggf. unter welchen Voraussetzungen Schulzeugnisse Gesundheitsdaten enthalten dürfen. So hatte beispielsweise in einem mir zur Stellungnahme vorgelegten Fall eine Lehrkraft im Zeugnis darauf hingewiesen, dass der betroffene Schüler wegen einer Aufmerksamkeitsdefizit-/Hyperaktivitätsstörung (ADHS) medikamentös behandelt wird.

Ausgangspunkt für die Beurteilung der datenschutzrechtlichen Zulässigkeit der Aufnahme von Gesundheitsdaten in Schulzeugnisse sind die schulrechtlichen Regelungen über den Inhalt von Zeugnissen. Nach Art. 52 Abs. 3 Satz 2 BayEUG werden in den Schulzeugnissen die gesamten Leistungen einer Schülerin bzw. eines Schülers unter Wahrung der Gleichbehandlung aller Schülerinnen und Schüler in pädagogischer Verantwortung der Lehrkraft bewertet. Daneben sollen gemäß Art. 52 Abs. 3 Satz 3 BayEUG Bemerkungen über Anlagen, Mitarbeit und Verhalten der Schülerin oder des Schülers in das Zeugnis aufgenommen werden.

Sinn und Zweck der Bemerkungen über Anlagen, Mitarbeit und Verhalten ist es, der schulischen Erziehungsaufgabe auch über die Bewertung der objektiv erbrachten Leistung hinaus nachzukommen. Der in Bayern maßgebliche Kommentar zum Schulrecht (Kiesl/Stahl, Das Schulrecht in Bayern, Band 1, Kronach/München/Bonn/Potsdam, Stand: 2007, Kennziffer 11.52, Anmerkung 14) führt insoweit wörtlich aus: „Bewertet wird nur die objektiv erbrachte Leistung. Anlagen, Mitarbeit und Verhalten des Schülers haben mit der objektiv erbrachten Leistung nichts zu tun, ihre Würdigung und auch Beeinflussung gehören jedoch zur Erziehungsaufgabe der Schule."

Bei der Erfüllung der aus dem verfassungsrechtlichen Bildungs- und Erziehungsauftrag des Art. 131 BV folgenden, in Art. 1 und 2 BayEUG näher umschriebenen Aufgaben der Schulen wirken gemäß Art. 2 Abs. 3 Satz 1 BayEUG alle Beteiligten, insbesondere Schule und Elternhaus, vertrauensvoll zusammen. Daher darf die Schule den Eltern Umstände mitteilen, die die schulische Entwicklung des Kindes beeinflussen können; diese Umstände können auch die Gesundheit des Schülers betreffen. Da sich Schulzeugnisse nicht nur an den jeweiligen Schüler, sondern vor allem an die Eltern richten, kann und soll diese Mitteilung auf der Grundlage des Art. 52 Abs. 3 Satz 3 BayEUG in den Zeugnissen erfolgen. Die Begriffe „Anlagen" und „Verhalten" können somit je

nach Lage des Einzelfalls auch Daten zur Gesundheit umfassen.

Vor diesem Hintergrund kommt es für die datenschutzrechtliche Beurteilung im Einzelfall zunächst entscheidend darauf an, ob die Aufnahme von Gesundheitsdaten in ein Zeugnis im Rahmen der schulischen Erziehungsaufgabe aus pädagogischen Gründen erfolgt. Selbst wenn dies der Fall ist, bedeutet dies jedoch keineswegs, dass Gesundheitsdaten in beliebigem Umfang und in beliebiger Sensibilität in das Zeugnis aufgenommen werden dürfen. Vielmehr ist in jedem Einzelfall sorgfältig zu prüfen, ob die zur Aufnahme in das Zeugnis vorgesehenen Gesundheitsdaten nach Umfang und Sensibilität tatsächlich erforderlich sind, um den Bildungs- und Erziehungsauftrag von Schule und Elternhaus erfüllen zu können. So ist es auch durchaus vorstellbar, dass pädagogische Gründe zum Schutz des Kindes gerade gegen die Aufnahme von Gesundheitsdaten in ein Zeugnis sprechen. Jedenfalls ist die Aufnahme von Gesundheitsdaten in ein Schulzeugnis im konkreten Einzelfall nur dann datenschutzrechtlich zulässig, wenn dem Anspruch des betroffenen Schülers auf Persönlichkeitsschutz unter Beachtung des Verhältnismäßigkeitgrundsatzes im Wege einer umfassenden Gesamtabwägung Rechnung getragen wird.

Die Feststellung und Bewertung der pädagogischen Motivation zur Aufnahme von Gesundheitsdaten in ein Schulzeugnis stellt in erster Linie eine Fachfrage dar. Diese lässt sich nach meiner Einschätzung am ehesten in einem persönlichen Gespräch der Erziehungsberechtigten mit der betreffenden Lehrkraft, ggf. auch mit der Schulleitung klären. In diesem Gespräch könnte einerseits die Lehrkraft gebeten werden, ihre Motivationslage im Einzelnen darzulegen; andererseits könnte auf Gesichtspunkte hingewiesen werden, die zum Schutz des Kindes gegen eine Aufnahme der Gesundheitsdaten in das Zeugnis sprechen.

### 12.7 Lautsprecherdurchsagen mit namentlicher Nennung der von Erziehungsmaßnahmen betroffenen Schüler

Auf der Grundlage eines Beschlusses des Schulforums wurden an einer Schule Schülerinnen und Schüler bei Regelverletzungen zu so bezeichneter „Sozialarbeit“ auf dem Schulgelände wie beispielsweise Aufräumen angehalten. Hierbei handelte es sich um pädagogisch-erzieherische Maßnahmen unterhalb der Stufe von Ordnungsmaßnahmen (z.B. Verweis). Immer freitags forderte der für die „Sozialarbeit“ zuständige Lehrer mittels Lautsprecherdurchsage im gesamten Schulbereich die jeweils betroffenen Schülerinnen und Schüler unter Namensnennung auf, sich bei ihm nach Unterrichtsschluss einzufinden; diese Durchsage war daher an der Schule als „Freitagsdurchsage“ bekannt.

Nach Anhörung der betroffenen Schule habe ich diesen Sachverhalt aus datenschutzrechtlicher Sicht wie folgt bewertet:

Nach Art. 85 Abs. 1 Satz 1 BayEUG sind die Erhebung und die Verarbeitung von Daten zur Erfüllung der den Schulen durch Rechtsvorschriften jeweils zugewiesenen Aufgaben zulässig. Entscheidend für die datenschutzrechtliche Beurteilung war es demnach, ob der Ausruf der betroffenen Schülerinnen und Schüler über Lautsprecher im gesamten Schulgelände im Hinblick auf den den Schulen gemäß Art. 1 und 2 BayEUG obliegenden gesetzlichen Bildungs- und Erziehungsauftrag aus pädagogischen Gründen erforderlich war.

In diesem Zusammenhang ist zunächst darauf hinzuweisen, dass die Schulen bei der Wahl des Übermittlungsmediums nach Nr. 4.4 Buchst. a) Satz 3 der „Erläuternden Hinweise für die Schulen zum Vollzug des Bayerischen Datenschutzgesetzes“ (Bekanntmachung des Bayerischen Staatsministeriums für Unterricht und Kultus und Wissenschaft, Forschung und Kunst vom 19.04.2001, KWMBl S. 112, geändert durch Bekanntmachung vom 10.10.2002, KWMBl S. 354) im Hinblick auf die enge lokale Begrenzung ihres Aufgaben- und Wirkungskreises darauf zu achten haben, dass das Persönlichkeitsrecht der Schüler weitmöglichst gewahrt bleibt und Vorrang vor einem allgemeinen Informationsinteresse hat.

Daher machte allein die von der Schule vorgebrachte Tatsache, dass Lautsprecherdurchsagen aus diversen Anlässen üblich sind und ein geeignetes Organisationsmittel für die Schulabläufe darstellen, diese in der vorliegenden Fallgestaltung noch nicht aus pädagogischen Gründen erforderlich. Ohnehin waren Zeitpunkt und Organisation der „Sozialarbeit“ sowohl den an der Schule Beschäftigten als auch den Schülerinnen und Schülern bekannt. Die Aufforderung des für die „Sozialarbeit“ zuständigen Lehrers an einzelne Schülerinnen und Schüler, sich bei ihm am Freitag nach Unterrichtsschluss einzufinden, ließ auch ohne nähere anlassbezogene Angaben den Grund der Einbestellung für alle Zuhörer erkennen. So wurde diese Durchsage nicht ohne Grund allgemein „Freitagsdurchsage“ genannt.

Durch die schulöffentlichen Lautsprecherdurchsagen wurden die von Maßnahmen der „Sozialarbeit“ betroffenen Schülerinnen und Schüler vielmehr in erheblichem Maße in ihrem Persönlichkeitsrecht beeinträchtigt. Einige Schüler fühlten sich durch die Lautsprecherdurchsagen sogar in der Schulöffentlichkeit „an den Pranger gestellt“. Jedenfalls bestand die Gefahr, dass die Durchsage eines betroffenen Schülers zu einer schulöffentlichen Vorverurteilung führte, die insbesondere auch die (künftigen) Lehrer des Betroffenen negativ beeinflussen konnte, so dass den Betroffenen im Extremfall nur der Schulwechsel blieb. Da die betroffenen Schülerinnen und Schüler

zudem problemlos auf vielfältigen anderen Wegen über ihren abzuleistenden Dienst unterrichtet werden konnten, war die Durchsage der Namen mittels Lautsprecher zur Aufgabenerfüllung der Schule in datenschutzrechtlicher Hinsicht nicht erforderlich. Die Voraussetzungen des Art. 85 Abs. 1 Satz 1 BayEUG lagen damit nicht vor.

Da die Schule die datenschutzrechtlich unzulässige „Freitagsdurchsage“ schließlich eingestellt hat, habe ich im Rahmen meines Ermessens von einer förmlichen Beanstandung gemäß Art. 31 Abs. 1 und 3 BayDSG abgesehen.

Das von mir in der vorliegenden Angelegenheit eingeschaltete Staatsministerium für Unterricht und Kultus hat mir zugesagt, bei den Schulen auf die Beachtung dieser datenschutzrechtlichen Vorgaben in vergleichbaren Fällen hinzuwirken.

# 13 Hochschulen

## 13.1 Einsicht in Hochschulzeugnisse verstorbener Verwandter zur Familienforschung

„Aus Datenschutzgründen“ hatte eine Hochschule der Bitte einer Bürgerin um Überlassung einer Zweitschrift des vor über 50 Jahren ausgestellten Diplomzeugnisses ihres vor drei Jahren verstorbenen Vaters nicht entsprochen. Da sie das Zeugnis benötigte, um den Lebensweg ihres Vaters für die Familiengeschichte zu dokumentieren, wandte sich die Bürgerin mit einer Petition an mich.

Im Wege einer umfassenden datenschutzrechtlichen Überprüfung des vorgetragenen Sachverhalts bin ich zu dem Ergebnis gelangt, dass der Petentin zwar kein Anspruch auf Einsicht in das Hochschulzeugnis ihres Vaters zustand. Allerdings konnte sie verlangen, dass die Hochschule über einen Antrag auf Akteneinsicht nach pflichtgemäßem Ermessen entscheidet.

- Das Begehren ließ sich freilich nicht auf Art. 10 Abs. 1 Satz 1 Nr. 1 BayDSG stützen. Denn diese Vorschrift gewährt nur dem Betroffenen - im konkreten Fall also dem (zwischenzeitlich verstorbenen) Vater - einen Anspruch auf Auskunft über die zur Person gespeicherten Daten.

- Für die Daten Verstorbener ist das Bayerische Archivgesetz (BayArchivG) von besonderer Bedeutung. Im konkreten Fall konnte jedoch dahingestellt bleiben, ob es sich bei dem Diplomzeugnis des verstorbenen Vaters überhaupt um Archivgut handelt. Denn selbst wenn dies so sein sollte, waren hier keine Ansprüche aus dem Bayerischen Archivgesetz ableitbar. Art. 10 Abs. 2 Satz 1 BayArchivG (auf Archivgut der staatlichen Hochschulen anwendbar gemäß Art. 14 Abs. 1 Satz 3 i.V.m. Art. 13 Abs. 2 BayArchivG) bestimmt, dass Archivgut u.a. nur benützt werden kann, wenn Schutzfristen nicht entgegenstehen. Art. 10 Abs. 3 Satz 2 BayArchivG bestimmt für Archivgut, das sich - wie im vorliegenden Fall - auf natürliche Personen bezieht (personenbezogenes Archivgut), eine Schutzfrist von zehn Jahren nach dem Tod des Betroffenen.

  Die Voraussetzungen für eine Verkürzung dieser Schutzfrist waren nicht gegeben. Zum einen lag schon die nach Art. 10 Abs. 4 Satz 1 BayArchivG hierzu erforderliche Zustimmung der Hochschule nicht vor. Zum anderen verlangt Art. 10 Abs. 4 Satz 2 BayArchivG u.a., dass die Benützung aus „im überwiegenden Interesse der abgebenden Stelle oder eines Dritten liegenden Gründen unerlässlich“ ist. Gemessen an diesen strengen Anforderungen reichte der ideelle Wunsch der Eingabeführerin nach einer Dokumentation des Lebensweges ihres verstorbenen Vaters für eine Verkürzung der Schutzfristen nicht aus. Ein überwiegendes Interesse der Petentin, das eine Benützung unerlässlich erscheinen lässt, war so nicht begründbar.

- Auch Art. 29 Abs. 1 BayVwVfG, der den Beteiligten einen Anspruch auf Einsicht in die das Verfahren betreffenden Akten gewährt, war keine Rechtsgrundlage für das Begehren. Von dem abgesehen, dass die Petentin selbst nicht Beteiligte an dem das Diplomzeugnis ihres Vaters betreffenden Verwaltungsverfahren gewesen war, gewährt Art. 29 Abs. 1 BayVwVfG nur bis zu dem vorliegend schon vor Jahrzehnten erfolgten Abschluss des Verfahrens ein Akteneinsichtsrecht.

- Ein allgemeiner Anspruch eines Nicht-Beteiligten auf Akteneinsicht außerhalb des Verwaltungsverfahrens besteht nach der Rechtsprechung des Bundesverwaltungsgerichts (BVerwG) und des Bayerischen Verwaltungsgerichtshofs (BayVGH) grundsätzlich nicht. Kann der Antragsteller in solchen Fällen ein berechtigtes Interesse an der Auskunftserteilung geltend machen, hat die Behörde allerdings nach pflichtgemäßem Ermessen darüber zu entscheiden, ob sie die Auskunft erteilen will oder nicht (BVerwG vom 01.10.1987, Az. 8 B 108/97 m.w.N.; BayVGH vom 17.02.1998, Az. 23 B 95.1954 m.w.N.). Nach Auffassung des BayVGH ist die Ermessensentscheidung dabei so zu treffen, dass „unter Berücksichtigung des Grundprinzips des rechtsstaatlichen, fairen Verfahrens eine

beiderseits sachgerechte Interessenwahrung möglich ist“ (BayVGH a.a.O.).

Diese Grundsätze entsprechen denen einer Prüfung nach Art. 19 Abs. 1 Nr. 2 BayDSG. Nach dieser Vorschrift ist eine Datenübermittlung zulässig, wenn die nicht-öffentliche Stelle ein berechtigtes Interesse an der Kenntnis der zu übermittelnden Daten glaubhaft darlegt und der Betroffene kein schutzwürdiges Interesse an dem Ausschluss der Übermittlung hat. Ein berechtigtes Interesse ist jedes nach vernünftigen Erwägungen unter Berücksichtigung der Besonderheiten des Einzelfalls anzuerkennendes, der Rechtsordnung nicht widersprechendes Interesse. Umfasst sind damit nicht nur die im Zusammenhang mit der Verfolgung von Rechten stehenden rechtlichen Interessen, sondern auch ideelle und wirtschaftliche Interessen. Ein berechtigtes Interesse setzt allerdings voraus, dass der Empfänger die Daten in irgendeiner Form benötigt, wofür schon das Interesse an der Schaffung eines vernünftigerweise zuzubilligenden Informationsstandes an sich ausreichen kann. (Vgl. zum Ganzen Wilde/Ehmann/Niese/Knoblauch, Bayerisches Datenschutzgesetz, Kommentar, München, Art. 19 BayDSG Rdnr. 15.)

Daran gemessen war der Eingabeführerin nach meiner Auffassung im konkreten Fall ein berechtigtes Interesse an der Akteneinsicht zuzugestehen. Denn hierfür reicht das ideelle Interesse an der Dokumentation des Lebensweges ihres verstorbenen Vaters für die Familiengeschichte aus.

Ich habe der Petentin deshalb geraten, bei der Hochschule einen Antrag auf Akteneinsicht zu stellen. Die Hochschule hatte dann nach pflichtgemäßem Ermessen darüber zu entscheiden, ob sie Akteneinsicht gewährt. Dabei hatte sie entsprechend den Grundsätzen des Art. 19 Abs. 1 Nr. 2 BayDSG eine umfassende Abwägung vorzunehmen. Für die Gewährung der Akteneinsicht sprach insbesondere, dass es sich bei der Antragstellerin um die Tochter des Verstorbenen, also ein nahe Verwandte, handelte. Allerdings konnte ich nicht von vornherein ausschließen, dass die Hochschule das Akteneinsichtsrecht ermessensfehlerfrei verweigern kann. Aus datenschutzrechtlichen Gründen zwingend war eine ablehnende Entscheidung jedoch keinesfalls.

# 14 Gesundheitsverwaltung, Veterinärverwaltung und Verbraucherschutz

## 14.1 Errichtung einer zentralen und einheitlichen Datenbank zur Lebensmittel-, Veterinär- und Futtermittelkontrolle durch die Gesundheitsverwaltung („TIZIAN“)

Im Berichtszeitraum betrieb das Bayerische Landesamt für Gesundheit und Lebensmittelsicherheit (LGL) im Auftrag des Bayerischen Staatsministeriums für Umwelt und Gesundheit (StMUG) die Einführung einer „Gemeinsamen EDV für den Gesundheitlichen Verbraucherschutz“ („TIZIAN“), mit dem Ziel, ein zentrales EDV-System zur effizienten und qualitätsgesicherten Erfüllung der Aufgaben im gesundheitlichen Verbraucherschutz aufzubauen, das behördenübergreifend von den insgesamt 105 zuständigen Behörden (96 Kreisverwaltungsbehörden, 7 Regierungen, LGL, StMUG) einheitlich im Veterinärbereich, der Lebensmittel- und Futtermittelkontrolle genutzt werden kann. Dazu wurde beim Bayerischen Rechenzentrum Süd in München eine zentrale Datenbank eingerichtet, in die umfangreiche Datenbestände eingestellt und von dort abgefragt werden können.

Leider hat mich das StMUG erst in einem sehr fortgeschrittenen Stadium des Projekts beteiligt. Es war mir deshalb auch erst sehr spät möglich, die datenschutzrechtlichen Anforderungen für das Projekt TIZIAN aufzuzeigen:

Es handelt sich bei dem Projekt um ein automatisiertes Verfahren, das mehreren Daten verarbeitenden Stellen gemeinsam die Verarbeitung und Nutzung personenbezogener Daten ermöglicht. Eine solche Konstruktion wird als gemeinsames und/oder verbundenes (automatisiertes) Verfahren oder auch kurz als Verbunddatei bezeichnet. Durch den Einsatz der Verbunddatei werden personenbezogene Daten erhoben, verarbeitet und genutzt. Dies stellt einen Eingriff in das durch Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 Grundgesetz (GG) gewährleistete Grundrecht auf informationelle Selbstbestimmung als besondere Ausprägung des allgemeinen Persönlichkeitsrechts dar. Das Recht auf informationelle Selbstbestimmung kann im überwiegenden Allgemeininteresse eingeschränkt werden. Das StMUG hat mir dargelegt, dass das Projekt TIZIAN dem gesundheitlichen Verbraucherschutz dient. Ich bin im Rahmen meiner datenschutzrechtlichen Prüfung zu dem Ergebnis gelangt,

dass dieses Ziel einen legitimen Gemeinwohlbelang darstellt, der Einschränkungen des Grundrechts auf informationelle Selbstbestimmung im Rahmen des Grundsatzes der Verhältnismäßigkeit grundsätzlich zu rechtfertigen vermag.

Das StMUG hat die Notwendigkeit des Projektes damit begründet, dass die Behörden des gesundheitlichen Verbraucherschutzes ihre vielfältigen, überwiegend durch EU- und Bundesrecht vorgegebenen Aufgaben nur durch eine gemeinsame Datenbank erfüllen könnten. Die bisherige Form der Zusammenarbeit, also im Wesentlichen Datenerhebung und -übermittlung im Einzelfall auf Anfrage, reiche ebenso wenig aus, wie die (dezentrale) Vernetzung der getrennten Datenbestände zur Ermöglichung eines automatisierten Abrufs. Auf der Grundlage dieser fachlichen Beurteilung erschien mir die Annahme der grundsätzlichen Erforderlichkeit der Einrichtung einer Verbunddatei vertretbar.

Ich habe jedoch nachdrücklich darauf hingewiesen, dass der mit dem Projekt TIZIAN verbundene Grundrechtseingriff einer gesetzlichen Grundlage bedarf, die hinreichend klar und bestimmt ist.

Zum Zeitpunkt der Beurteilung für die Verbunddatei des Projekts TIZIAN fehlte eine solche hinreichend klare und bestimmte gesetzliche Grundlage.

Auf die allgemeinen Rechtsgrundlagen des BayDSG für die Datenerhebung, -verarbeitung und -nutzung (Art. 15 ff. BayDSG) sowie für die Einrichtung eines automatisierten Abrufverfahrens (Art. 8 BayDSG) konnte die Verbunddatei nicht gestützt werden. Denn diesen Vorschriften liegt die Vorstellung zu Grunde, dass jede öffentliche Stelle ihre jeweiligen Daten getrennt von den Daten anderer öffentlicher Stellen erhebt, verarbeitet und nutzt. Auch bei einem automatisierten Abrufverfahren bleiben die Datenbestände der öffentlichen Stellen getrennt, lediglich die Art und Weise der Datenerhebung und -übermittlung wird modifiziert. Eine gemeinsame oder verbundene Datenverarbeitung mehrerer Daten verarbeitenden Stellen ist hingegen im BayDSG nicht vorgesehen. Es ist aus den Vorschriften des BayDSG weder für die Behörden noch für die Gerichte und schon gar nicht für den betroffenen Bürger erkennbar, ob und ggf. unter welchen Voraussetzungen, in welcher Art und Weise und in welchem Umfang mehreren öffentlichen Stellen eine gemeinsame oder verbundene Datenverarbeitung erlaubt sein soll.

Darüber hinaus nimmt die Eingriffsintensivität durch die Einrichtung einer Verbunddatei deutlich zu: Eine Verbunddatei beinhaltet einen umfassenden Datenbestand, für den eine Vielzahl von Zugriffsberechtigungen besteht (hier: Zusammenführung der Daten sämtlicher Behörden des gesundheitlichen Verbraucherschutzes in Bayern, umfassende gegenseitige Zugriffsrechte sämtlicher damit befasster Mitarbeiter dieser Behörden). Damit wird der Zugriff auf von Dritten gespeicherte Daten wesentlich erleichtert und schwerer kontrollierbar. Die Gefahr einer missbräuchlichen Verwendung der Daten ist deutlich erhöht. Für den Bürger wird zudem unklarer, wer für die Datenerhebung, -verarbeitung und -nutzung verantwortlich ist und wem gegenüber er seine Rechte (z.B. den Anspruch auf Auskunft) geltend machen kann.

Ich habe das StMUG darauf hingewiesen, dass nach meiner Auffassung das Projekt TIZIAN eine gesetzliche Ermächtigung zur Einrichtung einer Verbunddatei erfordert, ggf. ergänzt durch eine Rechtsverordnung, die insbesondere folgende Punkte regelt:

- allgemeine Ermächtigung zur Einrichtung einer Verbunddatei bzw. eines gemeinsamen und/oder verbundenen (automatisierten) Verfahrens
- Zweck der Einrichtung einer Verbunddatei
- Angaben zum Inhalt und Umfang der Verbunddatei
- Angabe der öffentlichen Stellen, welche Daten in der Verbunddatei erheben, verarbeiten und nutzen
- Vorgaben z.B. zur Verantwortlichkeit, zu den Zugriffsberechtigungen, zu den Auskunftsregelungen, zur Protokollierung

Darüber hinaus müssen die Grundzüge der Lese- und Schreibberechtigungen und die Zugriffsmodalitäten in einer Rechtsgrundlage für die Verbunddatei des Verfahrens TIZIAN, ggf. ergänzend in einer Rechtsverordnung, normenklar und normenbestimmt geregelt werden.

Die Regelung sollte insbesondere folgende Punkte umfassen:

- Festlegung, welche öffentlichen Stellen/Funktionen zur Speicherung welcher Datenarten und unter welchen Voraussetzungen zur Veränderung befugt sind (Schreibzugriff)
- Festlegung, welche öffentlichen Stellen/Funktionen unter welchen Voraussetzungen zur Erhebung, Übermittlung und Nutzung welcher Datenarten befugt sind (Lesezugriff)
- Zulassung der Datenerhebung und -übermittlung im Wege eines automatisierten Abrufverfahrens
- Regelungen, die sicherstellen, dass bei der konkreten Ausgestaltung des Datenverarbeitungsprogramms für die Verbunddatei des

Projekts TIZIAN der Grundsatz der Datenvermeidung und Datensparsamkeit beachtet wird, hier insbesondere: statt unbeschränkter Einsicht in den Gesamtbestand aller Betriebe nur Zugriff auf die angezeigten Treffer nach Eingabe eines Begriffs in eine Suchmaske

- vollständige Protokollierung der Lese- und Schreibzugriffe zum Zweck der Datenschutzkontrolle, Festlegung eines Zeitpunkts, zu dem die Protokolldaten spätestens zu löschen sind.

Inhaltlich dürfen die Festlegungen zu den Lese- und Schreibberechtigungen sowie den Zugriffmodalitäten selbstverständlich nur dem Grundsatz der Verhältnismäßigkeit entsprechende Eingriffe in das Grundrecht auf informationelle Selbstbestimmung vorsehen.

Um dem Grundsatz der Normenklarheit und Normenbestimmtheit Genüge zu tun, sollte in die Rechtsgrundlage für das Projekt TIZIAN eine Sondervorschrift zur eindeutigen Regelung der datenschutzrechtlichen Verantwortlichkeiten aufgenommen werden. Solange keine abweichende Sondervorschrift zur Regelung der Verantwortlichkeit besteht, wären sonst bei der Verbunddatei des Projekts TIZIAN das StMUG sowie sämtliche Kreisverwaltungsbehörden, alle Regierungen und das Landesamt für Gesundheit und Lebensmittelsicherheit (LGL) speichernde bzw. verantwortliche Stellen.

Löschfristen sind für die Gewährleistung des Grundrechts auf informationelle Selbstbestimmung von erheblicher Bedeutung. Bei der Schaffung einer Rechtsgrundlage für das Projekt TIZIAN sollten deshalb auf normativer Ebene verbindliche Löschfristen festgeschrieben werden.

Den Grundrechten der Behördenmitarbeiter ist meiner Auffassung nach wegen des umfassenden Datenbestands der Verbunddatei und den weit verbreiteten Zugriffsrechten nur dann ausreichend Rechnung getragen, wenn diese Festlegungen in normenklarer und normenbestimmter Weise gesetzlich geregelt werden. Dies erfordert insbesondere folgende Regelungen:

- ausdrückliches Verbot der Verwendung der in der Verbunddatei gespeicherten Daten für eine Verhaltens- und Leistungskontrolle der Mitarbeiter

- Verpflichtung, dass das Datenverarbeitungsprogramm technisch so ausgestaltet wird, dass soweit möglich die Herstellung eines Personenbezugs zu bestimmten oder bestimmbaren Behördenmitarbeitern verhindert wird, insbesondere bei der Erstellung von Auswertungen, Übersichten, Tabellen oder Listen.

Darüber hinaus ist auch aus personaldatenschutzrechtlichen Gründen eine vollständige Protokollierung der Lese- und Schreibzugriffe zum Zweck der Datenschutzkontrolle erforderlich.

Klargestellt werden sollte das Verhältnis der Rechtsgrundlage für die Verbunddatei des Projekts TIZIAN zu den in Art. 30 GDVG bereits bestehenden datenschutzrechtlichen Vorschriften. Es sollte deshalb bei der Regelung der Schreib- und Lesezugriffe für das Projekt TIZIAN (siehe oben zu 1.2) berücksichtigt werden, dass die von Art. 30 Abs. 1 GDVG umfassten Daten nicht zur Datenübermittlung und -nutzung vorgesehen werden. Ich habe deshalb vorgeschlagen, in die Rechtsgrundlage zur Klarstellung eine

- Bestimmung, dass Art. 30 GDVG unberührt bleibt

aufzunehmen und in der Gesetzesbegründung darauf hinzuweisen, dass die Rechtsgrundlagen für die Verbunddatei des Projektes TIZIAN keine über Art. 30 GDVG hinausgehende Befugnis zur Verarbeitung und -nutzung der in dieser Vorschrift genannten Daten enthalten.

Ich habe dem StMUG mitgeteilt, dass über die Schaffung einer verfassungskonformen Rechtsgrundlage hinaus nach meiner Auffassung beim Projekt TIZIAN folgende weitere datenschutzrechtliche Anforderungen bestehen:

- Die in Art. 75 a Abs. 1 Nr. 1 BayPVG statuierten Mitbestimmungsrechte der Personalvertretungen (siehe Art. 80 BayPVG) sind zu beachten.

- Bei automatisierten (Groß-)Vorhaben entspricht es allgemeiner Praxis, ein umfassendes Datenschutz- und Sicherheitskonzept zu erstellen.

- Die gesetzlichen Vorgaben zur Freigabe, zur Verfahrensbeschreibung, zur allgemeinen Beschreibung der Art der eingesetzten Datenverarbeitungsanlagen und der technischen und organisatorischen Maßnahmen nach Art. 7 und 8 BayDSG sowie zur Verpflichtung der an einem automatisierten Abrufverfahren beteiligten Stellen zu einer Dokumentation des Abrufverfahrens sind zu berücksichtigen.

Ich habe das StMUG insbesondere im Hinblick auf eine verfassungskonforme Rechtsgrundlage um Stellungnahme gebeten und meine weitere Unterstützung angeboten.

### 14.2 Übermittlung einer amtsärztlichen Bescheinigung zur Prüfungsunfähigkeit an eine Hochschule nach freiwilliger Untersuchung

Ein Student wandte sich an das für ihn örtlich zuständige Gesundheitsamt mit der Bitte, ihm eine amtsärztliche Bescheinigung über eine vorübergehende Prüfungsunfähigkeit für bestimmte Semester zu erteilen. Ein Untersuchungsauftrag der Hochschule lag nicht vor. Der Student bat das Gesundheitsamt darum, die amtsärztliche Bescheinigung nur ihm auszuhändigen und nicht unmittelbar an das Prüfungsamt der Hochschule zu senden. Denn er beabsichtigte, der Hochschule das Attest nur dann vorzulegen, wenn ihm das Gesundheitsamt eine vorübergehende Prüfungsunfähigkeit bescheinigt, nicht hingegen, wenn das Gesundheitsamt von einer dauerhaften Prüfungsunfähigkeit ausgeht. Das Gesundheitsamt führte die Begutachtung durch und kam dabei zu dem Ergebnis, dass bei dem Studenten eine dauerhafte Prüfungsunfähigkeit vorliegt. Eine amtsärztliche Bescheinigung dieses Inhalts übermittelte das Gesundheitsamt unmittelbar an die Hochschule.

Diesen Sachverhalt habe ich aus datenschutzrechtlicher Sicht wie folgt bewertet:

Die Weitergabe der in der amtsärztlichen Bescheinigung enthaltenen personenbezogenen Daten durch das Gesundheitsamt an die Hochschule stellt eine Verarbeitung personenbezogener Daten in Form einer Datenübermittlung dar. Nach Art. 30 Abs. 1 Satz 3 i.V.m. Satz 1 Gesundheitsdienst- und Verbraucherschutzgesetz (GDVG) dürfen u.a. die Gesundheitsämter Geheimnisse, die Amtsangehörigen in der Eigenschaft als Arzt im Zusammenhang mit einer Untersuchung oder Begutachtung, der sich der Betroffene freiwillig unterzogen hat, anvertraut oder sonst bekannt geworden sind, grundsätzlich nicht an Dritte übermitteln. Vorliegend handelte es sich bei den in der amtsärztlichen Bescheinigung enthaltenen Feststellungen zur Prüfungsunfähigkeit um derartige Geheimnisse, von welchen die Ärzte des Gesundheitsamtes bei einer Begutachtung erfahren hatten, der sich der Student freiwillig unterzogen hatte. Auf eine der in Art. 30 Abs. 2 GDVG geregelten Ausnahmen vom Übermittlungsverbot des Art. 30 Abs. 1 GDVG konnte sich das Gesundheitsamt nicht berufen, da weder eine die Datenübermittlung ausdrücklich zulassende Rechtsvorschrift vorlag (Art. 30 Abs. 2 Satz 1 Nr. 1 GDVG), noch der Student in die Datenübermittlung ausdrücklich oder den Umständen nach eingewilligt hatte (Art. 30 Abs. 2 Satz 1 Nr. 2 GDVG), noch die Datenübermittlung dem mutmaßlichen Willen des Studenten entsprach (Art. 30 Abs. 2 Satz 1 Nr. 3 GDVG), noch dies zur Abwehr von Gefahren für Freiheit, Leben oder Gesundheit Dritter erforderlich gewesen wäre (Art. 30 Abs. 2 Satz 2 Halbsatz 1 GDVG).

Im Ergebnis habe ich deshalb festgestellt, dass das Gesundheitsamt durch die Übermittlung der amtsärztlichen Bescheinigung an die Hochschule gegen datenschutzrechtliche Vorschriften verstoßen hat.

Dennoch habe ich nach Art. 31 Abs. 3 BayDSG von einer förmlichen Beanstandung des Gesundheitsamtes abgesehen, weil es sich - wie das Gesundheitsamt glaubwürdig dargestellt hatte - bei der Datenübermittlung um ein Versehen gehandelt hatte, das Gesundheitsamt das Vorliegen einer datenschutzrechtlichen Verfehlung eingeräumt und sich bei dem Studenten frühzeitig entschuldigt hatte und die amtsärztliche Bescheinigung „nur“ eine Feststellung zur Prüfungsunfähigkeit und nicht etwa medizinische Diagnosen enthielt.

### 14.3 Forschung mit Daten des Veterinäramts

Eine Studentin bat das Veterinäramt eines Landratsamtes, ihr Namen und Anschriften sämtlicher dort registrierter Schafhalter zur Verfügung zu stellen. Diese Daten wollte sie im Rahmen ihrer Diplomarbeit für eine repräsentative Befragung der Schafhalter nutzen.

Der behördliche Datenschutzbeauftragte des Landratsamtes hatte Bedenken, der Studentin die angeforderten Daten ohne Einwilligung der Schafhalter zu überlassen und bat mich deshalb um meine datenschutzrechtliche Bewertung. Dabei bin ich zu dem Ergebnis gelangt, dass eine Übermittlung der Daten der Schafhalter vom Veterinäramt an die Studentin unzulässig ist, weil ein Adressmittlungsverfahren möglich ist:

Da die Studentin ihre Diplomarbeit nicht im Rahmen eines Forschungsvorhabens der Hochschule fertigte, war die Rechtmäßigkeit einer Datenübermittlung an eine nicht-öffentliche Stelle zu prüfen. Nach Art. 19 Abs. 1 Nr. 2 BayDSG ist die Übermittlung personenbezogener Daten an nicht-öffentliche Stellen u.a. zulässig, wenn die nicht-öffentliche Stelle ein berechtigtes Interesse an der Kenntnis der zu übermittelnden Daten glaubhaft darlegt und der Betroffene kein schutzwürdiges Interesse an dem Ausschluss der Übermittlung hat. Bei der Prüfung dieser Vorschrift ist eine umfassende Abwägung der berechtigten Interessen des Empfängers mit den schutzwürdigen Interessen der Betroffenen vorzunehmen. Vorliegend überwog das Interesse der Schafhalter an der Geheimhaltung ihrer beim Veterinäramt gespeicherten Daten, da die Studentin zur Wahrung ihres zweifelsohne berechtigten Forschungsinteresses nicht auf die Übermittlung von Namen und Anschriften der Schafhalter angewiesen war, sondern auf ein Adressmittlungsverfahren zurückgreifen konnte.

Das Adressmittlungsverfahren ist insbesondere bei Forschungsvorhaben eine bekannte und bewährte

Vorgehensweise. Zu dessen Durchführung in vorliegendem Fall war es erforderlich, dass die Studentin dem Veterinäramt die an die Schafhalter zu versendenden Unterlagen (z.B. Fragebogen mit Begleitbrief) zur Verfügung stellt. Das Veterinäramt konnte dann diese Unterlagen an sämtliche Schafhalter oder an eine nach Kriterien der Studentin ausgewählte repräsentative Stichprobe der Schafhalter versenden. Bei dieser Vorgehensweise erübrigt sich die Übermittlung der personenbezogenen Daten aller Schafhalter an die Studentin.

### 14.4 Änderungen des Gesundheitsdienst- und Verbraucherschutzgesetzes

Mehrfach habe ich zu verschiedenen datenschutzrelevanten Gesetzentwürfen zur Änderung des Gesundheitsdienst- und Verbraucherschutzgesetzes (GDVG) Stellung genommen, über die mich das Staatsministerium für Umwelt und Gesundheit jeweils unterrichtet hatte. Dies betraf insbesondere folgende Punkte:

#### 14.4.1 BayDSG als Rechtsgrundlage für die Übermittlung und Weitergabe sensibler Daten

Ein Gesetzentwurf sah vor, dass für die Behörden für Gesundheit, Veterinärwesen, Ernährung und Verbraucherschutz und weitere Stellen bei der Verarbeitung und Nutzung sonstiger personenbezogener Daten - gemeint waren insbesondere Daten, die keine Geheimnisse im Sinne des Art. 30 GDVG sind - die Vorschriften des Bayerischen Datenschutzgesetzes (BayDSG) gelten sollten. Hiergegen habe ich erhebliche Bedenken insbesondere verfassungsrechtlicher Art geltend gemacht:

Durch eine solche Bestimmung wäre nämlich die bereichsspezifische Regelung in Art. 31 Abs. 5 GDVG a.F. (jetzt: Art. 31 Abs. 8 GDVG n.F.) ersetzt worden, welche die Übermittlung und Weitergabe personenbezogener Daten nur in den Fällen des Art. 30 Abs. 2 GDVG oder bei Zweckidentität vorsah. Die Festlegung der zulässigen Verwendungszwecke in dieser bereichsspezifischen Vorschrift trägt insbesondere den Feststellungen des Bundesverfassungsgerichts in seinem Urteil zum Volkszählungsgesetz 1983 (Urteil vom 15.12.1983, Az. 1 BvR 209/83) Rechnung. Das Bundesverfassungsgericht hatte in diesem Urteil zur Zweckbindung bei zwangsweise erhobenen Daten ausgeführt: „Ein Zwang zur Abgabe personenbezogener Daten setzt voraus, dass der Gesetzgeber den Verwendungszweck bereichsspezifisch und präzise bestimmt und dass die Angaben für diesen Zweck geeignet und erforderlich sind.“ Mit der im Gesetzentwurf vorgesehenen Neuregelung sollte für alle sonstigen personenbezogenen Daten, egal ob zwangsweise erhoben oder freiwillig zur Verfügung gestellt, das BayDSG gelten. Im Hinblick darauf, dass es sich auch bei „sonstigen personenbezogenen Daten“ um äußerst sensible Daten z.B. über die Gesundheit handeln kann, bestimmt das BayDSG den Verwendungszweck jedoch nicht hinreichend bereichsspezifisch und präzise.

Das Bundesverfassungsgericht hatte zudem erst jüngst zur Videoüberwachung in Bayern entschieden (Beschluss vom 23.02.2007, Az. 1 BvR 2368/06, vgl. hierzu Nr. 9.1 dieses Tätigkeitsberichts), dass die allgemeinen Vorschriften des Bayerischen Datenschutzgesetzes keine Rechtsgrundlage für schwere Eingriffe in das Grundrecht auf informationelle Selbstbestimmung sein können. Einen vergleichbar schweren Grundrechtseingriff habe ich auch bei den Datenübermittlungen gesehen, die durch die Neuregelung gerechtfertigt werden sollten.

Demnach kam meiner Auffassung nach schon aus verfassungsrechtlichen Gründen eine allgemeine Verweisung auf das BayDSG nicht in Betracht.

Im Übrigen ging aus der Gesetzesbegründung nicht hervor, wieso das Schutzniveau für Daten bei den Behörden für Gesundheit, Veterinärwesen, Ernährung und Verbraucherschutz gegenüber der bislang geltenden Vorschrift des Art. 31 Abs. 5 GDVG a.F deutlich abgesenkt werden sollte. Es war nicht erkennbar, in welchen Fallkonstellationen die Beibehaltung der Bestimmungen im GDVG zu nicht sachgerechten Lösungen geführt hätte.

Ich habe mich deshalb dafür ausgesprochen, es wie bisher bei einer bereichsspezifischen Regelung zur Datenübermittlung und -weitergabe im GDVG zu belassen. Erfreulicherweise war das Staatsministerium für Umwelt und Gesundheit meiner Anregung gefolgt: spätere Gesetzentwürfe und auch die in Kraft getretenen Änderungsgesetze enthielten den pauschalen Verweis auf das BayDSG nicht mehr.

#### 14.4.2 Weitergabe von Daten zur Verfolgung von Straftaten und Ordnungswidrigkeiten

Ein weiterer Gesetzentwurf sah vor, dass die Behörden für Gesundheit, Veterinärwesen, Ernährung und Verbraucherschutz Geheimnisse im Sinne des Art. 30 GDVG zur Verfolgung von Straftaten oder Ordnungswidrigkeiten, zur Vollstreckung oder zum Vollzug von Strafen oder Maßnahmen im Sinne des Strafgesetzbuchs (StGB) oder von Erziehungsmaßregeln oder Zuchtmitteln im Sinne des Jugendgerichtsgesetzes sowie zur Vollstreckung von Bußgeldentscheidungen übermitteln und weitergeben können. Hiergegen habe ich erhebliche datenschutzrechtliche Bedenken erhoben. Denn durch diese Regelung wäre dem Strafverfolgungsinteresse generell ein höherer

Stellenwert als dem Geheimnisschutz im Sinne des § 203 StGB eingeräumt worden.

Im Rahmen des § 203 StGB rechtfertigt das Strafverfolgungsinteresse bezüglich bereits begangener Delikte die Verletzung der Schweigepflicht grundsätzlich nicht. Etwas anderes gilt nur bei besonders schweren, mit einer nachhaltigen Störung des Rechtsfriedens verbundenen Verbrechen (z.B. terroristische Gewaltakte), ferner wenn die Gefahr besteht, dass der Täter weiterhin erhebliche Straftaten begehen wird. Von dieser rechtsstaatlichen Grundentscheidung wich der Gesetzentwurf in erheblichem Maße ab, da er einen Geheimnisbruch generell zu Zwecken der Verfolgung von Straftaten oder Ordnungswidrigkeiten und sogar zur Vollstreckung von Bußgeldentscheidungen für zulässig erklärte.

In anderen bereichsspezifischen Regelungskomplexen, wie etwa dem Sozialrecht, wird der Konflikt zwischen Strafverfolgungsinteresse und Geheimnisschutz sehr differenziert geregelt. Nach § 73 SGB X ist eine Übermittlung von Sozialdaten etwa nur zulässig, soweit sie zur Durchführung eines Strafverfahrens wegen eines Verbrechens oder wegen einer sonstigen Straftat von erheblicher Bedeutung erforderlich ist. Die Übermittlung nach § 73 Abs. 1 SGB X muss vom Richter angeordnet werden. Bei besonders schutzwürdigen Sozialdaten, die der Sozialbehörde von einem Arzt oder einer anderen in § 203 Abs. 1 und 3 StGB genannten Person zugänglich gemacht worden sind, ist eine Übermittlung gar nur unter den Voraussetzungen zulässig, unter denen diese Person selbst übermittlungsbefugt wäre (§ 76 Abs. 1 SGB X). In bestimmten Fällen des besonderen Vertrauensschutzes ist eine Datenübermittlung nur dann zulässig, wenn auch aus strafrechtlicher Sicht eine Befugnisnorm bzw. ein Rechtfertigungsgrund bestünde (vgl. dazu z.B. § 65 Abs. 1 Satz 1 Nr. 5 SGB VIII). Eine vergleichbar differenzierte Abwägung zwischen dem Strafverfolgungsinteresse des Staates und dem Geheimnisschutz im Sinne des § 203 StGB fehlte bei dem ursprünglichen Gesetzentwurf.

Darüber hinaus habe ich darauf aufmerksam gemacht, dass es nach Art. 13 Abs. 1 Satz 2 Nr. 2 GDVG auch zu den Aufgaben der Gesundheitsämter gehört, gesundheitliche Beratung für Menschen, die an einer Sucht leiden, durchzuführen. In diesem Zusammenhang stehen in der Praxis vielfach Straftaten gegen das Betäubungsmittelgesetz im Raum. Wollte man hier die Übermittlung von Daten an Strafverfolgungsbehörden grundsätzlich zulassen, so werden weniger Personen das staatliche Angebot der Drogenberatung wahrnehmen. Denn sie müssen befürchten, dass sie vom Gesundheitsamt an die Polizei oder die Staatsanwaltschaft weiter gemeldet werden. Eine verminderte Inanspruchnahme öffentlicher Beratungsleistungen kann nicht im öffentlichen Interesse liegen.

In einem nachfolgenden Gesetzentwurf des Staatsministeriums für Umwelt und Gesundheit war dann nur noch vorgesehen, dass in die Vorschrift des Art. 31 Abs. 8 GDVG n.F. - die im übrigen Art. 31 Abs. 5 GDVG a.F. weitgehend inhaltsgleich ersetzt - eine neue Nr. 2 eingefügt wird, dessen Regelungen nur noch die Datenübermittlung und -weitergabe zur Verfolgung von Straftaten oder von Ordnungswidrigkeiten ermöglicht, wenn die Daten der Behörde bei Erfüllung der Aufgaben gemäß Art. 1 Abs. 3 Nrn. 2, 3 oder Nr. 4 GDVG bekannt geworden sind. Laut Gesetzesbegründung sollte dies zudem nur für personenbezogene Daten gelten, die keine Geheimnisse im Sinne des Art. 30 GDVG sind.

Dieser geplanten Gesetzesänderung bin ich nicht mehr grundsätzlich entgegengetreten, war doch meinen Anregungen zum vorhergehenden Gesetzentwurf überwiegend Rechnung getragen worden. Insbesondere sollte laut der Gesetzesbegründung keine Befugnis zur Übermittlung und Weitergabe von Geheimnissen im Sinne des Art. 30 GDVG mehr geschaffen werden. Ferner war eine Übermittlung z.B. zur Vollstreckung von Bußgeldentscheidungen oder von den Behörden bei der Erfüllung der Gesundheitsaufgaben nach Art. 1 Abs. 3 Nr. 1 GDVG - darunter auch die gesundheitliche Aufklärung und Beratung nach Art. 13 Abs. 1 GDVG - bekannt gewordenen Daten wenigstens hinsichtlich der Verfolgung von Ordnungswidrigkeiten nicht mehr vorgesehen. Allerdings wurde die laut Gesetzesbegründung bestehende Absicht, mit Art. 31 Abs. 8 Nr. 2 GDVG nur die Übermittlung solcher personenbezogener Daten zuzulassen, die keine Geheimnisse im Sinne des Art. 30 GDVG sind, im Gesetzestext nicht ausreichend deutlich. Ich habe es deshalb für erforderlich gehalten, diese Einschränkung konstitutiv oder doch zumindest für die Vollzugspraxis klarstellend im Wortlaut der Neuregelung zu verankern und hierzu die Worte „und wenn die Daten keine Geheimnisse im Sinne des Art. 30 sind.“ einzufügen. Erfreulicherweise wurde auch dieser Anregung in der schließlich in Kraft getretenen Neureglung des Art. 31 Abs. 8 GDVG entsprochen.

### 14.4.3 Schutz der Gesundheit von Kindern und Jugendlichen

Auf Grundlage eines weiteren Gesetzentwurfs wurde ein neuer Art. 14 in das GDVG eingefügt, der sich mit dem Schutz der Gesundheit von Kindern und Jugendlichen befasst. In meiner Stellungnahme zum Gesetzentwurf habe ich u.a. auf Folgendes hingewiesen:

Die Bestimmung in Art. 14 Abs. 3 Satz 1 GDVG, wonach die unteren Behörden für Gesundheit, Veterinärwesen, Ernährung und Verbraucherschutz im Rahmen ihrer Aufgaben nach Art. 14 GDVG mit anderen Stellen und öffentlichen Einrichtungen zu-

sammenzuarbeiten haben, enthält selbst keine Befugnisse zu Eingriffen in das Grundrecht auf informationelle Selbstbestimmung. Sollten für die Zusammenarbeit Datenübermittlungen erforderlich sein, müssten sich diese an den einschlägigen Befugnisnormen, also insbesondere an Art. 30 und 31 GDVG messen lassen.

Art. 14 Abs. 3 Satz 2 GDVG verpflichtet die unteren Behörden für Gesundheit, Veterinärwesen, Ernährung und Verbraucherschutz, bei gewichtigen Anhaltspunkten für eine erhebliche Gefährdung des Wohls eines Kindes oder Jugendlichen das Jugendamt einzuschalten. Zu dieser Regelung habe ich angemerkt, dass Ärzte des Gesundheitsamts z.B. im Rahmen der Mütterberatung ein besonderes Vertrauensverhältnis zu den Beratenen aufbauen. Gerade im Fall der Mütterberatung könnte es deshalb kontraproduktiv sein, wenn ein Amtsarzt dazu verpflichtet wird, dem Jugendamt Meldungen zu machen. Denn es ist zu befürchten, dass gerade in problematischen Fällen die Mütterberatung nicht mehr aufgesucht wird. Darüber hinaus habe ich darauf hingewiesen, dass bei gewichtigen Anhaltspunkten für eine erhebliche Gefährdung des Wohls eines Kindes oder Jugendlichen bereits bisher Art. 31 Abs. 5 GDVG a.F. (jetzt: Art. 31 Abs. 8 GDVG n.F.) i.V.m. Art. 30 Abs. 2 GDVG als Befugnisnorm für eine Datenübermittlung im Raum steht. Mir ist keine Fallgestaltung bekannt, in der diese Möglichkeiten zur Datenübermittlung und -weitergabe in Fällen von Kindeswohlgefährdung nicht ausgereicht hätten.

Zum neuen Art. 14 Abs. 6 GDVG, der Ärztinnen und Ärzte, Hebammen und Entbindungspfleger verpflichtet, gewichtige Anhaltspunkte für eine Misshandlung, Vernachlässigung oder einen sexuellen Missbrauch eines Kindes oder Jugendlichen, die ihnen im Rahmen ihrer Berufsausübung bekannt werden, unter Übermittlung der erforderlichen personenbezogenen Daten unverzüglich dem Jugendamt mitzuteilen, äußere ich mich aus Gründen des Sachzusammenhangs in Nr. 17.3 dieses Tätigkeitsberichts. Diese Bestimmung stellt im GDVG einen Fremdkörper dar, da dieses Gesetz die Aufgaben und Befugnisse der Behörden für Gesundheit, Veterinärwesen, Ernährung und Verbraucherschutz regelt (vgl. Art. 1 Abs. 2 GDVG). Damit hat die Meldepflicht in Art. 14 Abs. 6 GDVG nichts zu tun.

# 15 Medizinische Forschung und Evaluation

## 15.1 Errichtung einer Forschungsdatenbank für kinder- und jugendpsychiatrische Studien

Im Berichtszeitraum plante ein zu diesem Zweck gegründeter eingetragener Verein, dessen Mitglieder, kinder- und jugendpsychiatrische Kliniken, aus verschiedenen Bundesländern stammen, die Errichtung einer Datenbank zu Forschungszwecken im Bereich Kinder- und Jugendpsychiatrie. In der Datenbank sollten Daten zur Psychopharmakotherapie im Kindes- und Jugendalter gesammelt werden, die in der klinischen Routine von den jungen Patienten der an dem Kompetenznetz teilnehmenden kinder- und jugendpsychiatrischen, zumeist universitären Kliniken (Zentren) erhoben werden, um insbesondere Korrelationen zwischen Altersstufen, Dosierungen, Arzneimittel-Plasmaspiegeln im Blut, Wirkungen und Nebenwirkungen und anderen Einflussfaktoren der Wirksamkeit herstellen zu können. Auf die pseudonymisiert bzw. anonymisiert gespeicherten Daten sollten Berechtigte der Zentren (zentrumsintern, zentrumsübergreifend) und externe Forscher zugreifen können.

Ausschlaggebend für das Projekt sei gewesen, dass die Studienlage zu Wirkungen und Nebenwirkungen von Psychopharmaka im Kindes- und Jugendalter sehr gering sei, die meisten modernen Psychopharmaka demnach für Kinder und Jugendliche nicht zugelassen seien und die aus Zulassungsstudien optimierte Arzneimittelsicherheit für Kinder und Jugendliche somit nicht vorausgesetzt werden könne, sowie der Umstand, dass die Verstoffwechselung von Psychopharmaka bei Kindern und Jugendlichen altersabhängig sehr von derjenigen im Erwachsenenalter abweiche, so dass das Risiko ineffizienter oder aber überhöhter Dosierungen mit Nebenwirkungsgefahr schwieriger abschätzbar sei.

In einem genetischen Teilprojekt sollte darüber hinaus Patienten mit auffälligem Stoffwechsel angeboten werden, zur weiteren Abklärung genetische Besonderheiten der am Stoffwechsel beteiligten Enzyme zu analysieren und die gewonnenen Blutproben in einer Biomaterialbank im Genetik-Labor für Forschungszwecke aufzubewahren.

Ich habe im Rahmen meiner Beratungstätigkeit und Zuständigkeit den Aufbau des Projektes begleitet. Dabei habe ich eine Vielzahl von Änderungen und Ergänzungen zum Datenschutzkonzept und zum Verfahrensablauf vorgeschlagen. Insbesondere habe ich folgende Verbesserungen in allgemeiner datenschutzrechtlicher Hinsicht angeregt bzw. gefordert:

- Nach Art. 25 Abs. 2 Satz 1 Bayerisches Datenschutzgesetz (BayDSG) ist für bayerische öffentliche Stellen ein behördlicher Datenschutzbeauftragter zu bestellen.

- Den Bestimmungen des Art. 26 BayDSG zufolge ist insbesondere eine Verfahrensbeschreibung zu erstellen und hat eine datenschutzrechtliche Freigabe zu erfolgen.

- Dem Datenschutzkonzept muss zweifelsfrei zu entnehmen sein, welchen der beteiligten Stellen (Prüfarzt, Zentren, e.V.) jeweils die datenschutzrechtliche Verantwortung zustehen soll.

