Bayerischer Landtag

15. Wahlperiode Drucksache 15/**6700**

29.01.2007

22. Tätigkeitsbericht des Landesbeauftragten für den Datenschutz

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

Berichtszeitraum 2005/2006

Der Bayerische Landesbeauftragte für den Datenschutz

Nr. DSB/1 - 510 - 23 München, 29.01.2007

An den
Präsidenten
des Bayerischen Landtags
Herrn Alois Glück

81627 München

22. Bericht über die Tätigkeit des Landesbeauftragten für den Datenschutz

Sehr geehrter Herr Landtagspräsident,

in der Anlage übersende ich gem. Art. 30 Abs. 5 des Bayerischen Datenschutzgesetzes den 22. Bericht über die Tätigkeit des Landesbeauftragten für den Datenschutz.

Mit freundlichen Grüßen

Dr. Karl Michael Betzl

1 Ich habe einen Traum …..

Stellen Sie sich vor, Sie erwachen eines Morgens und spüren: Es hat sich etwas verändert im Lande. Ein Zauberer hat über Nacht alle Datenschützer und alle Vorschriften über den Datenschutz verschwinden lassen. Sämtliche klugen Urteile und Kommentare zum informationellen Selbstbestimmungsrecht sind Makulatur geworden.

Erleichtert und irgendwie befreit machen Sie sich auf den Weg ins Büro. Zuvor sehen Sie noch in Ihren Briefkasten und ärgern sich maßlos, weil Ihre neue Wohnadresse schon überall bekannt ist und Sie deshalb mit Werbung überschwemmt werden. Angesichts des wunderschönen Morgens ist allerdings im Auto der Ärger gleich wieder verflogen und daher stört es Sie auch nicht, dass man Ihren momentanen Standort und Ihre Fahrtroute auf mindestens sieben verschiedenen Wegen nachvollziehen kann: Über allerlei Videokameras mit Gesichtserkennung, über das Mautsystem, über die mobile Kennzeichenerkennung, über die Rückkanäle in Ihrem Navigationssystem, Ihrem Verkehrstelematiksystem und Ihrem Autoradio sowie über weitere in Ihr Fahrzeug eingebaute Fahrtdatenaufzeichnungsgeräte (z.B. event data recorder). Nicht zu vergessen auch Ihr Handy, von dem nicht nur sämtliche Verkehrsdaten ein halbes Jahr lang gespeichert werden, sondern welches auch eine jederzeitige Ortung ermöglicht. Ihr Handy klingelt übrigens gerade, aber Sie nehmen nicht ab, weil die vernetzten Systeme um Sie herum sofort festhalten würden, dass Sie verbotenerweise während der Fahrt telefonieren. Allerdings würden Sie sich auch ohne die Online-Erfassung aller Verkehrsverstöße exakt an die Straßenverkehrsordnung halten.

Dennoch sind Sie enttäuscht, dass Sie infolge der neuen Entwicklung nicht mehr diesen 22. Tätigkeitsbericht des Bayerischen Datenschutzbeauftragten, den ersten in meiner am 01.02.2006 begonnenen Amtszeit, zu lesen brauchen. Schade ist das schon, weil meine Mitarbeiterinnen und Mitarbeiter sowie mein Amtsvorgänger Reinhard Vetter, in dessen Ägide dieser Bericht noch weitgehend fällt, gute und engagierte Arbeit geleistet haben. Wenn ich mich gleichwohl durchgängig der Ich-Form bediene, so halte ich mich an die Übung unter den Datenschützern, will aber nicht verhehlen, dass ich mich insoweit gerne auch mit fremden Federn schmücke.

Mittlerweile sind Sie im Büro angekommen und widmen sich mit Ihrem Team der Aufgabe, das Bescheinigungswesen im Sozialbereich elektronisch zu gestalten.

Es ist erstaunlich, auf was für unterschiedliche staatliche Leistungen man Anspruch hat: Arbeitslosengeld, Mutterschaftsgeld, Kindergeld, Wohngeld, Erziehungsgeld, Krankengeld, Rente usw. bis hin zur Prozesskostenhilfe. Je nach Fallgestaltung müssen persönliche Daten, z.B. Einkommensnachweise samt Nebenverdiensten, Erwerbsbiographie einschließlich Kündigungen und Kündigungsgründe, Familienstand, bezahlte Steuern und Sozialversicherungsbeiträge und tausend andere Dinge nachgewiesen werden, darunter in einer Art Zirkelschluss andere staatliche Leistungen, die sich mit der gerade beantragten wechselseitig beeinflussen. All dies soll nun elektronisch erfolgen, um Arbeitgebern und Arbeitnehmern das ganze papierene Bescheinigungswesen zu ersparen.

Das Projekt hieß bisher JobCard, Sie haben es gestern eingedeutscht - ELENA, Elektronischer Einkommensnachweis. Einige Grundentscheidungen sind bereits gefallen: Wegen der großen Datenmenge und aus Sicherheitsgründen sollen alle Angaben nicht lokal auf einer Chipkarte, sondern auf einem zentralen Server gespeichert werden. Die Datenschützer hatten diesbezüglich Bedenken angemeldet und etwas von verbotener Vorratsspeicherung geschrieben.

Als Erstes denken Sie darüber nach, wie Sie verhindern, dass jeder Hacker den Datenbestand auf dem zentralen Server lesen oder gar verändern kann. Nach langer Diskussion entwickelt Ihr Team ein ausgefeiltes Berechtigungskonzept, wer wann auf welche Daten zugreifen darf. Wie aber kann sichergestellt werden, dass der Abrufende wirklich die richtige Person ist? Eine Unterarbeitsgruppe findet die Lösung: Authentifizierung mit Chipkarte sowohl durch den Mitarbeiter des Arbeitsamts wie auch durch den Antrag stellenden Bürger, also ein Zweikartenprinzip. Für die Übertragungssicherheit einigt sich derweil das Team auf ein Verschlüsselungsverfahren. Und als Sahnehäubchen sehen Sie auch noch eine verschlüsselte Datenablage im zentralen Server vor, nur für den Fall, dass doch einmal ein Hacker durchdringt. Der Controller hatte Sie allerdings merkwürdig angesehen und gefragt, ob es diesen Luxus mit der Verschlüsselei wirklich braucht. Das koste schließlich eine Menge und die paar Hacker könne man doch vergessen.

Rrrrr rrrrr rrrrr rrrrr

Sie fahren aus dem Schlaf hoch, der Wecker hat geklingelt. Erleichtert stellen Sie fest, dass Sie geträumt haben und dass der neue Tag Ihnen nun doch einen Anlass gibt, nachfolgenden Tätigkeitsbericht zu lesen.

2 Einige Grundsatzprobleme des Datenschutzes

Mit vorstehender Parabel zur Frage „was wäre, wenn es keinen Datenschutz gäbe“ will ich zeigen: Wir wären in unserem Alltag noch stärkeren Überwa-

chungen und Kontrollen ausgesetzt (Autofahrt), komplizierte Geschäftsprozesse (ELENA) würden ohne Datenschutz nur vermeintlich einfacher, in Wirklichkeit jedoch noch problematischer. Im Einzelnen will ich sechs zentrale Punkte zum Thema Datenschutz herausstellen:

2.1 Datenschutz, Freiheit und Sicherheit

Da ist, anhand der Autofahrt gezeigt, der Spannungsbogen von Freiheit und Sicherheit mit dem immer engmaschiger werdenden Überwachungsnetz: Wir gewöhnen uns allmählich an diesen Zustand, nicht zuletzt, weil er so unmerklich stattfindet und sich so schleichend ausbreitet. Auf die Barrikaden steigen die Bürger nur, wenn sie die Auswirkungen unmittelbar am eigenen Leib spüren, wie bei der Werbung als Folge einer relativ banalen Adressenweitergabe. Dann allerdings sind sie sehr sensibel. Zur Frage der Adressenweitergabe durch verschiedene Stellen erreichen mich regelmäßig wesentlich mehr Anfragen als z.B. zur Antiterrordatei. Erstaunlicherweise löst auch die Datenweitergabe im europäischen und internationalen Rahmen, etwa bezüglich der Flugpassagierdaten, kaum Empörung aus.

Ich will kein Schreckensgemälde ausbreiten, welche technischen Möglichkeiten zur Erfassung und Kontrolle des individuellen Verhaltens heute bereits und in absehbarer Zukunft möglich sind und wo unsere Daten überall weitergeleitet, vernetzt und ausgewertet werden - die Realität ist hier schlimmer als jede Phantasie. Ich will auch kein Klagelied zur informationellen Selbstbestimmung und zur Wahrung der Privatsphäre anstimmen: Wer hier das Offenkundige immer noch nicht sehen will, wird sich von mir auch jetzt die Augen nicht öffnen lassen.

Ich will die Bürger dieses Landes vielmehr zu einer gesellschaftlichen Diskussion ermuntern, wie viel Überwachung und Gängelung wir uns gegenseitig wirklich antun wollen und welche Legitimation der Staat hat, uns ein immer dichter werdendes Kontrollnetz aufzuoktroyieren. Ich weise auf diesen Punkt besonders hin, weil nach den Terroranschlägen von 2001 neuere politische Strömungen spürbar sind, das Rad der demokratischen und rechtsstaatlichen Entwicklung der freiheitlichen Staaten des Westens wieder zurückzudrehen. Das Konzept der mühselig erkämpften bürgerlichen Freiheit kann hier wenig Widerstand leisten, weil es heute kaum mehr verstanden wird.

2.2 Datenschutz zwischen Repression und Prävention

Wir erleben derzeit einen Paradigmenwechsel von der Strafverfolgung zur Prävention, Argument: Es ist wichtiger, eine Straftat zu verhindern, als sie hinterher aufzuklären. Dagegen kann zwar niemand etwas einwenden, aber man begibt sich auf die Rutschbahn vom gegenwärtigen Angriff über die konkrete und abstrakte Gefahr bis hin zur vagen Vermutung. Parallel dazu werden immer mehr präventive Eingriffsbefugnisse geschaffen. Die habeas-corpus-Akte ist zwar schon über 350 Jahre alt, aber man sollte sich ihrer gelegentlich erinnern und in ihrem Geiste von präventiven Eingriffsbefugnissen zurückhaltend Gebrauch machen. Dies gilt insbesondere im Lichte neuerer mathematisch-statistischer Methoden, die unter Stichworten wie „scoring“ oder „data mining“ Menschen auf Grund bloßer Wahrscheinlichkeitsbeziehungen und Muster in bestimmte Kategorien einordnen. Mittlerweile ist es z.B. mittels einer Korrelationsanalyse möglich, dass der Computer verborgene Zusammenhänge herstellt und Antworten auf Fragen liefert, die niemand gestellt hat. Die Gefahr ist greifbar, dass auf diese Weise einem Individuum abträgliche Merkmale zugeordnet werden mit der Folge einer scheinobjektiven polizeilichen und sozialen Stigmatisierung. Es handelt sich sozusagen um eine computergenerierte Vorurteilsbildung. Selbstverständlich kann der Bürger versuchen, die Unrichtigkeit der ihn betreffenden Vermutung zu beweisen. Allerdings können Computer manchmal recht hartleibig gegenüber Gegenvorstellungen sein.

2.3 Datenschutz und informationelles Prozessmanagement

Das Beispiel JobCard/ELENA soll zeigen, dass die Strukturierung eines Geschäftsprozesses unter dem Gesichtspunkt des Informationsmanagements (informationelles Prozessmanagement) bei einem derart komplexen Vorhaben schon aus dessen innerer Sachlogik heraus komplizierteste Überlegungen auslöst. Es wäre wesentlich zu kurz gedacht, wollte man annehmen, der Datenschutz sei hierfür ursächlich. Diese Überlegungen müssten auch angestellt werden, wenn es überhaupt keinen Datenschutz gäbe. Der Datenschutz setzt lediglich als Steuerungselement auf das informationelle Prozessmanagement auf und gibt ihm die Feinstruktur.

Allerdings hat man bei der Strukturierung eines Geschäftprozesses die Wahl, sich auf das unbedingt Notwendige zu beschränken, so dass sich die Komplexität des Prozesses ebenfalls auf das unumgängliche Maß beschränkt, was immer noch sehr viel sein kann. Es gibt aber auch ein Perfektionierungsstreben nach dem Motto, das könnten wir doch auch gleich noch machen und diese Zusatzfunktion wäre ebenfalls nützlich, und bei der Gelegenheit böte sich doch an ….. Auf diese Weise wird der Geschäftsprozess immer komplexer, mit ihm auch das informationelle Prozessmanagement und in dessen Folge wiederum der Datenschutz. Immer aber ist der Datenschutz die

Folge und nicht die Ursache der Komplexität, wenn auch zugegebenermaßen manchmal als additives Element.

2.4 Datenschutz und Normenflut

Das Projekt JobCard/ELENA hat seinen inneren Grund in der Kompliziertheit unserer Rechtsvorschriften; ohne unseren Hang zu immer weiter gehenden Regeln, Sonderregeln, Erweiterungen, Ausnahmebestimmungen, wechselseitigen Bezügen, Zu- und Anrechnungen usw. bräuchte es wahrscheinlich das ganze Projekt nicht. Summum ius, summa iniuria, Recht auf die Spitze getrieben wird Unrecht, wussten die alten Römer. Wir dagegen meinen, das gelte für uns nicht, und verzetteln uns solange in gesetzgeberischer Einzelfallgerechtigkeit, bis wir den Wald vor lauter Bäumen nicht mehr sehen und auch der ausgebildete Jurist außerhalb seines eng begrenzten Spezialgebiets keine Chance mehr hat zu erkennen, was rechtens ist.

Ich schreibe bewusst „wir“, weil unser Rechtssystem das Ergebnis wechselseitiger Beeinflussung von Politik und Bürgern ist: Generell ist man sich einig, alles möglichst schlank und einfach haben zu wollen. Ausgehend vom Einzelfall jedoch bilden Forderungen von Bürgern und Interessengruppen einerseits, die Tendenz der Politiker, den Wählern entgegenzukommen andererseits, dazu das Perfektionierungsstreben der Verwaltung und nicht zuletzt eine kasuistische Rechtsprechung jene unheilvolle Allianz, die sich seit über fünfzig Jahren zu immer neuen Verkomplizierungen hochschaukelt.

Beispiel Steuerrecht: Rund zwei Drittel der gesamten weltweiten Literatur, so ist zu hören, beziehen sich allein auf das deutsche Steuerrecht, nicht ohne Grund. So sind die Regelungen zur Abzugsfähigkeit des häuslichen Arbeitszimmers und zur Besteuerung der Kapitalerträge derart verästelt, dass weder Bürger noch Verwaltung durchblicken; zu allem Überdruss - und das ist mein Thema - ziehen sie enorme Kontrollmechanismen nach sich bis hin zur Privatsphäre der Wohnung beim häuslichen Arbeitszimmer und zu europaweiten Kontrollmitteilungen bei den ausbezahlten Kapitalerträgen. Dieser Kontrollapparat frisst nicht nur einen mehr oder minder großen Teil der Erträge auf, er ist auch aus dem Blickwinkel der Mittel-Zweck-Relation unverhältnismäßig. Schließlich werden die bürgerlichen Freiheiten und die Privatsphäre nicht eingeschränkt, um terroristische Anschläge oder Kapitalverbrechen aufzuklären und zu verhindern, sondern lediglich, um einen in vielen Fällen (häusliches Arbeitszimmer) eher geringen staatlichen Geldanspruch durchzusetzen. Ich begrüße daher außerordentlich, dass nach mehreren unter leichter Belustigung des Publikums gescheiterten Anläufen zu einem einfacheren Steuersystem mittlerweile doch Schritte in Richtung auf Vereinfachungen, Stichwort Abgeltungssteuer, unternommen werden. Allerdings eröffnet jede Vereinfachung und Pauschalierung endlose Diskussionen unter Gerechtigkeitsaspekten und Vorher-Nachher-Vergleichen. Den Pfennigfuchsern unter uns muss entgegengehalten werden, dass bereits die ökonomischen Vorteile in der Summe die Nachteile überwiegen und dass der Gewinn an Freiheit von Kontrolle und Überwachung nicht hoch genug eingeschätzt werden kann.

Noch deutlicher wird dies, wenn man weitere Bereiche in die Überlegungen mit einbezieht, Beispiel Sozialrecht: Die JobCard/ELENA ist sozusagen nur die datenmäßige Benutzeroberfläche des Systems, die Aufzählung im Beispielsfall lässt aber bereits erahnen, was alles dahinter liegt. Ich will mich auf eine besonders problematische Fallgruppe beschränken, nämlich die Feststellung, ob zwei Hartz-IV Empfänger in eheähnlicher Lebensgemeinschaft zusammenleben. Der Hintergrund sind vom Gerechtigkeitssinn wie von staatlicher Sparsamkeit - man verspricht großzügige Leistungen, die Leute sollen sie aber möglichst wenig in Anspruch nehmen - gleichermaßen geprägte Regelungen, die verhindern sollen, dass nicht verheiratet Zusammenlebende besser gestellt werden als Ehepaare. Um den eheähnlichen Lebensgemeinschaften auf die Spur zu kommen, werden die Arbeitsgemeinschaften bei ihren Anstrengungen, in die Privatsphäre einzudringen, immer erfinderischer, Stichwort „häusliche Nachschau“. Es ist nicht meines Amtes, mich hier mit Vorschlägen zu einfacheren Regelungen hervorzutun, aber ich bin überzeugt: Es gäbe sie, die Gesellschaft muss nur wollen.

2.5 Datenschutz und zentrale Datenbestände

In den letzten Jahren hat sich die Entwicklung hin zu großen, zentralen Datenbeständen verstärkt. Die Schwierigkeiten, die sich aus der Komplexität des informationellen Prozessmanagements solcher Datenbestände sowie aus den damit verknüpften Rechtsfragen ergeben, scheinen offenbar den Ehrgeiz der Planer solcher Projekte zu beflügeln. Sichtbares Beispiel hierfür ist das LKW-Maut-System, welches nach verbreiteter Ansicht unnötig kompliziert ist und deshalb erhebliche Anlaufschwierigkeiten hatte. Ein weiteres Beispiel, noch in der Entwicklungsphase, ist die hier ausführlich behandelte JobCard/ELENA. Nicht genug damit, befinden sich vergleichbare informationelle Großvorhaben bereits in der Pipeline: Die elektronische Gesundheitskarte, die Schülerdatenbank, die zentrale Speicherung der Grunddaten aller Einwohner der Bundesrepublik Deutschland beim Bundeszentralamt für Steuern, die Absicht, auf Landesebene zentrale elektronische Personenstandsregister einzurichten. Hinzu kommen Bestrebungen, weitere zentrale Rechner- und IT-Zentren zu bilden.

All diese Datenbestände sind in sich schon wahre Bergwerke für das oben bereits angesprochene data mining, weil sie, je größer, desto mehr Möglichkeiten zu den unterschiedlichsten Rasterungen und Profilbildungen bieten. Potenziert wird diese Gefahr noch durch die Zusammenführung der unterschiedlichen Großdatenbestände im Wege von Online-Abfragen oder unmittelbaren elektronischen Vernetzungen. Dies ist nicht einfach ein quantitatives Mehr gegenüber dem Zustand zuvor, sondern eine neue Qualität des über den Bürger gestülpten elektronischen Datenkäfigs. Selbstverständlich war es auch schon bisher bei einfacheren Datenbankstrukturen oder im rein manuellen Betrieb möglich, über einzelne Bürger eine Menge Informationen zusammenzutragen. Dieser Aufwand war jedoch so hoch, dass man sich die Mühe nur in seltenen Ausnahmefällen gemacht hat. Außerdem war es selbst dann nicht möglich, das Individuum in einen statistischen Gruppen- oder Verhaltenszusammenhang mit anderen Individuen oder Gruppen zu setzen.

2.6 Datenschutz und Beschlagnahmesicherheit

Zentrale Datenbestände bergen aber nicht nur in sich erhebliche Sicherheitsrisiken, z.B. wenn sie kompromittiert, korrumpiert oder physikalisch zerstört werden. Das Hauptproblem, jedenfalls unter dem Thema Freiheit und Sicherheit, sind die Begehrlichkeiten, die sich von allen Seiten auf einmal vorhandene Datenbestände richten. Zwar werden bei der Konzipierung großer Datenbestände regelmäßig der Datenschutz und insbesondere die strenge Zweckbindung der jeweiligen Datensammlung betont und umfangreiche Überlegungen angestellt, wie sich dies sicherstellen ließe. Solche Überlegungen reichen von diversen Verschlüsselungskonzepten bis zu Notar- und Treuhandlösungen mit oder ohne besonders verwahrten Masterkeys. Außerdem wird, wie beim Maut-System, das Publikum mit der Zusicherung beruhigt, dass die Daten wirklich nur für den jeweiligen Zweck erhoben und verwendet werden dürfen, zu dem die Datei eingerichtet wurde.

Allerdings hat das Maut-System gezeigt, dass die Halbwertszeit solcher Zusicherungen sehr gering ist. In einer 80-Millionen-Bevölkerung findet sich immer ein schwerer Kriminalfall, der sich unter Benutzung eines einmal vorhandenen Datenpools, hier des MautDatenpools, leichter lösen ließe. Dementsprechend entsteht sofort politischer Druck auf eine Nutzung des Datenpools für die Verbrechensaufklärung, zunächst selbstverständlich nur eng begrenzt auf Schwerstkriminalität. Ist die Bresche erst einmal geschlagen, ist nach aller Erfahrung zu erwarten, dass es im Laufe der Zeit zu enormen Weiterungen kommen wird.

Im Umkehrschluss heißt dies freilich, alle Daten, die ein Bürger von sich irgendwo preisgeben muss - vom Einwohnermeldeamt bis zur JobCard - oder die er mehr oder minder freiwillig von sich preisgibt - von der Gesundheitskarte bis zur Kreditkarte - unterliegen am Ende jeglichem staatlichen Zugriff, jeglicher Verknüpfung, jeglicher Rasterung und jeglicher Auswertung jenseits aller Zwecke, für die die Datenbestände eingerichtet wurden.

Wir stehen aufgrund der rasanten technischen Entwicklung vor einem Paradigmenwechsel: Über unser Leben fallen anders als jemals in der Geschichte der Menschheit ungeheure Datenmengen der verschiedensten Art an. Diese Daten werden mehr oder minder lang, tendenziell eher länger, gespeichert mit der Folge, dass sie in ihrer Verknüpfung unser Leben lückenlos von außen nachvollziehbar machen und zwar wesentlich präziser, als unsere eigene Erinnerung das hergibt. Auf der anderen Seite denken wir nach wie vor in den klassischen Kategorien des staatlichen Strafanspruchs, der im Grunde das ganze Universum habhaftbarer Daten als Beweismittel gegen das Individuum in Anspruch nimmt, wie es in § 94 Strafprozessordnung (StPO) „Gegenstände, die als Beweismittel für die Untersuchung von Bedeutung sein können, …“ so schön heißt.

Leider erschöpft sich die Problematik nicht im Spannungsverhältnis von ausufernden Datensammlungen und dadurch erheblich erweiterten Zugriffsmöglichkeiten der Strafverfolgungsbehörden. Vielmehr richten sich unzählige weitere staatliche und private Begehrlichkeiten auf die entsprechenden Datenbestände, beginnend bei der wissenschaftlichen Forschung über Infrastruktur- und Bildungsplanung bis zum Gesundheits-, Banken- und Versicherungswesen und schlussendlich zur Werbewirtschaft. Auch diesen Begehrlichkeiten wird der Gesetzgeber über kurz oder lang zumindest teilweise nachgeben, wie z.B. jetzt schon absehbar mit den privaten Auskunftsansprüchen bezüglich Telekommunikationsverkehrsdaten. Hinzu kommen noch die Datenbanken im nichtöffentlichen Bereich, die noch weniger Einschränkungen unterliegen als die Datenbanken des Staates.

Im Ergebnis bedienen sich auf diese Weise Staat und Wirtschaft ungehemmt auf Kosten der Privatsphäre, ohne dass im Moment auch nur ansatzweise erkennbar wäre, an welchem Punkt dieses informationelle Ausweiden des Individuums endet.

2.7 Schlussfolgerung

Meine Schlussfolgerung ist:

Das Polizei- und Sicherheitsrecht beeinträchtigt unsere Privatsphäre und unsere Freiheit in ganz erheblichem Maße. Leider gibt es aber noch andere Lebens-

bereiche mit mindestens vergleichbaren, aber nicht so augenfälligen Freiheitsbeschneidungen.

In dieser Situation müssen wir über vier Optionen nachdenken:

- Wir vereinfachen unser Rechtssystem: Ich weiß, dass dies leichter gefordert als in der politischen und gesellschaftlichen Praxis umgesetzt ist, es löst außerdem nicht die Problematik des staatlichen Zugriffs auf immer mehr Datenbestände. Gleichwohl begrüße und unterstütze ich alle Anstrengungen der Politik, zu einer Rechts- und Bürokratievereinfachung zu kommen. Damit wäre wenigstens etwas gewonnen.

- Wir üben Datensparsamkeit und verzichten zumindest auf den Aufbau großer Datenbanken: Das schützt zwar die Restbereiche unserer Privatsphäre, aber um den Preis, dass wir unter den heutigen technischen Möglichkeiten bleiben und in erheblichem Maß auf die Vorteile verzichten, die uns das informationelle Prozessmanagement bietet. Im Grunde würden wir damit den von vornherein aussichtslosen Versuch unternehmen, den Fortschritt aufzuhalten.

- Wir machen wirklich Ernst mit dem Datenschutz und vor allem mit dem Schutz von Datenbeständen vor jeglicher Inanspruchnahme zu anderen als den erklärten Zwecken. Meiner Auffassung nach wäre dies der einzig gangbare Weg. Er setzt allerdings klare Regelungen hinsichtlich Zweckbindung und Beschlagnahmefreiheit voraus. Auch müssen alle Interessierten äußerste Zurückhaltung hinsichtlich Forderungen nach einem Abrücken von der einmal getroffenen Regelung walten lassen. Zusätzlich müsste ein gesellschaftlicher Konsens bestehen, Durchbrechungsversuche nicht zu akzeptieren. Leider sieht es in der politischen und gesellschaftlichen Realität ganz anders aus: Eher verhungert ein Hund vor einem Wurstvorrat, als dass der Staat und auch die Wirtschaft dauerhaft große Datenbestände unberührt ließen und die Bürger nehmen dies hin.

- Wir machen weiter wie bisher: Dann wird die Informationsverarbeitung immer effizienter und unsichtbarer. Staat und Wirtschaft werden uns mit der Zeit lückenlos überwachen und nach allen Richtungen katalogisieren können. Abweichungen über ein beliebig vordefiniertes Maß hinaus werden sofort erfasst und strafrechtlich oder ökonomisch sanktioniert mit der Folge eines enormen Anpassungsdrucks. Vielleicht ist dies aber gar nicht so schlimm und einfach der nächste Evolutionsschritt zum homo cyberneticus, der eine ganz andere individuelle und soziale Lebens- und Denkweise haben wird als wir.

3 Schwerpunkte im Berichtszeitraum - ein Überblick

3.1 Telekommunikationsüberwachung, Kennzeichenerkennung und Rasterfahndung

Die Änderung des Polizeiaufgabengesetzes hat mit neuen zusätzlichen Maßnahmen der automatisierten Kennzeichenerkennung und der präventiven Telekommunikationsüberwachung zu einer erheblichen Erweiterung der polizeilichen Überwachungsinfrastruktur geführt. Während die zahlenmäßige Entwicklung der präventiven Telekommunikationsüberwachung derzeit keinen besonderen Anlass zur Besorgnis gibt (Nr. 4.13.3), sehe ich bei der automatisierten Kennzeichenerkennung zunehmend datenschutzrechtliche Probleme. Zum einen soll der Umfang des Kennzeichenabgleichs mit dem Fahndungsbestand dadurch ausgeweitet werden, dass dieser Bestand durch eine Vielzahl bisher nicht fahndungsrelevanter personenbezogener Daten aufgefüllt wird. Darüber hinaus soll die automatisierte Kennzeichenerkennung ohne eine dafür notwendige bereichsspezifische Rechtsgrundlage in der Strafprozessordnung auch zur Strafverfolgung eingesetzt werden (Nr. 6.3.2).

Nicht zum Ausbau des polizeilichen Befugnissystems, sondern zum Schutz der Grundrechte der Betroffenen halte ich Nachbesserungen des Polizeiaufgabengesetzes für dringend erforderlich. Dies gilt im Hinblick auf die Rechtsprechung des Bundesverfassungsgerichts insbesondere für die Rasterfahndung (Nr. 4.8). Diese Maßnahme ist nur noch in engen Grenzen zulässig, die ihren Einsatz ohne das Vorliegen konkreter Gefahren nicht mehr zulassen, wie das Bundesverfassungsgericht hinsichtlich der bundesweiten Rasterfahndung zur Enttarnung potentieller Attentäter (sog. Schläfer) nach den Anschlägen vom 11. September 2001 festgestellt hat.

3.2 Akkreditierungsverfahren anlässlich der Fußballweltmeisterschaft 2006

Ohne besondere gesetzliche Grundlage wurden im Rahmen eines Akkreditierungsverfahrens anlässlich der Fußballweltmeisterschaft 2006 Zuverlässigkeitsprüfungen durch Polizei und Verfassungsschutz durchgeführt (Nr. 4.4.1). Ein vergleichbares Verfahren fand auch anlässlich des Papstbesuchs 2006 in Bayern Anwendung. Grundlage für die Einbeziehung der Betroffenen war deren zuvor abgegebene schrift-

liche Einwilligung. Ich habe in beiden Fällen im Hinblick auf die Besonderheit der Ereignisse keine grundsätzlichen Einwendungen erhoben. Sollte dieses Verfahren aber Schule machen, ist eine Entscheidung des Gesetzgebers über das „ob“ und das „wie“ einer solchen Zuverlässigkeitsprüfung notwendig. Auch dann müssen diese Zuverlässigkeitsprüfungen auf wirklich sicherheitsempfindliche Großereignisse beschränkt bleiben.

3.3 Abfragen im polizeilichen Informationssystem

Aufgrund einer datenschutzrechtlichen Kontrolle habe ich festgestellt, dass nahezu jeder dritte Polizeibedienstete einen landesweiten Zugriff auf die Datei Polizeiliche Sachbearbeitung/Vorgangsverwaltung-Verbrechensbekämpfung hat (Nr. 4.2). Damit ist - entgegen meiner Forderung - das Prinzip der regionalen Speicherung von Vorgängen mit nur regionaler Bedeutung (z.B. Beleidigungen, Verkehrsunfälle) endgültig aufgegeben worden. Anders als im früheren regionalen Kriminalaktennachweis und in der bisherigen regionalen Vorgangsverwaltung ist eine Begrenzung des Zugriffs entsprechend der Bedeutung des Vorgangs nicht mehr vorgesehen. Dies stellt einen wesentlichen Rückschritt im polizeilichen Datenschutz dar.

Die Abfragen Polizeibediensteter im polizeilichen Informationssystem dürfen nur für dienstliche und nicht für private Zwecke erfolgen. Ich habe deshalb stichprobenweise 53 aktuelle Datenabfragen überprüft. Dabei konnten sich die betreffenden Polizeibediensteten bei 15 Abfragen nicht mehr konkret an den jeweiligen Anlass erinnern, 3 Abfragen waren eindeutig dem privaten bzw. sozialen Umfeld der abfragenden Polizeibediensteten zuzurechnen. Wegen der Frage des Umfangs der Protokollierung von Abfragen befinde ich mich weiterhin in der Diskussion mit dem Innenministerium. Die von mir geforderte zusätzliche Protokollierung des Grundes der polizeilichen Abfrage und ggf. des polizeilichen Aktenzeichen wird vom Innenministerium trotz der offensichtlichen Notwendigkeit nach wie vor abgelehnt. Bei Datenabfragen aus dem sog. Verkehrsordnungswidrigkeitenverfahren erfolgt sogar überhaupt keine Protokollierung. Ich bin der Auffassung, dass die Polizei im Interesse ihrer Integrität und ihres Ansehens alles daran setzen muss, zur Unterbindung unzulässiger Abfragen und zur Durchführung effektiver, auch polizeiinterner datenschutzrechtlichen Kontrollen alle Zugriffe ausreichend zu protokollieren (Nr. 4.17). Bezüglich der Verkehrsordnungswidrigkeitenverfahren hat mir das Innenministerium mittlerweile eine zeitnahe Realisierung der Protokollierung in Aussicht gestellt.

3.4 Videoüberwachung von Versammlungsteilnehmern

Besonders sensibel sind Videoaufzeichnungen von Versammlungsteilnehmern, weil hier nicht nur in das informationelle Selbstbestimmungsrecht, sondern auch in das für eine Demokratie wesentliche Grundrecht der Versammlungsfreiheit (Art. 8 Abs. 1 GG) eingegriffen wird. Aus diesem Grunde lassen §§ 12 a, 19 a VersammlG polizeiliche Bild- und Tonaufnahmen von Versammlungsteilnehmern nur dann zu, wenn tatsächliche Anhaltspunkte die Annahme rechtfertigen, dass gerade von ihnen erhebliche Gefahren für die öffentliche Sicherheit oder Ordnung ausgehen. Bei der Sichtung von insgesamt 45 Videokassetten mit Aufzeichnungen über drei sensible Versammlungen musste ich leider feststellen, dass vorstehende Anforderungen nicht in allen Fällen beachtet wurden. So wurden zum Teil auch friedliche Versammlungsteilnehmer klar erkennbar in Nahaufnahmen gefilmt (Nr. 4.15.4). Das verantwortliche Polizeipräsidium habe ich schon in der Vergangenheit auf vergleichbare Fehler hingewiesen. Ich glaube aber, dass aufgrund der neuerlichen Vorkommisse, meiner schriftlichen Intervention und intensiver Gespräche ein nachhaltiger Lernprozess eingesetzt hat, der Wiederholungen vermeiden hilft. Darauf werde ich auch in Zukunft achten.

3.5 HEADS (Haft-Entlassenen-Auskunfts-Datei-Sexualstraftäter)

Die Konzeption „Haft-Entlassenen-Auskunfts-Datei-Sexualstraftäter (HEADS)“ sieht zum Schutz der Bevölkerung vor Sexualstraftaten erstmals die zentrale Speicherung rückfallgefährdeter Sexualstraftäter vor. Besonders problematisch dabei ist die unter bestimmten Voraussetzungen vorgesehene Möglichkeit der Bekanntgabe früher begangener Sexualdelikte im Wohnumfeld des Betroffenen. Auf keinen Fall darf es - bei allem Verständnis für den Zweck der Konzeption - dazu kommen, dass dadurch ohne zwingende Notwendigkeit in das Grundrecht auf informationelle Selbstbestimmung, das allgemeine Persönlichkeitsrecht und das Recht auf Resozialisierung eingegriffen wird (Nr. 4.6). Eine unnötige Stigmatisierung bringt keinen Gewinn an Sicherheit, sie birgt vielmehr neue Gefahren aufgrund der sozialen Aussenseiterposition der Betroffenen.

3.6 Neuregelung der Wohnraumüberwachung und der Auskunftserteilung nach dem Verfassungsschutzgesetz

Bereits vor weit über zwei Jahren habe ich das Staatsministerium des Innern auf die Notwendigkeit hingewiesen, die Wohnraumüberwachung durch das Landesamt für Verfassungsschutz neu zu regeln und

dabei die Grundsätze des Bundesverfassungsgerichts zum Schutz privater Lebensgestaltung zu beachten (vgl. hierzu Nr. 8.1, 21. Tätigkeitsbericht). Trotz mehrfacher Erinnerungen ist mir bisher kein entsprechender Gesetzentwurf bekannt geworden. Darüber hinaus fehlt es offenbar nach wie vor an der Bereitschaft des Innenministeriums, sonstige verdeckte Datenerhebungsmaßnahmen an die Grundsätze der Entscheidung des Bundesverfassungsgerichts anzupassen. Dieser Zustand muss schnellstmöglich geändert werden (Nr. 5.1).

Weiterhin habe ich eine Änderung des Bayerischen Verfassungsschutzgesetzes zur Auskunftserteilung an Betroffene angeregt (Nr. 5.2). Bayern ist leider das einzige Bundesland, das keinen grundsätzlichen Auskunftsanspruch, sondern nur eine Entscheidung „nach pflichtgemäßem Ermessen“ vorsieht, wenn ein „besonderes Interesse“ an der Auskunft vorliegt. Nachdem effektiver Rechtschutz, auf dessen Bedeutung das Bundesverfassungsgericht wiederholt hingewiesen hat, eine Kenntnis des Betroffenen über die zu seiner Person gespeicherten Daten voraussetzt, muss ich aus datenschutzrechtlicher Sicht auf einem grundsätzlichen Auskunftsanspruch bestehen. In diesem Sinne habe ich mich an das Staatsministerium des Innern gewandt.

3.7 Antiterrordatei

Besondere Beachtung verdient der Entwurf eines bundesrechtlichen „Gemeinsamen-Dateien-Gesetzes“, der vor allem die Einrichtung einer gemeinsamen Antiterrordatei des Bundes und der Länder zum Inhalt hat (Nr. 5.4). In der Datei sollen Polizei und Nachrichtendienste Daten zu Personen und Objekten speichern, die grundsätzlich allen an der Datei beteiligten Behörden zur Verfügung gestellt werden. Angesichts der derzeitigen Bedrohungslage halte ich eine Antiterrordatei im Interesse des Selbstschutzes des Staates und der Schutzpflicht des Staates gegenüber seinen Bürgern im Prinzip für gerechtfertigt. Ich sehe aber die Gefahr einer Verletzung des sog. Trennungsgebots von Polizei und Nachrichtendiensten. Erforderlich sind zudem eine Präzisierung des zu speichernden Personenkreises, insbesondere auch der sog. Kontaktpersonen, eine Begrenzung von Freitextfeldern, eine Konkretisierung der zugriffsberechtigten Behörden und eine strikte Zweckbindung der gespeicherten Daten zur Aufklärung und Bekämpfung des internationalen Terrorismus. Es darf nicht dazu kommen, dass in den Freitextfeldern nach Belieben zusätzliche Daten eingestellt und frei recherchiert werden können; es darf auch nicht dazu kommen, dass die Datei eines Tages eher der allgemeinen Kriminalitätsbekämpfung als der Abwehr des Terrorismus dient. Und auch die Frage, welche Dienststellen Zugriff auf die Datei nehmen dürfen, sollte gesetzlich geregelt werden und darf nicht die Möglichkeit eröffnen, durch landesrechtliche Organisationsregelungen beliebig vielen Polizei- und Sicherheitsbehörden den Zugriff auf den Datenverbund der Antiterrordatei zu eröffnen. Auch eine zeitliche Befristung der Geltungsdauer der gesetzlichen Regelungen und eine Verpflichtung zu ihrer Evaluierung durch unabhängige externe Sachverständige sind aus datenschutzrechtlicher Sicht zu fordern.

3.8 Harmonisierung der strafprozessualen verdeckten Ermittlungsmaßnahmen

Ich habe bereits wiederholt gefordert, dass die in der Strafprozessordnung geregelten verdeckten Ermittlungsmaßnahmen, wie insbesondere die Telekommunikationsüberwachung auf der Grundlage der Rechtsprechung des Bundesverfassungsgerichts neu gefasst werden (Nr. 6.1.3). Dabei müssen die Voraussetzungen und Grenzen der Eingriffsbefugnisse klar erkennbar und verfassungskonform geregelt sein. Insbesondere sind Regelungen zu schaffen, die einen aus der Menschenwürde abgeleiteten unantastbaren Kernbereich privater Lebensgestaltung sowie den Schutz von Vertrauensverhältnissen gewährleisten. Darüber hinaus müssen als Voraussetzungen für verdeckte Maßnahmen die Erforderlichkeit sowie die Angemessenheit überprüft und ausreichende Regelungen zur Zweckbindung der erhobenen Daten zusammen mit Benachrichtigungspflichten und Löschungsfristen vorgesehen werden. In den letzten Jahren hat der Gesetzgeber neue repressive Eingriffsbefugnisse (z.B. Maßnahmen bei Mobilfunkendgeräten und Funkzellenabfrage) sowie Änderungen bei bestehenden Regelungen (z.B. Erweiterung des Straftatenkatalogs für die Telekommunikationsüberwachung) eingefügt, ohne in ausreichendem Maße dafür zu sorgen, dass verdeckte Ermittlungsmaßnahmen klar und verständlich geregelt und an die Rechtsprechung des Bundesverfassungsgerichts angepasst werden. Es bedarf deshalb einer grundlegenden Überarbeitung aller verdeckten Ermittlungsmaßnahmen.

Auch bei der sog. Funkzellenabfrage (Abfrage aller in einer bestimmten Funkzelle in einem bestimmten Zeitraum angefallenen Telekommunikationsverbindungsdaten) habe ich festgestellt, dass die Regelungen über die repressiven verdeckten Ermittlungsmaßnahmen reformbedürftig sind (Nr. 6.1.4). Diese Maßnahmen haben eine weite Streubreite und beziehen zahlreiche, auch unbescholtene Personen in ihren Wirkungsbereich ein. Ich halte die gesetzliche Vorschrift (§ 100 h StPO), auf die diese Maßnahme gestützt wird und die als reine Verfahrensvorschrift konzipiert ist, für unzureichend. Für Funkzellenabfragen zum Zwecke eines automatisierten Abgleichs mit Telekommunikationsverbindungsdaten anderer sog. tatrelevanter Örtlichkeiten sehe ich in der Strafprozessordnung keine Rechtsgrundlage.

Die in dem Koalitionsvertrag vom 11.11.2005 angekündigte „harmonische Gesamtregelung der strafprozessualen heimlichen Ermittlungsmaßnahmen“ begrüße ich daher nachdrücklich. Sie wird die oben aufgezeigten verfassungsrechtlichen Anforderungen zu beachten, Wertungswidersprüche zu beseitigen und den gesamten Regelungskomplex neu zu strukturieren haben. Leider lässt die notwendige Reform noch auf sich warten, ein entsprechender Entwurf liegt mir noch nicht vor.

3.9 Videoüberwachung im Kommunalbereich

Mit Sorge verfolge ich eine zunehmende Tendenz in Kommunen, öffentliche Plätze, Gebäude und Einrichtungen mit Videokameras zu überwachen. Anlass einer solchen Überwachung können für die Gemeinden z.B. Ruhestörungen im Umfeld von Gaststätten und Schmierereien sowie sonstige Beschädigungen an kommunalen Gebäuden oder Einrichtungen sein. Ein besonders krasser Fall, der mir bekannt wurde, war die Videoüberwachung des Innenraums einer öffentlichen Toilette (siehe Nr. 8.8). Nach meinem Eindruck ist vielen Gemeinden noch nicht ausreichend bewusst, dass die Beobachtung ihrer Bürger mittels Videotechnik einen Eingriff in deren allgemeines Persönlichkeitsrecht darstellt und sie einem Anpassungsdruck aussetzt. Das Recht der Bürger, sich grundsätzlich unbeobachtet im öffentlichen Raum bewegen zu können, wird durch die Ausdehnung dieser Form der Überwachung zunehmend eingeschränkt. Die Kommunen, die den Einsatz einer Videoüberwachung in Betracht ziehen, müssen deshalb im Rahmen der Prüfung der Zulässigkeit einer solchen Maßnahme sehr genau überlegen, ob die Maßnahme zur Erfüllung des damit angestrebten Zwecks geeignet erscheint, keine milderen Mittel ergriffen werden können und eine Videoüberwachung die von ihr ausgehenden Grundrechtsbeeinträchtigungen noch rechtfertigt. Das Innenministerium hat zu Recht den Einsatz privater Sicherheitsdienste auf öffentlichen Straßen und Plätzen abgelehnt und den Kommunen empfohlen, aktuelle Sicherheits- und Ordnungsprobleme mit der Leitung der örtlichen Polizeiinspektion zu besprechen. Je nach Fallkonstellation könnte dann etwa der verstärkte Einsatz von Polizeistreifen das Ergebnis sein. Zusätzlich könnten auch weitere Aspekte wie z.B. konsequente gaststättenrechtliche Auflagen zur Lösung der Sicherheitsproblematik beitragen. Solche und andere Maßnahmen können auch gegenüber einer Videoüberwachung mit dem damit verbundenen Eingriff in das informationelle Selbstbestimmungsrecht der Bürger das mildere und damit rechtlich allein zulässige Mittel sein.

3.10 Auf dem Weg zur elektronischen Schulverwaltung

Die Staatsregierung verstärkte im Berichtszeitraum ihre Bestrebungen, den Bildungsbereich für die sich auch auf internationaler Ebene stellenden Anforderungen der heutigen Zeit fit zu machen.

So beabsichtigt das Kultusministerium mit der Neukonzeption des Verfahrens „Amtliche Schuldaten“ letztlich die Umstellung der gesamten Schulverwaltung auf eine netzbasierte elektronische Verwaltung. Damit einher geht die Umstellung der Schulstatistik auf Individualdaten im Rahmen eines bundeseinheitlichen Kerndatensatzes. So sehr ich auch eine Rationalisierung von Arbeitsprozessen befürworte, stellt doch die mit einem derartigen Großprojekt entstehende Dateninfrastruktur besondere datenschutzrechtliche Anforderungen. Ich habe daher gegenüber dem Kultusministerium die Schaffung einer klaren und umfassenden gesetzlichen Rechtsgrundlage angemahnt, in der insbesondere die Datenschutzrechte der Schüler und Lehrer, aber auch die statistikrechtlichen Anforderungen sicher gestellt werden müssen (siehe Nr. 21.1). Dass die Kultusverwaltung sich derzeit noch mit ersten Ansätzen zu einer netzbasierten Schulverwaltung schwer tut, wird an einem Einzelfall deutlich (Nr. 21.2). Vor allem internationalen Vorgaben versucht das Kultusministerium durch die Einführung einer Verpflichtung aller Schüler zur Teilnahme an schulischen Leistungsvergleichen nachzukommen, auch wenn diese meiner Auffassung nach letztlich keine nennenswerten Verfahrenserleichterungen mit sich bringt (Nr. 11.2). Das Modellprojekt „fit & pfundig“ zeigt exemplarisch die Probleme mit der datenschutzkonformen Durchführung eines wissenschaftlichen Vorhabens; man kann daraus aber auch Erkenntnisse für die Durchführung künftiger Projekte ableiten (Nr. 11.4).

3.11 „Hochschulreform 2006“ und mehr

Mit der „Hochschulreform 2006“ hat der Landtag ein neues, grundlegend modernisiertes bayerisches Hochschulrecht beschlossen. Im Rahmen meiner Beteiligung im Gesetzgebungsverfahren konnte ich hier zahlreiche Verbesserungen in datenschutzrechtlicher Hinsicht erreichen. Allerdings geht die Veröffentlichung der Ergebnisse der studentischen Bewertungen der Lehre aus meiner Sicht einen Schritt zu weit (Nr. 12.1). Mit dem Projekt CEUS^{HB} soll ein Führungsinformationssystem für die Hochschulen und das Wissenschaftsministerium geschaffen werden. Dieses soll auf der Grundlage eines hierarchisch aufgebauten Data-Warehouse-Systems Effizienz und Wirtschaftlichkeit des Hochschulmanagements steigern. Aus datenschutzrechtlicher Sicht ist hier insbesondere Augenmerk zu legen auf die Wahrung der Anonymisierung der eingestellten Daten; differen-

zierte und einschränkende Berechtigungskonzepte können dabei zur Problemlösung beitragen (Nr. 21.3). Wichtige Entscheidungsgrundlagen für eine Optimierung der bayerischen Hochschulpolitik sollen auch mithilfe des Langzeitprojekts „Bayerisches Absolventenpanel“ gewonnen werden. Mit diesem auf Länderebene bislang einzigartigen Projekt soll eine Absolventenbefragung in Bayern etabliert werden, die sowohl das Wissenschaftsministerium als auch die bayerischen Hochschulen in regelmäßigen Abständen über die Qualität der Ausbildung sowie den Arbeitsmarkt- und Berufserfolg bayerischer Absolventen informiert (Nr. 12.2).

3.12 Elektronische Gesundheitskarte

Wohl kaum ein Vorhaben wird so viele Umwälzungen im Gesundheitswesen mit sich bringen, wie die elektronische Gesundheitskarte (Nr. 14.1.1). Die Öffentlichkeit scheint sich jedoch nur zögerlich für die Thematik zu interessieren. Dabei wäre gerade hier eine gesamtgesellschaftliche Diskussion darüber erforderlich, worin die Chancen und Risiken der elektronischen Gesundheitskarte liegen. Denn jeder Bundesbürger wird von der elektronischen Gesundheitskarte, wenn sie einmal kommt, betroffen sein.

Inhaltlich wird durch die elektronische Gesundheitskarte eine Vernetzung aller Beteiligten (z.B. niedergelassene Ärzte, Krankenhäuser, Krankenkasse, Heilberufe, Apotheken) möglich gemacht. Die wichtigsten medizinischen Basisdaten eines Patienten (wie z.B. Allergien, schwerwiegende Krankheiten, Arzneimittelunverträglichkeiten) sollen für alle Akteure im Gesundheitswesen ständig verfügbar sein, um eine adäquate Behandlung sicherzustellen. Neuartige Anwendungen, wie der elektronische Arztbrief oder die elektronische Patientenakte, sollen durch die elektronische Gesundheitskarte ebenfalls ermöglicht werden. Außerdem sollen getrennte Datenbestände zu einer integrierten medizinischen Dokumentation zusammengeführt werden, so dass der behandelnde Arzt die Vorerkrankungen sowie die Diagnosen und Behandlungen seiner Vorgänger unkompliziert und schnell einsehen kann. All dies steht unter der Zielsetzung, die Behandlung zu verbessern.

Von Seiten des Datenschutzes wurden bereits frühzeitig u.a. folgende Schwerpunktthemen herausgestellt:

- Wer hat welche Zugriffsrechte?
- Wie erfolgt die Autorisierung?
- Wo ist der Speicherort der Daten?
- Welches Betreiberkonzept gibt es?
- Wie werden die gespeicherten und übertragenen Daten geschützt?

Trotz dieser gewichtigen Probleme bin ich in meiner Amtszeit zwar von einzelnen Bürgern auf die elektronische Gesundheitskarte angesprochen worden, auch Hörfunk und Presse interessieren sich gelegentlich für das Thema, eine breite Diskussion hat jedoch noch nicht eingesetzt. Dies mag auch daran liegen, dass entgegen den Ankündigungen der Politik die praktische Umsetzung und Testung immer weiter verschoben wird. Angesichts der Komplexität des Themas ist dies auch verständlich. Es darf jedoch nicht dazu kommen, dass die Einführung der elektronischen Gesundheitskarte im stillen Kämmerchen vor sich geht und der Bürger eines Tages vor vollendete Tatsachen gestellt wird.