- Dem Datenschutzkonzept muss zweifelsfrei zu entnehmen sein, ob die Studien mit pseudonymisierten oder anonymisierten Daten durchgeführt werden sollen. Vorrang hat die Verwendung anonymisierter Daten, das bedeutet, dass die in der Datenbank gespeicherten Daten ohne PID oder eine sonstige rückführbare Nummer an die Forscher herausgegeben werden. Vorsorglich habe ich darauf hingewiesen, dass auch bei der Verwendung nur pseudonymisierter Daten die Forscher keinesfalls Zugriff auf die PID des Probanden erhalten dürfen. Vielmehr müsste für diesen Fall eine zweistufige Pseudonymisierung, d.h. eine weitere kryptografische Transformation der PID vorgesehen werden. Hierzu müsste die PID von einem Treuhänder in ein sog. PSN umgewandelt werden.

- Für Biomaterialbanken bestehen besondere datenschutzrechtliche Anforderungen hinsichtlich der Pseudonymisierung der Proben. Grund hierfür ist, dass diese in der Regel genetisches Material enthalten, das für jeden Menschen einmalig ist. Dieser Umstand kann die Reidentifizierung deutlich erleichtern, z.B. wenn eine Referenzprobe mit den gleichen genetischen Eigenschaften zugänglich ist. Deshalb sind besondere Schutzmaßnahmen beim Umgang mit Proben erforderlich.

  So ist z.B. in den Konzepten des TMF e.V. entsprechend dem allgemein anerkannten datenschutzrechtlichen Standard vorgesehen, dass die Biomaterialbank - vorliegend also das Genetik-Labor - keine Kenntnis von der PID des Patienten erlangen darf, um ein Zusammenführen der Probe mit den identifizierenden Daten zu vermeiden. Für die Proben müsste deshalb im Zentrum eine sog. LabID generiert werden, mit der die Probe vor dem Versand beschriftet wird. Damit die in der Datenbank gespeicherten Daten nicht mit der Probe verknüpft werden können, darf die Datenbank (die die PID speichert) die LabID nicht kennen. Es ist daher sicherzustellen, dass das Gentik-Labor die LabID vor der Weitergabe der ProbDAT an die Datenbank kryptografisch in eine sog. LabID_trans transformiert, unter der dann die ProbDAT an die Datenbank weitergeleitet und dort gespeichert werden.

  Die Einzelheiten eines derartigen Pseudonymisierungskonzepts sind im Datenschutzkonzept festzulegen. Hierzu gehört insbesondere auch eine Risikobewertung aus dem Blickwinkel unbefugter Depseudonymisierungsversuche und der Kompromittierung einzelner Stellen. Grundsätzlich muss dabei gewährleistet werden, dass weder durch eine alleinige Kompromittierung der Datenbank noch des Genetik-Labors eine Depseudonymisierung möglich ist.

- Im Datenschutzkonzept sollen die Fallgruppen der Reidentifizierung genau und abschließend benannt werden. Darüber hinaus ist für jeden Fall der Ablauf der Reidentifizierung festzulegen, insbesondere, wer im Einzelfall über die Berechtigung zur Reidentifizierung entscheidet und wie die Reidentifizierung konkret abgewickelt wird.

- Für sehr bedenklich habe ich gehalten, dass der Prüfarzt einer am Projekt teilnehmenden Klinik (Zentrum) ein Formular mit Name, Adresse, Geburtsdatum und Geschlecht des Probanden und dem Pseudonym in seiner Patientenakte aufbewahren soll. Da die Patientenakte für eine Vielzahl von Mitarbeitern des Krankenhauses zumindest faktisch zugänglich ist, wäre durch eine solche Vorgehensweise die Pseudonymisierung nachhaltig geschwächt.

- Darüber hinaus habe ich es für geboten gehalten, einen Zeitpunkt festzulegen, zu dem die Daten spätestens anonymisiert werden sollen.

- Nicht nur beim genetischen Teilprojekt, sondern für das gesamte Projekt ist eine informierte - also auf einer ausreichenden Patienteninformation beruhende - datenschutzrechtliche Einwilligung erforderlich. Denn soweit Daten verwendet werden, die im Behandlungszusammenhang erhoben wurden, stellt die Speicherung in einer zentralen Datenbank und die Auswertung zu Forschungszwecken eine Zweckänderung dar, die einer gesonderten Einwilligung bedarf. Die Einwilligung in die Datenerhebung zum Zwecke der Behandlung umfasst nämlich nicht die Verarbeitung und Nutzung der Daten zu Forschungszwecken (siehe hierzu auch meine Ausführungen im 22. Tätigkeitsbericht Nr. 13.3.1 zum Aufbau einer Biomaterialbank).

- Für dringend notwendig habe ich verbindliche Regelungen bezüglich des gesamten Projekts einschließlich des genetischen Teilprojekts gehalten, ob und ggf. unter welchen Voraussetzungen die datenschutzrechtlichen Einwilligungen nur von den Sorgeberechtigten, nur von den Kindern und Jugendlichen bzw. von beiden einzuholen sind. In diesem Zusammenhang bin ich der Auffassung, dass bei Kindern und Jugendlichen, sobald diese die natürliche Einsichtsfähigkeit (ca. 14 Jahre) er-

langt haben, zumindest auch deren Einwilligung erforderlich ist. Die Patienteninformation und die Einwilligungserklärungen für Kinder und Jugendliche müssen dann altersgerecht abgefasst werden.

Zum Zeitpunkt des Redaktionsschlusses für diesen Tätigkeitsbericht waren noch nicht alle datenschutzrechtlichen Anforderungen erfüllt worden. Der eingetragene Verein hatte jedoch das Datenschutzkonzept sowie die Einwilligungserklärungen überarbeitet, so dass ich gegen den Beginn einer Pilotphase des Projektes keine Einwendungen erhoben habe, sofern insbesondere folgende datenschutzrechtlichen Mindestanforderungen sichergestellt sein würden:

- In der Pilotphase wird ausschließlich das Basisprojekt, nicht hingegen das pharmakogenetische Teilprojekt durchgeführt.

- Die Datenbank des e.V. wird ausschließlich für wissenschaftliche Studien/Auswertungen genutzt, zur konkreten Behandlung der Patienten wird hingegen nicht auf die Datenbank mit den pseudonymisierten Daten zugegriffen. Für den Zugriff auf die Datenbank im Behandlungszusammenhang müsste eine zusätzliche Pseudonymisierung mit einer eigenen PID durchgeführt werden. Darüber hinaus wäre zu prüfen, ob und ggf. inwieweit es den beteiligten Kliniken gestattet ist, Daten für den Behandlungszusammenhang außerhalb des Krankenhauses zu speichern (hier bestehen in Bayern Einschränkungen durch Art. 27 Abs. 4 Satz 6 Bayerisches Krankenhausgesetz).

- Das Formular mit den IDAT des Probanden und dessen PID wird zu keinem Zeitpunkt in der Patientenakte des Probanden aufbewahrt.

- Für sämtliche Auswertungen/Studien werden vorerst ausschließlich anonymisierte Daten zur Verfügung gestellt.

Ich habe mir ausdrücklich vorbehalten, auf Grund der weiteren datenschutzrechtlichen Prüfung unter Einbeziehung der sonstigen betroffenen Landesbeauftragten für den Datenschutz weitergehende Änderungen des Datenschutzkonzeptes, der Einwilligungserklärung und der Verfahrensbeschreibung zu verlangen.

## 15.2 Mammographie-Screening

Wie schon in früheren Jahren (vgl. hierzu Nr. 13.1.3, 22. Tätigkeitsbericht) war ich auch im aktuellen Berichtszeitraum intensiv mit verschiedenen datenschutzrelevanten Aspekten des Mammographie-Screening-Programms gemäß den Krebsfrüherkennungs-Richtlinien (KFÜ-RL) des Gemeinsamen Bundesausschusses befasst:

### 15.2.1 Einladungswesen

Zahlreiche Petitionen erreichten mich zum sog. Einladungswesen des Mammographie-Screening-Programms.

Die Krebsfrüherkennungs-Richtlinien sehen vor, dass die anspruchsberechtigten Frauen von einer sog. Zentralen Stelle eingeladen werden, diese ist in Bayern bei der Kassenärztlichen Vereinigung Bayerns (KVB) angesiedelt. Für die Einladung erhält die Zentrale Stelle von den Melderegistern die Daten aller in Frage kommenden Frauen. Die Zentrale Stelle weist jeder anspruchsberechtigten Frau eine eindeutige, lebenslang geltende Screening-Identifikationsnummer zu und legt Ort und Termin der Untersuchung auf Grundlage der Angaben der Screening-Einheit zu ihren Kapazitäten fest. Die Ärzte in den Screening-Einheiten erhalten von der Zentralen Stelle Name und Screening-Identifikationsnummer der Frau sowie Ort und Termin, zu dem sie eingeladen wurde (Einladungslisten). In die Liste trägt der Arzt ein, ob die eingeladene Frau teilgenommen hat. Die Einladungslisten sind spätestens nach vier Wochen von der Screening-Einheit an die Zentrale Stelle zu übermitteln, damit diese eine Erinnerung der Frauen veranlasst, die sich nicht auf die Einladung gemeldet haben. Bei der Screening-Einheit sind die von der Zentralen Stelle zur Verfügung gestellten personenbezogenen Daten nach Rückgabe der Einladungslisten an die Zentrale Stelle zu löschen. Auch die Zentrale Stelle löscht die personenbezogenen Daten der Einladungsliste einschließlich die der Nichtteilnehmerinnen und leitet die Angaben zur Teilnahme nur in anonymisierter Form zur Evaluation des Einladungswesens weiter.

Um das in den Krebsfrüherkennungs-Richtlinien beschriebene Verfahren auf landesrechtlicher Ebene in Bayern umzusetzen, wurde zum einen das Gesundheitsdienst- und Verbraucherschutzgesetz (GDVG) und zum anderen die Verordnung zur Übermittlung von Meldedaten (Meldedatenverordnung - MeldDV) geändert. Art. 31 a Satz 1 GDVG bestimmt, dass Zentrale Stellen, die befugt sind, Maßnahmen zur Früherkennung von Erkrankungen der Bevölkerung zu koordinieren, von den Meldebehörden Daten aus dem Melderegister erheben und verarbeiten können, soweit es zur Erfüllung ihrer Aufgaben erforderlich ist. Gemäß Art. 31 a Satz 2 GDVG erhält eine nach den Krebsfrüherkennungsrichtlinien des Gemeinsamen Bundesausschusses errichtete Zentrale Stelle zur Durchführung von bevölkerungsbezogenen Screening-Maßnahmen auch die Meldedaten der nicht gesetzlich versicherten Frauen. Nach § 15 Abs. 1 Satz 1 MeldDV übermittelt die AKDB (Anstalt für Kommunale Datenverarbei-

tung in Bayern) der Zentralen Stelle bei der Kassenärztlichen Vereinigung in Bayern jeweils zum ersten eines Monats personenbezogene Daten (Familiennamen, Geburtsnamen, Vornamen, Doktorgrad, Tag und Ort der Geburt, gegenwärtige Anschrift) aller Einwohnerinnen, die an diesem Tag das 50. Lebensjahr, aber noch nicht das 70. Lebensjahr vollendet haben und mit alleiniger oder Hauptwohnung in Bayern gemeldet sind. Die Übermittlung ist nur in dem seltenen Fall ausgeschlossen, dass eine Auskunftssperre nach Art. 31 Abs. 7 MeldeG wegen Gefahr für Leben, Gesundheit, persönliche Freiheit oder ähnliche schutzwürdige Interessen vorliegt (§ 15 Abs. 1 Satz 2 MeldDV), nicht hingegen bei den sonstigen Übermittlungs- und Auskunftssperren. Die Zentrale Stelle bei der Kassenärztlichen Vereinigung in Bayern darf die Daten nur verwenden, um die weibliche Bevölkerung über Vorsorgeuntersuchungen gegen Brustkrebs flächendeckend zu informieren und um ein Einladungswesen zur Teilnahme am Mammographie-Screening-Projekt aufzubauen und fortzuführen (§ 15 Abs. 2 Satz 1 MeldDV).

Im Ergebnis ist festzustellen, dass für das derzeitige Einladungswesen des Mammographie-Screening-Programms eine ausreichende Rechtsgrundlage besteht. Eine andere, von den betroffenen Frauen, die sich an mich wenden, nicht zu Unrecht thematisierte Frage ist allerdings, ob das in den Krebsfrüherkennungs-Richtlinien festgelegte Einladungsverfahren mit einer automatisierten Terminvergabe bei einem einzigen bestimmten Arzt fachlich sinnvoll ist oder ob nicht mit einem Alternativverfahren eine höhere Akzeptanz bei den angeschriebenen Frauen erreicht werden könnte.

### 15.2.2 Begriffserläuterungen in der Einladung

Eine Petentin hat mich darauf aufmerksam gemacht, dass in den bei der Einladung zu einem Screening-Termin versandten Schreiben und Unterlagen an keiner Stelle erklärt wird, wer oder was sich hinter den Begriffen „Zentrale Stelle Mammographie-Screening“ und „Mammographie-Screening-Programm“ verbirgt und wie sich die organisatorischen Zusammenhänge darstellen. Mein entsprechender Hinweis an die KVB hat diese zumindest dazu bewogen, in das Einladungsschreiben die Erläuterung „Die Zentrale Stelle Mammographie-Screening Bayern ist eine gemeinsame Einrichtung der bayerischen Krankenkassen und der Kassenärztlichen Vereinigung Bayerns, angesiedelt bei der Kassenärztlichen Vereinigung Bayerns.“ aufzunehmen.

### 15.2.3 Evaluation der Intervallkarzinome und der Mortalität im Mammographie-Screening

Schon bislang ist in den Krebsfrüherkennungs-Richtlinien die Evaluation der sog. Intervallkarzinome geregelt. Als Intervallkarzinome werden alle jene Brustkrebsfälle verstanden, die bei Teilnehmerinnen am Screening zwischen den alle zwei Jahre stattfindenden Screening-Terminen diagnostiziert werden. Bei der Evaluation solcher Intervallkarzinome gilt es insbesondere die sog. falsch-negativen Diagnosen zu identifizieren, also jene Fälle, in denen der Arzt beim Screening einen bereits bestehenden Brustkrebs fehlerhaft übersehen hat.

Bei der Evaluation der Mortalität im Mammographie-Screening geht es darum, aussagefähige Vergleiche zwischen der Sterblichkeit von gescreenten und nicht gescreenten Tumorpatientinnen durchführen zu können. Auf diese Weise soll ermittelt werden, ob das Mammographie-Screening-Programm zu einer Verbesserung des Überlebens beitragen kann.

Die Kooperationsgemeinschaft Mammographie, eine in den Krebsfrüherkennungs-Richtlinien vorgesehene gemeinsame Einrichtung der Kassenärztlichen Bundesvereinigung und der Spitzenverbände der Krankenkassen, hat im Berichtszeitraum veränderte Konzeptionen für die Evaluation der Intervallkarzinome sowie neue Konzeptionen für die Evaluation der Mortalität im Mammographie-Screening mit Hilfe der Krebsregister vorgestellt und die Datenschutzbeauftragten des Bundes und der Länder um eine datenschutzrechtliche Prüfung gebeten. Diese Konzepte und auch deren datenschutzrechtliche Bewertung sind außerordentlich komplex, so dass es nicht möglich ist, diese im Rahmen eines Tätigkeitsberichts erschöpfend zu erläutern.

Ich habe durch meine Stellungnahme darauf hingewirkt, dass die Konzepte möglichst datenschutzfreundlich ausgestaltet werden.

Ferner habe ich darauf aufmerksam gemacht, dass die Konzepte eine Änderung der Krebsfrüherkennungs-Richtlinie voraussetzen. Diese ist mittlerweile erfolgt.

Sollen die Konzepte der Kooperationsgemeinschaft Mammographie tatsächlich umgesetzt werden, sind allerdings zusätzlich diverse Änderungen des Bayerischen Krebsregistergesetzes (BayKRG) notwendig. Dies betrifft insbesondere die Regelung des Datenabgleichs zur Feststellung der Intervallkarzinome in Art. 8 Abs. 1 Nr. 8 BayKRG, aber auch die Einführung der Evaluation der Mortalität im Mammographie-Screening als neue Aufgabe des Krebsregisters

einschließlich der hierfür notwendigen Rechtsgrundlagen für die Meldung, Erhebung und Verarbeitung der erforderlichen Daten.

#### 15.2.4 Datenhaltung in einem externen Rechenzentrum

Im letzten Tätigkeitsbericht (vgl. hierzu Nr. 13.1.3, 22. Tätigkeitsbericht) hatte ich darauf hingewiesen, dass die von der KVB als Zentrale Stelle praktizierte Datenhaltung bei einem externen Provider diverse Sicherheitsmaßnahmen erfordert, insbesondere eine verschlüsselte Datenspeicherung, damit der Provider keine Kenntnis von den bei ihm gespeicherten Daten nehmen kann. Diese Problematik stellt sich derzeit nicht mehr, da die KVB ein Insourcing der ausgelagerten Infrastruktur vorgenommen hat.

#### 15.2.5 Externe Call-Center

Im Berichtszeitraum hat mich die KVB darüber informiert, dass sie eine private Firma mit der Erbringung von Call-Center-Dienstleistungen für die Zentrale Stelle im Mammographie-Screening beauftragten möchte. Hierzu habe ich die KVB auf Folgendes hingewiesen:

Nachdem die Mitarbeiter des Call-Centers auch auf die Datenbank der Zentralen Stelle zugreifen müssen, ist besonders an das Thema Rechtevergabe zu denken. Insbesonders muss sichergestellt sein, dass die Mitarbeiter der Call-Center nur auf die für ihre Aufgaben (z.B. Terminverschiebungen) benötigten Daten zugreifen können und dass die Datenzugriffe revisionsfähig sind.

Ferner hat die KVB darauf zu achten, zu welchen anderen Systemen der KVB die Mitarbeiter des Call-Centers Zugriff für andere Aufgaben erhalten, um die Gefahr einer Wissenshäufung bei diesen Mitarbeitern gering zu halten.

Schließlich sind bei der Beauftragung einer privaten Firma mit einem externen Call-Center auch die Anforderungen des Art. 6 BayDSG an eine Auftragsdatenverarbeitung einzuhalten.

## 16 Änderungen des Heilberufe-Kammergesetzes

Zu berichten ist auch über zwei datenschutzrelevante Änderungen des Heilberufe-Kammergesetzes (HKaG):

Nach Art. 2 Abs. 2 Satz 1 Halbsatz 2 HKaG n.F. ist die Berufsvertretung der Ärzte dazu verpflichtet, den zuständigen Behörden auf deren Verlangen nicht nur - wie bislang schon - Gutachten zu erstatten, sondern nun auch Sachverständige zur Erstattung von Gutachten zu benennen. Zudem ist die Berufsvertretung nun nach Art. 2 Abs. 2 Satz 3 HKaG berechtigt, auch den Gerichten auf Verlangen Gutachten zu erstatten oder Sachverständige zur Erstattung von Gutachten zu benennen. Soweit es zur Erfüllung dieser Aufgaben erforderlich ist, ist die Berufsvertretung nach Art. 2 Abs. 2 Satz 4 HKaG berechtigt, die in den jeweiligen Verfahrensakten enthaltenen personenbezogenen Gesundheitsdaten zu nutzen und zu verarbeiten.

Diese Gesetzesänderung habe ich begrüßt. Denn durch sie wurde die gängige Praxis der Landesärztekammer, den Behörden und Gerichten Gutachten zu erstatten oder Sachverständige zur Erstattung von Gutachten zu benennen und hierbei auch die in den Verfahrensakten enthaltenen Gesundheitsdaten zu nutzen und zu verarbeiten, auf eine gesetzliche Grundlage gestellt. Damit wurde meiner Forderung nach einer klarstellenden Regelung Rechnung getragen.

Darüber hinaus ist in Art. 4 Abs. 8 HKaG n.F. nunmehr geregelt, dass die für die Berufszulassung zuständigen Behörden die Landesärztekammer über Personen unterrichten, denen die Berufszulassung neu erteilt wurde. Diese Datenübermittlung dient dem Zweck, die Landesärztekammer auch von denjenigen Mitgliedern der Ärztlichen Kreisverbände in Kenntnis zu setzen, die ihrer persönlichen Meldepflicht nach Art. 4 Abs. 7 HKaG nicht nachkommen, damit die Berufsvertretung ihre Aufgaben erfüllen und insbesondere die Berufsaufsicht führen kann. Da diese Regelung fachlich notwendig erscheint, bin ich ihr nicht entgegengetreten.

## 17 Soziales

### 17.1 Soziale Forschung

#### 17.1.1 Forschungsvorhaben zur Untersuchung der Situation von Kindern in gleichgeschlechtlichen Lebenspartnerschaften

Ein Institut einer bayerischen Hochschule hatte sich im Berichtszeitraum an mich gewandt und um datenschutzrechtliche Stellungnahme zu einem Forschungsvorhaben gebeten, bei dem die Situation von Kindern in gleichgeschlechtlichen Lebenspartnerschaften untersucht werden sollte. Hierzu wollte das Institut bundesweit eine Melderegisterauskunft über sämtliche Personen bzw. Haushalte mit dem Familienstand „Lebenspartnerschaft“ einholen. Die Meldedaten sowie mit deren Hilfe zusätzlich recherchierte Telefonnummern sollten dann für eine Kontaktaufnahme mit den Betroffenen genutzt werden. Dabei wollte das Institut zunächst herausfinden, in welchen Haushalten mit dem Familienstand „Lebenspartner-

schaft“ überhaupt Kinder leben. Diese Betroffenen sollten dann gebeten werden, auf freiwilliger Basis an einer Befragung teilzunehmen.

In meiner Stellungnahme hatte ich dem Institut mitgeteilt, dass nach meiner Auffassung keine Rechtsgrundlage für die Erhebung der Meldedaten besteht. Denn nach Art. 16 Abs. 1 Bayerisches Datenschutzgesetz (BayDSG) ist das Erheben personenbezogener Daten nur zulässig, wenn ihre Kenntnis zur Erfüllung der in der Zuständigkeit der erhebenden Stelle liegenden Aufgaben erforderlich ist. Erforderlich ist die Datenerhebung dann, wenn die Datenkenntnis die Aufgabenerfüllung objektiv unterstützt, fördert oder beschleunigt. Zwar konnte man dem geplanten Vorgehen die Förderlichkeit für das Forschungsprojekt nicht absprechen. Um die Erforderlichkeit bejahen zu können, hätte jedoch darüber hinaus die zu erfüllende Aufgabe wie auch die konkrete Unterstützung, Förderung oder Beschleunigung in Folge der Datenkenntnis mit den schutzwürdigen Interessen der Betroffenen an einer Nichtverwendung ihrer Daten in einem angemessenen Verhältnis stehen müssen. Vorliegend war bei dieser Güterabwägung den Interessen der Betroffenen Vorrang einzuräumen. Denn es handelte sich bei den zu erhebenden Daten um äußerst sensible Informationen über die Betroffenen.

Hinzu kommt, dass für das Forschungsvorhaben ein Adressmittlungsverfahren in Betracht kam. Dazu konnte das Institut die zu versendenden Schreiben den Meldebehörden zur Verfügung stellen, die diese wiederum an die Zielpersonen senden konnten, ohne dass die personenbezogenen Daten der anzuschreibenden Personen dem Institut zur Verfügung gestellt werden mussten. Es war für mich nicht erkennbar, welche wesentlichen Vorteile das geplante Vorgehen gegenüber einem Adressmittlungsverfahren gehabt hätte. Der Umstand, dass ein Adressmittlungsverfahren aufwendiger und kostenintensiver ist, musste angesichts der besonderen Schutzwürdigkeit der zu erhebenden Daten zurückstehen.

Durch Eingaben mehrerer Betroffener erfuhr ich einige Zeit später, dass das Institut offenbar entgegen meiner Stellungnahme Melderegisterauskünfte eingeholt hatte. Darauf angesprochen erklärte mir das Institut, es habe in jenen Bundesländern, in denen die Landesbeauftragten für den Datenschutz das Adressmittlungsverfahren empfohlen hätten (darunter u.a. auch Bayern), ein Adressmittlungsverfahren durchgeführt. Nur soweit die Landesdatenschutzbeauftragten anderer Bundesländer keine Einwände gegen eine Datenübermittlung aus den Melderegistern vorgebracht hätten, seien die personenbezogenen Daten aus den Melderegistern erhoben worden.

Ich habe das Institut hierzu darauf aufmerksam gemacht, dass es sich bei der Anforderung der Adressdaten bei den Meldebehörden durch das Institut um eine Datenerhebung des Instituts handelt, bei der Weitergabe der Adressdaten durch die Meldebehörden an das Institut hingegen - soweit erfolgt - um eine Datenübermittlung der jeweiligen Meldebehörden. Die datenschutzrechtliche Zulässigkeit der Datenerhebung und der Datenübermittlung ist getrennt für den jeweiligen Vorgang nach den jeweils hierfür geltenden Vorschriften zu beurteilen. Im Rahmen meiner Kontrollzuständigkeit für das Institut einer bayerischen Hochschule war allein bedeutsam, ob dieses die bei den Meldebehörden anderer Länder angeforderten personenbezogenen Daten überhaupt erheben durfte. Dies hatte ich in meiner früheren Stellungnahme bereits verneint. Im Ergebnis bedeutete dies, dass bereits unter dem Gesichtspunkt der Datenerhebung durch das Institut Adressmittlungsverfahren durchzuführen waren, unabhängig von Einschätzungen in anderen Bundesländern bezüglich der Zulässigkeit von Datenübermittlungen durch die dortigen Meldebehörden.

Auf eine förmliche Beanstandung des Instituts habe ich dennoch verzichtet. Denn zum einen hat mir das Institut glaubhaft versichern können, dass es die personenbezogenen Daten aus den Melderegistern - soweit erfolgt - gutgläubig erhoben hatte, nachdem eine Billigung der Datenübermittlung durch einige Landesdatenschutzbeauftragte vorlag. Soweit die Landesdatenschutzbeauftragten auf das Adressmittlungsverfahren verwiesen hatten, hat das Institut ohnehin keine Meldedaten erhoben. Zum andern hatte mir das Institut mitgeteilt, dass die Melderegisterdaten und auch die mit deren Hilfe selbst recherchierten Telefonnummern mittlerweile vollständig gelöscht sind, soweit die Betroffenen nicht bereits ihre Einwilligung zur Teilnahme an der Studie erklärt hatten. Ich konnte deshalb davon ausgehen, dass der Verstoß gegen datenschutzrechtliche Vorschriften nicht mehr fortdauert.

## 17.2 Zentrum Bayern Familie und Soziales

### 17.2.1 Evaluation des Bundeselterngeld- und Elternzeitgesetzes

Für einen Bericht der Bundesregierung (Bundesfamilienministerium) nach § 25 des Bundeselterngeld- und Elternzeitgesetzes (BEEG) gegenüber dem Bundestag über die Auswirkungen des BEEG sowie die ggf. notwendige Weiterentwicklung seiner Vorschriften wurde zur Durchführung der Befragung von Elterngeldbeziehern das Rheinisch-Westfälische Institut für Wirtschaftsforschung e.V. (RWI) beauftragt, das seinerseits mit dem Datendienstleister Wirtschafts- und Sozialforschung Kerpen (WSF) zusammenarbeitet.

Für die Zusendung eines Fragebogens an Elterngeldbezieher sollten dem WSF von den jeweiligen Elterngeldstellen der Länder (in Bayern: Zentrum Bay-

ern Familie und Soziales) auf der Grundlage des § 75 Abs. 1 SGB X die Adressen der Elterngeldbezieher mit einem zwischen dem 1.1.2007 und 31.3.2007 geborenem Kind übermittelt werden. Das für die Genehmigung nach § 75 Abs. 2 SGB X zuständige Staatsministerium für Arbeit und Sozialordnung, Familie und Frauen ist mit der Bitte um datenschutzrechtliche Prüfung der Datenübermittlung von den Elterngeldstellen an das RWI bzw. WSF an mich herangetreten.

Nach meiner Auffassung lagen die Voraussetzungen für eine Genehmigung der begehrten Datenübermittlung nach § 75 Abs. 2 SGB X nicht vor. Nach § 75 Abs. 1 Satz 1 SGB X ist eine Übermittlung von Sozialdaten u.a. nur dann zulässig, wenn sie für ein dort genanntes bestimmtes Vorhaben erforderlich ist. Eine Übermittlung ohne Einwilligung des Betroffenen ist u.a. nicht zulässig, soweit es zumutbar ist, den Zweck der Forschung oder Planung auf andere Weise zu erreichen (§ 75 Abs. 1 Satz 2 SGB X). Für die begehrte Datenübermittlung fehlte es nach meiner Auffassung an der Erforderlichkeit bzw. konnte der Zweck des Vorhabens zumutbar auf andere Weise erreicht werden. Denn es war möglich, ein bewährtes datenschutzfreundliches Verfahren, nämlich das sog. Adressmittlungsverfahren durchzuführen:

Bei diesem Verfahren bedarf es einer Datenübermittlung an das RWI bzw. WSF nicht. Das RWI bzw. das WSF muss lediglich dem Zentrum Bayern Familie und Soziales (ZBFS) die zu versendenden Fragebögen zur Verfügung stellen. Das ZBFS verschickt dann die Fragebögen an die in der Bruttostichprobe enthaltenen Adressen der Elterngeldbezieher. Die befragten Eltern können den freiwillig beantworteten, anonymen Fragebogen an das WSF zurückschicken. Um Irritationen zu vermeiden, kann im Rahmen des Anschreibens deutlich gemacht werden, dass das ZBFS die Anschriften nicht an das RWI bzw. das WSF weitergegeben hat, sondern lediglich die Fragebögen versendete. Auf diese Weise kann die Befragung durchgeführt werden, ohne dass die Sozialdaten der anzuschreibenden Personen dem WSF für den Versand zur Verfügung gestellt werden müssen. Das Argument, ein Adressmittlungsverfahren sei unzumutbar, weil damit eine für solche Fragebögenaktionen erforderliche Erinnerung der angeschriebenen Elterngeldbezieher nicht oder nur schwer durchführbar sei, überzeugt nicht. Selbst bei Unterstellung der Notwendigkeit einer Erinnerungsaktion ist nach meiner Auffassung die Durchführung eines Adressmittlungsverfahrens weiterhin möglich. Dies gilt auch dann, wenn die Elterngeldstellen nicht wissen, welche Eltern auf das erste Schreiben hin geantwortet haben. Denn es besteht die Möglichkeit, an alle Eltern aus der Bruttostichprobe eine Erinnerung seitens der Elterngeldstellen zu versenden. In einem solchen Erinnerungsschreiben könnte der Hinweis aufgenommen werden, dass die Erinnerung gegenstandslos ist, wenn der Fragebogen bereits ausgefüllt und versandt worden ist. Auch angesichts der Größe der Bruttostichprobe von bundesweit insgesamt 6000 Müttern bzw. Familien und einer anteilig in Bayern deutlich niedrigeren Anzahl ist diese Vorgehensweise möglich.

### 17.3 Kindeswohl und Datenschutz

Die Themen Kindeswohlgefährdung und Missbrauch von Kindern stehen seit einiger Zeit im Blickpunkt der Öffentlichkeit (Medien, Politik, Verwaltung). Hierbei werden immer wieder Schlagworte wie „Kinderschutz vor Datenschutz“ oder „Datenschutz darf das Kindeswohl nicht gefährden“ geäußert.

Der Arbeitskreis Gesundheit und Soziales der Bundes- und Landesbeauftragten für den Datenschutz hat deshalb am 6./7.03.2008 in Vorbereitung zur 75. Datenschutzkonferenz am 03./04.04.2008 die Thematik ausführlich diskutiert. Im Wesentlichen hat der Arbeitskreis folgende Positionen vertreten:

- „Datenschutz behindert den Kinderschutz nicht, noch steht er im Widerspruch zum Kinderschutz. Formulierungen wie „Kinderschutz vor Datenschutz“ sind zwar einprägsam, aber wenig zielführend und verstellen den Blick auf die zu lösenden Probleme.

- Die pauschale Formel „Kinderschutz vor Datenschutz“ verkennt insbesondere die schützende Funktion von Vertraulichkeit in Hilfebeziehungen. Es ist eine offene Diskussion auch darüber erforderlich, welche Schweigepflichten und Vertrauensverhältnisse für das Kindeswohl unabdingbar sind und wie weit man diese sinnvollerweise einschränken oder gar aufheben kann. Zu erwähnen ist z.B. die Gefahr, dass Hilfe aus Angst vor nachfolgenden Offenbarungen nicht mehr in Anspruch genommen wird. Auch die Auswirkungen von Stigmatisierungen Betroffener und folgende Beeinträchtigungen der Familien in „Verdachtsfällen“, die sich nicht bestätigen, sollten dabei nicht außer Acht gelassen werden.

- Erforderlich ist eine genaue Analyse, ob die vorhandenen Strukturen und Möglichkeiten in der Praxis bereits ausgeschöpft sind bzw. optimiert werden können, um den Kinderschutz bereits auf dieser Basis zu gewährleisten.

- Weitere gesetzliche Eingriffe in das informationelle Selbstbestimmungsrecht und damit vielfach in Vertrauensverhältnisse und Schweigepflichten sind allenfalls nach gründlicher Analyse der Geeignetheit, Erforderlichkeit und Verhältnismäßigkeit der entsprechenden Maßnahmen sowie nachfolgender Evaluation zu erwägen.“

In Bayern sind durch den Gesetzgeber zwischenzeitlich erhebliche Neuerungen zum Kinderschutz beschlossen worden. Mit Inkrafttreten des Gesetzes zur Änderung des Gesundheitsdienst- und Verbraucherschutzgesetzes und des Bayerischen Gesetzes über das Erziehungs- und Unterrichtswesen am 16.05.2008 (GVBl S. 158, BayRS 2120-1-UG, 2230-1-1-UK) gelten in Bayern insbesondere folgende, im neuen Art. 14 verankerte Regelungen (siehe hierzu auch Nr. 14.4 dieses Tätigkeitsberichts „Änderungen des GDVG“):

- Pflicht der Personensorgeberechtigten, die Teilnahme ihrer Kinder an den Früherkennungsuntersuchungen im Sinn der Richtlinien des Gemeinsamen Bundesausschusses gemäß § 26 in Verbindung mit § 25 Abs. 4 Satz 2 des Fünften Buches Sozialgesetzbuch sicherzustellen,

- Zusammenarbeit der Behörden für Gesundheit, Veterinärwesen, Ernährung und Verbraucherschutz mit anderen Stellen und öffentlichen Einrichtungen, insbesondere mit Schulen und Stellen der Schulverwaltung sowie mit Einrichtungen und Trägern der öffentlichen und freien Jugendhilfe; Einschaltung des Jugendamtes, wenn ihnen gewichtige Anhaltspunkte für eine Gefährdung des Wohls eines Kindes bekannt werden,

- Teilnahme an einer Schuleingangsuntersuchung im Jahr vor der Aufnahme in die Jahrgangsstufe 1,

- Vorlage eines Nachweises über die Teilnahme an der U9-Früherkennungsuntersuchung im Rahmen der Schuleingangsuntersuchung, bei fehlendem Nachweis Teilnahme an einer schulärztlichen Untersuchung, bei Verweigerung der schulärztlichen Untersuchung Mitteilung an das Jugendamt,

- Verpflichtung von Ärztinnen und Ärzten, Hebammen und Entbindungspflegern, gewichtige Anhaltspunkte für eine Misshandlung, Vernachlässigung oder einen sexuellen Missbrauch eines Kindes oder Jugendlichen, die ihnen im Rahmen ihrer Berufsausübung bekannt werden, dem Jugendamt mitzuteilen.

Im Rahmen des Gesetzgebungsverfahrens habe ich darauf hingewiesen, dass das Vertrauensverhältnis und der Geheimnisschutz zwischen dem Arzt und Eltern/Kind nicht gestört werden dürfe. Ich habe darauf aufmerksam gemacht, dass durch eine Meldepflicht von Ärzten und Hebammen gegenüber dem Jugendamt bei „gewichtigen Anhaltspunkten“ dieses Vertrauensverhältnis auf Seiten der Eltern beeinträchtigt werden könnte. Das könnte dazu führen, dass gerade in schwerwiegenden Fällen im Hinblick auf die Gefährdung des Kindeswohls die Eltern den Arzt nicht mehr aufsuchen werden, weil die Eltern damit rechnen müssen, an das Jugendamt gemeldet zu werden. Dies würde die Zielsetzung des Gesetzgebers, den Kinderschutz zu verbessern, im Ergebnis sogar infrage stellen.

In einem Fall, der die Thematik Kindeswohlgefährdung zum Gegenstand hatte, habe ich eine Beanstandung ausgesprochen. Es lag folgender Sachverhalt zu Grunde:

Die Meldebehörde einer kreisfreien Gemeinde (Bürgeramt) hat an das Amt für Kinder, Jugend und Familie (Jugendamt) dieser Gemeinde monatlich einen Ausdruck mit Vorname, Geschlecht und Geburtsdatum der Neugeborenen sowie Vornamen, Familienname und Adresse der Eltern bei ehelichen Kindern oder Vorname, Familienname und Adresse der Mutter bei nichtehelichen Kindern weitergegeben. Das Jugendamt hat es für notwendig gehalten, im Rahmen des Schutzauftrages zur Erhaltung des Kindeswohls, die Eltern aller neugeborenen Kinder anzuschreiben bzw. anzusprechen, um vor allem Hilfe und Beratung anzubieten. In diesem Zusammenhang sollten Hausbesuche durch Kinderkrankenschwestern durchgeführt werden, die bei der Gemeinde angestellt sind. Ich habe dazu folgende Rechtsauffassung vertreten:

Die Zulässigkeit der Übermittlung von personenbezogenen Daten (Art. 4 Abs. 6 Satz 2 Nr. 3 Buchst. a) Bayerisches Datenschutzgesetz - BayDSG) von der Meldebehörde (Bürgeramt) an das Jugendamt beurteilt sich nach Art. 28 Abs. 7 Meldegesetz. Die Meldebehörde prüft allerdings nur die Plausibilität der vom Jugendamt vorgetragenen Begründung für die Anforderung der Daten. Ob die Anforderung der Daten, die nach § 67 Abs. 5 SGB X eine Erhebung von Sozialdaten durch das Jugendamt darstellt, zulässig ist, entscheidet sich jedoch nach den Bestimmungen der §§ 61 ff. SGB VIII, § 35 SGB I, §§ 67 ff. SGB X. Sozialdaten dürfen vom Jugendamt demnach nur erhoben werden, soweit ihre Kenntnis zur Erfüllung der jeweiligen Aufgabe erforderlich ist (§ 62 Abs. 1 SGB VIII). Die Formulierung „jeweilige Aufgabe“ stellt klar, dass eine Datenerhebung einzelfallbezogen sein muss. Dementsprechend findet sich auch in den §§ 11 bis 60 SGB VIII keine Aufgabe, die generelle Ermittlungen des Jugendamtes ohne Anhaltspunkte im Einzelfall erforderte. Für eine regelmäßige und pauschale Erhebung der Daten aller Eltern und deren neugeborenen Kinder zur Erfüllung des Schutzauftrags „Kindeswohl“ bietet § 62 Abs. 1 SGB VIII jedenfalls keine Rechtsgrundlage. Dies ist auch nachvollziehbar, weil nicht bei allen Eltern neugeborener Kinder unterstellt werden kann, dass eine Kindeswohlgefährdung zu befürchten ist, vielmehr müssten, wie in § 8 a SGB VIII festgelegt, gewichtige Anhaltspunkte dafür vorliegen.

Fazit: Der monatliche Erhalt eines Ausdrucks von Vornamen, Geschlecht und Geburtsdatum Neugeborener sowie Vornamen, Familienname und Adresse der Eltern bei ehelichen Kindern oder Vornamen, Familienname und Adresse der Mutter bei nichtehelichen Kindern (Ausnahme § 21 b Personenstandsgesetz) ist in dieser pauschalen Form nicht durch eine Rechtsgrundlage im SGB VIII gedeckt. Da insoweit bereits eine gesetzliche Befugnis zur pauschalen Datenerhebung nicht vorliegt, ist auch eine pauschale Nutzung (§ 67 Abs. 7 SGB X) durch Weitergabe der Sozialdaten an von der Gemeinde angestellte Kinderkrankenschwestern zum Zwecke von Hausbesuchen bei allen Eltern bzw. Müttern nicht zulässig.

In einer dazu eingeholten Stellungnahme hat das Bayerische Staatsministerium für Arbeit und Sozialordnung, Familie und Frauen meine oben dargelegte Rechtsauffassung geteilt. Anlassunabhängige Hausbesuche mitsamt einer vorherigen „pauschalen“ Erhebung von Meldedaten seien auch in den vom Bayerischen Landesjugendhilfeausschuss zu § 8 a SGB VIII erstellten fachlichen Empfehlungen vom 15.03.2006 (abrufbar unter http://www.blja.bayern.de/Textoffice.Startseite.htm) nicht vorgesehen und somit nicht zulässig. Zulässig nach § 62 Abs. 1 i.V.m. Abs. 2 Nr. 2 lit. D SGB VIII sei nur ein einzelfallbezogenes Vorgehen, wie es in den fachlichen Empfehlungen beschrieben sei.

Auf meine Beanstandung hin hat mir die Gemeinde mitgeteilt, dass aufgrund der von mir dargelegten Rechtslage die pauschale monatliche Datenerhebung durch das Amt für Kinder, Jugend und Familie unverzüglich eingestellt wurde. Die Einstellung der Datenübermittlung wurde auch vom Bürgeramt der Gemeinde schriftlich bestätigt.

### 17.4 Krankenversicherungsrecht (Krankenkassen, MDK)

#### 17.4.1 MDK ISmed 3

ISmed 3 ist ein Verfahren zur vollständigen elektronischen Erstellung, Verarbeitung und Speicherung von Gutachten beim MDK (Medizinischer Dienst der Krankenkassen). Zudem soll der Auftraggeber für ein Gutachten (z.B. die Krankenkasse) zukünftig die Möglichkeit erhalten, Aufträge elektronisch zu erteilen, die Unterlagen hierzu bereitzustellen und den Stand der Bearbeitung so wie das Ergebnis elektronisch zu erhalten. Des Weiteren ist angedacht, auch zwischen MDKs Aufträge elektronisch weiterzuleiten. Damit soll ein vollständig elektronischer Workflow erreicht werden.

ISmed 3 wird von der ISmed-Gemeinschaft entwickelt und beim MDK Bayern im Rahmen eines Pilotbetriebs getestet, den ich unter rechtlichen und technisch-organisatorischen Gesichtspunkten geprüft habe.

Die ISmed-Gemeinschaft ist in Form einer Gesellschaft bürgerlichen Rechts organisiert. Ihr gehören 13 MDKs an. Zweck ist die Schaffung und Betreuung einer gemeinsamen EDV-Infrastruktur. Für die technischen Fragen wurde die ITSO (IT Service Organisation) eingerichtet, die den Betrieb der zentralen Systeme sicherstellt und die Fehlerbehebung im Pilotprojekt koordiniert.

Die Server für ISmed 3 werden von der GSKV GmbH (Rechenzentrum der BKKs in München) betrieben. Im Rechenzentrum der GSKV GmbH werden somit die Sozialdaten, die vom MDK erhoben bzw. dorthin übermittelt werden, verarbeitet. Hierbei handelt es sich um eine Verarbeitung von Sozialdaten durch die GSKV GmbH im Auftrag des MDK, so dass die Bestimmungen des § 80 Zehntes Buch Sozialgesetzbuch (SGB X) maßgeblich sind. Ich habe den MDK darauf hingewiesen, dass der Auftrag schriftlich zu erteilen ist, wobei die Datenverarbeitung, die technischen und organisatorischen Maßnahmen und etwaige Unterauftragsverhältnisse festzulegen sind (§ 80 Abs. 2 Satz 2 SGB X). Daraufhin wurde vom MDK ein Vertrag vorgelegt, der den Anforderungen des § 80 SGB X im Wesentlichen entspricht.

Auf der technischen Infrastruktur bei der GSKV GmbH wird für jeden MDK eine eigene Instanz von ISmed 3 betrieben, so dass jeder MDK nur auf seine eigenen Gutachten Zugriff hat. Die Gutachten sind in Versichertenakten organisiert. Ich habe in diesem Zusammenhang auf die Vorgaben des § 276 Abs. 2 Sätze 5 bis 8 Fünftes Buch Sozialgesetzbuch (SGB V) hingewiesen, die eine getrennte Speicherung der Sozialdaten zur Identifizierung des Versicherten von den medizinischen Sozialdaten erfordern (Trennungsgebot). Zum Prüfungszeitpunkt waren diese Vorgaben noch nicht umgesetzt, weil Gutachter im Begutachtungsfall Zugriff auf die bereits zusammengeführten medizinischen und identifizierenden Daten in der Versichertenakte hatten.

Für die Erstellung/Bearbeitung werden die Gutachten auf lokalen Servern der Zentrale bzw. der Außenstellen des MDK Bayern in einem Dokumentenmanagementsystem gespeichert. Nach ihrer Fertigstellung werden sie vom Gutachter elektronisch signiert und im zentralen System abgelegt. Alle lokalen Kopien werden dann gelöscht. Aus dem zentralen System werden sie nach Ablauf der 5-jährigen Aufbewahrungsfrist gelöscht.

Zum Prüfungszeitpunkt bestand die Möglichkeit, bereits erstellte Gutachten für neue Gutachtensaufträge heranzuziehen. Damit sollte sich die Löschfrist des alten Gutachtens automatisch auf die Frist des hinzuziehenden Gutachtens verlängern. Ich habe den MDK darauf hingewiesen, dass nach § 276 Abs. 2 Satz 3

SGB V die Sozialdaten nach 5 Jahren zu löschen seien. Soweit auf § 276 Abs. 2 Satz 4 SGB V in Verbindung mit § 304 Abs. 1 Satz 3 SGB V verwiesen werde, um eine Verlängerung der Aufbewahrungsfrist von Gutachten zu rechtfertigen, habe ich darauf aufmerksam gemacht, dass in diesem Fall sichergestellt sein müsse, dass ein Bezug zum Arzt und Versicherten nicht mehr herstellbar sei. Dies setze eine Anonymisierung der Sozialdaten voraus (§ 67 Abs. 8 SGB X). Sollte dies nicht möglich sein, müssten die Sozialdaten in Gutachten nach der insoweit nicht auslegungsfähigen Grundregel des § 276 Abs. 2 Satz 3 SGB V nach 5 Jahren gelöscht werden. Eine automatische Verlängerung der Aufbewahrungsfristen bestehender Gutachten durch die Hinzuziehung dieser bestehenden Gutachten zu neu in Auftrag genommenen Gutachten könne somit nicht angenommen werden.

Zum Prüfungszeitpunkt waren alle Arbeitsplätze, also auch alle Außenstellen des MDK Bayern, mit ISmed 3 ausgerüstet, es wurden jedoch noch nicht alle Gutachten darüber abgewickelt. Zudem waren alle Gutachter mit einer Signaturkarte mit qualifiziertem Zertifikat für die elektronische Unterzeichnung der Gutachten ausgestattet.

Aus technisch-organisatorischer Sicht ist ISmed 3 von besonderem Interesse, da es sich einerseits bei den gespeicherten Daten um medizinische Daten handelt, die einem besonderen Schutzbedarf unterliegen und daher erhöhte Schutzmaßnahmen nötig sind. Gleichzeitig befinden sich die Server in einem externen Rechenzentrum, so dass die Gefahr einer unbefugten Kenntnisnahme durch die dortigen Administratoren besteht. Drittens handelt es sich bei ISmed 3 um eines der ersten Verfahren im aktiven Betrieb, das vollständig auf Papier verzichtet und die Integrität und Authentizität der Gutachten über eine qualifizierte Signatur sicherstellt.

Zur Gewährleistung der Vertraulichkeit der sensiblen Daten wurden diverse Sicherheitsmaßnahmen ergriffen. Unter anderem werden alle Daten für den Transport zwischen dem MDK und dem zentralen Server verschlüsselt. Bei den im Rechenzentrum gespeicherten Daten werden alle identifizierenden Daten (Name, Adresse etc.) verschlüsselt. Damit sollen die gesetzlichen Vorgaben zu einer pseudonymisierten Speicherung der Gutachten erfüllt werden. Zudem ist es auf diese Art möglich, die Gutachtensinhalte für statistische und andere Zwecke ohne Personenbezug auszuwerten. Es muss allerdings sichergestellt werden, dass nur der jeweilige MDK und nicht das Rechenzentrum Zugriff auf die Verschlüsselungsschlüssel hat. Zudem habe ich eine Verschlüsselung der gesamten Daten empfohlen, um den Mitarbeitern des Rechenzentrums keinerlei Einblick in die Daten zu gewähren.

Jeder Gutachter kann nur auf diejenigen zentral gespeicherten Gutachten mit Personenbezug zugreifen, für die er einen Auftrag hat. Dies wird über ein differenziertes Berechtigungskonzept sowie die Authentifizierungszertifikate der Chipkarte kontrolliert.

Um Sicherheitsvorfälle feststellen zu können, findet an mehreren Stellen eine Protokollierung statt, z.B. Depseudonymisierung der Daten, Änderung von Rollen und Rechten, erfolglose Authentifizierungsversuche, Bearbeitung von Gutachten, Konfigurationsänderung, Administratortätigkeiten.

Soweit die erwähnten rechtlichen Anmerkungen beachtet werden, bestehen keine Einwände gegen den Einsatz von ISmed 3 in der geplanten Form. In einigen Punkten habe ich zusätzliche technisch-organisatorische Maßnahmen vorgeschlagen, um das Sicherheitsniveau des Verfahrens noch weiter zu erhöhen. Die zukünftige Entwicklung des Verfahrens werde ich auch weiterhin in Kooperation mit den anderen betroffenen Landesbeauftragten verfolgen.

## 17.5 Wohngeldstellen

### 17.5.1 Presse- und Öffentlichkeitsarbeit mit Sozialdaten

Zur Presse- und Öffentlichkeitsarbeit mit Sozialdaten habe ich mich bereits in der Vergangenheit geäußert (vgl. hierzu Nr. 4.1 und 16.1, 19. Tätigkeitsbericht). Ein Vorgang aus dem aktuellen Berichtszeitraum veranlasst mich, nochmals ausdrücklich auf meine damaligen Ausführungen hinzuweisen und diese hier zu ergänzen.

Sozialdaten und damit auch die im Rahmen eines Wohngeldantrags gemachten Angaben unterliegen dem Sozialdatenschutz des § 35 Sozialgesetzbuch - Erstes Buch - (SGB I). Solche Daten dürfen nur dann an Dritte übermittelt werden, wenn eine entsprechende, wirksame Einwilligung des Betroffenen vorliegt oder eine gesetzliche Befugnisnorm im Sozialgesetzbuch diese Datenübermittlung erlaubt.

Im konkreten Fall hat eine Wohngeldstelle bzw. Kommune Strafanzeige gegen einen Leistungsbezieher erstattet. Die örtliche Presse hat hierüber einschließlich detaillierter Informationen aus dem Wohngeld-Vorgang berichtet. Für die Weitergabe dieser Informationen an die Presse seitens der Kommune wäre keine gesetzliche Befugnisnorm im Sozialgesetzbuch ersichtlich gewesen. Da diese Informationen aber bereits vor der Veröffentlichung nicht nur der Kommune bekannt waren und auch die vom Betroffenen eingeschaltete Staatsanwaltschaft nicht herausfinden bzw. nachweisen konnte, von wem die Daten letztlich an die Presse weitergegeben worden sind, konnte ich keine konkrete Stelle beanstanden.

Im weiteren Verlauf der Presseberichterstattung waren zusätzliche Informationen im Hinblick auf diesen Wohngeld-Vorgang veröffentlicht worden. Teilweise hat sich die Presse hierbei auf Aussagen des Betroffenen selbst berufen, teilweise hatte sich die Kommune gegenüber der Presse geäußert und teilweise ließ sich nicht aufklären, von wem eine einzelne Information im weiteren Verlauf an die Presse weitergegeben worden ist.

Im Rahmen meines Schriftwechsels mit der Kommune hat diese u.a. darauf hingewiesen, dass die Kommune zu keiner Zeit aktiv auf die Presse zugegangen sei, sondern immer nur insbesondere auf (unrichtige) Äußerungen des Leistungsbeziehers in der Presse reagiert habe.

Gemäß § 69 Abs. 1 Nr. 3 Sozialgesetzbuch - Zehntes Buch - (SGB X) ist die Übermittlung von Sozialdaten zulässig, soweit sie erforderlich ist für die Richtigstellung unwahrer Tatsachenbehauptungen des Betroffenen im Zusammenhang mit einem Verfahren über die Erbringung von Sozialleistungen. Gemäß der genannten Regelung bedarf diese Übermittlung dann allerdings der vorherigen Genehmigung durch die zuständige oberste Bundes- oder Landesbehörde. Auch wenn aus Sicht der Kommune hier Richtigstellungen unwahrer Tatsachenbehauptungen erforderlich waren, so hätte sie jedenfalls vorher die Genehmigung der zuständigen obersten Landesbehörde einholen müssen. Dies hat sie jedoch nicht getan.

Weiterhin waren - auch wenn man die Erforderlichkeit einer Richtigstellung dem Grunde nach unterstellt - nicht alle Informationen für die Richtigstellung als solche erforderlich. Für darüber hinausgehende Datenübermittlungen lediglich im Zusammenhang mit einer Richtigstellung kann § 69 Abs. 1 Nr. 3 SGB X keine Rechtsgrundlage darstellen.

Ich habe die Kommune daher eindringlich auf die sozialdatenschutzrechtlichen Vorgaben im Hinblick auf eine Presse- und Öffentlichkeitsarbeit mit Sozialdaten hingewiesen sowie zur entsprechenden Beachtung und Einhaltung aufgefordert.

Ich rate allen Behörden dringend an, vor der Übermittlung von Sozialdaten im Zusammenhang mit einer Presse- oder Öffentlichkeitsarbeit sehr genau zu prüfen, ob im konkreten Fall überhaupt und ggf. in welchem Umfang eine solche Übermittlung zulässig wäre.

## 17.6 Arbeitsgemeinschaften (ARGEn) und Sozialämter

### 17.6.1 Datenschutz bei Arbeitsgemeinschaften nach § 44 b SGB II

Die an mich gerichteten Eingaben und Anfragen aus dem Bereich Soziales standen oftmals im Zusammenhang mit Leistungen nach dem Sozialgesetzbuch - Zweites Buch - (SGB II), umgangssprachlich auch häufig als „Hartz-IV“ bezeichnet.

In diesem Zusammenhang sind an mich sowohl neue Fallgestaltungen als auch „alt bekannte“ datenschutzrechtliche Themen herangetragen worden. Nachfolgend stelle ich eine Auswahl der von mir behandelten Vorgänge vor.

Meine Kontrollzuständigkeit für die ARGEn in Bayern kann nur auf der Grundlage bestehen, dass die ARGEn selbst eigenverantwortlich speichernde Stellen sind, auch wenn die ARGEn durch einerseits einen kommunalen Träger und andererseits die Agentur für Arbeit errichtet werden. Gemäß Urteil des Bundesverfassungsgerichts vom 20.12.2007 (2 BvR 2433/04, 2 BvR 2434/04) verstößt die in § 44 b SGB II getroffene Regelung, wonach die kommunalen Träger und die Bundesagentur für Arbeit zur einheitlichen Wahrnehmung ihrer Aufgaben Arbeitsgemeinschaften bilden sollen, gegen Art. 28 Abs. 2 i.V.m. Art. 83 des Grundgesetzes. Das in der Vorschrift geregelte Zusammenwirken von Bundes- und Landesbehörden überschreite die Grenzen des verfassungsrechtlich Zulässigen. Bis zu einer gesetzlichen Neuregelung, längstens bis zum 31.12.2010, bleibe die Norm jedoch anwendbar. Demzufolge sehe ich derzeit keinen Anlass, insofern von der bisherigen Verfahrensweise abzuweichen.

Das Bundesverfassungsgericht hat darauf hingewiesen, dass Ausdruck der mangelhaften Zuordnung von Verantwortlichkeiten, die mit der unklaren Zuordnung der Arbeitsgemeinschaften zur Bundes- oder zur kommunalen Ebene zusammenhängt, auch Unsicherheiten hinsichtlich der Anwendbarkeit von Bundes- und Landesrecht sind, wie sie etwa im Vollstreckungsrecht und beim Datenschutz aufgetreten sind. Es bleibt zu hoffen, dass nach einer gesetzlichen Neuregelung insbesondere die datenschutzrechtlichen Zuständigkeiten eindeutig und nachvollziehbar festgelegt sind.

Ich vertrete die Auffassung, dass die ARGEn nach § 44 b SGB II gemäß der Regelung in Art. 25 Abs. 2 BayDSG einen behördlichen Datenschutzbeauftragten zu bestellen haben. Diese Sichtweise teilen offensichtlich jedoch nicht alle ARGEn. Einzelne ARGEn haben nach meiner Intervention einen behördlichen Datenschutzbeauftragten oder einen „Datenschutzverantwortlichen“ bestellt. Ich werde diese Auffassung weiterhin gegenüber den ARGEn vertreten und auf die Bestellung eines behördlichen Datenschutzbeauftragten nach Art. 25 Abs. 2 BayDSG drängen.

Ein immer wieder kehrendes Thema sind die organisatorischen Rahmenbedingungen in den ARGEn bei persönlichen Kontakten. Als Beispiele seien etwa offen stehende Türen bei Gesprächen mit dem Sachbearbeiter oder Diskretionsabstände an einem Empfangsschalter genannt (vgl. hierzu Nr. 14.4.1, 22. Tätigkeitsbericht). Im Hinblick auf die Antragsannahme bzw. „Sichtung“ der Unterlagen hatte eine ARGE eine ganz besondere Idee. Ein hiervon betroffener Bürger hatte sich daraufhin an mich gewandt. Er wollte seine Antragsunterlagen bei der ARGE vorlegen, sei von dort jedoch darauf verwiesen worden, die Unterlagen bei der örtlichen Volkshochschule abzugeben. Erst nach Weigerung des betroffenen Bürgers und Rücksprache mit dem „Amtsleiter“ habe er die Unterlagen persönlich bei der ARGE abgeben dürfen.

Ich bin daraufhin an die ARGE mit datenschutzrechtlichen Hinweisen und der Aufforderung zur unverzüglichen Stellungnahme herangetreten. Die ARGE hat mir daraufhin mitgeteilt, dass Kunden mit sofortiger Wirkung nicht mehr verpflichtet würden, den Antrag auf Arbeitslosengeld II bei der Volkshochschule abgeben zu müssen. Die Annahme der Antragsunterlagen erfolge somit wieder ausschließlich bei der ARGE. Darüber hinaus werde die ARGE dafür Sorge tragen, dass sämtliche Daten, die bei der Volkshochschule erhoben und dort gespeichert worden seien, gelöscht bzw. vernichtet würden. Zudem wurde ich gebeten, dem betroffenen Bürger das ausdrückliche Bedauern für die entstandenen Unannehmlichkeiten zu übermitteln. Der Geschäftsführer der ARGE stehe diesem für eine persönliche Entschuldigung jederzeit zur Verfügung.

Zum Sachverhalt selbst hatte die ARGE noch mitgeteilt, dass insofern ein „Informations- und Orientierungsseminar, Sofortmaßnahme“ gemäß §§ 15 a, 16 Abs. 1 SGB II i.V.m. § 48 SGB III bei der Volkshochschule durchgeführt worden sei. Die Maßnahme sei seit kurzem und bislang jedem erwerbsfähigen Hilfebedürftigen anlässlich der Antragstellung angeboten worden. In diesem Rahmen habe es auch ein Modul gegeben, in dem die Annahme und „Sichtung“ des Antrags enthalten sei. Es habe ein Coaching im Hinblick auf die Sichtung und Bearbeitung der Leistungsanträge bzw. im Hinblick auf die Annahme der vollständigen Leistungsanträge mit anschließender Weiterleitung an die ARGE gegeben.

Bei den Datenerhebungen von ARGEn hat wiederholt die Zulässigkeit von Datenerhebungen im Zusammenhang mit Hausbesuchen eine Rolle gespielt. Soweit hier im Einzelfall die datenschutzrechtlichen Voraussetzungen für Datenerhebungen bzw. entsprechende datenschutzrechtlichen Hinweis- und Belehrungspflichten im Zusammenhang mit einem Hausbesuch nicht eingehalten wurden, habe ich die jeweilige ARGE auf die aus datenschutzrechtlicher Sicht einzuhaltenden Verfahrensweisen hingewiesen und zur Einhaltung der datenschutzrechtlichen Voraussetzungen aufgefordert.

Im Zusammenhang mit einem Antrag auf Gewährung von Reisekosten hat eine ARGE die Vorlage einer ausgefüllten „Bescheinigung zur Vorlage bei dem Träger der Grundsicherung“ unter Hinweis auf die Mitwirkungspflicht des Antragstellers verlangt. Der Betroffene hatte sich zuvor bei einem potentiellen auswärtigen Arbeitgeber vorgestellt. Das Formular, das aus der Formulierung und dem Formularkopf ersichtlich anschließend an die ARGE zu übergeben bzw. zu schicken war, hätte vom potentiellen Arbeitgeber ausgefüllt bzw. bestätigt werden müssen, der damit vom Leistungsbezug Kenntnis erlangt hätte. Ich habe daraufhin die ARGE angeschrieben und um Stellungnahme zur Erforderlichkeit der einzelnen Fragen bzw. der Ausgestaltung des Verfahrens und des Formulars gebeten. Die ARGE hat mein Schreiben daraufhin der Bundesagentur für Arbeit vorgelegt, da es sich um eine zentrale Vorlage von dort handelte. Die Bundesagentur für Arbeit hat mir letztlich mitgeteilt, dass dieser Vordruck künftig nicht mehr zum Einsatz komme und eine Datenerhebung bei einem potentiellen Arbeitgeber insofern nicht mehr erfolgen werde.

Soweit eine ARGE erforderliche Daten erheben will, gilt der Grundsatz, dass diese Daten beim Betroffenen selbst zu erheben sind. Nur in den gesetzlich bestimmten Fällen (§ 67 a Abs. 2 Satz 2 SGB X) sind Datenerhebungen bei Dritten zulässig. Die gesetzlich geregelten Voraussetzungen lagen in Einzelfällen bei Datenerhebungen bspw. bei Nachbarn und Vermietern, der Schule oder dem Arbeitgeber nicht vor, so dass ich die im Einzelfall handelnden ARGEn dann jeweils zur Beachtung der sozialdatenschutzrechtlichen Voraussetzungen und zur Unterlassung einer vergleichbaren Verfahrensweise aufgefordert habe. In Vergessenheit gerät neben den Voraussetzungen für die Datenerhebung als solche gerne auch die der Behörde obliegende Hinweispflicht nach § 67 a Abs. 4 SGB X: „Werden Sozialdaten bei einer nichtöffentlichen Stelle erhoben, so ist diese Stelle auf die Rechtsvorschrift, die zur Auskunft verpflichtet, sonst auf die Freiwilligkeit hinzuweisen.“

Ein (ausdrücklicher) Hinweis auf die Freiwilligkeit kann dabei auch nicht dadurch ersetzt werden, dass die Behörde lediglich eine Verpflichtung zur Auskunft nicht ausdrücklich behauptet. Gleiches gilt für die ggf. nach Maßgabe des § 67 a Abs. 5 SGB X bestehende Pflicht zur Unterrichtung des Betroffenen bei solchen Dritterhebungen.

ARGEn erheben aber nicht nur Daten, sondern übermitteln in verschiedenen Fallkonstellationen auch Sozialdaten. Dies ist nur dann zulässig, wenn entweder die Einwilligung des Betroffenen vorliegt oder eine gesetzliche Befugnisnorm im Sozialgesetzbuch dies gestattet (§ 67 d Abs. 1, § 67 b Abs. 1 SGB X).

Im nachfolgenden Fall habe ich insbesondere die Datenübermittlung einer ARGE beanstandet und die ARGE aufgefordert, die dorthin mitgeteilten Gesichtspunkte zum Sozialdatenschutz zu beachten und ein Vorgehen wie geschehen zukünftig zu unterlassen.

Ein Sachbearbeiter einer ARGE hatte eine Antragstellerin, die in einem Pflegeheim gearbeitet hatte, telefonisch nach den Umständen des Verlustes ihrer letzten Arbeitsstelle befragt. Die Antragstellerin hatte sich u.a. dahin geäußert, dass sie auf Missstände gestoßen sei und diese auch der Heimaufsicht angezeigt habe. Weiterhin hatte sie sich in diesem Zusammenhang auch über den Leiter der Heimaufsicht negativ geäußert.

Die ARGE hat über das Telefongespräch im Rahmen der Antragsbearbeitung einen (personenbezogenen) Gesprächsvermerk angefertigt und diesen an den besagten Leiter der Heimaufsicht weitergegeben. Dieser hat daraufhin eine Unterlassungsklage gegen die Antragstellerin im Hinblick auf deren negative Äußerung angestrengt und den Aktenvermerk als Beweismittel bezeichnet.

Entgegen der Auffassung der ARGE in deren Stellungnahme unterfallen Daten aus diesem Gesprächsvermerk hier eindeutig den sozialdatenschutzrechtlichen Vorschriften. Die hilfsweise von der ARGE angeführten Befugnisnormen (§ 68 Abs. 1 Satz 1 SGB X und § 71 Abs. 1 Satz 1 Nr. 1 SGB X) waren ebenfalls eindeutig nicht erfüllt. Die ARGE hat nicht nur aufgrund der eigentlichen Datenübermittlung, sondern auch durch ihre nachfolgende Stellungnahme gezeigt, dass die sozialdatenschutzrechtlichen Vorschriften dort offensichtlich nicht ausreichend bekannt sind bzw. beachtet werden. Ich habe die ARGE daher beanstandet. Die Heimaufsichtsbehörde habe ich zudem auf die fehlende Datenübermittlungsbefugnis der ARGE aufmerksam gemacht und eindringlich darauf hingewiesen, dass die unbefugt übermittelten Sozialdaten nicht genutzt und/oder (weiter) übermittelt werden dürfen.

Eine Datenübermittlung liegt auch in der Überweisung der Miete von der ARGE direkt an den Vermieter. Denn bereits hierdurch wird der Vermieter regelmäßig von einem Sozialleistungsbezug seines Mieters in Kenntnis gesetzt. Auch hier gilt der datenschutzrechtliche Erforderlichkeitsgrundsatz. Die ARGE müsste daher genau begründen, warum diese direkte Überweisung an den Vermieter zur Aufgabenerfüllung der ARGE nach dem SGB II erforderlich ist. Der Gesetzgeber hat in § 22 Abs. 4 SGB II geregelt, dass die Kosten für Unterkunft und Heizung an den Vermieter oder andere Empfangsberechtigte gezahlt werden sollen, wenn die zweckentsprechende Verwendung durch den Hilfebedürftigen nicht sichergestellt ist. An mich haben sich Leistungsbezieher nach dem SGB II mit der Bitte gewandt, die Überweisung an sie selbst sicherzustellen, da die zuständige ARGE dies auch auf entsprechende Hinweise der Betroffenen verweigerte. Nach rechtlichen Hinweisen meinerseits hat die ARGE den Vorgang nochmals geprüft und ist zu dem Ergebnis gekommen, dass in diesem Fall die Miete wieder direkt an die Leistungsbezieher ausgezahlt wird.

## 17.7 Heimrecht

### 17.7.1 Anonymisierung der Prüfberichte der Heimaufsicht

Die für die Heimaufsicht zuständigen Behörden haben eine wichtige Aufgabe: Sie kontrollieren zum Schutz pflege- und betreuungsbedürftiger Menschen, ob insbesondere in den Heimen die gesetzlichen Qualitätsanforderungen erfüllt sind. Dazu führen die Heimaufsichtsbehörden u.a. wiederkehrende und anlassbezogene Prüfungen in den Heimen durch, deren Ergebnisse sie in Prüfberichten zusammenfassen.

Durch eine Eingabe habe ich erfahren, dass eine Heimaufsichtsbehörde die Prüfberichte nicht nur an die Träger des jeweils kontrollierten Heims, sondern - per einfacher E-Mail - auch an andere Stellen wie z.B. das Gesundheitsamt, eine gesetzliche Krankenkasse, den Medizinischen Dienst der Krankenkassen (MDK), den Bezirk, und die Regierung weitergibt. Im konkreten Fall waren die betroffenen Bewohnerinnen und Bewohner in dem Prüfbericht sinngemäß wie folgt aufgeführt: „Wohnbereich 1: Frau A., Herr Z., Frau N.; Wohnbereich 2: Frau Doris F., Herr P., Frau F.“ Im weiteren Verlauf waren bezogen auf die einzelnen Bewohnerinnen und Bewohner die Ergebnisse der Prüfung sehr detailliert dargestellt. Dies betraf z.B. die Wohnsituation bei Frau F., die Verordnung bestimmter Medikamente wegen bestimmter Erkrankungen bei Frau A., Frau N. sowie Frau F., erforderliche Prophylaxen bei Frau A. und Frau F., Feststellungen zur Ernährungssituation, Körperpflege und zum Umgang mit Dekubital-

geschwüren jeweils bei Herrn Z. sowie über freiheitsentziehende Maßnahmen bei Frau F.

Ich habe der Heimaufsichtsbehörde mitgeteilt, dass ein derart gestalteter Prüfbericht personenbezogene Daten über die Bewohnerinnen und Bewohner des Heims enthält. Dabei handelt es sich vor allem um besonders sensible Daten über die Gesundheit (vgl. Art. 15 Abs. 7 BayDSG). Eine Anonymisierung im Sinne des Art. 4 Abs. 8 BayDSG liegt nicht vor, da durch Angabe des Wohnbereichs, des Geschlechts, des Anfangsbuchstabens des Nachnamens und teilweise des vollen Vornamens die Daten in den meisten Fällen ohne unverhältnismäßig großen Aufwand an Zeit, Kosten und Arbeitskraft einer bestimmten oder bestimmbaren natürlichen Person zugeordnet werden können.

Die Weitergabe der in dem Prüfbericht enthaltenen personenbezogenen Daten der Bewohnerinnen und Bewohner an die oben genannten Stellen stellt eine Datenübermittlung bzw. -nutzung dar. Hierfür besteht keine Rechtsgrundlage, insbesondere weil diese Stellen - das war unstreitig - keine personenbezogenen Daten über Bewohnerinnen und Bewohner benötigen, um ihre Aufgaben zu erfüllen.

Darüber hinaus habe ich in technisch-organisatorischer Hinsicht auf Folgendes hingewiesen: Der Versand personenbezogener Daten per E-Mail über das Internet entspricht ohne zusätzliche Sicherheitsmaßnahmen nicht den Anforderungen des Datenschutzes, da hier u.a. die Vertraulichkeit, Integrität und Revisionsfähigkeit der Daten nicht gegeben ist. Art. 7 BayDSG fordert technisch-organisatorische Sicherheitsmaßnahmen, die auch bei diesem Transportmedium gewährleistet sein müssen. Üblicherweise ist für den E-Mail-Versand mindestens die Verschlüsselung der Daten zu fordern. Weiterhin können Maßnahmen erforderlich sein, um die Überprüfbarkeit von Sender und Empfänger zu gewährleisten.

Daraus folgt: Will die Heimaufsichtsbehörde den Prüfbericht weiterhin an die oben genannten Stellen weitergeben, muss sie die personenbezogenen Daten der Bewohnerinnen und Bewohner den Anforderungen des Art. 4 Abs. 8 BayDSG entsprechend anonymisieren. Im Hinblick auf die in den Prüfberichten enthaltenen besonders sensiblen Daten über die Gesundheit, die Vielzahl der Empfänger der Prüfberichte und den vorgesehenen Versand per E-Mail ist hier ein strenger Maßstab anzulegen. Für eine Anonymisierung genügt es daher nicht, dass für die Bewohnerinnen und Bewohner statt des abgekürzten Namens die Pseudonyme „Bewohner 1“, „Bewohner 2“, etc. verwendet werden. Zwar wäre die Zuordnung der in den Prüfberichten enthaltenen Daten zu einer bestimmten Person im Vergleich zur bisherigen Praxis erschwert, allerdings nicht in einem für die Beseitigung des Personenbezugs ausreichenden Maße. Dies lässt sich am Beispiel des oben beschriebenen Prüfberichts erkennen: Wäre dort z.B. Frau F als „Bewohner 1“ bezeichnet und verfügt ein Dritter über Zusatzwissen, weil diesem z.B. bekannt ist, dass Frau F. aus dem Wohnbereich 2 unter einer bestimmten Krankheit leidet, kann der Dritte der Bezeichnung „Bewohner 1“ einer konkrete Person, nämlich Frau F, zuordnen. Durch den Prüfbericht werden dem Dritten dann auch Einzelheiten zur Wohnsituation sowie zu erforderlichen Prophylaxen und freiheitsentziehenden Maßnahmen bei Frau F bekanntgegeben. Von einer Anonymisierung kann erst dann ausgegangen werden, wenn entweder im Prüfbericht selbst die Identifikationsmerkmale vollständig gelöscht sind oder die Daten in einem für die Weitergabe an andere Stellen bestimmten eigenständigen Bericht aggregiert, also zusammengefasst werden.

Die Thematik der Anonymisierung der Prüfberichte der Heimaufsicht wird zukünftig über den mir vorgelegten konkreten Fall hinaus Bedeutung erlangen. Denn das zum 01.08.2008 in Kraft getretene Pflege- und Wohnqualitätsgesetz (PfleWoqG) sieht in Art. 6 Abs. 2 vor, dass ab dem 01.01.2011 die Prüfberichte der Heimaufsichtsbehörden in geeigneter Form zu veröffentlichen sind. Darüber hinaus bestimmt Art. 11 Abs. 10 PfleWoqG, dass alle Organisationseinheiten innerhalb der für die Heimaufsicht zuständigen Behörden, deren Prüfungen sich auf stationäre Einrichtungen erstrecken (gemeint sind laut Gesetzesbegründung z.B. die Lebensmittelkontrolle oder die Bauaufsichtsbehörden), die jeweiligen Prüfberichte auszutauschen haben. Die Weitergabe personenbezogener, insbesondere auch medizinischer Daten der Bewohnerinnen und Bewohner an Stellen wie z.B. die Bauaufsichtsbehörden oder gar die Öffentlichkeit (Aushang im Heim? Veröffentlichung im Internet?) würde deren Persönlichkeitsrechte massiv verletzen. Daher wird besonders darauf zu achten sein, dass die Prüfberichte nur in anonymisierter Form ausgetauscht und veröffentlicht werden. Es gilt zu verhindern, dass das wichtige Ziel des Pflege- und Wohnqualitätsgesetz, durch die Veröffentlichung der Prüfberichte im Interesse der Bewohnerinnen und Bewohner mehr Transparenz zu schaffen, nicht durch eine Veröffentlichung intimer Daten der Bewohnerinnen und Bewohner diskreditiert wird.

### 17.8 Jugendämter - Auskunft über Namen von Behördeninformanten

Gerade im Bereich des Kindeswohls wird immer wieder eine Kultur des Hinsehens eingefordert. Dies wird oftmals nicht nur auf Behörden, sondern vielmehr auch auf alle Bürgerinnen und Bürger bezogen.

Aus einem solchen Hinsehen entsteht manchmal Besorgnis um das Wohl von bestimmten Kindern. Mancher Nachbar oder Verwandter teilt seine Beobachtungen dann dem Jugendamt mit, das bei entsprechender Veranlassung tätig wird.

Soweit das Jugendamt aufgrund solcher Beobachtungen bspw. eines Nachbarn tätig wird und die betroffenen Eltern hiervon Kenntnis erlangen, wollen diese in der Folge oftmals vom Jugendamt wissen, welche Person (Name und ggf. Anschrift) sich an das Jugendamt gewandt hat. Hierbei führen die betroffenen Eltern beispielsweise an, sie wollten nach entsprechender Auskunft gerichtlich gegen den Behördeninformanten vorgehen. Im Berichtszeitraum haben sich betroffene Eltern an mich gewandt, da sie der Auffassung waren, dass sie einen Anspruch auf Offenlegung des Namens des Behördeninformanten hätten. Das Jugendamt hatte insoweit jeweils sowohl eine entsprechende Akteneinsicht als auch eine Auskunft verweigert. Das Jugendamt müsse bei Nennung des Namens des Behördeninformanten im Übrigen damit rechnen, dass sich wiederum dieser hierüber beschwere, denn auch sein Name falle unter das Sozialgeheimnis des § 35 SGB I und dürfe nur nach Maßgabe der sozialdatenschutzrechtlichen Vorschriften weitergegeben werden.

Doch wer hat nun Recht? Grundsätzlich in Frage kommende Anspruchsgrundlagen wie § 25 SGB X (Akteneinsicht) oder § 83 SGB X (Auskunft) enthalten auch Ausschlusstatbestände. Ich kann an dieser Stelle nicht alle rechtlichen Detailfragen darstellen, möchte aber auf wesentliche Formulierungen hierzu in der Rechtsprechung hinweisen. Gemäß dem Bundesverwaltungsgericht (Urteil vom 04.09.2003, Az. 5 C 48/02 zu einem Vorgang aus dem Bereich Sozialhilfe) kommt eine Akteneinsicht bzw. eine Auskunft im Hinblick auf den Namen eines Behördeninformanten dann in Betracht, wenn ausreichende Anhaltspunkte für die Annahme vorlägen, dass der Behördeninformant wider besseres Wissen und in der vorgefassten Absicht, den Ruf des Klägers zu schädigen, gehandelt oder der Behörde leichtfertig falsche Informationen übermittelt haben könnte.

Für den Bereich der Kinder- und Jugendhilfe (SGB VIII), also bei einer Information an ein Jugendamt, hat eine erstinstanzliche Gerichtsentscheidung darauf hingewiesen, dass das Jugendamt zur Gestattung einer Akteneinsicht bzw. zu einer Auskunft gemäß § 65 SGB VIII nicht berechtigt sei, soweit die streitbefangenen Sozialdaten den Mitarbeitern des Jugendamts zum Zwecke persönlicher und erzieherischer Hilfe anvertraut worden seien und kein Ausnahmefall gemäß § 65 Abs. 1 Satz 1 Nrn. 1 bis 5 SGB VIII vorliege. Der Sozialdatenschutz im Jugendhilferecht gehe weiter als der allgemeine Sozialdatenschutz. Das Gericht hat im dort entschiedenen Fall einen Anspruch auf entsprechende Akteneinsicht bzw. Auskunft im Hinblick auf den Namen des Informanten abgelehnt.

Jedenfalls in der vom Bundesverwaltungsgericht angesprochenen Konstellation einer Information wider besseres Wissen und in Schädigungsabsicht wäre es zwar fraglich, ob das Tatbestandsmerkmal „zum Zwecke persönlicher und erzieherischer Hilfe anvertraut“ erfüllt sein und damit § 65 SGB VIII zur Anwendung kommen könnte.

In den im Berichtszeitraum aufgetretenen und mir vorgetragenen Fällen, in denen das Jugendamt (oder eine andere Behörde) eine Auskunft bzw. Akteneinsicht im Hinblick auf den Namen des Behördeninformanten verweigert hat, habe ich jeweils keinen Verstoß gegen datenschutzrechtliche Vorschriften festgestellt.

### 17.9 Gesetzentwurf über das Verfahren des elektronischen Entgeltnachweises (ELENA-Verfahrensgesetz)

Die Bundesregierung hat am 25.06.2008 den Gesetzentwurf über das Verfahren des elektronischen Entgeltnachweises (ELENA-Verfahrensgesetz) beschlossen (BT-Drs. 16/10492) und in das Gesetzgebungsverfahren eingebracht. Der Entwurf sieht die Schaffung einer bundesweiten Zentraldatei vor, in der Einkommensdaten der über 30 Millionen abhängig Beschäftigten, Beamten, Richter und Soldaten gespeichert werden sollen. Dadurch werden massenhaft sensible personenbezogene Daten an einer Stelle vorgehalten. Die Nutzung dieser Daten ist zwar bisher auf den Fall beschränkt, dass soziale Leistungen der Bundesagentur für Arbeit sowie der Elterngeld- und Wohngeldstellen beantragt werden. Es ist aber schon jetzt absehbar, dass die Nutzung der Daten künftig auch auf andere Sozialleistungsbereiche ausgeweitet werden soll, nachdem der Gesetzentwurf bereits selbst auf weitere geplante Nutzungsmöglichkeiten hinweist. Eine solche Einkommensdatei, der erhebliche datenschutzrechtliche Bedeutung zukommt, darf nur dann eingerichtet werden, wenn die verfassungsrechtlichen Voraussetzungen, die Erforderlichkeit und Verhältnismäßigkeit sowie die technisch-organisatorischen Vorkehrungen zum Schutz der dort gespeicherten Daten vorliegen. Darauf hat die Konferenz der Datenschutzbeauftragten des Bundes und der Länder bereits wiederholt hingewiesen. Da der nun vorliegende Gesetzentwurf die bestehenden erheblichen Zweifel an der Verfassungsmäßigkeit des ELENA-Verfahrens nicht ausräumen konnte, hat vor allem auf Initiative Bayerns die 76. Datenschutzkonferenz am 06./07.11.2008 erneut und eindringlich auf die verfassungsrechtlichen und technisch-organisatorischen Mängel des Verfahrens aufmerksam gemacht und eine Nachbesserung des Gesetzentwurfs gefordert.

# 18 Verkehrswesen - Anbindung der Fahrerlaubnisbehörden an das Kraftfahrt-Bundesamt

Seit der Novellierung des Straßenverkehrsgesetzes (StVG) im Jahre 1998 befindet sich das Zentrale Fahrerlaubnisregister beim Kraftfahrt-Bundesamt im Aufbau. Die in den örtlichen Fahrerlaubnisregistern bei den Fahrerlaubnisbehörden dezentral gespeicherten Eintragungen über erteilte Fahrerlaubnisse sollen zukünftig ausschließlich im Zentralen Fahrerlaubnisregister elektronisch gespeichert werden. Nach § 65 Abs. 10 StVG darf ein örtliches Fahrerlaubnisregister u.a. nicht mehr geführt werden, sobald sein Datenbestand mit den in § 50 Abs. 1 StVG genannten Daten in das Zentrale Fahrerlaubnisregister übernommen worden ist und die Daten von der örtlichen Fahrerlaubnisbehörde im automatisierten Verfahren abgerufen werden können.

Aus der Schaffung des Zentralen Fahrerlaubnisregisters beim Kraftfahrt-Bundesamt, der ausschließlich zentralen elektronischen Speicherung der Fahrerlaubnisinhaberdaten und einer verändernden Zugriffsberechtigung aller Fahrerlaubnisbehörden auf die beim Kraftfahrt-Bundesamt gespeicherten Daten ergeben sich datenschutzrechtliche und technisch-organisatorische Anforderungen, die derzeit nicht ausreichend gesetzlich geregelt sind. So besteht z.B. ein Regelungsbedarf hinsichtlich

- der Anforderungen an den Online-Dialogbetrieb (lesender und schreibender Zugriff der Erlaubnisbehörden),
- der Beweissicherheit einzelner Verfahrensschritte auch über lange Zeit und
- der datenschutzrechtlichen Verantwortlichkeit.

Angesichts des Umfangs der personenbezogenen Daten, die zukünftig ausschließlich zentral und mit Schreibbefugnis für alle Fahrerlaubnisbehörden verarbeitet werden sollten, ist die Rechtsverbindlichkeit dieser Informationen sowohl für die Betroffenen als auch für die Behörden dauerhaft sicherzustellen.

Die Datenschutzbeauftragen des Bundes und der Länder beschäftigen sich seit geraumer Zeit in ihrem Arbeitskreis Verkehr mit der Konzeption der Online-Anbindung der Fahrerlaubnisbehörden an das Kraftfahrt-Bundesamt. Sie haben Vorschläge zur Anpassung der gesetzlichen Regelungen im Straßenverkehrsgesetz und in der Fahrerlaubnisverordnung an die tatsächlichen und zukünftig angestrebten Verhältnisse erarbeitet und diese Vorschläge dem Bundesministerium für Verkehr, Bau- und Stadtentwicklung sowie den zuständigen Landesministerien übermittelt.

# 19 Gewerbe und Handwerk

## 19.1 Bekanntgabe personenbezogener Daten von Bezirkskaminkehrermeistern im Internet

Eine Kaminkehrer-Innung hat sich an mich mit der Frage gewandt, welche Daten ihrer Mitglieder sie im Internet veröffentlichen darf. Es sei geplant, dass der Bürger nach Angabe seiner Adresse den Namen, die Anschrift und die Telekommunikationsdaten seines zuständigen Bezirkskaminkehrermeisters erhalte. Die Einarbeitung und Pflege der Daten würden von einem externen Softwareunternehmen vorgenommen. Ich habe der Kaminkehrer-Innung dazu Folgendes mitgeteilt:

Nach Art. 15 Abs. 1 Nrn. 1 und 2 BayDSG ist die Erhebung, Verarbeitung und Nutzung personenbezogener Daten nur zulässig, wenn entweder das Bayerische Datenschutzgesetz oder eine andere Rechtsvorschrift sie erlaubt oder anordnet oder der Betroffene eingewilligt hat. Die geplante Veröffentlichung im Internet ist eine Datenübermittlung an die Allgemeinheit. Mangels einer bereichsspezifischen Rechtsvorschrift kommt als Rechtsgrundlage der Datenübermittlung Art. 19 Abs. 1 Nr. 1 BayDSG in Betracht. Die Übermittlung personenbezogener Daten an nicht-öffentliche Stellen ist danach zulässig, wenn sie zur Erfüllung der in der Zuständigkeit der übermittelnden Stelle liegenden Aufgaben erforderlich ist und die Voraussetzungen vorliegen, die eine Nutzung nach Art. 17 Abs. 1 Nr. 2, Abs. 2 bis 4 BayDSG zulassen würden. Die Veröffentlichung der organisatorischen Grunddaten der zuständigen Bezirkskaminkehrermeister - hierzu zählen Name, Vorname, betriebliche Anschrift und betriebliche Telekommunikationsdaten (Telefon, Fax, E-Mail-Anschrift) - halte ich danach im Rahmen der Aufgabenerfüllung der Kaminkehrer-Innung für erforderlich. So muss insbesondere aus Gründen des Brandschutzes und der Feuerstättensicherheit jeder zuständige Bezirkskaminkehrermeister für die Bürger zu den üblichen Geschäftszeiten erreichbar sein. Diese Veröffentlichung liegt auch im Rahmen der Zweckbestimmung der Datenerhebung (Art. 17 Abs. 1 Nr. 2 BayDSG).

Eine Veröffentlichung darüber hinausgehender Daten der Bezirkskaminkehrermeister - wie z.B. private Anschrift und berufliche Zusatzqualifikationen - wäre allerdings nicht mehr als zur Aufgabenerfüllung i.S.d. Art. 19 Abs. 1 Nr. 1 BayDSG erforderlich anzusehen. Sie käme daher nur mit ausdrücklicher Einwilligung der Betroffenen in Betracht (Art. 15 Abs. 1 Nr. 2 BayDSG).

Die Einschaltung eines externen Softwareunternehmens zur Einarbeitung und Pflege der Daten ist im Rahmen einer Auftragsdatenverarbeitung nach Art. 6 BayDSG zulässig. Ein Mustervertrag zur Auftragsda-

tenverarbeitung ist unter der Rubrik „Technik/Orientierungshilfen/Mustervorlagen“ auf meiner Homepage unter www.datenschutz-bayern.de abrufbar.

### 19.2 Veröffentlichung von Insolvenzen im Mitteilungsblatt einer Industrie- und Handelskammer

Ein betrieblicher Datenschutzbeauftragter hat sich an mich mit der Bitte um Prüfung gewandt, ob die Veröffentlichung der Insolvenzdaten von Gewerbetreibenden, die natürliche Personen sind, im Mitteilungsblatt einer Industrie- und Handelskammer (IHK) datenschutzrechtlich zulässig ist.

Die von mir dazu befragte IHK teilte mit, dass den Industrie- und Handelskammern als Körperschaften des öffentlichen Rechts insolvenzrechtlich relevante Sachverhalte unmittelbar von den Insolvenzgerichten des Kammerbezirks auf der Basis der Anordnung über Mitteilungen in Zivilsachen übermittelt werden. Die in der IHK-Zeitschrift, dem offiziellen Mitteilungsblatt der IHK, veröffentlichten Insolvenzdaten würden, - nach einem entsprechenden Abgleich mit den amtlich übermittelten Daten - ausschließlich den aktuellen Ausgaben des Bundesanzeigers entnommen. Es würden nur Insolvenzdaten publiziert, die sich nach Sitz bzw. Wohnort dem Bezirk der Industrie- und Handelskammer zuordnen lassen.

Weiter teilte die IHK mit, dass der im Bundesanzeiger veröffentlichte Text im Regelfall aus Platzgründen gekürzt werde. Sofern der Inhalt der Mitteilungen der Insolvenzgerichte über den Veröffentlichungstext im Bundesanzeiger hinausgehe, werde dieser grundsätzlich nicht publiziert. Durch das sorgfältige Verfahren der IHK bei der Ermittlung der Daten werde ausgeschlossen, dass im Mitteilungsblatt der IHK Angaben gemacht werden, die über die im Bundesanzeiger veröffentlichten Insolvenzdaten hinaus gehen.

Diesen Sachverhalt habe ich datenschutzrechtlich wie folgt bewertet:

Die Veröffentlichung von Name, Vorname und Adresse des Insolvenzschuldners, das Datum der Insolvenzeröffnung sowie Name, Vorname und Ort des Insolvenzverwalters in der IHK-Zeitschrift stellen eine Datenübermittlung an nicht-öffentliche Stellen dar. Nach Art. 19 Abs. 1 Nr. 1 BayDSG ist die Datenübermittlung zulässig, wenn sie zur Erfüllung der Aufgaben der IHK erforderlich ist und die Voraussetzungen vorliegen, die eine Nutzung nach Art. 17 Abs. 1 Nr. 2, Abs. 2 bis 4 BayDSG zulassen würden.

Gemäß § 1 Abs. 1 IHK-Gesetz haben die Industrie- und Handelskammern u.a. die Aufgabe, das Gesamtinteresse der ihnen zugehörigen Gewerbetreibenden ihres Bezirks wahrzunehmen, für die Förderung der gewerblichen Wirtschaft zu wirken und dabei die wirtschaftlichen Interessen einzelner Gewerbezweige oder Betriebe abwägend und ausgleichend zu berücksichtigen. Hierzu gehört unter dem Aspekt des Gläubigerschutzes auch die Information der Kammermitglieder über Insolvenzen derzeitiger oder potentieller Geschäftspartner. Dass es zu den Aufgaben einer Industrie- und Handelskammer gehört, wirtschaftliche Nachteile von ihren Mitgliedern abzuwenden, die daraus entstehen, dass Schuldner ihren Zahlungsverpflichtungen nicht nachkommen, ergibt sich auch aus den §§ 915 Abs. 3 und 915 e der Zivilprozessordnung (ZPO). So erhalten die Industrie- und Handelskammern nicht nur Abdrucke von Schuldnerverzeichnissen, sondern sind auch gemäß § 915 e Abs. 2 Satz 1 ZPO dazu berechtigt, ihren Mitgliedern Auskünfte aus diesen Abdrucken zu erteilen.

Die Insolvenzdaten werden im vorliegenden Fall in der IHK-Zeitschrift, dem offiziellen Organ der Industrie- und Handelskammer, veröffentlicht. Bei der Kammerzeitschrift einer IHK handelt es sich um eine gegenüber der Masse der Medien herausgehobene Publikation. Sie ist das satzungsgemäße Verlautbarungsorgan der IHK als Körperschaft des öffentlichen Rechts. Die Kammerzeitschrift dient ausschließlich dazu, dass die IHK ihren gesetzlichen Auftrag erfüllt und geht auch nur dem begrenzten Kreis der Kammermitglieder zu. Die Veröffentlichung der Insolvenzen in der Kammerzeitschrift auf der Grundlage der Veröffentlichungen im Bundesanzeiger halte ich daher zur Aufgabenerfüllung der IHK für geeignet und angemessen und damit für erforderlich im Sinne des Art. 19 Abs. 1 Nr. 1 BayDSG. Da die in der IHK-Zeitschrift veröffentlichten Daten über die Insolvenzen ausschließlich dem Bundesanzeiger als eine allgemein zugängliche Quelle entnommen werden (können), ist auch die Vorschrift des Art. 17 Abs. 2 Nr. 8 1. Alternative BayDSG erfüllt. Nach dieser Vorschrift ist eine Datennutzung für andere Zwecke zulässig, wenn die Daten aus allgemein zugänglichen Quellen entnommen werden können. Im Ergebnis kann danach festgestellt werden, dass die Veröffentlichung von Insolvenzen im offiziellen Mitteilungsblatt einer Industrie- und Handelskammer aus datenschutzrechtlicher Sicht nicht zu beanstanden ist.

## 20 Landwirtschaft - Öffentlichkeitsarbeit in der Verwaltung für Ländliche Entwicklung

Im Rahmen der Öffentlichkeitsarbeit erstellen die Behörden der Verwaltung für Ländliche Entwicklung Broschüren über einzelne Verfahren der Flurneuordnung und Dorferneuerung. Diese werden an die jeweiligen Verfahrensteilnehmer, aber auch an (über-) regionale politische Mandatsträger (wie z.B. Gemeinderäte) und zudem über die Infostände der Gemeinden an alle interessierten Bürger verteilt.

In einer mir zur datenschutzrechtlichen Überprüfung vorgelegten Broschüre wurden die Eigentumsverhältnisse vor und nach der Flurneuordnung graphisch dargestellt. Auch wenn hierbei weder die Eigentümer noch die Nummern der in den abgebildeten Karten dargestellten Flurstücke genannt wurden, so wurden doch die verschiedenen, einem bestimmten landwirtschaftlichen Betrieb zugehörigen Flurstücke jeweils mit der gleichen Farbe markiert.

Die farbliche Markierung der Zugehörigkeit verschiedener Flurstücke zu einem bestimmten landwirtschaftlichen Betrieb stellt für die ortsansässigen Hauptadressaten der Broschüre, denen die Inhaberschaft zumindest eines der dargestellten landwirtschaftlichen Betriebe - gleich ob vor oder nach der Bodenordnung - bekannt ist, ein personenbeziehbares Datum im Sinne des Art. 4 Abs. 1 BayDSG dar. Aufgrund seines Zusatzwissens und der Art der graphischen Darstellung ist dieser Leserkreis unschwer in der Lage, auf die Zugehörigkeit bestimmter, ihm bekannter Flurstücke zu bestimmten landwirtschaftlichen Betrieben und damit mittelbar auf die Eigentumsverhältnisse an diesen Flurstücken zu schließen. Darüber hinaus ist es den ortskundigen Lesern der Broschüre möglich, aufgrund ihrer Kenntnis der wertbestimmenden Faktoren des in der Broschüre dargestellten Grundeigentums eine personenbezogene Zuordnung von Vermögensverhältnissen und Betriebsgrößen vorzunehmen.

Damit stellt die durch die Broschüre erfolgende Bekanntgabe von personenbeziehbaren Daten an private Dritte eine Übermittlung personenbezogener Daten an nicht-öffentliche Stellen dar, die mangels Einwilligung der betroffenen Betriebsinhaber einer Rechtsgrundlage bedarf (vgl. Art. 15 Abs. 1 BayDSG).

Dabei ist zunächst festzuhalten, dass das Flurbereinigungsrecht hierfür keine spezialgesetzliche Rechtsgrundlage zur Verfügung stellt.

Aber auch Art. 19 Abs. 1 Nr. 1 BayDSG rechtfertigt die Datenübermittlung nicht. Diese Vorschrift setzt u.a. voraus, dass die Übermittlung personenbezogener Daten an nicht-öffentliche Stellen zur Erfüllung der in der Zuständigkeit der übermittelnden Stelle liegenden Aufgaben erforderlich ist. Allgemeine Öffentlichkeitsarbeit ist zwar eine Aufgabe der öffentlichen Stellen; jedoch ist nicht erkennbar, warum zur Erfüllung dieser Aufgabe die - wenn auch nur mittelbare - Angabe von Eigentums- und Vermögensverhältnissen erforderlich sein soll. Für die ordnungsgemäße Aufgabenbewältigung reicht vielmehr die bloße Abbildung eines Flurkartenausschnittes aus. Der zusätzlichen Mitteilung der Betriebszugehörigkeit bestimmter Flurstücke durch farbliche Hervorhebung bedarf es nicht.

Schließlich sind auch die Voraussetzungen des Art. 19 Abs. 1 Nr. 2 BayDSG nicht erfüllt. Denn es fehlt an dem von dieser eng auszulegenden Vorschrift geforderten berechtigten Interesse der nicht-öffentlichen Stelle an der Kenntnis der zu übermittelnden Daten. Als berechtigtes Interesse kommt jedes nach vernünftigen Erwägungen unter Berücksichtigung der Besonderheiten des Einzelfalles anzuerkennendes, der Rechtsordnung nicht widersprechendes Interesse in Betracht. Dazu rechnet zwar auch das Interesse an der Schaffung eines vernünftigerweise zuzubilligenden Informationsstandes, etwa das Interesse, sich über die Arbeit der Verwaltung für Ländliche Entwicklung zu unterrichten. Jedoch ist hierzu die Mitteilung der Eigentumsverhältnisse an bestimmten Flurstücken offensichtlich nicht erforderlich. Darüber hinaus haben die betroffenen Grundstückseigentümer ein schutzwürdiges Interesse an dem Ausschluss der Übermittlung der Eigentumsverhältnisse an sämtliche mit Ortskenntnis ausgestatteten Leser der Broschüre.

Ich habe daher die Verwaltung für Ländliche Entwicklung gebeten, die weitere Verwendung der mir vorgelegten Broschüre umgehend zu unterbinden, zumindest aber die farblichen Hervorhebungen unkenntlich zu machen. Bei Neuauflagen und Neuveröffentlichungen vergleichbarer Broschüren ist darauf zu achten, dass keinesfalls Eigentumsverhältnisse an Flurstücken - auch nicht mittelbar und nur für ortskundige Leser - dargestellt werden, da dies für die ordnungsgemäße Erfüllung der Aufgabe „Öffentlichkeitsarbeit der Verwaltung für Ländliche Entwicklung“ nicht erforderlich und damit auch datenschutzrechtlich unzulässig ist.

# 21 Personalwesen

## 21.1 Neuordnung des Bayerischen Beihilferechts

Das Krankenfürsorgesystem der Beihilfe für Beamte und Richter war in Bayern bislang durch eine Verweisung auf die als Verwaltungsvorschriften ergangenen Beihilfevorschriften des Bundes geregelt. Im Jahr 2004 hatte das Bundesverwaltungsgericht allerdings festgestellt, dass die ausschließliche Normierung der Beihilfe in bloßen Verwaltungsvorschriften nicht den verfassungsrechtlichen Anforderungen des Gesetzesvorbehalts genügt (Urteil vom 17.06.2004, Az. 2 C 50/02) und auch dem Freistaat Bayern aufgegeben, seine Regelungen über die Fürsorge in Krankheits-, Pflege- und Geburtsfällen den grundgesetzlichen Erfordernissen anzupassen (Urteil vom 28.10.2004, Az. 2 C 32/03). Auch inhaltlich hatte sich die Verweisung auf die Bundesvorschriften nach Auffassung des innerhalb der Staatsregierung federführenden Staatsministeriums der Finanzen als problematisch erwiesen, insbesondere da die Bundesvorschriften zunehmend Regelungen aus dem Bereich der gesetzlichen Krankenversicherungen übernommen hatten, ohne der Eigenständigkeit des Krankenfürsorgesystems der Beihilfe Rechnung zu tragen.

Vor diesem Hintergrund hat der Landtag im Herbst 2006 eine Neuordnung des Bayerischen Beihilferechts beschlossen. Der ab dem 01.01.2007 geltende, in das Bayerische Beamtengesetz neu eingefügte Art. 86 a BayBG ersetzt nun die Verweisung auf das Beihilferecht des Bundes durch eine eigenständige bayerische Regelung der grundlegenden Fragen der Beihilfe. Zur näheren Ausgestaltung dieser Regelung enthält Art. 86 a Abs. 5 BayBG eine Rechtsverordnungsermächtigung, von der das Staatsministerium der Finanzen durch Erlass der Verordnung über die Beihilfefähigkeit von Aufwendungen in Krankheits-, Geburts-, Pflege- und sonstigen Fällen (Bayerische Beihilfeverordnung - BayBhV) vom 02.01.2007 Gebrauch gemacht hat. Diese Bestimmungen werden ergänzt durch die Verwaltungsvorschriften zur Bayerischen Beihilfeverordnung (VV-BayBhV), die das Staatsministerium der Finanzen am 26.07.2007 bekannt gemacht hat.

Die im Berichtszeitraum zum Abschluss gekommene Neuordnung des Bayerischen Beihilferechts habe ich im Rahmen meiner Beteiligung im Normsetzungsverfahren umfassend und eingehend begleitet. Im Einzelnen ergaben sich insbesondere folgende Problemschwerpunkte:

### 21.1.1 Vernichtung nicht zurückgegebener und Löschung elektronisch gespeicherter Belege

Der ursprüngliche Gesetzentwurf des Staatsministeriums der Finanzen enthielt keine Regelung zum Umgang mit nicht zurückgegebenen Belegen. Überdies war keine Höchstspeicherungsdauer mit anschließender Löschungsverpflichtung für elektronisch gespeicherte Belege vorgesehen. Ich habe dies kritisiert, woraufhin das Staatsministerium der Finanzen auf der Grundlage meiner Vorschläge den Gesetzentwurf entsprechend ergänzt hat.

Nunmehr ist in Art. 100 g Abs. 2 Satz 2 BayBG vorgeschrieben, dass nicht zurückgegebene Unterlagen, aus denen die Art der Erkrankung ersichtlich ist, unverzüglich zu vernichten sind, wenn sie für den Zweck, zu dem sie vorgelegt worden sind, nicht mehr benötigt werden. Darüber hinaus bestimmt nun Art. 100 g Abs. 5 Satz 3 BayBG, dass elektronisch gespeicherte Beihilfebelege spätestens ein Jahr nach Ablauf des Jahres, in dem die Unterlagen elektronisch erfasst wurden, zu löschen sind, sofern sie nicht darüber hinaus für die Bearbeitung oder aufgrund sonstiger gesetzlicher Vorschriften benötigt werden.

### 21.1.2 Überprüfung der Notwendigkeit und Angemessenheit von Aufwendungen durch Dritte

Das bisherige Beihilferecht hatte in § 5 Abs. 1 Satz 4 der Allgemeinen Verwaltungsvorschrift über die Gewährung von Beihilfen in Krankheits-, Pflege- und Geburtsfällen (Beihilfevorschriften - BhV a.F.) vorgesehen, dass im Rahmen der Entscheidung der Festsetzungsstelle über die Notwendigkeit und die Angemessenheit von Aufwendungen Gutachten des Amts- oder Vertrauensarztes(-zahnarztes) eingeholt werden können. Nach Art. 86 a Abs. 5 Satz 2 Nr. 3 lit. c) Halbsatz 1 BayBG und § 48 Abs. 8 Halbsatz 1 BayBhV kann die Festsetzungsstelle nun zur Überprüfung der Notwendigkeit und Angemessenheit einzelner geltend gemachter Aufwendungen Gutachter, Beratungsärzte und sonstige geeignete Stellen unter Übermittlung der erforderlichen Daten beteiligen, wobei personenbezogene Daten nur mit Einwilligung des Beihilfeberechtigten übermittelt werden dürfen. Ergänzend hierzu regeln die VV zu § 48 Abs. 8 BayBhV in Nr. 1 Satz 3, dass eine Beihilfe nicht gewährt wird, wenn das Einverständnis verweigert wird und die Berechtigung des Anspruchs nicht anderweitig nachgewiesen werden kann.

Die mit der Neuregelung verbundene Ausweitung der Beteiligung von Dritten auf „sonstige geeignete Stellen“ halte ich aus datenschutzrechtlicher Sicht für problematisch. Zur Begründung dieser Erweiterung wurde angeführt, dass „neben der auch weiterhin möglichen Beteiligung von Amts- und Vertrauensärzten … die Beteiligung von Dritten außerhalb der Verwaltung u.a. eine Bewertung des jeweiligen Einzelfalls nach dem aktuellen Stand der Wissenschaft bzw. eine fachkompetente Überprüfung komplexer Abrechnungsgegebenheiten“ gewährleistet. Diese Erwägungen kann ich nicht nachvollziehen, insbesondere die letztlich darin zum Ausdruck kommenden Vorbehalte gegenüber der Fachkompetenz der Amts- und Vertrauensärzte einerseits und der Beihilfesachbearbeiter andererseits. Hinzu kommt, dass die Übermittlung von sensiblen Gesundheitsdaten an behördenfremde, nichtärztliche Dritte datenschutzrechtlich als besonders kritisch einzustufen ist. Meiner dringenden, mehrfach vorgebrachten Bitte, die vorgesehene Möglichkeit der Beteiligung von nichtärztlichen Dritten deshalb wieder zu streichen, wurde aber leider nicht entsprochen.

Erreichen konnte ich hingegen, dass nach Art. 86 a Abs. 5 Satz 2 Nr. 3 lit. c) Halbsatz 1 BayBG und § 48 Abs. 8 Halbsatz 1 BayBhV entsprechend der bislang geltenden Regelung in Nr. 9 zu Abs. 1 zu § 5 der Vollzugsbestimmungen zur Allgemeinen Verwaltungsvorschrift über die Gewährung von Beihilfen in

Krankheits-, Pflege- und Geburtsfällen (VB-BhV) die Übermittlung der erforderlichen personenbezogenen Daten nur mit Einwilligung des Beihilfeberechtigten zulässig ist; der ursprüngliche Gesetzentwurf des Staatsministeriums der Finanzen enthielt noch keine derartige Bestimmung. Darauf hinzuweisen ist auch, dass nach Art. 86 a Abs. 5 Satz 2 Nr. 3 lit. c) Halbsatz 2 BayBG und § 48 Abs. 8 Halbsatz 2 BayBhV die Zuerkennung der Eignung der Dritten voraussetzt, dass die mit der Bewertung betrauten Personen nach dem Verpflichtungsgesetz zur Wahrung der Daten verpflichtet werden.

Zur Regelung in Nr. 1 Satz 3 VV zu § 48 Abs. 8 BayBhV, wonach eine Beihilfe nicht gewährt wird, wenn das Einverständnis verweigert wird und die Berechtigung des Anspruchs nicht anderweitig nachgewiesen werden kann, habe ich das Staatsministerium der Finanzen auf Folgendes hingewiesen: Eine Fallgestaltung, in der der Beihilfeberechtigte seine Einwilligung in die Übermittlung personenbezogener Daten verweigert und die Berechtigung des Anspruchs nicht anderweitig nachgewiesen werden kann, ist kaum denkbar. Denn auch wenn dieses Einverständnis nicht erteilt wird, bleibt als sonstige Möglichkeit der Nachweisführung in aller Regel die Übermittlung pseudonymisierter Daten. Meiner Anregung, in Nr. 1 Satz 3 VV zu § 48 Abs. 8 BayBhV hierauf klarstellend hinzuweisen, ist das Finanzministerium leider nicht gefolgt. Dies ändert aber nichts daran, dass die Verweigerung der Einwilligung eine Ablehnung des Beihilfeantrags nicht rechtfertigen kann, soweit der Nachweis mittels Übermittlung pseudonymisierter Daten geführt werden kann.

### 21.1.3 Übertragung der Beihilfesachbearbeitung auf Dritte

Nach Art. 86 a Abs. 4 Satz 5 Halbsatz 1 BayBG können die Gemeinden, Gemeindeverbände und die sonstigen der Aufsicht des Staates unterstehenden Körperschaften, Anstalten und Stiftungen des öffentlichen Rechts zur Erfüllung ihrer Beihilfe-Verpflichtungen eine Versicherung abschließen oder sich der Dienstleistungen von Versicherungsunternehmen oder sonstiger geeigneter Stellen bedienen und hierzu die erforderlichen Daten übermitteln. In diesem Zusammenhang ordnet Art. 86 a Abs. 4 Satz 7 BayBG die entsprechende Geltung der Art. 100 a Abs. 1 Satz 1 Halbsatz 2, Art. 100 b Satz 4, Art. 100 d und Art. 100 g BayBG an.

Im Rahmen meiner Beteiligung habe ich das Staatsministerium der Finanzen daran erinnert, dass ich mich bereits gegen die mit Wirkung vom 01.01.2001 durch Art. 12 Abs. 3 Satz 2 Bayerisches Besoldungsgesetz (BayBesG) a.F. geschaffene Erweiterung der Übertragungsmöglichkeit der Beihilfesachbearbeitung auf „sonstige geeignete Stellen“ ausgesprochen hatte (vgl. hierzu Nr. 12.1.1 meines 19. Tätigkeitsberichts 2000). Denn aus datenschutzrechtlicher Sicht ist zu befürchten, dass bei einer solchen Übertragung die Grundsätze des geltenden Personalaktenrechts - also bereichsspezifischer Datenschutzvorschriften mit einem anerkannt hohen Schutzniveau - letztlich (faktisch) „ausgehebelt“ werden (vgl. insoweit auch das Urteil des Oberverwaltungsgerichts Koblenz vom 19.04.2002, Az. 2 A 10209/02). Es liegt auf der Hand, dass der Beihilfeträger bei einer Weitergabe von Beihilfedaten an Behördenexterne das Schicksal des Beihilfedatenbestandes nicht mehr vollumfänglich kontrollieren kann. Dazu kommt noch, dass den betroffenen Beihilfeberechtigten jegliche Wahlmöglichkeit fehlt. Vor dem Hintergrund dieser schwerwiegenden datenschutzrechtlichen Problematik einerseits und der meinem Eindruck nach geringen praktischen Relevanz andererseits habe ich gefordert, die Erweiterung der Übertragungsmöglichkeit auf „sonstige geeignete Stellen“ anlässlich der Neuordnung des Beihilferechts wieder zu streichen. Wie die in Kraft getretene Fassung des Art. 86 a Abs. 4 Satz 5 Halbsatz 1 BayBG zeigt, blieb meine Forderung jedoch leider unberücksichtigt. Zumindest setzt aber gem. Art. 86 a Abs. 4 Satz 5 Halbsatz 2 BayBG die Zuerkennung der Eignung voraus, dass die mit der Beihilfebearbeitung betrauten Personen nach dem Verpflichtungsgesetz zur Wahrung der Daten verpflichtet werden. Zudem darf nach der strikten Zweckbindungsregelung des Art. 86 a Abs. 4 Satz 6 BayBG die mit der Beihilfebearbeitung beauftragte Stelle die Daten, die ihr im Rahmen der Beihilfebearbeitung bekannt werden, nur für diesen Zweck bearbeiten und nutzen.