Immerhin wurde festgelegt, dass in Bayern das Vorhaben in der Testregion Ingolstadt geprüft werden soll. Auch die Verknüpfung der verschiedenen Großverfahren im Rahmen der E-Card-Strategie der Bundesregierung (ELENA, Personalausweis, eGK) sollte bei Einführung der elektronischen Gesundheitskarte kritisch erörtert werden. Denn hier ist die Tendenz erkennbar, dass unterschiedliche Verfahren und Datenbestände zusammengeführt werden (vgl. 2.5). Damit entsteht ein völlig neues Risikopotenzial für den Bürger. Von daher wird die elektronische Gesundheitskarte als „Vorreiterkarte“ in meiner Tätigkeit auch weiterhin eine wichtige Rolle spielen.

3.13 Informationelle Selbstbestimmung und Hartz IV

Das im Berichtszeitraum mit am intensivsten diskutierte Thema im Sozialbereich war sicherlich „Hartz IV“ (s. auch Nr. 14.4.1). Es ist schon erstaunlich, was hier in vergleichsweise geringer Zeit bereits alles wieder geändert, fortentwickelt und verschärft werden soll. Dabei sind weiterhin grundlegende verfassungsrechtliche Fragen ungeklärt. In der täglichen Arbeit eines Landesbeauftragten für den Datenschutz zeigt sich, dass auch bei neuen Gesetzen altbekannte datenschutzrechtliche Problemstellungen wieder auftauchen. So geht es auch hier um die klassischen Fragen der Akteneinsicht, der Mitwirkungspflicht (z.B. bei der Vorlage von Kontoauszügen) oder der technisch-organisatorischen Maßnahmen des Datenschutzes.

Unverkennbar besteht eine Tendenz, die Bedingungen des Leistungsbezugs für die Betroffenen zu verschärfen. Die generelle Zulässigkeit der verdachtslosen Datenerhebung wird im politischen Raum gefordert, der automatisierte Sozialdatenabgleich wurde auch im Bereich des SGB II Wirklichkeit. Paradigmenwechsel im materiellen Recht, wie z.B. die Betonung des Grundsatzes „Fördern und Fordern“, haben

auch Auswirkungen auf den Datenschutz. Denn der Weg vom Nachtwächterstaat, der sich nur auf die unbedingt notwendigen Aufgaben der Daseinsvorsorge beschränkt, den Bürger aber im Übrigen in Ruhe lässt, hin zum allgegenwärtigen Versorgungsstaat und unter dem Diktat der leeren Kassen wieder teilweise zurück zur staatlichen „Kernkompetenz“ führt dazu, dass eben dieser Staat trotz seines Teilrückzugs den Bürger erst recht nicht in Ruhe lässt. Vielmehr sammelt er immer mehr personenbezogene Daten, um den Betroffenen aus der Sicht des Staates eine optimale, aber nicht zu teure Hilfe angedeihen zu lassen und jedem Individuum eine nicht zu bequeme soziale Minimalhängematte maßzuschneidern. Das geht aber nur mit einem immer noch intensiveren Einmischen in private Angelegenheiten. So erfolgen z.B. intensive Datenerhebungen, um möglichst alle denkbaren Einsatzmöglichkeiten Betroffener auszuloten. In bestimmten Regionen Bayerns und bei manchen Personenkreisen geht dies jedoch an den Realitäten des Arbeitsmarkts vorbei.

Deutlich wird in diesem Zusammenhang Folgendes: Auch hier ist Datenschutzrecht nur Annex zu Entwicklungen in der Gesellschaft und im materiellen Recht.

3.14 Private Auskunftsansprüche und Vorratsdatenspeicherung

Das Bundesministerium der Justiz beabsichtigt, in Umsetzung der europäischen Richtlinie zur Durchsetzung der Rechte des geistigen Eigentums den Rechteinhabern in bestimmten Fällen Auskunftsansprüche auch gegenüber unbeteiligten Dritten - wie etwa Internet-Providern - einzuräumen. Nachdem das grundrechtlich geschützte Fernmeldegeheimnis in den letzten Jahren immer stärker und in immer kürzeren Abständen für Zwecke der Strafverfolgung und der Geheimdienste eingeschränkt wurde, soll es nun auch erstmals zugunsten privater wirtschaftlicher Interessen nicht unerheblich weiter eingeschränkt werden. Vor dem Hintergrund der im Jahr 2006 auf EU-Ebene beschlossenen Vorratsspeicherungs-Richtlinie wäre es völlig unakzeptabel, wenn Telekommunikationsverkehrsdaten, deren zwangsweise Speicherung mit der Abwehr terroristischer Gefahren begründet wurde, nun auf breiter Basis für die Verfolgung von Urheberrechtsverletzungen genutzt würden. Ich hoffe, dass der Gesetzgeber im Zuge der Umsetzung dieser europäischen Richtlinien den datenschutzrechtlichen Aspekten die notwendige Bedeutung beimisst; dafür werde ich mich auch weiterhin persönlich einsetzen (Nr. 20.2).

3.15 Rund um die GEZ

Ständig erreichen mich auch Beschwerden über die GEZ, die Gebühreneinzugszentrale der öffentlich-rechtlichen Rundfunkanstalten. Verärgerte Bürger wollen wissen, wie die GEZ an ihre Daten gekommen ist. Neben Melderegisterauskünften, die die GEZ auf der Grundlage melderechtlicher Bestimmungen erhält (siehe dazu näher unter Nr. 9.2), beschafft sie sich Daten insbesondere beim kommerziellen Adresshandel. Den Bürgern muss ich dabei jedes Mal mitteilen, dass ich für die Kontrolle des Datenschutzes bei der GEZ selbst nicht zuständig bin. Meine Prüfungskompetenz beschränkt sich auf die Kontrolle der Datenübermittlung durch öffentliche bayerische Stellen, hier die Meldebehörden, an die GEZ. Darüber hinaus halte ich im Hinblick auf das Steuergeheimnis beispielsweise eine Datenübermittlung aus der kommunalen Grundsteuerdatei an die GEZ nur unter Einschränkungen für datenschutzrechtlich zulässig (Nr. 20.4). Gleichwohl kann ich die Augen nicht davor verschließen, dass mich hinsichtlich der Aktivitäten der GEZ mehr Beschwerden als in manch anderen Bereichen erreichen, für die ich zuständig bin. Hier wäre es erforderlich, nach einer Gebührenstruktur zu suchen, die die Datenerhebungen und die Kontrolltätigkeit der GEZ auf ein für die Bürger erträgliches Maß zurückschraubt. In dieser Hinsicht habe ich mich u.a. für eine datenschutzkonforme Befreiung von der Rundfunkgebührenpflicht eingesetzt: Nach derzeitiger, datenschutzrechtlich äußerst problematischer Rechtslage können die Empfänger bestimmter Sozialleistungen die Befreiungsvoraussetzungen nur durch Vorlage des - vollständigen - Sozialleistungsbescheides im Original oder in beglaubigter Kopie zentral bei der GEZ nachweisen. In langwierigen Verhandlungen haben meine Kollegen und ich erreicht, dass die Antragsteller diese Voraussetzungen künftig auch durch Vorlage (lediglich) einer Bestätigung des Sozialleistungsträgers über die Gewährung und die Dauer der Sozialleistung nachweisen können (Nr. 20.3).

3.16 Umgang mit Biomaterial

Biomaterialbanken, d.h. Sammlungen von Proben des menschlichen Körpers (z.B. Blut, Gewebe, etc.), können vielfältige Facetten haben: Zum einen gibt es die klassische Biomaterialbank in einem Universitätsklinikum, die der medizinischen Forschung und der Patientenversorgung dient. Daneben werden zunehmend deutschland- und europaweit Biomaterialdatenbanken (Datensammlungen mit Auswertungen der Biomaterialien) aufgebaut, die außer zu wissenschaftlichen auch zu kommerziellen Zwecken verwendet werden können. Mit der zunehmenden Verbreitung genetischer Analysen gewinnt der Umgang mit menschlichem Biomaterial nochmals an Brisanz.

Allgemein war zu beobachten - und das ist positiv herauszustellen -, dass die Institutionen, mit denen ich Kontakt hatte, für Belange des Datenschutzes durchaus aufgeschlossen waren. Auch das Schutzniveau von Proben und Daten war durchgängig hoch. Dies mag zum einen daran liegen, dass die beteiligten Kreise in vielen Fällen der ärztlichen Schweigepflicht unterliegen und deshalb für die Belange des Datenschutzes bereits seit dem Hippokratischen Eid (ca. 420 vor Christus) besonders sensibilisiert sind, zum anderen jedoch auch daran, dass die Proben einen enormen wirtschaftlichen und wissenschaftlichen Wert darstellen können. So achten z.B. Institutsdirektoren sorgsam darauf, dass kein Unberufener Zugang zu wertvollem Probenmaterial hat und es verschwendet.

Ohne dass ich mich auf die These versteifen möchte, dass das Niveau des Datenschutzes primär am Wert der Daten für die datenhaltende Stelle orientiert ist, zeigt sich auch hier: Besonders geschützt wird, was als wertvoll erachtet wird. Dass das hohe Schutzniveau auch dem informationellen Selbstbestimmungsrecht der Betroffenen zugute kommt, ist leider nur Nebeneffekt, wenn auch ein erfreulicher.

Im Umgang mit Proben, die im Zusammenhang mit einer Behandlung anfallen, wäre aus Datenschutzsicht eine Pseudonymisierung der Proben wünschenswert und möglich. Gleichwohl ist nicht zu verkennen, dass eine Beschriftung der Proben mit identifizierenden Angaben zum Patienten die Verwechslungsgefahr erheblich reduziert. Da eine Verwechslung u.U. zu lebensbedrohlichen Situationen für den Patienten führen könnte, muss eine personenbezogene Beschriftung und Nutzung von Proben im Behandlungszusammenhang datenschutzrechtlich hingenommen werden. Dies gilt auch für die im Zusammenhang mit den Proben anfallenden Daten, z.B. Analyseergebnisse. Dennoch müssen nach wie vor gewisse Datenschutzanforderungen beachtet werden. Diese sind in Nr. 23.5.3 zusammengestellt.

Im Rahmen der Forschung wird in vielen, aber noch nicht in allen Fällen bereits heute mit anonymisierten oder pseudonymisierten Daten gearbeitet. Dabei fallen die Verfahren zur Anonymisierung bzw. Pseudonymisierung jedoch sehr unterschiedlich aus. Besonders komplex wird das Ganze, wenn es sich um sog. Multicenter-Studien handelt, bei denen Daten und Proben mehrerer, über das Bundesgebiet verteilter Stellen gesammelt und anschließend von allen oder von einigen genutzt werden. Hier ist noch vieles im Fluss, aber ich werde meinen Beitrag zur Erarbeitung allgemein anerkannter Standards leisten.

Leider lag auch nicht in allen Fällen von Forschungsvorhaben die hierfür zwingend erforderliche Einwilligung des Patienten vor; es fehlte auch an einer eingehenden und ausführlichen Patienteninformation über das Vorhaben. Ich verkenne nicht die praktische Schwierigkeit hierbei - insbesondere, wenn sich ein Forschungsvorhaben erst im Laufe der Zeit ergibt und der Patient z.B. nicht mehr unmittelbar kontaktiert werden kann, weil er sich nicht mehr zur Behandlung im Klinikum befindet. Es ist aber dennoch nicht statthaft, eine pauschale Einwilligung des Patienten für jedwedes künftige Forschungsvorhaben vorab einzuholen. Eine Liste mit Mindeststandards für den Umgang mit Biomaterialien in der Forschung ist in Nr. 23.5.3 zusammengestellt.

3.17 Internetauftritt und sichere elektronische Kommunikation

Das Internet ist ein Dauerbrenner. Untrennbar damit verbunden sind gesetzliche Anforderungen für die Homepage-Anbieter und Sicherheitsmaßnahmen wie Verschlüsselung und elektronische Signatur, private Nutzung dienstlicher Einrichtungen und Protokollierung.

Obwohl es die gesetzlichen Vorgaben des Teledienstegesetzes (TDG) und Teledienstedatenschutzgesetzes (TDDSG) seit mehr als neun Jahren gibt, finden sich immer wieder Behörden, die die datenschutzrechtlichen Forderungen dieser Vorschriften nach Anbieterkennzeichnung und Online-Datenschutzerklärung noch nicht erfüllen. Ich fordere daher alle öffentlichen Stellen mit einer eigenen Homepage auf, ihre Angebote umgehend hinsichtlich der Konformität mit dem TDG und dem TDDSG zu überprüfen und ggf. zu ergänzen bzw. zu korrigieren.

Verschlüsselung und elektronische Signatur bedingen eine Public Key Infrastruktur (PKI), ob sie nun für die Kommunikation über das Internet z.B. mit anderen Behörden oder Bürgern eingesetzt werden sollen oder in geschlossenen Netzen wie dem bayerischen Behördennetz BayKOM. Seit mehreren Jahren mahne ich die Verwendung dieser Mechanismen auch in meinen Tätigkeitsberichten an. Im BayKOM hat es hier nicht zuletzt aufgrund neuerer organisatorischer Maßnahmen erhebliche Verbesserungen und positive Entwicklungen gegeben (vgl. 23.2). Dennoch sind wir noch einiges von einer durchgängig vertraulichen, authentischen und integren Kommunikation und Datenverarbeitung entfernt. Die entsprechenden Anstrengungen sind in diesem Bereich daher auszubauen und zu forcieren, sonst wird das angestrebte eGovernment dauerhaft nicht zu erreichen sein.

3.18 E-Mails und Fernmeldegeheimnis

Der Umgang mit E-Mail gibt unverändert immer wieder Anlass für Eingaben oder Fragestellungen an mich. Ich möchte hier nur das Thema Spam-Behandlung und Fernmeldegeheimnis herausgreifen,

welches unter Nr. 23.3 sowohl aus rechtlicher wie aus technischer Sicht eingehend erörtert wird.

Soweit es sich um den dienstlichen E-Mail-Verkehr von Behörden handelt, können E-Mails von einem zentralen Mail-Server bzw. Spam-Filter als Spam identifiziert, markiert, blockiert und auch gelöscht werden. Probleme ergeben sich vor allem dann, wenn der Dienstherr darüber hinaus die private Nutzung des E-Mail-Dienstes zulässt oder auch nur toleriert. In diesem Fall unterliegen Spam-Mails im Zusammenhang mit dem an den privaten Nutzer gerichteten E-Mail-Verkehr dem Fernmeldegeheimnis des Nutzers. Die gesamte soeben angesprochene Spam-Behandlung ist daher ohne Einwilligung des Nutzers rechtlich nicht zulässig. Dies bedeutet, dass Behörden ihren Bediensteten nur dann die private Nutzung des E-Mail-Dienstes ermöglichen sollten, wenn sie gleichzeitig eine Einwilligung des jeweiligen Bediensteten zur Spam-Behandlung erhalten.

3.19 Berechtigungskonzepte bei IuK-Anwendungen

Bei der konventionellen, d.h. papiergebundenen, Datenverarbeitung ist es eine Selbstverständlichkeit, dass nicht jeder Mitarbeiter Zugriff auf jede Akte hat. Dafür sorgen einerseits klare Aufgabenzuweisungen und Zuständigkeitsregelungen und andererseits organisatorische Maßnahmen, die die Einhaltung dieser aus guten Gründen vorhandenen Regeln sicherstellen. Mit der Informations- und Kommunikationstechnik (IuK) und der damit einhergehenden zentralen Speicherung von Daten sowie der schnellen und allerorts gleichzeitigen Verfügbarkeit der Information wird die Einhaltung dieser Grundsätze umso wichtiger. Gleichwohl scheinen sich hier aber Nachlässigkeiten dahingehend eingeschlichen zu haben, dass diese aufgabenbezogene Abschottung mitunter als nicht mehr so zwingend erforderlich angesehen wird. Schlamperei wird hier häufig mit Effizienzsteigerung, Arbeits- und Verwaltungsvereinfachung sowie Modernisierung und Mängelbeseitigung im innerbehördlichen oder teilweise gar behördenübergreifenden Informationsfluss zu rechtfertigen versucht. Hierfür fehlt mir jedes Verständnis.

Richtig ist:

Für jede IuK-Anwendung ist ein klares Berechtigungskonzept erforderlich (vgl. auch Nr. 23.5.5). Dies kann einmal sehr einfach und zugegebenermaßen ein anderes Mal durchaus auch sehr komplex sein. Generell sind aber folgende Grundsätze zu beachten:

- Für jeden einzelnen Berechtigten sind eine persönliche Benutzerkennung und ein persönliches Passwort zum Zugang zu IuK-Systemen und -Verfahren vorzusehen. Dies kann auch mit Hilfe technischer Mittel wie Chipkarten u.ä. unterstützt werden. Der Benutzer muss selbst in der Lage sein, sein nur ihm bekanntes persönliches Passwort jederzeit selbst ändern zu können. Das IuK-System muss den Benutzer in regelmäßigen Abständen (z.B. alle 90 Tage) zur Passwortänderung zwingen und definierte Qualitätsregeln für Länge, Aufbau und Struktur von Passworten durchsetzen.

- Die Berechtigungen für jeden einzelnen Benutzer dürfen nur nach dem Erforderlichkeitsprinzip zugeteilt werden, d.h. jeder Benutzer darf keinen Zugriff auf mehr Daten erhalten als zu seiner Aufgabenerfüllung erforderlich ist - aber auch nicht weniger. Bei IuK-Verfahren mit größerem Benutzerkreis ist die Verwendung eines Rollenkonzeptes mit modular aufgebauten Einzelberechtigungen hilfreich und empfehlenswert.

- Die gesamte Benutzerverwaltung mit Berechtigungsverwaltung muss revisionsfähig erfolgen, d.h. es muss nachträglich nachweisbar sein, wer zu welcher Zeit welche Befugnisse, Zugriffsberechtigungen und -möglichkeiten im IuK-System hatte.

Mit der zunehmenden Verbreitung von IuK-Technik zur Aufgabenerfüllung scheint gelegentlich die Aufmerksamkeit beim Umgang mit personenbezogenen Daten auf dem Medium Papier abzunehmen. Mängel wie das Fehlen oder auch nur die mangelnde Nutzung abschließbarer Behältnisse und Aktenschränke zur zugriffssicheren Aufbewahrung personenbezogener Unterlagen sowie eine nicht datenschutzgerechte Entsorgung von Papierunterlagen sollten eigentlich der Vergangenheit angehören. Leider scheint dem aber nicht so zu sein. Ich fordere daher alle öffentlichen Stellen auf, über der Einführung und datenschutzgerechten Nutzung der IuK-Technik nicht die „konventionelle“ Datenverarbeitung zu vergessen - auch hier muss nach wie vor sauber gearbeitet werden und dazu gehört die Einhaltung des Datenschutzes.

3.20 Rechtsvorschriften zum Datenschutz auf meiner Homepage

Kurz erwähnen möchte ich noch folgenden Service meiner Geschäftsstelle: Viele Bürgerinnen und Bürger, aber auch Beschäftigte im Öffentlichen Dienst haben mitunter Schwierigkeiten, aktuell gültige und für ihre Fragestellung einschlägige Rechtsvorschriften zum Datenschutz zu finden. Auch aus diesem Grunde biete ich in Zusammenarbeit mit der Juris GmbH seit Juni 2005 auf meiner Homepage www.datenschutz-bayern.de über vierzig einschlägi-

ge Vorschriften und Normen - gruppiert nach Themenbereichen - an. Diese Rechtsvorschriften werden im täglichen Turnus aktuell gehalten, so dass neueste Gesetzes- und Vorschriftenänderungen zeitnah auch der interessierten Öffentlichkeit und öffentlich Bediensteten zur Verfügung stehen. Die Nutzung dieses Services ist für den Abrufenden selbstverständlich kostenlos.

4 Polizei

Meine Tätigkeit im Polizeibereich umfasste die Kontrolle von Speicherungen in Dateien, wie z.B. im Kriminalaktennachweis, den Dateien „Gewalttäter Sport“ und „Prostitution/Zuhälter“, dem „Rauschgift-Informationssystem“, sowie in weiteren Dateien, insbesondere in regional geführten Dateien zur Gefahrenabwehr und Verfolgung von Straftaten und Ordnungswidrigkeiten (GAST-Dateien). Ich habe außerdem Datenerhebungsmaßnahmen wie beispielsweise erkennungsdienstliche Behandlungen, Speichelprobenentnahmen zum Zwecke der DNA-Analyse sowie Telekommunikationsüberwachungsmaßnahmen überprüft. Die polizeilichen Überwachungsmaßnahmen und Speicherungen im Zusammenhang mit der Fußballweltmeisterschaft sowie den Münchener Sicherheitskonferenzen 2005 und 2006, die Durchführung von DNA-Massenscreenings in zwei Fällen sowie die Videoüberwachung auf öffentlichen Straßen und Plätzen und bei Versammlungen waren weitere Prüfungsschwerpunkte.

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

Durch datenschutzrechtliche Beurteilungen habe ich auf die datenschutzkonforme Ausgestaltung von Gesetzen und Richtlinien hingewirkt. Besonders bei der Änderung des Polizeiaufgabengesetzes habe ich mich für Normenklarheit und Bestimmtheit der Eingriffsvoraussetzungen sowie die Beachtung des Verhältnismäßigkeitsgrundsatzes und des Schutzes des Kernbereichs privater Lebensgestaltung eingesetzt. Daneben habe ich auch zahlreiche Errichtungsanordnungen für polizeiliche Dateien geprüft und an Prüfungen von bundesweiten polizeilichen Dateien mitgewirkt.

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

Die nachfolgenden Darstellungen sind eine Auswahl meiner Feststellungen im Polizeibereich.

4.1 Kriminalaktennachweis (KAN)

Auch in meinem 21. Tätigkeitsbericht (vgl. Nr. 7.1) hatte ich von den Verhandlungen mit dem Staatsministerium des Innern zur datenschutzrechtlichen Verbesserung des Verfahrens der personenbezogenen Speicherung von Erkenntnissen aus strafrechtlichen Ermittlungsverfahren insbesondere im Kriminalaktennachweis berichtet. Die Neufassung der hierfür geltenden Richtlinien für die Führung polizeilicher personenbezogener Sammlungen (PpS-Richtlinien) und der Errichtungsanordnung für die Personen- und Fall-Auskunftdatei (EA PFAD) ist im März 2005 vom Innenministerium in Kraft gesetzt worden. Das Innenministerium hat einen Teil meiner Forderungen zur datenschutzrechtlichen Verbesserung dieser Vorschriften aufgenommen. Dabei handelt es sich insbesondere um

- die Klarstellung, dass grundsätzlich Fälle „geringerer Bedeutung“ nicht auf wenige Straftatbestände aus dem Bagatellbereich beschränkt sind,
- die Aufnahme eines Hinweises, dass in Fällen von geringerer Bedeutung auch für Kinder und Jugendliche kürzere Fristen festzulegen sind,
- die Änderung der Deliktsbezeichnung im KAN nicht nur dann, wenn die Verurteilung wegen einer Straftat einer völlig anderen Deliktsrichtung erfolgt, sondern in jedem Fall bei einer Verurteilung wegen einer anderen Straftat,
- eine Pflicht zur Dokumentation der Gründe, wenn aus kriminologischer Sicht ein Fall geringerer Bedeutung als einzige Speicherung im KAN und nicht in der Vorgangsverwaltung nachgewiesen werden soll,
- die Festlegung, dass die Speicherung von Suizidversuchen, die nicht im Zusammenhang mit einer Straftat stehen, keine Verlängerung der Aufbewahrungsfristen bestehender Speicherungen im KAN bewirkt,
- die Verdeutlichung, dass Datenübermittlungen im Einzelfall grundsätzlich nur aus schriftlichen Unterlagen und nicht nur auf der Grundlage der Dateispeicherungen erfolgen dürfen,
- die Aufnahme einer Regelung, dass im Falle einer Datenübermittlung durch die Polizeidienststelle auch die Rechtsgrundlage der Verfahrensbeendigung durch die Justiz (z.B.

§ 170 II StPO, § 47 JGG, Freispruch etc.) mitzuteilen ist, soweit diese bekannt ist.

Leider hat das Staatsministerium des Innern - entgegen meiner Forderung - festgelegt, dass die Annahme eines Falles geringerer Bedeutung (Art. 38 Abs. 2 Satz 4 PAG) über die vom Innenministerium vorgegebenen Regelfälle hinaus eine „strenge“ Einzelfallprüfung voraussetzt. Die nachfolgenden Beispiele lassen befürchten, dass dabei ein zu strenger Maßstab angelegt wird.

Eine Petentin hatte sich an mich gewandt, nachdem es im Zusammenhang mit der Einhaltung der Hausordnung zu Streitigkeiten zwischen ihr, ihrem Vermieter und einer im selben Haus wohnenden Mieterin gekommen war. Folge waren gegenseitige Anzeigen wegen falscher Verdächtigung und Beleidigung. Darüber hinaus war die Petentin wegen des Verdachts der Nötigung gespeichert, da sie einer anderen Mieterin den Zugang zu deren Wohnung verwehrt haben soll. Die zuständigen Staatsanwaltschaften stellten die Verfahren mangels öffentlichen Interesses nach §§ 374, 376 StPO bzw. nach § 153 Abs. 1 StPO mit der Begründung ein, dass es sich in erster Linie um zivilrechtliche Streitigkeiten handelt. Trotzdem war die Petentin mit den genannten Delikten im KAN mit einer 10-jährigen Aussonderungsprüffrist gespeichert. Meiner Forderung, auch bei der falschen Verdächtigung und der Nötigung einen Fall geringerer Bedeutung mit der Folge einer 5-jährigen Aussonderungsprüffrist anzunehmen, ist das betreffende Polizeipräsidium nachgekommen.

In einem anderen Fall war ein 18-Jähriger von der Polizei angehalten worden, weil er ein Absperrgitter mit sich führte. Er gab an, dass er das Gitter vor dem Eingang einer Diskothek mitgenommen habe, um es seinen Freunden zu zeigen. Eine Diebstahlsabsicht bestritt er mit dem Argument, er könne mit einem Sperrgitter schließlich nichts anfangen. Über ihn lagen zu diesem Zeitpunkt keine weiteren polizeilichen Erkenntnisse vor. Von der Verfolgung wurde nach § 45 Abs. 2 i.V.m. § 109 Abs. 2 JGG abgesehen. Der Betroffene wurde trotzdem im KAN wegen Diebstahls geringwertiger Sachen mit einer Aussonderungsprüffrist von 10 Jahren gespeichert. Die Frist wurde auf meine Aufforderung hin auf 5 Jahre verkürzt.

Das Innenministerium hat aber leider eine Reihe meiner datenschutzrechtlichen Forderungen im Rahmen der Neufassung der o.g. Richtlinien nicht umgesetzt. Dies sind insbesondere:

- die Ausweitung der Regelfälle von geringerer Bedeutung,

- die Löschung von Speicherungen aus dem KAN, wenn der strafprozessuale Anfangsverdacht vernünftigerweise nicht mehr aufrecht erhalten werden kann (nicht erst, wenn sich „eindeutig ergibt“, dass „jeglicher Tatverdacht ausgeräumt worden ist“),

- die Berücksichtigung justizieller Entscheidungen über die Verfahrensbeendigung (z.B. Einstellung wegen geringer Schuld oder mangels öffentlichen Interesses) bei der Speicherungsdauer,

- die Speicherung des Verfahrensausgangs im KAN.

Die zu hohen Anforderungen an den Wegfall des Tatverdachts, aber auch die unzureichende Berücksichtigung justizieller Entscheidungen dürften in den folgenden Beispielsfällen mit zur Verhinderung einer Löschung bzw. Korrektur der Speicherungen beigetragen haben:

In einem Fall war ein Betroffener zusammen mit seiner Familie beim Einkaufen. Er wollte dabei Musik-CDs kaufen und hatte nach seinen Angaben an der Kasse stehend bemerkt, dass vor ihm eine Kundin mit einer identischen CD einen erheblich geringeren Preis bezahlt hatte. Er sei deshalb zurückgegangen und habe entsprechend günstiger ausgezeichnete CDs genommen und an der Kasse bezahlt. Als er diese am Informationsstand abholen wollte, habe man ihm die Herausgabe verweigert. Der benachrichtigte Marktleiter und der Kaufhausdetektiv hätten ihm angeboten, die CDs einzubehalten und das von ihm bezahlte Geld zurück zu geben. Nachdem er dies abgelehnt und auf den Erhalt der Ware bestanden habe, habe der Marktleiter Anzeige wegen Betruges erstattet, auch weil er am CD-Stand keine einzige verbilligt etikettierte CD gefunden und deshalb dem Betroffenen ein Austauschen der Etiketten unterstellt habe. Über den Betroffenen lagen zu diesem Zeitpunkt keine polizeilichen Erkenntnisse vor. Der Angeklagte wurde vom Amtsgericht freigesprochen, da es erhebliche Zweifel hatte, dass er tatsächlich die Manipulation an den Preisetiketten vorgenommen hatte. Trotzdem blieb der zum Tatzeitpunkt 25-Jährige wegen Warenbetruges im KAN mit einer Aussonderungsprüffrist von 10 Jahren gespeichert. Erfreulicherweise sagte das betreffende Polizeipräsidium bereits im Rahmen der Vorbereitung der datenschutzrechtlichen Prüfung die Löschung dieser Speicherung zu.

Die Bedeutung justizieller Entscheidungen für die polizeiliche Speicherung zeigt folgender Fall: Der Inhaber eines Personenschutz- und Sicherheitsunternehmens war von einem Kunden beauftragt worden, dessen Kinder, die von ihrer leiblichen Mutter nach Frankreich verbracht worden waren, von dort zurück nach Deutschland zu holen. Dem Auftrag lag der Beschluss eines Amtsgerichts zu Grunde, der die Widerrechtlichkeit der Verbringung der Kinder durch

die Kindsmutter ins Ausland festgestellt und mit einem weiteren Beschluss der Kindsmutter aufgegeben hatte, die beiden Kinder an den Vater herauszugeben. Nach vorheriger Absprache begab sich der Betroffene mit seinen in diesem Verfahren Mitbeschuldigten nach Frankreich. Gemeinsam blockierten sie dann mit zwei Fahrzeugen in einer Nebenstraße den Wagen der Mutter, in dem auch die Kinder saßen. Der Petent übergab der Mutter ein Schreiben ihres Mannes mit den Entscheidungen des Amtsgerichts. Als diese aus dem Auto ausstieg, setzte sich der Betroffene hinter das Steuer dieses Fahrzeugs und fuhr mit den Kindern davon und brachte sie nach Deutschland zurück zu ihrem Vater. Aufgrund des Vorfalls wurde von den französischen Behörden ein internationales Rechtshilfeersuchen gestellt, was dazu führte, dass gegen den Petenten zunächst ein Ermittlungsverfahren wegen des Verdachts des Raubes und der Entziehung Minderjähriger geführt wurde.

Die zuständige Staatsanwaltschaft stellte das Verfahren wegen gemeinschaftlicher Kindesentziehung nach § 170 Abs. 2 StPO ein. In ihrer Begründung führte die Staatsanwaltschaft u.a. an, dass die Rückholung der Kinder keine Entziehungshandlung gewesen sei und dem Petenten allenfalls fahrlässige - und somit nicht strafbare - Begehungsweise vorgeworfen werden könne. Das Verfahren sei deshalb aus tatsächlichen Gründen einzustellen gewesen. Auch der Tatvorwurf des gemeinschaftlichen Raubes könne aus tatsächlichen Gründen (keine rechtwidrige Zueignungsabsicht bezüglich des Pkw) nicht aufrechterhalten werden. Schließlich wurde das Verfahren wegen des verbliebenen Verdachts der Nötigung mit Zustimmung der Staatsanwaltschaft und des Angeklagten nach § 153 a Abs. 2 StPO eingestellt.

Die Polizei hat auf meine Forderung hin die Speicherung wegen des Verdachts des Raubes und der Entziehung Minderjähriger in „Nötigung“ abgeändert.

Das Innenministerium hat die Geltungsdauer der PpS-Richtlinien zunächst auf 3 Jahre festgesetzt. Ich werde in dieser Zeit die Auswirkungen der Richtlinien beobachten und ggf. erneut datenschutzrechtliche Verbesserungen einfordern.

4.2 Polizeiliche Sachbearbeitung/Vorgangsverwaltung-Verbrechensbekämpfung (PSV)

Bezüglich der Vorgangsverwaltung der Polizei hat das Innenministerium bei der Neufassung der oben unter Nr. 4.1 genannten Richtlinien nur einen Teil meiner Forderungen berücksichtigt. So konnte ich überlange Aufbewahrungsfristen für Vorgangssammlungen verhindern und insbesondere auch eine Verkürzung der Speicherfristen von Vorgängen im automatisierten Verkehrsordnungswidrigkeitenverfahren auf ein Jahr erreichen. Leider hat sich das Innenministerium geweigert, neben der Dokumentation einer polizeilichen Maßnahme, ggf. auch deren durch justizielle Entscheidung festgestellte Rechtswidrigkeit zu dokumentieren. Auch die Forderungen nach einer Speicherung des Verfahrensausgangs in der PSV sowie nach einer Definition des Inhalts der Freitextfelder hat das Staatsministerium des Innern nicht umgesetzt.

Das Zugriffs- und Berechtigungskonzept, das den landesweiten Zugriff auf die PSV auf einen begrenzten Personenkreis funktionsbezogen einschränken sollte, wurde vom Innenministerium in Kraft gesetzt, obwohl ich mich dagegen ausgesprochen hatte. Grund für meine Ablehnung war die große Zahl der zugriffsberechtigten Funktionen, bei der zu viele Polizeibedienstete einen landesweiten Zugriff erhalten. Ich habe das zum Anlass genommen, die konkrete Vergabe der Zugriffsberechtigungen und den praktischen Gebrauch des bayernweiten Zugriffs datenschutzrechtlich zu überprüfen. Aufgrund der Anzahl der Berechtigten konnte ich feststellen, dass nahezu jedem dritten Polizeibediensteten ein landesweiter Zugriff eröffnet wurde. Daraufhin habe ich die Polizeipräsidien gebeten, für alle berechtigten Funktionen - nicht personenbezogen - die Erforderlichkeit des bayernweiten Zugriffs zu begründen. Die mir daraufhin vorgelegten Begründungen konnten meine grundsätzlichen Bedenken gegen den bayernweiten Zugriff auf die PSV nicht ausräumen (siehe hierzu Nr. 7.2, 21. Tätigkeitsbericht). Zur Überprüfung der Erforderlichkeit der einzelnen personenbezogenen landesweiten Datenabfragen habe ich das Landeskriminalamt um Auswertung der Protokolldatei entsprechender Abfragen der bayerischen Polizei gebeten. Auf der Grundlage der Auswertungsliste (15 % bayernweite Abfragen) habe ich dann die Polizeipräsidien, das Landeskriminalamt und das Polizeiverwaltungsamt um Mitteilung der Funktion des Abfragenden, des Anlasses und der Rechtsgrundlage der Datenabfrage, sowie um Begründung der Erforderlichkeit der bayernweiten Abfrage gebeten. Bei 7 der von mir überprüften 92 Abfragen wurde von den betreffenden Dienststellen eingeräumt, dass eine bayernweite Abfrage nicht erforderlich gewesen wäre, weil in den meisten Fällen die gesuchten Vorgänge den eigenen Präsidiumsbereich betrafen. Die Dienststellen haben ihre Bediensteten nochmals auf die Beachtung der Voraussetzungen für landesweite Abfragen hingewiesen.

Im Zusammenhang mit einer Bürgereingabe habe ich festgestellt, dass Betroffene im „Integrationsverfahren der Polizei“ (IGVP) im Gegensatz zum Ballungsraumverfahren (BrV), das nur bei den Polizeipräsidien München und Mittelfranken eingesetzt wird, als Beschuldigte, Betroffene einer Ordnungswidrigkeit oder einer polizeilichen Maßnahme differenziert entsprechend dem jeweiligen Speicherungsgrund und

damit zutreffend gespeichert werden. Im BrV werden unterschiedslos ohne Differenzierung nach dem jeweiligen Speicherungsgrund und der damit verbundenen Belastung des Betroffenen, Beschuldigte und Betroffene unter den sog. B-Personalien in der Vorgangsverwaltung erfasst.

Eine Anpassung des BrV an IGVP und damit eine Verbesserung des Datenschutzes hat das Innenministerium abgelehnt. Es begründet dies insbesondere damit, dass sich aus der gesamten Vorgangsspeicherung der jeweilige Status der Person und der Speicherungsgrund erkennen lasse und sich die Praxis des BrV bewährt habe. Die Differenzierung in IGVP dagegen habe zu Falscherfassungen geführt. Sie solle deshalb wieder aufgegeben werden.

Eine ausreichende Erkennbarkeit des Speicherungsgrundes ist - wie meine Feststellungen ergeben haben - auch aus dem gesamten Inhalt der Vorgangsspeicherung des BrV nicht immer gegeben. Erfassungsfehler könnten durch entsprechende Schulungsmaßnahmen vermieden werden. Einen Grund, von einer datenschutzkonformen Speicherung abzusehen, sehe ich deshalb nicht.

Im Sommer 2005 wurde von verschiedenen Medien berichtet, dass Homosexuelle in der Vorgangsverwaltung der Polizei (nicht nur in Bayern) gespeichert würden. Nachdem auch von anderer Seite Hinweise auf solche Speicherungen an mich herangetragen worden waren, habe ich mich an das Staatsministerium des Innern mit der Bitte um Aufklärung gewandt. Dieses hat mir daraufhin mitgeteilt, dass eine Speicherung von Tätergruppen, Tätern oder sonstigen Personen mit dem Hinweis auf Homosexualität in der Vorgangsverwaltung, dem PVP (einem Formularerstellungsprogramm) oder dem Kriminalaktennachweis der bayerischen Polizei weder vorgenommen wurde noch beabsichtigt war. Lediglich der Katalogbegriff „Aufenthalt von Homosexuellen“ bei der Tatörtlichkeit habe vorgangsbezogen erfasst werden können. Diese auf den Tatort bezogenen Zusatzspeicherung habe keinen Rückschluss auf die sexuelle Ausrichtung (homosexuell oder heterosexuell) von Tätern, Geschädigten, Zeugen oder Mitteilern zugelassen. Das Innenministerium hatte jedoch bereits eine Löschung solcher näheren Bezeichnungen von Tatörtlichkeiten veranlasst und die weitere Erfassung unterbunden. Im späteren Verlauf hat das Innenministerium diese Aussagen dahingehend ergänzt, dass auch bei den sog. B-Personalien im Datenfeld „Täterrolle“ das Attribut „Homosexueller“ gespeichert werden konnte, ohne dass eine Suchmöglichkeit durch den polizeilichen Anwender bestanden habe. Auch in diesem Fall seien alle bereits erfassten Werte (bayernweit 7 Fälle) gelöscht und die Speicherungsmöglichkeit unterbunden worden.

Ich habe daraufhin beim Landeskriminalamt eine datenschutzrechtliche Prüfung vorgenommen. Dabei haben sich die o.g. Angaben des Innenministeriums zur Speicherung von „Tatörtlichkeit“ und „Täterrolle“ bestätigt. Darüber hinaus habe ich aber festgestellt das auch bei den sog. Z-Personalien (Zeugen, Geschädigte, Anzeigeerstatter etc.) im Datenfeld „Opfertyp“ der Zusatz „Homo“ gespeichert werden konnte, wenn auch keine Suchmöglichkeit danach bestand. Auf meine Forderung hin hat das Innenministerium die Löschung dieses Zusatzes angeordnet. Eine von mir geforderte Überprüfung der Zentralkataloge der PSV habe ergeben, dass keine Werte mehr festgestellt werden konnten, die direkt oder indirekt auf die sexuelle Orientierung zu gleichgeschlechtlichen Personen schließen lassen können.

Ein weiteres Problem im Zusammenhang mit der Vorgangsverwaltung sehe ich in der sog. Freitextrecherche über sämtliche Datenfelder (Realisierung voraussichtlich nicht vor dem Jahr 2007). Zum einen ist der Inhalt der Freitextfelder nicht definiert. Zum anderen können im Rahmen von Sachverhaltsschilderungen auch Daten unbelasteter Personen gespeichert sein (z.B.: Der Vergewaltiger verließ nach der Tat die Wohnung von Frau Mustermann). Nach solchen Daten (Frau Mustermann) kann künftig auch elektronisch recherchiert werden. Diese personenbezogene Recherche kann auch dann noch durchgeführt werden, wenn die Speicherung des Opfers unter den sog. Z-Personalien bereits gelöscht, der Vorgang aber noch nicht vernichtet ist (vgl. hierzu Nr. 7.2 meines 21. Tätigkeitsberichts).

Das Innenministerium will meine Verbesserungsvorschläge (z.B. Nichterfassen oder Anonymisieren personenbezogener Daten in Freitexten) leider nicht umsetzen.

4.3 Speicherungen in sonstigen Dateien

Anlässlich meiner Prüfungen bei verschiedenen Polizeidienststellen habe ich neben Speicherungen im Kriminalaktennachweis und in der Vorgangsverwaltung auch Speicherungen in deliktsspezifischen Dateien überprüft. Im Folgenden sind die wichtigsten Ergebnisse dieser Prüfungen zusammengefasst:

In meinem 21. Tätigkeitsbericht hatte ich meine Bedenken gegen die Speicherung aufgrund „polizeilichen Tatverdachts“ mit einer mindestens 5-jährigen Aussonderungsprüffrist dargelegt (vgl. Nr. 7.6). Ich habe deshalb im zurückliegenden Berichtszeitraum insbesondere solche „Tatverdächtige“ zum Schwerpunkt meiner datenschutzrechtlichen Prüfungen gemacht und dabei insgesamt 4 regional geführte GAST-Dateien (Dateien zur Gefahrenabwehr und Verfolgung von Straftaten und Ordnungswidrigkei-

ten) sowie die Arbeitsdatei „Rauschgift-Informationssystem“ (RGIS) überprüft.

In drei dieser GAST-Dateien waren keine „Verdächtigen“ erfasst. Die mir zu diesem Personenkreis gemeldeten Speicherungen betrafen Beschuldigte oder sog. „Sonstige Personen“, wobei letztere mit kürzeren Überprüfungsfristen (2 Jahre) gespeichert waren.

Bei der vierten GAST-Datei, die der Verhütung und Aufklärung von Straftaten in den Bereichen des Trickdiebstahls, -betrugs, Taschendiebstahls und räuberischen Diebstahls dient, habe ich die Polizei bei 7 von 10 überprüften Speicherungen zu „Tatverdächtigen“ zur Löschung bzw. zur Einstufung als „Andere Person“ mit kürzerer Überprüfungsfrist aufgefordert. Bei einer weiteren Speicherung war mir Folgendes aufgefallen: In zwei Fällen hatten Passanten mitgeteilt, dass Personen um Geld betteln. Zu strafbaren Handlungen sei es aber nicht gekommen. Nach der Personalienfeststellung wurden Fotos von den Betroffenen gefertigt, obwohl den Vorgängen keine Anhaltspunkte für einen Straftatenverdacht zu entnehmen waren. Lediglich das Betteln der Betroffenen ist für eine Speicherung als „Tatverdächtige“ nicht ausreichend. Auch die Gründe für das Anfertigen von Fotos, eine erkennungsdienstliche Maßnahme, waren für mich nicht erkennbar. Deshalb habe ich die Polizei - neben der Löschung der Speicherungen als „Tatverdächtige“ - zur Mitteilung des Anlasses und der Rechtsgrundlage für das Anfertigen der Fotos aufgefordert. Die Polizei hat die Löschung der Daten veranlasst. In einem Fall konnte der Grund für das Anfertigen der Lichtbilder nicht mehr nachvollzogen werden. Im zweiten Fall seien die Bilder zur Identitätsfeststellung nach Art. 14 Abs. 1 Nr. 1 PAG gefertigt worden, ohne dass dafür Gründe angegeben wurden. Ich habe das Polizeipräsidium deshalb aufgefordert, künftig die für das Anfertigen von Lichtbildern maßgeblichen Gründe ausreichend zu dokumentieren. In beiden Fällen hat die Polizei die Lichtbilder vernichtet.

In RGIS sind „Tatverdächtige“ grundsätzlich mit einer 5-jährigen Überprüfungsfrist und in der Regel auf Grund von Hinweisen durch Polizeidienststellen, Verdeckten Ermittlern oder Informanten gespeichert. Die Erkenntnisse über „tatverdächtige“ Personen sind nach Angabe der Polizei noch nicht so fundiert, dass ein Ermittlungsverfahren eingeleitet werden könne. Bei 6 von 15 Betroffenen hatte ich jedoch erhebliche Zweifel an der Erforderlichkeit der Speicherung und deshalb die Polizei zur Löschung aufgefordert bzw. zur Einstufung als (nichtverdächtige) „Andere Personen“ (z.B. Kontakt- oder Begleitpersonen) mit der Folge einer 2-jährigen Aufbewahrungsfrist. So war beispielsweise eine Betroffene wegen eines „Verstoßes gegen das BtMG - illegaler Handel mit Amphetamin/-derivaten -“ in RGIS erfasst, weil sie mit zwei weiteren Personen in einem Fahrzeug kontrolliert worden war. Bei einem der Kontrollierten - nicht aber bei der Betroffenen - wurden 0,6 Gramm Marihuana gefunden. Allein der Umstand, dass die Betroffene im Fahrzeug mit einer Person gesessen hatte, bei der eine geringe Menge Marihuana gefunden wurde, begründet keinen (auch keinen „polizeilichen“) Tatverdacht des „Betäubungsmittelhandels“. Es müssten dafür zumindest weitere Anhaltspunkte hinzukommen. Ich habe die Polizei deshalb zur Löschung der Speicherung, zumindest aber zur Änderung der Speicherung in „Andere Person“ mit einer 2-jährigen Überprüfungsfrist aufgefordert. Nach einem intensiven Meinungsaustausch hat die Polizei die Änderung vorgenommen.

Bei einem anderen Präsidium habe ich die Datei „Prostitution/Zuhälter“ überprüft. Die Errichtungsanordnung für diese bei den meisten Polizeipräsidien eingerichtete Datei wurde im letzten Jahr vereinheitlicht. Dabei wurde bezüglich der Aussonderungsprüffristen für „Tatverdächtige“ und Betroffene von Ordnungswidrigkeiten, die im Allgemeinen höchstens 5 Jahre gespeichert werden, eine 10-jährige Frist, wie für die stärker belasteten Beschuldigten und Verurteilten, vorgesehen. Diese undifferenzierte Festlegung von Speicherfristen ohne Berücksichtigung des jeweiligen Belastungsgrads habe ich gegenüber dem Staatsministerium des Innern kritisiert. Das Innenministerium wollte aber zunächst mit der Begründung daran festhalten, dass in der Regel langwierige Strukturermittlungen im Rotlichtmilieu eine 10-jährige Vorhaltung der Daten auch von „Tatverdächtigen“ und „Betroffenen“ erforderlich machen. Im Gegensatz dazu habe ich festgestellt, dass in der Praxis „Tatverdächtige“ mit einer Speicherfrist von 5 Jahren erfasst werden. Nach Darstellung der geprüften Dienststelle sei die Vergabe einer längeren Speicherfrist weder systemseitig möglich, noch aus fachlicher Sicht erforderlich. Ich habe mich deshalb nochmals an das Innenministerium gewandt und gebeten, kürzere (5-jährige) Speicherfristen für Betroffene von Ordnungswidrigkeiten und „Tatverdächtige“ festzulegen. Inzwischen hat mir das Innenministerium die Bereitschaft zu einer solchen Verkürzung signalisiert.

Im Rahmen der Prüfung habe ich darüber hinaus festgestellt, dass auch Prostituierte in der Datei gespeichert werden, ohne dass sie Beschuldigte, Betroffene oder „Verdächtige“ sind. Nach Darstellung der Polizei sei dies insbesondere notwendig, um Zusammenhänge über das oftmals von Waffen- und Drogendelikten als auch der organisierten Kriminalität durchsetzte Milieu zu erkennen, aber auch, um Straftaten aufzuklären, beispielsweise wenn Prostituierte Opfer von Gewaltdelikten werden. Die auf freiwilliger Grundlage erhobenen personenbezogenen Daten und Lichtbilder würden grundsätzlich 5 Jahre gespeichert. Für die Einwilligung in die polizeilichen Maßnahmen wurde ein Formblatt entwickelt, mit dem die Betroffenen der Erhebung, Aufbewahrung und Nut-

zung des Lichtbildes durch die Polizei bis zur Löschung ihrer personenbezogenen Daten zustimmen. Ich habe die Polizei gebeten, zusätzlich konkrete Aussagen zur Speicherungsdauer in das Formblatt aufzunehmen. Dieser Bitte will die Polizei entsprechen.

4.4 Fußballweltmeisterschaft 2006

4.4.1 Akkreditierungsverfahren

Vor und während der Fußballweltmeisterschaft 2006 wurden im Rahmen eines bundesweiten Akkreditierungsverfahrens der Fédération Internationale de Football Association (FIFA) Zuverlässigkeitsüberprüfungen von Personen vorgenommen, die Zutritt zu den Stadien bekommen sollten. Diese Überprüfungen, an denen auch das Bayerische Landeskriminalamt und das Bayerische Landesamt für Verfassungsschutz mitgewirkt haben, betrafen insgesamt ca. 150 000 Personen.

Grundlage für die Einbeziehung der Betroffenen in das Verfahren zur Überprüfung ihrer Zuverlässigkeit war die zuvor abgegebene schriftliche Einwilligung. Darin erklärte sich der Betroffene mit der Teilnahme am Verfahren einverstanden. Eine Datenschutzinformation unterrichtete ihn u.a. über den Ablauf, Umfang, Beurteilungskriterien und Folgen der Überprüfung. Im Interesse der ausreichenden Information des Betroffenen und damit auch der Wirksamkeit der Einwilligung haben sich die Datenschutzbeauftragten des Bundes und der Länder dafür eingesetzt, dass die Datenschutzinformation insbesondere im Hinblick auf die für die Beurteilung der Zuverlässigkeit durch Polizei- und Verfassungsschutzbehörden maßgeblichen Kriterien möglichst umfassend ist. Wichtig war auch, dass sich der Betroffene im Falle der Ablehnung seines Antrags auf Akkreditierung an einen zentralen Ansprechpartner, das Landeskriminalamt des jeweiligen Wohnsitzlandes zum Zeitpunkt der Antragstellung, wenden kann. Sollte ein Betroffener konkrete Anhaltspunkte dafür haben, dass er im Rahmen des Verfahrens durch bayerische öffentliche Stellen in seinen Datenschutzrechten verletzt worden ist, kann er sich auch gerne an mich wenden. Die Speicherungen bei ablehnenden Voten werden allerdings nach einem Jahr ab dem offiziellen Ende der Fußballweltmeisterschaft gelöscht.

4.4.2 Überprüfung von Ablehnungsfällen

Ich habe sowohl beim Landeskriminalamt als auch beim Landesamt für Verfassungsschutz (siehe hierzu Nr. 5.3) eine Überprüfung von Ablehnungsfällen im Rahmen des Akkreditierungsverfahrens durchgeführt. Beim Landeskriminalamt wurde ein technisches Trefferbild erstellt, in dem die vom eingehenden Datensätze automatisiert mit Dateien der bayerischen Polizei abgeglichen wurden. Nichttreffer wurden anschließend dem Bundeskriminalamt als zugelassen gemeldet. Nicht zu verarbeitende Datensätze wurden als fehlerhaft zurückgegeben. Die Trefferfälle wurden je nach Trefferbild und fachlicher Zuständigkeit auf 6 Clearingstellen im Landeskriminalamt verteilt. Dort wurden die Personen aufgrund der vorliegenden Erkenntnisse und der offiziellen Beurteilungskriterien bewertet und mit einer entsprechenden Empfehlung (zugelassen oder abgelehnt) versehen. In Zweifelsfällen wurden auch die sachbearbeitenden Dienststellen kontaktiert, um weitere Informationen oder Unterlagen zu erhalten. Nach einer nochmaligen Überprüfung der Bewertung in einer zentralen Clearingstelle wurden die Datensätze mit dem jeweiligen Ergebnis an das Bundeskriminalamt zurückgemeldet. Bis zum Ende der Fußballweltmeisterschaft wurden an das Landeskriminalamt 25 764 Datensätze übermittelt. Davon wurden 239 wegen Fehlerhaftigkeit zurück gewiesen. 513 Überprüfungen führten zu einer ablehnenden Empfehlung.

Bei den von mir zur Prüfung ausgewählten Ablehnungen waren mit Ausnahme von 2 Vorgängen, bei denen ich für eine abschließende Bewertung noch die Übermittlung der staatsanwaltschaftlichen Ermittlungsakte erwarte, die Ablehnungsgründe in der Regel nachvollziehbar. Lediglich in einem Fall hätte ich bei Gesamtwürdigung des Sachverhalts eine andere Einschätzung für gerechtfertigt gehalten. Unabhängig davon ergab sich aber folgende grundsätzliche Problematik:

Einige Antragsteller waren auf Grund von Verurteilungen wegen Straftaten gegen die sexuelle Selbstbestimmung (z.B. Beleidigung auf sexueller Grundlage) bzw. uneidlicher Falschaussage oder falscher Verdächtigung abgelehnt worden. In der Aufzählung der Ablehnungsgründe in der Datenschutzinformation für die zu akkreditierenden Personen fehlen aber bei Vergehen Falschaussagedelikte sowie die Straftaten gegen die sexuelle Selbstbestimmung, soweit sie sich nicht auch noch gegen das Leben, die Gesundheit oder die Freiheit einer oder mehrerer Personen richten. Die Gründe, weshalb diese Deliktsbereiche nicht angeführt sind, sind mir nicht bekannt. Möglicherweise wurde insoweit keine „Stadionrelevanz“ gesehen. Die Ablehnungen in der Sache halte ich jedenfalls bei gravierenden Vergehen gegen die sexuelle Selbstbestimmung grundsätzlich für nachvollziehbar, allerdings im Hinblick auf den fehlenden Hinweis in der Datenschutzinformation durch die Einwilligung kaum gedeckt.

Bürgereingaben oder Beschwerden im Zusammenhang mit dem Akkreditierungsverfahren sind hier bisher nicht eingegangen. Die Löschung der in die-

sem Zusammenhang erhobenen Daten werde ich zu gegebener Zeit überprüfen.

4.4.3 Speicherungen in der Datei „Gewalttäter Sport“

Im Rahmen des Akkreditierungsverfahrens für die Fußballweltmeisterschaft 2006 konnte die Ablehnung auch erfolgen, wenn der Betroffene in der (bundesweiten) Datei „Gewalttäter Sport“ gespeichert war. Zweck der Datei ist die Verhinderung gewalttätiger Auseinandersetzungen und sonstiger Straftaten im Zusammenhang mit Sportveranstaltungen, insbesondere von Fußballspielen, durch recherchefähige Erfassung relevanter Anlässe, so weit diese im Zusammenhang mit Sportveranstaltungen festgestellt wurden. Diese Anlässe sind zum einen eingeleitete oder abgeschlossene Ermittlungsverfahren sowie rechtskräftige Verurteilungen wegen bestimmter Straftaten. Darüber hinaus können auch polizeiliche Maßnahmen wie Platzverweise oder Ingewahrsamnahmen erfasst werden, wenn Tatsachen die Annahme rechtfertigen, dass die Betroffenen in der Zukunft anlassbezogene Straftaten von erheblicher Bedeutung begehen werden.

Als Anlasstat für eine Speicherung wurde im letzten Jahr im Rahmen einer bundesweiten Abstimmung auch „Beleidigung“ in die Errichtungsanordnung aufgenommen. Die dadurch bedingte Gleichbehandlung eines Fußballfans, der sich bei einer verbalen Auseinandersetzung zu einer Beleidigung hinreißen lässt, mit einem gewalttätigen Hooligan, halte ich regelmäßig für unverhältnismäßig. Ich habe mich deshalb gegen die Aufnahme dieses Delikts ausgesprochen bzw. gefordert, zumindest durch eine entsprechende Ergänzung die Erheblichkeitsschwelle für eine Speicherung wegen eines solchen Delikts anzuheben. Dies wurde vom Innenministerium leider abgelehnt. Aus diesem Grund, aber auch im Hinblick auf das Akkreditierungsverfahren für die Fußballweltmeisterschaft, habe ich bei zwei Polizeipräsidien eine datenschutzrechtliche Prüfung von Speicherungen in dieser Datei vorgenommen.

Dabei habe ich festgestellt, dass in den geprüften Fällen keine Speicherung nur wegen Beleidigung erfolgte. Es war erkennbar, dass die Speichervoraussetzungen von der Polizei grundsätzlich beachtet werden. In einigen Fällen habe ich die Voraussetzungen für eine Speicherung in der Gewalttäterdatei jedoch nicht gesehen. Hier zwei Beispiele:

Ein Betroffener war bei einem Fußball-Bundesligaspiel auf Grund seiner Alkoholisierung (2,04 Promille) zwei Mal durch die Polizei des Platzes verwiesen und gegen ihn ein Stadionverbot für den Spieltag ausgesprochen worden. Beim zweiten Versuch war ihm auch seine Jahreskarte abgenommen worden. Beim dritten Versuch ins Stadion zu gelangen wurde er in Gewahrsam genommen. Er war deswegen in der Datei und im KAN mit dem Ereignis „Sonstige polizeiliche Gefahrenabwehr“ gespeichert. Wie oben angeführt, ist in Fällen von Gewahrsamnahmen ohne Vorliegen einer Straftat erforderlich, dass Tatsachen die Annahme rechtfertigen, dass der Betroffene anlassbezogene Straftaten von erheblicher Bedeutung begehen wird. Eine solche Negativprognose kann allein auf Grund der (wohl alkoholbedingten) Hartnäckigkeit, mit der der Dauerkartenbesitzer alkoholisiert ins Stadion wollte, nicht getroffen werden. Ich habe deshalb die Polizei zur Löschung dieser Speicherung aufgefordert.

Ein weiterer Betroffener wurde vor einem Spiel beobachtet, wie er über den Stadionzaun stieg. Gegenüber der Polizei konnte er keine gültige Eintrittskarte vorweisen. In seiner Beschuldigtenvernehmung führte er an, dass er sich zwar eine Karte hätte leisten könne, aber keine mehr bekommen habe. Er war deswegen in der Gewalttäterdatei und im KAN wegen Hausfriedensbruchs und Erschleichens von Leistungen gespeichert. Auch hier fehlt es an jeglicher Gewalttätigkeit des Betroffenen. Erhebliche zukünftige Straftaten sind aus seinem Verhalten ebenfalls nicht abzuleiten. Eine Erforderlichkeit zur Speicherung in der Datei „Gewalttäter Sport“ konnte ich deshalb nicht erkennen. Auch die 10-jährige Speicherung des zum Tatzeitpunkt 19-jährigen im KAN habe ich unter Berücksichtigung des Gesamtsachverhalts für zu lange gehalten. Ich habe deshalb die Polizei aufgefordert, die Speicherung des Betroffenen in der Gewalttäterdatei zu löschen und für die Speicherung im KAN wegen der geringen Bedeutung des Falles eine 5-jährige Speicherfrist festzusetzen.

Das betreffende Polizeipräsidium wird meinen Forderungen zum Ende des Jahres nachkommen.

4.5 Speicherungen im Zusammenhang mit den Münchner Sicherheitskonferenzen 2005 und 2006

In meinem 21. Tätigkeitsbericht (vgl. Nr. 7.4) hatte ich von meinen datenschutzrechtlichen Bedenken hinsichtlich des Speicherkonzepts der Polizei im Zusammenhang mit der Sicherheitskonferenz 2002, insbesondere auch wegen der massenhaften Speicherung von Ordnungswidrigkeiten in der bayerischen Staatsschutzdatei (ISIS) berichtet. Auch im Zusammenhang mit den Sicherheitskonferenzen in den Jahren 2005 und 2006 habe ich wieder datenschutzrechtliche Überprüfungen vorgenommen. Während sich die Prüfung im Jahr 2005 vorwiegend auf die von der Polizei gefertigten Videoaufzeichnungen (vgl. Nr. 4.15.4) konzentrierte, habe ich bei der SIKO 2006 auch wieder die Dateispeicherungen kontrolliert. In der Staatsschutzdatei waren „nur“ 71 Perso-

nen gespeichert, nachdem es bei der SIKO 2002 noch über 700 Personen waren. Die Voraussetzungen der Speicherung waren beim Großteil der Betroffenen erfüllt. Zwei Speicherungen hat die Polizei gelöscht, nachdem ich die Zugehörigkeit der Betroffenen zu einer extremistischen Organisation nicht gesehen habe. Bei einzelnen Speicherungen ist die Diskussion mit der Polizei noch nicht abgeschlossen:

So wurden z.B. 18 Betroffene wegen des Verdachts der Beleidigung von Organen und Vertretern ausländischer Staaten gespeichert, da sie Plakate mir der Aufschrift „Rumsfeld Massenmörder“ trugen. Von den deswegen eingeleiteten Strafverfahren wurden bisher elf Verfahren nach § 170 Abs. 2 StPO eingestellt. Ich habe hierzu exemplarisch 3 staatsanwaltschaftliche Ermittlungsakten zur Prüfung des Fortbestands des Tatverdachts angefordert. Dabei habe ich festgestellt, dass die drei Beschuldigten friedlich an der Demonstration teilgenommen hatten und wegen des Zeigens des o.g. Plakates in Gewahrsam genommen wurden. Eine der Personen war zum Zeitpunkt der Gewahrsamnahme erst 14 Jahre alt. Ein Betroffener äußerte in seiner Beschuldigtenvernehmung u.a., dass er mit der aktuellen amerikanischen Außenpolitik nicht einverstanden sei, aber an eine Beleidigung von Herrn Rumsfeld, nicht gedacht habe. Mit dem Plakat sollte lediglich Kritik an der amerikanischen Politik zum Ausdruck kommen. Allen drei Ermittlungsakten waren Vermerke der Staatsanwaltschaft München I mit dem Hinweis beigegeben, dass seitens der amerikanischen Behörden kein Interesse an der Strafverfolgung bestehe. Die Verfahren wurden mit der Begründung eingestellt, dass - nachdem ein Strafantrag nicht gestellt werde - ein absolutes Verfahrenshindernis bestehe.

Ich halte es unter Berücksichtigung der Urteils des Bundesverfassungsgerichts vom 25.08.1994 (Az.: BvR 1432/92) im Zusammenhang mit dem Aufkleber „Soldaten sind Mörder“ für fraglich, ob die im Grundgesetz festgelegte Meinungsfreiheit der Betroffenen bei der Speicherung im KAN und in ISIS ausreichend berücksichtigt wurde. Unabhängig davon sollte in den vorliegenden Fällen auch bedacht werden, dass es sich bei den Betroffenen um friedliche Demonstrationsteilnehmer gehandelt hat, die nur ihre politische Meinung zum Ausdruck bringen wollten. Ich habe deshalb unter Gesamtwürdigung des Sachverhalts eine ausnahmslose personenbezogene Speicherung dieser Erkenntnis in ISIS unter der Rubrik „Antiamerikanismus“ nicht für zulässig gehalten und die Polizei deshalb aufgefordert

- die Speicherungen in der Datei ISIS zu den betroffenen 18 Personen zu löschen, sofern über sie sonst keine staatsschutzrelevanten Erkenntnisse vorliegen,
- die Speicherungen im KAN zu löschen und lediglich in der PSV nachzuweisen bzw. zumindest die Speicherfrist im KAN als Fälle geringerer Bedeutung auf höchstens 5 Jahre (bei Erwachsenen) zu verkürzen,
- die Speicherung des 14-jährigen Betroffenen sowohl aus ISIS als auch aus dem KAN zu löschen und lediglich in der PSV nachzuweisen.

4.6 Konzeption „Haft-Entlassenen-Auskunfts-Datei-Sexualstraftäter HEADS)"

Das Staatsministerium des Innern hat mir die Konzeption „Haft-Entlassenen-Auskunfts-Datei-Sexualstraftäter (HEADS)" zur Kenntnisnahme übermittelt. 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. Zusätzlich müssen diese Personen als Risikoprobanden eingestuft worden sein. Die Einteilung wird nach Art und Schwere der begangenen Tat, der Persönlichkeit des Täters und seinem Verhalten nach der Tat von der Staatsanwaltschaft vorgenommen.

Die Staatsanwaltschaft informiert die HEADS-Zentralstelle über die „Risikoprobanden Sexualstraftäter“. Diese führt die Daten mit den bei der Polizei bestehenden Unterlagen über die betreffende Person zusammen, nimmt eine Kategorisierung (Gefahrenpotenzial I - III) vor, stellt die relevanten Daten in HEADS ein und übersendet die Unterlagen an die für HEADS zuständige Stelle bei den Polizeipräsidien, die eine übergeordnete Koordinationsfunktion wahrnehmen. Von dort erfolgt die Information der regionalen Kriminaldienststellen, die die erforderlichen Maßnahmen vor Ort durch eigene HEADS-Ansprechpartner umsetzen. Als Kernmaßnahmen nennt die Konzeption insbesondere die Vervollständigung und Aktualisierung der erkennungsdienstlichen Unterlagen und der DNA-Unterlagen, die Überprüfung der tatsächlichen Wohnsitznahme und Feststellungen hinsichtlich des Verstoßes gegen Auflagen oder Weisungen.

Ein Runder Tisch mit Vertreterinnen und Vertretern der Justiz, der Polizei und der Landeshauptstadt München soll einen engen Informationsaustausch zwischen allen Beteiligten sicherstellen. Auf die Gefahr, dass dabei personenbezogene Daten über die gesetzlichen Befugnisse hinaus übermittelt werden

könnten, habe ich hingewiesen. Das Staatsministerium des Innern hat meinen Bedenken insoweit Rechnung getragen, als in der Konzeption ein Satz eingefügt wurde, wonach die Voraussetzungen der jeweiligen Datenübermittlungsvorschriften bei der Kooperation in Form eines Runden Tisches zu beachten sind.

Bezüglich der Jugendämter sind in der Konzeption u.a. folgende personenbezogene Informationspflichten geregelt:

„Für den Fall, dass Kinder oder Jugendliche im sozialen Nahraum oder im selben Haushalt mit einem als Risikoprobanden eingestuften Sexualstraftäter leben und konkrete Anhaltspunkte für eine akute Gefährdung der Kinder oder Jugendlichen vorliegen, hat das Jugendamt die Eltern, in geeigneter, womöglich auch aufdeckender, nötigenfalls eindringlicher und nachhaltiger Weise über ihre Pflichten, Rechte und Handlungsmöglichkeiten zu informieren, aufzuklären und zu beraten."

Dies bedeutet, dass die frühere Begehung eines Sexualdelikts durch den Betroffenen unter bestimmten Voraussetzungen auch in dessen Wohnumgebung bekannt gegeben werden kann. Eine solche Bekanntgabe ist problematisch. Das Grundrecht auf informationelle Selbstbestimmung, das allgemeine Persönlichkeitsrecht in Art. 2 Abs. 1 GG und das Recht auf Resozialisierung werden dadurch berührt. Ich habe deshalb die Aufnahme folgender einschränkender Formulierung gefordert, die insbesondere den Aspekt der Verhältnismäßigkeit klarer zum Ausdruck bringt:

„Für den Fall, dass Kinder oder Jugendliche im sozialen Nahraum oder im selben Haushalt mit einem als Risikoprobanden eingestuften Sexualstraftäter leben und konkrete Anhaltspunkte für eine akute erhebliche Gefährdung der Kinder oder Jugendlichen vorliegen, hat das Jugendamt die Eltern in geeigneter, erforderlichenfalls, im Rahmen der Verhältnismäßigkeit auch aufdeckender, nötigenfalls eindringlicher und nachhaltiger Weise über ihre Pflichten, Rechte und Handlungsmöglichkeiten zu informieren, aufzuklären und zu beraten, soweit das Ziel nicht durch andere Maßnahmen erreicht werden kann."

Bei HEADS handelt es sich um die erstmalige zentrale Speicherung von Sexualstraftätern in einer besonderen Datei mit einer Vielzahl informationeller Eingriffsmöglichkeiten. HEADS ist deshalb aus datenschutzrechtlicher Sicht nicht unproblematisch. Ich habe diese Konzeption trotzdem im Hinblick auf den damit beabsichtigten Schutz der Bevölkerung vor Sexualstraftaten und die objektiven Kriterien für die Auswahl der zu erfassenden Personen, die vorgesehenen Datenübermittlungen und die beschränkte Anzahl zugriffsberechtigter „HEADS-Sachbearbeiter" nicht von vornherein abgelehnt. Ob HEADS tatsächlich die Grundsätze der Erforderlichkeit und Verhältnismäßigkeit hinreichend berücksichtigt, wird sich erst nach Aufnahme des Wirkbetriebs und datenschutzrechtlichen Prüfungen vor Ort abschließend beurteilen lassen. Dies gilt insbesondere für die Einstufung als Risikoproband sowie den Umfang der Datenübermittlungen.

4.7 Errichtungsanordnungen für GAST-Dateien

Auch in diesem Berichtszeitraum wurden mir von Polizeidienststellen wieder zahlreiche Errichtungsanordnungen für sog. GAST-Dateien (Dateien zur Gefahrenabwehr und Verfolgung von Straftaten und Ordnungswidrigkeiten) vorgelegt. Mit Ausnahme meiner grundsätzlichen Bedenken gegen die Speicherung aufgrund polizeilichen „Tatverdachts" (vgl. 21. Tätigkeitsbericht, Nr. 7.6) bestanden gegen die überwiegende Zahl dieser Errichtungsanordnungen aus datenschutzrechtlicher Sicht keine Einwände. Bei einzelnen wurden der betroffene Personenkreis und die Speicherfristen auf meine Forderung hin von der Polizei datenschutzkonform geändert oder ergänzt. Dies war insbesondere notwendig bei Speicherfristen für Nichtbeschuldigte und -verdächtigte wie z.B. Geschädigte, Zeugen, Hinweisgebern usw., für die ich in der Regel Überprüfungsfristen von 2 Jahre für ausreichend halte, sowie bei Speicherfristen für Jugendliche und Kinder.

4.8 Rasterfahndung

Auf die Verfassungsbeschwerde eines marokkanischen Staatsangehörigen islamischen Glaubens hin hat das Bundesverfassungsgericht mit Beschluss vom 04.04.2006 (Az. 1 BvR 518/02) festgestellt, dass die angegriffenen Beschlüsse der Gerichte, die die Rasterfahndung, welche in Nordrhein-Westfalen durchgeführt wurde, für rechtmäßig erklärten, den Beschwerdeführer in seinem Grundrecht auf informationelle Selbstbestimmung aus Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG verletzen. Eine präventive polizeiliche Rasterfahndung ist mit dem Grundrecht auf informationelle Selbstbestimmung nur vereinbar, wenn zumindest eine konkrete Gefahr für hochrangige Rechtsgüter, wie den Bestand oder die Sicherheit des Bundes oder eines Landes oder für Leib, Leben oder Freiheit einer Person gegeben ist. Als bloße Vorfeldmaßnahme entspricht eine solche Rasterfahndung verfassungsrechtlichen Anforderungen nicht. Daher reichen eine allgemeine Bedrohungslage, wie sie im Hinblick auf terroristische Anschläge seit dem 11. September 2001 durchgehend bestanden hat, oder außenpolitische Spannungslagen für die Anordnung der Rasterfahndung nicht aus. Voraussetzung ist vielmehr das Vorliegen weiterer Tatsachen, aus denen sich eine konkrete Gefahr, etwa im Hinblick auf

die Vorbereitung oder absehbare Durchführung terroristischer Anschläge, ergibt.

Das Bundesverfassungsgericht moniert, dass die gesetzlichen Voraussetzungen, unter denen eine präventive polizeiliche Rasterfahndung angeordnet werden kann, in mehreren Landesgesetzen in den letzten Jahren erleichtert worden sind. Die Ermächtigung zur Rasterfahndung ist also zu einer polizeilichen „Vorfeldbefugnis“ umgestaltet worden. Danach kann die Maßnahme etwa bereits dann durchgeführt werden, wenn tatsächliche Anhaltspunkte dafür vorliegen, dass dies zur Verhütung bestimmter Straftaten von erheblicher Bedeutung erforderlich ist.

Letzteres gilt auch für die bayerische Regelung. Nach Art. 44 Abs. 1 Satz 1 PAG kann die Polizei von öffentlichen und nicht öffentlichen Stellen die Übermittlung von personenbezogenen Daten bestimmter Personengruppen aus Dateien, insbesondere Namen, Anschriften, Tag und Ort der Geburt und fahndungsspezifische Suchkriterien zum Zweck des Abgleichs mit anderen Datenbeständen verlangen, soweit dies zur Abwehr von Straftaten von erheblicher Bedeutung erforderlich ist.

Ich habe deshalb das Staatsministerium des Innern aufgefordert, Art. 44 PAG baldmöglichst zu ändern. Eine verfassungskonforme Auslegung der Vorschrift reicht dagegen nicht aus. Das Bundesverfassungsgericht hat bereits mehrfach entschieden, dass Ermächtigungen zu Grundrechtseingriffen einer gesetzlichen Grundlage bedürfen, die dem rechtstaatlichen Gebot der Normenbestimmtheit und Normenklarheit entspricht.

Bei der gesetzlichen Neufassung sind aus datenschutzrechtlicher Sicht insbesondere folgende Punkte zu berücksichtigen:

- Der Eingriff setzt mindestens das Vorliegen einer konkreten Gefahr für hochrangige Rechtsgüter voraus.

- Die Maßnahme sollte - unabhängig von der Zustimmung des Staatsministeriums des Innern - nur durch den Richter angeordnet werden. Im Hinblick auf die vom Bundesverfassungsgericht dargestellte besondere Erheblichkeit des Eingriffs und seine möglichen Konsequenzen genügt die Anordnungskompetenz des in Art. 33 Abs. 5 PAG genannten Dienststellenleiters verfassungsrechtlichen Anforderungen nicht. Die Eingriffsintensität der Maßnahme, die das Bundesverfassungsgericht mit Grundrechtseingriffen nach Art. 10 und 13 GG vergleicht, verlangt nach Kontrolle durch den Richter und deshalb nach Aufnahme eines gesetzlichen Richtervorbehalts.

- Der Verwendungszweck der durch die Maßnahme erlangten Daten ist bereichsspezifisch und präzise zu bestimmen. Die gegenwärtige Möglichkeit, sie zur Verfolgung jedweder Straftat zu verwenden, stellt keine ausreichende Zweckbegrenzung dar.

- Zur Sicherstellung der Zweckbestimmung sollten die Daten gekennzeichnet und Zweckänderungen festgestellt und dokumentiert werden.

- Im Hinblick auf den verdeckten Charakter der Rasterfahndung sollte eine Benachrichtigung jedenfalls der Betroffenen normiert werden, deren Daten nach Abschluss der Maßnahme in der Gesamtdatenmenge enthalten sind. Die Gewährleistung effektiven Schutzes der betroffenen Grundrechte erfordert eine solche Benachrichtigung, damit den Betroffenen Rechtsschutzmöglichkeiten offen stehen.

Unabhängig von einer verfassungskonformen Änderung des Polizeiaufgabengesetzes bin ich der Auffassung, dass die Anforderungen des Bundesverfassungsgerichts bereits jetzt bei jeder zukünftigen Rasterfahndung zu beachten sind.

Die Ausführungen des Bundesverfassungsgerichts können 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 (z.B. automatisierte Kennzeichenerkennung). Ich werde auf die Umsetzung notwendiger Änderungen des Polizeiaufgabengesetzes hinwirken.

4.9 Schleierfahndung

In seiner Entscheidung vom 07.02.2006 hat der Bayerische Verfassungsgerichtshof Grundsätze für die Rechtmäßigkeit von polizeilichen Durchsuchungsmaßnahmen im Rahmen der sog. Schleierfahndung aufgestellt und damit seine Rechtsprechung aus dem Urteil vom 28.03.2003 (Az. Vf. 7 - VII - 00) fortgeführt. Im entschiedenen Fall waren das Kraftfahrzeug sowie mehrere Taschen des Beschwerdeführers auf dem Parkplatz eines in der Nähe einer Autobahn gelegenen Schnellrestaurants von der Polizei durchsucht worden, nachdem er sich durch die Fahrzeugpapiere ausgewiesen hatte. Die Klage des Beschwerdeführers auf Feststellung der Rechtswidrigkeit dieser Durchsuchung wurde von den Verwaltungsgerichten unter Hinweis auf die einschlägigen

Vorschriften des Polizeiaufgabengesetzes, die eine verdachtsunabhängige Durchsuchung auf Durchgangsstraßen zulassen, abgewiesen. Der Bayerische Verfassungsgerichtshof hat mit der Maßgabe, dass durch die Maßnahmen der Schleierfahndung in die Grundrechte der allgemeinen Handlungsfreiheit (Art. 101 BV) und auf informationelle Selbstbestimmung (Art. 100 i.V.m. 101 BV) eingegriffen wird, insbesondere folgende Grundsätze als Voraussetzung für deren Verfassungsmäßigkeit aufgestellt:

Die Polizei darf im Rahmen der Schleierfahndung (Art. 13 Abs. 1 Nr. 5 PAG) nur zur Verhütung oder Unterbindung der unerlaubten Überschreitung der Landesgrenze oder des unerlaubten Aufenthalts und zur Bekämpfung der grenzüberschreitenden Kriminalität handeln. Die Ziele verpflichten die Polizei, den Kontrollen entsprechende Lageerkenntnisse und einschlägige polizeiliche Erfahrung zu Grunde zu legen.

Es ist außerdem eine Gesamtabwägung der Schwere des mit der konkreten Maßnahme verbundenen Eingriffs und dem Gewicht der rechtfertigenden Gründe des Gemeinwohls durchzuführen. Je nach Intensität des Grundrechtseingriffs ist eine höhere (Einschreit-) Schwelle in die Befugnisnormen des Polizeiaufgabengesetzes zur Schleierfahndung hineinzulesen. Wegen des Eindringens in die private Sphäre eines Betroffenen im Wege eines ziel- und zweckgerichteten Suchens oder Ausforschens und des damit verbundenen Eingriffs in den Schutzbereich der Art. 101 und Art. 100 i.V.m. Art. 101 BV bedarf es für die Durchsuchung von Sachen einer besonderen verfassungsrechtlichen Rechtfertigung. Eine solche Rechtfertigung ist gegeben, wenn im Hinblick auf die Ziele der so genannten Schleierfahndung, nämlich die Verhütung oder Unterbindung der unerlaubten Überschreitung der Landesgrenze oder des unerlaubten Aufenthalts und die Bekämpfung der grenzüberschreitenden Kriminalität, als Einschreitschwelle eine erhöhte abstrakten Gefahr beachtet wird.

Die vom Bayerischen Verfassungsgerichtshof für die Durchführung der Schleierfahndung geforderte Begründung der Gefahrenlage durch Lageerkenntnisse, grenzpolizeiliche Erfahrung, Täterprofile und Hinweise, vor allem aber das Erfordernis einer „erhöhten abstrakten Gefahr“ bei der Durchsuchung von Sachen, macht grundsätzlich eine Dokumentation der der Eingriffsmaßnahme zugrunde liegenden Tatsachenbasis durch die Polizei notwendig. Dies gilt jedenfalls dann, wenn aufgrund der erheblichen Eingriffsintensität besondere Anforderungen an die Erforderlichkeit der Maßnahme gestellt werden. Wenn schon für die Durchsuchung von Sachen eine ungesicherte und diffuse Tatsachengrundlage sowie allgemeine Lageerkenntnisse und grenzpolizeiliche Erfahrungssätze nicht genügen, sondern tatsächliche Anhaltspunkte vorliegen müssen, die den Schluss auf die erhöhte abstrakte Gefahrenlage zulassen, gilt dies umso mehr für die Durchsuchung von Personen (Art. 21 Abs. 1 Nr. 3 i.V.m. Art. 13 Abs. 1 Nr. 5 PAG). Eine solche Maßnahme, die noch viel tiefer in das Persönlichkeitsrecht des Betroffenen eingreift und nur im Ausnahmefall in Betracht kommt, bedarf einer entsprechend gesteigerten Gefahrensituation. Die - ggf. auch stichpunktartige - Dokumentation dieser Gefahrensituation in diesen Einzelfällen dient nicht nur der Selbstkontrolle der handelnden Polizeibeamten, sondern auch der Nachvollziehbarkeit der Einhaltung der verfassungsrechtlichen Vorgaben. Ohne eine solche Dokumentation ist weder der Polizei selbst noch mir eine Kontrolle der Rechtmäßigkeit der Maßnahme möglich. Eine Kontrolle ist aber gerade bei anlasslosen Maßnahmen mit besonderer Grundrechtsrelevanz, wie der Durchsuchung von Personen im Rahmen der Schleierfahndung, besonders wichtig.

Das Staatsministerium des Innern will - entsprechend der bisherigen Praxis - solche gravierenden Durchsuchungsmaßnahmen auch in Zukunft nicht dokumentieren lassen.

4.10 Formblätter bei DNA-Maßnahmen

Am 01.11.2005 ist das Gesetz zur Novellierung der forensischen DNA-Analyse in Kraft getreten (Bundesgesetzblatt 2005 I, Seite 2360). Danach bedarf es für die molekulargenetische Untersuchung von Körperzellen zu Vergleichszwecken (§ 81 e Abs. 1 StPO) und zur Identitätsfeststellung bei Beschuldigten und Verurteilten in künftigen Strafverfahren (§ 81 g StPO) keiner richterlichen Anordnung, wenn eine schriftliche Einwilligung des Betroffenen vorliegt. Diese schließt aber die bei der DNA-Identitätsfeststellung für künftige Strafverfahren einzuhaltenden materiellen gesetzlichen Voraussetzungen der Maßnahme, wie z.B. das Vorliegen einer Straftat von erheblicher Bedeutung oder der Prognose einer Wiederholungsgefahr, nicht mit ein. Diese müssen unabhängig davon von der Polizei geprüft und dokumentiert werden, was auch dem Betroffenen (vor Erteilung seiner Einwilligung) deutlich zu machen ist.

Ich habe die dafür vorgesehenen Formblätter geprüft und insbesondere Folgendes festgestellt:

- Zunächst ist ein ausdrücklicher Hinweis notwendig, dass die Abgabe von Körperzellen und die Einwilligung in die DNA-Analyse freiwillig ist und eine Verpflichtung dazu nicht besteht.

- Der Hinweis, dass bei der molekulargenetischen Untersuchung „lediglich“ ein so genanntes DNA-Identifizierungsmuster erstellt wird, das ausschließlich eine Identifizierung

des Betroffenen ermöglicht und insbesondere keinerlei Rückschlüsse auf die Persönlichkeit oder gar auf Erbanlagen oder Erbkrankheiten des Betroffenen zulässt, ist in dieser Absolutheit nicht haltbar. So lassen sich nach heutigen Erkenntnissen mit Hilfe der nicht-codierenden Bereiche der DNA auch das Geschlecht und mit einer gewissen Wahrscheinlichkeit auch die ethnische Abstammung bzw. Herkunft des Betroffenen und Krankheitsdispositionen (z.B. Chorea Huntington, Mukoviscidose) feststellen.

– Notwendige Informationen der Beschuldigten und Verurteilten über die Speicherungsdauer des DNA-Identifizierungsmuster in der DNA-Analyse-Datei fehlen.

– Es fehlt der Hinweis, dass der Betroffene seine Einwilligung widerrufen kann und Ausführungen über die Rechtsfolgen eines Widerrufs. Erfolgt der Widerruf vor der Probenentnahme, so kann diese grundsätzlich nur durch den Richter angeordnet werden. Erfolgt der Widerruf nach der Probenentnahme, aber vor der molekulargenetischen Untersuchung, sind weitere Maßnahmen grundsätzlich erst nach richterlicher Anordnung zulässig. Wird diese unanfechtbar versagt, ist die Probe zu vernichten, falls sie nicht zulässigerweise zugleich für andere Zwecke erhoben wurde (z.B. zur Feststellung der Blutalkoholkonzentration). Erfolgt der Widerruf nach der molekulargenetischen Untersuchung, halte ich eine richterliche Bestätigung der bisher getroffenen Maßnahmen für notwendig.

– Für die Einwilligung zur Entnahme und molekulargenetischen Untersuchung von Körperzellen zu Vergleichszwecken im Strafverfahren sollten wegen rechtlich unterschiedlicher Konsequenzen für den Betroffenen zwei getrennte Formblätter verwendet werden, je nachdem, ob die Maßnahme bei einem Beschuldigten oder einem Zeugen/Dritten durchgeführt wird. Letzteren kann im Hinblick auf einen Beschuldigten ein Zeugnisverweigerungsrecht nach § 81 c Abs. 3 Satz 1 i.V.m. § 52 StPO zustehen. Sie sind deshalb im Interesse einer ausreichenden Information und damit auch der Wirksamkeit der Einwilligung darüber aufzuklären. Besteht ein Zeugnisverweigerungsrecht, sollte im Formblatt die Erklärung vorgesehen werden, dass der Betroffene darüber aufgeklärt wurde.

– Den Betroffenen sollten - neben den Hinweisen - Kopien der Einwilligungserklärung ausgehändigt werden. Nur auf diese Weise können sich die Betroffenen auch zu einem späteren Zeitpunkt noch einmal über die getroffene Maßnahme und ihr fortbestehendes Widerrufsrechts informieren. Eine Dokumentation der Aushändigung der Kopien sollte auf dem Vordruck der Einverständniserklärung vorgesehen werden.

– Die Einwilligungserklärung und Hinweise sollten auch in anderen (gängigen) Sprachen vorliegen (z.B. Englisch), damit Verständnisschwierigkeiten mit Auswirkungen auf die Wirksamkeit der Einwilligung vermieden werden.

Meine Forderungen habe ich dem Staatsministerium des Innern mitgeteilt und gebeten, die Formblätter entsprechend zu ändern. Die geänderten Formblätter liegen mir noch nicht vor.

4.11 Formblätter bei DNA-Reihenuntersuchungen

Bis zum Inkrafttreten des Gesetzes zur Novellierung der forensischen DNA-Analyse am 1. November 2005, das mit § 81 h Strafprozessordnung eine gesetzliche Grundlage für Reihengentests geschaffen hat, sind in Bayern bereits Reihengentests auf der Grundlage der Einwilligung des Betroffenen durchgeführt worden. Bereits in meinem letzten Tätigkeitsbericht (vgl. Nr. 7.8) habe ich über die Durchführung einer solchen DNA-Reihenuntersuchung berichtet.

Die für die Einladung zur Speichelprobenentnahme und für die Hinweise zur Einwilligung vorhandenen Formblätter für die DNA-Analyse beim Beschuldigten im Strafverfahren oder zu Speicherung in der DNA-Analyse-Datei eigneten sich für das spezielle Verfahren der DNA-Reihenuntersuchung nicht. Es war deshalb notwendig, hierfür eigene Formblätter zu entwickeln. Dazu hat mir das Staatsministerium des Innern Entwürfe vorgelegt. Ich habe darauf hingewirkt, dass der Hinweis auf die Freiwilligkeit der Einwilligung sowohl in der Einladung als auch in der Einwilligungserklärung durch Fettdruck hervorgehoben wird. Meiner Forderung, den im Formular enthaltenen (unzutreffenden) Vergleich zwischen DNA-Identifizierungsmuster und Fingerabdruck zu streichen, ist das Innenministerium leider nicht nachgekommen. Ich halte diesen Vergleich nicht nur für falsch, sondern auch für verharmlosend, da das DNA-Identifizierungsmuster z.B. auch Hinweise auf Krankheiten geben kann (Nr. 4.10). Darauf weist eine Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 17. Februar 2005 hin (Anlage Nr. 1).

Hinsichtlich der von der Polizei vorzunehmenden Anonymisierung des Untersuchungsmaterials habe ich bereits früher Bedenken gegenüber dem Staatsministerium des Innern gegen die Verwendung von Vornamen und dem mit einem Buchstaben abgekürzten Familiennamen erhoben. Wenigstens werden jetzt - auf meinen Anstoß hin - die für die Übermittlung an den Sachverständigen vorgesehenen Daten (Vorname, erster Buchstabe des Nachnamens, Geburtsjahr) ausdrücklich im Formblatt genannt.

Kritisiert habe ich auch die in den Entwürfen vorgesehenen missverständlichen Formulierungen im Hinblick auf die weitere Verwendung der Proben zum Abgleich mit Spuren eines neuen Tatorts (siehe hierzu 6.1.1).

4.12 Überprüfung von zwei DNA-Reihenuntersuchungen

Im zurückliegenden Berichtszeitraum habe ich zwei Reihenuntersuchungen geprüft:

Im ersten Fall war Ursache für die Maßnahme der Mord an einer Frau, bei dem am Tatort DNA-Spuren sichergestellt werden konnten, die dem Täter zugerechnet wurden. Die Ermittlungen erstreckten sich zunächst auf das unmittelbare Beziehungs- und Arbeitsumfeld des Opfers. Nachdem der DNA-Vergleich bei diesem Personenkreis negativ verlaufen war, wurde von der Polizei ein Täterprofil erstellt. Nach der Analyse sollte eine männliche Person mit sehr guter Ortskenntnis bis zu einem Alter von 45 Jahren als Täter in Betracht kommen, die zwar keinen engen Bezug, möglicherweise aber lose soziale oder berufliche Beziehung zum Opfer hatte. Auf Grund der Tatbegehungsweise wurde angenommen, dass eine entsprechende Tatwiederholung innerhalb der nächsten drei Monate wahrscheinlich sei. Deshalb entschloss sich die Polizei nach Rücksprache mit der Staatsanwaltschaft dazu, einen DNA-Reihentest durchzuführen.

Im zweiten Fall war eine Briefbombenserie, bei der ein zunächst unbekannter Täter an verschiedene Politiker und Behördenleiter insgesamt neun Briefbomben verschickt hatte, Grund für die DNA-Reihenuntersuchung. Nach einem ersten Täterprofil sollte es sich um einen Mann mit Orts- und Personenkenntnis sowie handwerklichen Fähigkeiten handeln, der konfliktscheu sei und zurückgezogen lebe. Sofern er bereits polizeilich in Erscheinung getreten wäre, kämen nicht offene, sozialschädliche Delikte (z.B. Trunkenheit im Verkehr, Fahren ohne Fahrerlaubnis oder einfache Diebstähle) und weniger Konfrontationsdelikte wie Körperverletzung, Beleidigung usw. in Betracht. Nachdem bei weiteren Briefbomben DNA-fähiges Material sichergestellt werden konnte, es erstmalig zu Verletzungen einer Angestellten gekommen war und eine Verbesserung der Auslöse- und Zündtechnik festgestellt wurde, hat die Polizei wegen der Gefahr weiterer Anschläge nach Rücksprache mit der Staatsanwaltschaft einen DNA-Reihentest durchgeführt.

Meine Überprüfung erstreckte sich insbesondere auf den Umfang der Reihenuntersuchung, d.h. auf die Frage, wie viele Personen und nach welchen Kriterien diese in die jeweilige Reihenuntersuchung einbezogen wurden (Nr. 4.12.1). Weiterhin habe ich überprüft, wie und unter welchen Bedingungen die Betroffenen zum Reihengentest eingeladen und die Entnahme der Speichelprobe durchgeführt wurde (Nr. 4.12.2) und ob die in diesem Zusammenhang erhobenen personenbezogenen Daten und Unterlagen von der Polizei datenschutzkonform verarbeitet wurden (Nr. 4.12.3).

4.12.1 Umfang der DNA-Reihenuntersuchung

Im Mordfall wurden nach der erfolglosen Überprüfung des unmittelbaren Umfelds der Ermordeten zunächst alle Männer im Alter zwischen 14 und 60 Jahren, die in der Wohnsiedlung unmittelbar am Tatort wohnten bzw. bis zum Jahr 2000 dort gemeldet waren, für die Untersuchung vorgesehen. Der erste Reihengentest umfasste 1165 Teilnehmer. Nachdem dieser nicht erfolgreich war, wurde eine Erweiterung des Betroffenenkreises für einen zweiten Test vorgenommen. Dabei sollten in einem Radius von fünf Kilometern vom Tatort alle Gemeinden einbezogen werden. Als weitere Schritte waren Erweiterungen des Radius um jeweils einen Kilometer vorgesehen. Auch innerhalb der einzelnen Bereiche waren Prioritäten vorgesehen. Bis zum Oktober 2003 waren insgesamt 4986 Datensätze angelegt und davon 4640 Speichelproben untersucht worden, ohne dass der Täter durch den Reihengentest überführt werden konnte. Kurze Zeit später wurde der Täter schließlich aufgrund von anderweitigen Hinweisen festgenommen.

Im Fall der Briefbombenanschläge hatten sich wegen der angenommenen guten Ortskenntnis des Täters die Ermittlungen zunächst verstärkt auf einen Gemeindebereich konzentriert. Dabei wurden die Betroffenen des Reihengentests nach bestimmten sich erweiternden Kriterien ausgewählt (Phase I bis III: 459 Personen). Ab der vierten Phase wurden erstmals auch umliegende Gemeinden einbezogen, wobei aufgrund kriminalistischer Vorarbeit nur eine Personenauswahl zum Test gebeten wurde. Insgesamt waren von der Maßnahme bis zu diesem Zeitpunkt 1764 Personen betroffen, ohne dass der Täter festgestellt werden konnte. Die Polizei entschloss sich deshalb, den Reihengentest auf alle männlichen Einwohner der betreffenden Gemeinde zwischen 17 und 70 Jahren auszudehnen. Dieser Test wurde schließlich für ein

bestimmtes Wochenende geplant, wobei insgesamt 2302 Personen eingeladen wurden. Am Samstag dieses Wochenendes wurde der Reihentest abgebrochen, nachdem sich der mutmaßliche Täter offensichtlich selbst getötet hatte.

Die in beiden Fällen vorgenommene Begrenzung des Betroffenenkreises und die nur sukzessive Erweiterung nach fachlichen Kriterien begrüße ich. Allerdings war im Zusammenhang mit dem Mord die Ausweitung des Betroffenenkreises im ersten Schritt auf bis zu 60-jährige Personen für mich nicht nachvollziehbar, da die polizeiliche Analyse ein Höchstalter des Täters von 45 Jahren ergeben hatte. Die Polizei begründete dies mit der Notwendigkeit, ein in der Bevölkerung merkbares Angst- und Unsicherheitsgefühl einzudämmen. Es sei vermehrt zu offenen und anonymen Verdächtigungen von Personen gekommen, die nach objektiven Gesichtspunkten haltlos gewesen seien. Deswegen sei zur Wiederherstellung gegenseitigen Vertrauens in der Bevölkerung der Personenkreis über die Zielgruppe hinaus ausgeweitet worden, um die Möglichkeit einer Entlastung einzuräumen. Die Einbeziehung in den Kreis der Betroffenen einer DNA-Reihenuntersuchung, die sich nicht an fachlichen Gesichtspunkten und am Grundsatz der Verhältnismäßigkeit orientiert, sondern lediglich an Stimmungslagen in der Bevölkerung, halte ich jedoch für unzulässig.

4.12.2 Haus-zu-Haus-Befragungen und Aushändigung der Hinweise

In beiden Verfahren sind viele Betroffenen im Rahmen von Haus-zu-Haus-Befragungen vor Ort um Abgabe einer Speichelprobe gebeten worden. Dabei sind ihnen auch die schriftlichen Hinweise zur Einwilligungserklärung ausgehändigt worden. Die Einwilligungserklärung wurde meist sofort unterschrieben und anschließend die Probenentnahme durchgeführt.

Für die Wirksamkeit der Einwilligung ist auch von Bedeutung, dass sich der Betroffene unbeeinflusst eine Meinung bilden kann und ihm dazu eine ausreichende Überlegungszeit zur Verfügung steht. Ich halte unter diesem Gesichtspunkt zeitlich kurz aufeinander folgende Verfahrenschritte wie Information, Aushändigung der Formblätter und Abnahme der Speichelprobe grundsätzlich für problematisch. Der Betroffene wird in seiner häuslichen Umgebung mit einer besonderen (eher belastenden) Situation konfrontiert und soll in dieser Situation in relativ kurzer Zeit im Beisein von Polizeibeamten und möglicherweise sogar unter Beobachtung Dritter entscheiden, ob er in die Teilnahme an einem DNA-Reihengentest einwilligt. Abgesehen von dieser Situation ist der Zeitraum zwischen Aushändigung des Hinweisblattes und der anschließenden Probenentnahme zu kurz. Dem Betroffenen sollte ausreichend Zeit gegeben werden, die Information unbeobachtet zu lesen, den Inhalt zu verstehen, ggf. sachkundigen Rat einzuholen und anschließend zu entscheiden, ob er einwilligen will oder nicht. Ihm sollten dafür regelmäßig mindestens 1 - 2 Tage Überlegungszeit eingeräumt werden. Zudem darf die Polizei im Rahmen eines solchen Verfahrens auch nicht den unzutreffenden Eindruck entstehen lassen, dass allein die Verweigerung der Einwilligung zwangsläufig zu einer gerichtlichen Anordnung der Maßnahme führen und der Betroffene lediglich zwischen Einwilligung und gerichtlicher Anordnung wählen könnte. Ich habe die Polizei gebeten, zukünftig von Haus-zu-Haus-Befragungen grundsätzlich abzusehen.

Weiter habe ich festgestellt, dass beim Versand der Einladungsschreiben in der Regel keine schriftlichen Hinweise zur Einwilligungserklärung mitgegeben wurden. Sie waren zum Teil erst zum Termin für die Abnahme der Speichelprobe auf den Entnahmetischen ausgelegt. Die Betroffenen seien nach Angaben der Polizei vorab ausreichend mündlich belehrt worden. Auch sei zwischen dem Durchlesen der Hinweise und der Abgabe der Einwilligung ausreichend Zeit eingeräumt worden. Das Innenministerium will leider nicht dafür sorgen, dass die Hinweise mit dem Einladungsschreiben versandt werden, da letzteres bereits über den Kern der Maßnahme und die Freiwilligkeit der Teilnahme belehre. Diese Auffassung ist für mich im Hinblick auf die nunmehr für den DNA-Reihengentest speziell vorliegenden ausführlichen schriftlichen Hinweise nicht nachvollziehbar. Trotz des Vorhandenseins dieser Hinweise sollen sie dem Eingeladenen für seine Entscheidung über die Teilnahme am Abnahmetermin nicht übersandt werden. Ein solches Verhalten halte ich nicht für akzeptabel. Ich werde Reihengentests - nunmehr auf der Grundlage des § 81 h StPO - auch in Zukunft überprüfen.

4.12.3 Datenerhebung, -abgleich und -löschung

In beiden Verfahren wurden zur Eingrenzung des Betroffenenkreises Rasterfahndungen durchgeführt. Von der Polizei waren dazu Anträge auf Einholung der richterlichen Anordnung der Rasterfahndung nach §§ 98 a, 98 b StPO bei der zuständigen Staatsanwaltschaft gestellt worden. Diesen Anträgen war vom Amtsgericht entsprochen worden. Die im § 98 b Abs. 4 Satz 2 StPO vorgesehene Unterrichtung des Landesbeauftragten für den Datenschutz nach Beendigung der Maßnahme ist allerdings in keinem Fall erfolgt. Diese Unterrichtungen hätten von der Staatsanwaltschaft veranlasst werden müssen. Zukünftig soll aber auch die ermittlungsführende Dienststelle der Polizei auf die Unterrichtung achten und zu gegebener Zeit einen entsprechenden Hinweis an die Staatsanwaltschaft geben.

Im Mordfall war den Betroffenen vor der Speichelprobe auch ein Abdruck des rechten Zeigefingers abgenommen und auf dem Meldebogen festgehalten worden. Nach Angaben der Polizei sollte diese erkennungsdienstliche Maßnahme die Verbindung von Person und Speichelprobe sicherstellen und Missbrauch verhindern. Es sei aber keine Abnahme zwangsweise durchgesetzt und jeder Betroffene über die Freiwilligkeit der Abgabe des Fingerabdrucks belehrt worden. Unabhängig davon, dass die Identifizierung des Betroffenen durch Vorlage des Personalausweises erfolgte und dies bei anderen Reihenuntersuchungen auch als ausreichend angesehen wurde, bedarf die Abnahme eines Fingerabdrucks als erkennungsdienstliche Maßnahme einer gesetzlichen Grundlage. Auch bei Einwilligung des Betroffenen ist die Maßnahme nur zulässig, wenn sie zur polizeilichen Aufgabenerfüllung erforderlich ist. Selbst wenn man davon ausgehen wollte, ist neben einer entsprechenden Belehrung über die Freiwilligkeit der Einwilligung zum Zeitpunkt der Einladung auch eine schriftliche Einwilligungserklärung zu fordern.

In dem gleichen Verfahren waren nach Durchführung der DNA-Analyse und Vorlage des DNA-Identifizierungsmusters zwar Speichelproben und DNA-Identifizierungsmuster gelöscht worden, eine Vielzahl anderer Daten (wie z.B. Nationalität, Zweitwohnsitz) aber noch personenbezogen gespeichert, obwohl der Spurenverursacher von der Polizei bereits vor längerer Zeit identifiziert worden war. Diese Speicherungen waren für das Strafverfahren nicht mehr erforderlich. Sie hätten deshalb bereits gelöscht sein müssen.