Bereits im Zusammenhang mit der Einfügung des Art. 12 Abs. 3 Satz 4 BayBesG a.F. hatte ich gefordert, dass die personaldatenschutzrechtlichen Vorschriften der Art. 100 ff. BayBG auch im Fall der Übertragung der Beihilfesachbearbeitung auf Dritte wirkungsgleich gelten müssen. Zu meinem Bedauern war dieser Forderung damals - abgesehen von der Anwendbarerklärung des Art. 100 b Satz 4 BayBG (Verwendung und Weitergabe des Beihilfeakts für andere als für Beihilfezwecke nur in bestimmten Fällen) - im Gesetz nicht Rechnung getragen worden. Anlässlich der anstehenden Neuordnung des Bayerischen Beihilferechts habe ich erneut auf das datenschutzrechtliche Erfordernis hingewiesen, dass auch bei Durchführung der Beihilfesachbearbeitung durch Dritte jedenfalls hinsichtlich des Einsichtsrechts der Betroffenen in ihren vollständigen Personalakt, der Vertraulichkeit des Beihilfeakts, der Aussonderung und Löschung der Unterlagen über Beihilfen sowie der unverzüglichen Rückgabe der Unterlagen, aus denen die Art der Erkrankung ersichtlich ist, auch die Art. 100 d, Art. 100 a Abs. 1 Satz 1 Halbsatz 2 sowie Art. 100 g BayBG Anwendung finden müssen. Ich habe ferner daran erinnert, dass auch das Staatsministerium der Finanzen zur bisherigen Regelung in Art. 12 Abs. 3 Sätze 2 bis 4 BayBesG a.F. die Auffassung vertreten hatte, dass die Möglichkeit der

Auslagerung der Beihilfesachbearbeitung an der rechtlichen Zuständigkeit und Verantwortung des (meist kommunalen) Dienstherrn nichts geändert hat. So war nach Meinung des Staatsministeriums der Finanzen auch bei der „Dienstleistungsvariante“ Ansprechpartner in erster Linie der Dienstherr geblieben; dies galt auch bezüglich der Rechte, die dem Beihilfeberechtigten in personalaktenrechtlicher Hinsicht zustehen. Daher habe ich angeregt, im Zuge der Neuordnung des Bayerischen Beihilferechts die Rechte des Beihilfeberechtigten im Gesetz selbst klarzustellen. Erfreulicherweise wurde meiner Anregung durch die Regelung des Art. 86 a Abs. 4 Satz 7 BayBG entsprochen.

### 21.1.4 Verwendung einer elektronischen Gesundheitskarte bei der Beihilfe

Nach Art. 86 a Abs. 5 Satz 2 Nr. 3 lit. b) BayBG kann durch Verordnung des Staatsministeriums der Finanzen hinsichtlich des Verfahrens der Beihilfengewährung die Verwendung einer elektronischen Gesundheitskarte unter sinngemäßer Anwendung des § 291 a SGB V vorgeschrieben werden; hierbei ist der Zugriff der Beihilfestellen auf Daten über die in Anspruch genommenen Leistungen und deren Kosten zu beschränken. Ausweislich der Gesetzesbegründung soll mit dieser Regelung u.a. ein künftiger Einsatz einer elektronischen Gesundheitskarte im Zusammenhang mit dem sog. elektronischen Rezept ermöglicht werden. Die Vorlage von Rezepten in der bisherigen Form soll entbehrlich gemacht werden. Hiervon sei eine Vereinfachung der Beihilfefestsetzung zu erwarten.

Ich habe das Staatsministerium der Finanzen darauf aufmerksam gemacht, dass die elektronische Gesundheitskarte nach § 291 a SGB V für dieses Gesetzesziel ungeeignet ist, da dafür den Beihilfesachbearbeitern Zugang zu den auf oder mit der elektronischen Gesundheitskarte gespeicherten Daten gegeben werden müsste. Dies ist jedoch nach der gesetzlichen Konzeption des § 291 a SGB V nicht möglich. Das sog. elektronische Rezept ist in § 291 a Abs. 2 Satz 1 Nr. 1 SGB V normiert. Nach dieser Vorschrift muss die elektronische Gesundheitskarte geeignet sein, Angaben für die Übermittlung ärztlicher Verordnungen in elektronischer und maschinell verwertbarer Form aufzunehmen. Dabei ist jedoch zu beachten, dass der Kreis der Zugriffsberechtigten in § 291 a Abs. 4 Satz 1 Nr. 1 SGB V auf Ärzte, Zahnärzte, Apotheker, Apothekerassistenten, Pharmazieingenieure, berufsmäßige Gehilfen und sonstige Erbringer ärztlich verordneter Leistungen beschränkt wird. Mitarbeiter der gesetzlichen Krankenkassen - geschweige denn Mitarbeiter der Beihilfestellen - gehören nicht zum zugriffsberechtigten Personenkreis. Verfahrensrechtlich abgesichert wird diese Zugriffsbeschränkung durch § 291 a Abs. 5 Satz 3 SGB V, wonach der Zugriff auf Daten nach § 291 a Abs. 2 Satz 1 Nr. 1 SGB V nur in Verbindung mit einem elektronischen Heilberufeausweis bzw. einem entsprechenden Berufsausweis erfolgen darf, der jeweils über eine Möglichkeit zur sicheren Authentifizierung und eine qualifizierte elektronische Signatur verfügt.

Da folglich eine Vorschrift, eine elektronische Gesundheitskarte unter sinngemäßer Anwendung des § 291 a SGB V für die Beihilfesachbearbeitung zu verwenden, keinen Sinn macht und darüber hinaus eine landesrechtliche Erweiterung des bundesrechtlich abschließend festgelegten Kreises der zugriffsberechtigten Personen - zudem noch in einer Rechtsverordnung - verfassungsrechtlich äußerst bedenklich wäre, habe ich die vollständige Streichung des Art. 86 a Abs. 5 Satz 2 Nr. 3 lit. b) BayBG gefordert. Dies war leider erfolglos.

Festzuhalten ist aber, dass das Staatsministerium der Finanzen bisher - aus gutem Grund - insoweit von der Rechtsverordnungsermächtigung noch keinen Gebrauch gemacht hat; so enthält die BayBhV keine Regelungen über die Verwendung einer elektronischen Gesundheitskarte bei der Beihilfe.

### 21.1.5 Vertrauensärztliches Gutachten bei psychotherapeutischen Leistungen

Gemäß § 9 Abs. 2 Satz 1 Nr. 3 BayBhV 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 der Stellungnahme eines vertrauensärztlichen Gutachtens zur Notwendigkeit und zu Art und Umfang der Behandlung anerkannt hat. Entsprechend sehen auch § 11 Abs. 7 Satz 8 BayBhV sowie § 12 Abs. 2 Satz 3 BayBhV für die dort geregelten besonderen Fälle psychotherapeutischer Leistungen eine Stellungnahme durch ein vertrauensärztliches Gutachten vor.

Nach der bisherigen Praxis wurden im Rahmen des Voranerkennungsverfahrens gemäß Nr. 5 sowie Anhang 5 der VB-BhV zu § 6 BhV a.F. dem mit der Fertigung dieser Stellungnahme betrauten Gutachter in dem vom Therapeuten zu erstellenden „Bericht an den Gutachter zum Antrag auf Anerkennung der Beihilfefähigkeit für Psychotherapie“ neben anderen personenbezogenen Daten auch Name und Vorname des Patienten übermittelt. Im Gegensatz dazu erfahren die Gutachter im Bereich der gesetzlichen Krankenkassen die Identität des Patienten nicht. So enthält das bundeseinheitliche, vom Therapeuten hier zu verwendende Formblatt „Bericht an den Gutachter zum Antrag des Versicherten auf tiefenpsychologisch fundierte oder analytische Psychotherapie bei Erwachsenen“ nicht den Namen des Versicherten. Vielmehr wird eine Chiffre übermittelt, die sich aus dem Anfangsbuchstaben des Familiennamens und

dem sechsstelligen Geburtsdatum zusammensetzt. Eine ähnliche Verfahrensweise gilt für die Beihilfeverwaltung der Freien und Hansestadt Hamburg.

Allein die letztgenannten Verfahren halte ich für datenschutzkonform. Da der vom Therapeuten zu fertigende Bericht einerseits weitgehende, insbesondere intime Angaben über Leben und Persönlichkeit des Patienten enthält, der Gutachter aber andererseits auf das Wissen um die Identität des Patienten - also den Namen - zur Erstellung seines Gutachtens nicht angewiesen ist, sind die Übermittlungen von Namen und Vornamen des Patienten an den Gutachter zu dessen Aufgabenerfüllung nicht erforderlich und damit datenschutzrechtlich unzulässig. Die Vorgehensweise der gesetzlichen Krankenkassen und der Beihilfeverwaltung in Hamburg gewährleistet nicht nur den Schutz des Patienten und seiner hier in erhöhtem Maße sensiblen Daten; sie ist auch mit keinem besonderen Verwaltungsaufwand verbunden. Nach Mitteilung des Hamburgischen Datenschutzbeauftragten hat sich das Verfahren nach Auskunft des in Hamburg für die Beihilfefestsetzung zuständigen Zentrums für Personaldienste auch in der Praxis bewährt.

Nachdem diese Problematik - wie zahlreiche Eingaben (auch aus der Ärzteschaft!) bei mir zeigen - immer noch virulent ist, habe ich das Staatsministerium der Finanzen zunächst darum gebeten, in Anlehnung an das Verfahren der gesetzlichen Krankenkassen und der Beihilfeverwaltung in Hamburg eine Pseudonymisierung der an den Gutachter übermittelten Daten in den §§ 9 Abs. 2 Satz 1 Nr. 3, 11 Abs. 7 Satz 8 und 12 Abs. 2 Satz 3 BayBhV vorzuschreiben. Wie die in Kraft getretene Fassung der BayBhV zeigt, ist das Finanzministerium dieser Bitte nicht nachgekommen. Daraufhin habe ich das Finanzministerium nachdrücklich darum ersucht, nun zumindest in den VV-BayBhV die Pseudonymisierung der Daten vorzusehen. Um dem Staatsministerium der Finanzen die Arbeit zu erleichtern, habe ich die Formblätter der Beihilfeverwaltung der Freien und Hansestadt Hamburg zum Psychotherapie-Begutachtungsverfahren vorgelegt. Auf dieser Basis habe ich sogar dem Finanzministerium in allen Einzelheiten dargelegt, wie die einschlägigen bayerischen Formblätter und der Text der VV-BayBhV datenschutzgerecht umzuformulieren wären.

Zu meinem großen Bedauern hat es das Staatsministerium der Finanzen jedoch auch abgelehnt, durch Regelungen in den VV-BayBhV eine pseudonymisierte Durchführung des Begutachtungsverfahrens sicherzustellen. Zur Begründung hat es ausgeführt, die Pseudonymisierung würde den erforderlichen Bewertungs- und Entscheidungsgang in zeitlicher Hinsicht verzögern, wenn nicht gar unmöglich machen. Bei einer Pseudonymisierung wäre insbesondere die eindeutige Zuordnung eines eingehenden Gutachtens zu einem bestimmten Beihilfeanspruch nicht möglich, da bei berücksichtigungsfähigen Angehörigen die Geburtsdaten von Patient und Beihilfeberechtigtem nicht identisch seien. Diese Argumentation kann ich nicht nachvollziehen: Warum sollte im Bereich der gesetzlichen Krankenversicherung (Familienversicherung!) und der Beihilfeverwaltung in Hamburg ein Verfahren mit pseudonymisierten Daten unproblematisch möglich sein, nicht hingegen im Bereich der bayerischen Beihilfeverwaltung? Weiter hat das Finanzministerium vorgetragen, dass die einzigen am Verfahren beteiligten Personen, die bei einer Pseudonymisierung vom Namen des Patienten keine Kenntnis erlangen würden, die ärztlichen Gutachter wären. Neben dem behandelnden sei aber auch der begutachtende Arzt/Psychotherapeut bereits aufgrund der strafbewehrten ärztlichen Schweigepflicht (§ 203 StGB) zur Geheimhaltung der Patientendaten verpflichtet. Im Übrigen erfolge die Übermittlung der personenbezogenen Daten nur bei Abgabe einer Erklärung über die Entbindung von der ärztlichen Schweigepflicht. Hierzu ist anzumerken, dass es bei dem pseudonymisierten Verfahren gerade darum geht, dass der ärztliche Gutachter die Identität des Patienten nicht erfährt, damit er die im Bericht des Therapeuten enthaltenen intimen Angaben über Leben und Persönlichkeit keiner bestimmten Person zuordnen kann. Die Problematik wird nur unwesentlich dadurch entschärft, dass sowohl Therapeut als auch Gutachter - worauf das Finanzministerium zunächst aufmerksam macht - der ärztlichen Schweigepflicht unterliegen. Denn auch innerhalb des ärztlichen Bereichs dürfen medizinische Daten nicht ohne Weiteres weitergegeben werden; vielmehr gilt die ärztliche Schweigepflicht auch gegenüber anderen Ärzten. Dementsprechend darf auch nicht davon ausgegangen werden, dass sich ein Patient, der seinem Therapeuten intime Details über sein Leben und seine Persönlichkeit offenbart, quasi automatisch damit einverstanden erklärt, dass dieser seine personenbezogenen Daten an einen anderen, ihm gänzlich unbekannten Arzt weitergibt. Schließlich wird die Problematik nicht dadurch vollständig gelöst, dass vorliegend der Patient - worauf das Finanzministerium zuletzt hinweist - seinen Therapeuten von der ärztlichen Schweigepflicht zu entbinden hat. Da die - zumeist sehr kostenintensiven - Aufwendungen für psychotherapeutische Leistungen nur bei (erfolgreicher) Durchführung des Begutachtungsverfahrens beihilfefähig sind, ist die Freiwilligkeit einer solchen Einwilligung in die Übermittlung der Daten an den Gutachter als problematisch anzusehen.

Im Ergebnis bleibe ich deshalb bei der Auffassung, dass nur eine Verfahrensweise mit pseudonymisierten Daten wie im Bereich der gesetzlichen Krankenversicherung und der Beihilfeverwaltung der Freien und Hansestadt Hamburg dem Grundrecht auf informationelle Selbstbestimmung der Patienten gerecht wird.

### 21.1.6 Eigenes Beihilfeantragsrecht für berücksichtigungsfähige Angehörige

Erfahrungen aus meiner datenschutzrechtlichen Beratungstätigkeit zeigen bis in die jüngste Zeit, dass das Fehlen eines eigenen Beihilfeantragsrechts für berücksichtigungsfähige Angehörige vor allem bei innerfamiliären Konfliktsituationen - zwischen den Ehegatten untereinander, aber auch zwischen dem Beihilfeberechtigten und seinen Kindern - zu datenschutzrechtlichen Problemen führen kann.

Erfreulicherweise hatte das Staatsministerium der Finanzen diese Problematik im Grundsatz bereits in der Vergangenheit erkannt. So konnte nach Abschnitt F Nr. 2 der Bekanntmachung des Bayerischen Staatsministeriums der Finanzen vom 13.12.1993 bei getrennt lebenden Ehegatten ausnahmsweise der berücksichtigungsfähige Ehegatte - nach Absprache unter den Beteiligten und im Benehmen mit der Festsetzungsstelle des Beihilfeberechtigten - die Belege mit der ausgefüllten Zusammenstellung der Aufwendungen unmittelbar der Festsetzungsstelle zuleiten. Der Beihilfeberechtigte hatte bei Stellung des Beihilfeantrages hierauf in geeigneter Weise Bezug zu nehmen. Die Belege mussten dann dem Ehegatten zurückgegeben werden. In Abschnitt D der Bekanntmachung des Bayerischen Staatsministeriums der Finanzen vom 23.07.1996 fand sich eine entsprechende Regelung zum Antragsverfahren hinsichtlich volljähriger berücksichtigungsfähiger Kinder, die nicht mehr im Haushalt der Eltern wohnen.

Allerdings eröffnete dieses umständliche Verfahren die Gefahr von Unklarheiten bei den Betroffenen und Fehlerquellen bei den Beihilfestellen. Ich habe deshalb das Staatsministerium der Finanzen gebeten, anlässlich der Neuordnung des Bayerischen Beihilferechts ein eigenes Beihilfeantragsrecht für getrennt lebende berücksichtigungsfähige Ehegatten und nicht im Haushalt des Beihilfeberechtigten lebende, volljährige berücksichtigungsfähige Kinder zu schaffen. Meiner Meinung nach kann auf diese Weise nicht nur dem Bestreben der Staatsregierung nach Verwaltungsvereinfachung, sondern auch datenschutzrechtlichen Belangen unschwer Rechnung getragen werden. So ist beispielsweise auch in § 5 der Landesverordnung über die Gewährung von Beihilfen an Beamtinnen und Beamte in Schleswig-Holstein ein eigenes Beihilfeantragsrecht für Angehörige verankert.

Auch dieser Anregung wollte das Staatsministerium der Finanzen nicht entsprechen. Nach der in Kraft getretenen Fassung des § 48 Abs. 1 Satz 1 BayBhV müssen Beihilfen vom Beihilfeberechtigten schriftlich beantragt werden. Ein eigenes Beihilfeantragsrecht für berücksichtigungsfähige Angehörige lässt sich dieser Vorschrift nicht entnehmen (vgl. auch Nr. 4 Satz 1 der VV zu § 48 Abs. 1 BayBhV: „Antragsberechtigt ist nur der Beihilfeberechtigte selbst“.).

Zumindest aber sieht die VV zu § 48 Abs. 1 BayBhV in Nr. 4 Satz 2 nunmehr ergänzend vor, dass bei getrennt lebenden Ehegatten ausnahmsweise der berücksichtigungsfähige Ehegatte - nach Absprache unter den Beteiligten und im Benehmen mit der Festsetzungsstelle des Beihilfeberechtigten - die ihn betreffenden Belege ggf. mit der ausgefüllten Zusammenstellung der Aufwendungen unmittelbar der Festsetzungsstelle zuleiten kann. Auf meine ausdrückliche Forderung hin hat das Staatsministerium der Finanzen in Nr. 4 Satz 3 der VV zu § 48 Abs. 1 BayBhV zudem angeordnet, dass Entsprechendes für berücksichtigungsfähige, volljährige Kinder, die nicht im Haushalt des Beihilfeberechtigten wohnen, gilt. In diesen Fällen hat der Beihilfeberechtigte bei der Stellung seines Beihilfeantrages hierauf in geeigneter Weise Bezug zu nehmen (Nr. 4 Satz 4 der VV zu § 48 Abs. 1 BayBhV). Damit sind im Ergebnis zumindest die schon bislang geltenden Regelungen in das neue Bayerische Beihilferecht übernommen worden.

### 21.1.7 Übermittlung von Beihilfebescheiden in elektronischer Form

Nach § 48 Abs. 4 BayBhV können Beihilfebescheide auch in elektronischer Form übermittelt werden, sofern der Beihilfeberechtigte diesem Verfahren zustimmt.

Zur Umsetzung dieser Vorschrift sah das Staatsministerium der Finanzen im Entwurf der VV-BayBhV ursprünglich einen unverschlüsselten Versand des Beihilfebescheids an die dienstliche E-Mail-Adresse vor. Das Formblatt „Antrag auf Beihilfe“ sollte hierzu folgende Erklärung des Beihilfeberechtigten enthalten: „Ich bin mit einer unverschlüsselten Rücksendung meines Beihilfebescheides an meine dienstliche E-mail-Adresse (Intranet) _____@_____ einverstanden.“ Diese Zustimmung - so das Finanzministerium - sei als bewusster Grundrechtsverzicht des Beihilfeberechtigten auszulegen. Alternativ sei auch eine Übermittlung an die private E-Mail-Adresse vorstellbar.

Ich habe dem Staatsministerium der Finanzen dazu mitgeteilt, dass aus Sicht des Datenschutzes eine elektronische Übermittlung von Beihilfebescheiden nur per verschlüsselter E-Mail oder noch besser über ein web-basiertes Pull-Verfahren erfolgen darf. Ein unverschlüsselter Versand des Beihilfebescheids an die dienstliche E-Mail-Adresse wäre dagegen ebenso unzulässig wie eine unverschlüsselte Bekanntgabe an die private E-Mail-Adresse. Zur Begründung habe ich im Einzelnen auf Folgendes hingewiesen:

Der unverschlüsselte Versand per E-Mail ist zur Übertragung personenbezogener Daten des Beihilfeberechtigten und seiner berücksichtigungsfähigen Angehörigen, darunter auch besonders sensibler

Daten über die Gesundheit (vgl. Art. 15 Abs. 7 BayDSG), generell nicht geeignet.

Dies trifft gerade auch für die Übersendung von E-Mails innerhalb des Bayerischen Behördennetzes an die dienstliche E-Mail-Adresse zu: Zunächst ist zu beachten, dass der Freistaat Bayern nicht selbst Betreiber des Behördennetzes ist und über keine unmittelbare Kontrolle über die Netzinfrastruktur verfügt. Vielmehr steht er in Vertragsbeziehung mit einem kommerziellen Betreiber mit eigenen Unterauftragnehmern. Eine Einsichtnahme in unverschlüsselte E-Mails ist daher sowohl dem Netzbereitsteller und -betreiber als auch den Unterauftragnehmern möglich. Zudem ist eine Einsichtnahme in unverschlüsselte E-Mails auch den Betreibern zentraler E-Mail-Server im Behördennetz (z.B. dem Landesamt für Statistik und Datenverarbeitung - Rechenzentrum Süd) und - im Falle des Verbots der privaten Mitbenutzung der dienstlichen E-Mail-Adresse u.U. sogar rechtmäßig - den Administratoren der Beschäftigungsdienststelle möglich. Hinzu kommt, dass die Ausgestaltung der Verwendung des E-Mail-Dienstes der Organisationshoheit der Beschäftigungsdienststelle überlassen ist und sich in den verschiedenen Bereichen der staatlichen Verwaltung ausgesprochen heterogen darstellt. Dies betrifft insbesondere die - für den betroffenen Beihilfeberechtigten weitgehend verpflichtenden - innerbehördlichen Regelungen zum Zugriff auf personenbezogene Postfächer durch Dritte, beispielsweise hinsichtlich der Vertreterfunktionen bei Abwesenheit, Krankheit, Urlaub etc. oder automatischer Weiterleitungsfunktionen. Es kann somit weder sichergestellt werden, dass ein Beihilfebescheid nur dem Antragsteller bekannt wird, noch davon ausgegangen werden, dass der Beihilfeberechtigte dies selbst beeinflussen kann, ohne gegen Dienstvorschriften der Beschäftigungsbehörde zu verstoßen.

Weiter habe ich dem Staatsministerium der Finanzen mitgeteilt, dass auch einer unverschlüsselten Übermittlung des Beihilfebescheids an die private E-Mail-Adresse aus Sicht des Datenschutzes nicht zugestimmt werden kann. Denn selbst wenn im Vergleich zum Versand an die dienstliche E-Mail-Adresse einige Problempunkte entfallen, bleibt auch hier den Netzbetreibern des Internets eine Einsichtnahme möglich.

An diesem Ergebnis ändert auch nichts, dass die Übermittlung des Beihilfebescheids per E-Mail nur mit Einverständnis des Beihilfeberechtigten möglich ist. Zur Auffassung des Staatsministeriums der Finanzen, die Zustimmung zum unverschlüsselten Versand per E-Mail sei als bewusster Grundrechtsverzicht auszulegen, habe ich zunächst darauf hingewiesen, dass ein Grundrechtsverzicht nur in Betracht kommt, wenn dieser freiwillig erfolgt (vgl. insoweit nur die strengen Anforderungen in Art. 15 Abs. 2 bis 4 und 7 BayDSG). Die Freiwilligkeit wiederum setzt u.a. voraus, dass der Betroffene über die Folgen seines Verzichts ausreichend informiert wird. Hierfür reicht es nicht aus, wenn dieser, wie in dem ursprünglichen Entwurf des Antragsformulars vorgesehen, lediglich auf die Tatsache hingewiesen wird, dass die Rücksendung unverschlüsselt erfolgt. Vielmehr wäre u.a. erforderlich, dass der Betroffene auch über die aufgezeigten Risiken eines unverschlüsselten Versands allgemeinverständlich aufgeklärt wird. Darüber hinaus ist zu berücksichtigen, dass der Beihilfeberechtigte allenfalls auf sein eigenes Grundrecht auf informationelle Selbstbestimmung verzichten könnte, nicht hingegen auf dasjenige seiner berücksichtigungsfähigen Angehörigen.

Als zeitgemäße und nicht kostenaufwändigere Alternative zur verschlüsselten E-Mail habe ich dem Staatsministerium der Finanzen für die Übermittlung des Beihilfebescheids in elektronischer Form nach § 48 Abs. 4 BayBhV ein datenschutzgerecht ausgestaltetes Pull-Verfahren als Web-Anwendung empfohlen. Hierbei wäre aus technisch-organisatorischer Sicht wie folgt vorzugehen:

- Der Beihilfebescheid wird auf einem geschützten, aber über das Internet zugänglichen Webserver abgelegt.

- Der Antragsteller erhält per E-Mail von der Beihilfestelle eine Nachricht, dass ein Beihilfebescheid für ihn vorliegt, wobei die E-Mail ansonsten keinerlei weitere Informationen zum Beihilfeantrag und -bescheid enthält und somit unverschlüsselt versandt werden kann.

- Der Antragsteller ruft seinen Beihilfebescheid nach erfolgreicher Identifizierung und Authentifizierung von diesem Webserver ab, wobei die Datenübertragung verschlüsselt (z.B. mit HTTPS) erfolgt.

- Identifizierung und Authentifizierung der Berechtigten ließen sich z.B. mittels des weit verbreiteten Systems einer einmalig zugewiesenen Benutzerkennung und einem auf sicherem Wege (postalisch) übermittelten Startpasswort ermöglichen. Das Startpasswort müsste vom Berechtigten - technisch erzwungen - nach der erstmaligen Anmeldung sowie in regelmäßigen Abständen geändert werden, wobei an die selbst gewählten Passworte Qualitätsanforderungen gemäß meiner diesbezüglichen Orientierungshilfe zu stellen sind.

Dieses Verfahren böte zudem den Vorteil, dass der Beihilfeberechtigte flexibel in der Wahl seines Abrufortes wäre - er könnte den Bescheid also beispielsweise auch im Urlaub von zuhause aus abrufen. Auch für Pensionäre etc. könnte dieses Verfahren von Interesse sein.

Erfreulicherweise hat das Staatsministerium der Finanzen daraufhin davon Abstand genommen, in den VV-BayBhV einen unverschlüsselten Versand des Beihilfebescheids an die dienstliche bzw. private E-Mail-Adresse vorzusehen; so enthalten die VV-BayBhV gegenwärtig keinerlei Regelungen zur Übermittlung von Beihilfebescheiden in elektronischer Form. Vielmehr konzipiert das Staatsministerium der Finanzen derzeit - entsprechend meinem Vorschlag - ein web-basiertes Pull-Verfahren. Ich werde die Entwicklung auch weiterhin kritisch begleiten.

Im Ergebnis bleibt festzustellen, dass die Neuordnung des Bayerischen Beihilferechts zwar zu zahlreichen datenschutzrechtlichen Verbesserungen geführt hat, leider aber noch ein - an einigen Stellen auch größeres - datenschutzrechtliches Optimierungspotenzial aufweist.

### 21.2 Geltendmachung von Regressansprüchen nach einem Dienstunfall

Nach einem vom Unfallgegner verschuldeten Dienstunfall musste sich ein Beamter - so seine Schilderung in einer Eingabe an mich - in privatärztliche Behandlung begeben; außerdem war er drei Tage lang dienstunfähig. Der Unfallverursacher war zum Schadensersatz verpflichtet, wozu hier sowohl die Kosten der Heilbehandlung als auch die Dienstausfallkosten gehörten. Da der Dienstherr dem Beamten die Heilbehandlungskosten im Rahmen der Dienstunfallfürsorge erstattet und auch die Dienstbezüge während der Dienstunfähigkeit fortgezahlt hatte, waren die dem Beamten insoweit zustehenden Schadensersatzansprüche nach Art. 96 BayBG auf den Dienstherrn übergegangen, so dass dieser den Unfallverursacher in Regress nehmen konnte. Zu diesem Zweck wandte sich die zuständige Behörde in dem mir vorgetragenen Fall schriftlich an den Schadensersatzpflichtigen. Dabei übermittelte sie diesem zum Nachweis der Höhe der übergegangenen Ansprüche die Rechnung des behandelnden Arztes sowie eine konkrete Berechnung des Dienstausfallschadens, aus der die Höhe der Jahresbezüge des Beamten einschließlich Sonderzuwendung und Urlaubsentgelt hervorging. Dem Schreiben lag zudem - eine Arbeitsunfähigkeitsbescheinigung war wegen der geringen Dauer der Dienstunfähigkeit nicht ausgestellt worden - zum Nachweis der Dauer der Dienstunfähigkeit ein Auszug aus der Dienstunfalluntersuchung mit dem Befundbericht des behandelnden Arztes bei.

Aus datenschutzrechtlicher Sicht habe ich diese Angelegenheit wie folgt bewertet:

Bei Dienstunfallunterlagen handelt es sich gemäß Art. 100 a Abs. 1 Satz 2 BayBG um dem Personalaktengeheimnis unterliegende Personalaktendaten. Da im Rahmen der Dienstunfallfürsorge ähnlich wie im Beihilfeverfahren Daten über den Gesundheitszustand des Beamten anfallen, werden die Dienstunfallunterlagen in Art. 100 b Satz 5 BayBG den Beihilfeunterlagen gleichgestellt. Durch diesen besonderen Schutz der Vertraulichkeit gegenüber Dritten will der Gesetzgeber nicht nur einen Ausgleich für die in Art. 119 Abs. 4 BayBG statuierte weitgehende Offenlegungspflicht des Beamten gegenüber dem Dienstherrn schaffen. Vielmehr will der Gesetzgeber durch Art. 100 b Satz 5 i.V.m. Satz 4 BayBG, der die Verwendung und Weitergabe der Dienstunfallunterlagen für die im Zusammenhang mit der Dienstunfallfürsorge stehenden behördlichen und gerichtlichen Verfahren im erforderlichen Umfang ohne Einwilligung des Beamten zulässt, auch die Erfüllung des mit Art. 119 Abs. 4 BayBG verfolgten Zwecks - die Geltendmachung von Regressansprüchen gegen Dritte - sicherstellen. Im Ergebnis dürfen daher Dienstunfallunterlagen nur insoweit an den Schadensersatzpflichtigen übermittelt werden, als dies zur Geltendmachung von Regressansprüchen unbedingt erforderlich ist. (Vgl. zum Ganzen den Standardkommentar Weiß/Niedermaier/Summer/Zängl, Bayerisches Beamtengesetz, München/Berlin, Stand: 2008, Art. 100 b BayBG Erl. 10.)

Der Dienstausfallschaden wird nach den konkreten individuellen Erwerbseinbußen bemessen, weshalb u.a. auf das Jahreseinkommen abzustellen ist. Da dem Dienstherrn als Anspruchsteller die volle Beweislast obliegt, habe ich im vorliegenden Fall die Übermittlung der konkreten Berechnung an den Schadensersatzpflichtigen zur Geltendmachung von Regressansprüchen gemäß Art. 100 b Satz 5 i.V.m. Satz 4 BayBG für erforderlich gehalten. In diesem Zusammenhang habe ich auch berücksichtigt, dass die Höhe der Dienstbezüge gesetzlich geregelt ist und damit ohnehin jedermann zugänglich ist.

Der Nachweis der Dauer der Dienstunfähigkeit kann von der zuständigen Behörde im Regelfall durch Übersendung der Arbeitsunfähigkeitsbescheinigung an den Schadensersatzpflichtigen geführt werden. Da aus einer Arbeitsunfähigkeitsbescheinigung weder Diagnose noch Befund des behandelnden Arztes hervorgehen, halte ich deren Übermittlung zur Geltendmachung von Regressansprüchen gemäß Art. 100 b Satz 5 i.V.m. Satz 4 BayBG datenschutzrechtlich für zulässig. Nachdem im konkreten Fall eine Arbeitsunfähigkeitsbescheinigung jedoch nicht vorlag, hätten zumindest die Diagnose und der Befund vor Übersendung des Befundberichts des behandelnden Arztes an den Schadensersatzpflichtigen geschwärzt oder sonst unkenntlich gemacht werden müssen. Dies ergibt sich bereits daraus, dass auch aus der im Regelfall übersandten Arbeitsunfähigkeitsbescheinigung weder Diagnose noch Befund ersichtlich sind.

Um den datenschutzrechtlichen Anforderungen Rechnung zu tragen, sollte der Dienstherr bei der

Geltendmachung von Regressansprüchen nach einem Dienstunfall wie folgt verfahren:

- Grundsätzlich ist lediglich eine Arbeitsunfähigkeitsbescheinigung an den Schadensersatzpflichtigen zu übersenden.

- Falls eine Arbeitsunfähigkeitsbescheinigung nicht vorliegt, ist eine solche beim betroffenen Beamten anzufordern und nach Eingang an den Schadensersatzpflichtigen zu übersenden.

- Lediglich wenn weder eine Arbeitsunfähigkeitsbescheinigung noch ein sonstiger geeigneter Beleg vom betroffenen Beamten vorgelegt werden kann, darf die Übersendung des Befundberichts aus der Dienstunfalluntersuchung nach Unkenntlichmachung aller zum Nachweis der Unfallbedingtheit nicht erforderlichen persönlichen Daten an den Schadensersatzpflichtigen erfolgen.

- 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.

### 21.3 Anforderung und Vorlage des Personalakts anlässlich einer Bewerbung

Immer wieder sind datenschutzrechtliche Fragen im Zusammenhang mit der Anforderung und Vorlage des Personalakts anlässlich einer Bewerbung Gegenstand von Anfragen und Eingaben. Daher halte ich zu diesem Problemkreis folgende grundlegenden Hinweise für veranlasst:

- Bewirbt sich ein öffentlich Bediensteter - aus eigenem Antrieb und ohne die für ihn zuständige(n) personalaktenführende(n) Behörde(n) zu informieren - auf eine Stelle bei einer anderen Behörde, dann darf diese Behörde den Personalakt nur mit ausdrücklicher Einwilligung des Bewerbers anfordern.

  Die Anforderung des Personalakts bringt nämlich zumindest mittelbar die Tatsache der Bewerbung und damit den Versetzungswunsch des Bewerbers zum Ausdruck. Dadurch nimmt die den Personalakt anfordernde Behörde bereits eine Datenübermittlung an die personalaktenführende(n) Behörde(n) vor. Im Hinblick auf den Anspruch des Bewerbers auf Persönlichkeitsschutz kommt als Rechtsgrundlage für diese Datenübermittlung allein die ausdrückliche Einwilligung des Bewerbers in Betracht. Andernfalls bestünde die Gefahr, dass die personalaktenführende(n) Behörde(n) - und in der Folge auch die aktuelle Beschäftigungsbehörde - ohne Wissen des Bediensteten von seiner Bewerbung und damit auch seinem Versetzungswunsch erfahren. Dies könnte zu erheblichen Nachteilen für den Betroffenen führen, insbesondere wenn seine Bewerbung nicht berücksichtigt wird.

- Vor diesem Hintergrund sind auch an den Zeitpunkt der Einwilligung besondere datenschutzrechtliche Anforderungen zu stellen.

  So halte ich es in zeitlicher Hinsicht für äußerst problematisch, wenn sich die Stellen ausschreibende Behörde vom Bewerber die Einwilligung in die Anforderung des Personalakts gleich mit der Bewerbung erteilen lässt. Insbesondere bei einer Vielzahl von Bewerbern ist die Anforderung aller Personalakten nicht nur sehr verwaltungsaufwändig, sondern auch für die Vor-Auswahlentscheidung sachlich nicht erforderlich. Auf der anderen Seite ist es aber natürlich auch fachlich wenig sinnvoll, den Personalakt erst nach erfolgter End-Auswahlentscheidung beizuziehen.

  Meiner Meinung nach darf der Personalakt daher erst in einem fortgeschrittenen Stadium des Auswahlverfahrens angefordert werden, wenn sich also die Bewerberauswahl auf einige wenige aussichtsreiche Kandidaten konzentriert hat, die dann auch zu einem Vorstellungsgespräch eingeladen werden sollen. Erst zu diesem Zeitpunkt sollte somit die Einwilligung bei den aussichtsreichen Bewerbern eingeholt werden.

  Wird die Einwilligung jedoch bereits mit der Bewerbung eingeholt, so dürfen die Personalakten - nur der aussichtsreichen Bewerber - zumindest erst in dem beschriebenen fortgeschrittenen Stadium des Bewerbungsverfahrens angefordert werden; darauf sind die Bewerber meines Erachtens auch hinzuweisen.

- Im Hinblick auf die dem Dienst- bzw. Arbeitsverhältnis schon im Stadium der Anbahnung immanente Problematik des faktischen Zwangs ist die Freiwilligkeit einer solchen Einwilligung grundsätzlich kritisch zu sehen. Allerdings kann dies nicht dazu führen, dass eine Einwilligung im (Anbahnungs-)Dienst- bzw. Arbeitsverhältnis praktisch ausgeschlossen ist.

  Daher sehe ich die Freiwilligkeit als gegeben an, wenn die Einwilligung erst in einem fortgeschrittenen Stadium des Bewerbungsverfah-

rens eingeholt wird, in dem der Bewerber also schon eine „konkretisierte Expektanz“ auf die neue Stelle hat. Hier kann der Bewerber „sehenden Auges“ die Vor- und Nachteile seiner Einwilligung abwägen.

- In Anbetracht der - meiner Auffassung nach als allgemein gültige Schutzprinzipien analog auch auf die nicht-verbeamteten Beschäftigten des öffentlichen Dienstes anwendbaren - personalaktenrechtlichen Vorschriften über die Erhebung von Bewerberdaten (Art. 100 Satz 1 BayBG) und über die Vorlage von Personalakten (Art. 100 e Abs. 4 BayBG) stellt sich schließlich die Frage, ob bereits im Bewerbungsverfahren die Anforderung und Vorlage des vollständigen Personalakts datenschutzrechtlich erforderlich ist.

  Meiner persönlichen Erfahrung nach ist der Personalakt in hohem Maße geeignet, der über die Bewerbung entscheidenden Stelle einen Gesamteindruck von der persönlichen und fachlichen Eignung und Befähigung des Bewerbers für die ausgeschriebene Stelle zu verschaffen. Auch Personalaktendaten, die bei erster Einschätzung nicht für die Personalauswahl erforderlich erscheinen, können im konkreten Fall eine bedeutsame Rolle spielen und zumindest wichtige Bausteine für diesen Gesamteindruck darstellen. Ich sehe daher die Anforderung und Vorlage des vollständigen Personalakts als erforderlich für die endgültige Auswahlentscheidung an.

Zusammengefasst ist meiner Auffassung nach erst in einem fortgeschrittenen Stadium des Bewerbungsverfahrens die auf der Rechtsgrundlage einer Einwilligung erfolgende Anforderung und Vorlage des vollständigen Personalakts datenschutzrechtlich zulässig.

### 21.4 Veröffentlichung von Mitarbeiterdaten im gemeindlichen Mitteilungsblatt

Im Mitteilungsblatt einer Gemeinde wurde unter der Rubrik „Jugendecke“ u.a. die Art der Beschäftigungsverhältnisse der Jugendbeauftragten und der Jugendbetreuer - „ehrenamtlich“ / „geringfügig beschäftigt“ - veröffentlicht. Dies habe ich gegenüber der betroffenen Gemeinde wie folgt datenschutzrechtlich bewertet:

Rechtsgrundlage für die Veröffentlichung von Mitarbeiterdaten ist Art. 19 Abs. 1 Nr. 1 i.V.m. Art. 17 Abs. 1 Nr. 2 BayDSG; im datenschutzrechtlichen Sinne liegt hier eine Datenübermittlung an nichtöffentliche Stellen vor. Im Rahmen der Prüfung dieser Rechtsgrundlage ist entscheidend, ob die Übermittlung der konkreten Mitarbeiterdaten zur Aufgabenerfüllung der Gemeinde erforderlich ist. Dabei kommt es nicht nur darauf an, dass die Datenübermittlung sachdienlich ist, sondern auch, dass sie als angemessen im Verhältnis zu etwaigen schutzwürdigen Interessen des Bediensteten an einer Nichtbekanntgabe seiner Daten erscheint.

Da zur ordnungsgemäßen Aufgabenerfüllung einer Gemeinde auch die Information der Öffentlichkeit über die zuständigen Ansprechpartner gehört, ist die Veröffentlichung personenbezogener Kommunikationsdaten von Bediensteten, die Funktionen mit Außenwirkung wahrnehmen, zur ordnungsgemäßen Aufgabenerfüllung im Sinne des Art. 19 Abs. 1 Nr. 1 BayDSG grundsätzlich als erforderlich anzusehen. Dieser Personenkreis muss aufgrund seiner auf die Öffentlichkeit bezogenen Aufgabenstellung beispielsweise hinnehmen, dass von ihm Name, Amts- und Dienstbezeichnung, Tätigkeitsbereich und Funktion sowie dienstliche Anschrift und Telefonnummer veröffentlicht werden (siehe zuletzt ausführlich Nr. 19.1 meines 22. Tätigkeitsberichts 2006).

Meiner Auffassung nach ist es für die Öffentlichkeit auch von Bedeutung, ob es sich bei dem Ansprechpartner um einen in das Organisationsgefüge der Gemeinde fest eingebundenen „regulären“ oder um einen - im dienstrechtlichen Sinne nicht weisungsgebundenen - „ehrenamtlichen“ Mitarbeiter handelt. Die Veröffentlichung des Datums „ehrenamtlich“ ist daher ebenfalls datenschutzrechtlich zulässig.

Anders verhält es sich dagegen mit der Veröffentlichung des Datums „geringfügig beschäftigt“. Ebenso wie die anderen „regulären“ Mitarbeiter sind diese Beschäftigten in das Organisationsgefüge der Gemeinde fest eingebunden. Vor diesem Hintergrund ist ein Interesse der Öffentlichkeit an der Kenntnis dieses Datums nicht ersichtlich. Vielmehr besteht hier sogar die Gefahr der Diskriminierung. Im Hinblick auf das Datum „geringfügig beschäftigt“ ist somit das Interesse des Beschäftigten an der Nichtbekanntgabe als schutzwürdig anzusehen. Die Veröffentlichung dieses Datums halte ich daher für datenschutzrechtlich unzulässig.

## 22 Medien und Telekommunikation

### 22.1 Orientierungshilfe zur datenschutzgerechten Nutzung von E-Mail und anderen Internetdiensten am Arbeitsplatz

Im Berichtszeitraum hat der Arbeitskreis Medien der Konferenz der Datenschutzbeauftragten des Bundes und der Länder unter meiner Mitwirkung seine „Orientierungshilfe zur datenschutzgerechten Nutzung von E-Mail und anderen Internetdiensten am Arbeitsplatz“ überarbeitet und aktualisiert. Die Orientierungshilfe ist auf meiner Homepage www.datenschutz-bayern.de in der Rubrik „Verwaltung’“ unter „Allgemeines“ zu finden.

Ziel der Orientierungshilfe ist es, sowohl den öffentlichen Dienstherrn als auch den Bediensteten eine Hilfestellung in Bezug auf die bei der dienstlichen und privaten Nutzung von E-Mail und anderen Internetdiensten am Arbeitsplatz auftretenden Rechtsfragen zu bieten. Die bei der Nutzung dieser Dienste zu beachtenden datenschutzrechtlichen Anforderungen - insbesondere im Hinblick auf die Vorschriften des Telekommunikations- und Telemedienrechts, des Personalvertretungs- und allgemeinen Datenschutzrechts - werden im Einzelnen dargestellt. In diesem Zusammenhang ist zu erwähnen, dass ich bereits in Nr. 20.1 meines 22. Tätigkeitsberichts 2006 und in Nr. 21.1 meines 21. Tätigkeitsberichts 2004 zu diesem - auch in meiner täglichen Beratungspraxis wichtigen - Problemkreis umfassende Hinweise gegeben habe.

Neu sind vor allem die Aussagen zur Spam-Filterung; diese darf grundsätzlich nur außerhalb der Reichweite des Fernmeldegeheimnisses bzw. mit Einwilligung der Bediensteten erfolgen. Auch in Bezug auf das Thema Spam-Behandlung und Datenschutz habe ich mich bereits unter Nr. 23.3 meines 22. Tätigkeitsberichts 2006 ausführlich geäußert.

## 22.2 Benutzung dienstlicher Telekommunikationsanlagen

Zu datenschutzrechtlichen Fragestellungen im Zusammenhang mit dienstlichen Telekommunikationsanlagen habe ich mich bereits in Nr. 17.1 Benutzung dienstlicher Telekommunikationsanlagen meines 18. Tätigkeitsberichts 1998, Nr. 13.3.2 Erfassung der Telefondaten von Berufsgeheimnisträgern meines 20. Tätigkeitsberichts 2002 sowie in Nr. 23.4.6 Telefondatenerfassung bei Privatgesprächen und von Berufsgeheimnisträgern meines 22. Tätigkeitsberichts 2006 ausführlich geäußert.

Bedingt durch die Novellierung des Telekommunikationsgesetzes im Jahr 2004, aber nach eigener Aussage auch „aufgrund datenschutzrechtlicher Vorgaben“ hat das Staatsministerium der Finanzen mit Wirkung vom 01.07.2007 die Bekanntmachung über die „Einrichtung und Benutzung dienstlicher Telekommunikationsanlagen (TK-Bek)“ neu gefasst (FMBl 2007, 178).

Erfreulicherweise hatte das Finanzministerium bereits im Entwurf der Neufassung zahlreiche Belange des Datenschutzes berücksichtigt. Dennoch konnte ich im Verlauf des Normsetzungsverfahrens weitere datenschutzrechtliche Verbesserungen erreichen.

Im Einzelnen sind insbesondere folgende Punkte hervorzuheben:

1. Im Hinblick auf die Speicherung von Verkehrsdaten abgehender Wählverbindungen bestimmt nunmehr Nr. 3.1.3 Satz 3 TK-Bek, dass bei nicht erstattungspflichtigen Nahgesprächen ein Nachweis der Zielrufnummer der angerufenen Person (einschließlich Vorwahl) generell nicht mehr erfolgen darf. Die frühere Regelung stellte dies noch unter den Vorbehalt des technisch Möglichen.

   Diese Neuregelung ist unter datenschutzrechtlichen Gesichtspunkten zu begrüßen, da eine Erforderlichkeit dieser Datenspeicherung - etwa zu Abrechnungszwecken - nicht gegeben ist.

2. Gemäß Nr. 3.1.3 Satz 5 TK-Bek sind die Verkehrsdaten für erstattungspflichtige private Telefongespräche bzw. für erstattungspflichtige Gespräche Dritter nach vollständiger Abrechnung der Entgelte, spätestens aber zum Ablauf der gesetzlich festgelegten Höchstspeicherdauer zu löschen, soweit gegen die Abrechnung keine Einwendungen erhoben wurden.

   Ich begrüße diese Neuregelung ausdrücklich, da sie die mit der Umsetzung befassten Dienststellen darauf aufmerksam macht, dass die angefallenen Verkehrsdaten längstens bis zum Ablauf der gesetzlich festgelegten Höchstspeicherdauer vorgehalten werden dürfen.

3. Die neu gefasste Nr. 3.1.4 Satz 2 TK-Bek statuiert ein umfassendes Zweckänderungsverbot bezüglich der Nachweise über dienstliche Verbindungen.

   Auch dies ist aus datenschutzrechtlicher Sicht sehr erfreulich, da die frühere Fassung lediglich die Unzulässigkeit einer Verknüpfung der Nachweise mit anderen Dateien angeordnet hatte.

4. Nach Nr. 3.1.5 TK-Bek sind bei Verbindungen von Stellen, deren Telefonverkehr nicht der Aufsicht unterliegt (z.B. Personalvertretungen in Personalangelegenheiten) und von Stellen, die im Rahmen einer freiwilligen Beratung (z.B. Drogen-, Gesundheits-, Ehe- und Familienberatung) tätig werden und damit einer besonderen Verschwiegenheitspflicht unterliegen, nur die Leistungsentgelte festzuhalten. Dies gilt im Unterschied zur früheren Regelung unabhängig davon, ob diese Stellen eine Aufzeichnung oder Speicherung der übrigen Verkehrsdaten verlangen.

   Ich begrüße die Streichung des Wahlrechts der Geheimnisträger, die ich bereits in Nr. 17.1 Benutzung dienstlicher Telekommunikationsanlagen meines 18. Tätigkeitsberichts 1998

sowie in Nr. 13.3.2 Erfassung der Telefondaten von Berufsgeheimnisträgern meines 20. Tätigkeitsberichts 2002 gefordert hatte. Denn die Einhaltung der Verschwiegenheitspflicht steht nicht zur freien Disposition der Geheimnisträger. In jedem Fall dürfen also nur die Leistungsentgelte festgehalten werden.

5. Eine Verbesserung in datenschutzrechtlicher Hinsicht haben auch die Bestimmungen über das Aufschalten auf Gespräche von Beschäftigten (Mithören) erfahren:

   - Während die frühere Fassung noch die Kenntlichmachung der Aufschaltung ausreichen ließ, bestimmt Nr. 3.1.6 Satz 3 TK-Bek nunmehr explizit, dass das Aufschalten auf Gespräche von Beschäftigten ohne deren Kenntnis unzulässig ist.

     Diese Neuregelung ist aus datenschutzrechtlicher Sicht grundsätzlich zu begrüßen. Allerdings kann es zu Missverständnissen Anlass geben, dass auch die Neufassung zur Erklärung noch das Beispiel „dem Beschäftigten erläuterte akustische Signale“ nennt. Ein erläutertes akustisches Signal mag für die Kenntlichmachung der Aufschaltung genügt haben, reicht jedoch keinesfalls aus, um von einer Kenntnis des Beschäftigten von der Aufschaltung ausgehen zu können. Der neuen Rechtlage ist nur Genüge getan, wenn die Kenntnis des Beschäftigten von der Aufschaltung sichergestellt ist. Dies kann etwa dadurch erreicht werden, dass der Beschäftigte durch positives Tun - wie z.B. einen Tastendruck - zu erkennen gibt, er habe das erläuterte akustische Signal tatsächlich wahrgenommen.

   - Auf meine Anregung hin hat das Staatsministerium der Finanzen in Nr. 3.1.6 Sätze 4 und 5 TK-Bek zusätzliche Schutzregelungen für Privatgespräche geschaffen. So wird ausdrücklich festgestellt, dass das Aufschalten auf besonders gekennzeichnete private Verbindungen unzulässig und - soweit möglich - durch technische Maßnahmen auszuschließen ist. Zudem ist das Aufschalten auf nicht besonders gekennzeichnete private Verbindungen zu beenden, sobald dem Aufschaltenden erkennbar wird, dass es sich um eine nicht dienstliche Verbindung handelt.

In Ergänzung zur Allgemeinen Geschäftsordnung (AGO) gilt die TK-Bek für nahezu alle Behörden des Freistaates Bayern, nicht hingegen für viele andere öffentliche Stellen meines Zuständigkeitsbereichs, wie z.B. die Kommunalverwaltungen. Aus datenschutzrechtlicher Sicht empfehle ich jedoch diesen öffentlichen Stellen, die Neufassung der TK-Bek zum Anlass und zum Vorbild für eine kritische Durchsicht und ggf. Verbesserung der internen Regelungen zur Benutzung dienstlicher Telekommunikationsanlagen zu nehmen.

# 23 Statistik

## 23.1 Nochmals: eGovernment-Projekt „Amtliche Schuldaten“

Bereits in Nr. 21.1 meines 22. Tätigkeitsberichts 2006 habe ich über das eGovernment-Projekt „Amtliche Schuldaten“ des Staatsministeriums für Unterricht und Kultus ausführlich berichtet. Gegenstand dieses Projekts ist zum einen eine umfassende Restrukturierung der Geschäftsprozesse der Kultusverwaltung mit dem Ziel eines effektiven, netzbasierten Schulverwaltungsverfahrens (sog. operative Datenbank) und zum anderen eine Neukonzeption der Schulstatistik, die insbesondere durch die Ermöglichung von Bildungsverlaufsuntersuchungen die längerfristige Bildungsplanung verbessern soll (sog. Auswertungsdatenbank).

Seit dem Start des Projekts im Jahr 2005 habe ich das Staatsministerium für Unterricht und Kultus wiederholt darauf hingewiesen, dass die Umstellung der Schulstatistik von Summendaten auf Individualdaten wegen der massiv erhöhten Grundrechtsintensität eine datenschutzgerechte, transparente Rechtsgrundlage erfordert, die auch den statistikrechtlichen Anforderungen gerecht wird (d.h. insbesondere Festlegung der Erhebungs- und Hilfsmerkmale, Regelung der Auskunftspflicht, Festlegung der technisch-organisatorischen Maßnahmen zur frühestmöglichen Pseudonymisierung/Anonymisierung sowie Festlegung der Zugriffsrechte). Anfang des Jahres 2007 hat mir das Kultusministerium erstmals einen umfassenden Gesetzentwurf für das Gesamtprojekt „Amtliche Schuldaten“ übermittelt. Obwohl ich im Zuge einer kritischen und intensiven Diskussion mit dem Staatsministerium für Unterricht und Kultus erhebliche datenschutzrechtliche Verbesserungen erreichen konnte (wie z.B. Reduzierung der gespeicherten Datenbestände, Festlegung strenger Zugriffsrechte, Aufnahme von Löschungsfristen in das Gesetz, Festschreibung einer unumkehrbaren Einweg-Verschlüsselung aller nicht für das aktuelle Schulverwaltungsverfahren benötigten Daten, Ansiedelung der Datenbanken beim Landesamt für Statistik und Datenverarbeitung - Rechenzentrum Süd), stellen der nun vorliegende, mehrmals überarbeitete Gesetzentwurf und der Entwurf einer entsprechenden Ausführungsverordnung aus datenschutzrechtlicher Sicht nicht das „Optimum“ dar. Insbesondere bestehen

meine grundsätzlichen datenschutzrechtlichen Bedenken

- keine Ausgestaltung als amtliche Statistik, sondern als Geschäftsstatistik,

- Totalerhebungen statt wissenschaftlich basierter repräsentativer Stichprobenerhebungen im Zusammenhang mit der Auswertungsdatenbank

weiterhin fort.