4.13 Kontrolle einzelner Datenerhebungsmaßnahmen

4.13.1 Erkennungsdienstliche Behandlungen

Aufgrund verschiedener Eingaben hatte ich den Eindruck gewonnen, dass bei einem Polizeipräsidium eine sehr niedrige Schwelle für die Durchführung erkennungsdienstlicher Behandlungen nach § 81 b 2. Alternative StPO (zum Zwecke der vorbeugenden Kriminalitätsbekämpfung) besteht. Ich habe dies zum Anlass für eine datenschutzrechtliche Prüfung solcher Maßnahme genommen, wobei ich darauf geachtet habe, dass die davon Betroffenen nur mit wenigen und nicht erheblichen Straftaten im KAN gespeichert waren.

Bei einer Vielzahl der geprüften Fälle war die Maßnahme im Zusammenhang mit „einfachen“ Fahrraddiebstählen bei in der Regel sehr jungen Tatverdächtigen vorgenommen worden. Nach Angaben des Polizeipräsidiums seien Fahrraddiebstähle im dortigen Bereich ein Massenphänomen. Das „besondere kriminalistische Interesse“ an diesen Delikten ergebe sich aus den hohen Fallzahlen und dem daraus resultierenden Schaden. Jährlich seien durchschnittlich rund 6900 Fahrraddiebstähle zu bearbeiten. 2004 habe dies zu einem geschätzten Gesamtschaden von 2,1 Millionen Euro geführt bei einer vermuteten hohen Dunkelziffer. Durch die erkennungsdienstliche Behandlung solle eine hohe Aufklärung, aber auch eine Abschreckung der Betroffenen bewirkt werden.

Solche präventiv-polizeilichen erkennungsdienstlichen Maßnahmen kommen gegen gewerbs- oder gewohnheitsmäßig handelnde oder sonstige Rückfalltäter in Betracht. Bei anderen Beschuldigten kommt es darauf an, ob an ihnen wegen der Art, Schwere und Begehungsweise der Straftat ein besonderes kriminalistisches Interesse besteht. Maßgebend ist, ob nach kriminalistischer Erfahrung angesichts aller Umstände des Einzelfalls Anhaltspunkte dafür vorliegen, dass der Beschuldigte in ähnlicher oder anderer Weise erneut straffällig werden könnte, und ob die erkennungsdienstlichen Unterlagen zur Förderung der dann zu führenden Ermittlungen geeignet erscheinen.

Grundsätzlich kann deshalb auch ein Fahrraddiebstahl Anlass für eine präventive erkennungsdienstliche Behandlung sein. Entscheidend ist aber, dass in jedem Einzelfall die Wiederholungsgefahr ausreichend belegt ist. Diese individuelle Prüfung, die auch die Persönlichkeit des Betroffenen und strafrechtlich relevantes Verhalten in der Vergangenheit berücksichtigen muss, kann beim Fahrraddiebstahl nicht durch das kriminalistische Interesse an einem Massenphänomen ersetzt werden. Ich habe deshalb die Polizei bei einer Reihe von Betroffenen zur Löschung der Unterlagen oder - wenn die erkennungsdienstliche Maßnahme noch vertretbar erschien - zur Fristverkürzung aufgefordert. Zwei Beispiele sollen dies verdeutlichen:

Ein 17-Jähriger war zusammen mit seinem gleichaltrigen Freund einer Kontrolle unterzogen worden, nachdem sie gemeinsam auf einem Damenfahrrad angetroffen wurden. Nach der Anhaltung sollen die beiden nach der Herkunft des Fahrrades angesprochen sehr nervös reagiert haben. Getrennt voneinander befragt soll der Betroffene angegeben haben, dass das Fahrrad der Mutter des anderen gehöre. Auf der Fahrt zur Dienststelle habe sein Freund gegenüber der Polizei geäußert, er habe dem Betroffenen erzählt, das Fahrrad gehöre seiner Mutter. Nur deshalb habe dieser das Fahrrad mitgenommen. Diese Version des Tathergangs wurde von den beiden Beschuldigten auch in ihren schriftlichen Einvernahmen wiedergegeben. Der Wert des Fahrrades wurde auf 50 DM geschätzt. Der Betroffene war zu diesem Zeitpunkt noch nicht polizeilich in Erscheinung getreten. Trotzdem wurde eine erkennungsdienstliche Behandlung durchgeführt. Die Staatsanwaltschaft stellte das Verfahren nach § 170 Abs. 2 StPO mit der

Begründung ein, dass letztlich nicht definitiv zu widerlegen sei, dass sich der Beschuldigte für nutzungsberechtigt gehalten habe.

Abgesehen davon, dass aufgrund des Fahrradwertes von 50 DM hier nur der Tatvorwurf des Diebstahls geringwertiger Sachen in Betracht kam, habe ich - angesichts des zweifelhaften Tatverdachts, vor allem aber wegen der nicht erkennbaren Wiederholungsgefahr - die erkennungsdienstliche Behandlung nicht für zulässig angesehen. Die Polizei hat auf meine Forderung hin die erkennungsdienstlichen Unterlagen vernichtet und den Vorgang aus dem KAN gelöscht.

In einem anderen Fall gehörten die Betroffenen zu einer Schülergruppe, die in der Jugendherberge untergebracht war. Die Gruppe, bestehend aus vier Personen, soll abends auf dem Rückweg zur Jugendherberge ein vor einem Geschäft stehendes Fahrrad mitgenommen und nach 40 Meter liegengelassen haben. Anschließend sollen zwei Gruppenmitglieder an einem Verkehrsschild so stark gerüttelt haben, dass sich die Stange verbogen habe. Der den Vorgang beobachtende Taxifahrer, der die Polizei benachrichtigt hatte, konnte lediglich einen der Betroffenen der tatverdächtigten Gruppe zuordnen. Die restlichen Drei konnten von ihm aufgrund der Dunkelheit nicht identifiziert werden. Die Betroffenen wurden zur Polizeidienststelle verbracht und erkennungsdienstlich behandelt. Keiner der Beschuldigten war bis zu diesem Zeitpunkt kriminalpolizeilich in Erscheinung getreten. Das Verfahren wurde von der Staatsanwaltschaft nach § 170 Abs. 2 StPO eingestellt. Die 18- bzw. 19-jährigen Betroffenen waren im KAN wegen gemeinschädlicher Sachbeschädigung und unbefugten Gebrauchs eines Fahrrades mit einer Aussonderungsprüffrist von 5 Jahren gespeichert.

Auch in diesem Fall erschien mir die erkennungsdienstliche Behandlung nicht gerechtfertigt. Bereits ein Tatverdacht von ausreichender Substanz ist jedenfalls bei drei der Betroffenen nicht erkennbar, da der einzige Zeuge lediglich einen der Beschuldigten identifizieren konnte. Darüber hinaus handelt es sich bei den Betroffenen um Schüler, die sich im Rahmen eines Schulausfluges unter Alkoholeinfluss möglicherweise übermütig verhalten haben. Die Gefahr der Begehung zukünftiger Straftaten konnte ich nicht erkennen. Die Polizei ist letztlich meiner Aufforderung, den Vorgang aus dem KAN zu löschen und die erkennungsdienstlichen Unterlagen zu vernichten, nachgekommen.

4.13.2 Einsatz des optischen Fingerabdrucksystems „Fast-Identification“

Die bayerische Polizei war im Rahmen eines Bund-Länder-Projekts unter Federführung des Bundeskriminalamts an der Entwicklung und Erprobung der Technik des optischen Fingerabdrucksystems „Fast-Identification“ beteiligt. Dabei übernahm Bayern die Pilotierung der mobilen Anwendung. Im Rahmen eines Besuchs beim Polizeipräsidium Mittelfranken haben sich meine Mitarbeiter über dieses Verfahren informiert.

Bei dem Verfahren werden vom Betroffenen in der Regel zwei Finger (meist Daumen und Zeigefinger einer Hand) gescannt. Die gescannten Fingerabdrücke werden an das Bundeskriminalamt übermittelt. Dort findet der automatische Abgleich mit der AFIS-Datenbank statt. Im Falle eines Treffers wird das Ergebnis zusätzlich durch zwei daktyloskopische Sachverständige verifiziert und danach der abfragende Stelle durch Angabe einer Nummer mitgeteilt. Mit Hilfe dieser Nummer kann der abfragende Beamte die Personalien feststellen und so den Betroffenen identifizieren. Die Fingerabdrücke werden - wenn die Anfrage keinen Treffer ergibt - bis zum Abschluss der Transaktion gespeichert. Mit dem Abmelden am Gerät sind die Daten gelöscht.

„Fast-Identification“ soll die Identifizierung von Personen in den Fällen ermöglichen und beschleunigen, in denen die Feststellung der Identität auf andere Weise nicht oder nur unter erheblichen Schwierigkeiten möglich ist. In der Praxis soll der Einsatz dieses Verfahrens z.B. bei der Schleierfahndung, bei Grenzkontrollen, bei Bahnkontrollen und zur Leichenidentifizierung erfolgen. Das Staatsministerium des Innern hat mir versichert, dass von den Betroffenen bei Kontrollen zunächst der Ausweis zwecks Identifizierung verlangt werde. Könne die Identität des Betroffenen auf diese Weise nachgewiesen werden und lägen keine Anzeichen für einen Missbrauch oder Fälschung des amtlichen Ausweises vor, unterbleibe der Einsatz von Fast-Identification.

Bei der Abnahme der Fingerabdrücke handelt es sich um eine erkennungsdienstliche Maßnahme mit dem Ziel der Identitätsfeststellung. Datenschutzrechtliche Bedenken gegen den Einsatz des optischen Fingerabdrucksystems habe ich nicht, wenn im Einzelfall die gesetzlichen Voraussetzungen für eine erkennungsdienstliche Maßnahme vorliegen.

4.13.3 Telekommunikationsüberwachungsmaßnahmen

Bei einer Dienststelle habe ich Telekommunikationsüberwachungsmaßnahmen zur Strafverfolgung nach § 100 a StPO überprüft. Solche Maßnahmen dürfen grundsätzlich nur durch den Richter angeordnet werden. Bei Gefahr im Verzug kann die Anordnung auch von der Staatsanwaltschaft getroffen werden. Sie tritt außer Kraft, wenn sie nicht binnen 3 Tagen von dem Richter bestätigt wird. Die Anordnung ist auf höchs-

tens 3 Monate zu befristen (§ 100 b Abs. 2 StPO). Nach dem Urteil des Bundesgerichtshofs vom 11.11.1998 beginnt die gesetzliche Dreimonatsfrist, innerhalb der das nicht öffentlich gesprochene Wort abgehört werden darf, mit dem Erlass der richterlichen Anordnung und nicht erst mit dem Vollzug der Abhörmaßnahme. Von der Telekommunikationsüberwachung sind die Beteiligten zu benachrichtigen, sobald dies ohne Gefährdung des Untersuchungszwecks geschehen kann (§ 101 Abs. 1 StPO).

Nachdem sich nach Art. 30 Abs. 4 Satz 2 BayDSG meine Prüfungszuständigkeit nicht auf Datenerhebungsmaßnahmen erstreckt, die gerichtlich überprüft wurden, waren Gegenstand meiner datenschutzrechtlichen Kontrolle insbesondere die Rechtmäßigkeit der Durchführung der Maßnahme im Rahmen der richterlichen Anordnung sowie die Einhaltung der Benachrichtigungspflicht. Bei den 16 zur Prüfung ausgewählten Überwachungsmaßnahmen im Rahmen von 6 Ermittlungsverfahren konnte ich feststellen, dass für alle Maßnahmen richterliche Beschlüsse vorlagen und die Überwachung grundsätzlich im Rahmen der Beschlüsse vollzogen wurde. Mängel habe ich aber bei der Benachrichtigung der Betroffenen festgestellt, die jedoch nicht von der Polizei, sondern von der zuständigen Staatsanwaltschaft als „Herrin des Verfahrens“ zu vertreten sind (siehe hier Nr. 6.3.3).

Im kommenden Berichtszeitraum werde ich mein besonderes Augenmerk auf die neu in Art. 34 a - c PAG geregelte präventive Telekommunikationsüberwachung (TKÜ) richten. Die mir von der Polizei bisher mitgeteilte Anzahl dieser Maßnahmen, deutet derzeit nicht darauf hin, dass sich die präventive TKÜ an die zahlenmäßig negative Entwicklung der repressiven TKÜ anschließt. Ich werde die Entwicklung jedoch weiter beobachten und durch die Überprüfung von Einzelfällen auf die Einhaltung der datenschutzrechtlichen Vorschriften, insbesondere des Schutzes des Kernbereichs privater Lebensgestaltung, achten.

4.14 Automatisierte Kennzeichenerkennung

In meinem letzten Tätigkeitsbericht (Nr. 7.12.4) habe ich dargestellt, welche datenschutzrechtlichen Probleme mit der Einführung einer präventiven automatisierten Kennzeichenerkennung verbunden sind. Insbesondere die Möglichkeit des Abgleichs mit anderen polizeilichen Dateien als der Fahndungsdatei bedarf für eine abschließende Beurteilung noch der Erfahrungen in der Praxis.

Das Staatsministerium des Innern hat mir auf Nachfrage mitgeteilt, dass die automatisierte Kennzeichenerkennung außerhalb von Grenzübergängen auch an Bundesautobahnen eingesetzt wird. Auch während der Fußballweltmeisterschaft 2006 kam dieses Instrument zum Einsatz. Dabei fand kein Abgleich mit anderen polizeilichen Dateien, sondern nur mit dem Fahndungsbestand statt. Allerdings wurden die Kfz-Kennzeichen von Personen, die in der Datei „Gewalttäter Sport“ gespeichert sind, für die Zeit der Fußballweltmeisterschaft in die Fahndungsdatei übernommen. Es ist schon fraglich, ob diese (befristete Übernahme) durch die entsprechenden polizeilichen Richtlinien, die den Umfang der Fahndungsdatei begrenzen, gedeckt ist. Jedenfalls stellt ein solches Vorgehen eine erhebliche Erweiterung der Fahndungsdatei dar, die bei Normierung der automatisierten Kennzeichenerkennung nicht zum Ausdruck gekommen ist. Zwar wurden die Kennzeichen der betroffenen Personen nach der Fußballweltmeisterschaft wieder aus dem Fahndungsbestand gelöscht, ich werde aber auch überprüfen, ob durch die Kennzeichenerkennung festgestellte Treffer in polizeilichen Dateien (zulässigerweise) gespeichert wurden.

4.15 Videoüberwachung öffentlicher Straßen und Plätze

4.15.1 Videoüberwachung in Innenstadtbereichen

In meinem letzten Tätigkeitsbericht (Nr. 7.13) hatte ich über die Entwicklung der polizeilichen Videoüberwachung öffentlicher Straßen und Plätze in München berichtet. Solche polizeiliche Videoüberwachung gibt es in der Innenstadt am Bahnhofsvorplatz, am Stachusrondell und am Marienplatz zur Zeit des Christkindlmarkts. Diesen Maßnahmen habe ich grundsätzlich zugestimmt. Die datenschutzrechtlichen Voraussetzungen für ihre Fortsetzung sehe ich gegeben. Zwischenzeitlich gehe ich nach wiederholten schriftlichen und persönlichen Kontakten mit dem Polizeipräsidium und entsprechenden Nachbesserungen durch die Polizei davon aus, dass auch in ausreichendem Umfang auf die Videoüberwachung am Bahnhofsvorplatz und am Stachusrondell hingewiesen wird.

Erstmals im Jahr 2005 hat das Polizeipräsidium den Christkindlmarkt videoüberwacht. Der Marienplatz, auf dem ein Großteil des vorweihnachtlichen Markts stattfindet, liegt im Zentrum der Fußgängerzone und ist ein touristischer Hauptanziehungspunkt. Dementsprechend kommt es dort vermehrt zu Straftaten, insbesondere von Taschendieben, die die Unübersichtlichkeit und das Gedränge zwischen den Verkaufbuden zu Diebstählen nutzen. Das Polizeipräsidium hat mir eine Kriminalitätsstatistik über die an bestimmten vorweihnachtlichen Veranstaltungsplätzen in München begangenen Straftaten der letzten Jahre vorgelegt. Diese weist für den Marienplatz eine vergleichsweise höhere Kriminalität aus.

Ausreichende Hinweise auf die Videoüberwachung am Marienplatz erfordern eine Beschilderung an sämtlichen Zugangswegen, einschließlich der U- und S-Bahnaufgänge. Im Rahmen eines gemeinsamen Ortstermins mit dem Polizeipräsidium wurden insgesamt 18 Hinweisschilder angebracht. Wegen des sehr kurzen zeitlichen Vorlaufs war eine Beschilderung an allen relevanten Stellen vor Beginn des Christkindlmarkts 2005 nicht mehr möglich. Zum Christkindlmarkt 2006 wurde dies erheblich verbessert.

Das Polizeipräsidium hat als Aufbewahrungsdauer für die Videoaufzeichnungen die nach Art. 32 Abs. 4 PAG maximal mögliche Speicherfrist von zwei Monaten vorgesehen. Es hat die Zeitdauer damit begründet, dass die Erfahrungen der vergangenen Jahre gezeigt hätten, dass sich aufgrund der nationalen und internationalen Besucher des Christkindlmarkts immer wieder ein zeitlich verzögertes Anzeigeverhalten von Geschädigten ergäbe bzw. strafrechtlich relevante Sachverhalte erst nachträglich bekannt würden. Zwischenzeitlich hat das Polizeipräsidium aufgrund meiner Bedenken gegen die Speicherungsdauer, diese auf einen Monat verkürzt.

4.15.2 Videoüberwachung auf dem Oktoberfest

Wie ich bereits in meinem letzten Tätigkeitsbericht (Nr. 7.13.2) berichtet habe, sind seit der Wiesn 2002 in München auf dem Wiesn-Gelände an verschiedenen Standorten Kameras installiert, mit denen während des Oktoberfests personenbezogene Bildaufnahmen angefertigt werden. Aufgrund der vom Polizeipräsidium München vorgelegten Kriminalitätsstatistiken sehe ich die gesetzlichen Voraussetzungen (Art. 32 Abs. 2 PAG) für eine polizeiliche Videoüberwachung als gegeben an und habe gegen die Durchführung dieser Videoüberwachung keine grundsätzlichen datenschutzrechtlichen Bedenken.

Allerdings habe ich wiederholt gefordert, dass auf die Videoüberwachung durch Schilder ausreichend hingewiesen wird. Während der Wiesn 2005 waren die meisten Hinweisschilder in den Schaukästen des Fremdenverkehrsamts untergebracht. Insbesondere aufgrund des Standorts der Schaukästen war diese Anbringungsart nicht geeignet, die Oktoberfestbesucher in ausreichendem Maße auf die Videoüberwachung hinzuweisen. Meine Forderung, dass deutlich sichtbare Hinweise an den Zugangswegen zum Gelände angebracht werden, konnte ich aufgrund der Kürze der Vorlaufzeit nicht mehr durchsetzen. Für die Wiesn 2006 habe ich erreicht, dass laminierte Schilder in Größe DIN A3 deutlich sichtbar bei den Zugängen angebracht wurden.

Da die Videobänder erst zwei Monate nach Erstellung der Aufnahmen gelöscht werden, habe ich - wie in meinem letzten Tätigkeitsbericht (Nr. 7.13.2) aufgelistet - für die Aufbewahrung und Auswertung der Videobänder datenschutzrechtliche Vorkehrungen, insbesondere zur Protokollierung des Zugriffs, gefordert. Die Nutzung des Filmmaterials durch Einsichtnahme in die Aufzeichnungen stellt einen Eingriff in das informationelle Selbstbestimmungsrecht der Betroffenen dar, der nur zur polizeilichen Aufgabenerfüllung zulässig ist. Es ist deshalb eine Protokollierung der Datennutzung und des Datennutzers sowie des Nutzungsumfangs und des Nutzungsgrundes notwendig. Zum Zwecke der Überprüfung der Rechtmäßigkeit der nachträglichen Zugriffe habe ich beim Polizeipräsidium München eine Auswertung der Protokolldatei sowie die Recherchelisten angefordert. Die Prüfung hat ergeben, dass - soweit aufgrund der Dokumentation nachvollziehbar - alle Zugriffe (mit Ausnahme von Abfragen aus technischen Gründen) zur Aufklärung oder Verfolgung von Straftaten erforderlich waren. In wenigen Fällen war allerdings der Umfang der Datennutzung nicht angegeben. Ich habe das Polizeipräsidium München aufgefordert, bei seinen Bediensteten darauf hinzuwirken, dass alle Zugriffe auf Videoaufzeichnungen vollständig protokolliert werden.

Im Zusammenhang mit der Wiesn 2005 ist das Staatsministerium des Innern wegen der Durchführung eines Pilotversuchs zur Videoüberwachung im Sammelzellenbereich der Oktoberfestwache an mich herangetreten. Es hat mir mitgeteilt, dass diese Videoüberwachung zum einen der Eigensicherung der eingesetzten Beamten und der bestehenden Fürsorgeverpflichtung dienen soll, indem die Behandlung der Arrestierten dokumentiert wird, damit bei evtl. Beschwerden Beweismittel zur Verfügung stehen. Außerdem sollen durch die Überwachung Konfliktsituationen zwischen den Arrestierten untereinander vermieden werden. Da es sich um einen Eingriff in das informationelle Selbstbestimmungsrecht des Betroffenen handelt, bedarf die Maßnahme einer ausreichenden Rechtsgrundlage. Ich sehe die Maßnahme grundsätzlich als vom Hausrecht gedeckt an.

Darüber hinaus muss die Maßnahme auch dem Erforderlichkeits- und Verhältnismäßigkeitsgrundsatz entsprechen. Ich habe deshalb insbesondere die Einhaltung folgender Voraussetzungen gefordert:

- Die Videoüberwachung darf nur durchgeführt werden, wenn mildere Mittel zur Erreichung des Zwecks (z.B. herkömmliche Überwachungsmethoden) nicht zur Verfügung stehen oder nicht ausreichen.

- Der Zweck der Videoüberwachung ist so eng wie möglich zu begrenzen und im Einzelnen schriftlich festzulegen. Dazu muss genau bestimmt werden, für welche Zwecke die Videoaufzeichnungen verwendet werden dürfen.

- Die Videoüberwachung ist auf den für den Zweck der Maßnahme erforderlichen Bereich zu beschränken.

- Die Betroffenen sind auf die Videoüberwachung durch Schilder hinzuweisen, die tatsächliche Überwachung muss für sie erkennbar sein.

- Der Kreis der Zugriffsberechtigten ist auf das erforderliche Maß zu beschränken.

- Aus der Protokollierung sollte sich ergeben, welche Person auf welche Sequenzen der Videoaufzeichnungen aus welchem Anlass (ggf.mit Angabe des Aktenzeichens) zugegriffen hat.

- Die Videoaufzeichnungen dürfen nur solange aufbewahrt werden, wie dies für die Erreichung des vorgesehenen Zwecks erforderlich ist.

Aus der Sicht des Staatsministerium des Innern und des Polizeipräsidiums München hat sich die Videoüberwachung der Sammelhaftzellen als geeignetes Unterstützungsinstrumentarium (neben den vorgeschriebenen Kontrollgängen) erwiesen, um mögliche Gefährdungen von verwahrten Personen sowie von Einsatzkräften abzuwehren bzw. entsprechende Vorkommnisse oder Gefahrenlagen entsprechend verwertbar zu dokumentieren. Sie soll auch in Zukunft durchgeführt werden.

Für die Dauer der Speicherung der Videoaufzeichnungen ist die gesetzliche Höchstfrist von zwei Monaten vorgesehen. Ich bin dagegen der Auffassung, dass diese Höchstfrist für die Aufbewahrung der Aufzeichnungen nicht als Regelfrist missverstanden werden darf, sondern vielmehr in jedem Einzelfall der Videoüberwachung zu prüfen ist, welche konkrete Aufbewahrungsfrist im Rahmen der Zweimonatsfrist erforderlich und verhältnismäßig ist. Insbesondere aufgrund der Verpflichtung der Beamten zur ständigen Monitorbetrachtung sehe ich keine Erforderlichkeit, die Videoaufnahmen zwei Monate lang aufzubewahren. Das Staatsministerium des Innern hat eingewandt, dass es sich beim Oktoberfest um ein Großereignis mit internationalem Publikum handelt und daher immer mit einem zeitlich erheblich verzögerten Anzeigeverhalten der Geschädigten zu rechnen ist. Aus diesem Grund werde ich nach gegebener Zeit, wenn Erfahrungswerte vorliegen, die Erforderlichkeit der Speicherfrist nochmals überprüfen.

4.15.3 Videoüberwachung während der Fußballweltmeisterschaft 2006

Das Staatsministerium des Innern hat mir auf Nachfrage im Vorfeld der Fußballweltmeisterschaft u.a. mitgeteilt, dass eine polizeiliche Videoüberwachung in der Münchner Innenstadt im Bereich des Marienhofs (sog. Public-Viewing-Bereich) und des Marienplatzes vorgesehen sei. Das Polizeipräsidium München begründete diese Maßnahme damit, dass aufgrund der polizeilichen Erkenntnisse aus jährlich wiederkehrenden Großveranstaltungen (z.B. Oktoberfest, Christkindlmarkt) davon auszugehen sei, dass die Plätze auch Taschendiebe anziehen werden, die das Gedränge von Menschenmengen für die Begehung von Straftaten ausnutzen. Die Videoüberwachung stelle ein wirksames Mittel zur Bekämpfung solcher Straftaten dar. Ich habe mich - insbesondere auch im Hinblick auf die von den Sicherheitsbehörden angenommenen Gefahren von Anschlägen in den Public-Viewing-Bereichen - nicht gegen die zeitlich befristete Videoüberwachung ausgesprochen. Ich habe aber darauf hingewirkt, dass in ausreichendem Umfang Schilder angebracht wurden, die auf die Videoüberwachung hinweisen.

4.15.4 Videoaufnahmen von Versammlungsteilnehmern

Im Rahmen der Sicherheitskonferenz vom 11. bis 13.02.2005 und bei der Gegendemonstration zur „Nazi-Mahnwache“ auf dem Marienplatz am 08.05.2005 wurden unter der Verantwortung des zuständigen Polizeipräsidiums Videoaufzeichnungen, auf denen Versammlungsteilnehmer erkennbar sind, angefertigt. Auch bei der NPD-Kundgebung am 02.04.2005 wurden - wie mir ein Abgeordneter des Landtags mit der Bitte um Überprüfung mitgeteilt hatte - von der Polizei Gegendemonstranten mittels Videokamera aufgezeichnet.

Bereits in den vergangenen Jahren habe ich das Polizeipräsidium mehrfach darauf hingewiesen, dass die Anfertigung von personenbezogenen Aufnahmen von Versammlungsteilnehmern zur Gefahrenabwehr nur zulässig ist, wenn eine gesicherte Gefahrenprognose bezüglich der gefilmten Personen vorliegt. Die Anfertigung von Bild- und Tonaufnahmen bei Versammlungen stellt nicht nur einen Eingriff in das Grundrecht der informationellen Selbstbestimmung (Art. 1 Abs. 1 und 2 Abs. 1 GG) dar, sondern auch in das für eine Demokratie wesentliche Grundrecht der Versammlungsfreiheit (Art. 8 Abs. 1 GG). Aus diesem Grund lässt die gesetzliche Regelung der §§ 12 a, 19 a VersammlG Bildaufzeichnungen nur unter engen Voraussetzungen zu. Nach §§ 12 a, 19 a VersammlG darf die Polizei Bild- und Tonaufnahmen von Versammlungsteilnehmern nur anfertigen, wenn tatsächliche Anhaltspunkte die Annahme rechtferti-

gen, dass von ihnen erhebliche Gefahren für die öffentliche Sicherheit oder Ordnung ausgehen.

Zur datenschutzrechtlichen Überprüfung der Videoaufzeichnung bei den drei o.g. Veranstaltungen habe ich insgesamt 45 Videokassetten gesichtet. Dabei habe ich bei den Videosequenzen anlässlich der Sicherheitskonferenz und der NPD-Kundgebung am 02.04.2005 wieder eine Reihe von datenschutzrechtlichen Verstößen festgestellt, die auch in einem gemeinsamen Gespräch mit Mitarbeitern des Polizeipräsidiums nicht ausgeräumt werden konnten. Versammlungsteilnehmer wurden gefilmt, obwohl keine Anhaltspunkte dafür erkennbar waren, dass gerade von ihnen „erhebliche Gefahren für die öffentliche Sicherheit und Ordnung“ ausgingen. So wurden etwa bei friedlich umherstehenden Teilnehmern deren Gesichter klar erkennbar in Nahaufnahmen gefilmt. Auch Teile eines friedlichen Zuges von Gegendemonstranten wurden auf dem Weg zur Versammlung gefilmt, wobei die vorbeilaufenden Personen und Personengruppen ebenfalls individuell deutlich erkennbar waren.

Ich habe das Polizeipräsidium erneut zur Einhaltung der gesetzlichen Voraussetzungen beim Filmen von Versammlungsteilnehmern aufgefordert und auf die Notwendigkeit einer Änderung des Filmkonzepts bei Versammlungen hingewiesen. Dazu sollte grundsätzlich vor Ort dokumentiert werden (z.B. durch Besprechen der Filmaufnahmen), welche Gründe für personenbezogene Filmaufnahmen von Versammlungsteilnehmern vorliegen. Zudem halte ich eine intensive Schulung der Verantwortlichen auf der Grundlage der gesetzlichen Bestimmungen und der dazu von mir wiederholt dargestellten Grundsätze für hilfreich, um in Zukunft Verstöße dagegen zu vermeiden. Ich habe das Polizeipräsidium aufgefordert, sämtliche Videobänder der genannten Versammlungen zu löschen, sofern sie nicht nach dem Versammlungsgesetz oder nach der Strafprozessordnung bzw. dem Gesetz über Ordnungswidrigkeiten weiter aufbewahrt werden dürfen.

4.15.5 Videoüberwachung im Straßenverkehr

Durch einen Presseartikel wurde ich auf einen Großversuch der Verkehrspolizei Nürnberg aufmerksam, bei dem auf Hauptverkehrsstraßen alle vorbeifahrenden Autofahrer mit „versteckten“ Mobilkameras gefilmt würden, um Ordnungswidrigkeiten wegen Verstößen gegen die Gurtpflicht oder Benutzung eines Mobiltelefons während der Fahrt festzustellen und zu verfolgen. Die Filme würden auf der Dienststelle ausgewertet, wobei im Falle von Ordnungswidrigkeiten der jeweilige Fahrer herangezoomt und identifiziert werde.

Wären - wie es nach dem Artikel den Anschein hatte - alle vorbeifahrenden Autofahrer unterschiedslos personenbezogen gefilmt worden, hätte es für diese Maßnahme keine Rechtsgrundlage gegeben, weder zur Gefahrenabwehr nach dem Polizeiaufgabengesetz noch zur Verfolgung von Ordnungswidrigkeiten. Die Maßnahme wurde deshalb zunächst eingestellt und mir Gelegenheit gegeben, mich über das Verfahren vor Ort zu informieren. Dabei stellte sich im Rahmen einer praktischen Verkehrskontrolle heraus, dass nur Fahrzeuge und Insassen gefilmt werden, bei denen ein Verkehrsverstoß vorliegt. Die Aufnahme wird nur ausgelöst, wenn für die Polizei erkennbar ist, dass ein Autofahrer nicht angeschnallt ist oder telefoniert. Eine Aufnahme von unbeteiligten Dritten findet nur in solchen Fällen statt, in denen der Verkehr besonders dicht ist, ein anderes Auto knapp voraus- oder hinterherfährt und dadurch eine Aufnahme nicht vermieden werden kann.

Gegen diese Form der Videoüberwachung habe ich keine datenschutzrechtlichen Bedenken. Jedoch habe ich gefordert, unvermeidbar aufgenommene unbeteiligte Dritte - sofern dies möglich ist - bei der nachfolgenden Auswertung unkenntlich zu machen.

4.16 Datenübermittlungen durch die Polizei

Auch in diesem Berichtszeitraum haben mich wieder Übermittlungen personenbezogener Daten durch die Polizei insbesondere auch an die Medien beschäftigt. Dabei habe ich erneut in einigen Fällen feststellen müssen, dass das Persönlichkeitsrecht der Betroffenen zum Teil erheblich verletzt wurde, weil es an der erforderlichen Güter- und Interessenabwägung fehlte. Gerade bei Datenübermittlung bezüglich bekannter Personen an die Presse bestand häufig kein legitimes Informationsinteresse der Öffentlichkeit, vielmehr wurde lediglich der Sensationslust Rechnung getragen:

Einem Zeitungsartikel konnte ich entnehmen, dass Beamte einer Polizeidirektion die Tatsache der Beteiligung eines bestimmten in der Öffentlichkeit bekannten Bundesliga-Fußballspielers an einem Verkehrsunfall an die Presse weitergegeben hatten. Nachdem der Spieler von vielen Personen am Unfallort erkannt worden sei und auch Anrufe deswegen eingegangen seien, habe sich die Polizei dazu entschieden, seinen Namen zu nennen. Eine Beeinträchtigung des Persönlichkeitsrechts des Betroffenen hat die betreffende Dienststelle zunächst nicht gesehen, da der Name der Presse bereits bekannt gewesen sei.

Diese Auffassung teile ich nicht. Auch die personenbezogene Bestätigung eines bestimmten Vorgangs durch die Polizei stellt eine Datenübermittlung dar. Entscheidend hierfür ist die besondere Qualität der amtlichen Bestätigung, die die Richtigkeit der Infor-

mation absichert. Gerade weil die Presse den Wahrheitsgehalt solcher Mitteilungen durch Dritte mitunter nicht eindeutig beurteilen kann, wendet sie sich vor einer Veröffentlichung an die Polizei. Hinzu kam, dass der Pressebericht aufgrund polizeilicher Mitteilung neben der konkreten Darstellung des Unfalls auch die Verletzungsfolgen des Spielers enthielt.

Im vorliegenden Fall war das Informationsinteresse der Öffentlichkeit als gering anzusehen. Die Erkenntnis, dass eine Person bei einem alltäglichen Verkehrsunfall leicht verletzt wurde, war nur im Hinblick auf die Person des Betroffenen von Interesse. Dies spricht für ein bloßes Sensationsinteresse, nicht für ein berechtigtes Informationsinteresse. Auf der anderen Seite ist das schutzwürdige Interesse des Betroffenen am Ausschluss der Übermittlung zu berücksichtigen. Die veröffentlichte Information, schuldlos an einem Verkehrsunfall beteiligt gewesen zu sein, ist für den Betroffenen zwar weniger belastend, wie beispielsweise der Vorwurf einer Ordnungswidrigkeit oder Straftat oder ein nächtlicher Unfall, der möglicherweise dem Ansehen eines Leistungssportlers geschadet hätte. Der Eingriff in das informationelle Selbstbestimmungsrecht des Betroffenen war aber auch so von Gewicht, weil er den privaten Bereich des Betroffenen berührte. Die Interessenabwägung hätte deshalb zu einem Verzicht auf die Datenübermittlung durch die Polizei führen müssen.

Ein Bürger hatte sich an mich gewandt, da er eine unzulässige Übermittlung von Informationen über seinen verstorbenen Sohn durch die Polizei an die Presse vermutete. Wie ich dem betreffenden Artikel einer Tageszeitung entnehmen konnte, war die Person des Verstorbenen zwar anonymisiert, jedoch ließ die Summe der Informationen (Wohnort/Stadtteil, Alter, Beruf, Drogenvorgeschichte) Rückschlüsse auf die Person des Verstorbenen durch das Umfeld des Verstorbenen bzw. seiner Eltern zu.

Die Polizei hielt die Mitteilung für erforderlich, um im Interesse der präventiven Drogenbekämpfung das Bewusstsein der Bevölkerung hinsichtlich der Gefahren des Drogenmissbrauchs zu schärfen. Dieser Auffassung konnte ich nicht zustimmen. Zwar kann die Polizei von sich aus personenbezogene Daten an Stellen außerhalb des öffentlichen Bereichs übermitteln, soweit dies zur polizeilichen Aufgabenerfüllung erforderlich ist. Grundsätzlich halte ich zur Bekämpfung des Drogenmissbrauchs auch eine Übermittlung polizeilicher Informationen über Drogentote an die Presse für geeignet. Jedoch ist dabei auch dem Persönlichkeitsschutz der Angehörigen des Verstorbenen in ausreichendem Maße Rechnung zu tragen. Im vorliegenden Fall wäre es zur polizeilichen Aufgabenerfüllung ausreichend gewesen, wenn der Presse allgemein und ohne Detailinformationen zur Person des Verstorbenen berichtet worden wäre. Ich habe die Polizei auf die Unzulässigkeit der Datenübermittlung hingewiesen und sie aufgefordert, zukünftig meine Beurteilung bei Datenübermittlungen an die Presse zu beachten.

In einem anderen Fall hatte sich eine Petentin an mich gewandt, um die vermutete Weitergabe ihrer Handynummer durch einen Polizeibeamten überprüfen zu lassen. Bei der Anzeigenaufnahme wegen eines Einbruchsdiebstahls in der Wohnung ihres Freundes hatte die Petentin dem sachbearbeitenden Polizeibeamten ihre Handynummer angegeben. Die weiteren polizeilichen Ermittlungen ergaben, dass die Beschädigungen durch den Vermieter der Wohnung, der das Mietverhältnis wegen angeblich säumiger Miet- und Nebenkostenzahlungen gekündigt hatte, verursacht worden waren. Der Vermieter hatte den polizeilichen Sachbearbeiter um die Übermittlung der Telefonnummer der früheren Mieter gebeten, u.a. um seine Forderungen aus dem Mietverhältnis geltend zu machen. Das zuständige Polizeipräsidium teilte mir mit, dass der Polizeibeamte für die Weitergabe der Handynummer der Petentin ein berechtigtes Interesse des Vermieters angenommen und ein entgegenstehendes schutzwürdiges Interesse der Petentin nicht gesehen habe.

Bei der Überprüfung des Sachverhalts bin ich zu dem Ergebnis gekommen, dass die Weitergabe der Handynummer der Petentin an den Vermieter nach den polizeirechtlichen Datenübermittlungsvorschriften nicht zulässig war. Nach Art. 41 Abs. 2 Nr. 1 PAG kann die Polizei auf Antrag von Personen außerhalb des öffentlichen Bereichs personenbezogene Daten übermitteln, soweit der Auskunftsbegehrende ein rechtliches Interesse an der Kenntnis der zu übermittelnden Daten glaubhaft macht und kein Grund zu der Annahme besteht, dass der Betroffene ein schutzwürdiges Interesse an dem Ausschluss der Übermittlung hat. Ein rechtliches Interesse ist dann anzunehmen, wenn der Empfänger die Daten zur Verfolgung subjektiver Rechtsansprüche benötigt. Die Einforderung von Mietzinsansprüchen stellt zwar grundsätzlich ein rechtliches Interesse in diesem Sinne dar. Mieter der Wohnung war aber offenbar nicht die Petentin selbst, sondern ihr Freund. Unabhängig davon, ob im vorliegenden Fall der Anspruch glaubhaft gemacht wurde, ist von der Polizei vor einer Datenübermittlung auch zu prüfen, ob der Auskunftsbegehrende nicht an eine andere Stelle, etwa die Meldebehörde verwiesen werden kann. Diese Prüfung ist im vorliegenden Fall nicht erfolgt. Außerdem ist vor der Weitergabe der Daten eine Interessenabwägung vorzunehmen, wobei für die Polizei kein Grund zu der Annahme bestehen darf, dass der Betroffene ein schutzwürdiges Interesse an dem Ausschluss der Übermittlung hat. Aufgrund der Gesamtumstände musste der Polizeibeamte davon ausgehen, dass die Petentin ein schutzwürdiges Interesse hatte, dass ihre Daten nicht übermittelt werden.

Ich habe das Polizeipräsidium aufgefordert, für die künftige Beachtung dieser Rechtsauffassung Sorge zu tragen. Bei künftigen vergleichbaren Verstößen werde ich eine förmliche Beanstandung prüfen.

4.17 Abfragen im polizeilichen Informationssystem

Ich habe die in den zwei vorangegangenen Berichtszeiträumen festgestellten Probleme im Hinblick auf Abfragen Polizeibediensteter im polizeilichen Informationssystem, die ihr soziales Umfeld betrafen (vgl. Nr. 6.25 im 20. Tätigkeitsbericht und 7.19 im 21. Tätigkeitsbericht), zum Anlass genommen, eine anlassunabhängige Überprüfung von polizeilichen Datenabfragen bei allen Polizeipräsidien durchzuführen. Dazu hatte ich um Auswertung der Protokolldateien sowohl zu INPOL-alt als auch zu INPOL-neu für nicht weit zurückliegende Abfragezeiträume gebeten. Aus der übermittelten Liste habe ich für jedes Polizeipräsidium eine Anzahl von Abfragen ausgewählt und um Mitteilung des Anlasses und der Rechtsgrundlage für insgesamt 53 Datenabfragen gebeten.

Für diese 53 Datenabfragen wurden folgende Anlässe angegeben:

- 21 Abfragen zur Verfolgung von Straftaten oder Ordnungswidrigkeiten (40 %),
- 15 Abfragen zur Gefahrenabwehr (28 %),
- 1 Abfrage zur sonstigen Aufgabenerfüllung (Aktenaussonderung) nach Art. 43 Abs. 1 Satz 2 PAG,
- 1 Abfrage auf der Grundlage der Einwilligung der Betroffenen,
- 15 Abfragen, bei denen sich die Polizeibediensteten nicht mehr konkret an den jeweiligen Anlass erinnern konnten (28 %).

Bei 8 Datenabfragen wurde von der Polizei ohne konkrete Angabe des Anlasses lediglich auf Schleierfahndung bzw. auf grenzpolizeiliche Kontrollen hingewiesen. Nachdem ohne konkreten Anlass lediglich der Fahndungsbestand nach Art. 43 Abs. 1 Satz 3 PAG abgerufen werden darf, habe ich unter Hinweis darauf um ergänzende Stellungnahme gebeten. Nur in einem Fall konnte ein entsprechender Anlass nachgemeldet werden. In allen anderen Fällen konnte der konkrete Anlass der Abfrage nicht mehr benannt werden. In zwei weiteren Fällen habe ich festgestellt, dass die Abfragen stellvertretend für einen anderen Polizeibediensteten durchgeführt wurden (durch einen Beamten der Einsatzzentrale bzw. den Dienstgruppenleiter), ohne dass die vorgeschriebene Protokollierung des Funkrufnamens des die Abfrage Veranlassenden erfolgt ist. Auf die Notwendigkeit einer entsprechenden Protokollierung habe ich hingewiesen.

Der Umstand, dass bei ca. jeder vierten der überprüften Abfragen kein konkreter Grund angegeben werden konnte, ist bedenklich. Er mag mit der Zahl täglicher Abfragen und dem Zeitablauf seit der Abfrage zusammenhängen. Umso dringlicher erscheint mir eine Zusatzprotokollierung des Grundes der polizeilichen Abfrage und ggf. des polizeilichen Aktenzeichens, die ich bereits im Jahr 1994 gefordert habe. Nur dadurch lässt sich die spätere Nachvollziehbarkeit und die präventive Wirkung der Protokollierung sicherstellen. Ich habe deshalb unter Bezugnahme auf das Prüfungsergebnis das Innenministerium nochmals gebeten, seine damalige ablehnende Haltung zur Einführung einer solchen Zusatzprotokollierung zu überdenken. Leider hält das Innenministerium weiter an seiner ablehnenden Haltung fest.

Bei der Überprüfung der Zulässigkeit landesweiter Datenabfragen aus der Vorgangsverwaltung (siehe Nr. 4.2) habe ich festgestellt, dass bei einer Dienststelle drei Abfragen nicht im Rahmen ihrer sachlichen Zuständigkeit gelegen hatten, sondern schwerpunktmäßig dem privaten bzw. sozialen Umfeld der abfragenden Polizeibediensteten zuzurechnen waren. Insbesondere eine dieser Datenabfragen, bei der der betreffende Beamte anlassunabhängig die polizeilichen Einsätze des vorangegangenen Wochenendes in seiner Wohnortgemeinde recherchiert hatte, war unzulässig, da sie nicht zur Aufgabenerfüllung des abfragenden Beamten erforderlich war. Auf meine Aufforderung hin hat die Dienststelle den Beamten aufgefordert, solche Datenabfragen zu unterlassen.

Ich halte es unbedingt für notwendig, dass auch die Polizei selbst anlassunabhängige Überprüfungen von Dateiabfragen durchführt. Im Hinblick auf mehrere Presseberichte in der jüngsten Vergangenheit über den Verdacht unzulässiger Dateiabfragen einer Reihe von Polizeibeamten, habe ich das Innenministerium gebeten mir mitzuteilen, ob bei den bayerischen Polizeidienststellen solche anlassunabhängigen Überprüfungen durchgeführt werden, ggf. auf Veranlassung welcher Dienststellen, in welchem Umfang, in welchen zeitlichen Abständen und mit welchen Ergebnissen. Das Staatsministerium des Innern hat dazu auf die Einführung der „anlassunabhängigen Auswahlprotokollierung“ im Jahr 1998 hingewiesen. Da es mir aber keine konkreten Angaben zum Umfang und zu den Ergebnissen der darauf gestützten Überprüfungen machen konnte, habe ich diesbezüglich beim Landeskriminalamt nachgefragt. Eine Antwort steht noch aus.

Im Zusammenhang mit einer Eingabe, bei der eine Bürgerin eine unzulässige Datenabfrage eines Poli-

zeibeamten vermutet hatte, habe ich erfahren, dass eine Protokollierung von Datenabfragen aus dem sog. Verkehrsordnungswidrigkeiten-Verfahren nicht erfolgt. Eine Überprüfung, ob eine Abfrage personenbezogener Daten der Petentin in diesem Verfahren durchgeführt wurde, war mir daher nicht möglich. Nachdem zwischenzeitlich auch für dieses Verfahren eine Protokollierung vorschrieben ist, habe ich beim Innenministerium nachgefragt, ab welchem Zeitpunkt die aus datenschutzrechtlicher Sicht notwendige Protokollierung erfolgt. Es hat mir mitgeteilt, dass bereits Vorarbeiten für eine solche Protokollierung vorgenommen wurden und eine zeitnahe Realisierung beabsichtigt ist.

4.18 Auskunftserteilung über polizeiliche Speicherungen

Auch in diesem Berichtszeitraum habe ich das Auskunftsverhalten bayerischer Polizeidienststellen überprüft. Dazu waren auch Auskunftsablehnungen Gegenstand der Überprüfung. Weit überwiegend waren diese Ablehnungen nach Art. 48 Abs. 2 PAG rechtmäßig erfolgt. In einigen wenigen Fällen war es notwendig, die Polizei zur vollständigen Auskunftserteilung aufzufordern.

Bei einzelnen Auskünften ist mir aufgefallen, dass diese - ohne Hinweis darauf - lediglich aus dem Kriminalaktennachweis und der polizeilichen Vorgangsverwaltung erfolgt waren. Dabei ließ sich aber auch in den Fällen, in denen der Antragsteller eine generelle Auskunftserteilung verlangt hatte, für diesen nicht erkennen, dass es sich nur um eine beschränkte und nicht wie beantragt um eine umfassende Auskunft aus polizeilichen Dateien handelt. Ich halte es für notwendig, dass der Antragsteller darauf hingewiesen wird, dass ohne seinen Hinweis auf einen bestimmten Sachverhalt oder eine bestimmte personenbezogene polizeiliche Sammlung lediglich Auskunft aus Kriminal- und Vorgangsakten erteilt wird. Das Innenministerium hat die Polizeidienststellen zur Aufnahme eines entsprechenden Hinweises bei der Auskunftserteilung angehalten.

5 Verfassungsschutz

Im Bereich der bayerischen Gesetzgebung habe ich auf die datenschutzkonforme Ausgestaltung der geplanten Änderung des Bayerischen Verfassungsschutzgesetzes (vgl. Nr. 5.1) hingewirkt. Sie wird insbesondere die Rechtsprechung des Bundesverfassungsgerichts zum Schutz des Kernbereichs privater Lebensgestaltung zu berücksichtigen haben.

Beim Landesamt für Verfassungsschutz habe ich im Berichtszeitraum wieder Überprüfungen von Datenerhebungen, -speicherungen und -übermittlungen sowie Auskunftserteilungen bzw. -ablehnungen vorgenommen. Die Prüfungen erfolgten anlassunabhängig (2 Prüfungen vor Ort) oder aufgrund von Bürgereingaben. Geprüft habe ich darüber hinaus Änderungen von Errichtungsanordnungen für fachliche Speicherungen und Speicherungen im Rahmen der Vorgangsverwaltung sowie Änderungen von Arbeitsanweisungen zur Speicherung personenbezogener Daten im Zusammenhang mit der Beobachtung des Extremismus und der Organisierten Kriminalität.

Zum Entwurf eines bundesrechtlichen Antiterrordateigesetzes (ATDG) habe ich datenschutzrechtliche Hinweise gegeben (vgl. Nr. 5.4).

5.1 Novellierung des Bayerischen Verfassungsschutzgesetzes

In meinem letzten Tätigkeitsbericht (Nr. 8.1) habe ich dargelegt, inwieweit das Urteil des Bundesverfassungsgerichts vom 03.03.2004 zum Großen Lauschangriff auch für die verdeckte Datenerhebung durch das Landesamt für Verfassungsschutz, insbesondere für den Einsatz besonderer technischer Mittel zur Informationsgewinnung in Wohnungen, Bedeutung hat. Im Hinblick auf die Heimlichkeit der Überwachung durch sonstige verdeckte Datenerhebungsmaßnahmen und die Gefahr der damit verbundenen Eingriffe in den Kernbereich privater Lebensgestaltung ist es erforderlich, grundsätzlich alle Formen der verdeckten Datenerhebung an den Maßstäben der o.g. verfassungsgerichtlichen Entscheidung auszurichten. Dies gilt nicht nur für die Wohnraum- und Telekommunikationsüberwachung, sondern zumindest auch für alle schwerwiegenden verdeckten Maßnahmen, wie insbesondere die längerfristige Observation, den verdeckten Einsatz technischer Mittel zur Aufzeichnung des nicht-öffentlich gesprochenen Wortes und zur Anfertigung von Bildaufnahmen oder –aufzeichnungen sowie den Einsatz von verdeckten Ermittlern.