### 23.1.1 Operative Datenbank

Die operative Datenbank dient vor allem dem Zweck, die Bearbeitung schulübergreifender Prozesse (z.B. Schulwechsel, Überwachung der Schulpflicht) zu vereinfachen. Zudem soll sie die Aufgabenerfüllung der Schulaufsichtsbehörden (beispielsweise bei der Unterrichtsplanung, Lehrerzuweisung und Schulfinanzierung) unterstützen. Die operative Datenbank liefert überdies die (Daten-)Grundlage für die Auswertungsdatenbank.

Im Hinblick auf die operative Datenbank erschien es mir aus datenschutzrechtlicher Sicht insbesondere von Bedeutung, die bestehenden Zuständigkeiten und Befugnisse der Schulaufsichtsbehörden nicht (faktisch) auszuweiten. Dies ist nach dem Gesetzentwurf gelungen; insbesondere bestehen weder ein Vollzugriff noch Auswertungsmöglichkeiten des Kultusministeriums hinsichtlich des gesamten Datenbestands. Zudem ist der Zugriff der Schulaufsichtsbehörden auf personenbezogene Daten der Schüler und Erziehungsberechtigten ausgeschlossen. In Bezug auf die Lehrkräfte wird die Wahrung der personalaktenrechtlichen Vorschriften sichergestellt. Der Gesetzentwurf sieht weiterhin vor, Zugriffe von Stellen außerhalb der Schulverwaltung und des Landesamts für Statistik und Datenverarbeitung (im Rahmen der Erstellung der Schulstatistik) auszuschließen, insbesondere also den u.a. von besorgten Eltern befürchteten Zugriff von potentiellen Arbeitgebern. Ohnehin werden Noten, „Schulstrafen“, Einkommensverhältnisse der Eltern etc. - im Gegensatz etwa zu den für eine entsprechende Unterrichtsversorgung erforderlichen Daten zum Migrationshintergrund (Geburtsland, Zuzugsjahr, Verkehrssprache) - in der operativen Datenbank nicht gespeichert. Schließlich werden alle künftig nicht mehr erforderlichen - das heißt also alle schuljahresbezogenen - Schülerdaten am Ende des Schuljahres gelöscht.

### 23.1.2 Auswertungsdatenbank

Die Auswertungsdatenbank soll zum einen die Erstellung der Schulstatistik erleichtern und beschleunigen, zum anderen - vor allem über die Ermöglichung von Bildungsverlaufsuntersuchungen - die Grundlagen für die längerfristige Bildungsplanung liefern. In diesem Zusammenhang wurden u.a. von besorgten Eltern die beliebige Erstellung und Weitergabe von personenbezogenen Bildungsverläufen befürchtet.

Ich habe es deshalb für erforderlich erachtet, dass eine Speicherung von identifizierenden Merkmalen wie Name, Geburtstag und Adresse in der Auswertungsdatenbank ausgeschlossen ist. Weiterhin stellt der Gesetzentwurf sicher, dass keine Zugriffe von Stellen außerhalb der Schulverwaltung und des Landesamts für Statistik und Datenverarbeitung (im Rahmen der Erstellung der Schulstatistik) erfolgen, insbesondere also nicht von potentiellen Arbeitgebern. Darüber hinaus sieht der Gesetzentwurf ein datenschutzgerechtes Pseudonymisierungsverfahren in Form einer unumkehrbaren Einweg-Verschlüsselung mittels einer Hash-Funktion vor. In einem feingranularen Berechtigungskonzept sind zudem für einen Standard-User nur eingeschränkte und vor allem nur vordefinierte Abfragemöglichkeiten vorgesehen. Der Ausschluss von Auswertungsergebnissen mit sog. „Tabelleneinsen“ macht schließlich allen Nutzern einen Rückschluss auf Einzelpersonen unmöglich.

Ich gehe allerdings davon aus, dass sich im Zuge des weiteren Gesetzgebungsverfahrens auch in Einzelpunkten noch Diskussionsbedarf ergeben wird. So sehe ich beispielsweise die vorgesehene 30-jährige Speicherung der - wenn auch spätestens mit dem Ausscheiden der Schüler anonymisierten - Datenbestände in der Auswertungsdatenbank weiterhin kritisch.

## 23.2 Datenschutz beim Mikrozensus

Der Mikrozensus ist die amtliche Repräsentativstatistik über die Bevölkerung, den Arbeitsmarkt und die Wohnsituation der Haushalte, an der jährlich 1% aller Haushalte in Deutschland beteiligt sind. Alle Haushalte haben beim Mikrozensus die gleiche Auswahlwahrscheinlichkeit (Zufallsstichprobe). Im Wege einer sog. „einstufigen geschichteten Flächenstichprobe“ werden aus dem Bundesgebiet Flächen (Auswahlbezirke) ausgewählt, in denen alle Haushalte und Personen befragt werden. Jährlich wird ein Viertel aller in der Stichprobe enthaltenen Haushalte (beziehungsweise Auswahlbezirke) ausgetauscht, so dass jeder Haushalt vier Jahre hintereinander befragt wird. Zweck des Mikrozensus ist es, statistische Angaben in tiefer fachlicher Gliederung über die Bevölkerungsstruktur, die wirtschaftliche und soziale Lage der Bevölkerung, der Familien und der Haushalte, den Arbeitsmarkt, die berufliche Gliederung und die Ausbildung der Erwerbsbevölkerung sowie die Wohnverhältnisse bereitzustellen. Der Mikrozensus dient dazu, die im Rahmen von umfassenden Volks-

zählungen erhobenen Daten in kurzen Zeitabständen mit überschaubarem organisatorischem Aufwand zu überprüfen und gegebenenfalls zu korrigieren; er wird deshalb häufig als „kleine Volkszählung“ bezeichnet. Beim Mikrozensus handelt es sich um eine Bundesstatistik; die Datenerhebung erfolgt aber durch die Statistischen Landesämter. Diese bedienen sich dabei sogenannter Erhebungsbeauftragter (Interviewer). Rechtsgrundlage für die Befragung ist das „Gesetz zur Durchführung einer Repräsentativstatistik über die Bevölkerung und den Arbeitsmarkt sowie die Wohnsituation der Haushalte (Mikrozensusgesetz 2005)“.

Unter Anführung datenschutzrechtlicher Bedenken hat sich im Berichtszeitraum eine nicht unerhebliche Anzahl „ausgewählter“ Bürgerinnen und Bürger an mich gewandt, um der Einbeziehung in die Mikrozensusbefragung zu entgehen. Die Betroffenen habe ich aus datenschutzrechtlicher Sicht auf Folgendes aufmerksam gemacht:

- 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 des Bürgers 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.

  Das Mikrozensusgesetz 2005 dürfte diesen Vorgaben genügen. In diesem Zusammenhang ist zu beachten, dass das Bundesverfassungsgericht in einem früheren Beschluss vom 16.07.1969 (Az. 1 BvL 19/63) das Mikrozensusgesetz in der damaligen Fassung als verfassungsgemäß beurteilt hat. Es hat in dieser Entscheidung insbesondere auch die im Mikrozensusgesetz vorgesehene Auskunftspflicht des Betroffenen als zulässig angesehen, vor allem im Hinblick darauf, dass bei einer Stichprobenbefragung bereits eine Verweigerung der Angaben durch wenige Befragte das Ergebnis der Repräsentativumfrage in Frage stellen könnte.

- Einer weit gehenden statistikrechtlichen Auskunftspflicht müssen aber - 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 Rechnung getragen. 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.

  Zudem sind die in § 5 Abs. 1 Mikrozensusgesetz 2005 genannten Hilfsmerkmale - in der Regel also die identifizierenden Merkmale - gemäß § 8 Mikrozensusgesetz 2005 nach Durchführung der Plausibilitätsprüfungen von den Erhebungsmerkmalen zu trennen und spätestens nach Abschluss der Aufbereitung der jeweils letzten aufeinander folgenden Erhebung in einem Auswahlbezirk zu vernichten.

  Verstöße gegen die genannten Bestimmungen seitens der Bediensteten des Landesamts für Statistik und Datenverarbeitung sind mir bisher nicht bekannt geworden.

- Die Betroffenen werden in den Erhebungsvordrucken auch gebeten, den Namen ihrer Arbeitsstätte anzugeben. In § 5 Abs. 2 Mikrozensusgesetz 2005 hat der Gesetzgeber insoweit ausdrücklich festgelegt, dass der Name der Arbeitsstätte ausschließlich für Zwecke der Zuordnung der Erwerbstätigen zu Wirtschaftszweigen verwendet werden darf. Diese Sachbehandlung erscheint nachvollziehbar; sie garantiert eine Zuordnung nach einheitlichen Kriterien. Soweit die Zuordnung durch die Befragten selbst vorgenommen würde, wären - insbesondere bei Großunternehmen, die in verschiedenen Wirtschaftszweigen tätig sind - unterschiedliche Ergebnisse durchaus vorstellbar, was die statistische Aussagekraft mindern würde. Darüber hinaus handelt es sich bei dem Namen der Arbeitsstätte um ein Hilfsmerkmal, das aufgrund § 8 Mikrozensusgesetz 2005, wie bereits ausgeführt, alsbald von den Erhebungsmerkmalen zu trennen und schließlich auch zu vernichten ist.

- Die Mikrozensusbefragungen werden im Regelfall unter Einsatz von Erhebungsbeauftragten, sogenannten Interviewern, durchgeführt (siehe § 6 Mikrozensusgesetz 2005). Allerdings weist das Landesamt für Statistik und Datenverarbeitung die Betroffenen in seinen „Zusätzlichen Informationen“ zur Erhebung darauf hin, dass sie den Erhebungsbeauftragten auch die bereits selbst ausgefüllten Erhebungsvordrucke übergeben können. Ebenso können die selbst ausgefüllten Erhebungsvor-

drucke direkt an das Landesamt übermittelt werden. Da die Übergabe an die Erhebungsbeauftragten in verschlossenem Umschlag erfolgen kann, entstehen für die direkte Übermittlung an das Landesamt nicht zwangsläufig Portokosten.

- In der Vergangenheit wurden die den Auskunftspflichtigen zur Verfügung gestellten Rücksendekuverts von den Interviewern oftmals bereits handschriftlich mit der Absenderangabe versehen. Zudem war auf den Kuverts neben der Empfängeradresse des Landesamts für Statistik und Datenverarbeitung auch der Zusatz „Mikrozensus“ aufgedruckt. Auf meine Bitte hin hat mir das Landesamt zugesichert, die eingesetzten Interviewer künftig anzuweisen, keine Absenderangaben mehr vorweg anzubringen, sondern diese Angaben den Auskunftspflichtigen selbst zu überlassen. Zudem hat mir das Landesamt auf meine Anregung hin zugesagt, den Aufdruck „Mikrozensus“ durch den nichtsprechenden Zusatz „Sachgebiet XX“ zu ersetzen.

- In verstärktem Umfang werden die sogenannten Interviews durch die Erhebungsbeauftragten unter Einsatz von Laptops geführt. In diesem Zusammenhang stellte sich mir die Frage, welche technisch-organisatorischen Maßnahmen zur Gewährleistung des Datenschutzes und der Datensicherheit vom Landesamt für Statistik und Datenverarbeitung verpflichtend vorgegeben werden. Meine diesbezügliche Überprüfung hat ergeben, dass die anfallenden Daten auf den verwendeten Laptops lokal verschlüsselt gespeichert werden. Die für die Speicherung der Mikrozensusdaten auf den Laptops ergriffenen Sicherungsmaßnahmen können als ausreichend angesehen werden.

Vor diesem Hintergrund habe ich im Ergebnis gegen die Erhebungen im Rahmen des Mikrozensus aus datenschutzrechtlicher Sicht keine Einwendungen.

### 23.3 Vorbereitung der Volkszählung 2011

Bereits in Nr. 21.5 meines 22. Tätigkeitsberichts 2006 habe ich darauf hingewiesen, dass sich Deutschland an der kommenden Volkszählungsrunde der Europäischen Union 2010/2011 mit einem registergestützten Zensus beteiligen wird. Derzeit sind die Vorbereitungen des Zensus in vollem Gange. Aus datenschutzrechtlicher Sicht erscheinen mir folgende Punkte erwähnenswert:

1. Am 13.12.2007 ist das vom Bundestag beschlossene „Gesetz zur Vorbereitung eines registergestützten Zensus einschließlich einer Gebäude- und Wohnungszählung 2011 (Zensusvorbereitungsgesetz 2011)“ in Kraft getreten. Im Wesentlichen regelt dieses Gesetz den Aufbau eines Anschriften- und Gebäuderegisters im abgeschotteten Bereich der Amtlichen Statistik. Es ist damit zu rechnen, dass dieses statistische Register mit den gemeindlichen Melderegistern nicht in allen Fällen übereinstimmen wird. Im Zuge des Gesetzgebungsverfahrens hat daher der Bundesrat einstimmig versucht, in Zweifelsfällen eine adressscharfe Überprüfung durch die Meldebehörden zu ermöglichen.

   Eine derartige Rückübermittlung von statistischen Daten in den Verwaltungsvollzug war jedoch der wesentliche Grund für das Bundesverfassungsgericht, das Volkszählungsgesetz 1983 in seinem sog. „Volkszählungsurteil“ (BVerfGE 65,1) teilweise als mit dem Grundgesetz unvereinbar anzusehen. Ich habe daher gegenüber dem Staatsministerium des Innern deutlich gemacht, dass die vom Bundesrat beabsichtigte Rückübermittlung das verfassungsrechtliche Gebot der Trennung von Statistik und Verwaltungsvollzug missachtet. Diese Thematik wurde auch von vielen meiner Kolleginnen und Kollegen problematisiert.

   Der Bundestag hat den Einspruch des Bundesrats schließlich mit Zwei-Drittel-Mehrheit zurückgewiesen. § 7 Zensusvorbereitungsgesetz 2011 spricht nunmehr von der Rückübermittlung von ggf. fehlerhaften „Anschriftenbereichen“; die Meldebehörden sind gehalten, eine Klärung nur anhand der vorhandenen Daten herbeizuführen und keine Einzelfallüberprüfung vor Ort vorzunehmen. Dies halte ich aus Datenschutzsicht für vertretbar.

2. Am 03.12.2008 hat die Bundesregierung den Entwurf eines „Gesetzes zur Anordnung des Zensus 2011 (Zensusgesetz 2011) sowie zur Änderung von Statistikgesetzen“ beschlossen. Mit diesem Gesetzentwurf sollen die rechtlichen Voraussetzungen für den vorgesehenen registergestützten Zensus geschaffen werden. Nicht zuletzt regelt der Gesetzentwurf den Zensusstichtag und die Erhebungs- und Hilfsmerkmale.

   Nachdem mir das Staatsministerium des Innern einen ersten Referentenentwurf zur Stellungnahme übermittelt hatte, habe ich in der Hauptsache zwei Problemfelder gesehen und diese auch gegenüber dem Staatsministerium des Innern thematisiert:

   - Als problematisch habe ich zunächst die Erhebung der „Zugehörigkeit zu einer Religionsgemeinschaft“ angesehen. Ich habe darauf hingewiesen, dass es

sich bei diesem äußerst sensiblen Erhebungsmerkmal schon nach der Verordnung (EG) Nr. 763/2008 des Europäischen Parlaments und des Rates vom 09.07.2008 über Volks- und Wohnungszählungen nicht um ein Pflichtmerkmal handelt. Überdies hatte das Europäische Parlament in seiner Sitzung vom 20.02.2008 mit überwältigender Mehrheit dafür gestimmt, die von der Europäischen Kommission vorgeschlagene freiwillige Abfrage bestimmter sensibler Merkmale - dazu zählte u.a. die Religionszugehörigkeit - vollständig zu streichen. Bereits vor diesem europarechtlichen Hintergrund erschien mir die im Referentenentwurf vorgesehene verpflichtende Angabe der Religionszugehörigkeit als nicht hinnehmbar. Erfreulicherweise ist die Erhebung des Merkmals „Zugehörigkeit zu einer Religionsgemeinschaft“ im Gesetzentwurf der Bundesregierung nicht mehr vorgesehen.

- Im Gegensatz zur letzten Volkszählung 1987 sollten sodann nach dem Referentenentwurf personenbezogene Erhebungen auch in sensiblen Sonderbereichen vorgenommen werden. Noch in der Begründung des Zensusvorbereitungsgesetzes 2011 war allerdings insoweit eine anonyme Erhebung angekündigt worden.

  Begründet wurde die personenscharfe Erhebung nun mit der Fehleranfälligkeit einer nur summarischen Erfassung. Der von Seiten der Statistik befürchtete Fehler bei einer Beibehaltung der bei der letzten Volkszählung durchgeführten anonymen Erhebung dürfte sich allerdings in der Praxis nicht als besonders gravierend herausstellen. Darüber hinaus vermag mich auch insbesondere der Hinweis auf die Bedeutung der Einwohnerzahlermittlung für die Gemeinden im Zusammenhang mit dem kommunalen Finanzausgleich nicht zu überzeugen. Es ist zum einen zu berücksichtigen, dass wohl kein Zensus die buchhalterisch exakte Ermittlung der Wohnbevölkerung in vertiefter regionaler Gliederung leisten kann, zum anderen, dass die amtlichen Einwohnerzahlen im Rahmen des Finanzausgleichs nur Messgrößen darstellen.

  Als Sonderbereiche gelten Gemeinschafts-, Anstalts- und Notunterkünfte, Wohnheime und ähnliche Unterkünfte. Ich habe angeregt zu prüfen, ob es nicht möglich ist, nur in wenig sensiblen Sonderbereichen, wie z.B. Studentenwohnheimen, die derzeit vorgesehene personenscharfe Erhebung durchzuführen, in sensiblen Sonderbereichen, wie z.B. bestimmten Heimen und Justizvollzugsanstalten, es aber bei einer summarischen Erfassung zu belassen.

  Zwar hat das Staatsministerium des Innern erfreulicherweise meine Argumente aufgegriffen. Der von der Bundesregierung beschlossene Gesetzentwurf sieht jedoch bedauerlicherweise nach wie vor eine personenscharfe Erhebung in Sonderbereichen vor.

Aus datenschutzrechtlicher Sicht werde ich auch weiterhin die Vorbereitung und die Durchführung der Volkszählung 2011 kritisch begleiten.

# 24 Spezielle datenschutzrechtliche Themen

## 24.1 Musterablaufplan für das datenschutzrechtliche Freigabeverfahren

Sowohl der erstmalige Einsatz als auch wesentliche Änderungen von automatisierten Verfahren, mit denen personenbezogene Daten verarbeitet werden, bedürfen - von wenigen Ausnahmen abgesehen - der vorherigen schriftlichen Freigabe durch den behördlichen Datenschutzbeauftragten der das Verfahren einsetzenden öffentlichen Stelle (Art. 26 BayDSG).

Im Rahmen meiner Beratungstätigkeit hat sich das praktische Bedürfnis gezeigt, die einzelnen Schritte auf dem Weg zur datenschutzrechtlichen Freigabe übersichtlich und leicht nachvollziehbar darzustellen. Deshalb habe ich gemeinsam mit dem Staatsministerium der Finanzen einen Musterablaufplan für das datenschutzrechtliche Freigabeverfahren entwickelt, der als Hilfestellung für alle dem Bayerischen Datenschutzgesetz unterfallenden öffentlichen Stellen gedacht ist.

Der Musterablaufplan kann auf meiner Homepage www.datenschutz-bayern.de in der Rubrik „Verwaltung“ unter „Allgemeines“ abgerufen werden.

## 24.2 Bayerisches Geodateninfrastrukturgesetz

Bereits seit einiger Zeit wird von den Datenschutzbeauftragten des Bundes und der Länder die Frage diskutiert, wie georeferenzierte Daten (Daten mit direktem oder indirektem Bezug zu einem bestimm-

ten Standort oder geografischen Gebiet) aus datenschutzrechtlicher Sicht zu bewerten sind. In diesem Zusammenhang ist insbesondere zu klären,

- wann es sich um personenbezogene bzw. -beziehbare Daten handelt,
- inwieweit ein Anspruch Privater auf öffentliche Geodaten besteht,
- ob es sich um Daten aus allgemein zugänglichen Quellen handelt,
- wann ein berechtigtes Interesse an der Nutzung von georeferenzierten Daten angenommen werden kann.

Diese Fragestellungen haben nunmehr hohe Aktualität dadurch erlangt, dass derzeit vom Bund und von verschiedenen Ländern die Umsetzung der Richtlinie 2007/2/EG des Europäischen Parlaments und des Rates zur Schaffung einer Geodateninfrastruktur in der Europäischen Union (INSPIRE) in nationales Recht - zeitlich außerordentlich forciert - vorangetrieben wird. Ziel der INSPIRE-Richtlinie ist es, den Zugang zu und die Nutzung von Geodaten für Bürger, Verwaltung und Wirtschaft europaweit zu vereinfachen. Auf Bundesebene ist hier der Entwurf für ein Gesetz über den Zugang zu digitalen Geodaten (Geodatenzugangsgesetz-Entwurf) zu nennen. Auf Länderebene ist der Freistaat Bayern als erstes Land bereits der europarechtlichen Umsetzungsverpflichtung nachgekommen: das Bayerische Geodateninfrastrukturgesetz (BayGDIG) ist am 01.08.2008 in Kraft getreten. Diesem Gesetz liegen die „Musterempfehlungen für die Geodateninfrastrukturgesetzgebungen in den Ländern“ zugrunde, die die von den Ländern eingesetzte Arbeitsgruppe „Geodateninfrastrukturgesetz“ aus Vertretern der Länder Bayern, Berlin, Hessen, Niedersachsen, Sachsen, Sachsen-Anhalt und Thüringen sowie der kommunalen Spitzenverbände unter Federführung Bayerns erarbeitet hat.

Sowohl bei den „Musterempfehlungen“ als auch beim Bayerischen Geodateninfrastrukturgesetz habe ich mich für eine datenschutzgerechte Fassung eingesetzt. So konnte ich in Verhandlungen mit dem innerhalb der Staatsregierung federführenden Staatsministerium der Finanzen an mehreren Stellen des Bayerischen Geodateninfrastrukturgesetzes Verweisungen auf das Bayerische Datenschutzgesetz erreichen, sodass im Ergebnis von einem „zweistufigen datenschutzrechtlichen Schutzkonzept“ gesprochen werden kann. Ich sehe darin einen großen Schritt zu einem angemessenen Ausgleich zwischen den berechtigten Interessen der Nutzer von Geodaten einerseits und den schutzwürdigen Belangen der Betroffenen andererseits.

Im Einzelnen konnte ich vor allem folgende Verbesserungen erreichen:

- Bereits die Bereitstellung von Geodaten und Geodatendiensten an das Geoportal hat nach Art. 8 Abs. 4 Satz 1 BayGDIG unter Beachtung der im Bayerischen Datenschutzgesetz und im Bundesdatenschutzgesetz festgelegten Grundsätze des Schutzes personenbezogener Daten zu erfolgen.
- Sodann ist der Zugang der Öffentlichkeit zu Geodaten nach Art. 11 Abs. 2 Satz 2 Nr. 1 BayGDIG zu beschränken, soweit dadurch personenbezogene Daten offenbart und schutzwürdige Interessen der Betroffenen beeinträchtigt würden. Ausnahmen sind nur zulässig, wenn die Betroffenen zugestimmt haben oder das öffentliche Interesse an dem Zugang die schutzwürdigen Interessen der Betroffenen überwiegt.
- Vor der Entscheidung über die Offenbarung personenbezogener Daten sind die Betroffenen gem. Art. 11 Abs. 2 Satz 3 BayGDIG anzuhören.
- Auch beim Zugang von bayerischen Behörden sowie entsprechenden Stellen der Länder, des Bundes, der Kommunen und anderer Mitgliedstaaten der Europäischen Gemeinschaft sowie von Organen und Einrichtungen der Europäischen Gemeinschaft zu Geodaten sind die im Bayerischen Datenschutzgesetz und im Bundesdatenschutzgesetz festgelegten Grundsätze des Schutzes personenbezogener Daten zu beachten (Art. 11 Abs. 3 Satz 2 i.V.m. Art. 8 Abs. 4 BayGDIG).
- Darüber hinaus stellt Art. 4 Abs. 3 Satz 2 BayGDIG nunmehr ausdrücklich klar, dass die Bestimmungen zum Schutz öffentlicher und sonstiger - hier vor allem datenschutzrechtlicher - Belange nach Art. 11 BayGDIG nicht nur für die Referenzversionen der Geodaten, sondern auch für identische Kopien der gleichen Geodaten bei verschiedenen Behörden gelten.
- Im Übrigen unterliegen die bei den Verwaltungsbehörden der Unterstufe und den Gemeinden vorhandenen Geodaten dem Bayerischen Geodateninfrastrukturgesetz nur, wenn ihre elektronische Sammlung und Verbreitung rechtlich vorgeschrieben und nicht datenschutz- oder urheberrechtlich eingeschränkt ist (Art. 4 Abs. 6 BayGDIG).

Die Umsetzung des Bayerischen Geodateninfrastrukturgesetzes in der Praxis werde ich aufmerksam beobachten.

# 25 Technischer und organisatorischer Bereich

## 25.1 Sicherheit bei Internetanwendungen und Servern

Fast jede Behörde oder öffentliche Stelle hat einen eigenen Internetauftritt, der mehr oder weniger wichtig für die Erfüllung der Aufgaben und für die Information der Öffentlichkeit ist. Unter Umständen fließt viel Arbeit und Geld in die Inhalte und deren Präsentation. Aktuelle Statistiken und auch meine Prüfungen zeigen mir, dass es bei einem Großteil der Betreiber von Webauftritten aber keine großen Anstrengungen gibt, die Sicherheit der Server und der Anwendungen darauf zu gewährleisten.

Ich weise darauf hin, dass es im Internet eine Vielzahl von unter Umständen leicht zu findenden Programmen gibt, die es jedem mehr oder weniger begabten Angreifer ermöglichen, Zugriff auf einen nicht ausreichend geschützten Server zu nehmen. Der Zugriff kann von einem unbefugten Verändern der Seiten über das Zerstören der Daten bis hin zum Missbrauch des Servers für weitere Angriffe reichen.

In meinen Prüfungen ist aufgefallen, dass grundlegende Sicherheitsrichtlinien nicht beachtet werden. Zum Teil sind seit Jahren keine Sicherheitslücken durch Programmaktualisierungen (Patches) geschlossen worden. Es laufen Dienste auf den Servern, von denen der Betreiber nicht weiß, warum diese laufen und dass diese aus dem Internet erreichbar sind.

Um eine Grundsicherung eines Webservers zu erreichen, sind mindestens die folgenden Anforderungen zu erfüllen:

- alle aktuellen Sicherheitspatches werden zeitnah eingespielt
- es sind keine unbenötigten Dienste aus dem Internet zu erreichen
- Logins und Passwörter für den Zugriff sind sicher gewählt
- die Webanwendungen werden regelmäßig auf neue Sicherheitsbedrohungen überprüft
- bei der Entwicklung wurde auf grundlegende Sicherheitsanforderungen geachtet
- in regelmäßigen Zeitabständen wird die Sicherheit des Servers geprüft (z.B. Protokolldateien, offene Ports, unbefugte Veränderungen im Dateisystem)

Ein Server im Internet ist keine einmalige Investition, sondern benötigt im laufenden Betrieb ständig Ressourcen, die sich um die Sicherheit kümmern. Dies kann sowohl durch eigenes Personal als auch durch geeignete Dritte erfolgen. Bei der Konzeption neuer Internetdienste ist bereits auf die langfristige sicherheitstechnische Wartung zu achten.

## 25.2 IP-Protokollierung auf Webservern

Im Urteil des Amtsgerichts Berlin-Mitte vom 27.03.2007 (Az. 5 C 314/06) im Verfahren einer Privatperson gegen die Bundesrepublik Deutschland, vertreten durch das Bundesministerium der Justiz, wurde in Bezug auf den Internetauftritt http://www.bmj.bund.de dem Kläger Recht gegeben, dass eine Speicherung von personenbezogenen Daten, hier die Speicherung der dynamischen IP-Adresse des Klägers, auf dem Webserver des Internetauftritts nicht zulässig ist, auch dann nicht, wenn dies aus Sicherheitsgründen lediglich für 14 Tage vorgenommen wird. Das Landgericht Berlin hat am 06.09.2007 (Az. 23 S 3/07) in der Berufung das Urteil grundsätzlich bestätigt, aber darauf hingewiesen, dass es sich um eine Einzelfallentscheidung in einer Sonderkonstellation handelt.

Die Zulässigkeit der Speicherung von IP-Adressen beim Aufruf von Web-Seiten bayerischer Behörden und öffentlicher Einrichtungen richtet sich nach § 15 Telemediengesetz (TMG). Danach ist die Erhebung personenbezogener Daten nur zur Ermöglichung der Inanspruchnahme von Telemedien, zu Zwecken der Abrechnung oder dann zulässig, wenn Anhaltspunkte dafür bestehen, dass entgeltliche Leistungen nicht oder nicht vollständig vergütet werden sollen. Damit wird grundsätzlich die Speicherung von IP-Adressen für andere Zwecke untersagt, da sie unter Umständen einem bestimmten Nutzer zugeordnet werden können und damit personenbezogene Daten sind.

Aus Sicherheitsgründen kann aber nach Art. 7 BayDSG (vgl. 4.3.2 meiner Orientierungshilfe zu Datenschutzfragen des Anschlusses von Netzen der öffentlichen Verwaltung an das Internet, abrufbar unter http://www.datenschutz-bayern.de) eine Protokollierung erforderlich sein. Es ist daher eine Speicherung der IP-Adresse als technische Vorkehrung zum Schutz der Datenverarbeitungssysteme gegen unerlaubte Zugriffe zulässig.

Auf Grund des oben Genannten halte ich eine Protokollierung personenbezogener Daten auf einem Webserver einer bayerischen Behörde, insbesondere der IP-Adresse eines Besuchers der Websiten, für nicht zulässig. Auf Sicherheitsinstanzen, wie etwa einer vor dem Webserver geschalteten Firewall, kann unter Zweckbindung aus Gründen der IT-Sicherheit für den Zeitraum von sieben Tagen auch die IP-Adresse protokolliert werden. Sollten für die Fehlersuche oder die Erstellung von Statistiken Protokolldaten eines Webservers benötigt werden, so sind diese ausrei-

chend zu anonymisieren. Eine Verkürzung der IPv4-Adresse um das letzte Segment ist hier ausreichend.

Bei den zur Zeit am häufigsten verwendeten Webserver-Softwarekomponenten findet sich in der Standardkonfiguration eine vollständige Protokollierung aller Daten bei einem Zugriff auf die Websiten. Es ist darauf zu achten, dass hier zumindest die Verkürzung der Besucheradressen vor einer Inbetriebnahme des Angebots aktiviert wird. Detaillierte Anleitungen und Softwarekomponenten für den Apache und den Microsoft Internet Information Web Server zur Anonymisierung der IP-Adressen in den jeweiligen Protokolldateien finden Sie auf den Seiten des Sächsischen Datenschutzbeauftragten unter http://www.saechsdsb.de/ipmask.

### 25.3 Geltungsbereich der Vorratsdatenspeicherung für Behörden

Nach § 113a Telekommunikationsgesetz (TKG) ist jeder, der öffentlich zugängliche Telekommunikationsdienste für Endnutzer erbringt, verpflichtet, von diesem bei der Nutzung seines Dienstes erzeugte oder verarbeitete Verkehrsdaten sechs Monate zu speichern. Gestattet ein Dienstherr beispielsweise die private Nutzung von Internet und E-Mail in seiner Behörde, so ist er als Telekommunikationsanbieter im Sinne des TKG zu sehen und somit wäre auch hier auf den ersten Blick eine Speicherpflicht über sechs Monate für die Verbindungsdaten der Beschäftigten gegeben.

Allerdings ist im Sinne des § 113a Absatz 1 Satz 1 TKG ein Öffentlichkeitsbezug des Angebotes erforderlich, der bei behördeninternen Diensten jedoch nicht gegeben ist. In der Gesetzesbegründung zu § 113a TKG findet man, „... dass für den nicht öffentlichen Bereich (z.B. unternehmensinterne Netze, Nebenstellenanlagen oder E-Mail-Server von Universitäten ausschließlich für ... Bedienstete ...) eine Speicherungspflicht nicht besteht...“.

Aus § 113a TKG lässt sich somit weder eine Protokollierungspflicht noch eine Erlaubnis zur Protokollierung von Verkehrsdaten für Behörden ableiten. Da auch die Teilnahme am bayerischen Behördennetz nicht für die Öffentlichkeit zugänglich ist, gilt dies auch für die Protokollierung innerhalb und an den Internetübergängen des Behördennetzes.

### 25.4 Erkenntnisse aus Prüfungen

#### 25.4.1 Geprüfte Einrichtungen

Im Berichtszeitraum habe ich bei folgenden Dienststellen die Einhaltung der gebotenen technischen und organisatorischen Datensicherheits- und Datenschutzmaßnahmen überprüft:

- BRK Kreisverband München
- Institut für Medizinmanagement und Gesundheitswissenschaften der Universität Bayreuth
- Integrationsamt des Zentrum Bayern Familie und Soziales in Bayreuth und München
- Klinik und Poliklinik für Psychiatrie und Psychotherapie des Universitätsklinikums München
- Kreiskrankenhaus St. Elisabeth Dillingen
- MDK Bayern
- Passbehörde der Stadt Landshut
- Passbehörde der Stadt Nürnberg
- Passbehörde der Stadt Starnberg
- Passbehörde der Gemeinde Vogtareuth
- Reha-Klinik der Deutschen Rentenversicherung Bayern Süd in Bad Reichenhall
- Städtisches Krankenhaus Rosenheim

#### 25.4.2 Beschriftung von Etiketten in Reha-Kliniken

Die Prüfung einer Reha-Klinik der Deutschen Rentenversicherung Bayern Süd hat gezeigt, dass dort die Patientenetiketten standardmäßig mit dem Namen, Geburtsdatum, Rentenversicherungs-Nummer, Zimmernummer und dem ICD-10 Code der Krankheit beschriftet sind. Diese Etiketten werden für alle Unterlagen und Probenbehälter im Haus, aber auch für den Versand an externe Labore verwendet.

Die Etiketten sind zumeist gut sichtbar auf der Außenseite von Unterlagen und Behältnissen angebracht. Dadurch können unbefugte Personen relativ einfach und auch unabsichtlich Kenntnis von medizinischen personenbezogenen Daten erlangen.

Der Abdruck des ICD-10 Codes auf dem Etikett ist in weiten Teilen nicht erforderlich, da das behandelnde Personal Zugriff auf die Patientenakte und im Bedarfsfall damit detailliertere Informationen zur Erkrankung des Patienten hat.

Der ICD-10 Code ist daher von den Etiketten zu entfernen. Soweit er nach Prüfung in einzelnen Bereichen benötigt wird, können hierfür gesonderte

Etiketten verwendet werden, die jedoch nicht für die anderen Bereiche genutzt werden dürfen.

Zur grundsätzlichen Frage der Beschriftung von Proben im Krankenhaus und auch bei Versand an externe Labore gibt der Beitrag zu Biomaterialien in meinem letzten Tätigkeitsbericht Auskunft (vgl. Nr. 23.5.3, 22. TB).

### 25.4.3 Löschen der E-Mail-Konten ausgeschiedener Mitarbeiter

Bei vielen öffentlichen Stellen herrscht Unklarheit darüber, wie mit den E-Mail-Konten ausgeschiedener Mitarbeiter zu verfahren ist. Ich empfehle hierzu folgende Verfahrensweise:

Auch nach Ausscheiden eines Mitarbeiters ist es durchaus sinnvoll, dessen E-Mail Account noch einige Zeit weiter „leben“ zu lassen, da nicht ausgeschlossen ist, dass noch wichtige dienstliche Mails an diese Adresse gesandt werden. Als angemessen kann hierfür ein Zeitraum von drei bis sechs Monaten angenommen werden. So lange der Account besteht, müssen auch weiterhin eingehende E-Mails an den Mitarbeiter angenommen und dürfen nicht gelöscht oder zurückgesandt werden.

Der zuständige Systembeauftragte sollte daher auf dem Server die für einen ausgeschiedenen Mitarbeiter eingehenden dienstlichen E-Mails an dessen Nachfolger oder Vertreter weiterleiten. War dem ausgeschiedenen Mitarbeiter auch die private E-Mail-Nutzung gestattet, so sind offensichtlich private E-Mails so weit möglich an den Mitarbeiter weiterzuleiten oder zu speichern. In jedem Fall sollte der Absender darüber informiert werden, dass der Mitarbeiter nicht mehr über diese E-Mail-Adresse zu erreichen ist.

Das Löschen oder Zurücksenden der E-Mails kann bei einer gestatteten privaten Nutzung wegen unzulässiger Datenveränderung sowie wegen Eingriffs in das Fernmeldegeheimnis strafbar sein, es sei denn der ausgeschiedene Mitarbeiter hat hierzu vorab schriftlich sein Einverständnis erklärt.

### 25.4.4 Datenschutzgerechter Einsatz von Outlook auf den Clients

Wurde Microsoft Outlook früher ausschließlich als E-Mail-Client eingesetzt, dient das Produkt heutzutage als Schaltzentrale für die komplette Verwaltung der Nachrichten, Termine, Kontakte, Aufgaben und vieler weiterer Informationen auf den Arbeitsplatzrechnern. Da dabei (z.T. sensible) personenbezogene Daten verarbeitet werden und Outlook Komponenten umfasst, die sowohl den Dialog über das Internet als auch die gemeinsame Nutzung von Daten ermöglichen, müssen strenge Anforderungen an die zu ergreifenden Datenschutz- und Datensicherheitsmaßnahmen beim Einsatz von Outlook gestellt werden.

Auf die Bekämpfung von Schadenssoftware (in Zusammenhang mit dem E-Mail-Verkehr) habe ich schon häufiger hingewiesen, so dass ich an dieser Stelle darauf verzichte und stattdessen auf weitere wesentliche Schutzmaßnahmen eingehe.

Häufig bleibt es dem Anwender selbst überlassen zu entscheiden, welche Funktionen von Outlook er zu welchem Zweck nutzen möchte. Dies führt aber in der Regel zu erheblichen Sicherheitsdefiziten, da dem Benutzer schlichtweg die Kenntnis über und das Verständnis für die zu ergreifenden Sicherheitsmaßnahmen fehlt. Deshalb ist jede Behörde gut beraten, genau zu regeln, für welche Zwecke Outlook eingesetzt werden soll. Danach sind die zu ergreifenden Sicherheitsmaßnahmen verbindlich festzulegen.

Zur Vermeidung von Fehlbedienungen und zur Gewährleistung der Einhaltung der vorgegebenen Outlook-Richtlinien sollte eine entsprechende Benutzerschulung erfolgen.

Viele Outlook-Nutzer vertrauen darauf, dass sie einen alleinigen Zugriff auf ihren PC und die darauf gespeicherten Daten besitzen und sehen daher beispielsweise keine Notwendigkeit, ihre persönlichen Outlook-Ordner gegen einen unberechtigten Zugriff abzusichern. Dies ist aber ein Trugschluss, da zum einen die Outlook-Dateien in der Regel auf einem Netzlaufwerk gespeichert sind und zum anderen zumindest der Systemadministrator auch auf lokale Speichermedien zugreifen kann. Daher sind alle Anwender dazu anzuhalten, ihre persönlichen Outlook-Ordner gegen einen unberechtigten Zugriff mittels Passwort zu schützen, auch wenn dieser von Outlook angebotene Kennwortschutz relativ leicht mit entsprechenden Tools - die z.B. über das Internet beziehbar sind - ausgehebelt werden kann. Sensible Daten sollten daher nur verschlüsselt abgespeichert werden.

Eine Kennwortvergabe kann auch geschehen, während Outlook bereits aktiv ist. Das Kennwort kann alle Zeichen (inkl. Leerzeichen) enthalten und bis zu 15 Stellen lang sein. Dabei wird zwischen Groß- und Kleinschreibung unterschieden. Ab Outlook XP kann das Passwort über die Funktion „Datei/Datendateiverwaltung/Einstellungen/Kennwort ändern“ vergeben und geändert werden. Auf diese Weise kann also sowohl ein neues Kennwort vergeben als auch ein bereits bestehendes geändert werden.

Auch im Rahmen des Zugriffs auf den Mail-Server sollte der Benutzer gezwungen werden, sich mittels Benutzernamen und Passwort zu identifizieren und zu authentifizieren. Dabei ist darauf zu achten, dass das

Kontrollkästchen „Kennwort speichern“ deaktiviert ist, da sonst das Passwort ausgelesen werden kann.

Für den Fall einer (un)vorhersehbaren Abwesenheit vom Arbeitsplatz sind die Mitarbeiter häufig dazu angehalten, so genannte Stellvertreter im Outlook einzurichten, die im Bedarfsfall auf die persönlichen Ordner des Abwesenden auf dem Exchange-Server zugreifen können. Diese Zugriffsberechtigungsvergabe muss allerdings sehr restriktiv und revisionsfähig erfolgen. Zusätzlich sind die Rechte und Pflichten eines Stellvertreters detailliert in einer entsprechenden Dienstanweisung zu regeln. So sind beispielsweise alle Mitarbeiter im Rahmen dieser Anweisung darauf hinzuweisen, dass sie in der Rolle eines „Stellvertreters“ nicht dazu berechtigt sind, offensichtlich private E-Mails des Postfachinhabers zu öffnen. Stellt sich der Privatbezug erst nach Öffnung einer entsprechenden E-Mail heraus, so haben sie unverzüglich diese E-Mail wieder zu schließen. Außerdem ist die Ausübung der Stellvertreterfunktion während der Anwesenheit des Besitzers des Postfaches zu untersagen. Die Vorgehensweise bei der Einrichtung der Vertreterfunktion sollte auch Bestandteil einer Vereinbarung mit der Arbeitnehmervertretung sein.

Im Rahmen der Einrichtung von Stellvertretern müssen auch Maßnahmen ergriffen werden, um schützenswerte (private) Einträge auch von deren Zugriff auszunehmen. So ist jeder Anwender anzuweisen, schützenswerte (private) Einträge manuell und nicht automatisch zu erzeugen und mit „privat“ zu kennzeichnen. Dadurch werden beispielsweise Termine anderen Personen, denen ein Zugriff auf den betreffenden Ordner eingeräumt ist, nur in der Form angezeigt, dass die Zeiten als vergeben markiert sind. Es werden aber weder Titel noch nähere Erläuterungen eines entsprechenden Eintrags angezeigt, es sei denn, die Einsichtnahme in private Termine wurde vom Betroffenen freigegeben. Eine weitere Schutzmöglichkeit besteht darin, private Termine in einem Unterordner des Ordners „Kalender“ abzuspeichern, der nicht für andere Mitarbeiter freigegeben wird. Dadurch können zwar andere Beschäftigte Zugriff auf die (dienstlichen) Termine des Hauptordners bekommen, der Zugriff auf den Unterordner wird ihnen jedoch verwehrt. Der sicherste Schutz vor einem unerwünschten Zugriff auf private Termineinträge besteht darin, einen zusätzlichen Kalenderordner (für die privaten Termine) auf den lokalen Laufwerken (also nicht wie standardmäßig üblich auf dem Exchange-Server) eines Bediensteten in einer so genannten PST-Datei (Persönlicher Ordner) anzulegen und diesen Ordner nicht freizugeben. Damit wird jeglicher Zugriff auf diesen Ordner über das Netzwerk unterbunden. Dies hat allerdings den kleinen Nachteil, dass Zeiten für private Termine im Hauptkalender - soweit sie dort nicht als „nicht verfügbar“ gekennzeichnet werden - für Kollegen, die beispielsweise Besprechungstermine vereinbaren wollen, als „Frei“ angezeigt werden.

Natürlich sind auch bei der Nutzung von Outlook alle über das Internet zu versendenden schutzwürdigen Daten zu verschlüsseln und soweit möglich elektronisch zu signieren. Dies gilt sowohl für E-Mails als auch für deren Anlagen, soweit sie schützenswerte Informationen enthalten.

Standardmäßig können alle E-Mails, die nicht elektronisch signiert sind, vom Empfänger nachträglich geändert werden. Um dies zu verhindern, sollten alle E-Mails mit der Vertraulichkeitsstufe Privat verschickt werden. Auch Änderungen an beigefügten Dokumenten (Attachments) sollten natürlich verhindert werden. Die sicherste Vorgehensweise dazu ist, Anhänge nur mittels Adobe Acrobat im PDF-Format zu erstellen. Bei diesen Dokumenten kann mittels Sicherheitseinstellungen dafür gesorgt werden, dass Dokumente nicht ohne weiteres gedruckt, kopiert oder geändert werden können.

### 25.4.5 Zugriffsbefugnisse des behördlichen Datenschutzbeauftragten

Im Rahmen meiner Prüfungen muss ich immer wieder feststellen, dass dem behördlichen Datenschutzbeauftragten ein Zugriff auf alle Datenbestände seiner öffentlichen Stelle ermöglicht ist. Dies ist aber im Regelfall nicht erforderlich.

Gemäß Art. 26 Absatz 4 des Bayerischen Datenschutzgesetzes (BayDSG) haben behördliche Datenschutzbeauftragte die Aufgabe, auf die Einhaltung des BayDSG und anderer Vorschriften über den Datenschutz in der öffentlichen Stelle hinzuwirken.

Zur Erfüllung dieser Aufgabe können sie die dazu notwendige Einsicht in Dateien und Akten der öffentlichen Stelle nehmen, soweit nicht gesetzliche Regelungen entgegenstehen. Sie dürfen Akten mit personenbezogenen Daten, die dem Arztgeheimnis unterliegen, Akten über die Sicherheitsüberprüfung und nicht in Dateien geführte Personalakten nur mit Einwilligung der Betroffenen einsehen.

Die öffentlichen Stellen sind dazu verpflichtet, den Datenschutzbeauftragten bei der Erfüllung seiner Aufgaben aktiv zu unterstützen und ihm insbesondere, soweit dies zur Erfüllung seiner Aufgaben erforderlich ist, entsprechende Räume, Einrichtungen, Geräte und Mittel zur Verfügung zu stellen. Im Rahmen dieser Unterstützungspflicht sind dem Datenschutzbeauftragten zweifellos auch ein Zutrittsrecht zu Räumen, in denen eine personenbezogene Datenverarbeitung stattfindet, ein Einsichtsrecht in Behördenunterlagen und ein Zugriffsrecht auf personenbezogene Daten einzuräumen.

Nähere Aussagen zum Zugriffsrecht des Datenschutzbeauftragten auf Dateien beinhaltet das BayDSG nicht. Der einzige Gesetzesvorbehalt beruht damit darin, dass die Einsicht zur Erfüllung seiner Aufgaben erforderlich sein muss. Was der Begriff „erforderlich“ in diesem Zusammenhang bedeutet, ist gesetzlich nicht näher definiert.

So gibt es lediglich einen Beschluss des Bundesarbeitsgerichts vom 11.11.1997 (1 ABR 21/97), der dem betrieblichen Datenschutzbeauftragten die Kontrollrechte bei der Personalvertretung (und damit auch den Zugriff auf deren Dateien) versagt. Strittig sind weiterhin generelle Zugriffsrechte auf Personal-, Steuer- und Geheimdaten. Unter Beachtung des Verhältnismäßigkeitsprinzips kann dem Datenschutzbeauftragten aber sicherlich nicht das Kontrollrecht im Einzelfall versagt werden.

Ein Einsichtsrecht besteht ferner nicht bei entgegenstehenden gesetzlichen Regelungen.

Zusammenfassend ist dem behördlichen Datenschutzbeauftragten zwar kein genereller Zugriff auf alle Dateien einer öffentlichen Stelle, sehr wohl aber der Zugriff im konkreten Einzelfall zu ermöglichen.

### 25.4.6 Hinweise zur datenschutzrechtlichen Freigabe und zur Führung des Verfahrensverzeichnisses

Im Rahmen meiner Prüfungen muss ich leider noch immer feststellen, dass viele öffentliche Stellen entweder gar kein Verfahrensverzeichnis führen oder die darin beinhalteten Verfahrensbeschreibungen nicht den gesetzlichen Anforderungen entsprechen.

Gemäß Art. 26 Abs. 1 Satz 1 BayDSG bedarf der erstmalige Einsatz von automatisierten Verfahren, mit denen personenbezogene Daten verarbeitet werden, der vorherigen schriftlichen Freigabe durch die das Verfahren einsetzende öffentliche Stelle.

Die Freigabe dieser Verfahren erfolgt durch die behördlichen Datenschutzbeauftragten der öffentlichen Stellen, soweit es sich nicht um Verfahren der AKDB oder um Verfahren für öffentliche Stellen des Freistaates Bayern handelt, welche durch das fachlich zuständige Staatsministerium oder die von ihm ermächtigte öffentliche Stelle für den landesweiten Einsatz datenschutzrechtlich freigegeben worden sind (Art. 26 Abs. 3 Satz 2 BayDSG). Dabei ist zu beachten, dass diese ministerielle Freigabe nicht für Kommunen gilt. Diese müssen ein entsprechendes Verfahren selbst freigeben.

Viele öffentliche Stellen sind sich bezüglich der Frage, ob ein Verfahren freigegeben werden muss, nicht bewusst, was alles unter den Begriff „personenbezogene Daten“ fällt. Gemäß Art. 4 Abs. 1 BayDSG sind personenbezogene Daten

- Einzelangaben
- über persönliche oder sachliche Verhältnisse
- bestimmter oder bestimmbarer
- natürlicher Personen (Betroffene).

Zu den Einzelangaben über persönliche oder sachliche Verhältnisse gehören natürlich auch der Name und die Anschrift natürlicher Personen (Menschen). Ist eine E-Mail-Adresse eindeutig einer natürlichen Person zuordenbar, so fällt auch sie unter den Begriff personenbezogene Daten. Nicht darunter fallen jedoch E-Mail-Adressen, die nicht eindeutig einer bestimmen Person zuordenbar sind (z.B. poststelle@datenschutz-bayern.de).

Damit sind grundsätzlich auch Verfahren freizugeben, die lediglich eines der oben angeführten personenbezogenen Daten beinhalten, soweit es sich nicht um ein Verfahren handelt, das gemäß § 2 der Datenschutzverordnung (DSchV) keiner Freigabe bedarf. Dies wird aber häufig missachtet.

Ein Verfahren ist gemäß der Begründung zu Art. 18 EG-Datenschutzrichtlinie ein Bündel von Verarbeitungen, die über eine vom Verantwortlichen definierte Zweckbestimmung verbunden sind. Ein Verfahren kann somit aus mehreren einzelnen Verarbeitungen bzw. Verarbeitungsgruppen bestehen.

Ein „automatisiertes Verfahren“ bzw. die „automatisierte Verarbeitung“ umfasst analog zu § 3 Abs. 2 BDSG

- die Erhebung, Verarbeitung oder Nutzung personenbezogener Daten

- unter Einsatz von Datenverarbeitungsanlagen.

Der Begriff „Datenverarbeitungsanlage“ wird gesetzlich nicht näher definiert. Wesentlich erscheint jedoch, dass ein bestimmter Vorgang programmgesteuert abläuft. Das Verarbeitungsmittel selbst (Großrechner, PC, etc.) ist demgegenüber gleichgültig.

Nach Art. 26 Abs. 3 Satz 1 1. Halbsatz BayDSG haben öffentliche Stellen ihren behördlichen Datenschutzbeauftragten rechtzeitig vor dem Einsatz oder der wesentlichen Änderung eines automatisierten Verfahrens eine Verfahrensbeschreibung mit den in Abs. 2 aufgeführten Angaben zur Verfügung zu stellen, damit dieser entscheiden kann, ob er eine datenschutzrechtliche Freigabe für dieses Verfahren erteilt.

Da es sich hierbei nur um gesetzlich vorgeschriebene Mindestanforderungen handelt, können diese Angaben natürlich noch um weitere, als erforderlich angesehene Angaben ergänzt werden.

Gemäß Art. 27 Abs. 1 BayDSG führen die behördlichen Datenschutzbeauftragten ein Verzeichnis der bei der öffentlichen Stelle eingesetzten und datenschutzrechtlich freigegebenen automatisierten Verfahren, mit denen personenbezogene Daten verarbeitet werden.

In diesem Verzeichnis sind nach Art. 27 Abs. 2 BayDSG für jedes automatisierte Verfahren die in Art. 26 Abs. 2 BayDSG genannten Angaben fest zu halten.

Das Verfahrensverzeichnis kann gemäß Art. 27 Abs. 3 Satz 1 BayDSG von jedem kostenfrei eingesehen werden, soweit es sich dabei nicht um öffentliche Stellen handelt, die gemäß Art. 27 Abs. 3 Satz 2 BayDSG von der Verpflichtung zur Gewährung der Einsichtnahme ausgenommen sind.

Der Begriff „von jedem“ ist weit zu fassen, darunter fällt nicht nur der Betroffene. Somit muss ein Verfahrensverzeichnis geführt werden, das auf Wunsch auch ohne Nachweis eines berechtigten Interesses eingesehen werden kann.

Unter die Möglichkeit der Einsichtnahme fallen nicht nur schriftliche Auskünfte. Denkbar ist auch eine mündliche Auskunft oder die Möglichkeit zur Einsichtnahme vor Ort. Die Einsichtnahme kann auch durch Übergabe einer Kopie der ausgefüllten Verfahrensbeschreibungen an den Interessierten ermöglicht werden. Auch eine Veröffentlichung des Verfahrensverzeichnisses im Internet ist denkbar, damit ein jeder Interessierter online darauf zugreifen kann. Allerdings besteht meines Erachtens keine Verpflichtung dazu, das Verfahrensverzeichnis einem Interessierten zuzusenden, wenn er es auch auf andere Weise zur Kenntnis nehmen kann. Es sollte außerdem darauf geachtet werden, dass das öffentliche Verfahrensverzeichnis einerseits hinreichend aussagekräftige Informationen über die Verfahren gibt, andererseits auch nicht zu detailliert ist, damit keine Behördeninterna bekannt werden. So sind die gemäß Art. 26 Abs. 3 Satz 1 2. Halbsatz dem behördlichen Datenschutzbeauftragten zur Verfügung zu stellenden Angaben zu den Sicherheitsmaßnahmen und den zugriffsberechtigten Personen nicht in das öffentliche Verfahrensverzeichnis aufzunehmen. Der Umfang des Verfahrensverzeichnisses wird in Art. 27 Abs. 2 i.V.m. Art. 26 Abs. 2 BayDSG abschließend geregelt.

Die Einsichtnahme hat in der Regel kostenfrei zu erfolgen.

Bezüglich der Beweislast hinsichtlich des vermuteten Einsatzes der automatisierten Verarbeitung personenbezogener Daten bei einer öffentlichen Stelle und damit dem Recht der Einsichtnahme enthält das BayDSG keine Angaben. Generell kann jedoch wohl davon ausgegangen werden, dass jede öffentliche Stelle eine derartige Verarbeitung durchführt.

Ein Mustervordruck zur Verfahrensbeschreibung ist auf meiner Homepage (www.datenschutz-bayern.de) im Bereich Technik/Orientierungshilfen/Mustervorlagen abrufbar. Dabei handelt es sich lediglich um ein Muster, so dass natürlich auch andere und auch selbst erstellte Schemata zur Verfahrensbeschreibung genutzt werden können, soweit sie den Anforderungen des Art. 26 Abs. 2 BayDSG entsprechen.