Ausgangspunkt der Entscheidung des Bundesverfassungsgerichts ist zwar die verfassungsrechtliche Prüfung der Vorschriften der repressiven akustischen Wohnraumüberwachung in der Strafprozessordnung. Die Grundsätze des Bundesverfassungsgerichts sind aber weder auf den Schutz des Wohnraums noch auf repressive Maßnahmen beschränkt. Nach ständiger Rechtsprechung des Bundesverfassungsgerichts ist bei jeder staatlichen Beobachtung ein aus der Menschenwürdegarantie des Art. 1 Abs. 1 GG abzuleitender unantastbarer Kernbereich privater Lebensgestaltung zu wahren. Würde der Staat in ihn eindringen, verletzte dies die jedem Menschen gewährte Freiheit zur Entfaltung in den ihn betreffenden höchstpersönlichen Angelegenheiten. Dadurch wird klargestellt, dass auch bei verdeckten Informationseingriffen außerhalb von Wohnungen der Kernbereich privater

Lebensgestaltung von staatlicher Überwachung frei bleiben muss.

Die Grundsätze des Bundesverfassungsgerichts zur repressiven Wohnraumüberwachung gelten auch nicht nur für repressive verdeckte Maßnahmen, vielmehr sind sie ebenso für den Bereich der präventiven Datenerhebung durch staatliche Stellen zu beachten. Dies hat das Gericht in seinem Beschluss vom 03.03.2004 zu §§ 39 ff. Außenwirtschaftsgesetz deutlich gemacht, indem es dem Gesetzgeber aufgegeben hat, bei einer Neuregelung der präventiven Telekommunikationsüberwachung im Außenwirtschaftsgesetz auch diese Grundsätze zu beachten.

Danach bildet der Kernbereich privater Lebensgestaltung wegen seines engen Bezugs zu der grundgesetzlich geschützten Menschenwürde eine absolute Schranke, die auch nicht durch Abwägung mit Straftatenverfolgungs-, Straftatenvorbeugungs- oder Gefahrenabwehrinteressen nach Maßgabe des Verhältnismäßigkeitsgrundsatzes relativiert werden darf (vgl. auch Anlage Nr. 10).

Ich halte deshalb eine Änderung der Regelungen des Verfassungsschutzgesetzes über den Einsatz nachrichtendienstlicher Mittel zur Erhebung personenbezogener Daten, insbesondere in folgenden Bereichen für notwendig:

- Zur Entfaltung der Persönlichkeit im Kernbereich privater Lebensgestaltung gehört die Möglichkeit, innere Vorgänge, wie Empfindungen und Gefühle sowie Überlegungen, Ansichten und Erlebnisse höchstpersönlicher Art zum Ausdruck zu bringen, und zwar ohne Angst, dass staatliche Stellen dies überwachen. Dies umfasst den Kontakt mit Familienangehörigen oder sonstigen engsten Vertrauten sowie mit bestimmten Berufsgeheimnisträgern. Schutzvorschriften für diesen Kernbereich privater Lebensgestaltung fehlen bislang gänzlich.

- Aufgrund der hohen Eingriffsintensität von verdeckten Maßnahmen und zur Gewährleistung eines effektiven Rechtschutzes (Art. 19 Abs. 4 GG) ist es erforderlich, dass Betroffene, in deren Grundrechte durch die Maßnahme eingegriffen worden ist, grundsätzlich benachrichtigt werden. Nach den Ausführungen des Bundesverfassungsgerichts steht dem Betroffenen ein solcher Anspruch auf spätere Kenntnis „bei nicht erkennbaren Eingriffen“ zu. Ohne eine solche Kenntnis könnte der Betroffene weder die Rechtmäßigkeit der Informationsgewinnung überprüfen lassen, noch etwaige Rechte auf Löschung der gespeicherten Daten geltend machen. Zwar können von der grundsätzlichen Benachrichtigungspflicht Ausnahmen gemacht werden, die aber in ihren Voraussetzungen konkret und eng zu fassen sind.

Bisher liegt mir ein Änderungsentwurf nicht vor. Ein Referentenentwurf ist nach Mitteilung des Staatsministerium des Innern noch in Bearbeitung. Ich habe das Staatsministerium des Innern gebeten, mich frühzeitig zu beteiligen.

5.2 Auskunftsanspruch über die beim Landesamt für Verfassungsschutz gespeicherten Informationen

In Art. 11 Abs. 1 Satz 1 BayVSG ist geregelt, dass ein Anspruch auf Auskunft über die beim Landesamt für Verfassungsschutz in Dateien oder Akten gespeicherten Informationen nicht besteht. Vielmehr entscheidet das Landesamt für Verfassungsschutz gemäß Satz 2 nach pflichtgemäßem Ermessen über das Auskunftsbegehren, wenn eine Person ein besonderes Interesse an einer Auskunft über die zu ihrer Person gespeicherten Daten hat. Die Vorschriften in den Landesverfassungsschutzgesetzen der anderen Bundesländer sowie § 15 BVerfSchG für das Bundesamt für Verfassungsschutz sehen vor, dass eine grundsätzliche Auskunftspflicht der Verfassungsschutzbehörden besteht.

Nicht zuletzt aufgrund des Volkszählungsurteils des Bundesverfassungsgerichts vom 15.12.1983 (BVerfGE 65, 1) finden sich in den Verfassungsschutzgesetzen des Bundes und der übrigen Länder Vorschriften über das Auskunftsrecht der Bürger, die dem in Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG enthaltenen Grundrecht auf informationelle Selbstbestimmung Rechnung tragen. Dadurch wird es den Bürgern ermöglicht, ggf. gerichtlichen Rechtschutz gegen einen unrechtmäßigen Umgang mit seinen Daten in Anspruch zu nehmen. Das Bundesverfassungsgericht hat im Volkszählungsurteil festgestellt, dass Art. 19 Abs. 4 GG nicht nur das formelle Recht und die Möglichkeit, die Gerichte anzurufen, garantiert, sondern auch die Effektivität des Rechtschutzes, wonach der Bürger einen substanziellen Anspruch auf eine tatsächlich wirksame gerichtliche Kontrolle hat. Der Bürger muss daher grundsätzlich Kenntnis davon erlangen können, wer wo über welche seiner personenbezogenen Daten in welcher Weise und zu welchen Zwecken verfügt.

Diese hohe Bedeutung des Auskunftsanspruchs kommt auch im Nichtannahmebeschluss des Bundesverfassungsgerichts vom 10.10.2000 (Az. 1 BvR 586/90, 1 BvR 683/90) zum Ausdruck. Dort musste aufgrund des vorliegenden Rechtstreits zwar nicht entschieden werden, in welcher Weise ein grundsätzliches Auskunftsrecht gesetzlich ausgestaltet werden muss, jedoch kommt das Gericht zu dem Ergebnis, dass die prinzipielle Auskunftspflicht des Bundes-

amts für Verfassungsschutz gemäß § 15 BVerfSchG verfassungskonform ist.

Unabhängig von der Frage der verfassungsrechtlichen Notwendigkeit einer Änderung des Art. 11 Abs. 1 BayVSG ist es aus datenschutzrechtlicher Sicht dringend wünschenswert, wenn die Auskunftserteilung an den Betroffenen wie in den Landesgesetzen der anderen Bundesländer und im Bundesverfassungsschutzgesetz geregelt und ein grundsätzlicher Auskunftsanspruch vorgesehen würde. Ich habe deshalb das Staatsministerium des Innern gebeten, im Zuge der Novellierung des Verfassungsschutzgesetzes die Regelung entsprechend zu ändern.

5.3 Datenschutzrechtliche Prüfungen beim Verfassungsschutz

Ein Schwerpunkt meiner Prüfungen im Bereich des Verfassungsschutzes, von denen auch mehrere vor Ort durchgeführt wurden, betraf u.a. Speicherverlängerungen im Informationssystem des Landesamts für Verfassungsschutz (IBA). Ein Grund dafür, dass Betroffene trotz Ablauf der Löschfrist weiter gespeichert werden sollen, liegt u.a. vor, wenn diese Person zeitgeschichtlich oder politisch bedeutsam ist oder war. Der Grund ist in einem Vermerk aktenkundig zu machen.

Im Rahmen der Prüfung einer Speicherverlängerung wegen der Einstufung als zeitgeschichtlich bedeutsame Person waren der Dokumentation die maßgeblichen Gründe für die Verlängerung nicht zu entnehmen. Ich habe dies zum Anlass genommen, solche Speicherverlängerungen einer besonderen Prüfung zu unterziehen. Bei einigen der überprüften Fälle konnte ich keine entsprechenden Gründe für eine Speicherverlängerung feststellen. Das Landesamt für Verfassungsschutz hat diese Speicherungen gelöscht. In anderen Fällen war aus der Begründung für eine solche Speicherverlängerung nicht klar erkennbar, weshalb eine zeitgeschichtliche Bedeutsamkeit im Einzelfall angenommen wurde. Ein bloßer Hinweis auf eine Tätigkeit als Funktionär bei einer bestimmten Organisation ist dazu nicht ausreichend. Das Landesamt für Verfassungsschutz hat auf meinen Vorschlag hin eine entsprechende Änderung der Arbeitsanweisung vorgenommen, die eine deutliche datenschutzrechtliche Verbesserung der bisherigen Praxis bewirken sollte.

Überprüft habe ich auch Speicherungen zu Personen, die extremistisch beeinflussten Organisationen zugerechnet werden. Dabei handelt es sich meist um lose Gruppierungen ohne Vereinscharakter und ohne Satzung, bei denen Extremisten einen maßgeblichen Einfluss haben. Problematisiert habe ich u.a. die Speicherung von „Aktivisten“ extremistisch beeinflusster Gruppierungen. Ich bin der Auffassung, dass beispielsweise Art, Ausmaß und Anlass der Aktivität, relevante Vorerkenntnisse und Erkennbarkeit der extremistischen Beeinflussung bei einer Speicherung berücksichtigt werden müssen. So hielte ich z.B. die ausnahmslose Speicherung aller Unterzeichner von Massenflugblättern extremistisch beeinflusster Organisationen, die zur Beteiligung an Demonstrationen aufrufen, als Aktivisten in IBA nicht für zulässig. Das Landesamt für Verfassungsschutz teilt diese Auffassung.

Neben der Überprüfung von Ablehnungsfällen im Rahmen des Akkreditierungsverfahrens zur Fußballweltmeisterschaft 2006 durch die Polizei (siehe hierzu Nr. 4.4) habe ich auch die vom Landesamt für Verfassungsschutz zur Ablehnung empfohlenen Fälle überprüft. Dem Landesamt für Verfassungsschutz wurden vom Bundesamt für Verfassungsschutz im Rahmen des Akkreditierungsverfahrens 213 Personen gemeldet, bei denen ein bayerischer Datenbestand vorlag. Das Landesamt für Verfassungsschutz hat diese Personen mit dem IBA-Bestand abgeglichen und auf dieser Grundlage unter Berücksichtigung der offiziellen Beurteilungskriterien sein Votum (Zustimmung oder Ablehnung) gegenüber dem Bundesamt für Verfassungsschutz abgegeben. Insgesamt wurden 24 Personen zur Ablehnung vorgeschlagen. Für alle abgelehnten Personen wurden die Gründe für die Ablehnung dokumentiert. Diese Gründe waren in den von mir ausgewählten Fällen nachvollziehbar.

Nachdem das Landesamt für Verfassungsschutz im Zusammenhang mit Versammlungen personenbezogene Lichtbilder von Teilnehmern angefertigt hatte, habe ich eine datenschutzrechtliche Überprüfung dieser Aufnahmen vorgenommen. Das Landesamt für Verfassungsschutz führte im Rahmen der Prüfung an, dass es Zielsetzung der Anfertigung von Lichtbildern gewesen sei, Personen aus dem linksextremistischen, autonomen oder antiimperialistischen Bereich zu identifizieren und ihre Aktivitäten festzuhalten.

Eine Erhebung und Speicherung von Lichtbildern durch das Landesamt für Verfassungsschutz erscheint allenfalls dann gerechtfertigt, wenn es sich bei den Betroffenen um Personen handelt, bei denen tatsächliche Anhaltspunkte für Bestrebungen i.S. Art. 3 Abs. 1 Satz 1 Nr. 1, 3 und 4 BayVSG vorliegen oder die Aufnahme für die Bewertung oder Erforschung solcher Bestrebungen erforderlich ist. Die Voraussetzungen für die Erhebung und Speicherung habe ich für eine Reihe von Aufnahmen nicht erkennen können. Eine Aufbewahrung auf Vorrat für eine mögliche spätere Identifizierung halte ich für unzulässig. Ich habe deshalb das Landesamt für Verfassungsschutz gebeten, die betreffenden Bildaufnahmen zu löschen oder darzulegen, aus welchen Gründen die weitere Speicherung für erforderlich gehalten wird.

Bei den restlichen Bildaufnahmen handelte es sich augenscheinlich vorwiegend um Ablichtungen sog. schwarzer Blöcke. Da die Überprüfung dieser Aufnahmen durch das Landesamt für Verfassungsschutz noch nicht abgeschlossen war, beabsichtige ich etwa gegen Ende des Jahres meine datenschutzrechtliche Überprüfung dieser Bildaufnahmen fortzusetzen.

5.4 Gemeinsame Datei von Polizei und Nachrichtendiensten (Antiterrordateigesetz)

Im letzten Tätigkeitsbericht (Nr. 6.8) habe ich zu dem Niedersächsischen Gesetzentwurf zur Errichtung einer gemeinsamen Datei der deutschen Sicherheitsbehörden zur Beobachtung und Bekämpfung des islamistischen Extremismus und Terrorismus Stellung genommen. Inzwischen wurde unter der Federführung des Bundesinnenministeriums der Entwurf eines Gesetzes zur Errichtung gemeinsamer Dateien von Polizeibehörden und Nachrichtendiensten des Bundes und der Länder (Gemeinsame-Dateien-Gesetz) erarbeitet. In diesem Entwurf sind die Errichtung einer standardisierten zentralen Antiterrordatei von Polizeibehörden und Nachrichtendiensten von Bund und Ländern (Antiterrordateigesetz) und Änderungen des Bundesverfassungsschutzgesetzes, des Gesetzes über den Bundesnachrichtendienst und des Bundeskriminalamtgesetzes zur Errichtung projektbezogener gemeinsamer Dateien für die Dauer von höchstens zwei Jahren (mit Verlängerungsmöglichkeit) vorgesehen.

Am 20.09.2006 wurde der Gesetzentwurf vom Bundeskabinett beschlossen. In der zu errichtenden gemeinsamen Antiterrordatei des Bundes und der Länder sollen Erkenntnisse der Sicherheitsbehörden zu Personen und Objekten gespeichert werden. Dazu sollen neben den Grunddaten, die zur Identifizierung einer Person erforderlich sind, auch eine Vielzahl „erweiterter Grunddaten“ erfasst werden, die eine fachliche Erstbewertung im Sinne einer zuverlässigen Gefährdungseinschätzung ermöglichen. Dazu können auch zusammenfassende besondere Bemerkungen, ergänzende Hinweise und Bewertungen nach pflichtgemäßem Ermessen der speichernden Behörde erfasst werden. Solche nicht standardisierten Freitexte sind grundsätzlich abzulehnen, weil sie die Möglichkeit eröffnen, über die im Gesetz konkret bestimmten Daten hinaus weitere Daten ohne vorherige Festlegung ihres Inhalts zu speichern und abzufragen.

Die grundsätzliche Problematik der Antiterrordatei liegt aber darin, dass personenbezogene Informationen sowohl der Polizei als auch den Nachrichtendiensten und Verfassungsschutzbehörden in einer gemeinsamen Datei zur Verfügung gestellt werden. Aufgrund des Trennungsgebots ist aber neben der organisatorischen Trennung von Polizei, Nachrichtendiensten und Verfassungsschutzbehörden auch auf eine informationelle Trennung zu achten. Dieses Gebot wird durch das vorliegende Konzept tangiert, da es zur Abwehr terroristischer Gefahren zwar nur einen punktuellen Informationsverbund zulässt, der aber durch die „erweiterten Grunddaten“, insbesondere die Möglichkeit der Aufnahme von nicht standardisierten Freitexten in die Datei, über den bloßen Austausch von Hinweisen auf vorhandene Informationen weit hinausgeht. Darüber hinaus muss man sehen, dass auf der Grundlage dieses Gesetzentwurfs personenbezogene Informationen für alle Teilnehmer des Informationsverbundes verfügbar werden, die für unterschiedliche Aufgaben aufgrund unterschiedlicher Befugnisse erhoben und gespeichert wurden, die der einzelnen Behörde vom Gesetzgeber gerade im Hinblick auf ihre spezifischen Aufgaben zugestanden wurden. So bewegt sich z.B. die Erkenntnisgewinnung der Nachrichtendienste naturgemäß weiter im Vorfeld von Gefahren oder Straftaten als die der Polizei. Trotzdem könnte die Polizei mit Hilfe der Datei im Einzelfall auch auf „weiche Vorfelddaten“ zugreifen, die sie mit eigenen polizeilichen Befugnissen nicht hätte erheben dürfen. Aus datenschutzrechtlicher Sicht wäre es deshalb wünschenswert, wenn der Dateiinhalt auf die Daten beschränkt würde, die nach den derzeit für die beteiligten Verbundteilnehmer geltenden Übermittlungsvorschriften schon jetzt weitergegeben werden könnten.

Inhaltlich sehe ich es insbesondere als kritisch an, dass der Kreis der zur Teilnahme an der Antiterrordatei Berechtigten um zusätzliche Polizeibehörden erweitert wurde, keine strikte Zweckbindung für die gespeicherten Daten zur Aufklärung und Bekämpfung des internationalen Terrorismus besteht und der Kreis der zu speichernden Personen relativ weit und unbestimmt gefasst ist. Dies wird besonders problematisch, soweit es um die Speicherung von so genannten Kontaktpersonen geht. Bereits der Kontakt zu einem Befürworter von Gewaltanwendung könnte eine Speicherung der Person in der Datei auslösen, ohne dass es darauf ankommt, ob diese Person einen wissentlichen Bezug zur Terrorszene hat oder ihr die Gründe für die Speicherung der Bezugsperson bekannt sind. Ich bin daher der Ansicht, dass die Speicherung solcher unverdächtigen Personen nochmals überdacht und zumindest deutlich eingeschränkt werden sollte. Andernfalls besteht die Gefahr, dass auch eine Vielzahl von Personen gespeichert wird, die in keinem terroristischen Kontext steht, mithin auch völlig unbescholtene Bürger.

Ein besonderes verfassungsrechtliches Problem stellt die Aufnahme des Merkmals „Religionszugehörigkeit“ dar, auch wenn Angaben dazu nach dem Entwurf nur aufgenommen werden dürfen, wenn sie im Einzelfall zur Aufklärung oder Bekämpfung des internationalen Terrorismus erforderlich sind. Hierbei ist eine Konkordanz zu anderen ebenfalls verfas-

sungsrechtlich geschützten Rechtsgütern wie Leben, körperliche Unversehrtheit und Schutz des Staates herzustellen. Eine Aufnahme des Merkmals „Religionszugehörigkeit“ in die Datei muss - ebenso wie die Aufnahme von anderen in Art. 3 Abs. 3 GG genannten Merkmalen - verfassungsrechtlich besonders legitimiert sein, da es sich um einen gravierenden Eingriff in das Recht auf informationelle Selbstbestimmung handelt (vgl. auch Anlage Nr. 19).

6 Justiz

Im Berichtszeitraum habe ich anlassunabhängig zwei Staatsanwaltschaften und ein Amtsgericht vor Ort datenschutzrechtlich geprüft. Ferner habe ich einen Prüf- und Informationstermin bei der forensischen Abteilung eines Bezirkskrankenhauses durchgeführt. Bei zwei Justizvollzugsanstalten habe ich den Umgang mit den Gefangenendaten geprüft. Darüber hinaus habe ich mir Protokolle der Abrufe im Online-Abrufverfahren für das automatisierte Grundbuch SolumSTAR/SolumWEB angesehen und diese auf ihre formelle und materielle Richtigkeit überprüft.

Neben diesen anlassunabhängigen Prüfungen habe ich anlassbezogen aufgrund von Bürgereingaben einzelfallbezogene Prüfungen durchgeführt und bei Entwürfen von Gesetzen und Verwaltungsvorschriften sowie im Rahmen der Einführung von Formblättern für die Praxis, wie für die Dokumentation von Wohnraumüberwachungsmaßnahmen oder den DNA-Reihenuntersuchungen, auf die Berücksichtigung der datenschutzrechtlichen Erfordernisse hingewirkt.

6.1 Gesetzgebung

6.1.1 Gesetzliche Regelung von DNA-Massenscreening (DNA-Reihenuntersuchung)

In meinem 21. Tätigkeitsbericht (Nr. 7.8) hatte ich dargelegt, dass für die Probenentnahme und anschließende DNA-Analyse zum Zwecke der Aufklärung schwerwiegender Straftaten bei einem größeren Kreis von Personen, die nach bestimmten Kriterien ausgewählt wurden, ohne Tatverdächtige oder Beschuldigte zu sein (DNA-Reihenuntersuchung), eine Rechtsgrundlage fehlt. Wegen des völligen Fehlens verbindlicher Kriterien für die Durchführung eines DNA-Massenscreenings und dem mit der Maßnahme verbundenen sozialen Druck auf den zur Teilnahme ausgewählten Personenkreis war eine Durchführung allein auf der Grundlage der Einwilligung der Betroffenen aus datenschutzrechtlicher Sicht äußerst problematisch.

Diese Rechtsgrundlage hat der Gesetzgeber mit dem Gesetz zur Novellierung der forensischen DNA-Analyse vom 12.08.2005, das zum 01.11.2005 in Kraft getreten ist, geschaffen. Reihengentests sind nach § 81 h StPO nur zulässig bei Verbrechen gegen Leib oder Leben, Freiheit oder sexuelle Selbstbestimmung. Die Maßnahme darf nur von einem Richter angeordnet werden. Die Anordnung muss den betroffenen Personenkreis konkret anhand bestimmter Prüfungsmerkmale bezeichnen und ist zu begründen. Die betroffenen Personen sind zur Mitwirkung an der Untersuchung aber nicht verpflichtet. Sie ist nur mit ihrer Einwilligung zulässig. Darüber sind die betroffenen Personen schriftlich zu belehren.

Die erhobenen Daten dürfen nicht in der DNA-Analysedatei beim Bundeskriminalamt gespeichert werden. Die entnommenen Körperzellen sind unverzüglich zu vernichten, sobald sie für die Untersuchung im Rahmen des Reihengentests nicht mehr erforderlich sind.

Verweigert eine Person die freiwillige Teilnahme, darf dies nicht als Indiz für das Bestehen eines Tatverdachts angesehen werden. Nur für den Fall, dass aufgrund anderer Erkenntnisse die Entnahme einer Blutprobe zur Erforschung der Wahrheit unerlässlich ist, kann bei anderen Personen als Beschuldigten nach § 81 c StPO die Entnahme einer Blutprobe und deren molekulargenetische Untersuchung nach § 81 e StPO durch einen Richter angeordnet werden.

Ich habe das Innenministerium darauf hingewiesen, dass Tatorte einer neuen Tat weder von der ursprünglichen richterlichen Anordnung nach § 81 h StPO noch von der erteilten Einwilligung erfasst werden, auch wenn aufgrund der Tatausführung und anderer Umstände davon ausgegangen werden kann, dass es sich um denselben Täter handelt. Es bedarf in einem solchen Fall einer neuen richterlichen Anordnung sowie einer erneuten Einwilligung der Teilnehmer des früheren Reihengentests auch in diesen Abgleich. Vorstellbar ist m.E. lediglich, dass diese Teilnehmer nicht erneut zur Abgabe von Spurenmaterial aufgefordert werden, sondern die Einwilligung zur weiteren Verwendung des noch vorhandenen Spurenmaterials eingeholt wird. Wird diese (weitere) Einwilligung nicht erteilt, kann auch in diesem Fall bei Vorliegen der gesetzlichen Voraussetzungen auf Antrag eine richterliche Einzelfallanordnung ergehen.

Das Staatsministerium des Innern hat sich meiner Auffassung angeschlossen und die Polizeiverbände auf die künftige Beachtung der Rechtslage hingewiesen.

6.1.2 Akustische Wohnraumüberwachung

In meinem 21. Tätigkeitsbericht (Nr. 9.3.5) hatte ich das Urteil des Bundesverfassungsgerichts zur akustischen Wohnraumüberwachung vom 03.03.2004 und

den Gesetzgebungsentwurf der Bundesregierung zur Neuregelung dieser Vorschriften in der Strafprozessordnung dargestellt. Ich habe außerdem darauf hingewiesen, welche datenschutzrechtlichen Forderungen in diesem Entwurf bislang keine Beachtung gefunden hatten.

Mit dem Gesetz vom 24.06.2005 hat der Bundesgesetzgeber die Vorgaben des Bundesverfassungsgerichts zum Schutz des Kernbereichs privater Lebensgestaltung im Grundsatz umgesetzt. Eine Wohnraumüberwachung darf nur noch dann angeordnet werden, soweit aufgrund tatsächlicher Anhaltpunkte anzunehmen ist, dass durch die Überwachung Äußerungen, die dem Kernbereich privater Lebensgestaltung zuzurechnen sind, nicht erfasst werden. Das Abhören und Aufzeichnen ist unverzüglich zu unterbrechen, soweit sich während der Überwachung Anhaltspunkte dafür ergeben, dass Äußerungen, die dem Kernbereich privater Lebensgestaltung zuzurechnen sind, erfasst werden. Dies bedeutet aber, dass beim Abhören von Gesprächen in den Privatwohnungen in der Regel live mitgehört werden muss, damit diese gesetzlichen Voraussetzungen in der Praxis eingehalten werden.

Zum Schutz der informationellen Selbstbestimmung hat der Gesetzgeber - wie von mir seit langem gefordert - auch eine Kennzeichnungspflicht für Daten, die durch eine Wohnraumüberwachung erlangt wurden, eingeführt. Nur durch eine derartige Kennzeichnung ist gewährleistet, dass die strikte Zweckbindung dieser Daten eingehalten wird und ihre vollständige Löschung zügig erfolgen kann, sobald sie für das konkrete Verfahren nicht mehr erforderlich sind.

Das Staatsministerium der Justiz hat auf meine Anregung hin einen Dokumentationsbogen zur akustischen Wohnraumüberwachung erstellt, der die Vorgaben des Urteils des Bundesverfassungsgerichts vom 03.03.2004 und meine datenschutzrechtlichen Anforderungen umsetzt. Dieser soll den bayerischen Staatsanwaltschaften zur Verfügung gestellt werden. Er sieht insbesondere Angaben vor zum Objekt der angeordneten Maßnahme, zu evtl. Erkenntnissen über mögliche Kernbereichsgespräche sowie zu den verfahrenssichernden Voraussetzungen, wie Kennzeichnung der Daten, Weitergabe der erlangten Unterlagen, Akteneinsichtsgewährung und Benachrichtigung Betroffener oder deren Zurückstellung. Dadurch soll sichergestellt werden, dass die gesetzlichen Vorgaben in der Praxis beachtet werden. Die Umsetzung und Vollständigkeit dieser Dokumentation sowie die Beachtung der gesetzlichen Vorgaben werde ich anlässlich meiner datenschutzrechtlichen Prüfungen kontrollieren.

6.1.3 Reform der verdeckten Ermittlungsmaßnahmen in der Strafprozessordnung

Die Große Koalition schreibt in ihrer Koalitionsvereinbarung vom 11.11.2005: „Wir werden die Regelungen zur Telekommunikationsüberwachung in der Strafprozessordnung im Sinne einer harmonischen Gesamtregelung der strafprozessualen heimlichen Ermittlungsmaßnahmen überarbeiten“. Ich habe bereits mehrfach gefordert, dass der Gesetzgeber diese Überarbeitung auf der Grundlage der Rechtsprechung des Bundesverfassungsgerichts in Angriff nimmt.

Am 27.07.2005 hat das Bundesverfassungsgericht die Regelung der präventiven Telekommunikationsüberwachung in § 33 a Abs. 1 Nr. 2 und 3 Niedersächsisches Sicherheits- und Ordnungsgesetz für verfassungswidrig erklärt. Seine Ausführungen zum Schutz des Kernbereichs privater Lebensgestaltung knüpfen an das Urteil vom 03.03.2004 zur strafprozessualen Wohnraumüberwachung an. Daraus folgt, dass der durch die Menschenwürde garantierte unantastbare Kernbereich privater Lebensgestaltung im Rahmen aller verdeckten Datenerhebungen der Sicherheitsbehörden uneingeschränkt zu gewährleisten ist. Im Falle tatsächlicher Anhaltspunkte für die Annahme, dass eine Telekommunikationsüberwachung zum Kernbereich zählende Inhalte erfasst, ist ein Beweiserhebungsverbot zu normieren.

Die 70. Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat in einer Entschließung festgestellt, das die Gesetzgeber in Bund und Ländern aufgerufen sind, alle Regelungen über verdeckte Ermittlungsmethoden, auch im Bereich der Strafverfolgung, diesen gerichtlichen Vorgaben entsprechend auszugestalten (siehe Anlage Nr. 10). Diese Verpflichtung erstreckt sich auch auf die Umsetzung der gerichtlichen Vorgaben zur Wahrung des rechtsstaatlichen Gebots der Normenbestimmtheit und Normenklarheit. Im Rahmen der verfassungskonformen Ausgestaltung der Vorschriften sind die Gesetzgeber darüber hinaus verpflichtet, die gerichtlichen Vorgaben im Hinblick auf die Wahrung des Verhältnismäßigkeitsgrundsatzes - vor allem die Angemessenheit der Datenerhebung - und eine strikte Zweckbindung umzusetzen.

Insbesondere halte ich folgende Punkte für dringend umsetzungsbedürftig:

– Der Umfang des - seit Einführung der Vorschrift regelmäßig erweiterten - Straftatenkataloges des § 100 a StPO sollte im Hinblick auf Art und Schwere der Straftaten einer Überprüfung unterzogen werden. Ziel sollte dabei sein, die Telekommunikationsüberwachung auf schwere Straftaten zu begrenzen und die tat-

sächliche Relevanz der aufgeführten Tatbestände für die Praxis zu berücksichtigen.

Um eine umfassende Kontrolle der Entwicklung von Telekommunikationsüberwachungsmaßnahmen zu gewährleisten, muss in der Strafprozessordnung eine Pflicht zur Erstellung aussagekräftiger Berichte geschaffen werden. Daneben muss auch die in § 110 Abs. 8 TKG geregelte statistische Berichtspflicht der Betreiber von Telekommunikationsanlagen und der Regulierungsbehörde beibehalten werden.

- Der gesetzliche Richtervorbehalt darf nicht gelockert werden. Die Verwertung der angefertigten Aufzeichnungen sollte in Fällen staatsanwaltschaftlicher Eilanordnungen davon abhängig gemacht werden, dass ein Gericht rückwirkend deren Rechtmäßigkeit feststellt.

- Um die Qualität der Entscheidungen zu verbessern, sollte die Regelung des § 100 b StPO dahingehend ergänzt werden, dass die gesetzlichen Voraussetzungen der Anordnungen nach § 100 a StPO einzelfallbezogen darzulegen sind.

- Der durch die Menschenwürde garantierte Kernbereich privater Lebensgestaltung ist zu gewährleisten. Datenerhebungen in diesem Bereich sind deshalb grundsätzlich unzulässig. Werden im konkreten Fall Inhalte erfasst, die den Kernbereich der privaten Lebensgestaltung betreffen, müssen ein absolutes Beweisverwertungsverbot, ein Speicherungsverbot und ein Löschungsgebot gesetzlich normiert werden.

- Zum Schutz von Vertrauensverhältnissen sollte eine Regelung geschaffen werden, nach der Gespräche zwischen den Beschuldigten und zeugnisverweigerungsberechtigten Personen, also mit Angehörigen (§ 52 StPO), Berufsgeheimnisträgern (§ 53 StPO) und Berufshelfern (§ 53 a StPO), grundsätzlich nicht verwertet werden dürfen.

- Die Verwendung der durch die Maßnahmen erlangten personenbezogenen Informationen ist einer strikten Zweckbindung, insbesondere im Hinblick auf die Einhaltung der jeweiligen Anforderungen für ihre Erhebung, zu unterwerfen. Verkehrsdaten, die nach Umsetzung der europäischen Richtlinie zur Vorratsdatenspeicherung von den Telekommunikationsunternehmen zu Strafverfolgungszwecken bereitzuhalten sind, dürfen nur zum Zwecke der Verfolgung schwerer Straftaten - insbesondere, wie in den Erwägungsgründen der Richtlinie genannt, in Fällen organisierter Kriminalität und Terrorismus - verwendet werden. § 100 g StPO bedarf einer entsprechenden Überarbeitung.

- Zur Sicherung der Zweckbindung muss eine gesetzliche Verpflichtung zur Kennzeichnung der erlangten Daten geschaffen werden.

- Der Umfang der Benachrichtigungspflichten ist im Gesetz näher zu definieren. Die Benachrichtigungsfrist und die richterliche Überprüfung ihrer Einhaltung bzw. ihres Aufschubs sollten geregelt werden.

Diese Forderungen sind grundsätzlich bei allen verdeckten Datenerhebungsmaßnahmen der Strafverfolgungsbehörden zu berücksichtigen. Dies gilt insbesondere für die Forderungen nach Überprüfung der Voraussetzungen für diese Maßnahme, Zweckbindung der erhobenen Daten, ausreichenden Kernbereichsschutz, Schutz von Vertrauensverhältnissen und Regelung von Benachrichtigungspflichten sowie Löschungsfristen.

6.1.4 Funkzellenabfrage

Unter „Funkzellenabfrage“ ist das Verlangen der Ermittlungsbehörden gegenüber Telekommunikationsdiensteanbietern nach Auskunft über Telekommunikationsverbindungsdaten zu verstehen, die in einer bestimmten, räumlich bezeichneten Funkzelle, dem kleinsten geografischen Funkversorgungsbereich, in einem bestimmten Zeitraum anfallen. Sie wird auf die §§ 100 g, 100 h Abs. 1 Satz 2 StPO gestützt. Diese Regelungen halte ich als Grundlage einer Funkzellenabfrage für unzureichend. Im Hinblick auf die Intensität eines solchen Eingriffs, seine große Streubreite und die Einbeziehung zahlreicher Personen in den Wirkungsbereich dieser Maßnahme, die in keiner Beziehung zu einem konkreten Fehlverhalten stehen und den Eingriff durch ihr Verhalten nicht veranlasst haben, genügt der als Verfahrensvorschrift ausgestaltete § 100 h StPO dem verfassungsrechtlichen Gebot nach ausreichender Bestimmtheit gesetzlicher Regelungen nicht. Eine datenschutzkonforme Regelung muss insbesondere folgende Punkte berücksichtigen:

- Funkzellenabfragen dürfen nur dann durchgeführt werden, wenn eine erhebliche Straftat begangen wurde und eine hinreichend sichere Tatsachenbasis vorliegt, dass der Täter telefoniert hat.

- Im Rahmen einer Verhältnismäßigkeitsprüfung im Einzelfall sind die Schwere der Straftat und die Anzahl der durch die Maßnahme

möglicherweise betroffenen unbeteiligten Dritten gegeneinander abzuwägen.

- Die Maßnahme ist räumlich und zeitlich auf den unbedingt notwendigen Umfang zu begrenzen.

- Die Verbindungsdaten der Betroffenen müssen unverzüglich gelöscht werden, sobald ihre weitere Speicherung für das Ermittlungsverfahren nicht mehr erforderlich ist.

- Funkzellenabfragen, insbesondere die Zahl der Maßnahmen, die Zahl der Betroffenen und die Bedeutung der Maßnahmen für die Ermittlungen sollten statistisch erfasst werden, um eine datenschutzrechtliche Überprüfung und Evaluation zu ermöglichen.

In der Praxis habe ich festgestellt, dass die erlangten Telekommunikationsverbindungsdaten in einer Reihe von Fällen für einen automatisierten Abgleich mit anderen Telekommunikationsverbindungsdaten von sog. tatrelevanten Örtlichkeiten genutzt werden. Hierfür sehe ich in der Strafprozessordnung keine Rechtsgrundlage.

Die Datenschutzbeauftragten des Bundes und der Länder haben die Bundesministerin für Justiz auf die Unzulässigkeit dieser Vorgehensweise hingewiesen.

6.1.5 Datenschutz in der Dritten Säule der Europäischen Union

Die Europäische Union hat auch erhebliche Bedeutung für die Entwicklung des Datenschutzes in Europa. Für den Bereich der sog. dritten Säule (Innere Sicherheit und Justizpolitik) hat der Amsterdamer Vertrag, der am 01.05.1999 in Kraft getreten ist, die Zusammenarbeit neu geordnet und als neues Ziel die Schaffung eines Raums der Freiheit, der Sicherheit und des Rechts festgeschrieben.

Die in diesem Bereich gefassten Rahmenbeschlüsse haben jedoch keine unmittelbare innerstaatliche Wirkung, sondern müssen erst durch nationale Rechtsakte umgesetzt werden. Ich sehe es auch als meine Aufgabe an, mich bereits im Vorfeld solcher Beschlüsse für die Belange des Datenschutzes einzusetzen.

Der Europäische Rat hat das Haager Programm zur Stärkung von Freiheit, Sicherheit und Recht in der Europäischen Union am 04.11.2004 angenommen. Darin wird die Kommission ersucht, bis spätestens Ende 2005 Vorschläge zur Verwirklichung des Verfügbarkeitsgrundsatzes vorzulegen, damit der grenzüberschreitende Austausch von strafverfolgsrelevanten Informationen zwischen den Mitgliedstaaten verbessert wird. Die Kommission hat am 18.10.2005 einen Vorschlag für einen Rahmenbeschluss des Rates über den Austausch von Informationen nach dem Grundsatz der Verfügbarkeit sowie am 11.10.2005 einen Vorschlag für einen Rahmenbeschluss des Rates über den Schutz personenbezogener Daten, die im Rahmen der polizeilichen und justiziellen Zusammenarbeit in Strafsachen verarbeitet werden, vorgelegt.

Als Gegengewicht zu dem geplanten verstärkten grenzüberschreitenden Informationsaustausch zwischen den Strafverfolgungsbehörden müssen verbindliche Regelungen über den Datenschutz mit dem Ziel der Schaffung eines hohen und einheitlichen Datenschutzstandards geschaffen werden. Die Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom März 2006 „Mehr Datenschutz bei der polizeilichen und justiziellen Zusammenarbeit in Strafsachen“ (siehe Anlage Nr. 14) unterstützt diese Forderung und gibt Hinweise für deren Umsetzung.

6.1.6 Aufbewahrungsbestimmungen für Justizakten

Bereits in meinem 19. (Nr. 7.2.1.) und 20. (Nr. 8.1.3.1.) Tätigkeitsbericht hatte ich über meine seit langem andauernden Bemühungen um eine gesetzliche Regelung für die Aufbewahrung von gerichtlichen Akten der Zivil- und Strafjustiz berichtet. Ich halte es für dringend notwendig, dass unverzüglich ein Aktenaufbewahrungsgesetz für die Justiz geschaffen wird. Das Oberlandesgericht Frankfurt am Main hatte bereits im Jahr 1998 entschieden, dass der Zustand einer fehlenden gesetzlichen Grundlage für die Aufbewahrung von Strafakten für eine Übergangsfrist noch hinzunehmen sei, dass dies jedoch nicht nur als mittelfristige Aufgabenstellung des Gesetzgebers betrachtet werden dürfe, sondern alsbald in Angriff zu nehmen sei (OLG Frankfurt, NJW 99, 73, 75).

Das Staatsministerium der Justiz geht hingegen davon aus, dass die Dauer der Aufbewahrung von Strafakten nach rechtskräftigem Abschluss des Strafverfahrens, ihre Aussonderung und Vernichtung einer Regelung durch ein eigenes formelles Gesetz nicht bedürfe. Die Strafprozessordnung biete eine hinreichende Rechtsgrundlage für die Aktenaufbewahrung. Eine Konkretisierung der Aufbewahrung und Aussonderung von Akten erfolge durch die bundeseinheitlichen Aufbewahrungsbestimmungen und die Aussonderungsbekanntmachung der Justiz.

Diese Ausführungen des Staatsministeriums der Justiz sind für mich nicht nachvollziehbar. Bereits das Bundesverfassungsgericht hat im Volkszählungsurteil vom 15.12.1983 (BVerfGE 65, 1) entschieden, dass

der Einzelne zwar grundsätzlich Einschränkungen seines Rechts auf informationelle Selbstbestimmung im überwiegenden allgemeinen Interesse hinnehmen muss, diese Beschränkungen aber nach Art. 2 Abs. 1 GG einer verfassungsmäßigen gesetzlichen Grundlage bedürfen, aus der sich die Voraussetzungen und der Umfang der Beschränkungen klar und für den Bürger erkennbar ergeben und die damit dem rechtsstaatlichen Gebot der Normenklarheit entsprechen. Daran fehlt es nach wie vor. Verwaltungsvorschriften - wie die Aussonderungsbekanntmachung - können dieses Defizit nicht beheben. Bis zu einer durch den Gesetzgeber getroffenen Entscheidung ist deshalb für die Übergangszeit der grundrechtsfreundlichste Ausgleich zwischen dem staatlichen Interesse an der Aufgabenerfüllung der Strafverfolgungsbehörden und dem Anspruch des Einzelnen auf Löschung seiner Daten geboten. Dem entsprechen die Aussonderungsregelungen in der Bekanntmachung des Staatsministeriums der Justiz nicht. Sie sehen eine Aussonderung für Justizakten nach Ablauf der Aufbewahrungsfristen in vom Behördenleiter zu bestimmenden Zeitabständen, etwa alle fünf bis zehn Jahre vor. Ich halte es hingegen für notwendig, dass nach Ablauf der Aufbewahrungsfristen eine unverzügliche Aussonderung der Akten erfolgt. Dies habe ich dem Staatsministerium der Justiz mitgeteilt.

Das Ministerium hat daraufhin eine Befragung der Staatsanwaltschaften nach der tatsächlichen Praxis bei der Aktenaussonderung durchgeführt. Diese hat ergeben, dass mit einer Ausnahme jährlich zumindest Teilaussonderungen durchgeführt werden. Soweit eine Staatsanwaltschaft noch nicht jährlich Aussonderungen vornehme, werde das Staatsministerium der Justiz den Hintergründen nachgehen. Ich werde das Staatsministerium der Justiz auffordern, dafür Sorge zu tragen, dass nach Ablauf der Aufbewahrungsfristen bei allen bayerischen Staatsanwaltschaften zeitnah die Aktenaussonderung durchgeführt wird.

Zwischenzeitlich hat mir das Justizministerium des Landes Nordrhein-Westfalen einen ersten Entwurf für ein Aktenaufbewahrungsgesetz zugeleitet, der unter Federführung von Nordrhein-Westfalen von einer durch die Justizministerkonferenz eingesetzten länderoffenen Arbeitsgruppe erarbeitet worden ist. Als Vorsitzender des Arbeitskreises Justiz der Datenschutzbeauftragten des Bundes und der Länder habe ich eine mit den Landesbeauftragten abgestimmte Stellungnahme abgegeben, die konkrete Verbesserungsvorschläge enthält.

6.1.7 Entwurf eines Gesetzes über genetische Untersuchungen zur Klärung der Abstammung in der Familie

Die Datenschutzbeauftragten des Bundes und der Länder haben sich bereits in der Vergangenheit gegen heimliche Vaterschaftstests ausgesprochen. Um Missbrauch zu verhindern, dürfen Gentests nur durchgeführt werden, wenn alle Betroffenen wirksam einwilligen oder wenn eine gerichtliche Anordnung auf Basis einer gesetzlichen Ermächtigungsgrundlage vorliegt. Bei allem Verständnis für das Interesse des Vaters an der Feststellung seiner Vaterschaft müssen die elementaren Persönlichkeitsrechte des Kindes geschützt bleiben. Der Ausgleich von unterschiedlichen Interessen kann nicht durch heimliche Gentests, sondern nur im Rahmen gesetzlicher Regelungen erfolgen. So hat auch der Bundesgerichtshof in seinen beiden Entscheidungen vom 12.01.2005 festgestellt, heimlich veranlasste DNA-Vaterschaftsanalysen verstießen gegen das Persönlichkeitsrecht und die informationelle Selbstbestimmung des Kindes. Das Interesse des Vaters oder Scheinvaters, sich Gewissheit über seine Vaterschaft zu verschaffen, könne auch dann nicht als höherrangig angesehen werden, wenn es der Abwehr zivilrechtlicher Ansprüche, denen er als gesetzlicher Vater ausgesetzt sei, dienen solle.

An dieser verfassungsrechtlichen Bewertung kann die Schaffung einer einfachgesetzlichen Rechtsgrundlage, die - wie in einem Gesetzentwurf des Landes Baden-Württemberg vorgesehen - die Durchführung heimlicher DNA-Vaterschaftsanalysen ohne Einwilligung der Betroffenen oder gerichtliche Anordnung erlaubt, nichts ändern. Dies gilt auch unter Berücksichtigung der Gefahr, dass die offene Durchführung genetischer Untersuchungen auch in den Fällen, in denen sich herausstellt, dass das Kind vom Ehemann abstammt, zu einer schwerwiegenden Belastung der familiären Beziehungen führen kann. Ich habe meine datenschutzrechtlichen Erwägungen dem Staatsministerium der Justiz mitgeteilt und es gebeten, sich gegen den Gesetzentwurf des Landes Baden-Württemberg auszusprechen.

Im Zusammenhang mit der Problematik heimlicher Abstammungsuntersuchungen hat der Freistaat Bayern den Entwurf eines Gesetzes über genetische Untersuchungen zur Klärung der Abstammung in der Familie in den Bundesrat eingebracht (BR-Drs. 369/05). Der Gesetzentwurf sieht die Einfügung eines § 1600 f BGB-E vor, wonach die zur Vaterschaftsanfechtung gemäß § 1600 Abs. 1 BGB berechtigten Personen (rechtlicher Vater, Vaterschaftsprätendent und Mutter) einen Anspruch gegen das Kind auf Einwilligung in die Gewinnung einer genetischen Probe und die gendiagnostische Abstammungsuntersuchung haben. Die Mutter und das Kind sollen auch gegen die anderen anfechtungsberechtigten Personen einen solchen Anspruch haben, wenn deren Mitwirkung bei der Untersuchung erforderlich ist. Die Regelung bezieht sich auf außerhalb eines gerichtlichen Verfahrens privat in Auftrag gegebene von privaten Genlabors durchgeführte Tests; allerdings soll die Verwendung auf diesem Wege erlangter Tests im

Rahmen eines nachfolgenden Vaterschaftsanfechtungsverfahrens zulässig sein.

Positiv beurteile ich am Gesetzentwurf Bayerns, dass Vaterschaftstests nur auf der Grundlage einer Einwilligung der Betroffenen durchgeführt werden können. Auch dass die Durchführung solcher Tests nicht die Anfechtung der Vaterschaft im Rahmen eines gerichtlichen Verfahrens zur Voraussetzung haben soll, halte ich für sachgerecht, da durchaus denkbar ist, dass anfechtungsberechtigte Personen die Frage der Abstammung klären möchten, ohne die rechtlichen Folgen auszulösen, die mit einer begründeten Anfechtung verbunden sind.

Sowohl der Gesetzesantrag des Freistaats Bayern als auch der Gesetzesantrag des Landes Baden-Württemberg sind derzeit noch in den Ausschüssen des Bundesrats anhängig. Das Plenum des Bundesrats hat über die Einbringung beider Gesetzentwürfe noch nicht abgestimmt. Vielmehr hat der federführende Rechtsausschuss des Bundesrats seine Beratungen über beide Entwürfe bis zum Wiederaufruf vertagt, damit die Möglichkeit besteht, Vorschläge zur Änderung oder Ergänzung der Gesetzentwürfe zu erörtern. Daraufhin wurde eine Bund-Länder-Arbeitsgruppe eingerichtet, die nach Auskunft des Staatsministeriums der Justiz angesichts der komplexen Problemlage aber noch keinen konsensfähigen Vorschlag vorgelegt hat.

6.2 Gerichtlicher Bereich

6.2.1 Automatisiertes Grundbuchabrufverfahren SolumSTAR/SolumWEB

In meinem 21. Tätigkeitsbericht (Nr. 9.2.3) hatte ich bereits die Einführung des automatisierten Abrufverfahrens beim Grundbuch SolumSTAR/SolumWEB dargestellt. Ich habe mich in diesem Zusammenhang für eine Beschränkung der Abrufberechtigung für Gemeinden auf das Gemeindegebiet und eine Protokollierung der Abrufe dergestalt eingesetzt, dass nicht nur die abfragende Stelle, sondern auch der einzelne Bedienstete, der den Abruf vorgenommen hat, erkennbar ist. Dies erst ermöglicht es, die in § 83 Abs. 1 Satz 3 Grundbuchverordnung vorgesehenen Stichprobenkontrollen durch die aufsichtsführenden Stellen sinnvoll durchzuführen.

Das Staatsministerium der Justiz hat auf meine Forderung hin die gemeinsame IT-Stelle der bayerischen Justiz, unter deren Verantwortung das Verfahren entwickelt wurde, beauftragt, für Teilnehmer des Online-Grundbuch-Abrufverfahrens Gruppenkennungen einzurichten. Dabei ist für eine ordnungsgemäße Systemanmeldung die Eingabe des Bearbeiternamens erforderlich, der auch entsprechend protokolliert wird. Hinsichtlich der Forderung einer Beschränkung der Zugriffsberechtigung der Gemeinden haben sich die Datenschutzbeauftragten des Bundes und der Länder mit einem Schreiben an die Vorsitzende der Justizministerkonferenz gewandt. Eine Antwort auf dieses Schreiben steht noch aus.

Auf meine Veranlassung hat das Staatsministerium des Innern die Regierungen und die Landratsämter auf die Kontrollmöglichkeit beim Online-Abrufverfahren aus dem Grundbuch hingewiesen und gebeten, in geeigneten Abständen durch Stichproben die Rechtmäßigkeit der Abrufe zu kontrollieren. Ich habe durch Rückfrage beim Präsidenten des Oberlandesgerichts München, Zentrale Grundbuchspeicherstelle für Bayern, festgestellt, dass bisher 21 aufsichtsführende Stellen Protokolldaten zur Durchführung von Stichprobenkontrollen angefordert haben.

Zum Zwecke einer eigenen anlassunabhängigen Überprüfung der Rechtmäßigkeit von Abrufen habe ich die Zentrale Grundbuchspeicherstelle gebeten, eine Auswertung der Protokolldatei nach den jeweils 100 aktuellsten Abfragen durch bayerische Dienststellen durchzuführen. Aus den mir übersandten Protokolldaten habe ich zehn öffentliche Stellen ausgewählt und diese um Mitteilung des Anlasses und des berechtigten Interesses i.S.v. § 12 Grundbuchordnung sowie evtl. weiterer Rechtsgrundlagen der Datenabfragen gebeten. Die Prüfung hat ergeben, dass die Abfragen durch ein berechtigtes Interesse gerechtfertigt waren. In einem Fall wurde als Abfragegrund eine „Testabfrage“ unter Verwendung des eigenen Grundstücks angegeben. Zu kritisieren war allerdings die in zahlreichen Fällen mangelhafte Angabe des Aktenzeichens bzw. des zugrunde liegenden Abfragegrundes. Ich habe mich deswegen an das Staatsministerium des Innern gewandt und darum gebeten, dafür Sorge zu tragen, dass in Zukunft eine ordnungsgemäße Dokumentation der Abfragen erfolgt. Dieses hat daraufhin die Aufsichtsbehörden daran erinnert, in geeigneten Abständen durch Stichprobenverfahren die Rechtmäßigkeit der Abrufe aus dem automatisierten Grundbuch zu kontrollieren und auf die Notwendigkeit einer ausreichenden Dokumentation hingewiesen.

6.2.2 Akteneinsicht in Bewährungshelferakten

Zur Zeit werden beim Oberlandesgericht München Qualitätsstandards in der Bewährungshilfe in Bayern als Arbeitshilfe für die bayerischen Bewährungshelfer erarbeitet. Der Präsident des Oberlandesgerichts München hat mich hierzu um Stellungnahme gebeten. Ich habe insbesondere auf die besondere Rolle des Bewährungshelfers und die sich daraus ergebenden Konsequenzen hingewiesen. Der Bewährungshelfer ist gegenüber dem Probanden auch unterstützend und helfend tätig und erfährt im Rahmen seiner

Aufgabenwahrnehmung oft vertrauliche Dinge. So enthalten die Akten der Bewährungshelfer häufig sensible Daten, die der Proband z.B. gegenüber der Staatsanwaltschaft nicht offenbart hätte. § 203 Abs. 1 Nr. 5 StGB legt deshalb fest, dass ein Bewährungshelfer, weil er regelmäßig als staatlich anerkannter Sozialarbeiter oder Sozialpädagoge arbeitet, sich strafbar macht, wenn er unbefugt ein fremdes Geheimnis, namentlich ein zum persönlichen Lebensbereich gehörendes Geheimnis oder ein Betriebs- oder Geschäftsgeheimnis offenbart, das ihm in seiner Eigenschaft als Sozialarbeiter anvertraut oder sonst bekannt geworden ist. § 203 StGB verdeutlicht, dass der Gesetzgeber die in den Bewährungshelferakten enthaltenen Daten als besonders sensibel und schützenswert beurteilt, da zum Schutz dieser Daten die unbefugte Weitergabe unter Strafe gestellt ist.

Für zulässig halte ich deshalb die Erteilung von Auskünften und die Gewährung von Akteneinsicht durch den Bewährungshelfer an das die Bewährung überwachende Gericht im Rahmen der Regelung des § 56 d StGB und an die Richter und Beamten der Aufsichtsbehörden (vgl. Art. 17 Abs. 3 Satz 1 BayDSG). Über diese Regelungen hinaus sehe ich - im Gegensatz zum Staatsministerium der Justiz - keine weitere Rechtsgrundlage für eine Datenübermittlung. Dies gilt auch für die Vorschriften über die Akteneinsicht in Gerichts- und Staatsanwaltschaftsakten in § 474 Abs. 1 StPO, die ich auf Bewährungshelferakten nicht für anwendbar halte.

Ich habe das Staatsministerium der Justiz aufgefordert, meine Auffassung in den Standards für die Bewährungshelfer umzusetzen. Eine Antwort des Staatsministeriums der Justiz steht noch aus.

6.3 Strafverfolgung

6.3.1 Mautdaten - Keine Verwendung zu Strafverfolgungszwecken

Eine staatliche Datennutzung von Mautdaten zu Strafverfolgungszwecken, die im Falle der Einführung einer entsprechenden Maut für Personenkraftwagen sämtliche Autofahrer betreffen würde, lehne ich ab. Politische Forderungen nach Nutzung der Mautdaten zur Verbrechensbekämpfung, die für die Öffentlichkeit vordergründig auf Mordfälle gestützt werden, zielen in Wirklichkeit auf eine Vielzahl von Straftaten, auch auf Vergehen (Straftaten von erheblicher Bedeutung) ab.

Solche Einzelfälle, so schwerwiegend und bedauerlich sie auch sind, dürfen nicht als Vehikel für die Mehrung staatlicher Überwachung missbraucht werden.

Der Umfang staatlicher Überwachungsmaßnahmen in den letzten Jahren ist stetig gewachsen (Wohnungs-, Telefon- und Videoüberwachung, Kennzeichenerkennung, Kontenabfrage). Es hat sich auch gezeigt, dass der Anwendungsbereich von Eingriffsbefugnissen, die zunächst mit dem Schutz vor besonders schwerwiegenden Bedrohungen begründet wurden, später erheblich erweitert wurden. Dieser Tendenz gilt es entgegenzuwirken. Staatliche Überwachungsmöglichkeiten müssen auf ein vertretbares Maß begrenzt werden, um einen Ausgleich zwischen informationeller Selbstbestimmung und Eingriffsbefugnissen zu schaffen.

Im Jahr 2004 wurde das Autobahnmautgesetz dahingehend geändert, dass eine Übermittlung, Nutzung oder Beschlagnahme nach anderen Rechtsvorschriften ausdrücklich für unzulässig erklärt wurde. Noch vor weniger als drei Jahren war der Gesetzgeber also der Auffassung, dass neben einem personenbezogenen Mautsystem keine allgemeine Überwachungsinfrastruktur geschaffen werden dürfe. Vor diesem Hintergrund sollte jetzt nicht eine Verwendung der Mautdaten für Zwecke der Verfolgung von Straftaten zugelassen und damit innerhalb verhältnismäßig kurzer Zeit das verfassungsrechtliche Gebot der Zweckbindung relativiert werden. Dabei geht es nicht um „Täterschutz“ sondern um die Begrenzung staatlicher Überwachungsmöglichkeiten und um einen Ausgleich zwischen informationeller Selbstbestimmung und Eingriffsbefugnissen. Ich plädiere daher nachdrücklich dafür, dass eine staatliche Nutzung von Mautdaten zu Strafverfolgungszwecken nicht Realität werden darf.

6.3.2 Automatisierte Kennzeichenerkennung zu Strafverfolgungszwecken

Das Staatsministerium des Innern hat mir die durch die Projektgruppe automatisierte Kennzeichenerkennung des Polizeipräsidiums Niederbayern/Oberpfalz erarbeitete Errichtungsanordnung für die Arbeitsdatei automatisierte Kennzeichenerkennung (AKE-AD) zugesandt und mitgeteilt, dass es dieser in der beiliegenden Fassung gemäß Art. 47 Abs. 1 PAG zugestimmt hat. Aus der Errichtungsanordnung ergibt sich, dass die automatisierte Kennzeichenerkennung nicht nur entsprechend der Neuregelung im Polizeiaufgabengesetz im präventiven Bereich (siehe hierzu Nr. 4.14), sondern auch zu Zwecken der Strafverfolgung Anwendung finden soll. Dies soll nach Abstimmung des Staatsministeriums des Innern mit dem Staatsministerium der Justiz auf die Regelung der Kontrollstellen auf Straßen und Plätzen (§ 111 StPO) und, wegen der beabsichtigten Heimlichkeit der Maßnahme, zusätzlich auf § 100 f StPO (Maßnahmen ohne Wissen des Betroffenen außerhalb von Wohnungen) gestützt werden. Die Speicherung der Daten soll sich nach § 163 d Abs.1 Nr.1 StPO richten, der

im Rahmen einer Schleppnetzfahndung die Speicherung von Daten, die an einer Kontrollstelle nach § 111 StPO angefallen sind, zulässt.

Ich habe das Staatsministerium des Innern darauf hingewiesen, dass ich für den repressiven Einsatz der automatisierten Kennzeichenerkennung in der Strafprozessordnung keine Rechtsgrundlage sehe:

Es liegt nicht in der Entscheidungskompetenz der Vollzugsbehörden, die durch die Fortschritte der Informationstechnologie neu geschaffenen Möglichkeiten von Erhebung, Verarbeitung und Verknüpfung von Daten, die mit Grundrechtseingriffen verbunden sind, beliebig in der Praxis einzusetzen. Es ist zunächst Aufgabe des Gesetzgebers eine grundsätzliche Entscheidung über das Ob des Einsatzes einer neuartigen (technischen) Maßnahme zu treffen und dann ggf. Zweck und Umfang der Maßnahme in einem verfassungskonformen Rahmen gesetzlich festzuschreiben.

Das Erfordernis einer speziellen gesetzlichen Rechtsgrundlage ergibt sich bereits aus der ständigen Rechtsprechung des Bundesverfassungsgerichts, wonach Grundrechtseingriffe einer klaren und detaillierten gesetzlichen Regelung bedürfen (vgl. auch Beschluss des 1. Senats des BVerfG vom 04.04.2006 zur Rasterfahndung). Das gilt insbesondere für repressive Grundrechtseingriffe, die 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. Bei der automatisierten Kennzeichenerkennung handelt es sich um eine solche Maßnahme, die, wie die Rasterfahndung, einen unbestimmten Personenkreis trifft, der den Eingriff durch kein konkretes (Fehl-)Verhalten veranlasst hat. Anschließende informationsbezogene Ermittlungsmaßnahmen bergen im Falle ihres Bekanntwerdens bei Dritten die Gefahr einer stigmatisierenden Wirkung für die Betroffenen und so mittelbar das Risiko, im Alltag oder im Berufsleben diskriminiert zu werden, in sich. Dies stellt einen besonders intensiven Eingriff in das informationelle Selbstbestimmungsrecht des Einzelnen aus Art. 2 Abs. 1 i.V.m. Art.1 Abs. 1 GG dar, da er nicht mehr mit hinreichender Sicherheit überschauen kann, welche ihn betreffenden Informationen bestimmten Bereichen seiner sozialen Umwelt bekannt sind (vgl. hierzu BVerfGE 65, 1 ff).

§ 111 StPO enthält keine Rechtsgrundlage für eine automatisierte Kennzeichenerkennung. Er regelt die Einrichtung von Kontrollstellen, an welchen nach dem Gesetzeswortlaut jedermann verpflichtet ist, seine Identität feststellen und sich, sowie mitgeführte Sachen durchsuchen zu lassen. Die Befugnisse an einer Kontrollstelle sind damit in § 111 StPO ausdrücklich und abschließend benannt. Weder der Gesetzeswortlaut noch die Kommentierung in der Rechtsliteratur lassen darauf schließen, dass darüber hinaus weitere einschneidende Eingriffe, insbesondere verdeckte Maßnahmen mit Hilfe des Einsatzes technischer Mittel, die zahlreiche unbeteiligte Dritte treffen, im Rahmen von Kontrollstellen i.S.v. § 111 StPO zulässig wären.

§ 111 StPO enthält zudem auch keinen Verweis auf § 100 f StPO und umgekehrt. Es liegt aber nicht im Ermessen der Vollzugsbehörden, Eingriffsgrundlagen nach Belieben kumulativ anzuwenden, um zum erwünschten Ergebnis zu gelangen. Dies kann ausschließlich mit entsprechenden Verweisungen durch den Gesetzgeber bestimmt werden.

Die Maßnahme der repressiven automatisierten Kennzeichenerkennung ist auch nicht allein von der Eingriffsgrundlage des § 100 f StPO gedeckt. § 100 f StPO bestimmt, dass ohne Wissen des Betroffenen außerhalb von Wohnungen Bildaufnahmen hergestellt werden dürfen, wenn bestimmte Voraussetzungen erfüllt sind. § 100 f Nr. 2 StPO regelt die Verwendung „sonstiger besonderer für Observationszwecke bestimmte technische Mittel“. Hieraus folgt, dass Bildaufnahmen nach Nr. 1 ebenfalls ausschließlich zu Observationszwecken hergestellt werden dürfen. Die Fahndung nach einem flüchtigen Straftäter mit Hilfe von Kontrollstellen an Ausfallstraßen stellt jedoch keine Observation dar, denn unter Observation versteht man das planmäßig angelegte Beobachten einer bestimmten Person und deren Umfeld, um sich ein Bewegungsbild zu verschaffen und Strukturen aufzuspüren.

Zu unterscheiden von der Frage einer Rechtsgrundlage für die automatisierte Kennzeichenerkennung ist die Frage der Zulässigkeit der Speicherung der durch diese Maßnahme erlangten Daten und deren späterer Abgleich mit Dateien. § 163 d StPO stellt dafür keine Rechtsgrundlage dar. Dort ist die Zulässigkeit der Speicherung von Daten über die Identität von Personen sowie von Umständen geregelt, die an Kontrollstellen nach § 111 StPO angefallen sind. Solche Umstände können auch amtliche Kennzeichen von Kraftfahrzeugen sein. Da § 111 StPO aber keine Rechtsgrundlage für eine automatisierte Kennzeichenerkennung darstellt, kann sich eine Speicherung auch nicht auf § 163 d StPO berufen.

Ich habe deshalb den Staatsminister des Innern und die Staatsministerin der Justiz gebeten, dafür Sorge zu tragen, dass die automatisierte Kennzeichenerkennung ohne ausreichende gesetzliche Grundlage auch in Bayern nicht zu Strafverfolgungszwecken eingesetzt wird.

6.3.3 Benachrichtigungspflicht gemäß § 101 StPO bei Telekommunikationsüberwachungsmaßnahmen

Bereits in meinem 21. Tätigkeitsbericht (Nr. 9.3.6) hatte ich dargestellt, dass ich anlässlich der Prüfung der praktischen Durchführung von Telekommunikationsüberwachungsmaßnahmen (TKÜ-Maßnahmen) bei einer Staatsanwaltschaft festgestellt habe, dass datenschutzrechtliche Mängel vor allem hinsichtlich der Benachrichtigung der Beteiligten über die durchgeführte Maßnahme zu verzeichnen waren.

In meinem Schriftwechsel mit dem Staatsministerium der Justiz ist mir insbesondere entgegengehalten worden, dass der Benachrichtigungspflicht der Staatsanwaltschaft auch durch die vollständige Akteneinsicht des Verteidigers des Beschuldigten Rechnung getragen werde. Ich teile diese Auffassung grundsätzlich nicht. § 101 Abs. 1 StPO legt fest, dass die Beteiligten durch die Staatsanwaltschaft von den getroffenen Maßnahmen zu benachrichtigen sind, sobald dies ohne Gefährdung des Untersuchungszwecks, der öffentlichen Sicherheit von Leib oder Leben einer Person sowie der Möglichkeit der weiteren Verwendung eines eingesetzten, nicht offen ermittelnden Beamten geschehen kann. Diese Benachrichtigung ist als aktive Pflicht der Staatsanwaltschaft normiert. Die Gewährung von Akteneinsicht an einen bevollmächtigten Verteidiger kann diese aktive Benachrichtigungspflicht grundsätzlich nicht ersetzen. Die Staatsanwaltschaft muss vielmehr sicherstellen, dass der Beschuldigte von der getroffenen TKÜ-Maßnahme tatsächlich Kenntnis erlangt. Solange offenbleibt, ob sich zum Zeitpunkt der Akteneinsicht die Information, dass eine TKÜ-Maßnahme durchgeführt wurde, in der Akte befand, in welchem Umfang Einsicht in die Akten genommen und ob Erkenntnisse bezüglich der TKÜ-Maßnahme daraus gewonnen wurden, bleibt es bei der nachträglichen Benachrichtigungspflicht. Auf die grundrechtliche Bedeutung der Benachrichtigung hat auch das Bundesverfassungsgericht in seinem Urteil vom 03.03.2004 zur Wohnraumüberwachung hingewiesen. Durch die gesetzlich geregelte Benachrichtigung sei der nachträgliche Rechtschutz der Betroffenen hinreichend gesichert. Dies entspreche dem Anspruch auf effektiven Rechtschutz aus Art. 19 Abs. 4 Grundgesetz.

Das Staatsministerium der Justiz hat schließlich eine Änderung der Textbausteine der Formblätter für die Gewährung der Akteneinsicht der Staatsanwaltschaften veranlasst. Es wird nun bei Gewährung der Akteneinsicht nach Durchführung von TKÜ-Maßnahmen der akteneinsichtnehmende Verteidiger schriftlich auf die Anordnung der Telefonüberwachung hingewiesen.

Diese Änderung der Formblätter begrüße ich aus datenschutzrechtlicher Sicht. Es ist jedoch festzustellen, dass dieser Vermerk im Rahmen der Akteneinsicht nicht dazu führen kann, dass eine Benachrichtigung generell unterbleibt. Es verbleibt selbstverständlich bei der primären gesetzlichen Pflicht der Staatsanwaltschaft, die Beteiligten von den getroffenen Maßnahmen dann zu benachrichtigen, sobald dies ohne Gefährdung des Untersuchungszwecks möglich ist. Ein Abwarten bis zu einem etwaigen Einsichtsgesuch des Verteidigers ist demnach nicht vertretbar.

Ich werde mich weiterhin für die Beachtung dieser Benachrichtigungspflicht einsetzen und die Handhabung der geänderten Formblätter in der Praxis beobachten.

6.3.4 Speicherung Minderjähriger in der staatsanwaltschaftlichen Vorgangsverwaltung

Im Zusammenhang mit zwei Eingaben gesetzlicher Vertreter strafunmündiger Kinder, gegen die staatsanwaltschaftliche Ermittlungsverfahren eingeleitet worden waren, hatte ich die Zulässigkeit folgender datenschutzrechtlich relevanter Eingriffe zu klären:

- Speicherung personenbezogener Daten strafunmündiger Kinder in der staatsanwaltschaftlichen Vorgangsverwaltung unter dem Status eines Beschuldigten,

- Eintragung von Vorgängen, die den Verdacht des von Kindern begangenen rechtswidrigen und mit Strafe bedrohten Handelns zum Gegenstand haben, in das staatsanwaltschaftliche Js-Register.

Die Speicherung personenbezogener Daten strafunmündiger Kinder zum Zwecke der staatsanwaltschaftlichen Vorgangsverwaltung sehe ich in Übereinstimmung mit dem Staatsministerium der Justiz grundsätzlich als zulässig an, da dies zum Nachweis des Vorgangs erforderlich ist. Strafunmündige Kinder, die verdächtig sind, objektiv Straftatbestände verwirklicht zu haben, werden aber unter der Kennziffer 01 als Beschuldigte gespeichert. Das Staatsministerium der Justiz begründet dies im Wesentlichen wie folgt:

Der Katalog der Kennzahlen sei abschließend und könne nicht ohne Änderung des Vorgangsverwaltungsprogramms erweitert werden, denn die Kennzahlen dienten nicht nur der Unterrichtung des Sachbearbeiters, sondern auch der Steuerung des Fachverfahrens selbst. Die Kennzahl 01 stehe zwar für Beschuldigter, durch die Vergabe dieser Kennzahl werde dem strafunmündigen Kind aber nicht ein Beschuldigtenstatus im materiell-rechtlichen oder strafprozessualen Sinne verliehen. Die Kennzahl weise lediglich aus, welche zu einem Verfahren erfasste

Person diejenige sei, deren Verhalten Gegenstand des Ermittlungsverfahrens sei. Eine besser geeignete Kennzahl für registrierte strafunmündige Kinder stehe in dem Programm nicht zur Verfügung. Auf dem Auszug der Verfahrensliste sei im Übrigen vermerkt: „Eingestellt mangels Schuldfähigkeit".

Schon die in Bayern praktizierte Eintragung von Kindern ins Js-Register, das Register der Staatsanwaltschaften für Straf- und Bußgeldsachen, erscheint datenschutzrechtlich nicht unproblematisch, selbst wenn sich aus den gespeicherten Daten ergeben würde, dass es sich bei dem betroffenen Kind nicht um einen Beschuldigten handelt. Es besteht nämlich die Möglichkeit der Eintragung des Vorgangs in das sog. AR-Register, in das alle Mitteilungen einzutragen sind, die nicht auf die Einleitung eines Strafverfahrens abzielen oder bei denen zweifelhaft ist, in welches Register sie einzutragen sind. Auf jeden Fall ist aber die Zuweisung eines Beschuldigtenstatus an strafunmündige Kinder abzulehnen, weil strafunmündige Kinder keine Beschuldigten im rechtlichen Sinne sind und deshalb ihre Speicherung unter diesem Status unzutreffend und damit unzulässig ist (vgl. § 489 Abs. 1 StPO). Rein technische Umstände, wie die Notwendigkeit der Änderung des Vorgangsverwaltungsprogramms zur korrekten Speicherung von Strafunmündigen oder die Anfügung eines die unzutreffende Speicherung erläuternden Vermerks können diesen Mangel nicht beheben.

Ich halte es deshalb für erforderlich, dass strafunmündige Kinder unter einem anderen Status gespeichert werden, der ihrem materiell-rechtlichen bzw. strafprozessualen Status entspricht. Aufgrund der Tatsache, dass die Strafunmündigkeit durch den Vermerk „Eingestellt mangels Schuldunfähigkeit" jedenfalls für die zugriffsberechtigten Justizangehörigen erkennbar sein dürfte, sehe ich von weiteren Maßnahmen ab.

6.3.5 Förmliche Verpflichtung bei Übermittlung personenbezogener Informationen aus Strafakten an private Forschungseinrichtungen

Die Erforderlichkeit einer förmlichen Verpflichtung von privaten Forschern, die personenbezogene Daten von Staatsanwaltschaften erhalten, ergibt sich aus § 476 Abs. 1 Nr. 1, Abs. 3 Satz 1, letzter Halbsatz StPO. § 476 Abs. 3 Satz 2 StPO verweist ausdrücklich auf § 1 Abs. 4 Nr. 2 Verpflichtungsgesetz, wonach diejenige Behörde die für die Verpflichtung zur Geheimhaltung zuständig ist, von der Landesregierung durch Rechtsverordnung bestimmt wird. Die förmliche Verpflichtung dient dem Schutz des Persönlichkeitsrechts desjenigen, dessen personenbezogene Daten in den Akten der Staatsanwaltschaften gespeichert sind. Eine (wirksame) förmliche Verpflichtung würde für den Fall, dass der Forscher Privatgeheimnisse verletzte, eine Strafbarkeit gemäß § 203 Abs. 2 Nr. 6 StGB nach sich ziehen. Auf meine Anfrage beim Staatsministerium der Justiz, wen die Landesregierung durch Rechtsverordnung als für die Verpflichtung zuständige Behörde bestimmt hat, wurde mir mitgeteilt, dass grundsätzlich für die Verpflichtung die Stelle zuständig sei, die auch für die Entscheidung über die Auskunftserteilung oder die Bewilligung von Akteneinsicht zu entscheiden habe, mithin also die Staatsanwaltschaften bzw. das mit der Sache befasste Gericht. Eine bayerische Zuständigkeitsverordnung gebe es insoweit nicht. Dies entspreche auch dem Regelungszustand in den anderen Bundesländern. Da bislang Schwierigkeiten in der Praxis nicht aufgetreten seien, werde kein Handlungsbedarf gesehen.

Der Hinweis auf die in der Praxis nicht bekannt gewordenen Probleme ist angesichts der eindeutigen Rechtslage ohne Relevanz. Eine Verpflichtung durch eine aufgrund praktischer Erwägungen aber ohne ausreichende Rechtsgrundlage handelnde Stelle ist rechtlich nicht wirksam und dürfte auch nicht den vom Gesetzgeber durch die Strafbarkeitsfolge des § 203 Abs. 2 Nr. 6 StGB beabsichtigten Schutz auslösen. Die Haltung des Staatsministeriums der Justiz ist deshalb für mich nicht verständlich. Auch andere Bundesländer, beispielsweise Hamburg und Hessen hatten dieses Problem erkannt und haben mittlerweile eine entsprechende Verordnung erlassen. Ich sehe im Gegensatz zum Staatsministerium der Justiz dringenden Handlungsbedarf und habe gefordert, dass entweder auch in Bayern eine entsprechende Regelung in die Wege geleitet wird oder aber Datenübermittlungen an private Stellen zu Forschungszwecken generell ausgeschlossen werden.

6.3.6 Aktenübersendung der Staatsanwaltschaften an meine Behörde

Gemäß Art. 9 Bayerisches Datenschutzgesetz (BayDSG) kann sich jeder an den Landesbeauftragten für den Datenschutz mit dem Vorbringen wenden, bei der Erhebung, Verarbeitung oder Nutzung seiner personenbezogenen Daten durch öffentliche Stellen in seinen Rechten verletzt worden zu sein. Wenn mir Petenten unter Schilderung eines konkreten Sachverhalts Anhaltspunkte für Datenschutzverletzungen durch die Speicherung strafrechtlicher Vorgänge in polizeilichen Dateien benennen, benötige ich für meine datenschutzrechtliche Überprüfung regelmäßig die der Speicherung zugrundeliegenden staatsanwaltschaftliche Ermittlungsakten. Die Übersendung der von mir angeforderten Akten durch die aktenführenden Justizbehörden erfolgt leider nicht unmittelbar an mich, sondern auf dem Dienstweg über das Staatsministerium der Justiz. Von dort erhalte ich die Akten in der Regel nicht vor Ablauf eines Monats seit der

Anforderung, in nicht wenigen Fällen dauert die Aktenübersendung auch erheblich länger. Dies verzögert die Bearbeitung der der Anforderung zugrunde liegenden Eingabe durch mich in einer für den Petenten nicht zumutbaren Weise.

Obwohl die Pflicht zur Unterstützung meiner Behörde und damit die Verpflichtung zur Übersendung der angeforderten Akten nach Art. 32 BayDSG die jeweilige speichernde Stelle selbst betrifft, habe ich in den seinerzeitigen Verhandlungen zugestimmt, dass die Zuleitung von Verfahrensakten der Justiz auf dem Dienstweg erfolgt. Dabei bin ich allerdings davon ausgegangen, dass eine Übersendung der Akten in einem angemessenen Zeitraum erfolgt. Da dies in der Regel nicht der Fall ist, habe ich das Staatsministerium der Justiz bereits mehrfach darum gebeten, dass die Akten - wie in anderen Geschäftsbereichen auch - durch die aktenführende Stelle unmittelbar an mich übersandt werden. Dies würde nicht nur die Dauer der Zuleitung verkürzen, sondern auch die Arbeitsbelastung der bisher mit der Übersendung befassten Dienststellen (Staatsanwaltschaft, Generalstaatsanwaltschaft, Justizministerium) reduzieren. Da Gegenstand meiner Prüfung, für die ich die Justizakten benötige, fast ausschließlich nicht Maßnahmen der Justizbehörden, sondern regelmäßig polizeiliche Speicherungen sind, ist auch im Hinblick auf die vom Staatsministerium der Justiz ausgeübte Dienstaufsicht über die Justizbehörden der bisherige arbeitsaufwendige, zeitraubende und auch unübliche Weg der Aktenübersendung auf dem Dienstweg nicht notwendig.

Das Staatsministerium der Justiz hat eine solche Änderung bisher abgelehnt, gleichwohl aber die Leiter der Staatsanwaltschaften gebeten, für eine zügige Aktenübersendung zu sorgen. Eine signifikante Besserung ist trotz dieser Bitte aber nicht zu erkennen. Das Verfahren bedarf deshalb im Interesse einer zügigen Bearbeitung von Eingaben dringend der Änderung.

6.4 Justizvollzug

Die im Juni und Juli 2006 vom Bundestag und Bundesrat beschlossene Föderalismusreform hat u.a. die Verteilung der Gesetzgebungskompetenz von Bund und Ländern sowie die Zuständigkeiten und Mitwirkungsrechte der Länder bei der Gesetzgebung des Bundes zum Inhalt. Sie ist am 1. September 2006 in Kraft getreten. Danach liegt künftig die ausschließliche Gesetzgebungskompetenz für den Strafvollzug bei den Ländern. Dies gilt auch für den Jugendstrafvollzug, für den das Bundesverfassungsgericht in seiner Entscheidung vom 31. Mai 2006 die Schaffung einer spezifischen gesetzlichen Grundlage gefordert hat. Hierzu hat das Bundesverfassungsgericht dem Gesetzgeber eine Frist bis Ende 2007 gesetzt. Nach meiner Kenntnis gibt es bereits einen bayerischen Diskussionsentwurf eines Gesetzes über den Vollzug der Freiheitsstrafe, der Jugendstrafe und der Sicherungsverwahrung (Bayerisches Strafvollzugsgesetz - BayStVollzG). Dieser ist mir bisher leider vom Staatsministerium der Justiz noch nicht zur datenschutzrechtlichen Beurteilung zugeleitet worden. Sobald dies der Fall sein wird, werde ich den Entwurf einer umfassenden datenschutzrechtlichen Prüfung unterziehen. Dabei werde ich insbesondere auf einen hohen datenschutzrechtlichen Standard achten und mich dafür einsetzen, dass keine Reduzierung des bisherigen bundesrechtlich geregelten Datenschutzniveaus erfolgt. Dies gilt insbesondere für die Vorschriften zur Erhebung, Verarbeitung, Nutzung und Zweckbindung von Daten, den Schutz besonders sensibler Daten, Berichtigungs- und Löschungsvorschriften, sowie für Regelungen zur Überwachung des Besuchs- und Schriftverkehrs. Dabei werde ich auch die Erfahrungen aus meinen datenschutzrechtlichen Prüfungen von Justizvollzugsanstalten einbringen.

6.4.1 Zentrale Vollzugsdatei

Wie bereits in meinem 21. Tätigkeitsbericht (Nr. 9.4.1) dargelegt, hat das Staatsministerium der Justiz eine Zentrale Vollzugsdatei Bayern (ZVD) auf der Grundlage von §§ 179 ff. Strafvollzugsgesetz aufgebaut. Diese Datei ist nunmehr endgültig freigegeben worden. Polizei, Staatsanwaltschaften, Strafgerichte und Justizvollzugsanstalten können im Rahmen ihrer Aufgaben in Ermittlungs-, Straf- und Strafvollstreckungsverfahren sowie im Strafvollzug auf die Datei zugreifen. Die Datenkommunikation zwischen den beteiligten Behörden erfolgt automatisiert über das Justiznetz. Neuzugänge und Veränderungen der Datei werden im Rahmen der gesetzlichen Mitteilungspflichten zeitgleich automatisiert an das Bayerische Landeskriminalamt übermittelt und in das dortige INPOL-System übernommen.

Rechtsgrundlage für die Datenübermittlungen bezüglich Beginn, Unterbrechung und Beendigung von Freiheitsentziehungen durch die Justizvollzugsanstalt an das Landeskriminalamt ist § 180 Abs. 4 Satz 2 Strafvollzugsgesetz i.V.m. § 13 Abs. 1 Satz 3 Bundeskriminalamtsgesetz. Die Übermittlung der aus erkennungsdienstlichen Maßnahmen der JVA erlangten Daten ist zulässig gemäß § 86 Abs. 2 Satz 2 Strafvollzugsgesetz. Als Rechtsgrundlage einer Übermittlung weiterer Daten kommt § 180 Abs. 2 Nr. 2 und Nr. 4 Strafvollzugsgesetz in Betracht.

Ich halte die Übermittlung von sog. Sicherheitsvermerken, die Beschreibungen wie „gewalttätig“ u.a. enthalten, nur im Einzelfall, soweit sie für ein Ermittlungsverfahren oder zum Zweck der Abwehr konkreter Gefahren benötigt werden, gemäß § 180 Abs. 2 Nr. 2 und Nr. 4 Strafvollzugsgesetz für zulässig. Das

Staatsministerium der Justiz ist anderer Ansicht. Die generelle Übermittlung der Sicherheitsvermerke sei notwendig, weil die Justiz im Gegensatz zur Polizei nach Abschluss des Strafverfahrens über qualitativ und quantitativ bessere Informationen zur Persönlichkeit der Täter verfüge. Die Sicherheitsvermerke dienten z.B. im Rahmen der Auswertung von Aktenbeständen oder Informationen aus dem Informationssystem der Polizei auch zur Einschätzung von Tatverdächtigen in aktuellen Ermittlungsverfahren. Daneben dienten sie dem Schutz von Leib und Leben der Polizeibeamten in den Fällen, in denen entflohene und nicht wieder zurückgekehrte Häftlinge in die Justizvollzugsanstalt zurückgeführt werden müssen oder wenn die Polizei Gefangene während einer Hafterleichterung kontrolliert.

Ich meine, dass für eine Übermittlung der Sicherheitsvermerke sämtlicher inhaftierter Personen kein Anlass besteht, nachdem in keiner Weise ersichtlich ist, von welchen dieser Personen künftig konkrete Gefahren ausgehen oder gegen welche erneut wegen Straftaten ermittelt werden wird. Die fehlende Erforderlichkeit einer generellen Datenübermittlung ergibt sich insbesondere aus der Anzahl der Entweichungen und Ausbrüche, die in den Jahren 2004 und 2005 jeweils bei ca. 10 Entweichungen und 0 Ausbrüchen lag. Soweit die Übermittlung dem Schutz von Leib und Leben von Polizeibeamten in den Fällen der Rückführung entwichener Häftlinge, der Vernehmung von Häftlingen und der Kontrolle dieser Personen während einer Hafterleichterung dienen soll, müsste im Einzelfall das Vorliegen der Voraussetzungen des § 180 Abs. 2 Nr. 2 oder Nr. 4 Strafvollzugsgesetz festgestellt werden. Insbesondere im Falle von Hafterleichterungen dürften diese grundsätzlich nicht vorliegen, da nach der gesetzlichen Regelung des § 11 Abs. 2 Strafvollzugsgesetz Gefangenen, von denen die konkrete Gefahr erneuter Straftaten ausgeht, keine Vollzugslockerungen genehmigt werden dürfen. Die generelle Datenübermittlung zum Zwecke der Vorratsdatenspeicherung ist deshalb aus meiner Sicht unzulässig.

Insbesondere sog. gesundheitsbezogene Sicherheitsvermerke (z.B. „Ansteckungsgefahr“) unterliegen als Daten, die einem Arzt i.S.v. § 203 Abs. 1 StGB anvertraut wurden, einem strengen Schutz. Für sie gilt die strenge Zweckbindung des § 182 Abs. 2 (für den Berufsgeheimnisträger) und Abs. 3 Strafvollzugsgesetz (für die JVA). Die Übermittlung dieser sensiblen Gesundheitsdaten an die Polizei kann für den Fall der konkreten Entweichung zum Zwecke der Eigensicherung, der Gefahrenabwehr oder auch zum Schutz des Entwichenen zulässig sein. Eine generelle Übermittlung ist dagegen nicht gerechtfertigt.

Das Staatsministerium der Justiz hat trotz meiner Bedenken die Zentrale Vollzugsdatei ohne Änderung in diesem Punkt freigegeben.

6.4.2 Nutzung des Vollzugsgeschäftsstellenprogramms ADV-Vollzug

Bereits in meinem 20. Tätigkeitsbericht (Nr. 8.3.6) hatte ich über das Informationssystem ADV-Vollzug berichtet. Ich habe die fehlende Beschränkung des Zugriffs für die Bediensteten auf die Daten der Gefangenen, für die sie dienstlich zuständig sind, leider im Hinblick auf die vom Staatsministerium der Justiz angeführte hohe Fluktuation bei Gefangenen und Personal sowie der Vielzahl unterschiedlicher Aufgaben der Bediensteten nicht durchsetzen können. Umso wichtiger ist unter Gesichtspunkten der Prävention und der Nachvollziehbarkeit eine vollständige Protokollierung sämtlicher Zugriffe auf die Daten im Verfahren ADV-Vollzug. Bei einer Prüfung in einer Justizvollzugsanstalt habe ich festgestellt, dass eine Protokollierung der Zugriffe nur dann erfolgt, wenn Daten verändert, eingetragen oder gelöscht werden. Eine Protokollierung lesender Zugriffe auf die gespeicherten Daten erfolgt nicht.

Ich habe dies gegenüber dem Staatsministerium der Justiz und der Justizvollzugsanstalt bemängelt. Mir wurde entgegengehalten, dass der Schutz der Daten vor unbefugtem Zugriff durch die Kontrolle des Zugangs zu den Rechnern und des Zugriffs auf die Anwendungsprogramme gewährleistet werde. Außerdem lägen bisher keine Erkenntnisse vor, dass Bedienstete des Bayerischen Justizvollzugs gegen ihre Pflichten verstoßen und sich unzulässig Informationen über Gefangene beschafft hätten. Diese Argumentation überzeugt nicht. Eine personengebundene Beschränkung der Zugriffsmöglichkeiten für die einzelnen Bediensteten erfolgt nicht, so dass von einer individuellen Zugangskontrolle nicht die Rede sein kann. Zweckfremde Nutzung kann bislang mangels Überprüfungsmöglichkeit kaum bekannt werden, so dass eine Berufung auf fehlende Kenntnis wenig hilfreich ist. Eine Protokollierung hat präventive Wirkung und ermöglicht ggf. die Sanktionierung unzulässiger Datenabfragen. Dies gilt umso mehr vor dem Hintergrund, dass in dem Informationssystem ADV-Vollzug auch sensible Gesundheitsdaten, die grundsätzlich der in § 203 Abs. 1 Nr. 1 StBG sanktionierten Schweigepflicht unterliegen, in Form von sog. Sicherheitsvermerken gespeichert werden (vgl. 20. Tätigkeitsbericht Nr. 8.3.5.1).

Das Staatsministerium der Justiz hat sich zwischenzeitlich zumindest zu einer beschränkten Protokollierung lesender Zugriffe bereit erklärt.

6.4.3 Gesundheitsdatenübermittlung innerhalb einer Justizvollzugsanstalt

Wie ich bereits in meinem 20. Tätigkeitsbericht (Nr. 8.3.5.1) ausgeführt habe, unterliegen auch die Erkenntnisse des Anstaltsarztes in einer Justizvoll-

zugsanstalt grundsätzlich der in § 203 Abs. 1 Nr. 1 StGB sanktionierten ärztlichen Schweigepflicht. Bei der Prüfung in einer Justizvollzugsanstalt habe ich festgestellt, dass eine schriftliche Regelung dieses sensiblen Bereichs nicht existiert. Der Anstaltsleiter teilte mir dazu mit, es gebe aber eine Absprache, nach der bei ansteckenden Krankheiten von erheblichem Gewicht der Anstaltsleiter, sein Vertreter und die für die Betreuung des infizierten Gefangenen zuständigen Sozialarbeiter zum Zwecke des Schutzes der eigenen Gesundheit und auch der anderen in der Justizvollzugsanstalt befindlichen Personen informiert würden. Der stellvertretende Anstaltsleiter würde ferner den Vollzugsgeschäftsstellenverwalter informieren, damit in den Gefangenenpersonalakt und die EDV ein entsprechender Sicherheitsvermerk eingetragen werde. Derartige Sicherheitsvermerke könnten im Rahmen der allgemeinen Zulassung zur Nutzung der EDV eingesehen werden.

Aus datenschutzrechtlicher Sicht sollte im Hinblick auf die Sensibilität der Gesundheitsdaten der Gefangenen und zur Verbesserung der Rechtssicherheit eine schriftliche Regelung erfolgen, in welchen Fällen Erkrankungen offenbart werden. Im Hinblick auf den besonderen Schutz von Gesundheitsdaten gemäß § 182 Strafvollzugsgesetz erscheint es zudem problematisch, dass Sicherheitsvermerke mit Gesundheitsbezug von sämtlichen Bediensteten einer Justizvollzugsanstalt sowohl in der Vollzugsdatei wie auch in der Gefangenenpersonalakte eingesehen werden können. Nach Ansicht der Justizvollzugsanstalt sei sowohl im Hinblick auf die Behandlung der Gefangenen als auch die Ordnung der Anstalt eine Beschränkung der Einsichtnahme in diese Vermerke auf einzelnen Bedienstete oder eine bestimmte Gruppe von Bediensteten nicht sachgerecht. Sie wäre zudem mit der Organisationsstruktur einer Justizvollzugsanstalt nicht vereinbar. Eine schriftliche Regelung der Fälle, in denen Erkrankungen von Gefangenen offenbart werden, sei in Vorbereitung. Das Staatsministerium der Justiz teilt die Ansicht der Justizvollzugsanstalt, dass der Anstaltsleiter im Hinblick auf seine Gesamtverantwortung für seine Anstalt, insbesondere die ihm unterstellten Beschäftigten, die ihm anvertrauten Gefangenen und ggf. für Dritte in der Lage sein muss, auch gesundheitsbezogene Daten zu offenbaren. Eine Beschränkung der Einsichtnahme in Sicherheitsvermerke auf einzelne, womöglich namentlich bestimmte Beschäftigte sei nicht praktikabel.

Angesichts dieser Argumentation und der fehlenden Beschränkung des Zugriffs auf Gefangenenpersonalakten und automatisiert gespeicherte Daten für Justizvollzugsbedienstete, halte ich es für dringend, dass eine nachprüfbare Dokumentation erfolgt, welcher Bedienstete zu welchem Zweck und zu welchem Zeitpunkt Einsicht in die EDV und die Gefangenenpersonalakten genommen hat (siehe hierzu auch Nr. 6.4.2).

6.4.4 Überwachung und Aufzeichnung des Besucherverkehrs mittels Videokamera

In vier bayerischen Justizvollzugsanstalten werden Besuchsräume videoüberwacht und Aufzeichnungen gefertigt. Auf meine Nachfrage nannte das Staatsministerium der Justiz als Rechtsgrundlage §§ 27 Abs. 1 Satz 1, 81 Abs. 2 StVollzG, Art. 16 Abs. 2 Satz 2 Nr. 2 a BayDSG und das Hausrecht.

Ich meine, dass eine bloße Echtzeitüberwachung ohne Aufzeichnung der Überwachung durch einen anwesenden Bediensteten der Justizvollzugsanstalt gleichzustellen ist und damit auf § 27 Abs. 1 StVollzG gestützt werden kann. Eine Rechtsgrundlage für die Fertigung von Aufzeichnungen ist § 27 Abs. 1 StVollzG hingegen nicht. Auch wenn die Art und Weise der Überwachung der Anstalt überlassen ist, müsste die Möglichkeit des Einsatzes von Videoaufzeichnungen zu diesem Zweck ausdrücklich geregelt sein, da sie im Vergleich zur bloßen Überwachung durch einen anwesenden Bediensteten einen zusätzlichen Eingriff von erhöhter Intensität darstellt. Sie kann auch nicht auf andere Vorschriften wie § 81 Abs. 2 StVollzG oder Art. 16 Abs. 2 BayDSG gestützt werden, da § 27 Abs. 1 StVollzG die Überwachung der Besuche abschließend regelt.

Auch das Hausrecht rechtfertigt Videoaufzeichnungen von Gefangenenbesuchen nicht. Das Strafvollzugsgesetz enthält eine abschließende Regelung der zulässigen Eingriffe durch Bedienstete von Justizvollzugsanstalten in die Rechte Strafgefangener. Eine Heranziehung des Hausrechts zur Begründung solcher Eingriffe ist daher nicht möglich.

Ich habe das Staatsministerium der Justiz bisher vergeblich dazu aufgefordert, Videoaufzeichnungen des Besuchsverkehrs durch die Justizvollzugsanstalten zu unterbinden, solange dafür keine spezielle ausdrückliche gesetzliche Regelung existiert. Es hat sich jedoch lediglich, um meinen Bedenken wenigstens teilweise Rechnung zu tragen, dazu bereit erklärt, die Justizvollzugsanstalten aufzufordern, die im Rahmen von Besuchen angefertigten Videoaufzeichnungen nach dem Ablauf von zehn Tagen und nicht wie bisher teilweise erst nach 2 Monaten zu löschen. Die Aufzeichnung wird aber leider ohne ausreichende Rechtsgrundlage weiter fortgeführt.

Bei der Prüfung einer Justizvollzugsanstalt habe ich festgestellt, dass sowohl der Besuchsraum durch drei Kameras als auch die Besucherterrasse überwacht und Aufzeichnungen gefertigt werden. Ein Hinweis auf die Videoüberwachung erfolgt nicht. Unabhängig von der grundsätzlichen Frage der Rechtmäßigkeit

derartiger Aufzeichnungen ist jedenfalls auf die Videoüberwachung durch Hinweisschilder im Besuchsraum und auf der Besuchsterrasse hinzuweisen. Dies gilt auch für Videoüberwachung mittels Echtzeitübertragung ohne Aufzeichnung. Entsprechende Hinweise wurden auf meine Aufforderung hin von der Justizvollzugsanstalt angebracht.

6.4.5 Datenübermittlung durch Bezirkskrankenhäuser an die örtlichen Polizeidienststellen

Die Unterbringung in einer Anstalt des Maßregelvollzugs wird durch das Gericht insbesondere dann angeordnet, wenn eine Tat im Zustand der Schuldunfähigkeit oder verminderten Schuldfähigkeit begangen wurde und eine Gesamtwürdigung ergibt, dass vom Täter infolge seines Zustands erhebliche rechtswidrige Taten zu erwarten sind und er deshalb für die Allgemeinheit gefährlich ist.

Das Staatsministerium des Innern hat im Rahmen der Umsetzung von Maßnahmen zur Verbesserung des Informationsaustauschs zwischen Maßregelvollzugseinrichtungen und der Polizei verschiedene Informationsverpflichtungen vorgesehen. Zum einen ist bei Beginn, Fortsetzung, Unterbrechung und Beendigung einer gerichtlich angeordneten Freiheitsentziehung die für das psychiatrische Krankenhaus örtlich zuständige Polizeiinspektion zu unterrichten. Diese leitet die Daten an das Landeskriminalamt weiter. Diese Information der örtlichen Polizei erfolgt bei allen in der Maßregelvollzugseinrichtung Untergebrachten, unabhängig davon, ob bei ihnen ein besonderes Sicherungsbedürfnis vorliegt oder nicht. Das Staatsministerium des Innern begründet diese Datenübermittlung damit, dass sie eine unverzichtbare Grundlage für polizeiliche Lagebeurteilung sowie für die vorbereitende Entscheidung über die zu treffenden polizeilichen Maßnahmen insbesondere für den Fall einer Entweichung sei. Der örtlich zuständigen Polizeidienststelle müssten die Informationen über Maßregelvollzugspatienten bereits vor dem Entweichen zur Verfügung stehen. Sie müsse in die Lage versetzt werden, die Informationen mit eigenen, für den Fall des Entweichens wichtigen Erkenntnissen zu einem personenbezogenen Konzept anzureichern.

Ich halte eine generelle Datenübermittlung bezüglich aller Maßregelvollzugspatienten an die örtlich zuständige Polizeidienststelle im Vorfeld von Gefahren für eine unzulässige Vorratsdatenspeicherung. Nach den mir bekannten Zahlen stellt eine Entweichung die Ausnahme dar, so dass die örtliche Polizeidienststelle die Informationen über die Aufnahme des Patienten in den meisten Fällen nicht benötigen wird. Anlässlich einer Prüfung bei einer örtlichen Polizeidienststelle habe ich festgestellt, dass die Polizei selbst bei der Bearbeitung der Informationen des Bezirkskrankenhauses zwischen Patienten mit und ohne besonderem Sicherungsbedürfnis unterscheidet. Bei Patienten ohne besonderes Sicherungsbedürfnis werden die Informationen lediglich namentlich sortiert und in Aktenordnern abgelegt. Die Erforderlichkeit einer vorsorglichen Datenübermittlung erscheint mir jedenfalls bei diesen Patienten nicht gegeben. Im Falle der tatsächlichen Entweichung wird die Polizei ohnehin per Fax oder E-Mail informiert. Die generelle Information des Landeskriminalamts über Maßregelvollzugspatienten zur Einstellung in die Haftdatei kann unmittelbar durch das Bezirkskrankenhaus erfolgen. Mein Schriftwechsel mit dem Staatsministerium des Innern dazu dauert noch an.

Darüber hinaus habe ich bei der Prüfung eines Bezirkskrankenhauses festgestellt, dass von allen Patienten im Maßregelvollzug erkennungsdienstliche Unterlagen erstellt und im Fall einer Entweichung an die Polizei übermittelt werden. Außerdem werden diese Unterlagen im Fall der Entlassung bei Personen mit besonderem Sicherungsbedürfnis an die für das Bezirkskrankenhaus örtlich zuständige Polizeidienststelle übermittelt, die diese an das Landeskriminalamt zur Einstellung in INPOL weiterleitet.

Ich halte es nicht für erforderlich, dass die erkennungsdienstlichen Unterlagen vom Bezirkskrankenhaus an die örtlich zuständige Polizeiinspektion zur Weiterleitung an das Landeskriminalamt übermittelt werden. Die örtlich zuständige Polizeidienststelle fungiert in diesem Fall quasi nur als Bote, da die erkennungsdienstlichen Unterlagen nach Entlassung der Patienten für ihre Aufgabenerfüllung nicht erforderlich sind. Ihre Einschaltung sollte deshalb unterbleiben.

Die erkennungsdienstliche Behandlung wird, weil eine gesetzliche Grundlage für diese Maßnahme nicht besteht, mit Einwilligung der Patienten durchgeführt. Das dazu verwendete Formblatt entspricht jedoch nicht den datenschutzrechtlichen Anforderungen. Die Maßnahme kann nur dann auf die Einwilligung gestützt werden, wenn diese von einem voll informierten, einwilligungsfähigen Betroffenen freiwillig abgegeben wird. Wegen der Überarbeitung des Formblatts habe ich mich an das für Bezirkskrankenhäuser zuständige Staatsministerium für Arbeit und Sozialordnung, Familie und Frauen, gewandt. Dieses hat meinen Anregungen Folge geleistet und das Formblatt entsprechend neu gefasst. Insbesondere wird der Patient nun darauf hingewiesen, dass keine gesetzliche Grundlage für eine erkennungsdienstliche Behandlung existiert und sie deshalb nur mit seiner Einwilligung erfolgen kann, die Einwilligung freiwillig ist, ohne Angabe von Gründen verweigert und jederzeit, auch nach der Entlassung des Patienten, widerrufen werden kann. Die Einverständniserklärung ist nur dann wirksam, wenn der Patient den Inhalt und die Auswirkungen seiner Erklärung auch

verstehen kann. Vor Abgabe der Einwilligungserklärung hat das Bezirkskrankenhaus deshalb zu prüfen, ob beim Patienten eine ausreichende Einwilligungsfähigkeit besteht. Der Patient wird bisher aber weder von der Übermittlung der erkennungsdienstlichen Unterlagen an die Polizei noch über die Speicherung in polizeilichen Dateien unterrichtet. Auch diese Unterrichtung ist für die Wirksamkeit der Einwilligung von Bedeutung. Das für den Bereich der polizeilichen Informationserhebung und -verarbeitung zuständige Staatsministerium des Innern steht deshalb in der Pflicht, die Erforderlichkeit der erkennungsdienstlichen Behandlung aller Maßregelvollzugspatienten, die vorgesehenen Übermittlungen der gewonnenen Unterlagen und Dateispeicherungen zu begründen und einen Textvorschlag für die Information der Patienten vorzulegen.