### 25.4.7 Entsorgung von Datenträgern mit personenbezogenem Inhalt

Obwohl ich in fast jedem meiner Tätigkeitsberichte auf die Pflicht zur datenschutzgerechten Entsorgung von Datenträgern mit personenbezogenem Inhalt hinweise, muss ich leider immer wieder feststellen, dass gerade in diesem Bereich viel Unwissenheit vorherrscht. Daher nochmals einige diesbezügliche Hinweise:

Werden personenbezogene Daten auf Datenträger jeglicher Art (also egal ob es sich um Papierunterlagen, magnetische, optische oder elektronische Datenträger handelt) gespeichert und werden diese nicht mehr benötigt, so sind sie datenschutzgerecht zu vernichten. Die Art der Vernichtung hängt dabei von der Art des Datenträgers ab.

Gemäß DIN 33858 bezeichnet der Begriff „Vernichten“ das Löschen der auf einem Datenträger aufbewahrten Daten in der Art, dass ihre Reproduktion unmöglich ist oder weitgehend erschwert wird. Die Vernichtung erfolgt in der Regel durch Zerkleinerung oder Stoffumwandlung.

Bei der Vernichtung von Datenträgern ist zu beachten, dass die Anforderungen an technische und organisatorische Maßnahmen bei der Vernichtung von Datenträgern umso höher sein müssen, je höher die Sensibilität der Daten ist. Dabei können die Festlegungen zur Informationsdatenträgervernichtung (insbesondere für Papierunterlagen) bei unterschiedlichen Sicherheitsstufen in der DIN-Norm 32757 Teil 1 und Teil 2 als Anhaltswert herangezogen werden, auch wenn sie keine Rechtsnorm ist.

Der Teil 1 der DIN 32757 beschreibt die Anforderungen an Maschinen und Einrichtungen zum Vernichten von Datenträgern durch Stoffumwandlung oder Verkleinerung (z.B. durch Aktenvernichter) sowie an Prüfmaterial, -verfahren und -zeugnisse.

In Teil 2 der DIN 32757 werden die Mindestangaben für derartige Maschinen und Einrichtungen festgelegt. Abhängig vom Reproduktionsaufwand der zu vernichtenden Daten legt die Norm dazu fünf Sicherheitsstufen (S1-S5) fest. Diese werden zur Klassifizierung der Maschinen und Einrichtungen verwendet und liefern somit eine Aussage über den Vernichtungsgrad in Abhängigkeit von der Art der zu ver-

nichtenden Datenträger. Dabei gilt: Je vertraulicher die zu vernichtenden Unterlagen sind, desto kleiner muss die Schnittgröße sein, d.h. desto höher ist die Sicherheitsstufe.

Als Mindestanforderung an eine datenschutzgerechte Entsorgung personenbezogener Daten ist die Sicherheitsstufe 3 anzusehen. Denn nur bei Vernichtung nach mindestens dieser Stufe sind die Reststücke so klein, dass eine Reproduktion der jeweiligen Informationen nur unter erheblichem Aufwand von Personen, Zeit und Hilfsmittel möglich und die Gefahr dafür gering ist. Die dazu verwendeten Geräte (z.B. Aktenvernichter) müssen der Norm entsprechend gekennzeichnet werden. Keine Rolle spielt dabei, ob es sich um ein mobiles (z.B. auf einem Lkw) oder ein stationäres Gerät handelt.

Die Sicherheitsstufen 1 (allgemeines Schriftgut ohne besondere Vertraulichkeit) und 2 (interne Unterlagen) gelten nur für nicht schützenswertes Schriftgut bzw. Unterlagen, die keiner besonderen Geheimhaltung bedürfen. Ab der Sicherheitsstufe 4 (geheimes Schriftgut) sind leistungsfähige Aktenvernichter in der Regel nicht mehr einsetzbar, da sie nicht den erforderlichen Partikelschnitt bieten können. Für die Sicherheitsstufen 4 und 5 (streng geheim) sind somit nur so genannte Cross Cutter für die Entsorgung von Papiergut geeignet, die allerdings nicht für die Massenvernichtung dienen können. Die DIN 32757 lässt jedoch die Möglichkeit offen, bei großen Durchsatzmengen und entsprechender Nachbehandlung durch Vermischung oder Verpressung (z.B. durch Einsatz von Ballenpressen und Verwirblern oder einer Nachbehandlung in Form von Verbreiung oder Brikettierung) wegen der dadurch erschwerten Reproduktionsmöglichkeit eine niedrigere Sicherheitsstufe zu wählen.

Müssen Daten auf magnetischen Datenträgern, wie Festplatten, Magnetbänder, Magnetbandkassetten, Disketten, CDs, DVDs, Chipkarten etc. gelöscht werden, ist die DIN 33858 (Löschen von schutzbedürftigen Daten auf magnetischen Datenträgern) zu beachten. Diese Norm legt Mindestanforderungen an Geräte zum Löschen schutzbedürftiger Daten sowie an Prüfeinrichtungen und Prüfverfahren fest.

Neben dem Einsatz von Löschgeräten können kleinere magnetische Datenträger (z.B. Disketten, CDs, DVDs) auch mit Multimedia-Shreddern vernichtet werden. Das jeweilige Medium wird dabei in kleine Partikel geshreddert. Festplatten, die sich nicht mehr mittels Softwaretools komplett und mehrfach überschreiben lassen, müssen ebenfalls physikalisch zerstört bzw. mit Hilfe eines starken Magnetfelds irreversibel gelöscht werden. Auch ein Durchbohren oder Häckseln von Festplatten führt zum gewünschten Erfolg.

Die erwähnten DIN-Normen können vom Beuth Verlag GmbH, Burggrafenstraße 4-10, 10787 Berlin, bezogen werden.

Wo die Entsorgung stattfindet - ob selbst im Haus oder außerhalb bei einem Unternehmen - ist nicht entscheidend. Allerdings muss bei einer externen Datenträgerentsorgung auch der sichere Transport des Vernichtungsguts eingeschlossen sein, d.h. es muss ausgeschlossen sein, dass während des gesamten Prozesses von der Abholung über den Transport bis hin zur Vernichtung Datenträger verloren gehen oder dass dabei Unbefugte auf schutzbedürftige Daten zugreifen können.

Es ist deshalb üblich, den Transport des Vernichtungsguts in abgeschlossenen Containern durchzuführen. Dabei muss darauf geachtet werden, dass sich die Schlüssel für die Container nicht im Besitz des Transporteurs befinden.

Bei einer externen Datenträgerentsorgung ist es nicht nur wichtig, sich die daten-schutzgerechte Entsorgung der Datenträger vom Auftragnehmer schriftlich bescheinigen zu lassen, sondern es sollten auch Kontrollen bei den mit der Entsorgung beauftragten Vertragsfirmen vorgenommen werden, um mögliche Schwachstellen leichter erkennen zu können. Der Auftraggeber der Datenträgervernichtung trägt schließlich auch dann die Verantwortung für die Einhaltung der Datenschutzvorschriften, wenn er einen Dritten mit der Vernichtung der Datenträger mit personenbezogenen Daten beauftragt (Art. 6 Abs. 1 Satz 1 BayDSG).

Der Auftraggeber muss außerdem einen Auftragnehmer unter Berücksichtigung seiner Eignung und der von ihm getroffenen technischen und organisatorischen Maßnahmen sorgfältig auswählen (Art. 6 Abs. 2 Satz 1 BayDSG).

Zu einer sorgfältigen Auswahl eines Auftragnehmers gehört es auch, dass vor Vertragsabschluss geprüft wird,

- ob der Auftragnehmer die geforderte Sicherheit in allen seiner Zuständigkeit unterliegenden Phasen gewährleisten kann,
- ob er einen fachkundigen Datenschutzbeauftragten gemäß § 4 f Abs. 2 BDSG bzw. Art. 25 Abs. 2 BayDSG bestellt, sowie
- ob seine Mitarbeiter über die Bestimmungen des einschlägigen Datenschutzgesetzes unterrichtet und auf die Wahrung des Datengeheimnisses nach § 5 BDSG verpflichtet sind bzw. den öffentlich Bediensteten die Bestimmungen des Art. 5 BayDSG bekannt sind (Datengeheimnis).

Auch sollten entsprechende Referenzen über den Auftragnehmer eingeholt werden.

Gemäß Art. 6 Abs. 2 Satz 2 BayDSG muss ein Auftrag schriftlich erteilt werden. Im Vertrag muss insbesondere klar geregelt sein, für welche Phasen der Auftragnehmer zuständig sein soll, wie die Übergabe der Datenträger erfolgt, dass die Vernichtung außer in genau festgelegten Ausnahmefällen unverzüglich entsprechend den Weisungen des Auftraggebers zu erfolgen hat, welche technisch-organisatorischen Maßnahmen bestehen oder noch zu treffen sind, und ob der Auftragnehmer Subunternehmer einschalten darf und unter welchen Bedingungen. Weiterhin sollte festgelegt werden, dass der Auftragnehmer den Auftraggeber über alle Vorfälle (z.B. Betriebsstörungen oder Fehler) zu informieren hat, die zu einem Schaden für den Auftraggeber führen können.

Ein Auftraggeber hat sich von der Einhaltung der beim Auftragnehmer getroffenen technischen und organisatorischen Maßnahmen zu überzeugen (Art. 6 Abs. 2 Satz 3 BayDSG). Bereits vor Vertragsunterzeichnung sollte der Auftraggeber deshalb vor Ort überprüfen, ob der Auftragnehmer auch tatsächlich dazu in der Lage ist, die daten-schutzgerechte Entsorgung sicherzustellen (z.B. ob die eingesetzten Gerätschaften den Anforderungen der DIN 32757 Teil 1 entsprechen).

Der Auftraggeber darf sich nicht mit der Erklärung eines Auftragnehmers zufrieden geben, dass dieser die Vorschriften der Datenschutzgesetze beachten werde. Auch die ordnungsgemäße Durchführung der Vernichtung der Datenträger ist sporadisch zu überprüfen. Dazu sollte bei der Vertragsgestaltung mit den beauftragten Entsorgungsunternehmen das Recht auf unangemeldete Kontrollen bei der Entsorgung vereinbart werden.

Einen „Mustervertrag zur Auftragsdatenverarbeitung“ finden Sie auf meiner Homepage (http://www.datenschutz-bayern.de) im Bereich Technik/Orientierungshilfen/Mustervorlagen.

### 25.4.8 Sicherheit im ePass Verfahren

Auf Grund des neu in den Reisepass aufgenommenen biometrischen Merkmals Fingerabdruck und der damit verbundenen Änderungen bei dem Beantragungsverfahren habe ich im Berichtszeitraum mehrere Passämter geprüft. Die Prüfungen hatten nicht die Sicherheit des auf dem Pass vorhandenen RFID-Chips zum Inhalt, sondern ausschließlich das Antrags- und Ausgabeverfahren für Reisepässe.

Die Passbehörde speichert die Fingerabdrücke für die Dauer des Herstellungsvorgangs des Reisepasses, um diese z.B. bei Produktionsfehlern erneut an die Bundesdruckerei liefern zu können. Diese gespeicherten Fingerabdruckdaten sind bei der Passbehörde spätestens nach Aushändigung des Passes an den Passbewerber zu löschen (§ 16 Abs. 2 PassG). Eine Überschreitung der Löschfristen für die biometrischen Daten im ePass Verfahren durch die Speicherung auf Sicherungsmedien ist vor allem bzgl. der Fingerabdrücke nicht zulässig.

Es ist aufgefallen, dass es für die Passbehörden keine Möglichkeiten gibt, die vorgeschriebenen Löschfristen in Bezug auf die Fingerabdrücke auch auf eventuell vorhandenen Sicherungsmedien einzuhalten. Die Bilder der Fingerabdrücke sind entweder von der Sicherung auszunehmen oder es müssen nach der Ausgabe der Pässe die jeweiligen Fingerabdrücke auch von den Sicherungsmedien entfernt werden. Sollte dies auf Grund von Vorgaben oder Eigenschaften der eingesetzten Software nicht möglich sein, so ist von den Herstellern diesbezüglich eine Änderung zu fordern.

Für das Verfahren muss ebenso wie für alle Verfahren, die personenbezogene Daten verarbeiten, eine sichere Zugangsauthentifizierung der zur Benutzung berechtigten Personen gewährleistet sein. Die Mindestanforderungen an die Passwortvergabe, -wahl und -verwaltung, zu finden auf meiner Website im Bereich Technik, müssen eingehalten werden. Darüber hinaus ist auf die zugriffssichere Aufbewahrung der PIN der für die Übermittlung der Daten an die Bundesdruckerei nötigen Signaturkarte besonders zu achten.

Gemäß Art. 26 Abs. 3 Satz 1 BayDSG ist dem Antrag auf datenschutzrechtliche Freigabe eine Beschreibung der technisch-organisatorischen Sicherheitsmaßnahmen (Sicherheitskonzept) beizufügen. In diesem Sicherheitskonzept sind, neben den Maßnahmen für das Verfahren selbst, sowohl für den Umgang mit Zugangskennungen und -karten als auch für die Einbindung der Lesegeräte in die Netzwerkumgebung der Behörde Vorgaben zu treffen.

Da der Antragsteller das Recht hat, die auf dem Chip des ePasses gespeicherten Daten bei der Aushändigung zu prüfen, sollten die dazu nötigen Lesegeräte gut sichtbar für die Antragsteller aufgestellt sein. Die Antragsteller sind auf die Möglichkeit hinzuweisen, dass sie ihren ePass prüfen können. Sobald es technisch möglich ist, sind Lesegeräte zu verwenden, bei denen der Fingerabdruck automatisch mit der auf dem RFID-Chip gespeicherten Referenz verglichen werden kann. Bei den momentan im Einsatz befindlichen Geräten ist dies nur optisch möglich. Um die optische Erkennung der Fingerabdrücke etwas zu verbessern, empfiehlt es sich, die Lesegeräte mit einem zusätzlichen, größeren Monitor zu betreiben.

Bei der Erfassung der Daten der Antragsteller ergaben sich aus unserer Sicht grundsätzlich keine Mängel. Es sollte aber sichergestellt werden, dass der

Sachbearbeiter sowohl das Erfassungsgerät für die Fingerabdrücke als auch den Monitor gleichzeitig im Blickfeld haben kann, um ein (un-)absichtliches Auflegen eines anderen Fingers leichter erkennen zu können.

## 25.5 Beratungsleistungen

### 25.5.1 Vorbemerkungen

Wie in den früheren Berichtszeiträumen nahm auch in diesem Berichtszeitraum die nachgefragte Beratungsleistung erheblich zu.

Wegen der Vielzahl der durchgeführten Beratungen kann ich hier nicht auf alle Projekte und Vorhaben eingehen, in die ich eingebunden war. Auf einige Projekte bin ich wegen des rechtlichen Schwerpunkts bereits in den Kapiteln Errichtung einer zentralen und einheitlichen Datenbank zur Lebensmittel-, Veterinär- und Futtermittelkontrolle durch die Gesundheitsverwaltung („TIZIAN“) (vgl. Nr. 14.1.1), MDK ISmed 3 (vgl. Nr. 15.4.1) und Gesetzentwurf über das Verfahren des elektronischen Entgeltnachweises (ELENA-Verfahrensgesetz) (vgl. Nr. 15.9.1) eingegangen. Weitere Projekte werden im Nachfolgenden dargestellt.

### 25.5.2 Entwicklungen zur elektronischen Gesundheitskarte

Seit den Ausführungen zur elektronischen Gesundheitskarte im letzten Tätigkeitsbericht (vgl. hierzu Nr. 14.1.1, 22. Tätigkeitsbericht) ist das Projekt deutlich vorangeschritten. Die Begleitung des Projekts durch mich lässt sich in folgende Aspekte untergliedern:

- Spezifikation der Telematikinfrastruktur und Anwendungen durch die Gematik
- Testung in den Pilotregionen
- Evaluation der Tests

Die Spezifikationen der Gematik richten sich nach den Vorgaben der „Verordnung über Testmaßnahmen für die Einführung der elektronischen Gesundheitskarte“ in der Fassung der Bekanntmachung vom 05.10.2006 und umfassen daher folgende Schritte:

Release 1 beinhaltet den Test der Versichertenstammdaten, des eRezepts und der Notfalldaten in der Offline-Variante, d.h. die Daten werden ohne Anbindung an die Telematikinfrastruktur direkt auf der Gesundheitskarte gespeichert. Die Tests mit Echtdaten laufen in den Pilotregionen seit Anfang 2008. Diesen Sachstand habe ich in der Pilotregion Ingolstadt in einer Arztpraxis und einer Apotheke geprüft und keine Probleme bezüglich der bisherigen Tests aus Sicht des Datenschutzes festgestellt.

Im Anschluss an Release 1 ist Release 2 vorgesehen, der die Online-Variante der Anwendungen betrifft, beginnend mit den Versichertenstammdaten und dem eRezept. Voraussetzung ist hierbei der Aufbau der Telematikinfrastruktur in den Pilotregionen, woran bereits gearbeitet wird. Die eigentlichen Tests sollen im nächsten Jahr starten.

Release 3 umfasst erste freiwillige Anwendungen im Online-Betrieb sowie auch die Anwendungen des Versicherten, die besonders aus Datenschutzsicht von Interesse sind. Sie sollen dem Versicherten die Möglichkeit zur differenzierten Rechtevergabe, zur Einsichtnahme in die Daten, zum Verbergen von Rezepten u.ä. bieten.

Für die Begleitung der Spezifikationen und die Klärung grundsätzlicher Fragen bin ich weiterhin in der Unterarbeitsgruppe des Bundesbeauftragten und der Landesbeauftragten für den Datenschutz aktiv, um frühzeitig in die Gestaltung der Anwendungen und der Infrastruktur eingebunden zu sein. Derzeit aus Sicht der Unterarbeitsgruppe zu klärende Punkte sind u.a.:

- Datenschutzrechtlich verantwortliche Stelle

  Auch für ein komplexes System wie die Telematikinfrastruktur muss es für die Versicherten Ansprechpartner für Fragen bezüglich ihrer Daten geben. Dabei kann es sich einerseits um Auskunftsansprüche handeln, andererseits aber auch z.B. um die Forderung nach Berichtigung oder Löschung von Daten. Da in vielen Fällen zwar der Arzt inhaltlicher Ersteller der Daten ist, diese aber nicht in seiner Obhut, sondern auf mehrere Diensteanbieter verteilt in der Telematikinfrastruktur gespeichert werden, hat er häufig keine Möglichkeit, die Anfragen des Patienten bezüglich seiner Daten alleine zu klären. Die Gematik muss daher Konzepte erarbeiten, wie der Versicherte auch über die Grenzen verschiedener Dienstanbieter und medizinischer Einrichtungen hinweg seine Rechte wahrnehmen kann.

- Anwendungen des Versicherten

  Des Weiteren wird derzeit intensiv diskutiert, wie der Patient ohne Beisein des Arztes Rechte vergeben und Einsicht in Daten nehmen kann. Zur Diskussion stehen der Zugang über Internet vom heimischen PC aus oder über einen eKiosk, der beispielsweise im Wartezimmer des Arztes vorhanden ist. Hierbei muss ein Ausgleich geschaffen werden zwischen dem möglichst umfassenden und komfortablen

Zugriff für den Patienten und dem Schutz vor unbefugtem (eventuell erzwungenem) Zugriff z.B. beim Arbeitgeber.

- Technische Fragen zu Sicherheit und Praktikabilität

  Darüber hinaus wird eine Vielzahl von technischen Einzelfragen diskutiert, wie die Vertraulichkeit der Daten hergestellt werden kann und die Anwendungen gleichzeitig für den IT-technischen Laien nutzbar bleiben. Ein Beispiel hierfür ist die Diskussion um die PIN-Eingabe durch den Versicherten für die freiwilligen Anwendungen, die einerseits ein wichtiges Element zur Kontrolle des Datenzugriffs für den Patienten ist, andererseits aber mit zunehmender Anzahl von PINs praktische Schwierigkeiten beim Merken von PINs auftreten.

- Mehrwertanwendungen

  Auch wird derzeit die Ausgestaltung von Mehrwertanwendungen diskutiert, die nicht im § 291a SGB V festgelegt sind, aber zukünftig über die Infrastruktur betrieben werden sollen. Hierbei ist insbesondere zu klären, welche Anforderungen sich aus Datenschutzsicht stellen.

Neben diesen Diskussionen wurde ich von der Unterarbeitsgruppe beauftragt, die Evaluierung der Testregionen durch das IMG (Institut für Medizinmanagement und Gesundheitswissenschaften) der Universität Bayreuth zu überprüfen. In allen Testregionen sollen im Auftrag der Gematik sowohl Ärzte und Apotheker als auch die Versicherten zu ihren Erfahrungen in der Testregion befragt werden.

Die Versicherten werden hierzu von ihrer Krankenkasse ausgewählt und erhalten von dieser ein Informationsschreiben des IMG sowie einen anonymen Fragebogen. Diesen sollen die Versicherten ohne weitere Angaben zur Person in einem mitgelieferten Briefumschlag ohne Absenderangaben an das IMG zurückschicken. So erhält weder die Krankenkasse Einblick in die ausgefüllten Fragebögen, noch das IMG die identifizierenden Daten der befragten Versicherten.

Die Ärzte und Apotheker (im weiteren Anwender genannt) werden von der Projektleitung der jeweiligen Pilotregion auf eine Teilnahme an der Befragung hin angesprochen. Willigt der Anwender ein, werden seine identifizierenden Daten an das IMG weitergegeben, das dann die Befragung vor Ort durchführt. Dabei wird im ersten Schritt der Anwender über das Evaluierungsverfahren informiert und seine schriftliche Einwilligung eingeholt. Danach werden die Fragebögen in Interview-Form gemeinsam ausgefüllt. Die Fragebögen sind nur mit dem Pseudonym des Anwenders beschriftet, das das IMG vergibt. Hierzu wird eine Liste geführt, die das Pseudonym den identifizierenden Daten des Anwenders zuordnet. Diese Liste wird besonders geschützt und getrennt von den Befragungsdaten verwahrt und ist nur wenigen Mitarbeitern des IMG zugänglich. Der Zugriff hierauf ist genau geregelt und darf nur für die Organisation der Befragung oder die Korrektur von Daten erfolgen.

Nach Beendigung des Interviews werden die Befragungsdaten in eine Datenbank eingegeben, wobei hier auch nur das Pseudonym verwendet wird. Die wissenschaftliche Auswertung erfolgt somit pseudonymisiert, die Wissenschaftler haben keinen Zugriff auf die Liste mit den identifizierenden Daten.

Die Befragung der Anwender und Versicherten soll mehrmals in zeitlichen Abständen erfolgen - jeweils zur Umsetzung der oben dargestellten Releases in den Testregionen, also gemäß dem Testfortschritt.

Aus Sicht des technisch-organisatorischen Datenschutzes ist ein wichtiger Aspekt die Verwendung eigener IT-Systeme ausschließlich für die Evaluierung. Diese werden getrennt von den sonstigen Systemen des IMG und der Universität Bayreuth betrieben. Die Forderungen zur technisch-organisatorischen Sicherheit gemäß Art. 7 BayDSG wurden umgesetzt. Unter diesen Voraussetzungen bestanden keine Einwände gegen das Evaluierungsverfahren.

### 25.5.3 Projekt elektronische Fallakte (eFA) im Städtischen Klinikum München

Das Städtische Klinikum München ist Partner einer Initiative zur Entwicklung eines Standards für elektronische Fallakten (eFA). Dieser Initiative gehören diverse private Klinikketten sowie staatliche / universitäre Großkrankenhäuser an. Mit der Erarbeitung der Spezifikationen wurde das Fraunhofer ISST beauftragt. Ziel ist die Entwicklung eines übergreifenden Standards zum sicheren Austausch von medizinischen Daten in Versorgungsverbünden. Die Entwicklung der eFA verläuft zunächst unabhängig von der Einführung der elektronischen Gesundheitskarte (vgl. hierzu Nr. 23.5.2), soll aber zukünftig als Mehrwertanwendung auf der Telematikinfrastruktur betrieben werden.

In der eFA sollen medizinische Informationen zu einem Patienten fallbezogenen, d.h. bezogen auf eine bestimmte Erkrankung, während des Behandlungszeitraums für alle beteiligten Behandler elektronisch zugänglich gemacht werden. Damit entfällt der zeitraubende Versand von Arztbriefen oder die Doppelerhebung von medizinischen Informationen. Im Projekt des Städtischen Klinikums München soll dies im Rahmen des Pilotprojekts zur Integrierten Versorgung Darmkrebs realisiert werden. Hierbei greifen

das Klinikum und niedergelassene Ärzte für die Behandlung von Darmkrebspatienten auf eine gemeinsame Fallakte zurück.

Zur grundsätzlichen Beurteilung der eFA-Standards wurde eine Arbeitsgruppe des Bundesbeauftragten und der Landesbeauftragten für den Datenschutz ins Leben gerufen, in der ich Mitglied bin. Ziel ist es, eine Bewertung der Datenschutzkonformität der eFA sowie Prüfungshilfen für eFA-basierte Projekte zur Verfügung zu stellen.

Zentrale Voraussetzung aus Datenschutzsicht für derartige Projekte ist die informierte Einwilligung der Patienten in die Nutzung einer eFA. Darin muss genau dargelegt werden, welche Daten in die eFA aufgenommen werden dürfen, wer zugriffsberechtigt ist und wann Daten gelöscht / gesperrt werden. Auch ein Ausstieg des Patienten muss jederzeit ohne Nachteile für ihn möglich sein.

Ein wichtiges Thema aus Sicht des Datenschutzes sind die Zugriffsrechte. Im Gegensatz zu den differenzierten Zugriffsrechten, die gesetzlich für die Anwendungen der elektronischen Gesundheitskarte gefordert sind, ist Derartiges bei der eFA nicht vorgesehen. Hier sollen alle Ärzte auf sämtliche in einer Fallakte enthaltenen Daten zugreifen können. Eine Differenzierung auf bestimmte Dokumente u.ä. ist nicht vorgesehen.

Dies wird von der Arbeitsgruppe nach derzeitigem Stand nur dann als akzeptabel angesehen, wenn die Nutzung der eFA eindeutig im Sinne der Erforderlichkeit eingeschränkt werden kann. Dies bedeutet zum einen, dass eine eFA nur für solche Krankheiten eingerichtet werden darf, die inhaltlich und zeitlich begrenzbar sind und zudem nicht das gesellschaftliche Ansehen des Patienten gefährden, wie z.B. psychische Erkrankungen, HIV. Für derartige Erkrankungen muss der Patient die Möglichkeit haben, differenzierte Zugriffsrechte zu vergeben und Inhalte zu verbergen.

Zudem müssen der Kreis der Behandler sowie der Datenumfang auf das erforderliche Minimum festlegbar sein. Für jedes eFA-Projekt muss vorab definiert werden, welche Daten übergreifend erforderlich sind und daher aufgenommen werden sollen. Des Weiteren muss die zeitliche Befristung der eFA-Nutzung sichergestellt werden, derzeit erscheint sie für lebenslange Erkrankungen als nicht geeignet. Im Rahmen der Einwilligung muss für den Patienten erkennbar sein, welche (namentlich aufgeführten) Ärzte zugreifen sollen, um zu entscheiden, ob er damit einverstanden ist. Auch die Einbeziehung von Hilfspersonal oder die Vergabe von Zugriffsrechten für eine ganze Station im Krankenhaus müssen geregelt werden.

Darüber hinaus sind sowohl in der grundsätzlichen Spezifikation als auch für die Realisierung im Einzelfall technische und organisatorische Maßnahmen zum Schutz der Integrität, Authentizität, Vertraulichkeit, Revisionsfähigkeit und Verfügbarkeit der enthaltenen Daten zu ergreifen und schriftlich zu fixieren, z.B. in einem Datenschutz- und Sicherheitskonzept.

Ich werde das Projekt weiterhin aufmerksam begleiten und zu gegebenem Zeitpunkt wieder darüber berichten.

### 25.5.4 Weitere Entwicklung Fortbildungspunktekonto für Ärzte

Über die Einrichtung des elektronischen Fortbildungspunktekontos der Ärztekammer habe ich bereits im letzten Tätigkeitsbericht berichtet (vgl. hierzu Nr. 13.4.1, 22. Tätigkeitsbericht). Mittlerweile wird das Verfahren in Bayern wie auch in anderen Bundesländern erfolgreich eingesetzt.

Der 30.06.2009 ist gemäß § 95d SGB V der erste Stichtag für den Nachweis der Fortbildung gegenüber der Kassenärztlichen Vereinigung. Als Service für die Ärzte bietet die Bayerische Landesärztekammer (BLÄK) ihren Mitgliedern an, die gesammelten Punkte elektronisch an die Kassenärztliche Vereinigung Bayern (KVB) zu übermitteln, so dass der Arzt dort keine Nachweise mehr einreichen muss.

Der Arzt wird über diese Möglichkeit im Online-Portal „Meine BLÄK“, auf dem der Arzt schon bisher seinen aktuellen Punktestand abrufen konnte, informiert und kann dort seine Einwilligung erteilen. Diese Einwilligung kann jederzeit widerrufen werden, dann finden keine weiteren Datenübermittlungen statt. Der übermittelte Datensatz enthält nur die Daten, die für eine sichere Identifizierung und den Nachweis des Punktestandes nötig sind; also beispielsweise keine Angaben zu den besuchten Veranstaltungen.

Nach der ersten Gesamtlieferung werden von der BLÄK in regelmäßigen Abständen Änderungen an die KVB übermittelt. Es werden dabei aber jeweils nur Daten von den Ärzten übermittelt, die eingewilligt und zum Übermittlungszeitpunkt erstmalig die erforderliche Punktzahl erreicht haben.

Für den Übertragungsweg zwischen BLÄK und KVB wurden technische Sicherheitsmaßnahmen, wie z.B. eine Verschlüsselung der Datenübertragung, ergriffen. Aufgrund dieser Maßnahmen und der Einwilligungslösung habe ich keine Einwendungen gegen das Verfahren.

### 25.5.5 Verfahrensfreigabe bei verteilten Verfahren / Online-Portalen

Im Gesundheitswesen werden sowohl im Forschungsbereich als auch für die Behandlung von Patienten zunehmend Kooperationsformen angestrebt, bei denen untereinander Daten ausgetauscht werden. Dies ist beispielsweise bei Multicenter-Studien der Fall. Häufig sind diese so konzipiert, dass die Studienzentren, die den Patienten behandeln und die Daten erheben, studienrelevante Daten in ein zentrales Online-Portal eingeben. Die Datenspeicherung findet in einer zentralen Datenbank statt. Ähnliche Konstellationen treten im Bereich der Telemedizin auf. Dort werden zum Beispiel für die konsiliarische Mitbehandlung durch Experten medizinische Daten oder auch Live-Videobilder übermittelt, die zumindest für einen gewissen Zeitraum dort auch gespeichert werden. Ein Beispiel für ein derartiges Projekt ist TEMPiS (vgl. hierzu Nr. 5.1, 21. Tätigkeitsbericht).

Soweit es sich hierbei um die Verarbeitung personenbezogener Daten handelt, müssen die Verfahren bei allen beteiligten Stellen durch den behördlichen Datenschutzbeauftragten nach Art. 26 BayDSG freigegeben werden. Um doppelte Arbeit oder unterschiedliche und insgesamt unvollständige Freigaben zu vermeiden, empfiehlt sich folgendes Vorgehen:

Eine Stelle übernimmt zentral die Erarbeitung der benötigten Unterlagen (Verfahrensbeschreibung nach Art. 26 Abs. 2 BayDSG, Übersicht technisch-organisatorische Maßnahmen Art. 26 Abs. 3 BayDSG) für alle Teilnehmer. Es bietet sich an, dass dies die Projektleitung im Rahmen der Konzipierung des Gesamtprojektes durchführt. Neben den sonstigen Projektdokumenten können die Freigabeunterlagen parallel erstellt werden. Es ist somit keine mehrfache Arbeit bei allen Teilnehmern nötig.

Die behördlichen Datenschutzbeauftragten aller Teilnehmer erhalten die vorgefertigten Unterlagen und führen nach einer Prüfung die Verfahrensfreigabe durch. Auch derartige Projekte mit mehreren Partnern müssen in die jeweiligen örtlichen Verfahrensverzeichnisse aufgenommen werden, um eine vollständige Übersicht aller vor Ort betriebenen Verfahren zu gewährleisten. Eine zentrale Freigabe ohne weitere Beteiligung der behördlichen Datenschutzbeauftragten vor Ort ist nicht statthaft und nicht ausreichend.

### 25.5.6 Bestellung eines IT-Sicherheitsbeauftragten

Im Berichtszeitraum haben sich mehrere Behörden mit der Frage an mich gewandt, was sie bei der Bestellung eines IT-Sicherheitsbeauftragten beachten müssen. Dazu nehme ich folgendermaßen Stellung:

Gemäß Art. 25 Abs. 2 Bayerisches Datenschutzgesetz (BayDSG) haben alle öffentlichen Stellen in Bayern, die personenbezogene Daten mit Hilfe von automatisierten Verfahren verarbeiten oder nutzen, einen ihrer Beschäftigten zum behördlichen Datenschutzbeauftragten zu bestellen. Eine analoge Regelung zur Funktion eines IT-Sicherheitsbeauftragten enthält das BayDSG nicht.

Während also die Bestellung eines Datenschutzbeauftragten für bayerische Behörden und sonstige öffentliche Stellen gesetzlich vorgeschrieben ist, besteht eine derartige Verpflichtung für die Bestellung eines IT-Sicherheitsbeauftragten nicht.

Dennoch spricht nichts dagegen, wenn insbesondere größere Behörden über einen IT-Sicherheitsbeauftragten verfügen. Dessen Aufgaben könnten beispielsweise sein:

- Erarbeitung und Umsetzung eines Sicherheitskonzeptes für die öffentliche Stelle
- regelmäßige Aktualisierung und Überprüfung dieses Sicherheitskonzeptes
- Beratung der Behördenleitung und Mitwirkung in Fragen der IT-Sicherheit
- Sensibilisierung der Mitarbeiter und Durchführung von Schulungen bezüglich IT-Sicherheit

Dementsprechend benötigt ein IT-Sicherheitsbeauftragter insbesondere Kenntnisse bezüglich der Informationstechnologie und der Datensicherheit. Ein Datenschutzbeauftragter sollte über das notwendige technische Verständnis zur Umsetzung der erforderlichen Datensicherheitsmaßnahmen verfügen, benötigt aber auch - im Gegensatz zu einem IT-Sicherheitsbeauftragten - ausreichende Rechtskenntnisse bezüglich der einschlägigen datenschutzrechtlichen Regelungen.

Somit können sich ein Datenschutzbeauftragter und ein IT-Sicherheitsbeauftragter gut ergänzen. Während sich der Datenschutzbeauftragte in erster Linie um die Einhaltung des Datenschutzes (also der Beachtung der entsprechenden gesetzlichen Vorschriften) in der Behörde kümmert, überwacht der IT-Sicherheitsbeauftragte die Gewährleistung der Datensicherheit.

Sollte der Datenschutzbeauftragte selbst über weiter gehende EDV-Kenntnisse verfügen, z.B. aufgrund eines Informatikstudiums, kann er bei kleineren Behörden und Kommunen gegebenenfalls zusätzlich die Position eines IT-Sicherheitsbeauftragten ausfüllen. Dabei ist allerdings zu beachten, dass ihm von Seiten der Behördenleitung genügend Zeit für diese beiden Tätigkeiten eingeräumt wird.

Nach dem Bayerischen Datenschutzgesetz ist es nicht erforderlich, dass der behördliche Datenschutzbeauftragte eine Zertifizierung vorweisen kann. Andererseits könnte die Vorlage entsprechender Ausbildungsnachweise hilfreich bei einer Bewerbung als Datenschutzbeauftragter sein.

Bei einem IT-Sicherheitsbeauftragten halte ich jedoch für sehr sinnvoll, dass der entsprechende Bewerber entweder über ein Informatikstudium und/oder über jahrelange Praxiserfahrung im Bereich der EDV verfügt. Seine Bestellung würde ich aber auch nicht nur von der Vorlage eines entsprechenden Zertifikates abhängig machen.

## 25.6 Technisch-organisatorische Einzelprobleme

### 25.6.1 Übertragung der Aufgaben eines behördlichen Datenschutzbeauftragten an einen Dritten

Gelegentlich wird die Frage an mich herangetragen, ob und in wieweit die Aufgaben eines behördlichen Datenschutzbeauftragten an einen externen Dritten übertragen werden könnten. Dazu äußere ich mich wie folgt:

Zum behördlichen Datenschutzbeauftragten kann gemäß Art. 25 Absatz 2 Satz 1 des Bayerischen Datenschutzgesetzes (BayDSG) nur ein Beschäftigter der jeweiligen öffentlichen Stelle bestellt werden. Die Berufung Externer scheidet somit aus. Ein Ausweichen auf § 4 f Abs. 2 Satz 3 Bundesdatenschutzgesetz (BDSG) - wonach zum Beauftragten für den Datenschutz auch eine Person außerhalb der verantwortlichen Stelle bestellt werden kann - ist nicht statthaft, da gemäß Art. 2 Abs. 1 BayDSG für Behörden, Gemeinden und sonstige öffentlichen Stellen des Freistaates Bayern generell die Vorschriften des Bayerischen Datenschutzgesetzes gelten und nicht die Bestimmungen des Bundesdatenschutzgesetzes.

Ausnahmen von dieser Regelung enthält der Art. 3 BayDSG, der beispielsweise im Abs. 1 Satz 1 festlegt, dass für öffentliche Stellen, die als Unternehmen am Wettbewerb teilnehmen, die Vorschriften des Bundesdatenschutzgesetzes mit Ausnahme des Zweiten Abschnitts gelten. Allerdings gelten gemäß Art. 3 Abs. 1 Satz 3 BayDSG für die Durchführung und die Kontrolle des Datenschutzes auch bei diesen Stellen die entsprechenden Vorschriften des Bayerischen Datenschutzgesetzes (Art. 9 und 25 bis 33 BayDSG). Damit ist auch diesen Stellen die Berufung eines Externen zum behördlichen Datenschutzbeauftragten untersagt.

Zu den im Art. 3 Abs. 1 BayDSG aufgeführten öffentlichen Stellen zählen beispielsweise auch die kommunalen Krankenhäuser, soweit sie am Wettbewerb teilnehmen. Damit sind auch diese Stellen verpflichtet, einen ihrer Bediensteten zum behördlichen Datenschutzbeauftragten zu berufen. Gleiches gilt für Krankenhäuser, die nicht am Wettbewerb teilnehmen (z.B. Universitätskliniken und Bezirkskrankenhäuser), die gänzlich unter die Vorschriften des Bayerischen Datenschutzgesetzes fallen.

Gemäß Art. 2 Abs. 2 Satz 1 Nr. 1 BayDSG gelten die Vorschriften des BayDSG auch für Vereinigungen des privaten Rechtes, die Aufgaben der öffentlichen Verwaltung wahrnehmen und an denen eine oder mehrere juristische Personen des öffentlichen Rechts (z.B. ein Landratsamt oder eine Kommune) beteiligt sind.

Entscheidend für die datenschutzrechtliche Einordnung dieser Stellen ist dabei, ob sie Aufgaben der öffentlichen Verwaltung wahrnehmen - z.B. in Form der kommunalen Daseinsvorsorge. Unzweifelhaft unter den Art. 2 Abs. 2 Satz 1 Nr. 1 BayDSG fallen beispielsweise kommunale Krankenhäuser (wie bereits erwähnt), Stadtwerke, Bäder und das Verkehrswesen. Dagegen nehmen beispielsweise Wohnungsbaugenossenschaften bzw. Wohnungsbaugesellschaften in der Regel keine öffentlichen Aufgaben wahr, auch wenn es sich dabei um 100%-Töchter einer öffentlichen Stelle handelt. Bei allen anderen - nicht erwähnten - Vereinigungen des Privatrechts wäre im Einzelfall zu klären, ob diese Stellen Aufgaben der öffentlichen Verwaltung wahrnehmen.

Zusammenfassend bleibt festzuhalten, dass alle öffentlichen Stellen des Freistaates Bayern (mit Ausnahme öffentlich-rechtlicher Versicherungsunternehmen und öffentlich-rechtlicher Kreditinstitute) und deren privatrechtlichen Vereinigungen, soweit sie Aufgaben der öffentlichen Verwaltung wahrnehmen, zumindest bezüglich der Durchführung des Datenschutzes unter die Vorschriften des Bayerischen Datenschutzgesetzes fallen und damit verpflichtet sind, einen ihrer Bediensteten zum behördlichen Datenschutzbeauftragten zu ernennen.

Natürlich besteht auch weiterhin für mehrere kleinere öffentliche Stellen die Möglichkeit - unter bestimmten Voraussetzungen - einen gemeinsamen Datenschutzbeauftragten zu bestellen (vgl. hierzu Nr. 22.1.6, 21. Tätigkeitsbericht).

### 25.6.2 Datenschutz im Bürgerbüro

Im Zuge unserer modernen Dienstleistungsgesellschaft sind auch Kommunen darum bemüht, ihren Bürgern den Kontakt mit der Gemeindeverwaltung so einfach wie möglich zu machen. Die Bürger sollen nicht mehr von einem Amt zum anderen laufen müssen, sondern ihre Anliegen möglichst bei einer Ansprechstelle zentral vorbringen können. Obwohl

Bürgerbüros daher bereits eine große Verbreitung erfahren haben, werden bei deren Einrichtung immer noch einige Versäumnisse begangen und so der Datenschutz und die Datensicherheit nicht gewährleistet.

Folgende technische und organisatorische Maßnahmen sind zu treffen:

- Gruppierung der Sachbearbeiterplätze in geschachtelten Zonen und gegenseitige Abschottung mittels schallisolierender Raumteiler und Sichtschutz, um so ein Mithören der Kommunikation über mehrere Bearbeitungsplätze hinweg auszuschließen.

- Einrichtung von Wartezonen in genügend großem Abstand zu den Sachbearbeiterplätzen.

- Zur Verfügung stellen und Anbieten von Einzelzimmern für das Führen besonders sensibler Gespräche.

Folgende bauliche Maßnahmen kommen in Betracht:

- Schaffung von Warte- und Diskretionszonen

- Schallisolierende Abschottung der Bearbeiterplätze

- Einbau schalldämmender Bodenbeläge und Deckenelemente

- Einrichtung von abgeschlossenen Einzelzimmern oder Sprechkabinen

Neben der Sensibilisierung und Schulung der Mitarbeiter auf Beachtung des Persönlichkeitsschutzes sind folgende organisatorische Maßnahmen zu ergreifen:

- Bildschirme dürfen nicht so aufgestellt werden, dass Dritte den Bildschirminhalt mitlesen können.

- Die Einsichtnahme Dritter in nicht zum aktuellen Fall gehörenden Unterlagen auf dem Bearbeiterplatz ist zu verhindern.

- Auf die Möglichkeit, vertrauliche Einzelfallbehandlung in einem gesonderten Dienstzimmer zu führen, muss hingewiesen werden.

- Eventuell könnte eine Besuchersteuerung erfolgen (z.B. durch Lichtzeichenanlage).

- Es ist darauf zu achten, dass immer nur eine Partei an einen Bearbeiterplatz herantreten darf.

- Informationen müssen vertraulich behandelt werden.

- Die Aufbewahrung personenbezogener Unterlagen muss zugriffssicher erfolgen.

- Die Entsorgung personenbezogener Unterlagen hat datenschutzgerecht zu geschehen.

Außerdem ist bei der Zusammenführung von unterschiedlichen Aufgabenstellungen und der Verarbeitung unterschiedlicher Datenbestände auf einem Arbeitsplatz im Bürgerbüro der Grundsatz der „informationellen Gewaltenteilung“ auch innerhalb der Gemeindeverwaltung zu berücksichtigen.

So ist beispielsweise gemäß § 67 Abs. 9 Satz 3 SGB X innerhalb einer Gebietskörperschaft jede für einen Sozialleistungsbereich zuständige Organisationseinheit eine (eigene) speichernde Stelle. Auch andere Organisationseinheiten in derselben Kommune dürfen Sozialdaten also nur zur Kenntnis erhalten, soweit Übermittlungsbefugnisse nach dem SGB einschlägig sind.

Bei der Einrichtung von Bürgerbüros muss dementsprechend darauf geachtet werden, dass nicht gegen das Sozialgeheimnis verstoßen wird. Solche Verstöße könnten sich etwa dadurch ergeben, dass Mitarbeiter im Bürgerbüro Zugriffs- und Kenntnisnahmemöglichkeiten betreffend Sozialdaten erhalten, die mit der Zweckbindung der für einen Sozialleistungsbereich bestimmten personenbezogenen Daten nicht zu vereinbaren sind.

Zur Reduzierung des Risikos von Verletzungen des Sozialgeheimnisses im Bürgerbüro empfehle ich dringend, die Bearbeitung von Sozialleistungsangelegenheiten nicht ausschließlich im Bürgerbüro, sondern dort nur zusätzlich anzubieten, so dass dem Bürger die Möglichkeit verbleibt, sein Anliegen unmittelbar im zuständigen Sachgebiet vorzutragen. Auf diese Alternative ist im Bürgerbüro ausdrücklich hinzuweisen.

Weitere Informationen zum Thema Datenschutz im Bürgerbüro können der Orientierungshilfe „Vom Bürgerbüro zum Internet - Empfehlungen zum Datenschutz für eine serviceorientierte Verwaltung“ sowie meinem 19. Tätigkeitsbericht (vgl. hierzu Nr. 8.5, 19. Tätigkeitsbericht) entnommen werden - beide sind abrufbar auf meiner Homepage www.datenschutz-bayern.de.

### 25.6.3 Übermittlung von Passbildern im Rahmen von Verkehrsordnungswidrigkeiten

Bestreitet ein Kfz-Halter, dass er im Zusammenhang mit der Verfolgung einer Verkehrsordnungswidrigkeit (z.B. im Rahmen von Geschwindigkeitskontrol-

len) sein Fahrzeug selbst geführt hat, so ist in diesen Fällen zulässig, das bei einer Radarüberwachung angefertigte Lichtbild mit dem bei der Ausweisbehörde hinterlegten Lichtbild des Fahrzeughalters abzugleichen (§ 2b Abs. 2 Personalausweisgesetz). In diesen Fällen werden immer wieder Einwohnermeldeämter dazu aufgefordert, das entsprechende Foto per E-Mail an die Polizei zu übertragen.

Häufig wird dabei aber übersehen, dass bei jeder Übermittlung personenbezogener Daten per E-Mail aus datenschutzrechtlicher Sicht Maßnahmen zur Gewährleistung der Vertraulichkeit, der Integrität und der Authentizität zu ergreifen sind. Da ein Lichtbild personenbezogene Daten über das Aussehen des Abgebildeten verkörpert, sollte auch diese Art der Datenübertragung zur Gewährleistung der Vertraulichkeit verschlüsselt erfolgen. Werden zusätzliche Personen identifizierende Angaben dem Bild beigefügt, so ist die Verschlüsselung zwingend.

Dabei ist zu beachten, dass die zum Einsatz kommenden Verfahren gegen Entschlüsselungsversuche hinreichend sicher sind. So gelten derzeit symmetrische Verfahren mit 128 Bit Schlüssellänge als hinreichend sicher. Für asymmetrische Verfahren wird empfohlen, eine Schlüssellänge von 2048 Bit zu verwenden.

Die Integrität der zu übertragenden Daten lässt sich durch geeignete Signaturverfahren verifizieren. Durch die elektronische Signatur lassen sich Dokumente außerdem eindeutig zuordnen (Gewährleistung der Authentizität).

Im Bayerischen Behördennetz sind S/MIME, PGP und GnuPGP für die Sicherung von E-Mail festgelegt. Eine entsprechende PKI bzw. ein entsprechender Keyserver stehen zur Verfügung. Fotos von Fahrzeughaltern müssen also wegen vermeintlich fehlender PKI oder vermeintlich fehlender technischer Werkzeuge nicht mehr ungeschützt per E-Mail versandt werden.

### 25.7 Orientierungshilfen

Im Berichtszeitraum wurden alle auf meiner Homepage veröffentlichten Orientierungshilfen bzgl. Aktualität überprüft und erforderlichenfalls aktualisiert.

Neu hinzugekommen sind „Gestaltung des Internetauftritts“ (http://www.datenschutz-bayern.de/technik/orient/internetauftritt.html) und das „Merkblatt zum Datenschutz bei medizinischen Studien mit Patientendaten“ (http://www.datenschutz-bayern.de/technik/orient/merkblatt_med_studien.html).

## 26 Die Datenschutzkommission

Der Datenschutzkommission beim Bayerischen Landtag gehörten in den vergangenen zwei Jahren folgende Mitglieder bzw. stellvertretende Mitglieder an:

Für den Landtag:
Ende der 15. Wahlperiode

| Mitglieder: | | stellvertretende Mitglieder: | |
|---|---|---|---|
| Prof. Dr. Hans G. Stockinger | CSU | Christian Meißner | CSU |
| Petra Guttenberger | CSU | Robert Kiesel | CSU |
| Joachim Haedke | CSU | Herbert Ettengruber | CSU |
| Ernst Weidenbusch | CSU | Peter Winter | CSU |
| Martin Neumeyer | CSU | Peter Schmid | CSU |
| Bärbel Narnhammer | SPD | Florian Ritter | SPD |
| Christine Stahl | BÜNDNIS 90/ Die Grünen | Christine Kamm | BÜNDNIS 90/ Die Grünen |

ab dem 17.12.2008:

| | | | |
|---|---|---|---|
| Eberhard Rotter | CSU | Peter Schmid | CSU |
| Walter Taubeneder | CSU | Christian Meißner | CSU |
| Prof. Dr. Winfried Bausback | CSU | Manfred Ländner | CSU |
| Dr. Florian Herrmann | CSU | Dr. Franz Rieger | CSU |
| Florian Ritter | SPD | Horst Arnold | SPD |
| Florian Streibl | Freie Wähler | Alexander Muthmann | Freie Wähler |
| Christine Kamm | BÜNDNIS 90/ DIE Grünen | Susanna Tausendfreund | BÜNDNIS 90/ Die Grünen |
| Dr. Andreas Fischer | FDP | Karsten Klein | FDP |

Für die Staatsregierung:
bis 26.11.2008

| | | | |
|---|---|---|---|
| Hubert Kranz | Ministerialrat im Bayerischen Staatsministerium der Finanzen | Christian Peter Wilde | Ltd. Ministerialrat im Bayerischen Staatsministerium des Innern |

Für die Sozialversicherungsträger:
bis 26.11.2008

| | | | |
|---|---|---|---|
| Werner Krempl | Erster Direktor und Geschäftsführer der Deutschen Rentenversicherung Ober- und Mittelfranken | Dr. Helmut Platzer | Vorstandsvorsitzender der AOK Bayern |

Für die Kommunalen Spitzenverbände:
bis Ende des Berichtszeitraums

| | | | |
|---|---|---|---|
| Rudolf Schleyer | Mitglied des Vorstands bei der AKDB | Klaus Laumer | Abteilungsleiter bei der AKDB |

Für den Verband freier Berufe e.V.:
bis 26.11.2008

| | | | |
|---|---|---|---|
| Hans-Ulrich Sorge | Geschäftsführer des Bayerischen Notarvereins e.V. | Klaus von Gaffron | Präsidiumsmitglied des Verbandes Freier Berufe in Bayern und Vorsitzender des Berufsverbandes Bildender Künstler Bayern |

Herr Prof. Dr. Hans Gerhard Stockinger, MdL, führte den Vorsitz in der Datenschutzkommission; stellvertretende Vorsitzende war Frau Bärbel Narnhammer, MdL.

Die Datenschutzkommission beim Bayerischen Landtag tagte im vergangenen Berichtszeitraum vier Mal. Dabei befasste sie sich u.a. mit folgenden Themen:

- Berichte über Beanstandungen
- Berichte von Datenschutzkonferenzen
- Berichte vom Europäischen Datenschutztag
- Rasterfahndung
- Online-Durchsuchungen von privaten Computern durch Strafverfolgungsbehörden
- Videoüberwachung öffentlicher Orte und Einrichtungen.

**Anlage 1:** **Entschließung der 73. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 08./09.03.2007 Elektronischer Einkommensnachweis muss in der Verfügungsmacht der Betroffenen bleiben**

Mit dem Verfahren ELENA (elektronische Einkommensnachweise) sollen die Einkommensdaten sämtlicher abhängig Beschäftigter in einem bundesweiten Register gespeichert werden. Dieses Verfahren ist angesichts der Sensibilität und des Umfangs der dabei erfassten personenbezogenen Daten von erheblicher datenschutzrechtlicher Brisanz.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder weist darauf hin, dass ein derartiges Register nur dann eingerichtet werden darf, wenn die verfassungsrechtlichen Voraussetzungen erfüllt und die gesetzlichen und technisch-organisatorischen Vorkehrungen zum Schutz der dort gespeicherten Daten getroffen werden.

Zu den wesentlichen verfassungsrechtlichen Voraussetzungen für die Einrichtung des Registers gehören der Nachweis der Erforderlichkeit und die Verhältnismäßigkeit. Angesichts bestehender Zweifel daran, dass diese Voraussetzungen gegeben sind, muss belastbar dargelegt werden, dass die Daten für die jeweiligen Zwecke tatsächlich benötigt werden und dass der angestrebte Zweck nicht mit einem geringeren Eingriff in das Recht auf informationelle Selbstbestimmung erreicht werden kann.

Im Hinblick auf den vom Bundesministerium für Wirtschaft und Technologie erarbeiteten Referentenentwurf sieht die Konferenz darüber hinaus in den folgenden Punkten Klärungsbedarf:

- Es muss gesetzlich festgelegt werden, dass die Daten aus der Datenbank nur mit Mitwirkung der Teilnehmerinnen und Teilnehmer des Verfahrens zu entschlüsseln sind.

- Das Verfahren muss so ausgestaltet werden, dass die Ver- und Entschlüsselung der Daten ohne Vorliegen der Signaturkarte des Betroffenen nur in klar definierten Ausnahmefällen durch eine unabhängige Treuhänderstelle möglich ist.

- Sämtliche im Rahmen des Verfahrens verarbeiteten Daten müssen einem gesetzlichen Beschlagnahmeschutz unterworfen sein.

- Die technischen Komponenten müssen auf der Basis einer unabhängigen Prüfung zertifiziert werden.

**Anlage 2:** **Entschließung der 73. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 08./09.03.2007 Keine heimliche Online-Durchsuchung privater Computer**

Bisher ist nur die offene Durchsuchung privater Computer gesetzlich geregelt. Trotzdem wollen staatliche Behörden auch heimliche Online-Durchsuchungen durchführen. Bei einer Online-Durchsuchung dringen Sicherheitsbehörden mittels sog. „Trojaner“ heimlich in den Rechner ein und verschaffen sich Zugriff auf alle gespeicherten Daten.

Der Bundesgerichtshof hat in seinem Beschluss vom 31.01.2007 (StB 18/06) die Auffassung der Datenschutzbeauftragten des Bundes und der Länder bestätigt, dass eine heimliche Online-Durchsuchung im Bereich der Strafverfolgung rechtswidrig ist. Weder die Bestimmungen zur Wohnungsdurchsuchung noch zur Telekommunikationsüberwachung können zur Rechtfertigung der heimlichen Durchsuchung und Ausforschung privater Computer herangezogen werden.