6.5 Ordnungswidrigkeitenverfahren

6.5.1 Lichtbildabgleich in Bußgeldverfahren

Bereits in meinem 21. Tätigkeitsbericht (Nr. 9.5.1) hatte ich über die Zulässigkeitsvoraussetzungen eines Lichtbildabgleichs mit dem Pass- bzw. Personalausweisregister zur Verfolgung von Ordnungswidrigkeiten im Straßenverkehr berichtet.

Im Rahmen der datenschutzrechtlichen Überprüfung zahlreicher Eingaben zu dieser Thematik sowie anlässlich eines Prüftermins in der Zentralen Verkehrsordnungswidrigkeitenstelle (Zentrale VOWi-Stelle) im Bayerischen Polizeiverwaltungsamt habe ich den Eindruck gewonnen, dass die materiellen Voraussetzungen für einen Zugriff auf die von der Pass- bzw. Personalausweisbehörde gespeicherten Lichtbilder weitgehend Beachtung finden. Eine abschließende Beurteilung, ob die Daten bei dem Betroffenen nicht erhoben werden konnten oder nur mit unverhältnismäßig hohem Aufwand hätten erhoben werden können, war mir bisher allerdings wegen der häufig mangelhaften Dokumentation in den Akten nicht möglich. Aufgrund der Vielzahl der Fälle und des bereits verstrichenen längeren Zeitraums konnten sich die Sachbearbeiter oft nicht mehr an die einzelnen Sachverhalte und die von ihnen veranlasste Maßnahmen erinnern.

Gem. §§ 22 Abs. 3 Passgesetz bzw. 2 b Abs. 3 Personalausweisgesetz jeweils i.V.m. Art. 14 Nr. 1 BayAG Passgesetz haben Polizeibehörden den Anlass des Ersuchens und die Herkunft der übermittelnden Daten und Unterlagen zu vermerken sowie den Namen und die Anschrift des Betroffenen unter Hinweis auf den Anlass der Übermittlung aufzuzeichnen. Aufgrund dieser Dokumentationspflicht hat die ersuchende Polizeibehörde - schon im Hinblick auf einen späteren Nachweis - aktenkundig zu machen, wodurch sie die Voraussetzungen des §§ 22 Abs. 2 Passgesetz bzw. 2 b Abs. 2 Personalausweisgesetz erfüllt sieht. Deshalb müssen sich aus der Akte insbesondere ergeben:

- das Datum der Anordnung,
- die Person des ersuchenden Bediensteten,
- die ersuchte Behörde,
- der Grund dafür, dass die Daten beim Betroffenen nicht erhoben werden konnten bzw. nur mit unverhältnismäßig hohem Aufwand hätten erhoben werden können.

Für die Dokumentation des Grundes genügt ein allgemeiner Hinweis wie z.B. „der Betroffene konnte nicht erreicht werden“ nicht, da daraus nicht deutlich wird, ob die Polizeibehörde z.B. versucht hat, den Betroffenen auf eine Art und Weise und zu einer Zeit zu erreichen, die als geeignet angesehen werden kann (z.B. nicht nur einmaliger Anruf in der Privatwohnung des Betroffenen während der üblichen Arbeitszeiten). Die Polizeibehörde muss vielmehr dokumentieren, zu welchem Zeitpunkt bzw. welchen Zeitpunkten und auf welche Weise sie versucht hat, den Betroffenen zu erreichen.

Ich habe das Staatsministerium des Innern im Hinblick auf eine Reihe unzureichender Dokumentationen aufgefordert dafür Sorge zu tragen, dass künftig die dargestellten Anforderungen an die Dokumentation von Lichtbildabgleichen beachtet werden. Das Staatsministerium des Innern hat daraufhin das Formular für Schreiben der Zentralen VOWi-Stelle im Bayerischen Polizeiverwaltungsamt anlässlich einer Fahrerermittlung an die örtliche Polizeiinspektion dahingehend abgeändert, dass für den Fall einer Lichtbildanforderung bei der Pass-/Personalausweisbehörde unbedingt dokumentiert werden muss, wann und wie der Betroffene versucht wurde zu erreichen und an welchem Datum die Übersendung des Lichtbildes bei welcher Behörde beantragt worden ist. Die Angaben sind mit Ort, Datum und Unterschrift des anordnenden Beamten zu versehen. Diese Änderung stellt eine begrüßenswerte datenschutzrechtliche Verbesserung dar.

6.5.2 Speicherung von Fahrverboten in örtlichen Fahrerlaubnisregistern

Ein Petent hat mir mitgeteilt, ihm sei vom zuständigen Landratsamt die Auskunft erteilt worden, dass ein vor mehr als zehn Jahren gegen ihn verhängtes einmonatiges Fahrverbot seit der damaligen Eintragung im Computer des Landratsamts immer noch dort zu finden sei und nicht mehr gelöscht werde, obwohl die Tilgungsfrist für das im zentralen Fahrerlaubnisregister beim Kraftfahrt-Bundesamt gespei-

cherte Fahrverbot bereits abgelaufen war. Der örtliche Datenschutzbeauftragte habe ihm mitgeteilt, dass nach § 4 Abs. 1 StVG die Fahrerlaubnisbehörde im Rahmen ihrer örtlichen Zuständigkeit ein örtliches Fahrerlaubnisregister führe. In diesem Register würden die Daten über Fahrerlaubnisinhaber sowie über Personen, denen ein Verbot erteilt wurde, ein Fahrzeug zu führen, gespeichert. Im Straßenverkehrsgesetz sei geregelt, dass Sachverhalte, die im Verkehrszentralregister eingetragen waren und dort gelöscht wurden, nicht verwertet werden dürften. Daran halte sich das Landratsamt auch. Eine Verpflichtung zur Löschung solcher Daten sei hingegen nicht normiert und erfolge daher auch nicht.

Ich habe die Speicherung des Fahrverbots überprüft und bin zu folgendem Ergebnis gelangt:

Nach § 28 Abs. 3 Nr. 2 bis 4 StVG werden Daten über Entscheidungen die Fahrverbote anordnen, im Verkehrszentralregister gespeichert. Nach § 61 Abs. 3 Satz 1 StVG gilt, soweit die örtlichen Fahrerlaubnisregister Entscheidungen enthalten, die auch im Verkehrszentralregister einzutragen sind, für die Löschung § 29 StVG entsprechend. Danach unterliegen Eintragungen von Fahrverboten im örtlichen Fahrerlaubnisregister den Löschungsfristen des § 29 StVG. Das bedeutete für den vorliegenden Fall, dass das immer noch eingetragene einmonatige Fahrverbot zu löschen war. Ich habe daher das Landratsamt aufgefordert, die Löschung des im Computer vermerkten Fahrverbots zu veranlassen und dafür Sorge zu tragen, dass die dargelegten Grundsätze auch in anderen Fällen beachtet werden.

Das Landratsamt ist dieser Aufforderung gefolgt und hat die Speicherung des Fahrverbots gelöscht. Außerdem wurde vom zuständigen Abteilungsleiter eine Arbeitsanweisung erlassen, wonach bei Befassung mit einer Akte vor Eintritt in die Sachbearbeitung die entsprechenden Fristen zu überprüfen sind. Bei der Überschreitung der Frist sind die betreffenden Daten aus der Akte zu entfernen und die Löschung in der EDV durchzuführen. Außerdem wird derzeit vom Landratsamt die Möglichkeit überprüft, in einem automatisierten Verfahren in regelmäßigen Abständen die entsprechenden Daten zu löschen. Zusätzlich soll eine Liste erstellt werden, mit deren Hilfe auch die entsprechenden Aktenteile vernichtet werden können.

7 Vermessungsverwaltung

7.1 Änderung des Gesetzes über die Landesvermessung und das Liegenschaftskataster

Mit Gesetz vom 26.07.2005 wurde in Art. 11 Abs. 2 Vermessungs- und Katastergesetz (VermKatG) die Möglichkeit eines automatisierten Abrufverfahrens aus dem Liegenschaftskataster eingeführt. Die Einsichtnahme in das Liegenschaftskataster erlaubt eine Kenntnisnahme von wesentlichen personenbezogenen Grundstücksdaten (Angaben über die Gestalt, Größe und örtliche Lage des Grundstücks sowie darauf liegende Gebäude, den Eigentümer sowie den Inhaber von Erbbaurechten, Nutzungsart und Ertragsfähigkeit des Bodens) und stellt damit einen Eingriff in das Recht auf informationelle Selbstbestimmung des Betroffenen dar. Bei Ausgestaltung der gesetzlichen Regelung habe ich darauf hingewirkt, dass die wesentlichen Voraussetzungen für eine solche Einsichtnahme durch den Gesetzgeber selbst geregelt und dass - entsprechend der Forderung des Bundesverfassungsgerichts im sog. Volkszählungsurteil (BVerfGE 65, 1 ff., 44) - organisatorische und verfahrensrechtliche Vorkehrungen getroffen werden, um der Gefahr einer Verletzung des Persönlichkeitsrecht entgegenzuwirken. Dies gilt insbesondere für die Zweckbindung der übermittelten Daten, die Protokollierung der Abrufe und deren Kontrolle. Auszüge aus dem Liegenschaftskataster dürfen - soweit personenbezogene Daten weitergegeben werden - auf meine Forderung hin nur im Einzelfall mit Genehmigung der das Kataster führenden Behörde vervielfältigt, verbreitet oder wiedergegeben werden. Ich habe mich darüber hinaus dafür eingesetzt, dass bei der Erarbeitung der Verordnung nach Art. 11 Abs. 2 VermKatG zum automatisierten Abrufverfahren datenschutzrechtlichen Belangen Rechnung getragen wurde. So wurde aufgenommen, dass abgerufene und gespeicherte Daten zu löschen sind, wenn eine weitere Speicherung unzulässig oder sobald ihre Kenntnis für die abrufende Stelle zur Aufgabenerfüllung nicht mehr erforderlich ist. Außerdem wurde der Zusatz eingefügt, wonach die übermittelnde Stelle durch technische Maßnahmen sicherzustellen hat, dass Abrufe durch Teilnehmer nicht ohne Angabe des Abrufgrunds erfolgen und sich die Kontrolle der Abrufe durch die übermittelnden Stellen nach Art. 8 Abs. 3 Satz 3 Bayerisches Datenschutzgesetz richtet. Leider ist eine Beschränkung des Zugriffsrechts der Gemeinden auf ihr Gemeindegebiet, die ich aus datenschutzrechtlicher Sicht begrüßen würde, bislang nicht erfolgt, da sie nach Angaben des Staatsministeriums der Finanzen derzeit technisch und praktisch nicht umsetzbar und rechtlich nicht notwendig sei. Die Zulassung zu einem automatischen Zugriffsverfahren sollte aber durch den jeweiligen Aufgabenbereich, der sich bei Gemeinden regelmäßig auf das Gemeindegebiet beschränkt, begrenzt sein.

8 Gemeinden, Städte und Landkreise

8.1 Änderung des Gemeinde- und Landkreiswahlgesetzes

Im Berichtszeitraum wurde das Gemeinde- und Landkreiswahlgesetz geändert (Gesetz zur Änderung des Gemeinde- und Landkreiswahlgesetzes und anderer Vorschriften vom 26.07.2006, GVBl. S. 405). Aus datenschutzrechtlicher Sicht sind insbesondere die Aufnahme einer Regelung über Wahlhelferdateien, die Verpflichtung der bayerischen Behörden zur Benennung von Bediensteten zur Besetzung der Wahlvorstände und der Briefwahlvorstände sowie die Ersetzung der öffentlichen Auslegung des Wählerverzeichnisses durch ein Recht auf Einsichtnahme von Bedeutung. Durch diese Änderungen wurde das Kommunalrecht an entsprechende Vorschriften im Bundes- und Landeswahlrecht angepasst (vgl. hierzu auch 21. Tätigkeitsbericht 2004 Nr. 11.7 und 20. Tätigkeitsbericht 2002 Nr. 9.1). Die Rechtslage stellt sich zusammengefasst wie folgt dar:

Nach Artikel 6 Abs. 4 des Gemeinde- und Landkreiswahlgesetzes (GLKrWG) dürfen die in dieser Vorschrift abschließend aufgeführten Daten von Wahlberechtigten zum Zweck ihrer Berufung zu Mitgliedern von Wahlvorständen und Briefwahlvorständen erhoben, verarbeitet und genutzt werden. Die zu diesem Zweck erhobenen Daten dürfen auch für künftige Wahlen verarbeitet werden, sofern der Betroffene nicht widersprochen hat. Der Betroffene ist über das Widerspruchsrecht zu unterrichten. Die Unterrichtung umfasst dabei die Pflicht zur umfassenden Aufklärung der betroffenen Person, welche ihrer Daten für künftige Wahlen verarbeitet und genutzt werden und dass sie auch der Verarbeitung und Nutzung einzelner Daten widersprechen kann.

Artikel 6 Abs. 5 GLKrWG soll es den Gemeinden erleichtern, die Wahlvorstände und die Briefwahlvorstände zu besetzen. Nach dieser Vorschrift werden die öffentlichen bayerischen Stellen auf Ersuchen der Gemeinden zur Benennung von Bediensteten verpflichtet. Aus kompetenzrechtlichen Gründen ist die Übermittlungspflicht wie im Landeswahlrecht auf die bayerischen öffentlichen Stellen beschränkt.

Artikel 12 Abs. 2 GLKrWG ersetzt in Angleichung an das Bundes- (§ 17 BWG) und Landeswahlrecht (Art. 4 LWG) die bisher vorgeschriebene öffentliche Auslegung des Wählerverzeichnisses durch ein Recht zur Einsichtnahme in das Wählerverzeichnis. Wahlberechtigte dürfen danach grundsätzlich nur die zu ihrer Person im Wählerverzeichnis eingetragenen Daten einsehen. Daten von anderen im Wählerverzeichnis eingetragenen Personen dürfen sie nur dann einsehen, wenn sie Tatsachen glaubhaft machen, aus denen sich insoweit eine Unrichtigkeit oder eine Unvollständigkeit des Wählerverzeichnisses ergeben kann. Mit dem Verzicht auf die Auslegung des Wählerverzeichnisses wurde einer von mir schon seit längerem erhobenen Forderung nunmehr auch für das Kommunalwahlrecht Rechnung getragen (vgl. 19. Tätigkeitsbericht 2000 Nr. 8.2 und 20. Tätigkeitsbericht 2002 Nr. 9.1).

8.2 Reform des Personenstandsrechts

Am 22.06.2005 hat das Bundeskabinett den Entwurf eines Gesetzes zur Reform des Personenstandsrechts (Personenstandsrechtsreformgesetz) beschlossen, mit dem das geltende Personenstandsgesetz 1937 i.d.F. vom 08. August 1957 grundlegend reformiert werden soll. Der von der Bundesregierung beschlossene Gesetzentwurf wurde am 15.06.2006 dem Bundestag zur Beschlussfassung vorgelegt. Dem Entwurf war die Stellungnahme des Bundesrates sowie die Gegenäußerung der Bundesregierung beigefügt. Ziel des Entwurfs ist die Ablösung des geltenden Personenstandsgesetzes durch ein neues Personenstandsgesetz und die damit zusammenhängenden Änderungen sonstigen Bundesrechts unter Nutzung der elektronischen Möglichkeiten der Registerführung und Kommunikation mit dem Bürger sowie mit Behörden und anderen Stellen. Aus datenschutzrechtlicher Sicht sind insbesondere folgende Neuerungen von Bedeutung:

Anstelle der bisherigen Personenstandsbücher in Papierform sollen elektronisch geführte Personenstandsregister eingeführt werden; die Beurkundungsdaten sollen auf das für die Dokumentation erforderliche Maß beschränkt werden; das sog. Familienbuch, das nach jeder Eheschließung angelegt wird und mit dem Ehepaar „wandert“, soll abgeschafft werden; die Benutzung der Personenstandsbücher soll neugeordnet werden; auf Landesebene soll die Möglichkeit zur Einrichtung zentraler elektronischer Personenstandsregister bestehen und es soll eine rechtliche Grundlage für die Schaffung einer Testamentsdatei geschaffen werden.

Gegen eine elektronische Führung der Personenstandsregister habe ich aus datenschutzrechtlicher Sicht dann keine Bedenken, wenn eine regelmäßige elektronische Sicherung der Personenstandsregister erfolgt, diese Sicherungen zugriffs- und brandsicher aufbewahrt werden und aufgrund des Einsatzes der elektronischen Signatur keinerlei unberechtigte und unbemerkte Änderungen an den Registerdaten möglich sind.

Die beabsichtigte Abschaffung des Familienbuchs, das u.a. Daten über die Ehegatten und deren Eltern enthält, begrüße ich. Die Forderung nach einer Abschaffung dieses Buchs wurde von mir bereits im Jahr 1996 im Zusammenhang mit dem Vorentwurf

eines Fünften Gesetzes zur Änderung des Personenstandsgesetzes unterstützt. Für die Abschaffung des Familienbuchs liegen berechtigte Gründe vor; so ist vor allem die Nachfrage nach Personenstandsurkunden aus diesem Buch, das auch in der Bevölkerung weitgehend unbekannt ist, nur gering, da für öffentliche und private Vorlagezwecke meist Personenstandsurkunden aus dem Primärbuch (z.B. Geburtsurkunde aus dem Geburtenbuch) gefordert werden.

Aus Gründen der Datensparsamkeit und der Erforderlichkeit begrüße ich auch, dass die in den einzelnen Registern gespeicherten Daten auf einen Kerndatenbestand beschränkt werden sollen. So soll künftig insbesondere auf die Angabe des Berufs, der in der heutigen Zeit keine personenstandsrechtliche Aussagekraft mehr aufweist, verzichtet werden.

Der Entwurf sieht außerdem vor, die Benutzung der Personenstandsbücher vor Ablauf der für die Führung der Personenstandsregister festgelegten Fristen bereits bei Glaubhaftmachung eines berechtigten Interesses zuzulassen, wenn seit dem Tod des zuletzt verstorbenen Beteiligten (Beteiligte sind beim Geburtseintrag die Eltern und das Kind, beim Eheeintrag die Ehegatten und beim Lebenspartnerschaftseintrag die Lebenspartner) dreißig Jahre vergangen sind. Diese Regelung liegt im Interesse der Familien- und Heimatforschung. Da der Begriff des „berechtigten“ Interesses allerdings weit umfassend ist (berechtigtes Interesse ist jedes rechtlich anerkennenswerte Interesse, also z.B. auch ein wirtschaftliches Interesse), habe ich gegenüber dem Bayerischen Staatsministerium des Innern eine Prüfung angeregt, ob hier Einschränkungen geboten sind. So wäre z.B. zu prüfen, ob die Benutzung der Personenstandsbücher auf Grund eines berechtigten Interesses auf bestimmte Forschungen beschränkt bleiben sollte oder ggf. auch versagt werden sollte, wenn Grund zu der Annahme besteht, dass schutzwürdige Interessen Betroffener oder Dritter entgegenstehen.

§ 67 des Gesetzentwurfs eröffnet die Möglichkeit der Einrichtung zentraler elektronischer Register auf Landesebene. Die Landesregierungen können durch Rechtsverordnung ein zentrales Register einrichten und nähere Vorschriften über die Führung des Registers treffen (§ 74 Abs. 1 Nr. 3 des Entwurfs). Aus datenschutzrechtlicher Sicht bestehen dagegen grundsätzliche Bedenken. Zentrale Datenbestände wecken generell Begehrlichkeiten, die mit der zunehmenden Automatisierung der Datenverarbeitung noch wachsen. Sie bergen auch ein erheblich größeres Gefahrenpotenzial für die Sicherstellung des Datenschutzes als dezentrale Datenbestände.

8.3 Datenerhebungen im Zusammenhang mit der Zweitwohnungssteuer

Aufgrund einer Änderung in Art. 3 Abs. 3 Kommunalabgabengesetz (KAG) durch § 6 Nr. 1 des Gesetzes zur Änderung des Kommunalrechts vom 26. Juli 2004 (GVBl. S. 272) haben die Kommunen die Möglichkeit erhalten, eine Zweitwohnungssteuer zu erheben. In diesem Zusammenhang haben sich mehrere Bürger an mich gewandt und um datenschutzrechtliche Prüfung insbesondere der Fragebögen (sog. Steuererklärungen zur Zweitwohnungssteuer) gebeten, die ihnen von den Kommunen zur Beantwortung übersandt worden waren. In den mir vorgelegten Fragebögen soll der Steuerpflichtige unter anderem Angaben über Namen, Vornamen, Geburtsdaten und Anschriften der Mitbewohner der gesamten Wohnung, über Wohnungseigenschaften (z.B. Baujahr, besondere Merkmale der Wohnung, Angaben zur Modernisierung etc.) sowie bei einer gemieteten Wohnung über die Höhe des Zinssatzes machen. Außerdem soll bei einer gemieteten Wohnung eine Kopie des Mietvertrags und eine aktuelle Mietbescheinigung des Vermieters vorgelegt werden.

Die Zulässigkeit der Datenerhebung durch die kommunalen Steuerbehörden richtet sich nach dem Kommunalabgabengesetz und der jeweiligen Zweitwohnungssteuersatzung. Das Kommunalabgabengesetz erklärt in Art. 13 eine Vielzahl von Vorschriften der Abgabenordnung (AO) für anwendbar. Hier sind insbesondere die Vorschriften der §§ 85 - 93 AO zu beachten. Nach § 85 AO hat die Finanzbehörde (hier: das kommunale Steueramt) die Steuern nach Maßgabe der Gesetze gleichmäßig festzusetzen und zu erheben. Sie bestimmt Art und Umfang der Ermittlungen (§ 88 Abs. 1 AO; Untersuchungsgrundsatz). Die Beteiligten (hier: i.d.R. die Steuerpflichtigen) sind zur Mitwirkung bei der Ermittlung des Sachverhalts verpflichtet (Art. 13 Abs. 1 Nr. 4 a KAG i.V.m. §§ 149 ff AO und der jeweiligen kommunalen Satzungen über die Erhebung einer Zweitwohnungssteuer). Sie kommen ihrer Mitwirkungspflicht insbesondere dadurch nach, dass sie die für die Besteuerung erheblichen Tatsachen vollständig und wahrheitsgemäß offen legen. Als Korrektiv für die i.d.R. weitreichenden Auskunftspflichten des Bürgers in steuerlichen Angelegenheiten hat der Gesetzgeber ein restriktives Steuergeheimnis in § 30 AO normiert. Die Vorschrift des § 30 AO gilt auch für kommunale Steuern wie die Zweitwohnungssteuer (Art. 13 Abs. 1 Nr. 1 c) KAG).

Zu der Frage, inwieweit die vom Steuerpflichtigen in den Steuererklärungen geforderten Angaben zur Veranlagung der Zweitwohnungssteuer tatsächlich erforderlich sind, habe ich fachliche Stellungnahmen beim Bayerischen Staatsministerium des Innern sowie beim Bayerischen Gemeindetag eingeholt. Nach Mitteilung des Bayerischen Staatsministeriums des

Innern und des Bayerischen Gemeindetags begründet sich die Erforderlichkeit der Angaben über Eigentums- und Mietverhältnisse, Wohnflächen und ggf. Beschränkungen auf Wohnteilflächen sowie über Baujahr und besondere Wohnungsmerkmale wie folgt:

Nach den kommunalen Satzungen über die Zweitwohnungssteuer ist derjenige steuerpflichtig, der die Wohnung innehat. Eine Wohnung hat inne, wer berechtigt die tatsächliche Verfügungsgewalt über die Wohnung besitzt (Eigentümer, Miteigentümer, Mieter, Untermieter, Mitbewohner etc.). Da je Wohnung maximal einmal die Zweitwohnungssteuer erhoben wird, ist bei der Veranlagung einer gemeinschaftlich genutzten Wohnung zu unterscheiden, ob jedem Verfügungsberechtigten die Nutzungsmöglichkeit über die gesamte Wohnung zusteht. Erstreckt sich die Nutzung eines Verfügungsberechtigten nur über einen Teilbereich der Wohnung, erfolgt lediglich eine anteilige Veranlagung der Steuerpflichtigen.

Nach den Zweitwohnungssteuersatzungen wird die Steuer nach dem jährlichen Mietaufwand berechnet. Für Wohnungen, die im Eigentum des Steuerpflichtigen stehen, ist die Nettokaltmiete in der ortsüblichen Höhe anzusetzen. Angaben über das Baujahr sowie die besonderen Wohnungsmerkmale (z.B. über die Ausstattung der Wohnung und den Modernisierungsgrad) sind bei einer im Eigentum stehenden Wohnung daher erforderlich, um die ortsübliche Nettokaltmiete ermitteln zu können. Auch bei allen Formen der Gebrauchsüberlassung sind diese Angaben notwendig, um die Nettokaltmiete ggf. schätzen zu können. Die Vorlage des Mietvertrags dient vor allem der Feststellung, ob die Wohnung ganz oder teilweise überlassen und ob die Wohnung ganzjährig und ggf. nur anteilig vermietet ist. Die Vorlage der Mietbescheinigung ist erforderlich, um die aktuelle Miethöhe belegen zu können.

Zu der Frage der Erforderlichkeit von Angaben des Steuerpflichtigen über Familienangehörige hat der Bayerische Gemeindetag darauf hingewiesen, dass jede (ggf. auch minderjährige) Person, die eine Zweitwohnung innehat, steuerpflichtig ist. Das in der Zweitwohnungssteuersatzung festgeschriebene Institut der Gesamtschuldnerschaft berechtigt die Steuerbehörde, die festgesetzte Zweitwohnungssteuer von jeder Person, die gemeinsam mit anderen eine Wohnung inne hat - insgesamt jedoch nur einmal - in voller Höhe zu verlangen. Die beim Betroffenen bestehende Verpflichtung zur Nennung dieser Personen ergibt sich aus § 93 Abs. 1 Satz 1 AO, da diese Angaben für die Besteuerung erheblich sind. Gemäß § 155 Abs. 3 AO kann gegen Steuerpflichtige, die eine Steuerschuld gesamtschuldnerisch schulden, ein zusammengefasster Steuerbescheid ergehen. Die Namen und Geburtsdaten aller Mitbewohner sind daher zur eindeutigen Feststellung des bzw. der Steuerpflichtigen - etwa bei Namensgleichheit - erforderlich. Des Weiteren lässt das Alter der Bewohner Rückschlüsse darüber zu, in welcher Reihenfolge die gesamtschuldnerisch haftenden Steuerpflichtigen herangezogen werden (z.B. wird in der Regel zunächst der Haushaltsvorstand und nicht das minderjährige Kind herangezogen).

Aus datenschutzrechtlicher Sicht halte ich die im Rahmen der Steuererklärungen gestellten Fragen sowie die Vorlage von Nachweisen (z.B. Mietvertrag) zur Aufgabenerfüllung der jeweiligen kommunalen Steuerbehörde aus den genannten Gründen für erforderlich. Da die kommunale Steuerbehörde die Zweitwohnungssteuer gleichmäßig festzusetzen hat (§ 85 AO), hat sie den steuerlichen Sachverhalt (hier: Feststellung des Steuerschuldners und der Bemessungsgrundlage für die Zweitwohnungssteuer) sorgfältig beim Betroffenen zu ermitteln. Dies gilt insbesondere vor dem Hintergrund, dass der Begriff des „Innehabens einer Zweitwohnung“ in der Rechtsprechung bereits umfassend judiziert wurde. Im Hinblick auf die dafür vorgetragenen Argumente habe ich auch keine Einwendungen dagegen erhoben, dass im Fragebogen unter anderem Angaben über Familienverhältnisse gefordert werden.

Personenbezogene Daten sind beim Betroffenen mit seiner Kenntnis zu erheben (Art. 16 Abs. 2 Satz 1 Bayerisches Datenschutzgesetz - BayDSG). Dadurch soll sichergestellt werden, dass der Einzelne über die Preisgabe und Verwendung seiner Daten grundsätzlich selbst bestimmen kann. Hierzu zählt auch, dass der Steuerschuldner hinreichend darüber informiert wird, inwiefern die von der Steuerbehörde geforderten Angaben oder Nachweise zur Ermittlung des steuerlichen Sachverhalts benötigt werden. Ich habe die überprüften Kommunen daher aufgefordert, den Steuerpflichtigen detailliert - z.B. im Rahmen eines der Steuererklärung beiliegenden Informationsblattes - darüber aufzuklären, warum die nachgefragten Daten sowie die Vorlage der Nachweise im Einzelnen für die Festsetzung der Zweitwohnungssteuer erforderlich sind. Des Weiteren habe ich die Kommunen auf die bei der Datenerhebung zu beachtenden Hinweis- und Aufklärungspflichten nach Art. 16 Abs. 3 BayDSG hingewiesen. So sollte insbesondere auch in der Steuererklärung selbst auf die Rechtsvorschrift hingewiesen werden, nach der der Steuerpflichtige zur Auskunft verpflichtet ist (Art. 16 Abs. 3 Satz 2 und Satz 4 BayDSG).

8.4 Biometrische Ausweisdokumente

Bereits mit den Artikeln 7 und 8 des Terrorismusbekämpfungsgesetzes vom 9. Januar 2002 wurden das Passgesetz und das Personalausweisgesetz dahingehend geändert, dass der Pass- bzw. Personalausweis neben dem Lichtbild und der Unterschrift weitere

biometrische Merkmale von Fingern oder Händen oder Gesicht des Passinhabers bzw. des Personalausweisinhabers enthalten darf. Die Einrichtung einer bundesweiten Datenbank hat der Gesetzgeber ausgeschlossen (§ 4 Abs. 4 Satz 2 PaßG und § 1 Abs. 5 Satz 2 PAuswG).)

Die Aufnahme biometrischer Merkmale in die Pässe wurde inzwischen von der Europäischen Gemeinschaft verbindlich geregelt. So sind nach Art. 1 Abs. 2 Satz 1 der am 18. Januar 2005 in Kraft getretenen „Verordnung (EG) Nr. 2252/2004 des Rates vom 13. Dezember 2004 über Normen für Sicherheitsmerkmale und biometrische Daten in von den Mitgliedsstaaten ausgestellten Pässen und Reisedokumenten“ (EG-PassVO) die Pässe und Reisedokumente mit einem Speichermedium zu versehen, das ein Gesichtsbild enthält. Nach Art. 1 Abs. 2 Satz 2 EG-PassVO fügen die Mitgliedstaaten auch Fingerabdrücke in inoperablen Formaten hinzu. Art. 1 Abs. 2 Satz 3 EG-PassVO sieht vor, dass die Daten zu sichern sind und das Speichermedium eine ausreichende Kapazität aufweisen und geeignet sein muss, die Integrität, die Authentizität und die Vertraulichkeit der Daten sicherzustellen. Die Verordnung ist in allen ihren Teilen verbindlich und gilt unmittelbar in allen Mitgliedstaaten.

In der Bundesrepublik Deutschland wird seit dem 1.11.2005 das digitalisierte Gesichtsbild auf den Reisepässen in einem integrierten Chip gespeichert. Dazu wurde vom Bundesministerium des Innern mit Zustimmung des Bundesrates die Zweite Verordnung zur Änderung passrechtlicher Vorschriften vom 8. August 2005 (BGBl I S. 2306) erlassen. Die Fingerabdrücke sollen in einer zweiten Stufe ab November 2007 auf dem Chip des biometrischen Passes (= ePass) gespeichert werden. Die EG-Verordnung sieht dies bis zum 28.2.2008 vor.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat in einer Entschließung vom 1. Juni 2005 vor den Risiken elektronisch lesbarer biometrischer Ausweisdokumente gewarnt. Sie hat dabei u.a. auf die Gefahren einer Falscherkennung und der damit verbundenen erheblichen Konsequenzen für die Betroffenen hingewiesen, die hier einem besonderen Rechtfertigungsdruck und zusätzlichen Kontrollmaßnahmen ausgesetzt werden. Zur Gewährleistung von Datenschutz und Datensicherheit hat sie die dafür erforderlichen rechtlichen, organisatorischen und technischen Maßnahmen gefordert. Die Entschließung ist als Anlage Nr. 4 abgedruckt.

8.5 Elektronische Ratsinformationssysteme

Gemeinden, die die Einführung eines elektronischen Ratsinformationssystems planten, haben sich mit der Bitte um datenschutzrechtliche Beratung an mich gewandt. Vorgesehen war, den Gemeinderatsmitgliedern in einem passwortgeschützten Bereich der Homepage der Gemeinde Sitzungsvorlagen, Sitzungsniederschriften und die Einladungen zu den Sitzungen zum Abruf bereit zu stellen. Aus datenschutzrechtlicher Sicht vertrete ich dazu folgende Auffassung:

Sitzungsvorlagen der Verwaltung sind interne Ausarbeitungen für den Gemeinderat bzw. die Ausschüsse. Die Vorlagen werden nur insoweit in die öffentliche Sitzung eingeführt, als sie der Bürgermeister mündlich vorträgt. Eine Bereitstellung von Sitzungsunterlagen zum Abruf durch die Gemeinderatsmitglieder kommt daher nur für solche Unterlagen in Betracht, die nicht lediglich als Tischvorlagen für die Dauer der Sitzung zur Verfügung gestellt werden sollen und setzt voraus, dass Dritte weder lesend noch schreibend auf die Unterlagen zugreifen können. Ebenso sind unbefugte Kenntnisnahmen und Zugriffe auf Einladungen zu Sitzungen, die auch die Angaben der Tagesordnungspunkte der nichtöffentlichen Sitzungen erfordern, und auf Sitzungsniederschriften, die nur für die Gemeinderatsmitglieder bestimmt sind, auszuschließen.

Um wirksam ausschließen zu können, dass Dritten ein Zugriff auf dienstliche Unterlagen im häuslichen Computer ermöglicht wird, sollte ein Speichern dieser Unterlagen auf dem häuslichen Computer der Gemeinderatsmitglieder, der in aller Regel keine professionellen Sicherheitskomponenten enthält, untersagt sein. Im Bedarfsfalle könnten die Unterlagen zu Hause ausgedruckt werden. Die Ausdrucke lassen sich im häuslichen Bereich kostengünstiger schützen als gespeicherte Informationen.

Aus technisch-organisatorischer Sicht ergeben sich darüber hinaus noch folgende Anmerkungen:

- Sollte für den Zugriffsschutz auf das Ratsinformationssystem lediglich ein gemeinsames Passwort zur Authentisierung genutzt werden (welches somit allen Berechtigten bekannt sein muss), ist dies abzulehnen, da ansonsten auch ausgeschiedene Gemeinderatsmitglieder weiterhin Zugriff auf diesen Bereich hätten. Es muss somit gewährleistet sein, dass jeder Berechtigte zur Identifizierung und Authentisierung über eine eigene Benutzerkennung und ein individuelles - nur ihm bekanntes - Passwort verfügt.

- Eine eventuelle Datenübertragung zwischen dem Ratsinformationssystem und dem Rechner eines Berechtigten über das Internet muss verschlüsselt erfolgen. Die Errichtung eines VPN (Virtuellen Privaten Netzes) zur Gewährleistung der Vertraulichkeit wird dringend angeraten.

– Die Authentizität und die Integrität der Daten im Ratsinformationssystem müssen (z.B. durch den Einsatz der elektronischen Signatur) gewährleistet sein. Gleiches gilt für eine eventuelle Datenübertragung über das Internet.

– Falls ein Download von Dateien aus dem Ratsinformationssystem erlaubt ist, müssen die PC der Empfänger der Datenübertragung ebenfalls gegen einen unerlaubten Zugriff auf die übermittelten Daten gesichert werden.

8.6 Aufstellung von Web-Cams durch Kommunen

Von der Presse und einem Bürger bin ich auf die Übertragung von Bildern des Marktplatzes einer Kommune im Internet mittels einer Web-Cam aufmerksam gemacht worden. Den Vorgang habe ich aus datenschutzrechtlicher Sicht wie folgt bewertet:

Nach Art. 15 Abs. 1 des Bayerischen Datenschutzgesetzes ist die Erhebung, Verarbeitung und Nutzung personenbezogener Daten nur auf der Grundlage eines Gesetzes oder einer Einwilligung der Betroffenen zulässig. Für die Erhebung personenbezogener Daten und deren Übermittlung über das Internet an die Allgemeinheit mittels einer Web-Cam durch Kommunen gibt es keine Rechtsgrundlage. Eine Einwilligung in die Datenerhebung und -übermittlung ist schon angesichts eines nicht bestimmbaren Personenkreises potenziell Betroffener und der fehlenden Freiwilligkeit ausgeschlossen. Web-Cam-Aufnahmen und deren Übertragung im Internet sind daher nur dann zulässig, wenn jede Beeinträchtigung schutzwürdiger Interessen, insbesondere des Persönlichkeitsrechts von Bürgern ausgeschlossen ist. Das ist nur dann der Fall, wenn die Aufnahmen nicht personenbezogen sind, d.h. wenn auf den Bildern weder Personen noch Fahrzeuge identifizierbar sind. Bloße Übersichtsaufnahmen ohne Personenbezug sind datenschutzrechtlich unbedenklich.

In dem zu beurteilenden Fall waren auf den Bildern vom Marktplatz der betreffenden Kommune im Internet zwar weder die Gesichter der aufgenommen Personen noch Kfz-Kennzeichen erkennbar. Allerdings war es möglich, dass Internetbenutzer, die aufgenommene Personen persönlich oder zumindest vom Sehen her kannten, diese z.B. anhand der Körperhaltung, Kleidung, mitgeführten Gegenständen etc. identifizieren konnten. Ich habe die Kommune deshalb gebeten, die Kameraeinstellung oder den Kamerastandort so zu ändern, dass auch eine derartige Identifizierung von Personen ausgeschlossen ist.

8.7 Beauftragung Privater mit der Videoüberwachung kommunaler Wertstoffhöfe

Zur Videoüberwachung kommunaler Wertstoffhöfe habe ich mich in meinem 18. Tätigkeitsbericht unter der Nr. 18.1. geäußert. Im Berichtszeitraum bin ich aufgrund einer Beschwerde über eine Gemeinde mit der Frage befasst worden, ob bzw. unter welchen Voraussetzungen damit auch private Dritte beauftragt werden können. Ich vertrete dazu die folgende Auffassung:

Das Bayerische Oberste Landesgericht hat sich mit Beschlüssen vom 05.03.1997 (Gz. 1 0bOwi 785/97) und vom 11.07.1997 (Gz. 1 0bOWi 282/97), die den Regierungen mit Schreiben vom 26.03. und 11.08.1997, Nr. IC4-3618.3011-13- Krä und vom 30.05.1997, Nr. IC4-3618.3011-13-Ben, übermittelt wurden, ausführlich über die Grenzen der Einbeziehung Privater bei der Verfolgung und Feststellung von Geschwindigkeitsverstößen im Rahmen der kommunalen Verkehrsüberwachung geäußert.

Im Hinblick darauf, dass bei einer Videoüberwachung und -aufzeichnung grundsätzlich ein erheblicher Eingriff in das Recht auf informationelle Selbstbestimmung vorliegt sowie in Anlehnung an die o.g. Gerichtsbeschlüsse halte ich die Beauftragung Privater mit der eigenständigen Feststellung und ggf. auch Verfolgung von Verstößen auch im Bereich der illegalen Entsorgung von Müll aus datenschutzrechtlicher Sicht für unzulässig:

Vergleichbar der Einbeziehung Privater bei Geschwindigkeitsverstößen in der kommunalen Verkehrsüberwachung war auch in dem hier zu beurteilenden Fall bei der von der betroffenen Gemeinde vorgenommenen Beauftragung einer privaten Firma mit der Videoüberwachung des Wertstoffhofs zum Zwecke der Feststellung und Verfolgung von Ordnungswidrigkeiten die Grenze zur Übertragung hoheitlicher Aufgaben überschritten. Solche Aufgaben dürfen nach Art. 33 Abs. 4 GG grundsätzlich nur von Angehörigen des öffentlichen Dienstes durchgeführt werden, solange nicht eine gesetzliche Beleihung erfolgt. Derartige eingriffsintensive Maßnahmen stehen daher ausschließlich der für das Ordnungswidrigkeitenverfahren zuständigen Verfolgungsbehörde zu. Lediglich einzelne Tätigkeiten können in diesem Zusammenhang auch durch private Dritte durchgeführt werden, wenn es sich dabei um bloße Hilfstätigkeiten handelt. Dabei muss jedoch sichergestellt sein, dass die verfahrensrechtlichen Entscheidungen (intern und nach außen) von der zuständigen Verfolgungsbehörde getroffen werden. Insbesondere dürfen alle hoheitlichen Maßnahmen (wie Versand von Anhörungsbögen, Erlass und Zustellung von Bußgeldbescheiden etc.) nur durch die zuständige öffentliche Stelle erfolgen.

Unter der Prämisse, dass die für die Verfolgung von Ordnungswidrigkeiten im Rahmen der illegalen Müllentsorgung zuständige Behörde „Herrin“ des Ermittlungsverfahrens bleibt, wäre daher eine Einbeziehung Privater nur gemäß der nachstehenden Modalitäten zulässig:

Bei der Durchführung der Videoüberwachung und -aufzeichnung zum Zweck der Ermittlung illegaler Müllentsorger kann die zuständige öffentliche Stelle die Dienste privater Firmen in Anspruch nehmen z.B. durch die Anmietung, das Leasing oder die Wartung von Überwachungsgerät (z.B. Videokameras). Dabei kann auch vereinbart werden, dass der private Vertragspartner das Überwachungsgerät mit eigenem Personal bedient sowie die Aufnahmen bzw. Aufzeichnungen entwickelt und auswertet. Voraussetzung ist dann jedoch, dass die Tätigkeit des privaten Personals vor Ort ständig von einem fachkundigen Bediensteten der zuständigen öffentlichen Stelle beaufsichtigt wird, der mit den technischen Details vertraut sein muss und die Videoaufnahmen sowie ggf. auch die Folgetätigkeiten verantwortlich leiten muss. Zum Einsatz Privater im Rahmen des Arbeitnehmerüberlassungsgesetzes verweise ich auf den Beschluss des Bayerischen Obersten Landesgerichts vom 05.03.1997, BayVBl 1997, S. 413. Eine ständige Beaufsichtigung vor Ort entfällt naturgemäß bei fest installierten Kameras, die automatisch Aufnahmen mittels eines Bewegungsmelders anfertigen.

Die Bestimmungen des Datenschutzes, insbesondere Art. 6 Abs. 1 und 2 Bayerisches Datenschutzgesetz (BayDSG), sind zu beachten. In der geforderten schriftlichen Auftragserteilung sind insbesondere Regelungen über die Art der Anlieferung bzw. Abholung der Videoaufnahmen, des Zugriffsschutzes und des Ausschlusses von Unterauftragsverhältnissen zu treffen. Die eingesetzten Mitarbeiter des privaten Vertragspartners sind im Hinblick auf § 203 Abs. 2 Nr. 2 Strafgesetzbuch (StGB) besonders zu verpflichten. Dies könnte z.B. mit dem Formblatt „Niederschrift über die Verpflichtung zur gewissenhaften Erfüllung von Obliegenheiten“ nach dem Verpflichtungsgesetz erfolgen. Das Formblatt ist abgedruckt im AllMBl 1996, Seite 281. Des Weiteren wird die vertragliche Festlegung von Konventionalstrafen empfohlen. Bei der Auswertung der Aufnahmen muss außerdem sichergestellt sein, dass letztlich der Bedienstete der zuständigen Behörde über die Beweiseignung einer Aufnahme und die Frage, ob ein Ordnungswidrigkeitenverfahren eingeleitet wird, entscheidet. Dies bedeutet, dass ihm auch Aufnahmen zur Entscheidung vorgelegt werden, bei denen nach Auffassung des privaten Personals eine Beweiseignung fehlt. Die Festlegung von Ort, Zeit und Umfang der Videoüberwachung ist ebenfalls ausschließlich der zuständigen Behörde vorbehalten. Die zuständige Stelle ist auch allein verantwortlich für die Durchführung der Videoüberwachung. Sie kann dem privaten Vertragspartner hoheitliche Aufgaben in keinem Falle zur eigenständigen Erledigung übertragen.

In dem zu beurteilenden Fall war die Videoüberwachung des Wertstoffhofs in mehrfacher Hinsicht unzulässig und wurde von mir deshalb beanstandet. Außer der Beauftragung eines privaten Dritten im Rahmen der Videoüberwachung nicht lediglich mit bloßen Hilfstätigkeiten war der Erfassungsbereich der Kameras nicht auf den Bereich des Wertstoffhofs beschränkt, sondern hatte einen angrenzenden Radweg einbezogen, und schließlich wurde die Videoüberwachung zunächst auch noch ohne ausreichende Hinweise auf die Überwachung durch entsprechende Schilder durchgeführt.

8.8 Videoüberwachung öffentlicher Toilettenanlagen

Ein Bürger hat sich bei mir darüber beschwert, dass eine Stadt ihre öffentlichen Toilettenanlagen videoüberwacht. Auf vom Beschwerdeführer übersandten Fotos konnte man erkennen, dass in den Innenräumen der Toiletten Kameras angebracht waren. Die von mir dazu befragte Kommune teilte mit, dass es bei ihren öffentlichen Toilettenanlagen, die erst vor wenigen Jahren mit beträchtlichem Aufwand saniert oder neu errichtet worden seien, immer wieder zu mutwilligen und gravierenden Beschädigungen gekommen sei. Um diese Beschädigungen zu verhindern und im Schadensfall den Täter gegebenenfalls identifizieren zu können, seien daher in allen Toilettenanlagen Überwachungskameras installiert worden. Der Überwachungsbereich der Kameras sei durch mechanische Sperren so beschränkt worden, dass Beeinträchtigungen der Rechte der Nutzer ausgeschlossen seien. Eine Auswertung der Videoaufnahmen erfolge nur, wenn konkrete Beschädigungen vorgefunden werden. Auf die Videoüberwachung werde an der Eingangstüre zur Toilette ausdrücklich hingewiesen. Ich habe die Videoüberwachung der öffentlichen Toilettenanlagen aus datenschutzrechtlicher Sicht wie folgt bewertet:

Die Beobachtung von Bürgern durch den Einsatz von Videotechnik stellt einen Eingriff in deren allgemeines Persönlichkeitsrecht dar. Soweit bei einer Videoüberwachung Personen erkennbar sind, stellt dies eine Erhebung personenbezogener Daten i.S.d. Art. 4 Abs. 1 Bayerisches Datenschutzgesetz (BayDSG) dar. Werden Videoaufzeichnungen gefertigt, die im Nachhinein betrachtet und ausgewertet werden können, liegt auch eine Speicherung personenbezogener Daten vor (Art. 4 Abs. 6 Satz 2 Nr. 1 BayDSG). Die nachträgliche Betrachtung und Auswertung stellt eine Datennutzung im Sinne des Art. 4 Abs. 7 BayDSG dar.

Die Erhebung, Verarbeitung und Nutzung personenbezogener Daten ohne Rechtsgrundlage oder infor-

mierte Einwilligung des Betroffenen ist unzulässig (Art. 15 Abs. 1 BayDSG). Eine Einwilligung ist hier angesichts eines nicht bestimmbaren Personenkreises potenziell Betroffener und der fehlenden Freiwilligkeit ausgeschlossen. Als Rechtsgrundlage für die Videoüberwachung kommt Art. 16 Abs. 1 BayDSG in Betracht. Danach ist das Erheben personenbezogener Daten zulässig, wenn ihre Kenntnis zur Erfüllung der in der Zuständigkeit der erhebenden Stelle liegenden Aufgaben erforderlich ist. Erforderlich ist eine Datenerhebung dann, wenn die Kenntnis der Daten zur Erreichung des Zwecks objektiv geeignet ist und im Verhältnis zu dem angestrebten Zweck auch angemessen erscheint (vgl. Wilde/Ehmann/ Niese/Knoblauch, Bayerisches Datenschutzgesetz, Art. 16 Rdnr. 9).

Eine Videoüberwachung der Toiletten halte ich zum Schutz öffentlichen Eigentums vor Beschädigungen und Randalismus zwar grundsätzlich für geeignet. Ob die Videoüberwachung aber auch angemessen erscheint, ist im Rahmen einer Güterabwägung zwischen den Belangen der Stadt (=Schutz des Eigentums vor Beschädigung und Vandalismus) und den schutzwürdigen Interessen der von der Überwachung betroffenen Personen zu prüfen.

In eine Güterabwägung ist einzubeziehen, dass das vom Grundgesetz in Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 geschützte allgemeine Persönlichkeitsrecht das Recht des Bürgers umfasst, sich unbeobachtet im öffentlichen Raum zu bewegen. In dieses Recht wird, wie oben ausgeführt, durch eine Videoüberwachung eingegriffen. Dabei sind die Bürger allein schon durch die Kenntnis der Überwachung hinsichtlich ihres Verhaltens einem latenten Anpassungsdruck ausgesetzt. Eine Videoüberwachung ist daher, ihre grundsätzliche Geeignetheit zu dem verfolgten öffentlichen Zweck vorausgesetzt, nur in engen Grenzen zulässig. Gegenüber dem mitgeteilten Zweck der Verhinderung und Verfolgung von Eigentumsstörungen sind überwiegende schutzwürdige Interessen der von der Überwachung betroffenen Bürger in aller Regel dann anzunehmen, wenn die Videoüberwachung Bereiche erfasst, die dem höchstpersönlichen Bereich oder dem Intimbereich der beobachteten Personen zuzuordnen sind. Dies ist etwa bei Duschen, Umkleideräumen und Toiletten der Fall (vgl. u.a. Kommentierung des LfD Niedersachsen zu § 25 a Abs. 1 NDSG unter www.lfd.niedersachsen.de).

Die Videoüberwachung der öffentlichen Toiletten durch die betroffene Stadt stellte daher einen unzulässigen Eingriff in das informationelle Selbstbestimmungsrecht der Betroffenen dar. Diese datenschutzrechtliche Bewertung erfuhr auch dadurch keine Änderung, dass nach den vorgelegten Fotos und der Aussage der Stadt dazu der Innenraum der Toiletten nicht lückenlos überwacht wurde, denn auch die nach den Fotos überwachten Bereiche der Toiletten, mithin die gesamten Innenräume der Toiletten, waren dem Intimbereich zuzurechnen, da das Verhalten der Bürger auch in diesen (überwachten) Bereichen besonders schutzwürdig ist. Aus datenschutzrechtlicher Sicht würde ich bei wiederholten und nicht unerheblichen Eigentumsstörungen jedoch eine Videoüberwachung der Toilettenzugänge und ggf. des räumlichen Umfelds von außen für vertretbar halten. Auch in diesem Fall wären die Betroffenen deutlich auf die Videoüberwachung hinzuweisen.

Nachdem die Kommune die Kameras in den öffentlichen Toiletten unverzüglich abgebaut hat, habe ich von einer Beanstandung abgesehen.