Die Datenschutzbeauftragten des Bundes und der Länder wenden sich entschieden gegen die Einführung entsprechender Eingriffsgrundlagen sowohl im repressiven als auch im präventiven Bereich. Sie appellieren an die Gesetzgeber, es beim bisherigen Rechtszustand des „offenen Visiers“ zu belassen. Der Staat darf nicht jede neue technische Möglichkeit ungeachtet ihrer Eingriffstiefe zur Ausforschung einsetzen. Dies gilt auch dann, wenn wichtige Belange, wie z.B. die Strafverfolgung, betroffen sind. Hier ist ein Umdenken erforderlich. Es muss ein Raum der Privatsphäre bleiben, der nicht durch heimliche staatliche Überwachungsmaßnahmen ausgehöhlt werden darf.

Eine heimliche Online-Durchsuchung greift tief in die Privatsphäre ein. Die auf einem Computer gespeicherten Daten können aufgrund ihrer Vielzahl und besonderen Sensibilität Einblick in die Persönlichkeit der Betroffenen geben. Der Schutz des Kernbereichs privater Lebensgestaltung wird gefährdet, wenn der Staat heimlich und fortdauernd in private Computer eindringt, um dort personenbezogene Daten auszuspähen. Dies gilt umso mehr, wenn Nachrichtendienste die Möglichkeit heimlichen Zugriffs auf diese Informationen erhalten, obwohl ihnen nicht einmal die offene Erlangung durch eine Beschlagnahme gestattet ist.

Es ist Aufgabe des Staates dafür Sorge zu tragen, dass den Einzelnen die Möglichkeit zur Entfaltung ihrer Persönlichkeit bleibt. Diese Möglichkeit würde unvertretbar eingeschränkt, wenn Durchsuchungs-

maßnahmen zugelassen würden, bei denen aufgrund ihrer Heimlichkeit keine Person wissen kann, ob, wann und in welchem Umfang sie von ihnen bereits betroffen ist oder in Zukunft betroffen sein wird. Der Gesetzgeber sollte deshalb davon absehen, derartige neue Eingriffsbefugnisse zu schaffen, nur weil sie ihm technisch möglich erscheinen und ihre Zweckmäßigkeit behauptet wird. Die technische Entwicklung allein kann nicht der Maßstab für die Rechtfertigung von Eingriffen sein.

Die Konferenz befürchtet massive Sicherheitseinbußen, weil zu erwarten ist, dass sich Computernutzer vor staatlicher Ausforschung zu schützen versuchen, indem sie etwa Softwaredownloads unterlassen. Somit werden aber auch die sicherheitstechnisch wichtigen Software-Updates verhindert und Computer anfälliger gegen Angriffe Krimineller. Die Einführung von Befugnissen zur Online-Durchsuchung würde das Ansehen des Rechtsstaats und das Vertrauen in die Sicherheit von Informationstechnik, insbesondere von E-Government und E-Commerce, massiv beschädigen. Schließlich würden die hohen Aufwendungen für IT-Sicherheit in Staat und Wirtschaft konterkariert. Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder appelliert deshalb an die Bundesregierung, die Landesregierungen und die Parlamente, auf die Einführung derartiger Befugnisnormen zu verzichten.

**Anlage 3:** **Entschließung der 73. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 08./09.03.2007 Pläne für eine öffentlich zugängliche Sexualstraftäterdatei verfassungswidrig**

In der aktuellen Diskussion um einen verbesserten Schutz von Kindern vor Sexualstraftätern wird u.a. die Einrichtung einer öffentlich zugänglichen Sexualstraftäterdatei mit Wohnsitzangaben gefordert. Es wird vorgeschlagen, die Namen und Adressen von verurteilten Sexualstraftätern z.B. über das Internet zu veröffentlichen.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder betont, dass an Kindern begangene Sexualstraftaten mit allen zur Verfügung stehenden rechtsstaatlichen Mitteln bekämpft werden müssen. Dies schließt jedoch die Anwendung eindeutig rechtsstaatswidriger Mittel aus. Um ein solches verfassungswidriges Mittel würde es sich aber bei einer solchen Datei handeln. Dadurch würden die Betroffenen an eine Art elektronischen Pranger gestellt. Sie würden durch die öffentliche Bloßstellung sozial geächtet. Tätern würde die Möglichkeit der Resozialisierung genommen, die ihnen nach unserer Rechtsordnung zusteht.

Der Vorschlag ist lediglich dazu geeignet, Misstrauen und Selbstjustiz zu fördern. Die Betroffenen könnten damit eher zu einem erhöhten Gefahrenpotenzial werden. Er sollte deshalb nach Auffassung der Datenschutzbeauftragten des Bundes und der Länder nicht weiter verfolgt werden.

**Anlage 4:** **Entschließung der 73. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 08./09.03.2007 Vorratsdatenspeicherung, Zwangsidentifikation im Internet, Telekommunikationsüberwachung und sonstige verdeckte Ermittlungsmaßnahmen**

Die gesetzlichen Regelungen der Telekommunikationsüberwachung und anderer verdeckter Ermittlungsmaßnahmen sollen nach der Ankündigung der Bundesregierung unter Berücksichtigung der Rechtsprechung des Bundesverfassungsgerichts einer umfassenden Neuregelung unterzogen werden. Die Bundesregierung will in diesem Zusammenhang auch die europäische Richtlinie zur Vorratsspeicherung von Telekommunikationsverkehrsdaten umsetzen. Das Bundesministerium der Justiz hat zwischenzeitlich einen Referentenentwurf vorgelegt.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder betont erneut, dass die Vorratsdatenspeicherung deutschem Verfassungsrecht widersprechen würde. Nach der Rechtsprechung des Bundesverfassungsgerichts ist die Speicherung von Daten auf Vorrat zu nicht hinreichend bestimmbaren Zwecken verfassungswidrig. Zudem würde die für eine freiheitliche Gesellschaft konstitutive unbefangene Kommunikation erheblich beeinträchtigt. Die Konferenz fordert die Bundesregierung auf, die Umsetzung der Europäischen Richtlinie zur Vorratsdatenspeicherung zumindest solange zurückzustellen, bis der bereits angerufene Europäische Gerichtshof über deren Rechtmäßigkeit entschieden hat.

Die geplante Ausweitung der Vorratsdatenspeicherung geht weit über die europarechtliche Umsetzungsverpflichtung hinaus und wäre ein zusätzlicher unverhältnismäßiger Eingriff in die Kommunikationsfreiheit der Bürgerinnen und Bürger. So sollen die Daten auch zur Verfolgung von Straftaten von erheblicher Bedeutung sowie mittels Telekommunikation begangener Straftaten genutzt werden. Zudem soll die Möglichkeit zur anonymen E-Mail-Kommunikation abgeschafft und die Nutzenden öffentlich zugänglicher E-Mail-Dienste sollen zur Angabe ihres

Namens und ihrer Adresse verpflichtet werden. Diese Angaben sollen außerdem einer Vielzahl von Behörden zum Online-Abruf zur Verfügung gestellt werden, darunter der Polizei, den Staatsanwaltschaften, den Nachrichtendiensten, dem Zoll und der Bundesanstalt für Finanzdienstleistungsaufsicht. Auch dies begegnet erheblichen datenschutzrechtlichen Bedenken.

Zwar stärken einige der vorgesehenen Änderungen der Strafprozessordnung die rechtsstaatlichen und grundrechtlichen Sicherungen bei verdeckten strafprozessualen Ermittlungsmaßnahmen. Es besteht jedoch noch erheblicher Verbesserungsbedarf, insbesondere im Hinblick auf den Schutz des Kernbereichs privater Lebensgestaltung, den Schutz von Berufsgeheimnisträgerinnen und Berufsgeheimnisträgern und die Voraussetzungen der Telekommunikationsüberwachung:

- Mit einer erneuten Ausweitung des Straftatenkatalogs für die Telekommunikationsüberwachung würde die Tendenz zunehmender Überwachungsmaßnahmen in verstärktem Maße fortgesetzt. Der Katalog sollte deshalb mit dem Ziel einer deutlichen Reduzierung kritisch überprüft werden. Es sollten nur Straftaten aufgenommen werden, deren Aufklärung in besonderem Maße auf die Telekommunikationsüberwachung angewiesen ist, die mit einer bestimmten gesetzlichen Mindeststrafe (z.B. ein Jahr) bedroht sind und die auch im Einzelfall schwer wiegen.

- Die vorgesehene Kernbereichsregelung ist ungenügend. Sie nimmt in Kauf, dass regelmäßig auch kernbereichsrelevante Informationen erfasst werden. Für solche Informationen muss stattdessen grundsätzlich ein Erhebungsverbot gelten. Erkenntnisse aus dem Kernbereich der privaten Lebensgestaltung, die dennoch erlangt werden, müssen zudem einem absoluten Verwertungsverbot unterliegen, nicht nur für Strafverfahren.

- Der Schutz des Kernbereichs privater Lebensgestaltung ist nicht nur in den Bereichen der Wohnraum- und Telekommunikationsüberwachung zu gewährleisten. Auch für alle anderen verdeckten Ermittlungsmaßnahmen ist eine Regelung zum Schutz des Kernbereichs zu treffen.

- Für die Kommunikation mit Berufsgeheimnisträgerinnen und Berufsgeheimnisträgern sollte ein absolutes Erhebungs- und Verwertungsverbot geschaffen werden, das dem jeweiligen Zeugnisverweigerungsrecht entspricht. Dieses sollte unterschiedslos für alle Berufsgeheimnisträgerinnen und Berufsgeheimnisträger und deren Berufshelferinnen und Berufshelfer gelten. Die im Entwurf enthaltene Differenzierung zwischen bestimmten Gruppen von Berufsgeheimnisträgerinnen und Berufsgeheimnisträgern ist sachlich nicht gerechtfertigt.

- Für Angehörige i.S.v. § 52 StPO sollte ein Erhebungs- und Verwertungsverbot für die Fälle vorgesehen werden, in denen das öffentliche Interesse an der Strafverfolgung nicht überwiegt. Die besonderen verwandtschaftlichen Vertrauensverhältnisse dürfen nicht ungeschützt bleiben.

- Für teilnehmende Personen von Kernbereichsgesprächen, die weder Berufsgeheimnisträgerinnen und Berufsgeheimnisträger noch Angehörige i.S.v. § 52 StPO sind, sollte insoweit ein Aussageverweigerungsrecht aufgenommen werden. Andernfalls bleibt der Kernbereich teilweise ungeschützt.

- Für die sog. Funkzellenabfrage, die alle Telefonverbindungen im Bereich einer oder mehrerer Funkzellen erfasst, sollten klare und detaillierte Regelungen mit engeren Voraussetzungen normiert werden. Diese sollten vorsehen, dass im Rahmen einer besonderen Verhältnismäßigkeitsprüfung die Anzahl der durch die Maßnahmen betroffenen unbeteiligten Dritten berücksichtigt und die Maßnahme auf den räumlich und zeitlich unbedingt erforderlichen Umfang begrenzt wird. Die Unzulässigkeit der Maßnahme zur Ermittlung von Tatzeuginnen und Tatzeugen sollte ins Gesetz aufgenommen werden.

- Die aufgrund einer Anordnung der Staatsanwaltschaft bei Gefahr in Verzug erlangten Daten dürfen nicht verwertet werden, wenn die Anordnung nicht richterlich bestätigt wird. Dieses Verwertungsverbot darf nicht - wie im Entwurf vorgesehen - auf Beweiszwecke begrenzt werden.

- Art und Umfang der Begründungspflicht für den richterlichen Beschluss der Anordnung der Telekommunikationsüberwachung sollte wie bei der Wohnraumüberwachung im Gesetz festgeschrieben werden. Im Sinne einer harmonischen Gesamtregelung sollten darüber hinaus qualifizierte Begründungspflichten für sämtliche verdeckte Ermittlungsmaßnahmen geschaffen werden.

- Zur Gewährleistung eines effektiven Rechtsschutzes ist sicherzustellen, dass sämtliche Personen, die von heimlichen Ermittlungsmaßnahmen betroffen sind, nachträglich von der Maßnahme benachrichtigt werden, soweit diese bekannt sind oder ihre Identifizierung ohne unverhältnismäßige weitere Ermittlun-

gen möglich ist und nicht überwiegende schutzwürdige Belange anderer Betroffener entgegenstehen. Darüber hinaus sollte bei Massendatenerhebungen über eine ergänzende Benachrichtigung durch eine öffentliche Bekanntmachung der Maßnahme nachgedacht werden.

- Die für die Telekommunikationsüberwachung vorgesehenen Berichts- und Statistikpflichten sollten um Angaben zur Dauer der Überwachung, zur Anzahl der Gespräche und zur Benachrichtigung Betroffener ergänzt werden.

- Die im Entwurf enthaltenen erweiterten Eingriffsgrundlagen sollten befristet und einer unabhängigen, gründlichen und wissenschaftlich unterstützten Evaluation unterzogen werden.

**Anlage 5:** **Entschließung der 73. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 08./09.03.2007 GUTE ARBEIT in Europa nur mit gutem Datenschutz**

Die Ministerinnen und Minister für Beschäftigung und Soziales in Europa haben am 19.01.2007 neun Schlussfolgerungen für GUTE ARBEIT aufgestellt: GUTE ARBEIT bedeute Arbeitnehmerrechte und Teilhabe, faire Löhne, Sicherheit und Gesundheitsschutz bei der Arbeit sowie eine familienfreundliche Arbeitsorganisation. Gute und faire Arbeitsbedingungen sowie angemessener sozialer Schutz seien unabdingbar für die Akzeptanz der Europäischen Union bei den Bürgerinnen und Bürgern.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder nimmt diese Initiative zum Anlass und fordert dazu auf, auch den Beschäftigtendatenschutz zu stärken. Angesichts stetig wachsender technischer Möglichkeiten muss klar geregelt werden, welche Daten Unternehmen über ihre Beschäftigten erheben dürfen, wie sie damit verfahren müssen und wozu sie die Daten nutzen dürfen.

Deshalb fordert die Konferenz seit langem ein Arbeitnehmerdatenschutzgesetz. Bereits 2003 hat sie darauf hingewiesen, dass Persönlichkeitsrechte und Datenschutz im Arbeitsverhältnis vielfältig bedroht sind, zum Beispiel durch

- die Sammlung von Beschäftigtendaten in leistungsfähigen Personalinformationssystemen, die zur Erstellung von Persönlichkeitsprofilen genutzt werden,

- die Übermittlung von Beschäftigtendaten zwischen konzernangehörigen Unternehmen, für die nicht der Datenschutz der EG-Datenschutzrichtlinie gilt,

- die Überwachung des Arbeitsverhaltens durch Videokameras, die Protokollierung der Nutzung von Internetdiensten am Arbeitsplatz,

- die Erhebung des Gesundheitszustands, Drogen-Screenings und psychologische Testverfahren bei der Einstellung.

Die Achtung des Grundrechts auf informationelle Selbstbestimmung der Arbeitnehmerinnen und Arbeitnehmer zählt ebenso zu guten und fairen Arbeitsbedingungen wie Chancengleichheit oder gerechte Bezahlung. Beschäftigtendatenschutz erhöht zudem die Motivation, trägt und fördert die Arbeitszufriedenheit und bedeutet damit einen nicht zu unterschätzenden Standortvorteil.

Die Konferenz fordert die Bundesregierung auf, sich für einen hohen gemeinsamen Mindeststandard des Arbeitnehmerdatenschutzes in Europa einzusetzen und in Deutschland zeitnah einen entsprechenden Gesetzentwurf vorzulegen.

**Anlage 6:** **Entschließung der 73. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 08./09.03.2007 Anonyme Nutzung des Fernsehens erhalten!**

Seit einiger Zeit werden in der Öffentlichkeit Pläne der großen privaten Fernsehveranstalter diskutiert, gemeinsam mit den Betreibern von Übertragungskapazitäten (Satellit, Kabel und DVB-T) ihre Programme nur noch verschlüsselt zu übertragen. Dabei werden vorrangig solche Geschäftsmodelle favorisiert, bei denen die kostenpflichtige Entschlüsselung des Signals nur mit personenbezogenen Smartcards möglich sein soll.

Die Datenschutzbeauftragten des Bundes und der Länder betrachten diese Entwicklung mit Sorge. Nachdem vor allem durch zahlreiche staatliche Eingriffe die verfassungsrechtlich gebotene unbeobachtete Nutzung von Telekommunikation und Internet kaum noch möglich ist, steht nun auch der seit jeher selbstverständliche anonyme und nicht registrierte Empfang von Rundfunkprogrammen auf dem Spiel. Gerade durch die Vermarktung individuell zugeschnittener Programmpakete im digitalen Rundfunk kann bei personenbezogener Abrechnung nachvollzogen werden, wer welche Angebote nutzt. Die entstehenden technischen Infrastrukturen werden zudem auch Möglichkeiten bieten, die konkrete Nutzung einzelner Sendungen zu registrieren. Damit wird die allgegenwärtige Bildung von Persönlichkeitsprofilen

um detaillierte Kenntnisse über den Rundfunkkonsum ergänzt.

Die bisher bekannt gewordenen Pläne der Unternehmen widersprechen dem im Rundfunkstaatsvertrag geregelten Gebot, die Inanspruchnahme von Rundfunk und deren Abrechnung anonym zu ermöglichen und verstoßen gegen das Prinzip der Datenvermeidung. Dies wäre nicht akzeptabel, zumal datenschutzfreundliche Varianten der Abrechnung - beispielsweise durch den Einsatz von vorbezahlten Karten - ohne wirtschaftliche Einbußen zur Verfügung stehen.

Die Datenschutzbeauftragten des Bundes und der Länder fordern deshalb die Länder auf, die Einhaltung der datenschutzrechtlichen Anforderungen des Rundfunkstaatsvertrages gegenüber den Veranstaltern durchzusetzen, und eine anonyme Nutzung von Rundfunkprogrammen auch in Zukunft sicherzustellen.

Angesichts der immer umfassenderen Individualisierung und Registrierbarkeit des Mediennutzungsverhaltens erinnert die Konferenz der Datenschutzbeauftragten des Bundes und der Länder an ihre Forderung, das grundgesetzlich geschützte Fernmeldegeheimnis zu einem allgemeinen Mediennutzungsgeheimnis weiterzuentwickeln.

**Anlage 7:** **Entschließung der Datenschutzbeauftragten des Bundes und der Länder vom 08.06.2007**
**Telekommunikationsüberwachung und heimliche Ermittlungsmaßnahmen dürfen Grundrechte nicht aushebeln**

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder wendet sich mit Nachdruck gegen die von Bundesregierung und Bundesratsgremien geplante Einführung der Vorratsspeicherung von Telekommunikationsverkehrsdaten und die Verschärfungen verdeckter Ermittlungsmaßnahmen, vor allem durch Telekommunikationsüberwachung:

Die Datenschutzbeauftragten haben am 08./09.03.2007 auf ihrer Konferenz in Erfurt einen ersten Gesetzentwurf als verfassungswidrig beanstandet. Insbesondere haben sie vor heimlichen Online-Durchsuchungen und der Vorratsdatenspeicherung gewarnt. Damit würde tief in die Privatsphäre eingegriffen und das Kommunikationsverhalten der gesamten Bevölkerung - ob via Telefon oder Internet - pauschal und anlasslos erfasst.

Die einhellige Kritik der Datenschutzbeauftragten und ihre Aufforderung, stattdessen verhältnismäßige Eingriffsregelungen zu schaffen, wurden von der Bundesregierung nicht beachtet. In ihrem Gesetzentwurf vom 27.04.2007 wird demgegenüber der Schutz der Zeugnisverweigerungsberechtigten verringert, Benachrichtigungspflichten gegenüber betroffenen Personen werden aufgeweicht, Voraussetzungen für die Erhebung von Standortdaten in Echtzeit und für den Einsatz des IMSI-Catchers erheblich ausgeweitet und die Verwendungszwecke für die auf Vorrat gespeicherten Daten über die europarechtlichen Vorgaben hinaus auch auf leichte Straftaten, auf Zwecke der Gefahrenabwehr und sogar der Nachrichtendienste erstreckt.

Die nun im Bundesratsverfahren erhobenen zusätzlichen Forderungen zeugen von mangelndem Respekt vor den Freiheitsrechten der Bürgerinnen und Bürger. Dies zeigen folgende Beispiele: Die ohnehin überzogene Speicherdauer aller Verkehrsdaten wird von 6 auf 12 Monate verlängert. Die Überwachungsintensität erhöht sich durch eine Verschärfung der Prüfpflichten der Telekommunikationsunternehmen - bis zum Erfordernis des Ablichtens und Aufbewahrens von Identitätsnachweisen aller Personen, die Prepaid-Produkte nutzen wollen. Die Sicherheitsbehörden erhalten Auskunft über Personen, die bestimmte dynamische IP-Adressen nutzen. Ausschüsse des Bundesrates wollen die Nutzung dieser Daten sogar zur zivilrechtlichen Durchsetzung der Rechte an geistigem Eigentum gestatten und bewegen sich damit weit jenseits des durch die EG-Richtlinie zur Vorratsspeicherung abgesteckten Rahmens, die Nutzung auf die Verfolgung schwerer Straftaten zu beschränken. Weiterhin ist eine Ausdehnung der Auswertung von Funkzellendaten von Mobiltelefonen mit dem Ziel der Ermittlung des Aufenthaltes von möglichen Zeuginnen und Zeugen geplant. Daten, die Beweiserhebungs- oder -verwertungsverboten unterliegen, sollen nicht unmittelbar gelöscht, sondern nur gesperrt werden.

Ganz nebenbei will der Innenausschuss des Bundesrats eine Rechtsgrundlage für die heimliche Online-Durchsuchung von Internet-Computern schaffen. Allein die Zulassung dieser Maßnahme würde rechtsstaatlichen Grundsätzen eklatant widersprechen und das Vertrauen in die Sicherheit der Informationstechnik massiv beschädigen.

Das Bundesverfassungsgericht hat in letzter Zeit eine Reihe von Sicherheitsgesetzen mit heimlichen Erhebungsmaßnahmen aufgehoben. Auch europäische Gerichte haben Sicherheitsmaßnahmen für rechtswidrig erklärt. Eine Entscheidung des Europäischen Gerichtshofs über die Verpflichtung zur Vorratsdatenspeicherung von Telekommunikationsverbindungsdaten sollte abgewartet werden ebenso wie die Entscheidung des Bundesverfassungsgerichtes zur nordrhein-westfälischen Regelung, die dem Verfassungsschutz die Online-Durchsuchung erlaubt.

Die Forderungen im Gesetzgebungsverfahren zeugen von einem überzogenen Sicherheitsdenken. Sie füh-

ren dazu, dass die Freiheitsrechte der Bevölkerung untergraben werden. Sicherheit in der Informationsgesellschaft ist nicht mit überbordenden Überwachungsregelungen zu erreichen, sondern nur durch maßvolle Eingriffsbefugnisse mit effektiven grundrechtssichernden Verfahrensregelungen und durch deren besonnene Anwendung. Die betroffenen Grundrechte verkörpern einen zu hohen Wert, als dass sie kurzfristigen Sicherheitsüberlegungen geopfert werden dürfen.

**Anlage 8:** **Entschließung der 74. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 25./26.10.2007 Gesetzesinitiative der Bundesregierung zu Auskunfteien und Scoring: Nachbesserung bei Auskunfteienregelungen gefordert**

Die fortschreitende technologische Entwicklung führt zu immer weitreichenderer Erfassung und Verknüpfung von persönlichen Daten und ermöglicht deren Auswertung für Kontroll- und Präventionszwecke. In der Privatwirtschaft ist daher ein engmaschiges Netz verschiedener Auskunftssysteme und branchenübergreifender Zentraldateien entstanden, die durch Profilbildung das Verhalten eines jeden Menschen ohne dessen Wissen und Wollen abbilden und bewerten können.

Vor diesem Hintergrund begrüßt die Konferenz der Datenschutzbeauftragten des Bundes und der Länder, dass das Bundesministerium des Innern endlich damit begonnen hat, die gesetzlichen Regelungen zu den Auskunfteien zu überarbeiten und neue Regelungen zum Scoring zu schaffen.

Die vorgesehenen Regelungen zu den Auskunfteien verschlechtern die Rechtsposition der Betroffenen. Sie tragen dem sich ständig weiter entwickelnden Auskunfteimarkt und den dadurch hervorgerufenen Bedrohungen für das Recht auf informationelle Selbstbestimmung nicht hinreichend Rechnung. Ziel einer gesetzlichen Regelung muss es sein, den rasant wachsenden, branchenübergreifenden Datenaustausch zu beschränken. Es kann nicht hingenommen werden, dass Auskunfteidienste nur einseitig das Informationsinteresse der angeschlossenen Unternehmen bedienen. Sie müssen auch in stärkerem Maße die schutzwürdigen Belange der betroffenen Bürgerinnen und Bürgern berücksichtigen. Mit der im Entwurf vorgesehenen Möglichkeit, die Auskunftstätigkeit auf jegliche rechtliche und wirtschaftliche Risiken zu erstrecken, wäre zu befürchten, dass letztlich bei allen vertraglichen Beziehungen - also auch bei Versicherungs- und Arbeitsverträgen - vorab Auskunfteien eingeschaltet werden. Damit würden die allgemeinen Vertragsrisiken im Wirtschaftsleben in nicht mehr angemessener Weise einseitig auf die Kundinnen und Kunden verlagert.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder fordert den Gesetzgeber auf, die Situation der Verbraucherinnen und Verbraucher deutlich zu verbessern und mit dem Gesetzesvorhaben einen fairen Ausgleich zwischen den Interessen der Wirtschaft und der betroffenen Verbraucherinnen und Verbraucher zu schaffen. Die Konferenz hält es für dringend erforderlich, die Auskunfteitätigkeit auf kreditorische Risiken zu begrenzen. Zudem fordert die Konferenz, Auskunfteidienste branchenspezifisch zu begrenzen.

Der vorgelegte Referentenentwurf eines Gesetzes zur Änderung des Bundesdatenschutzgesetzes sieht beim Scoring nun Ansätze für ein transparenteres Verfahren für die Betroffenen vor. Es muss jedoch darauf geachtet werden, dass dieser Ansatz auch vorbehaltlos umgesetzt wird. Das Scoring, bei dem mittels einer mathematisch-statistischen Formel das zukünftige vertragstreue Verhalten eines Menschen durch einen Zahlenwert ausgedrückt wird, dringt seit Jahren in immer mehr Bereiche des Wirtschaftslebens vor. Den Betroffenen wurde jedoch bisher das Wissen darüber, wie sich der Scorewert zusammensetzt, vorenthalten. Diese Praxis soll der Gesetzentwurf beenden. Die Betroffenen sollen Auskunft darüber erhalten, welche Daten mit welcher Gewichtung in den jeweiligen Scorewert eingeflossen sind. Die vorgeschlagenen Regelungen gehen jedoch noch nicht weit genug. Unbedingt zu streichen ist etwa eine im Entwurf enthaltene Regelung, wonach die Auskunft mit der Begründung verweigert werden kann, es würden Geschäftsgeheimnisse offenbart.

**Anlage 9:** **Entschließung der 74. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 25./26.10.2007 Nein zur Online-Durchsuchung**

Der Computer hat im täglichen Leben der meisten Menschen eine zentrale Bedeutung für die Aufbewahrung und Gestaltung privatester Informationen, wie Fotografien, Reiseberichte, Tagebuchaufzeichnungen, persönliche Briefe, Eindrücke, Vorstellungen und Gefühle. Die heimliche Online-Durchsuchung führt deshalb zu erheblichen Eingriffen in Grundrechte (informationelles Selbstbestimmungsrecht, Unverletzlichkeit der Wohnung, Telekommunikationsgeheimnis usw.). Die Installation von Überwachungssoftware etwa mit Hilfe des Internets oder die Versendung von E-Mails unter dem Namen einer anderen Behörde wird erwogen, sogar das unbemerkte Eindringen in Wohnungen zu diesem Zweck wird nicht ausgeschlossen.

Bei dem geforderten heimlichen Zugriff auf informationstechnische Systeme geht es nicht nur um „Online-Durchsicht“ als einmalige Durchsuchung und die damit verbundene Übertragung von Festplatteninhalten an die Strafverfolgungs- oder Sicherheitsbehörden, sondern auch um die anhaltende Überwachung, um das Ausspähen von Passworten und die Protokollierung aller elektronischen Aktivitäten. Auch sollen andere Kommunikations- und Datenverarbeitungssysteme, wie Computernetze, Mobiltelefone, PDA usw. in die heimliche Durchsuchung einbezogen werden. Dabei ist die Feststellung des Computers einer Zielperson technisch ohne Zusatzinformationen nicht ohne weiteres möglich. Die Gefahr ist daher sehr groß, dass von einer solchen Maßnahme eine Vielzahl von - auch unverdächtigen - Nutzerinnen und Nutzern betroffen sein werden.

Es steht fest, dass sich der unantastbare Kernbereich privater Lebensgestaltung bei Online-Durchsuchungen durch technische Mittel bei der Datenerhebung nicht schützen lässt. Ein automatisierter Kernbereichsschutz ist somit nicht realisierbar.

Darüber hinaus wird eingeräumt, dass sich mit Hilfe der entsprechenden Software die auf den Festplatten gespeicherten Inhalte manipulieren ließen, was die Beweiseignung der gewonnenen Erkenntnisse und damit - jedenfalls bei der Verfolgung von Straftaten - die Geeignetheit der Online-Durchsuchung in Frage stellt.

Derzeit wird zwar versichert, dass der Einsatz nur auf die Bekämpfung des Terrorismus sowie die Verfolgung schwerster Straftaten und insgesamt auf wenige Fälle beschränkt wird. Die Erfahrungen zeigen aber, dass solche Beschränkungen nicht von langer Dauer sein werden. So begründen z.B. die drohende Aufweichung der Zweckbindung der Mautdaten und die Entwicklung der Telekommunikationsüberwachung die Befürchtung, dass Online-Durchsuchungen entsprechend dem technischen Fortschritt als Standardmaßnahme künftig auch bei Gefahren und Straftaten von geringerer Bedeutung eingesetzt werden. Zudem ist davon auszugehen, dass Terrorverdächtige Mittel und Wege finden werden, durch geeignete Gegenmaßnahmen eine erfolgreiche Online-Durchsuchung zu verhindern. Die heimliche Online-Durchsuchung führt deshalb voraussichtlich nicht zu mehr Sicherheit, aber sicher zur Einschränkung der Freiheit.

Die Datenschutzbeauftragten des Bundes und der Länder bekräftigen daher ihre im Rahmen der 73. Konferenz im März 2007 erhobene Forderung an die Bundesregierung, die Landesregierungen und die Parlamente, auf die Einführung der repressiven und präventiven Online-Durchsuchung zu verzichten.

Sie halten es für zwingend notwendig, dass das Urteil des Bundesverfassungsgerichts in dem Verfahren gegen die Online-Durchsuchung im Verfassungsschutzgesetz Nordrhein-Westfalens abgewartet wird.

**Anlage 10:** **Entschließung der 74. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 25./26.10.2007 Zentrale Steuerdatei droht zum Datenmoloch zu werden**

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hält es für inakzeptabel, dass die Bundesregierung mit dem Jahressteuergesetz 2008 im Schnelldurchgang ohne ausführliche parlamentarische Beratung die beim Bundeszentralamt für Steuern aufzubauende zentrale Steuerdatei um zusätzliche - teilweise sensible - Daten anreichern will. Zugleich droht die Steueridentifikationsnummer (Steuer-ID) bereits vor ihrer endgültigen Einführung zu einem allgemeinen Personenkennzeichen zu werden.

Der Gesetzentwurf sieht die Ablösung des Lohnsteuerkartenverfahrens durch ein elektronisches Abrufverfahren (ElsterLohn II) ab 2011 vor. Bereits am 09.11.2007 soll das Gesetz abschließend im Bundestag beraten werden. Geplant ist unter anderem, die in Zusammenhang mit der seit dem 01.07.2007 vergebenen Steuer-ID errichtete Datenbank um weitere Daten zu ergänzen, etwa um die Religionszugehörigkeit, Ehepartner/Ehepartnerinnen/Kinder und deren Steuer-ID, dazu Angaben über Steuerklassen. Hierbei werden auch zahlreiche Datensätze auf Vorrat aufgenommen, da auch Personen betroffen sind, die (noch) keine Arbeitnehmer/Arbeitnehmerinnen sind.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder fordert vom Bundestag und Bundesrat, dieses Vorhaben der Umstellung auf ein elektronisches Verfahren mit dem Jahressteuergesetz 2008 nicht zu beschließen. Folgende Punkte sind datenschutzrechtlich kritisch:

- Der durch die Vergabe der Steueridentifikationsnummer an alle Steuerpflichtigen und damit für alle Einwohnerinnen und Einwohner der Bundesrepublik entstehende Datenpool erhält eine neue Dimension. Zwar sind die Lohnsteuerabzugsmerkmale auch bisher auf der Lohnsteuerkarte vermerkt. Die Speicherung dieser Daten in einer zentralen Datenbank würde aber erhebliche datenschutzrechtliche Fragen aufwerfen. In den zentralen Datenbestand würden die Daten aller Personen mit Lohnsteuerkarten einfließen, also auch von solchen Personen, die sich nicht in einem lohnsteuerpflichtigen Beschäftigungsverhältnis befinden. Es ist zweifelhaft, ob die Aufnahme dieses Personenkreises dem Erforderlichkeitsgrundsatz entspricht. Nützlichkeits-

erwägungen sind für eine Datenhaltung auf Vorrat in keinem Fall ausreichend.

- Die Daten würden bundesweit annähernd vier Millionen Arbeitgebern zur Verfügung stehen. Als einzige Sicherung ist dabei vorgesehen, dass nur ein autorisierter Arbeitgeber die Lohnsteuerabzugsmerkmale abrufen kann. Klärungsbedürftig ist allerdings, wie dies sichergestellt werden kann. Zwar ist ein Authentifizierungsverfahren für den Arbeitgeber vorgesehen. Die Frage ist jedoch, ob damit tatsächlich eine rechtswidrige Informationsbeschaffung Dritter auszuschließen ist. Zumindest sollten die Daten aus der zentralen Datenbank nur unter Mitwirkung der Betroffenen abgerufen werden können.

- Die gesetzlich vorgeschriebene Evaluierung des Verfahrens (§ 87 a Abs. 6 AO) ist noch nicht erfolgt. Gleichzeitig existieren bereits jetzt Bestrebungen, die Kommunikationsplattform „Elster“ für Nutzungen durch andere Verwaltungszweige zu öffnen (OpenElster). Dies aber bedeutete, dass damit die Steuer-ID auch für die Identitätsfeststellung bei steuerfremden Anwendungen herangezogen werden könnte, ohne damit der strikten Zweckbindung nach § 139 b Abs. 5 Abgabenordnung zu rein steuerlichen Zwecken Rechnung zu tragen. Diese Zweckbindung kann nach § 139 b Abs. 2 AO auch nicht durch die jeweilige Einwilligung der betroffenen Bürgerinnen und Bürger überwunden werden. Mit OpenElster sollen diese Vorkehrungen offenbar aufgeweicht werden, bevor die Steuer-ID überhaupt eingeführt wurde. Allein dies macht deutlich, dass jede Erweiterung des zentralen Datenbestandes kritisch hinterfragt werden muss.

Schließlich ist zu befürchten, dass die vorgesehene Erweiterung der Datenbank beim BZSt nicht den Schlusspunkt darstellt. Die im neuen Datenpool gespeicherten Daten wären auch für Sozialleistungsträger und Strafverfolgungsbehörden interessant. Es gibt zahlreiche Beispiele, dass Daten, die zunächst nur für einen engen Zweck gespeichert werden dürfen, später für viele andere Zwecke verwendet werden: Die für steuerliche Zwecke erhobenen Daten über Freistellungsaufträge werden mit den ebenfalls beim BZSt gespeicherten Daten der Empfänger von BaföG- und anderen Sozialleistungen abgeglichen. Die Mautdaten, die zunächst nur zur Mautberechnung erhoben wurden, sollen zukünftig auch zur Strafverfolgung verwendet werden. Der zunächst ausschließlich zur Terrorismusbekämpfung und der Bekämpfung der organisierten Kriminalität eingeführte Kontendatenabruf steht heute auch Finanzämtern und anderen Behörden wie z.B. der Bundesagentur für Arbeit über das BZSt offen. Das BZSt enthält so einen einzigartigen aktuellen Datenpool aller Bundesbürgerinnen und -bürger, der wesentliche Meldedaten, Bankkontenstammdaten und Steuerdaten zentral verknüpfen kann.

**Anlage 11:** **Entschließung der 74. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 25./26.10.2007 Zuverlässigkeitsüberprüfungen bei Großveranstaltungen**

Anlässlich der Fußball-WM 2006 wurden im Rahmen der Akkreditierung umfassende Zuverlässigkeitsüberprüfungen nach einem auf Verwaltungsebene festgelegten Verfahren durchgeführt. Dabei wurde auf die Datenbestände der Polizei- und Verfassungsschutzbehörden des Bundes und der Länder zurückgegriffen. Dieses gesetzlich nicht vorgesehene Verfahren soll nunmehr beliebigen weiteren Veranstaltungen als Vorbild dienen.

Solche Zuverlässigkeitsüberprüfungen greifen in das Grundrecht auf informationelle Selbstbestimmung ein. Grundrechtseingriffe dürfen nicht unter Umgehung gesetzlicher Vorschriften durchgeführt werden, die Voraussetzungen und Begrenzungen solcher Verfahren regeln. Die Sicherheitsüberprüfungsgesetze des Bundes und der Länder sind für die Durchführung von allgemeinen Zuverlässigkeitsprüfungen, z.B. anlässlich von Veranstaltungen, nicht einschlägig. Eine generelle rechtliche Grundlage für Zuverlässigkeitsüberprüfungen besteht außerhalb der spezialgesetzlichen Bestimmungen nicht.

Einwilligungen können - auch wenn die Betroffenen über die Umstände informiert wurden - diese Maßnahme alleine nicht legitimieren. Dies nicht nur deshalb, weil Betroffene oft Nachteile befürchten müssen, wenn sie die Einwilligung verweigern und insoweit eine echte Freiwilligkeit fehlt. Viele Regelungen zu Überprüfungsverfahren verlangen - zusätzlich - zu den materiellen und verfahrensrechtlichen Regelungen die Mitwirkung der betroffenen Personen in Form einer schriftlichen Erklärung bei der Einleitung einer solchen Überprüfung. Außerdem sollen die Vorschriften ein transparentes Verfahren gewährleisten, in dem u.a. die Rechte Betroffener geregelt sind, so etwa das Recht auf Auskunft oder Anhörung vor negativer Entscheidung. Diese flankierenden Schutzmechanismen sind bei Überprüfungsverfahren unerlässlich.

**Anlage 12:** **Entschließung der 75. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 03./04.04.2008 Mehr Augenmaß bei der Novellierung des BKA-Gesetzes**

Der vom Bundesministerium des Innern erarbeitete Referentenentwurf eines Gesetzes zur Abwehr des internationalen Terrorismus durch das Bundeskriminalamt hat zum Ziel, das Bundeskriminalamt mit umfassenden polizeilichen Befugnissen zur Verhütung von terroristischen Straftaten und zur Abwehr von Gefahren für die öffentliche Sicherheit in diesem Zusammenhang auszustatten. Insbesondere sind Befugnisse zur Durchsuchung, Rasterfahndung, Wohnraumüberwachung und Telekommunikationsüberwachung vorgesehen. Außerdem will das Bundesinnenministerium eine Befugnis zum heimlichen Zugriff auf informationstechnische Systeme („Online-Durchsuchung“) in das BKA-Gesetz aufnehmen.

Die Datenschutzbeauftragten des Bundes und der Länder sprechen sich dagegen aus, dass dem Bundeskriminalamt nach dem Gesetzentwurf mehr Befugnisse eingeräumt werden sollen, als einzelnen Landespolizeien zur Erfüllung ihrer eigenen Gefahrenabwehraufgaben zustehen. Sie halten es daher für geboten, im weiteren Gesetzgebungsverfahren die Befugnisse des BKA auf die zur Aufgabenerfüllung zwingend notwendigen Kompetenzen zu beschränken.

Die bisherige informationelle Gewaltenteilung zwischen den Polizeien der Länder und dem BKA diente auch dem Datenschutz. Die Konferenz fordert deshalb eine klare, d.h. hinreichend trennscharfe Abgrenzung der spezifischen Befugnisse des Bundeskriminalamts einerseits zu denen der Landespolizeien und Verfassungsschutzbehörden andererseits.

Dem Referentenentwurf zufolge soll die Aufgabenwahrnehmung durch das Bundeskriminalamt die Zuständigkeit der Landespolizeibehörden auf dem Gebiet der Gefahrenabwehr unberührt lassen. Dies führt zu erheblichen datenschutzrechtlichen Problemen, da nach geltendem Recht auch die Länder bei Abwehr einer durch den internationalen Terrorismus begründeten Gefahr parallele Abwehrmaßnahmen ergreifen können. Angesichts der Weite der für das Bundeskriminalamt vorgesehenen und den Landespolizeibehörden bereits eingeräumten Datenerhebungs- und Datenverarbeitungsbefugnisse steht zu befürchten, dass es zu sich überlappenden und in der Summe schwerwiegenderen Eingriffen in das informationelle Selbstbestimmungsrecht Betroffener durch das Bundeskriminalamt und die Landespolizeibehörden kommen wird.

Ebenso stellt sich die grundsätzliche Frage der Abgrenzung von Polizei und Verfassungsschutz. In den vergangenen Jahren sind die Polizeigesetze des Bundes und der Länder zunehmend mit Befugnissen zur verdeckten Datenerhebung (z.B. heimliche Video- und Sprachaufzeichnungen, präventive Telekommunikationsüberwachung) ausgestattet worden. Zudem wurden die Eingriffsbefugnisse immer weiter ins Vorfeld von Straftaten und Gefahren erstreckt. Damit überschneiden sich die polizeilichen Ermittlungsbefugnisse zunehmend mit denen des Verfassungsschutzes.

Das Bundesverfassungsgericht hat in seinem Urteil zur „Online-Durchsuchung“ vom 27.02.2008 den Gesetzgeber erneut verpflichtet, den unantastbaren Kernbereich privater Lebensgestaltung zu gewährleisten. Diese Vorgabe des Gerichts gilt nicht nur für eine etwaige gesetzliche Regelung zur „Online-Durchsuchung“, sondern für alle Eingriffsmaßnahmen. Die Datenschutzbeauftragten des Bundes und der Länder fordern den Gesetzgeber deshalb auf, im Rahmen der Novellierung des BKA-Gesetzes den Schutz des Kernbereichs privater Lebensgestaltung für alle Eingriffsmaßnahmen zu regeln.

**Anlage 13:** **Entschließung der 75. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 03./04.04.2008 Unzureichender Datenschutz beim deutsch-amerikanischen Abkommen über die Zusammenarbeit der Sicherheitsbehörden**

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder beobachtet mit Sorge, dass die Datenschutzrechte der Bürgerinnen und Bürger im Rahmen der internationalen Zusammenarbeit der Sicherheitsbehörden immer häufiger auf der Strecke bleiben. Aktuelles Beispiel ist das am 11.3.2008 paraphierte deutsch-amerikanische Regierungsabkommen über die Vertiefung der Zusammenarbeit bei der Verhinderung und Bekämpfung schwerwiegender Kriminalität. Die Konferenz fordert Bundestag und Bundesrat auf, dem Abkommen solange nicht zuzustimmen, bis ein angemessener Datenschutz gewährleistet ist.

Mit dem Abkommen wurde ein gegenseitiger Online-Zugriff auf Fundstellendatensätze von daktyloskopischen Daten und DNA-Profilen im hit/no-hit-Verfahren nach dem Muster des Prümer Vertrages vereinbart. Zudem wurden dessen Regelungen über den Austausch personenbezogener Daten zur Verhinderung terroristischer Straftaten weitgehend übernommen. Eine Übertragung des als Bedingung für diese umfangreichen Zugriffs- und Übermittlungsbefugnisse im Prümer Vertrag geschaffenen Datenschutzregimes erfolgte jedoch nicht.

Die Voraussetzungen, unter denen ein Datenaustausch erlaubt ist, sind nicht klar definiert. Der Datenaustausch soll allgemein zur Bekämpfung von Terrorismus und schwerer Kriminalität möglich sein. Welche Straftaten darunter konkret zu verstehen sind, wird nicht definiert. Es erfolgt hier lediglich der Verweis auf das jeweilige nationale Recht. Damit trifft nach dem Abkommen die USA einseitig eine Entscheidung über die Relevanz der abgerufenen Daten.

Bevor in so großem Umfang zusätzliche Datenübermittlungen erlaubt werden, muss zunächst geklärt werden, warum die bisherigen Datenübermittlungsbefugnisse für die internationale Polizeizusammenarbeit mit den USA nicht ausreichen.

Für die weitere Verarbeitung aus Deutschland stammender Daten in den USA bestehen für die Betroffenen praktisch keine Datenschutzrechte. Das Abkommen selbst räumt den Betroffenen keine eigenen Rechte ein, sondern verweist auch hierzu auf die Voraussetzungen im Recht der jeweiligen Vertragspartei. In den USA werden aber Datenschutzrechte, wie sie in der Europäischen Union allen Menschen zustehen, ausschließlich Bürgerinnen und Bürgern der Vereinigten Staaten von Amerika und dort wohnenden Ausländerinnen und Ausländern gewährt. Anderen Personen stehen Rechtsansprüche auf Auskunft über die Verarbeitung der eigenen Daten, Löschung unzulässig erhobener oder nicht mehr erforderlicher Daten oder Berichtigung unrichtiger Daten nicht zu. Außerdem besteht in den USA keine unabhängige Datenschutzkontrolle. Vor diesem Hintergrund sind die im Abkommen enthaltenen weiten Öffnungsklauseln für die weitere Verwendung der ausgetauschten Daten sowie der Verzicht auf Höchstspeicherfristen aus datenschutzrechtlicher Sicht nicht akzeptabel.

**Anlage 14:** **Entschließung der 75. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 03./04.04.2008 Berliner Erklärung: Herausforderungen für den Datenschutz zu Beginn des 21. Jahrhunderts**

Regelungen insbesondere zum großen Lauschangriff, zur Telekommunikationsüberwachung, zur Rasterfahndung, zur Online-Durchsuchung, zur automatischen Auswertung von Kfz-Kennzeichen und zur Vorratsspeicherung von Telekommunikationsdaten haben die verfassungsrechtlich zwingende Balance zwischen Sicherheitsbefugnissen der staatlichen Behörden und persönlicher Freiheit der Bürgerinnen und Bürger missachtet. Das Bundesverfassungsgericht hat mit einer Reihe von grundlegenden Entscheidungen diese Balance wieder hergestellt und damit auch den Forderungen der Datenschutzbeauftragten des Bundes und der Länder größtenteils Rechnung getragen.

Die Herausforderungen für den Datenschutz gehen aber weit über die genannten Bereiche hinaus. Datenverarbeitungssysteme dringen immer stärker in alle Lebensbereiche ein und beeinflussen den Alltag. Das Internet ist zum Massenmedium geworden. Vielfältig sind dabei die Möglichkeiten, das persönliche Verhalten zu registrieren und zu bewerten. Der nächste Quantensprung der Informationstechnik steht unmittelbar bevor: Die Verknüpfung von Informationstechnik mit Körperfunktionen, insbesondere bei der automatisierten Messung medizinischer Parameter und bei der Kompensation organischer Beeinträchtigungen. Die Miniaturisierung von IT-Systemen geht so weit, dass demnächst einzelne Komponenten nicht mehr mit bloßem Auge wahrgenommen werden können (Nanotechnologie).

Das Handeln staatlicher und nicht-öffentlicher Stellen ist verstärkt darauf gerichtet, viele Daten ohne klare Zweckbestimmung zu sammeln, um sie anschließend vielfältig auszuwerten, beispielsweise um versteckte Risiken aufzudecken oder um persönliches Verhalten unbemerkt zu beeinflussen. Geht es der Wirtschaft etwa darum, durch Scoringverfahren die Kundinnen und Kunden vorab einzuschätzen, gewinnt die immer exzessivere Registrierung und automatisierte Beobachtung für staatliche Stellen an Bedeutung. In beiden Bereichen wird ganz normales Verhalten registriert, unabhängig von konkreten Gefahren oder Verdachtsmomenten. Auch diejenigen, die sich nichts haben zu schulden kommen lassen, werden einem verstärkten Kontroll- und Anpassungsdruck ausgesetzt, der Einschüchterungseffekte zur Folge haben wird.

Der Schutz der Grundrechte, nicht zuletzt des Datenschutzes, dient in einer demokratischen Gesellschaft auch dem Gemeinwohl und ist zunächst Aufgabe jeglicher Staatsgewalt. Darüber hinaus ist er eine gesamtgesellschaftliche Aufgabe. Schließlich ist jede Bürgerin und jeder Bürger auch zur Eigenverantwortung aufgerufen. Hilfen zum informationellen Selbstschutz müssen zur Verfügung gestellt werden, die es den Betroffenen ermöglichen, eine Erfassung ihres Verhaltens zu vermeiden und selbst darüber zu entscheiden, ob und wem gegenüber sie Daten offenbaren. Von zunehmender Bedeutung sind auch Projekte, die das Datenschutzbewusstsein fördern, um vor allem jüngere Menschen von einem fahrlässigen Umgang mit ihren persönlichen Daten abzuhalten.

Alle diese Maßnahmen tragen zur Entwicklung einer neuen Datenschutzkultur bei. Voraussetzung dafür ist auch, dass nicht länger versucht wird, die verfassungsrechtlichen Grenzen und Spielräume auszureizen. Stattdessen muss dem Gebot der Datenvermeidung und -sparsamkeit Rechnung getragen werden.

**Anlage 15:** **Entschließung der 75. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 03./04.04.2008 Datenschutzförderndes Identitätsmanagement statt Personenkennzeichen**

Elektronische Identitäten sind der Schlüssel zur Teilnahme an der digitalen Welt. Die Möglichkeiten der pseudonymen Nutzung, die Gewährleistung von Datensparsamkeit und -sicherheit und der Schutz vor Identitätsdiebstahl und Profilbildung sind wichtige Grundpfeiler moderner Informations- und Kommunikationstechnologien. Darauf hat die Bundesregierung zu Recht anlässlich des Zweiten Nationalen IT-Gipfels im Dezember 2007 (Hannoversche Erklärung) hingewiesen.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder weist darauf hin, dass der gesetzliche Rahmen für die anonyme oder pseudonyme Nutzung elektronischer Verfahren bereits seit langem vorhanden ist. Beispielsweise hat jeder Diensteanbieter die Nutzung von Telemedien und ihre Bezahlung anonym oder unter Pseudonym zu ermöglichen, soweit dies technisch möglich und zumutbar ist (§ 13 Abs. 6 Telemediengesetz).

Bisher werden jedoch anonyme oder pseudonyme Nutzungsmöglichkeiten nur sehr selten angeboten. Vielmehr speichern Wirtschaft und Verwaltung immer mehr digitale Daten mit direktem Personenbezug. Erschlossen werden diese Datenbestände in der Regel über einheitliche Identifizierungsnummern. Mit der lebenslang geltenden, bundeseinheitlichen Steuer-Identifikationsnummer (Steuer-ID) oder der mit der Planung der Gesundheitskarte zusammenhängenden, ebenfalls lebenslang geltenden Krankenversichertennummer werden derzeit solche Merkmale eingeführt. Auch mit der flächendeckenden Einführung des ePersonalausweises wird jeder Bürgerin und jedem Bürger eine elektronische Identität zugewiesen, mit der sie bzw. er sich künftig auch gegenüber eGovernment-Portalen der Verwaltung oder eCommerce-Angeboten der Wirtschaft identifizieren soll.

Einheitliche Personenkennzeichen bergen erhebliche Risiken für das Recht auf informationelle Selbstbestimmung. So könnte sich aus der Steuer-ID ein Personenkennzeichen entwickeln, über das alle möglichen Datenbestände personenbezogen verknüpft und umfassende Persönlichkeitsprofile erstellt werden. Angesichts der stetig verbesserten technischen Möglichkeiten, zunächst verteilt gespeicherte Daten anwendungsübergreifend zu verknüpfen, wachsen entsprechende Begehrlichkeiten.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder weist darauf hin, dass die effektive Nutzung von Informationstechnik und hohe Datenschutzstandards keinen Widerspruch bilden. Ein datenschutzförderndes Identitätsmanagement kann den Einzelnen vor unangemessener Überwachung und Verknüpfung seiner Daten schützen und zugleich eine moderne und effektive Datenverarbeitung ermöglichen. Entsprechende EU-Projekte wie PRIME (Privacy and Identity Management for Europe) und FIDIS (Future of Identity in the Information Society) werden im Rahmen des 6. Europäischen Forschungsprogramms „Technologien für die Informationsgesellschaft“ gefördert.

Identitätsmanagement sollte auf der anonymen oder pseudonymen Nutzung von elektronischen Verfahren und der dezentralen Haltung von Identifikationsdaten unter möglichst weitgehender Kontrolle der betroffenen Bürgerinnen und Bürger basieren. Datenschutzfördernde Identitätsmanagementsysteme schließen Verknüpfungen nicht aus, wenn die Nutzenden es wünschen oder wenn dies gesetzlich vorgesehen ist. Sie verhindern jedoch, dass unkontrolliert der Bezug zwischen einer elektronischen Identität und einer Person hergestellt werden kann. Unter bestimmten, klar definierten Bedingungen kann mit Hilfe von Identitätsmanagementsystemen sichergestellt werden, dass ein Pseudonym bei Bedarf bezogen auf einen bestimmten Zweck (z.B. Besteuerung) einer Person zugeordnet werden kann.

Identitätsmanagementsysteme werden nur dann die Akzeptanz der Nutzerinnen und Nutzer finden, wenn sie einfach bedienbar sind, ihre Funktionsweise für alle Beteiligten transparent ist, möglichst alle Komponenten standardisiert sind und die Technik von unabhängigen Dritten jederzeit vollständig nachprüfbar ist.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder fordert die Bundesregierung daher auf, den Absichtserklärungen des IT-Gipfels Taten folgen zu lassen und den Einsatz datenschutzfördernder Identitätsmanagementsysteme voranzutreiben. Sowohl die öffentliche Verwaltung als auch die Wirtschaft sollte die Einführung solcher datenschutzfördernder Systeme unterstützen.

**Anlage 16:** **Entschließung der 75. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 03./04.04.2008 Medienkompetenz und Datenschutzbewusstsein in der jungen „online-Generation“**

1. Die Nutzung moderner Informationssysteme ist auch mit Risiken verbunden. Diese begründen ein besonderes Schutzbedürfnis der Bürgerinnen und Bürger. Dieses verlangt aber nicht nur rechtliche Vorkehrungen und Sicherungen, sondern auch Aufklärung und Infor-

mation darüber, mit welchen Risiken die Nutzung dieser Informationssysteme verbunden sind. Dies gilt vor allem für die junge „online-Generation“, die in der Altersgruppe der 14- bis 19-Jährigen zu 96 % regelmäßig das Internet nutzt und zwar im Durchschnitt länger als zweieinhalb Stunden täglich.

2. Die Datenschutzbeauftragten des Bundes und der Länder sehen es daher als wichtige Aufgabe an, Kinder und Jugendliche für einen sorgsamen und verantwortungsbewussten Umgang mit den eigenen Daten und den Daten anderer zu sensibilisieren. Diese Aufgabe obliegt gesellschaftlichen Einrichtungen ebenso wie staatlichen Organen.

   Die Erfahrungen, die anlässlich des 2. Europäischen Datenschutztages am 28.01.2008 gemacht wurden, stützen dies. Zu dem Motto „Datenschutz macht Schule“ wurde von den Datenschutzbeauftragten des Bundes und der Länder eine Vielzahl von Veranstaltungen und Schulbesuchen organisiert. Eltern, Lehrkräfte, Schülerinnen und Schüler, aber auch Studierende hatten dabei die Möglichkeit, sich z.B. bei Podiumsdiskussionen, Rollenspielen und Workshops über datenschutzrelevante Fragen bei der Nutzung moderner Medien zu informieren. Die dabei gewonnenen Erfahrungen lassen nicht nur einen enormen Informationsbedarf, sondern auch ein großes Informationsinteresse erkennen, und zwar bei allen Beteiligten, bei den Jugendlichen ebenso wie bei ihren Eltern und den Lehrkräften.

   Bei den Informationsangeboten, die derzeit den Schulen angeboten werden, um die Medienkompetenz junger Menschen zu verbessern, spielt das Thema „Datenschutz“ aber nur eine untergeordnete Rolle. Es beschränkt sich überwiegend auf Fragen der Datensicherheit und wird zudem häufig von Fragen des Jugendmedienschutzes und des Verbraucherschutzes überlagert.

3. Die Datenschutzbeauftragten des Bundes und der Länder halten es daher für notwendig, dass die für die schulische Bildung zuständigen Ministerinnen und Minister der Landesregierungen bei der Förderung der Medienkompetenz von Kindern und Jugendlichen - schon im Grundschulalter - deren Datenschutzbewusstsein stärken. Der Datenschutz muss bei den Angeboten und Projekten zur Förderung der Medienkompetenz eine größere Rolle spielen. Die bisherigen Ansätze reichen bei weitem nicht aus. Gerade bei jungen Menschen muss das Bewusstsein über den Datenschutz als Bürgerrecht und Bestandteil unserer demokratischen Ordnung stärker gefördert werden.

## Anlage 17: Entschließung der 75. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 03./04.04.2008 Keine Vorratsspeicherung von Flugpassagierdaten

Die EU-Kommission hat den Entwurf eines Rahmenbeschlusses des Rates zur Speicherung von Flugpassagierdaten und zu deren Weitergabe an Drittstaaten vorgelegt. Künftig sollen die Fluggesellschaften bei Flügen aus der EU und in die EU zu jedem Fluggast insgesamt 19 Datenelemente, bei unbegleiteten Minderjährigen sechs weitere Datenelemente, an eine von dem jeweiligen Mitgliedstaat bestimmte „Zentralstelle“ übermitteln. Die Daten sollen bei den Zentralstellen anlass- und verdachtsunabhängig insgesamt 13 Jahre lang personenbezogen gespeichert werden und zur Durchführung von Risikoanalysen dienen. Unter im Einzelnen noch unklaren Voraussetzungen sollen die Daten an Strafverfolgungsbehörden von Nicht-EU-Staaten (z.B. die USA), übermittelt werden dürfen. Neben Grunddaten zur Person, über Reiseverlauf, Buchungs- oder Zahlungsmodalitäten und Sitzplatzinformationen sollen auch andere persönliche Angaben gespeichert werden. Unklar ist, welche Daten unter „allgemeine Hinweise“ gespeichert werden dürfen. Denkbar wäre, dass beispielsweise besondere Essenswünsche erfasst werden.

Mit der beabsichtigten Vorratsspeicherung und der Datenübermittlung wird die EU es auswärtigen Staaten ermöglichen, Bewegungsbilder auch von EU-Bürgerinnen und -Bürgern zu erstellen. In Zukunft besteht die Gefahr, dass Menschen Angst haben werden, durch ihre Reisegewohnheiten aufzufallen.

Die in dem Rahmenbeschluss vorgesehene Vorratsdatenspeicherung von Daten sämtlicher Fluggäste, die EU-Grenzen überschreiten, verstößt nicht nur gegen Art. 8 der Europäischen Menschenrechtskonvention und die Europaratskonvention 108, sondern ist auch mit dem im Grundgesetz verankerten Recht auf informationelle Selbstbestimmung nicht vereinbar. Grundrechtseingriffe „ins Blaue hinein“, also Maßnahmen ohne Nähe zu einer abzuwehrenden Gefahr sind unzulässig.

Der Vorschlag für den Rahmenbeschluss erfolgte, ohne den Nutzen der erst jüngst in nationales Recht umgesetzten Richtlinie 2004/82/EG, die bereits alle Beförderungsunternehmen verpflichtet, die Daten von Reisenden an die Grenzkontrollbehörden zu übermitteln, auszuwerten. Hinzu kommt, dass der Vorschlag kaum datenschutzrechtliche Sicherungen enthält. Er bezieht sich nur auf eine bisher nicht bestehende und im Entwurf mit Mängeln behaftete EU-Datenschutzregelung. Diese Mängel wirken sich dadurch besonders schwerwiegend aus, dass in den Drittstaaten ein angemessenes Datenschutzniveau

nicht immer gewährleistet ist und eine Änderung dieser Situation auch in Zukunft nicht zu erwarten ist.

Die EU-Kommission hat nicht dargelegt, dass vergleichbare Maßnahmen in den USA, in Kanada oder in Großbritannien einen realen, ernst zu nehmenden Beitrag zur Erhöhung der Sicherheit geleistet hätten. Sie hat die kritischen Stellungnahmen der nationalen und des Europäischen Datenschutzbeauftragten sowie der Art. 29-Datenschutzgruppe nicht berücksichtigt.

Die Konferenz fordert die Bundesregierung auf, den Entwurf abzulehnen. Sie teilt die vom Bundesrat geäußerten Bedenken an der verfassungsrechtlichen Zulässigkeit der Speicherung der Passagierdaten.

**Anlage 18:** **Entschließung der 75. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 03./04.04.2008 Vorgaben des Bundesverfassungsgerichts bei der Online-Durchsuchung beachten**

1. Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder begrüßt, dass das Bundesverfassungsgericht die Regelung zur Online-Durchsuchung im Verfassungsschutzgesetz Nordrhein-Westfalen für nichtig erklärt hat. Hervorzuheben ist die Feststellung des Gerichts, dass das allgemeine Persönlichkeitsrecht auch das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme umfasst. 25 Jahre nach dem Volkszählungsurteil hat das Bundesverfassungsgericht damit den Datenschutz verfassungsrechtlich weiter gestärkt und ihn an die Herausforderungen des elektronischen Zeitalters angepasst.

2. Ein solches Grundrecht nimmt auch den Staat in die Verantwortung, sich aktiv für die Vertraulichkeit und Integrität informationstechnischer Systeme einzusetzen. Das Bundesverfassungsgericht verpflichtet den Staat, im Zeitalter der elektronischen Kommunikation Vertraulichkeit zu gewährleisten. Nunmehr ist der Gesetzgeber gehalten, diesen Auftrag konsequent umzusetzen. Dazu müssen die Regelungen, welche die Bürgerinnen und Bürger vor einer „elektronischen Ausforschung“ schützen sollen, gemäß den Vorgaben des Gerichts insbesondere im Hinblick auf technische Entwicklungen verbessert werden. Hiermit würde auch ein wesentlicher Beitrag geleistet, Vertrauen in die Sicherheit von E-Government- und E-Commerce-Verfahren herzustellen.

3. Die Konferenz unterstützt die Aussagen des Gerichts zum technischen Selbstschutz der Betroffenen. Ihre Möglichkeiten, sich gegen einen unzulässigen Datenzugriff zu schützen, etwa durch den Einsatz von Verschlüsselungsprogrammen, dürfen nicht unterlaufen oder eingeschränkt werden.

4. Die Konferenz begrüßt außerdem, dass das Bundesverfassungsgericht das neue Datenschutzgrundrecht mit besonders hohen verfassungsrechtlichen Hürden vor staatlichen Eingriffen schützt. Sie fordert die Gesetzgeber in Bund und Ländern auf, diese Eingriffsvoraussetzungen zu respektieren. Die Konferenz spricht sich in diesem Zusammenhang gegen Online-Durchsuchungen durch die Nachrichtendienste aus.

5. Das Bundesverfassungsgericht hat den Gesetzgeber erneut verpflichtet, den unantastbaren Kernbereich privater Lebensgestaltung auch bei Eingriffen in informationstechnische Systeme zu gewährleisten. Unvermeidbar erhobene kernbereichsrelevante Inhalte sind unverzüglich zu löschen. Eine Weitergabe oder Verwertung dieser Inhalte ist auszuschließen.

6. Auch wenn Online-Durchsuchungen innerhalb der durch das Bundesverfassungsgericht festgelegten Grenzen verfassungsgemäß sind, fordert die Konferenz die Gesetzgeber auf, die Erforderlichkeit von Online-Durchsuchungsbefugnissen kritisch zu hinterfragen. Sie müssen sich die Frage stellen, ob sie den Sicherheitsbehörden entsprechende Möglichkeiten an die Hand geben wollen. Die Konferenz bezweifelt, dass dieser weiteren Einbuße an Freiheit ein adäquater Gewinn an Sicherheit gegenüber steht.

7. Sollten gleichwohl Online-Durchsuchungen gesetzlich zugelassen werden, sind nicht nur die vom Bundesverfassungsgericht aufgestellten verfassungsrechtlichen Hürden zu beachten. Die Konferenz hält für diesen Fall zusätzliche gesetzliche Regelungen für erforderlich. Zu ihnen gehören vor allem folgende Punkte:

   - Soweit mit der Vorbereitung und Durchführung von Online-Durchsuchungen der Schutzbereich von Art. 13 GG (Unverletzlichkeit der Wohnung) betroffen ist, bedarf es dafür jedenfalls einer besonderen Rechtsgrundlage.

   - Der vom Bundesverfassungsgericht geforderte Richtervorbehalt ist bei Online-Durchsuchungen mindestens so auszugestalten wie bei der akustischen Wohnraumüberwachung. Ergänzend zu

einer richterlichen Vorabkontrolle ist eine begleitende Kontrolle durch eine unabhängige Einrichtung vorzuschreiben.

- Gesetzliche Regelungen, welche Online-Durchsuchungen zulassen, sollten befristet werden und eine wissenschaftliche Evaluation der dabei gewonnenen Erkenntnisse und Erfahrungen anordnen.

- Informationstechnische Systeme, die von zeugnisverweigerungsberechtigten Berufsgruppen genutzt werden, sind von heimlichen Online-Durchsuchungen auszunehmen.

- Für die Durchführung von „Quellen-Telekommunikationsüberwachungen“, die mit der Infiltration von IT-Systemen einhergehen, sind die gleichen Schutzvorkehrungen zu treffen wie für die Online-Durchsuchung selbst.

8. Schließlich sind die Gesetzgeber in Bund und Ländern aufgrund der Ausstrahlungswirkung der Entscheidung des Bundesverfassungsgerichts gehalten, die sicherheitsbehördlichen Eingriffsbefugnisse in Bezug auf informationstechnische Systeme, z.B. bei der Überwachung der Telekommunikation im Internet sowie der Beschlagnahme und Durchsuchung von Speichermedien, grundrechtskonform einzuschränken.

**Anlage 19:** **Entschließung der 75. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 03./04.04.2008 Keine Daten der Sicherheitsbehörden an Arbeitgeber zur Überprüfung von Arbeitnehmerinnen und Arbeitnehmern**

Die Datenschutzbeauftragten des Bundes und der Länder wenden sich entschieden gegen die Übermittlung polizeilicher und nachrichtendienstlicher Erkenntnisse an Arbeitgeber zur Überprüfung von Bewerberinnen und Bewerbern, Beschäftigten und Fremdpersonal (z.B. Reinigungskräfte) außerhalb gesetzlicher Grundlagen. In zunehmendem Maß bitten Arbeitgeber die Betroffenen, in eine Anfrage des Arbeitgebers bei der Polizei oder dem Verfassungsschutz zu etwaigen dort vorliegenden Erkenntnissen zu ihrer Person einzuwilligen. In anderen Fällen sollen die Betroffenen eine solche Auskunft („fremdbestimmte Selbstauskunft“) selbst einholen und ihrem Arbeitgeber vorlegen. Eine solche „Einwilligung des Betroffenen“ ist regelmäßig keine wirksame Einwilligung. Die Betroffenen sehen sich oftmals dem faktischen Druck des Wohlverhaltens zum Zwecke des Erhalts und der Sicherung des Arbeitsplatzes ausgesetzt.

Die gesetzliche Grundentscheidung, in einem „Führungszeugnis“ dem Arbeitgeber nur ganz bestimmte justizielle Informationen zu einer Person verfügbar zu machen, wird dadurch unterlaufen. Es stellt einen Dammbruch dar, wenn jeder Arbeitgeber durch weitere Informationen direkt oder indirekt an dem Wissen der Sicherheitsbehörden und Nachrichtendienste teilhaben kann. Die Übermittlung dieser Informationen an Arbeitgeber kann auch den vom Bundesarbeitsgericht zum „Fragerecht des Arbeitgebers“ getroffenen Wertentscheidungen widersprechen. Danach darf der Arbeitgeber die Arbeitnehmerinnen und Arbeitnehmer bei der Einstellung nach Vorstrafen und laufenden Ermittlungsverfahren fragen, wenn und soweit die Art des zu besetzenden Arbeitsplatzes dies erfordert.

Polizei und Nachrichtendienste speichern - neben den in ein „Führungszeugnis“ aufzunehmenden Daten - auch personenbezogene Daten, die in das Bundeszentralregister gar nicht erst eingetragen werden oder Arbeitgebern in einem „Führungszeugnis“ nicht übermittelt werden dürfen. Es stellt eine grundsätzlich unzulässige Durchbrechung des Zweckbindungsgrundsatzes dar, wenn ein Arbeitgeber diese Daten - über den Umweg über die Polizei oder einen Nachrichtendienst - für Zwecke der Personalverwaltung erhält. Dabei ist besonders zu beachten, dass polizeiliche oder nachrichtendienstliche Daten nicht zwingend gesicherte Erkenntnisse sein müssen, sondern oftmals lediglich Verdachtsmomente sind. Die Folgen von Missdeutungen liegen auf der Hand.

**Anlage 20:** **Entschließung der 76. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 06./07.11.2008 Abfrage von Telekommunikationsverkehrsdaten einschränken: Gesetzgeber und Praxis müssen aus wissenschaftlichen Erkenntnissen Konsequenzen ziehen**

Das Max-Planck-Institut für ausländisches und internationales Strafrecht in Freiburg hat im Auftrag des Bundesministeriums der Justiz die Nutzung von Telekommunikationsverkehrsdaten für Zwecke der Strafverfolgung (§§ 100 g, 100 h StPO alte Fassung) evaluiert. Die Studie geht zu Recht davon aus, dass Verkehrsdaten ein hohes Überwachungspotential in sich tragen und besser als andere Daten dazu geeignet sind, soziale Netzwerke nachzuweisen, Beziehungen zu identifizieren und Informationen über Individuen

zu generieren. Der Studie zufolge ist die Zahl der Verkehrsdatenabfragen erheblich und kontinuierlich von 10.200 (2002) auf 40.000 Abfragen (2005) angestiegen. Zudem erfasst die Maßnahme regelmäßig auch eine Vielzahl unbescholtener Bürgerinnen und Bürger.

Das Bundesministerium der Justiz hat die Studie erst im Februar dieses Jahres und somit nach der Neuregelung der Telekommunikationsüberwachung und Einführung der Vorratsdatenspeicherung veröffentlicht. Das Gutachten liefert Erkenntnisse, deren Berücksichtigung im Gesetz vom 21.12.2007 erforderlich gewesen wäre. Die Datenschutzbeauftragten des Bundes und der Länder sehen sich durch die Studie in ihrer schon früher geäußerten Kritik (vgl. ihre Entschließung vom 08./09.03.2007) bestätigt. Sie fordern den Gesetzgeber auf, die gesetzliche Regelung unter folgenden Aspekten nun zügig nachzubessern:

- Die Straftatenschwelle für Verkehrsdatenabfragen sollte insbesondere im Hinblick auf die inzwischen eingeführte Vorratsdatenspeicherung auf schwere Straftaten angehoben werden. Ein bedeutsamer Anteil der überprüften Verfahren war allenfalls der mittleren Kriminalität zuzuordnen.

- Die gesetzliche Höchstdauer der Maßnahme sollte von drei auf zwei Monate reduziert werden. Das Gutachten hat gezeigt, dass die praktischen Bedürfnisse, wie sie sich in den Aktendaten und Befragungsergebnissen äußern, dadurch vollständig abgedeckt würden.

- Für die Verkehrsdatenabfrage sollten (nach dem Vorbild der Regelungen für die akustische Wohnraumüberwachung) qualifizierte Begründungspflichten in der StPO vorgesehen werden. Dabei sollten auch die Rechtsfolgen für erhebliche Verstöße gegen die Begründungsanforderungen gesetzlich geregelt werden (z.B. Beweisverwertungsverbote). Wesentliche Kritikpunkte der Studie waren insbesondere die lediglich formelhafte Wiedergabe des Gesetzestextes sowie die häufig wörtliche Übernahme der staatsanwaltschaftlichen Anträge in den Begründungen.

- Zur Vermeidung von Rechtsunsicherheit und zur Stärkung des Richtervorbehalts sollte in den Fällen staatsanwaltschaftlicher Eilanordnung die Verwertbarkeit der erlangten Daten davon abhängig gemacht werden, dass ein Gericht rückwirkend die formelle und materielle Rechtmäßigkeit der Maßnahme feststellt. Dem Gutachten zufolge besteht insbesondere bei den Telekommunikationsunternehmen Unsicherheit, inwieweit sie zur Herausgabe der Verkehrsdaten verpflichtet sind, wenn eine staatsanwaltschaftliche Eilanordnung nicht innerhalb der gesetzlichen Frist richterlich bestätigt wird.

- Der tatsächliche Nutzen der Vorratsdatenspeicherung für die Strafverfolgung und damit die Erforderlichkeit der Maßnahme müssen in Frage gestellt werden. Bereits bei der früheren Höchstspeicherdauer von 3 Monaten waren nach der Studie 98 % der Abfragen erfolgreich.

Auch in der praktischen Anwendung der Regelungen zur Verkehrsdatenabfrage hat die Studie Defizite deutlich gemacht. Die Datenschutzbeauftragten des Bundes und der Länder appellieren daher auch an die Strafverfolgungsbehörden und Gerichte, aus dem Gutachten Konsequenzen zu ziehen. Besonderes Augenmerk ist vor allem auf die Prüfung der Angemessenheit der Maßnahme zu richten. Dies muss auch in substantiierten Begründungen zum Ausdruck kommen. Die gesetzlich festgeschriebenen, dem Grundrechtsschutz dienenden Benachrichtigungs-, Löschungs- und Dokumentationspflichten müssen - trotz hoher Belastungen in der Praxis - unbedingt eingehalten werden. Der Richtervorbehalt muss seine grundrechtssichernde Funktion effizient erfüllen können. Die Justizverwaltungen sind in der Verantwortung, hierfür ausreichende personelle Ressourcen zur Verfügung zu stellen.

Eine Fortführung der wissenschaftlichen Evaluation der Verkehrsdatenabfrage ist - unter den neuen rechtlichen Rahmenbedingungen und aufgrund der Weiterentwicklung der Technik - unerlässlich. Insbesondere sollten dabei Notwendigkeit und Nutzen der Verkehrsdatenabfrage - auch im Vergleich zu anderen möglichen Maßnahmen - mit Blick auf den Verhältnismäßigkeitsgrundsatz auf den Prüfstand gestellt werden.

**Anlage 21:** **Entschließung der 76. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 06./07.11.2008 Gegen Blankettbefugnisse für die Software-Industrie**

Gegenwärtig wird auf europäischer Ebene über Änderungen der Richtlinie zum Datenschutz in der elektronischen Kommunikation (2002/58/EG) beraten. Dabei geht es auch um die Frage, ob in Zukunft einzelfallunabhängig Verkehrsdaten zur Gewährleistung der Netz- und Informationssicherheit, also etwa zur Verfolgung von Hackerangriffen, verarbeitet werden dürfen.

Bereits auf der Grundlage der geltenden Richtlinie erlaubt § 100 Telekommunikationsgesetz den Telekommunikationsdiensteanbietern eine zielgerichtete, einzelfallbezogene Datenverarbeitung zur Fehlerbe-

seitigung und Missbrauchsbekämpfung. Diese Regelung hat sich in der Praxis bewährt. Es ist daher nicht erforderlich, zur Gewährleistung der Netz- und Informationssicherheit einzelfallunabhängig personenbezogene Verkehrsdaten zu speichern. Die Anbieter von Telekommunikationsdiensten sind aufgefordert, ihre Systeme so sicher zu gestalten, dass Angriffe von vornherein erfolglos bleiben.

Obwohl die Europäische Kommission eine Änderung der bisherigen Rechtslage nicht für erforderlich hält, schlagen mehrere Mitgliedstaaten bei den gegenwärtigen Beratungen im Rat vor, entsprechend den Vorstellungen der Software-Industrie (Business Software Alliance) eine generelle Ermächtigung in die Richtlinie aufzunehmen, wonach *„jede natürliche oder juristische Person mit einem berechtigten Interesse“* berechtigt sein soll, Verkehrsdaten zu verarbeiten, um „technische Maßnahmen zur Gewährleistung der Sicherheit eines öffentlichen Telekommunikationsdienstes, eines öffentlichen oder privaten Telekommunikationsnetzes, eines Dienstes der Informationsgesellschaft oder von Endgeräten zu deren Nutzung“ zu ergreifen. Damit wäre nicht nur der jeweilige Diensteanbieter, der Maßnahmen zum Schutz des eigenen Angebots treffen will, zur einzelfallunabhängigen Speicherung von Verkehrsdaten berechtigt, sondern praktisch jeder mit einem wirtschaftlichen Verarbeitungsinteresse, insbesondere auch die Hersteller von Sicherheitssoftware.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder lehnt eine solche zeitlich unbegrenzte und inhaltlich unbestimmte Blankett-Ermächtigung als inakzeptabel ab. Der Hinweis auf die „Informationssicherheit“ rechtfertigt es nicht, dass Verkehrsdaten nahezu uferlos auch von Dritten verarbeitet werden. Die Bundesregierung wird aufgefordert, einer derartigen Aufweichung des Telekommunikationsgeheimnisses im Rat ihre Zustimmung zu verweigern.

**Anlage 22: Entschließung der 76. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 06./07.11.2008 Weiterhin verfassungsrechtliche Zweifel am ELENA-Verfahren**

Die Bundesregierung hat am 25.06.2008 den Gesetzentwurf über das Verfahren des elektronischen Entgeltnachweises (ELENA-Verfahrensgesetz) beschlossen (BT-Drs. 16/10492). Danach haben Beschäftigte die monatliche Übermittlung ihrer Einkommensdaten an die Zentrale Speicherstelle zu dulden, obwohl zurzeit nicht verlässlich abgeschätzt werden kann, in welchem Umfang die Speicherung der Daten tatsächlich erforderlich ist. Ein großer Anteil der Betroffenen wird die dem Anwendungsbereich des ELENA-Verfahrens unterfallenden Sozialleistungen niemals oder erst zu einem erheblich späteren Zeitpunkt geltend machen. Es steht somit bereits jetzt zu vermuten, dass eine große Zahl der übermittelten Daten von der Zentralen Speicherstelle wieder zu löschen sein wird, ohne jemals für irgendein Verfahren genutzt worden zu sein.

Die Datenschutzbeauftragten des Bundes und der Länder haben deshalb wiederholt verfassungsrechtliche Bedenken unter dem Gesichtspunkt der Verhältnismäßigkeit und speziell der Erforderlichkeit geltend gemacht und eine substantiierte Begründung gefordert. Diese ist nicht erfolgt. Bisher bestehen lediglich höchst vage Erwartungen auf langfristige Effizienzsteigerungen insbesondere der Arbeitsverwaltung. Angesichts dieser Unklarheiten verbleiben erhebliche Zweifel an der Verfassungsmäßigkeit des Gesetzes. Hinzu kommt, dass derartige umfangreiche Datensammlungen Begehrlichkeiten wecken, die Daten für andere Zwecke zu verwenden.

Für den Fall, dass diese verfassungsrechtlichen Bedenken ausgeräumt werden können, sind unter dem Gesichtspunkt des *technisch-organisatorischen Datenschutzes* noch folgende Verbesserungen durch den Gesetz- bzw. Verordnungsgeber erforderlich:

- Es muss sichergestellt werden, (z.B. durch die Einrichtung eines Verwaltungsausschusses der Zentralen Speicherstelle), dass unter Mitwirkung von Datenschutzbeauftragten gemeinsame Grundsätze zur Wahrung des Datenschutzes und der technischen Sicherheit berücksichtigt werden.

- Für die Zentrale Speicherstelle muss ein Datenschutzbeauftragter eingesetzt werden, der dazu verpflichtet ist, regelmäßig an den Verwaltungsausschuss zu berichten.

- Schlüssel zur Ver- und Entschlüsselung der bei der Zentralen Speicherstelle gespeicherten Daten dürfen nicht in der Verfügungsgewalt der Zentralen Speicherstelle liegen. Die Ver- und Entschlüsselungskomponente muss von einer unabhängigen Treuhänderstelle verantwortet werden.

- Mittelfristig ist ein Verfahren anzustreben, das die technische Verfügungsmöglichkeit über die individuellen Daten den Betroffenen überträgt.

- Das im Rahmen der ELENA-Modellvorhaben erarbeitete differenzierte Löschungskonzept muss weiterentwickelt und umgesetzt werden.

- Für abrufende Stellen sind starke Authentisierungsverfahren vorzuschreiben, die dem Stand der Technik entsprechen und den Forderungen

der Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 11.10.2006 zur sachgemäßen Nutzung von Authentisierungs- und Signaturverfahren genügen.

- Für die technischen Komponenten muss eine Zertifizierung durch eine unabhängige Prüfung vorgeschrieben werden.

**Anlage 23: Entschließung der 76. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 06./07.11.2008 Datenschutzgerechter Zugang zu Geoinformationen**

Die Einführung einer einheitlichen Geodateninfrastruktur und die Veröffentlichung der staatlichen Daten eröffnen ein großes Potential an volkswirtschaftlichem Nutzen und ist geeignet, vielen E-Government- und E-Commerce-Anwendungen die erforderliche Infrastruktur zur Verfügung zu stellen. Als einen ersten Schritt regelt das europäische Recht mit der so genannten INSPIRE-Richtlinie, die bis Mai 2009 in nationales Recht umgesetzt werden muss, die Bereitstellung von amtlichen Geodaten nach einheitlichen Standards für europaweite behördliche, kommerzielle und private Nutzungen.

Durch diese neue Infrastruktur werden georeferenzierbare Angaben auf Grund der Erschließungsmöglichkeit über Wohnanschriften oder Eigentümer- bzw. Standortdaten als personenbezogene Daten zur Verfügung gestellt. Diesem Umstand müssen die gesetzlichen Regelungen gerecht werden und angemessene Datenschutzregelungen enthalten.

Bei der Bereitstellung amtlicher Geodaten ist sowohl nach der europäischen Richtlinie als auch nach deutschem Verfassungsrecht der Schutz personenbezogener Daten angemessen zu gewährleisten. Der Entwurf der Bundesregierung zur Umsetzung dieser Richtlinie in einem Geodatenzugangsgesetz (BT-Drs. 16/10530) sieht eine entsprechende Anwendung der Schutzvorschriften des Umweltinformationsgesetzes vor. Im Gegensatz zum einzelfallbezogenen Zugang nach den Umweltinformationsgesetzen birgt der im Entwurf eines Geodatenzugangsgesetzes vorgesehene massenhafte Abruf solcher Daten aber ein höheres datenschutzrechtliches Gefährdungspotenzial. Der Verweis auf das Umweltinformationsgesetz ist nach Ansicht der Konferenzen der Datenschutz- und der Informationsfreiheitsbeauftragten des Bundes und der Länder deshalb nicht interessengerecht. Ein Geodatenzugangsgesetz muss einen differenzierenden Ausgleich zwischen Informations- und Schutzinteressen für die spezielle Problematik der Geobasis- und der Geofachdaten vornehmen. Es ist insbesondere zu berücksichtigen, dass nach der INSPIRE-Richtlinie die Zugangsmöglichkeit eingeschränkt werden soll, wenn der Zugang nachteilige Auswirkungen auf die Vertraulichkeit personenbezogener Daten haben kann.

**Anlage 24: Entschließung der 76. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 06./07.11.2008 Steuerungsprogramme der gesetzlichen Krankenkassen datenschutzkonform gestalten**

Mit der Gesundheitsreform soll über die Einführung von Wettbewerbsmechanismen die Qualität und Effizienz der gesetzlichen Krankenkassen verbessert werden. Die Kassen sind daher bemüht und auch vom Gesetzgeber gehalten, Versicherten ein Versorgungsmanagement anzubieten. Von zentraler Bedeutung sind dabei Patientenschulungsmaßnahmen und strukturierte Behandlungsprogramme für chronisch kranke Versicherte, die jedoch lediglich Angebotscharakter haben dürfen. Ihre Teilnahme soll nach dem Willen des Gesetzgebers freiwillig sein und eine eingehende Unterrichtung voraussetzen. Diese Vorgaben werden von einzelnen Krankenkassen nicht beachtet, wenn sie versuchen, die Versicherten in ihrem Gesundheitsverhalten zu steuern und sie in bestimmte Maßnahmen und Programme zu drängen.

Um Teilnehmerinnen und Teilnehmer zu gewinnen und um Maßnahmen durchzuführen, bedienen sich die Kassen vielfach privater Dienstleister und offenbaren diesen teils höchst sensible Gesundheitsdaten ihrer Versicherten. Dies ist datenschutzrechtlich nach dem Sozialgesetzbuch unzulässig, wenn die Übermittlung ohne Kenntnis und vorherige Einwilligung der jeweiligen Versicherten erfolgt.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hält die Einhaltung insbesondere der folgenden Eckpunkte bei gesundheitlichen Steuerungsprogrammen der Krankenkassen für unerlässlich:

- Die Krankenkassen dürfen Versichertendaten nur dann zur Auswahl von Personen für besondere Gesundheitsmaßnahmen verwenden, wenn dies gesetzlich ausdrücklich vorgesehen ist. Es muss sich um valide und erforderliche Daten handeln. Mit der Auswahl darf kein privater Dienstleister beauftragt werden.

- Die erstmalige Kontaktaufnahme mit potentiell für eine Gesundheitsmaßnahme in Betracht kommenden Versicherten muss durch die Krankenkasse selbst erfolgen, auch wenn ein privater Dienstleister mit der späteren Durchführung der Gesundheitsmaßnahme beauftragt worden ist.

- Die Versicherten sind vor Übermittlung ihrer Daten umfassend zu informieren. Die Information muss auch den Umstand umfassen, dass ein privates Unternehmen mit der Durchführung betraut werden soll. Soweit die Versicherten ausdrücklich in die Teilnahme eingewilligt haben, dürfen die für die Durchführung der Maßnahme erforderlichen Daten an den Dienstleister übermittelt werden.

- Wenn Versicherte - zu welchem Zeitpunkt auch immer - eindeutig zum Ausdruck bringen, nicht an einer Maßnahme teilnehmen zu wollen oder nicht an weitergehenden Informationen, einer konkreten Anwerbung oder einer fortgesetzten Betreuung interessiert zu sein, ist dies zu respektieren. Weitere Maßnahmen (auch telefonische Überredungsversuche) sind zu unterlassen.

**Anlage 25:** **Entschließung der 76. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 06./07.11.2008 Angemessener Datenschutz bei der polizeilichen und justiziellen Zusammenarbeit in der EU dringend erforderlich**

Auf europäischer Ebene ist eine Vielzahl von Vorhaben beschlossen bzw. initiiert worden, die in ihrer Gesamtheit zu erheblichen Eingriffen in die Persönlichkeitsrechte führt:

- Die Telekommunikationsunternehmen in den Mitgliedstaaten der EU sind verpflichtet, die bei der Nutzung öffentlich zugänglicher Telekommunikationsdienste anfallenden Verkehrsdaten über das Kommunikationsverhalten der Einzelnen für die Sicherheitsbehörden ohne konkreten Anlass auf Vorrat zu speichern.

- Die Pässe der Bürgerinnen und Bürger der EU-Mitgliedstaaten werden mit biometrischen Merkmalen ausgestattet.

- Fluggastdaten (PNR) werden in die USA übermittelt, um sie den dortigen Behörden zur Verfügung zu stellen. Die Nutzung von Fluggastdaten zu Strafverfolgungszwecken wird auch in der Europäischen Union vorbereitet.

- Der Vertrag von Prüm, der in den Rechtsrahmen der Union überführt wird, ermöglicht den Polizei- und Strafverfolgungsbehörden der Mitgliedstaaten einen gegenseitigen Zugriff auf Fingerabdruck-, DNA- und Kfz-Daten.

- Es soll ein Europäisches Strafregisterinformationssystem geschaffen werden, mit dem Informationen über strafrechtliche Verurteilungen zwischen den Mitgliedstaaten ausgetauscht werden können.

- Das Schengener Informationssystem wird weiter ausgebaut, u.a. durch die Speicherung von biometrischen Merkmalen. Zudem wird der Kreis der Nutzer erweitert um das Europäische Polizeiamt EUROPOL und die Einheit für justizielle Zusammenarbeit in der EU (EUROJUST).

- Ein Europäisches Visa-Informationssystem (VIS) wird eingeführt, um den Austausch von Visa-Daten zwischen den Mitgliedstaaten zu erleichtern. Auch für EUROPOL, die Sicherheitsbehörden und die Nachrichtendienste soll dieser Datenbestand zugänglich sein.

- Das europäische Verfahren EURODAC, in dem die Fingerabdrücke von Asylbewerberinnen und Asylbewerbern gespeichert sind, soll auch von der Polizei und den Strafverfolgungsbehörden genutzt werden können.

- Der Aufgabenbereich von EUROPOL soll über die Bekämpfung der Organisierten Kriminalität hinaus auch auf andere Formen der schweren Kriminalität erweitert werden. Außerdem soll EUROPOL erstmals die Befugnis erhalten, Daten auch von privaten Stellen entgegenzunehmen und Zugriff auf alle polizeilich relevanten Datenbanken in der EU bekommen.

- Der Informationsaustausch zwischen den Strafverfolgungsbehörden der EU wird entsprechend dem Rahmenbeschluss des Rates vom 18.12.2006 („Schwedische Initiative“) ausgebaut. Danach soll der Austausch verfügbarer Daten innerhalb der EU zu den gleichen Bedingungen erfolgen wie nach nationalem Recht.

Neben diesen Vorhaben gibt es zudem Abkommen auf bilateraler Ebene zwischen EU-Mitgliedstaaten und Drittstaaten, wie z.B. das Abkommen der Bundesrepublik Deutschland mit den Vereinigten Staaten für einen erweiterten Informationsaustausch zwischen den Sicherheitsbehörden.

Der Aufbau zentraler Datenbestände und der Ausbau der grenzüberschreitenden Datenübermittlung greifen erheblich in das Grundrecht auf informationelle Selbstbestimmung ein und führen dadurch zu Gefahren für jede Einzelne und jeden Einzelnen. Diese werden noch gesteigert durch die angestrebte Verknüpfbarkeit der bestehenden und geplanten Datenbanken.

Umso wichtiger ist deshalb ein hoher und gleichwertiger Datenschutz bei der polizeilichen und justiziellen Zusammenarbeit in Europa. Dies wurde von den Datenschutzbeauftragten auf nationaler und europäischer Ebene mehrfach angemahnt. Der hierzu im Oktober 2005 vorgelegte Rahmenbeschluss-Vorschlag genügt diesen Anforderungen nicht (siehe dazu die Entschließung der 71. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 16./17.03.2006 „Mehr Datenschutz bei der polizeilichen und justiziellen Zusammenarbeit in Strafsachen“). Zur Wahrung des erforderlichen Gleichgewichts zwischen Freiheit und Sicherheit sollten die Parlamente und Regierungen ihre Einflussmöglichkeiten bei europäischen Vorhaben stärker nutzen und dabei auch datenschutzrechtliche Aspekte einbringen. Wie notwendig ein angemessener Datenschutz ist, hat sich beim Verfahren der Aufnahme Verdächtiger in die so genannte EU-Terrorliste gezeigt, das durch den Europäischen Gerichtshof für rechtswidrig erklärt wurde.

Die Datenschutzbeauftragten fordern deshalb:

- Bei jeder neuen Initiative ist das Verhältnismäßigkeitsprinzip zu wahren und deren Auswirkung auf das bestehende System von Eingriffsmaßnahmen zu berücksichtigen.

- Im Hinblick auf den Kumulationseffekt sind die verschiedenen europäischen Initiativen zudem grundrechtskonform aufeinander abzustimmen. Redundanzen und Überschneidungen müssen verhindert werden.

- Ein Rechtsakt muss unverzüglich beschlossen werden, der über den Rahmenbeschlussvorschlag hinaus einen hohen und gleichwertigen Datenschutzstandard bei der Verarbeitung personenbezogener Daten im Rahmen der polizeilichen und justiziellen Zusammenarbeit verbindlich vorschreibt. Die gesamte nationale und grenzüberschreitende Informationsverarbeitung in diesem Bereich muss davon erfasst sein, um ein einheitliches Datenschutzniveau in den EU-Mitgliedstaaten zu gewährleisten.

- Ein unabhängiges, beratendes Datenschutzgremium sowie eine unabhängige und umfassende datenschutzrechtliche Kontrolle müssen für die polizeiliche und justizielle Zusammenarbeit eingerichtet bzw. gewährleistet werden.

**Anlage 26:** **Entschließung der 76. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 06./07.11.2008 Besserer Datenschutz bei der Umsetzung der „Schwedischen Initiative“ zur Vereinfachung des polizeilichen Datenaustausches zwischen den EU-Mitgliedstaaten geboten**

Der Rahmenbeschluss des Rates zur Vereinfachung des Informationsaustausches zwischen den Strafverfolgungsbehörden der EU-Mitgliedstaaten (sog. „Schwedische Initiative“) vom 18.12.2006 verpflichtet diese, an die grenzüberschreitende Übermittlung personenbezogener Daten innerhalb der EU keine höheren Anforderungen zu stellen, als auf nationaler Ebene für den Datenaustausch zwischen Polizei- und Strafverfolgungsbehörden gelten. Seine Umsetzung wird zu einem deutlichen Anstieg und zur Beschleunigung des Informationsaustausches und damit zu einer weiteren Intensivierung der polizeilichen und justiziellen Zusammenarbeit in Strafsachen auf EU-Ebene führen. Das erstrebte Ziel, nämlich die Schaffung eines Raumes der Freiheit, der Sicherheit und des Rechts setzt aber auch voraus, dass in den Mitgliedstaaten ein möglichst gleichwertiger Datenschutz auf hohem Niveau besteht. Dies ist bislang nicht erfüllt. Es besteht nach wie vor der aus datenschutzrechtlicher Sicht unhaltbare Zustand, dass die auf EU-Ebene ausgetauschten polizeilichen Informationen in den jeweiligen EU-Mitgliedstaaten unterschiedlichen Datenschutzregelungen hinsichtlich ihrer Verwendung unterworfen sind. Zudem gelten keine einheitlichen Rechte auf Auskunft, Berichtigung und Löschung der Datenverarbeitung für die Betroffenen in den Empfängerstaaten.

Vor diesem Hintergrund fordern die Datenschutzbeauftragten des Bundes und der Länder den Gesetzgeber auf, den bei der innerstaatlichen Umsetzung der „Schwedischen Initiative“ verbleibenden Spielraum zu nutzen und die Befugnisse zum Informationsaustausch mit den Strafverfolgungsbehörden der EU-Mitgliedstaaten für die nationalen Polizei- und Strafverfolgungsbehörden normenklar und unter Beachtung des Grundsatzes der Verhältnismäßigkeit gesetzlich zu regeln. Dazu zählen insbesondere:

- Ausschluss der gesonderten Erhebung der angefragten Daten durch die Strafverfolgungsbehörden allein um diese zu übermitteln.

- Eindeutige inhaltliche Anforderungen, die an ein Ersuchen um Datenübermittlung zu stellen sind, um Überschussinformationen zu vermeiden,

- Regelung enger Voraussetzungen für sog. Spontanübermittlungen, um für den Empfänger nutzlose und damit nicht erforderliche Übermittlungen auszuschließen,

- Nutzung des Spielraums bei der Ausgestaltung der Verweigerungsgründe, um unverhältnismäßige Datenübermittlungen zu verhindern,

- normenklare Abgrenzung der Befugnis zur Übermittlung von Daten zu präventiven Zwecken gegenüber der justiziellen Rechtshilfe,

- vollständige Umsetzung der Datenschutzbestimmungen in Art. 8 des Rahmenbeschlusses und begrenzende Regelungen zur Weiterübermittlung an Drittstaaten,

- normenklare Bestimmung welche Behörden als zuständige Strafverfolgungsbehörden im Sinne des Rahmenbeschlusses gelten und welche Informationen nur durch Ergreifen von Zwangsmaßnahmen im Sinne des Rahmenbeschlusses verfügbar sind,

- normenklare Bestimmung, welche Informationen nicht vom Rahmenbeschluss erfasst werden, weil sie für die Strafverfolgungsbehörden nur durch das Ergreifen von Zwangsmaßnahmen verfügbar sind.

**Anlage 27:** **Entschließung der 76. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 06./07.11.2008 Elektronische Steuererklärung sicher und datenschutzgerecht gestalten**

Mit dem Steuerbürokratieabbaugesetz (BR-Drs. 547/08) sollen u.a. verfahrenstechnische Regelungen für die elektronische Übermittlung von Steuererklärungen durch Steuerpflichtige festgelegt werden. Zu diesem Zweck soll § 150 Abgabenordnung (AO) durch Abs. 7 Satz 1 dahingehend ergänzt werden, dass bei Einführung einer Verpflichtung zur elektronischen Abgabe die übermittelten Steuerdaten mit einer qualifizierten Signatur nach dem Signaturgesetz zu versehen sind.

Die Konferenz sieht es kritisch, dass § 150 Abs. 7 Satz 2 Nr. 6 und 7 AO auch vorsieht, zur Erleichterung und Vereinfachung des automatisierten Besteuerungsverfahrens anstelle der qualifizierten elektronischen Signatur ein so genanntes anderes sicheres Verfahren im Benehmen mit dem Bundesinnenministerium zuzulassen oder sogar auf beide Verfahren vollständig zu verzichten. In der Gesetzesbegründung wird darauf verwiesen, dass neben der qualifizierten elektronischen Signatur künftig auch eine Übermittlung der Daten unter Nutzung der Möglichkeiten des neuen elektronischen Personalausweises möglich sein soll.

Bereits in ihrer Entschließung zur sachgemäßen Nutzung von Authentisierungs- und Signaturverfahren vom 11.10.2006 hat die Konferenz gefordert, Nutzenden die Möglichkeit zu eröffnen, die elektronische Kommunikation mit der Verwaltung durch eine qualifizierte elektronische Signatur abzusichern. Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder begrüßt daher die vorgesehene Regelung in der AO zur Nutzung der qualifizierten elektronischen Signatur, da dieses Verfahren geeignet ist, die Authentizität und Integrität eines elektronisch übermittelten Dokuments sicherzustellen, und somit die handschriftliche Unterschrift ersetzen kann.

Die Datenschutzbeauftragten des Bundes und der Länder erklären hierzu:

1. Das Verfahren der qualifizierten elektronischen Signatur nach dem Signaturgesetz ist im Hinblick auf die Authentizität und Integrität elektronisch übermittelter Dokumente derzeit alternativlos.

2. Für die Bewertung anderer Verfahren sollte unmittelbar auf die Fachkenntnis unabhängiger Gutachter abgestellt werden. Als Gutachter für die Beurteilung der technischen Sicherheit kämen etwa die Bundesnetzagentur oder das BSI in Frage.

3. Steuerpflichtige müssen auch im elektronischen Besteuerungsverfahren die Möglichkeit haben, die elektronische Kommunikation mit der Finanzverwaltung durch das hierfür geeignete Verfahren der qualifizierten elektronischen Signatur abzusichern.

**Abkürzungsverzeichnis**

a.a.O. ..... am angegebenen Ort
a.F. ..... alte Fassung
Abs. ..... Absatz
AEAO ..... Anwendungserlass zur Abgabenordnung
AGO ..... Allgemeine Geschäftsordnung für die Behörden des Freistaates Bayern
AKDB ..... Anstalt für Kommunale Datenverarbeitung in Bayern
AKIS ..... Verbunddatei zur Aufklärung krimineller islamistischer Strukturen
ALBV ..... Verordnung über den automatisierten Abruf von personenbezogenen Daten aus dem Liegenschaftskataster
AO ..... Abgabenordnung
AOK ..... Allgemeine Ortskrankenkasse
ARGE ..... Arbeitsgemeinschaft nach § 44 b SGB II
Art. ..... Artikel
ATD ..... Antiterrordatei
ATDG ..... Antiterrordateigesetz
Az. ..... Aktenzeichen
BayArchivG ..... Bayerisches Archivgesetz
BayBesG ..... Bayerisches Besoldungsgesetz
BayBG ..... Bayerisches Beamtengesetz
BayBhV ..... Bayerische Beihilfeverordnung
BayBO ..... Bayerische Bauordnung
BayDSG ..... Bayerisches Datenschutzgesetz
BayEUG ..... Bayerisches Gesetz über das Erziehungs- und Unterrichtswesen
BayGDIG ..... Bayerisches Geodateninfrastrukturgesetz
BayKRG ..... Bayerisches Krebsregistergesetz
BayMeldeDÜV ..... Verordnung zur Durchführung von regelmäßigen Datenübermittlungen der Meldebehörden; Bayerische Meldedaten-Übermittlungsverordnung
BayPrG ..... Bayerisches Pressegesetz
BayPVG ..... Bayerisches Personalvertretungsgesetz
BayRS ..... Bayerische Rechtssammlung
BayStVollzG ..... Bayerisches Strafvollzugsgesetz
BayVersG ..... Bayerisches Versammlungsgesetz
BayVGH ..... Bayerischer Verwaltungsgerichtshof
BayVSG ..... Bayerisches Verfassungsschutzgesetz
BayVwVfG ..... Bayerisches Verwaltungsverfahrensgesetz
BDSG ..... Bundesdatenschutzgesetz
BEEG ..... Bundeselterngeld- und Elternzeitgesetz
BfV ..... Bundesamt für Verfassungsschutz
BhV ..... Beihilfevorschriften
Bit ..... Binary Digit
BKA ..... Bundeskriminalamt
BKAG ..... Bundeskriminalamtgesetz
BLÄK ..... Bayerische Landesärztekammer
BR-Drs. ..... Bundesratsdrucksache
BRK ..... Bayerisches Rotes Kreuz
BSI ..... Bundesamt für Sicherheit in der Informationstechnik
bspw. ..... beispielsweise
BT-Drs. ..... Bundestagsdrucksache
BV ..... Bayerische Verfassung
BVerfG ..... Bundesverfassungsgericht
BVerfGE ..... Entscheidungen des Bundesverfassungsgerichts (zitiert nach Band und Seite)
BVerwG ..... Bundesverwaltungsgericht
bzgl. ..... bezüglich
BZR ..... Bundeszentralregister
BZRG ..... Bundeszentralregistergesetz
bzw. ..... beziehungsweise
ca. ..... circa
CD ..... Compact Disc
CSU ..... Christlich Soziale Union
d.h. ..... das heißt
DIN ..... Deutsche Industrie Norm
DM ..... Deutsche Mark
DNA ..... Desoxyribonuclein Acid, Träger der Erbinformation
DNA-Analyse ..... Molekulargenetische Untersuchung
DOMEA ..... Dokumentenmanagementsystem
DSB ..... Datenschutzbeauftragter
DSchV ..... Datenschutzverordnung
DVD ..... Digital Versatile Disc, Digital Video Disc
EDV ..... Elektronische Datenverarbeitung
eFA ..... elektronische Fallakte
EFG ..... Sammlung der Entscheidungen der Finanzgerichte
EG ..... Europäische Gemeinschaft
EG-Datenschutzrichtlinie ..... Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24.10.1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr
EKAA ..... Elektronische Kriminalakten-Archivierung
ELENA ..... Elektronischer Entgeltnachweis
ELSTER ..... Elektronische Steuererklärung
E-Mail ..... Elektronische Post
ePass ..... elektronischer Pass
Erl. ..... Erläuterung
EStG ..... Einkommensteuergesetz
etc. ..... et cetera

EU .....Europäische Union
EuGH .....Europäischer Gerichtshof
evtl. .....eventuell
EWO .....Einwohnermeldeverfahren
FDP .....Freie Demokratische Partei
ff. .....folgende
FMBl.....Amtsblatt des Bayerischen Staatsministeriums der Finanzen
GAST-Dateien .....Dateien zur Gefahrenabwehr und Verfolgung von Straftaten
GDVG.....Gesundheitsdienst- und Verbraucherschutzgesetz
gem. .....gemäß
GEZ.....Gebühreneinzugszentrale der öffentlich-rechtlichen Rundfunkanstalten Deutschlands
GG.....Grundgesetz
ggf. .....gegebenenfalls
GmbH.....Gesellschaft mit beschränkter Haftung
GnuPGP .....PGP-Version für Unix
GO.....Gemeindeordnung
grds. .....grundsätzlich
GVBl.....Gesetz- und Verordnungsblatt
HEADS .....Haft-Entlassenen-Auskunfts-Datei-Sexualstraftäter
HKaG .....Heilberufekammergesetz
HTTPS .....Hyper Text Transfer Protocol Secure
i.S.d. .....im Sinne des
i.S.v. .....im Sinne von
i.V.m. .....in Verbindung mit
IBA.....Informationssystem des LfV
ICD.....International Statistical Classification of Deseases and Related Health Problems
IDAT.....Identifizierende Daten
IFIS .....INPOL-Fall-Datei „Innere Sicherheit“
IHK .....Industrie- und Handelskammer
IMEI.....International Mobile Station Equipment Identity
IMG.....Institut für Medizinmanagement und Gesundheitswissenschaften
IMS .....Schreiben des StMI
INPOL.....Informationssystem der Polizei (bundesweit)
IP.....Internet Protocol
ISIS .....Bayerische Staatsschutzdatei
ISmed 3 .....Medizinisches Informationssystem Version 3
IT.....Informationstechnik
ITSO.....IT Service Organisation
IuK .....Informations- und Kommunikationstechnik
JGG .....Jugendgerichtsgesetz
JVA .....Justizvollzugsanstalt
KAN.....Kriminalaktennachweis
KFÜ-RL .....Krebsfrüherkennungs-Richtlinien
KommHV-Doppik..... Kommunalhaushaltsverordnung-Doppik
KommHV-Kameralistik ..... Kommunalhaushaltsverordnung-Kameralistik
KONSENS ..... Koordinierte neue Software-Entwicklung der Steuerverwaltung
KVB ..... Kassenärztliche Vereinigung Bayerns
KWG ..... Gesetz über das Kreditwesen
KWMBl..... Kultus- und Wissenschaftsministerialblatt
LabID ..... Laboridentifikator
LfV ..... Landesamt für Verfassungsschutz
LGL ..... Landesamt für Gesundheit und Lebensmittelsicherheit
lit. ..... Buchstabe
LT-Drs. ..... Landtagsdrucksache
m.E. ..... meines Erachtens
m.w.N. ..... mit weiteren Nachweisen
MDK ..... Medizinischer Dienst der Krankenkassen
MdL..... Mitglied des Landtages
MeldDV ..... Meldedatenverordnung
MeldeG..... Bayerisches Gesetz über das Meldewesen
n.F. ..... neue Fassung
Nr. ..... Nummer
o.b. ..... oben bezeichnet
o.g. ..... oben genannt
OKIS ..... OK-Informationssystem
OWiG ..... Ordnungswidrigkeitengesetz
PAG..... Bayerisches Polizeiaufgabengesetz
PC..... Personalcomputer
PDA..... Personal Digital Assistent
PDF ..... Portable Document Format
PDS ..... Partei des Demokratischen Sozialismus
PfleWoqG..... Pflege- und Wohnqualitätsgesetz
PGP ..... Pretty Good Privacy
PID ..... Personenidentifikator/Personal Identifier
PIN ..... Personell Identification Number
PKI ..... Public Key Infrastructure
PpS-Richtlinien .... Richtlinien für die Führung polizeilicher personenbezogener Sammlungen
ProbDAT..... Probendaten
PSN ..... Pseudonym
PSV ..... Polizeiliche Sachbearbeitung/Vorgangsverwaltung-Verbrechensbekämpfung
Rdnr. ..... Randnummer
Reha ..... Rehabilitation
RFID ..... Radio Frequency Identification
RGIS ..... Rauschgiftinformationssystem
RiStBV ..... Richtlinien für das Straf- und Bußgeldverfahren

RWI.....Rheinisch-Westfälisches Institut für Wirtschaftsforschung e.V.
S. .....Seite
S/MIME .....Secure Multipurpose Internet Mail Extensions
SGB.....Sozialgesetzbuch
SIS.....Schengener Informationssystem
sog. .....sogenannt
SPD .....Sozialdemokratische Partei Deutschlands
StGB.....Strafgesetzbuch
StMI .....Staatsministerium des Innern
StMUG.....Staatsministerium für Umwelt und Gesundheit
StPO .....Strafprozessordnung
StVG .....Straßenverkehrsgesetz
StVollzG .....Strafvollzugsgesetz
TEMPiS .....Telemedizinisches Projekt zur integrierten Schlaganfallversorgung in der Region Süd-Ost-Bayern
TIZIAN .....Gemeinsame EDV für den Gesundheitlichen Verbraucherschutz
TK .....Telekommunikation
TK-Bek .....Bekanntmachung über die Einrichtung und Benutzung dienstlicher Telekommunikationsanlagen
TKG ..... Telekommunikationsgesetz
TMF e.V. ..... Telematikplattform für Medizinische Forschungsnetze
TMG..... Telemediengesetz
u.ä. ..... und ähnliches
u.a. ..... unter anderem
u.U. ..... unter Umständen
UnterbrG ..... Bayerisches Unterbringungsgesetz
v.a. ..... vor allem
VermKatG..... Vermessungs- und Katastergesetz
vgl. ..... vergleiche
VV..... Verwaltungsvorschriften
VV-BayBkV..... Verwaltungsvorschriften zur Bayerischen Beihilfeverordnung
VwZVG..... Bayerisches Verwaltungszustellungs- und Vollstreckungsgesetz
WSF ..... Wirtschafts- und Sozialforschung Kerpen
z.B. ..... zum Beispiel
z.T. ..... zum Teil
ZBFS ..... Zentrum Bayern Familie und Soziales
ZEVIS ..... Zentrales Verkehrsinformationssystem
ZOB..... Zentraler Omnibusbahnhof
ZPO ..... Zivilprozessordnung

**Stichwortverzeichnis**