8.9 Telefonisches Warnsystem

Ein Landratsamt hat mir mitgeteilt, dass es sich mit dem Gedanken trägt, zur Verbesserung der Information der Bevölkerung im Katastrophen- und Großschadensfall über einen privaten Anbieter ein telefonisches Warnsystem einzurichten. Der Anbieter stelle sich vor, in Zusammenarbeit mit der örtlichen Katastrophenschutzbehörde lokal oder regional der Bevölkerung bei sog. Großschadensereignissen amtliche Warnmitteilungen und Verhaltensempfehlungen telefonisch zuzuleiten. Zu dem Vorgang habe ich eine fachliche Stellungnahme des Staatsministeriums des Innern eingeholt. Aus datenschutzrechtlicher Sicht vertrete ich zu dem Vorhaben folgende Auffassung:

Bei dem Verfahren sollen die Telefonnummern der Landkreisbewohner erhoben und zu Warnzwecken gespeichert werden. Telefonnummern natürlicher Personen sind durch ihre Zuordnung zum jeweiligen Anschlussinhaber personenbezogene Daten im Sinne des Art. 4 Abs. 1 des Bayerischen Datenschutzgesetzes (BayDSG). Nach Art. 15 Abs. 1 BayDSG ist die Erhebung, Verarbeitung und Nutzung personenbezogener Daten nur zulässig, wenn das Bayerische Datenschutzgesetz oder eine andere Rechtsvorschrift sie erlaubt oder anordnet oder der Betroffene eingewilligt hat.

Die Einholung einer Einwilligung dürfte hier angesichts des damit verbundenen unverhältnismäßig hohen Aufwands wohl nicht in Betracht kommen. Mangels einer bereichsspezifischen Rechtsvorschrift für die Zulässigkeit der Datenerhebung richtet sich diese nach Art. 16 Abs. 1 BayDSG. Die Erhebung personenbezogener Daten ist danach zulässig, wenn ihre Kenntnis zur Erfüllung der in der Zuständigkeit der erhebenden Stelle liegenden Aufgaben erforderlich ist. Erforderlich ist eine Datenerhebung dann, wenn die Kenntnis der Daten zur Erreichung des Zwecks objektiv geeignet ist und im Verhältnis zu dem angestrebten Zweck auch angemessen erscheint (vgl. Wilde/Ehmann/Niese/Knoblauch, Bayerisches Datenschutzgesetz, Art. 16 Rdnr. 9). Die Zulässigkeit

der Datenerhebung vorausgesetzt, müssten die Daten hier nicht beim Betroffenen mit dessen Kenntnis erhoben werden, da sie aus allgemein zugänglichen Quellen (insbesondere aus öffentlichen Telefonbüchern) entnommen werden sollen (Art. 16 Abs. 2 Satz 1 BayDSG).

Bei der Prüfung der Geeignetheit der Datenerhebung zur Aufgabenerfüllung (Warnung der betroffenen Bevölkerung im Katastrophen- und Großschadensfall) ist zu berücksichtigen, dass wohl nicht alle Betroffene einen Telefonanschluss besitzen und dass nicht alle Anschlussinhaber in öffentlichen Telefonbüchern und elektronischen Telefonverzeichnissen eingetragen sind. Anschlussinhaber können auf einen Eintrag in öffentliche Verzeichnisse verzichten, einem solchen widersprechen und erfolgte Einträge jederzeit löschen lassen. Hinzu kommt, dass auch Personen, deren Telefonnummern in das Warnsystem aufgenommen worden sind, im Katastrophen- oder Großschadensfall durch einen Anruf nicht gewarnt werden können, weil sie den Anruf nicht entgegen nehmen, dieser lediglich auf einem Anrufbeantworter gespeichert wird oder das Telefon vom Betroffenen nicht gehört wird. Ein Warnanruf wird daher immer nur einen Teil der betroffenen Bevölkerung erreichen. Ein telefonisches Warnsystem könnte daher lediglich als ein zusätzliches Mittel zur Information der Bevölkerung eingesetzt werden.

Bei der Prüfung der Angemessenheit der Datenerhebung im Verhältnis zu dem angestrebten Zweck ist eine Güterabwägung vorzunehmen. Es ist hier zu prüfen, ob die zu erfüllende Aufgabe und deren konkrete Unterstützung durch telefonische Warnhinweise in einem angemessenen Verhältnis zu den schutzwürdigen Interessen der Betroffenen an einer Nichtverwendung ihrer Daten stehen. Dass der Schutz der Bürger im Katastrophen- und Großschadensfall von überragender Bedeutung ist steht außer Frage. Demgegenüber weisen die aus allgemein zugänglichen Quellen wie öffentlichen Telefonbüchern und elektronischen Telefonverzeichnissen entnommenen Telefonnummern nur eine geringe Sensibilität auf. Andererseits sind diese Daten für den genannten Zweck nur dann brauchbar, wenn sie so aufbereitet sind, dass im Katastrophen- bzw. Großschadensfall gezielt nur die davon betroffenen Bürger angerufen werden. Nach bestimmten Kriterien strukturierte Telefonnummern (z.B. nach dem Einwirkbereich von Störfallbetrieben) sind jedoch schutzwürdige personenbezogene Daten, weil sie auch für andere Zwecke genutzt werden können und deshalb für Dritte von Interesse sind.

Das Bayerische Staatsministerium des Innern hält es aus fachlicher Sicht für sachlich gerechtfertigt, eine Warnung der Bevölkerung auf telefonischem Weg einzurichten. Allerdings sollte nach Mitteilung des Ministeriums die Information bzw. die Warnung einen inhaltlichen Bezug zu einem bestimmten und feststehenden Empfängerkreis haben. Bei den Unwetterwarnungen wären dies z.B. bestimmte Ansprechpartner in den Gemeinden (Bürgermeister, Bauhof oder Feuerwehr). Auch für die Bevölkerung im Einwirkbereich von kerntechnischen Anlagen bzw. Störfallbetrieben mit einer erheblichen Gefahrenlast, die über den Luftpfad verbreitet werden können, sei eine unmittelbare und schnelle Alarmierung der Bevölkerung über Telefon zusätzlich zu Rundfunkdurchsagen durchaus zielführend. Unter diesen Einschränkungen halte ich im Ergebnis die Einrichtung eines telefonischen Warndienstes aus datenschutzrechtlicher Sicht für zulässig.

Soweit an eine Einbeziehung des privaten Anbieters über die Einrichtung des Warnsystems hinaus gedacht ist, halte ich dies nur im Rahmen einer Auftragsdatenverarbeitung nach Art. 6 BayDSG für zulässig. Speichernde Stelle wäre danach die Katastrophenschutzbehörde (vgl. Art. 4 Abs. 10 Satz 2 BayDSG sowie Wilde et al., a.a.O., Art. 4 Rdnrn. 99 und 100). Für eine Funktionsübertragung sehe ich keine Rechtsgrundlage.

Eine landesweite Aufnahme von Telefonanschlüssen ohne Bezug zu einer konkretisierten Gefährdungslage oder Aufgabe des Empfängers der Warnung hält das Bayerische Staatsministerium des Innern aus katastrophenschutzrechtlicher Sicht nicht für gerechtfertigt. Eine solche wäre daher nicht zulässig. Gegen eine landesweite Speicherung von Telefondaten in einer zentralen Datei hätte ich auch im Hinblick auf die allgemein von zentralen Datenbeständen ausgehenden Gefahren und angesichts der Begehrlichkeiten, die zentrale Datenbestände regelmäßig wecken, Bedenken.

8.10 Friedhofinformationssystem

Eine Stadt teilte mir mit, dass sie die Einführung eines sog. Friedhofinformationssystems beabsichtigt. Dabei soll auf dem Friedhof ein Informations-Terminal (PC) aufgestellt werden, das Friedhofsbesuchern die Möglichkeit eröffnet, nach dem Standort des Grabes eines Verstorbenen zu suchen. Zu diesem Zweck sollen auf dem PC der Name, das Geburtsdatum, das Sterbedatum sowie die Grabstelle gespeichert und ggf. auf dem Bildschirm angezeigt werden. Nach Auskunft der Stadt handelt es sich bei den personenbezogenen Daten nicht um Personenstands- oder Meldedaten, sondern um Daten, die der Friedhofsverwaltung von den Angehörigen mitgeteilt werden.

Gegen die Einführung eines solchen Friedhofinformationssystems habe ich im Hinblick darauf, dass es sich um die Bekanntgabe der Daten Verstorbener handelt, die zum überwiegenden Teil als offenkundig

betrachtet werden können (z.B. aufgrund der allgemein üblichen Beschriftung der Grabsteine mit dem Geburts- und Sterbedatum des Verstorbenen), und dass ein erheblicher Eingriff in das informationelle Selbstbestimmungsrecht der betroffenen Angehörigen hier nicht erkennbar ist, keine grundsätzlichen datenschutzrechtlichen Bedenken, sofern folgende Voraussetzungen beachtet werden:

- Die Suchfunktion des Terminals sollte so ausgestaltet werden, dass die Eingabe eines konkreten Namens eines Verstorbenen erforderlich ist.

- Auf die Anzeige des Tages und Jahrs der Geburt sowie des Sterbetages sollte (zumindest bei allen Altfällen) verzichtet werden. Die Anzeige des Todesjahrs (auch bei Altfällen) ist datenschutzrechtlich vertretbar.

- Bei allen Neufällen sollte vorab eine informierte Einwilligung der betroffenen Angehörigen eingeholt werden (Art. 15 BayDSG).

- Im Hinblick auf bereits bestehende Grabstätten sollte vorab eine Information der Bürger über die beabsichtigte Einführung eines Friedhofinformationssystems und die damit verbundene Speicherung bzw. Übermittlung von Daten Verstorbener erfolgen (z.B. durch eine Bekanntmachung in der Tageszeitung, im Amtsblatt etc.). Dabei ist auch darauf hinzuweisen, dass betroffene Angehörige der Veröffentlichung von Daten des Verstorbenen im Rahmen des Friedhofinformationssystems jederzeit und ohne Angabe von Gründen formlos widersprechen können.

8.11 Veröffentlichung der Namen schulpflichtiger Kinder im gemeindlichen Mitteilungsblatt

Eltern schulpflichtiger Kinder haben sich bei mir darüber beschwert, dass ihre Wohnsitzgemeinde die Namen aller Kinder, die erstmals zum Schuljahr 2005/2006 schulpflichtig geworden sind, im gemeindlichen Mitteilungsblatt veröffentlicht hat. Die von mir dazu angehörte Gemeinde teilte mit, die Veröffentlichung der Namen der schulpflichtigen Kinder im Mitteilungsblatt der Gemeinde sei in Absprache zwischen der Gemeinde und der Schulverwaltung vorgenommen worden. Zur zusätzlichen Veröffentlichung im Mitteilungsblatt habe man sich entschlossen, nachdem es schon mehrfach vorgekommen sei, dass die aus Kostengründen den betroffenen Kindergartenkindern im Kindergarten zur Weitergabe an ihre Eltern mitgegebenen Schreiben der Schulverwaltung von den Kindern verlegt worden seien oder verloren gegangen seien. Außerdem sei es üblich, dass z.B. Erstklässler mit Namen und Bild in den örtlichen Tageszeitungen abgedruckt werden. Den Vorgang habe ich aus datenschutzrechtlicher Sicht wie folgt bewertet:

Die Namen und Vornamen der Kinder sowie der Hinweis auf ihre Schulpflicht und Schuleinschreibung sind personenbezogene Daten im Sinne des Art. 4 Abs. 1 des Bayerischen Datenschutzgesetzes (BayDSG). Die Veröffentlichung dieser Daten im Mitteilungsblatt der Gemeinde stellte eine Datenübermittlung an eine Vielzahl unbestimmter Dritter dar. Die Datenübermittlung ist eine Form der Datenverarbeitung (Art. 4 Abs. 6 Nr. 3 BayDSG). Die Verarbeitung personenbezogener Daten ist nach Art. 15 Abs. 1 BayDSG zulässig, wenn das Bayerische Datenschutzgesetz oder eine Rechtsvorschrift sie erlaubt oder anordnet oder der Betroffene eingewilligt hat.

Die Einwilligung der betroffenen Eltern in die Veröffentlichung personenbezogener Daten ihrer Kinder im Mitteilungsblatt der Gemeinde lag nicht vor. Mangels einer bereichsspezifischen Rechtsvorschrift beurteilte sich daher die Veröffentlichung der Daten nach den Vorschriften des Bayerischen Datenschutzgesetzes.

Die Veröffentlichung der Daten der schulpflichtigen Kinder war nicht nach Art. 19 Abs. 1 Nr. 1 BayDSG zulässig, weil sie zur Aufgabenerfüllung der Gemeinde nicht erforderlich war. Die Übermittlung amtlicher Schreiben erfolgt, soweit sie nicht im Wege der Zustellung nach den Vorschriften des Bayerischen Verwaltungszustellungs- und Vollstreckungsgesetzes vorgenommen wird, regelmäßig durch die Post mittels eines verschlossenen Briefes. Aus Kostengründen ist es insbesondere in kleineren Gemeinden auch durchaus üblich und zulässig, dass ein Behördenmitarbeiter amtliche Schreiben austrägt. Im vorliegenden Fall wäre es darüber hinaus möglich gewesen, den Eltern der schulpflichtigen Kindergartenkinder das Schreiben zur Schulanmeldung bei der Abholung ihres Kindes im Kindergarten mitzugeben. Schließlich hätte auch noch durch einen allgemeinen Hinweis (ohne zusätzliche Nennung der Namen der Kinder) im Mitteilungsblatt der Gemeinde auf die Schulanmeldung hingewiesen werden können.

Die Veröffentlichung war auch nicht nach Art. 19 Abs. 1 Nr. 2 BayDSG zulässig. Ein berechtigtes Interesse der Allgemeinheit an der Kenntnis der Namen der schulpflichtigen Kinder besteht nicht. Diese und ihre Eltern müssen darauf vertrauen können, dass die nach § 6 Bayerische Meldedaten-Übermittlungsverordnung (BayMeldeDÜV) an die zuständige Schule übermittelten Daten nicht an unbefugte Dritte oder, wie im vorliegenden Fall, gar an die Öffentlichkeit übermittelt werden.

Zum Hinweis der Gemeinde auf die Veröffentlichung personenbezogener Daten von Erstklässlern in der örtlichen Presse habe ich die Kommune auf die Nr. 4.4 Buchstabe e der mit mir abgestimmten „Erläuternden Hinweise für die Schulen zum Vollzug des Bayerischen Datenschutzgesetzes“ - einer Bekanntmachung des Bayerischen Staatsministeriums für Unterricht und Kultus vom 19.04.2001, KWMBl I S. 112, geändert durch Bekanntmachung vom 10.10.2002, KWMBl I S. 354 - aufmerksam gemacht. Bereits dort ist geregelt, dass Veröffentlichungen der Schule der Einwilligung der Betroffenen bedürfen (s. dazu auch die Nr. 15.1 meines 19. Tätigkeitsberichts). Ergänzend habe ich darauf hingewiesen, dass die Schülerzeitung nach Art. 63 Abs. 1 Satz 2 des Bayerischen Gesetzes über das Erziehungs- und Unterrichtswesen (BayEUG) kein Druckwerk im Sinn des § 6 Abs. 1 des Gesetzes über die Presse ist. Sie ist nur zur Verbreitung innerhalb einer Schule bestimmt. Inhaltliche Beschränkungen der Schülerzeitung sind in Art. 63 Abs. 3 BayEUG gesetzlich normiert. Sie kann deshalb nicht als Vergleichsmaßstab herangezogen werden.

Die Veröffentlichung der Namen und Vornamen von schulpflichtigen Kindern im gemeindlichen Mitteilungsblatt habe ich nach Art. 31 Abs. 1 BayDSG beanstandet. Ein Absehen von der Beanstandung nach Art. 31 Abs. 3 BayDSG kam nicht in Betracht, weil es sich nicht um einen unerheblichen Mangel gehandelt hat und die Veröffentlichung auch nicht mehr rückgängig gemacht werden konnte.

8.12 Weitergabe einer Unterschriftenliste an einen Dritten

Bürger haben sich bei mir darüber beschwert, dass der erste Bürgermeister ihrer Gemeinde eine Unterschriftenliste an den Inhaber einer Privatfirma weitergegeben hat. Die Unterschriftenliste war einem Beschwerdeschreiben beigelegt, das mehrere Bürger im Zusammenhang mit dem Aufstellen von Containern in zwei Wohngebieten durch die Firma an den ersten Bürgermeister und die Gemeinderatsmitglieder gerichtet hatten. Die Weitergabe der Unterschriftenliste an den Firmeninhaber habe ich datenschutzrechtlich wie folgt bewertet:

Die Weitergabe der Unterschriftenliste stellte eine Übermittlung personenbezogener Daten an Dritte (Art. 4 Abs. 6 Nr. 3 a Bayerisches Datenschutzgesetz - BayDSG) dar. Personenbezogene Daten sind gemäß Art. 4 Abs. 1 BayDSG Einzelangaben über persönliche und sachliche Verhältnisse bestimmter oder bestimmbarer natürlicher Personen (Betroffene). Dazu gehörten hier Name und Vorname der Unterschriftsleistenden und die damit zum Ausdruck gebrachte Tatsache der Einwendungen durch diese Personen.

Die vorliegende Datenübermittlung beurteilte sich nach Art. 19 Abs. 1 Nr. 2 BayDSG. Nach dieser Vorschrift ist die Übermittlung personenbezogener Daten an eine nicht-öffentliche Stelle u.a. nur dann zulässig, wenn diese ein berechtigtes Interesse an der Kenntnis der zu übermittelnden Daten glaubhaft darlegt. Ein berechtigtes Interesse ist jedes nach vernünftigen Erwägungen gerechtfertigte Interesse wissenschaftlicher, rechtlicher oder ideeller Art. Im vorliegenden Fall hatte der Firmeninhaber ein wirtschaftliches Interesse an der Aufstellung von Containern in den zwei betroffenen Wohngebieten. Er hatte damit lediglich ein berechtigtes Interesse an der Kenntnis der Tatsache, dass gegen das Vorhaben eine Liste mit Unterschriften in der Gemeinde eingereicht worden war und welche Gründe von den Unterzeichnern gegen das Vorhaben vorgetragen wurden. Ein darüber hinausgehendes Interesse an der Kenntnis der Namen der einzelnen Unterzeichner der Liste bestand dagegen nicht.

Art. 19 Abs. 1 Nr. 2 BayDSG setzt im Übrigen voraus, dass die Betroffenen, d.h. die Unterzeichner der Liste, kein schutzwürdiges Interesse am Ausschluss der Datenübermittlung hatten. Das Schreiben mit der Unterschriftenliste war an den ersten Bürgermeister und die Gemeinderatsmitglieder der Wohnsitzgemeinde der Beschwerdeführer gerichtet. Ziel des Schreibens war es, auf die Entscheidungsfindung der Gemeinde dergestalt Einfluss zu nehmen, dass diese in den beiden Wohngebieten keine Container aufstellt. Die Unterzeichner der Liste durften darauf vertrauen, dass ihre an den ersten Bürgermeister und die Gemeinderatsmitglieder gerichteten persönlichen Daten von diesen nur zu dem übermittelten Zweck verwendet werden und nicht an das interessierte Unternehmen oder an sonstige Dritte weitergegeben werden. Es bestand somit ein überwiegendes schutzwürdiges Interesse der Unterzeichner daran, dass die Daten nicht an den Firmeninhaber weitergegeben wurden. Die Weitergabe der Unterschriftenliste war daher rechtswidrig und wurde von mir beanstandet.

8.13 Verwendung der Blind-Copy-Funktion oder von Einzelanschriften beim Versand von E-Mails an mehrere Empfänger

Im Berichtszeitraum haben sich erneut Bürger bei mir darüber beschwert, dass ihre E-Mail-Adresse von Behörden beim Versand von Schreiben per E-Mail an eine Vielzahl von Personen allen anderen Empfängern mitgeteilt wurde. In einem Fall hatte ein Betroffener bereits eine Stunde nach dem Versand der E-Mails durch eine Gemeinde von einem anderen Empfänger eine Werbung per E-Mail erhalten.

Die Weitergaben der E-Mail-Adressen jedes Empfängers der E-Mails an alle andere Empfänger waren

unzulässige Datenübermittlungen, die durch die Verwendung der Blind-Copy-Funktion (Bcc) oder durch Einzelanschriften hätten vermieden werden können. Ich nehme die erneuten Verstöße gegen den Datenschutz nochmals zum Anlass, auf die Beachtung der datenschutzrechtlichen Vorschriften beim Versand von E-Mails hinzuweisen (vgl. 20. Tätigkeitsbericht 2002 Nr. 9.10).

9 Einwohnermeldewesen

9.1 Änderung melderechtlicher Vorschriften

Die Staatsregierung hat einen Gesetzentwurf zur Änderung melderechtlicher Vorschriften in den Landtag eingebracht (LT-Drucksache 15/6304 vom 19.09.2006). Mit dem Gesetzentwurf sollen im Wesentlichen zwingende bundesrechtliche Vorgaben des Melderechtsrahmengesetzes, das in den letzten Jahren mehrfach geändert worden war, umgesetzt werden. Zu diesen Änderungen zählt u.a. die weitgehende Abschaffung der Abmeldepflicht sowie der Mitwirkungspflicht des Vermieters bei der An- und Abmeldung eines Mieters. Die weitgehende Abschaffung der Abmeldepflicht soll durch eine effektivere Rückmeldung zwischen den beteiligten Meldebehörden auf der Grundlage elektronischer Datenübertragung ausgeglichen werden. Des Weiteren werden in dem Gesetzentwurf in Anpassung an das Melderechtsrahmengesetz zahlreiche Bestimmungen, u.a. das Selbstauskunftsrecht eines Einwohners, die Ausnahmen von der Meldepflicht sowie die besondere Meldepflicht in Beherbergungsstätten, Krankenhäusern, Heimen und ähnlichen Einrichtungen neu gefasst.

Der Gesetzentwurf macht aber auch von den bundesrechtlich eröffneten Regelungsspielräumen des Melderechtsrahmengesetzes Gebrauch. So wird den Meldebehörden künftig beispielsweise ermöglicht, eine Anmeldung mittels eines sog. vorausgefüllten Meldescheins zuzulassen. Die Meldebehörde des Zuzugsortes kann in diesem Falle bestimmte Meldedaten eines Einwohners bei der Meldebehörde des Wegzugsorts elektronisch abrufen und ihm in seiner Anwesenheit oder elektronisch zur Kenntnis geben, um sie zu überprüfen und zu aktualisieren. Dadurch soll der Aufwand des Einwohners und der beteiligten Meldebehörden bei einer Anmeldung reduziert werden sowie der Grad der Richtigkeit der Melderegister erhöht werden. Die Möglichkeit der Anmeldung durch vorausgefüllten Meldeschein soll auch bei einem länderübergreifenden Umzug, soweit dies nach Landesrecht geregelt werden kann, eröffnet werden.

Ich habe mich zu dem Gesetzentwurf, der aufgrund der zahlreichen Änderungen eine Neufassung des Meldegesetzes auf der Grundlage des bisherigen Meldegesetzes vorsieht, geäußert. Dabei habe ich aus datenschutzrechtlicher Sicht begrüßt, dass nunmehr eine klare Unterscheidung zwischen Meldedatenverarbeitung im Auftrag und einer Funktionsübertragung getroffen wird. Im Gegensatz zur Meldedatenverarbeitung im Auftrag, die dadurch gekennzeichnet ist, dass die auftragnehmende Stelle lediglich unterstützende Hilfstätigkeiten ohne eigene Entscheidungsbefugnisse wahrnimmt, wird bei einer Funktionsübertragung die Aufgabe als solche übertragen.

Da eine Funktionsübertragung nicht nur auf einzelne Gemeinden, Zweckverbände und gemeinsame Kommunalunternehmen, sondern auch die auf Anstalt für kommunale Datenverarbeitung in Bayern (AKDB), die im Rahmen der Datenverarbeitung im Auftrag bereits jetzt schon bayernweit für Meldebehörden tätig wird, beabsichtigt ist, könnte faktisch ein landesweites zentrales Melderegister entstehen. Vor diesem Hintergrund habe ich erneut auf die grundsätzlichen Gefahren hingewiesen, die zentrale Datenbestände mit sich bringen. Ich habe außerdem darauf hingewiesen, dass ich es aus datenschutzrechtlicher Sicht nach wie vor für erforderlich halte, dass auch Meldedaten, die im Rahmen einer Funktionsübertragung von anderen Meldebehörden, Zweckverbänden, gemeinsamem Kommunalunternehmen oder von der AKDB verarbeitet werden, nach den einzelnen Gemeinden logisch getrennt voneinander gespeichert werden, wie dies bisher schon bei der AKDB geschieht.

9.2 Melderegisterauskünfte an den Bayerischen Rundfunk bzw. die GEZ

Ich erhalte immer wieder Zuschriften von Bürgern, die nach einem Wohnungswechsel Post von der Gebühreneinzugszentrale (GEZ) erhalten und wissen wollen, wie die GEZ von ihrer neuen Anschrift Kenntnis erlangen konnte. Ich weise deshalb auf Folgendes hin:

Rechtsgrundlage für eine Weitergabe von Melderegisterdaten durch die Einwohnermeldeämter an den Bayerischen Rundfunk bzw. die GEZ ist in der Regel Art. 31 Abs. 4 des Bayerischen Meldegesetzes i.V.m. § 12 a Abs. 1 der Bayerischen Meldedaten-Übermittlungsverordnung. Danach darf die Meldebehörde dem Bayerischen Rundfunk oder der von ihm nach dem Rundfunkgebührenstaatsvertrag beauftragten Stelle (GEZ) zum Zweck der Erhebung und des Einzugs der Rundfunkgebühren im Fall der An- bzw. der Abmeldung oder des Todes u.a. die Anschriften volljähriger Einwohner übermitteln. Die GEZ ist eine Gemeinschaftseinrichtung der ARD-Landesrundfunkanstalten und des Zweiten Deutschen Fernsehens mit der Aufgabe, für die Rundfunkanstalten die Rundfunkgebühren einzuziehen.

Darüber hinaus können Auskünfte aus dem Melderegister an den Bayerischen Rundfunk bzw. die GEZ im Einzelfall nach Art. 31 Abs. 1 MeldeG zulässig sein. Eine Auskunft nach dieser Vorschrift kommt z.B. in Betracht, wenn die GEZ die neue Adresse einer bestimmten Person, die umgezogen ist, wissen will (vgl. auch Nr. 20.4).

Häufig beschweren sich Bürger auch über die Datenverarbeitung durch die GEZ. Für die Kontrolle der Datenerhebung, -verarbeitung und -nutzung personenbezogener Daten durch den Bayerischen Rundfunk und die GEZ bin ich jedoch nicht zuständig. Diese wird durch eigene unabhängige Datenschutzbeauftragte des Rundfunks ausgeübt. Die Vorschriften im Fünften Abschnitt des Bayerischen Datenschutzgesetzes, die u.a. die Zuständigkeit des Bayerischen Landesbeauftragten für den Datenschutz regeln, finden nach Art. 22 Abs. 1 des Bayerischen Rundfunkgesetzes, der nach Art. 2 Abs. 7 BayDSG dem Bayerischen Datenschutzgesetz vorgeht, keine Anwendung. Grund für diese Regelung ist das verfassungsrechtliche Privileg der Rundfunkfreiheit.

10 Steuer- und Finanzverwaltung

10.1 Elektronische Lohnsteuerkarte ELSTERLohn

Zu dem bundesweiten Projekt ELSTERLohn habe ich bereits in früheren Tätigkeitsberichten ausführlich Stellung genommen (u.a. in Nr. 12.2 meines 20. Tätigkeitsberichts 2002 und in Nr. 15.1 meines 21. Tätigkeitsberichts 2004).

Nach § 41 b EStG sind nahezu alle Arbeitgeber verpflichtet, die Lohnsteuerbescheinigungsdaten ihrer Arbeitnehmer auf elektronischem Wege an die Finanzverwaltung zu übermitteln. Für Zwecke der Zuordnung hat der Arbeitgeber dabei nach amtlich festgelegter Regel ein Ordnungsmerkmal - die so genannte eTIN (electronic Taxpayer Identification Number) - aus Namen, Vornamen und Geburtsdatum des Arbeitnehmers zu bilden. Mittelfristig soll die eTIN durch ein für jeden Steuerpflichtigen dauerhaft vergebenes Identifikationsmerkmal ersetzt werden; die gesetzlichen Grundlagen dazu wurden bereits im Steueränderungsgesetz 2003 mit der Einführung der §§ 139 a bis 139 c AO geschaffen.

Für die elektronischen Lohnsteuerbescheinigungsdaten wurden in den Ländern Landesspeicher installiert. Um eine Verarbeitung dieser Daten im Rahmen der Einkommensteuerveranlagung zu ermöglichen, sind Steuerpflichtige mit Einkünften aus nichtselbstständiger Arbeit bei Abgabe der Einkommensteuererklärung gehalten, die ihnen vom Arbeitgeber zugeteilte eTIN gegenüber dem Finanzamt anzugeben. Bei einer Praxisvorführung anlässlich der Pilotierung des Verfahrens wurde mir dargelegt, dass ein Abruf der elektronischen Lohnsteuerbescheinigungsdaten ausschließlich mittels der eTIN erfolgen solle. Aufgrund von möglichen Umzügen des Arbeitnehmers im Zeitraum zwischen der Übermittlung der Lohnsteuerbescheinigungsdaten durch den Arbeitgeber und der Einreichung der Einkommensteuerklärung durch den Steuerbürger müsse dabei auch eine Abrufmöglichkeit aus den Landesspeichern anderer Länder bestehen.

Inzwischen hat die Finanzverwaltung jedoch weitere Suchvarianten realisiert. So ist nunmehr auch eine Suche mit einer nicht gespeicherten, frei eingegebenen eTIN möglich, ebenso eine Suche mit der freien Eingabe von Suchkriterien, also zum Beispiel mit einem beliebigen Namen. Die Finanzverwaltung begründet diese weiteren Suchvarianten mit nicht unerheblichen Falscheingaben der eTIN aufgrund von Schreibfehlern bzw. mit zahlreichen Nichtangaben durch Steuerbürger. Zudem bestehe auch ein Bedarf in den Fällen, in denen Lohndaten bereits vor Einrichtung eines Speicherkontos geprüft werden müssten.

Diese Argumente erscheinen durchaus nachvollziehbar. Aus datenschutzrechtlicher Sicht ist aber darauf hinzuweisen, dass derartige „freie“ und bundesweite Suchmöglichkeiten ein nicht unerhebliches Missbrauchspotential bergen. Das Staatsministerium der Finanzen hat mir auf eine entsprechende Anfrage hin mitgeteilt, dass es diese erhöhten datenschutzrechtlichen Anforderungen an die Sicherstellung der Zulässigkeit jedes einzelnen Abrufs anerkenne. Es habe deshalb festgelegt, dass die „freien“ Suchmöglichkeiten vollständig protokolliert werden müssten. Dabei würden nicht nur der Abruf an sich, sondern auch die verwendeten Suchkriterien in dezentral bei den einzelnen Finanzämtern vorgehaltenen Datenbanken festgehalten.

Auf meine Frage zu den Anweisungen zur Auswertung der Protokolldatei - und dabei insbesondere auch zum Auswahlabstand - hat mir das Staatsministerium der Finanzen mitgeteilt, dass ein von Sachsen entwickeltes maschinelles Auswertungsprogramm seit Oktober 2006 auch in Bayern im Einsatz sei. Es ermögliche dem Hauptsachgebietsleiter Abgabenordnung eine stichprobenartige Überprüfung der durchgeführten Abfragen. Das Staatsministerium der Finanzen beabsichtige, nach etwa einem halben Jahr Erfahrungsberichte der Finanzämter zu den bei der Protokollauswertung erzielten Erkenntnissen anzufordern. Ich werde das Auswertungsprogramm dann aus datenschutzrechtlicher Sicht abschließend beurteilen. Aufgrund der übermittelten Unterlagen sehe ich das Staatsministerium der Finanzen aber auf dem richtigen Weg.

Das Projekt ELSTERLohn zeigt beispielhaft, dass eGovernment-Anwendungen seitens der Finanzverwaltung mit hohem Tempo weiterentwickelt werden, ohne dass bereits in allen Fällen von Anfang an alle aus (datenschutz-)rechtlicher Sicht wünschenswerten Komponenten vorliegen. In diesem Zusammenhang darf ich auch auf meine Ausführungen zum ELSTEROnline-Portal (Nr. 10.2 dieses Tätigkeitsberichts) hinweisen.

10.2 ELSTEROnline-Portal

Auch zum bundesweiten Projekt ELSTER (Elektronische Steuererklärung) insgesamt habe ich in der Vergangenheit bereits mehrmals Stellung genommen. Im Berichtszeitraum haben sich aus datenschutzrechtlicher Sicht indes einige bedeutsame Entwicklungen ergeben.

Die Abgabenordnung sieht in § 150 Abs. 6 AO die Möglichkeit vor, Steuererklärungen oder sonstige für das Besteuerungsverfahren erforderliche Daten ganz oder teilweise auf maschinell verwertbaren Datenträgern oder durch Datenfernübertragung zu übermitteln; die Einführung eines derartigen Übermittlungsverfahrens ist aber an den Erlass einer Rechtsverordnung gebunden. § 87 a Abs. 3 AO bestimmt, dass eine durch Gesetz für Anträge, Erklärungen oder Mitteilungen an die Finanzbehörden angeordnete Schriftform durch die elektronische Form ersetzt werden kann; in diesem Fall ist das elektronische Dokument mit einer sog. „qualifizierten elektronischen Signatur“ nach dem Signaturgesetz zu versehen. Aufgrund der relativ geringen Verbreitung derartiger Signaturen war allerdings gem. § 87 a Abs. 6 AO bis zum 31.12.2005 auch der Einsatz einer qualifizierten elektronischen Signatur mit Einschränkungen nach Maßgabe einer Rechtsverordnung im Sinne des § 150 Abs. 6 AO möglich. Das Bundesministerium der Finanzen hat von den Ermächtigungen der §§ 87 a Abs. 6, 150 Abs. 6 AO Gebrauch gemacht und am 28.01.2003 die Steuerdaten-Übermittlungsverordnung (StDÜV) erlassen, deren § 7 bestimmt, dass in der genannten Übergangszeit auch sog. „fortgeschrittene elektronische Signaturen“ als ausreichend angesehen werden konnten.

Durch das Steueränderungsgesetz 2003 wurden Unternehmer und Arbeitgeber verpflichtet, Umsatzsteuer-Voranmeldungen, Lohnsteuer-Anmeldungen und Lohnbescheinigungen ab 2005 ausschließlich auf elektronischem Wege nach Maßgabe der genannten Steuerdaten-Übermittlungsverordnung abzugeben.

Problematisch ist, dass eine sichere Authentifizierung der Verpflichteten an sich nur durch den Einsatz einer „qualifizierten elektronischen Signatur“ zu gewährleisten ist. Nachdem darauf allerdings, wie oben dargestellt, bis zum 31.12.2005 verzichtet wurde, stellte sich die Frage nach einem anderen geeigneten Authentifizierungsverfahren. Ein nach Ansicht der Finanzverwaltung ausreichendes Authentifizierungsverfahren konnte von dieser aber erst in der zweiten Jahreshälfte 2005 vorgestellt werden.

Die Forderung der Datenschutzbeauftragten des Bundes und der Länder, aufgrund dieser Sachlage die Abgabe der genannten Steueranmeldungen und -bescheinigungen bis zum Vorliegen eines geeigneten Authentifizierungsverfahrens weiterhin auch in Papierform zuzulassen, konnte gegenüber der Finanzverwaltung jedoch nicht durchgesetzt werden.

Das ELSTEROnline-Portal ermöglicht allerdings nicht nur die elektronische Abgabe der bereits erwähnten Steueranmeldungen durch Unternehmer und Arbeitgeber, sondern auch die elektronische Einreichung der persönlichen Steuererklärungen, und zwar ohne dass - wie in der Vergangenheit - zusätzlich auch in Papierform eine eigenhändig unterschriebene (komprimierte) Steuererklärung übermittelt werden muss. Zur Nutzung dieses Portals ist jedoch die Erteilung eines Software-Zertifikats erforderlich. Von der Finanzverwaltung werden diesbezüglich drei Verfahren zur Auswahl angeboten:

- Auf dem persönlichen Rechner des Steuerbürgers wird ein Softwareschlüssel erzeugt, der bei Bedarf über eine PIN aktiviert werden muss.

- Der Softwareschlüssel wird auf dem so genannten „ELSTERStick“, einem dem Memory-Stick ähnlichen USB-Gerät, abgelegt.

- Schließlich ist auch die Nutzung der von ausgewählten Banken und Unternehmen ausgegebenen Smartcards möglich. Das persönliche Zertifikat befindet sich in diesem Fall auf der verwendeten Signaturkarte.

Zur rechtlichen Absicherung dieses Software-Zertifikats wurde mir zeitgleich mit Beginn des Pilotbetriebs des ELSTEROnline-Portals im Oktober 2005 ein Entwurf einer Ersten Verordnung zur Änderung der Steuerdaten-Übermittlungsverordnung (1.StDÜVÄndV-E) vorgelegt. Obwohl der Gesetzgeber, wie oben dargestellt, in § 87 a Abs. 6 AO nur bis zum 31.12.2005 die Verwendung der „fortgeschrittenen elektronischen Signatur“ für die Übermittlung von Steuerdaten als ausreichend angesehen hatte, sollte durch § 6 1.StDÜVÄndV-E diese gesetzlich angeordnete zeitliche Limitierung durch Rechtsverordnung praktisch unbegrenzt hinausgeschoben werden. Dies widersprach aber nicht nur der Intention des Gesetzgebers; vielmehr konnte sich die mit § 6 des damaligen Entwurfs beabsichtigte Regelung schon nicht auf die erforderliche Ermächtigungsgrundlage stützen.

Von dieser rechtlichen Problematik zu trennen ist allerdings die praktische Frage, ob in Anbetracht der nach wie vor mäßigen Verbreitung der „qualifizierten elektronischen Signatur“ - selbstverständlich nach Schaffung der entsprechenden Rechtsgrundlage - nicht auch andere Verfahren an deren Stelle treten könnten. Derzeit bleibt aber festzuhalten, dass seit dem 01.01.2006 bei elektronischer Einreichung der persönlichen Steuererklärung die Anwendung der „qualifizierten elektronischen Signatur“ nach § 87 a Abs. 3 AO zwingend ist.

Das von mir um Stellungnahme gebetene Staatsministerium der Finanzen hat insoweit das Bestehen einer gesetzlichen Lücke seit dem 01.01.2006 eingeräumt. Diese wurde Ende November 2006 - rechtssystematisch zutreffend - durch Neufassung des § 87 a Abs. 6 AO im Rahmen des Jahressteuergesetzes 2007 beseitigt. Neben der „qualifizierten elektronischen Signatur“ kann nun bis zum 31. Dezember 2011 ein anderes sicheres Verfahren zugelassen werden. Eine mit den Regelungen des Signaturgesetzes vergleichbare gesetzliche Definition von Bedingungen für ein derartiges „anderes Verfahren“ besteht allerdings zurzeit nicht. Die bisher vorliegenden Informationen über die Ausgestaltung des Verfahrens ermöglichen noch keine abschließende datenschutzrechtliche Bewertung. In der Folge des neu gefassten § 87 a Abs. 6 AO soll jedenfalls die StDÜV angepasst werden.

Die in Bayern und Nordrhein-Westfalen eingerichteten Clearingstellen - als zentrale Annahme- und Verteilstellen für die im Rahmen von ELSTER eingehenden elektronischen Steuerdaten - wurden von mir in früheren Tätigkeitsberichten bereits thematisiert. Ich habe in diesem Zusammenhang eine Klärung der rechtlichen Stellung dieser Clearingstellen gefordert.

Das Staatsministerium der Finanzen teilte mir bereits zum damaligen Zeitpunkt mit, dass Regelungen zur rechtlichen Stellung der Clearingstellen in eine in Arbeit befindliche Verwaltungsvereinbarung aufgenommen werden sollten. Eine entsprechende Verwaltungsvereinbarung wurde aber nicht abgeschlossen.

Durch Beschluss der Finanzminister der Länder wurde inzwischen die Verantwortung für die Entwicklung einer einheitlichen Software in der Steuerverwaltung auf die Länder Baden-Württemberg, Bayern, Hessen, Niedersachsen und Nordrhein-Westfalen (unter Mitwirkung des Bundes) übertragen. Das Projekt firmiert unter dem Namen KONSENS (Koordinierte neue Software-Entwicklung der Steuerverwaltung) und umfasst eine Vielzahl von bisher getrennt entwickelten Projekten, darunter auch ELSTER.

Das Projekt basiert auf einer Verwaltungsvereinbarung, die am 01.01.2007 in Kraft treten wird. Die Verwaltungsvereinbarung regelt in der Hauptsache die Beschaffung, Entwicklung, Pflege und den Einsatz einheitlicher Software für das Besteuerungsverfahren. Datenschutzrechtliche Komponenten sind allerdings nicht der Inhalt der Vereinbarung. Auch werden die Clearingstellen nicht explizit erwähnt. Es wird nur vereinbart, dass einheitliche Software von zentralen Produktions- und Servicestellen - wie sie die Clearingstellen darstellen - für alle Vertragspartner eingesetzt und administriert werden können.

Bezüglich der Clearingstellen, deren rechtliche Stellung und deren Handeln ursprünglich in einer eigenen Verwaltungsvereinbarung geregelt werden sollten, stellt der nunmehr erfolgte Abschluss der Verwaltungsvereinbarung zu KONSENS daher einen Rückschritt dar.

Das Staatsministerium der Finanzen vertritt in diesem Zusammenhang darüber hinaus die Auffassung, dass die grundlegende Entscheidung für die Übertragung von Aufgaben auf die erwähnten zentralen Produktions- und Servicestellen von den Referatsleitern Automation (Steuer) der Länder und des Bundes zu treffen sei. Ich interpretiere diese Aussage nach meinem derzeitigen Kenntnisstand so, dass diese grundlegende Entscheidung auch datenschutzrechtliche Gesichtspunkte umfasst. Hier sehe ich noch weiteren Diskussionsbedarf.

Die Ausführungen zeigen, dass die Finanzverwaltung das (Prestige-) eGovernment-Projekt ELSTEROnline-Portal auch im Berichtszeitraum mit hohem Tempo weiter entwickelt hat. Festzustellen ist, dass aufgrund der rasanten technischen Entwicklung nicht in allen Teilbereichen rechtzeitig - das heißt vor einer Pilotierung eines Verfahrens - die erforderlichen rechtlichen Regelungen vorliegen. Dies erscheint allenfalls in Ausnahmefällen hinnehmbar; nicht nur aus datenschutzrechtlicher Sicht darf dies aber keinesfalls zur Regel werden.

10.3 Datenabgleich zwischen den Finanzämtern und der Staatsoberkasse für Zwecke der Aufrechnung

Im Wege eines Verbesserungsvorschlags regte ein Bediensteter der Finanzverwaltung an, mittels eines maschinellen Verfahrens Aufrechnungsmöglichkeiten von Steuerforderungen gegen Verbindlichkeiten des Freistaats zu überprüfen. Der Vorschlag war ursprünglich auf den Bereich der Bauwirtschaft beschränkt. Das daraufhin entworfene und mittlerweile mehrfach modifizierte umfassende elektronische Datenabgleichsverfahren bezieht sich im aktuellen Planungsstadium aber auf alle Unternehmen. Kern des Verfahrens ist der Abgleich einer einmal täglich von der Steuerverwaltung übermittelten Steuerrückständedatei mit einer auf dieser Basis aufgebauten Auszahlungsdatei bei der Staatsoberkasse Bayern.

Aus Sicht des Staatsministeriums der Finanzen ist es zur Vermeidung von Vollstreckungsmaßnahmen wünschenswert, vor jeder Auszahlung an einen Unternehmer im Falle von an den Freistaat erbrachten Lieferungen oder Leistungen zu prüfen, ob verrechenbare Steuerrückstände bestehen.

So lässt § 226 AO unter den dort genannten Voraussetzungen die Aufrechnung mit Ansprüchen und gegen Ansprüche aus dem Steuerschuldverhältnis zu. Bei der Aufrechnung erfolgt eine zumindest teilweise wechselseitige Tilgung zweier sich gegenüberstehender gleichartiger Ansprüche durch Verrechnung aufgrund einseitiger Erklärung eines der Beteiligten. Nr. 34.2 VV zu Art. 70 BayHO bestimmt in diesem Zusammenhang: „Ist ein Einzahlungspflichtiger mit einer Einzahlung an die Kasse im Rückstand und ist ihr bekannt, dass er einen Anspruch gegen eine andere Staatskasse auf Auszahlung eines Betrages hat, so hat die Kasse ihre Forderung der anderen Staatskasse mitzuteilen und sie zu ersuchen, mit dieser Forderung gegen den Anspruch des Einzahlungspflichtigen aufzurechnen. Ist der für die Einziehung zuständigen Kasse eine konkrete Forderung nicht bekannt, soll sie in der Regel auch dann nach Satz 1 verfahren, wenn ein Anspruch auf Auszahlung eines anderen Betrages durch eine andere Kasse möglich ist (z.B. Steuererstattungsanspruch).“

In meinen Stellungnahmen gegenüber dem Staatsministerium der Finanzen habe ich mehrfach deutlich gemacht, dass mir diese Sicht zwar durchaus nachvollziehbar erscheint, ein solches umfassendes elektronisches Datenabgleichsverfahren aber dennoch datenschutzrechtlichen Kriterien genügen muss.

Dies ist nach dem derzeitigen Planungsstand allerdings leider nicht der Fall:

- So stellt sich bereits grundsätzlich die Frage nach einer normenklaren Rechtsgrundlage für das Verfahren. Schon als bloße Verwaltungsvorschrift kann Nr. 34.2 VV zu Art. 70 BayHO keine Rechtsgrundlage für das geplante maschinelle Datenabgleichsverfahren darstellen. Von Wortlaut und Sinn und Zweck her bezieht sich Nr. 34.2 VV zu Art. 70 BayHO allein auf die bisherige - allerdings in vergleichsweise geringem Umfang durchgeführte - Praxis des manuellen Abgleichs.

- Meiner Auffassung nach sind bei der derzeitigen Beschränkung des Verfahrens auf den Freistaat die Erhebung und die - auch nur temporäre - Speicherung der Daten von leistenden Unternehmern mit Sitz außerhalb Bayerns unzulässig.

  Bei dem geplanten Verfahren stellt sich deshalb die Frage, mittels welcher identifizierenden Daten der Ausschluss außerbayerischer Unternehmer erfolgen soll. Nach Ansicht des Staatsministeriums scheiden die bei den Behörden zumeist unterschiedlich gespeicherten Adressdaten insoweit aufgrund der unverhältnismäßig hohen Nacharbeiten aus. Das Finanzministerium bevorzugt deshalb einen Abgleich über die Steuernummer. Nach § 14 Abs. 4 Nr. 2 UStG muss eine Rechnung jedoch entweder die vom Finanzamt erteilte Steuernummer oder die vom Bundeszentralamt für Steuern erteilte Umsatzsteuer-Identifikationsnummer enthalten. So lässt die Angabe der Steuernummer zwar in der Regel einen zuverlässigen Rückschluss auf das Sitzland des leistenden Unternehmers zu; aufgrund der Angabe der Umsatzsteuer-Identifikationsnummer ist eine zuverlässige Abgrenzung zwischen bayerischen und nichtbayerischen Unternehmern jedoch nicht möglich. Aus diesen Gründen verbleibt für das Abgleichsverfahren als einziges eindeutig abgrenzbares Ordnungskriterium die Steuernummer; diese liegt allerdings nicht in allen Fällen vor.

- Schließlich habe ich das Staatsministerium der Finanzen darauf hingewiesen, dass eine Beschränkung des Verfahrens auf den Freistaat zu einer Ungleichbehandlung von bayerischen Unternehmen gegenüber außerbayerischen Unternehmen führt.

- Über diese grundsätzlichen Probleme hinaus bestehen auch noch zahlreiche klärungsbedürftige Detailfragen, die zumeist aus dem Fehlen einer normenklaren Rechtsgrundlage resultieren.

Aus meiner Sicht ist deshalb für einen dauerhaften und (nicht nur datenschutz-)rechtlich gesicherten Betrieb des geplanten umfassenden elektronischen Datenabgleichsverfahrens die Schaffung einer normenklaren gesetzlichen Regelung unumgänglich. Zur Vermeidung von Ungleichbehandlungen bevorzuge ich dabei eine bundesgesetzliche Regelung.

10.4 Optimierung der Kraftfahrzeugsteuer-Erhebung

Mit dem durch das „Zweite Gesetz zur Änderung des Kraftfahrzeugsteuergesetzes“ vom 01. August 2002 geänderten § 13 KraftStG wurde den Ländern die Möglichkeit eröffnet, durch Erlass einer Rechtsverordnung die Erhebung der Kraftfahrzeugsteuer neu zu gestalten. Die Aushändigung des Fahrzeugscheins durch die Zulassungsbehörde kann nunmehr auch davon abhängig gemacht werden, dass eine Ermächtigung zum Einzug der Kraftfahrzeugsteuer vom

Konto des Fahrzeughalters bei einem Geldinstitut erteilt worden ist (§ 13 Abs. 1 Satz 2 KraftStG). Zudem besteht nun die Möglichkeit, die Aushändigung des Fahrzeugscheins durch die Zulassungsbehörde auch davon abhängig zu machen, dass der Fahrzeughalter keine Kraftfahrzeugsteuerrückstände hat (§ 13 Abs. 1 a KraftStG).

In Anbetracht der bayernweit hohen Kraftfahrzeugsteuerrückstände einerseits und des erheblichen Missverhältnisses zwischen Vollstreckungsaufwand und Rückstandshöhe im jeweiligen Einzelfall andererseits hat das Staatsministerium der Finanzen beschlossen, von der neuen Verordnungsermächtigung Gebrauch zu machen. Im Verordnungserlassverfahren wurde auch ich beteiligt. Ich habe dabei aus datenschutzrechtlicher Sicht folgenden Standpunkt vertreten:

– Die Bekanntgabe der Kontonummer im Rahmen des obligatorischen Lastschriftverfahrens stellt zweifelsohne einen Eingriff in das Persönlichkeitsrecht dar. Angesichts der unverhältnismäßig hohen Bindung von Vollstreckungspersonal durch die Beitreibung der Kraftfahrzeugsteuerrückstände habe ich aber den in der Verpflichtung zur Bekanntgabe eines Kontos liegenden Eingriff für vertretbar gehalten.

  Im Übrigen erfolgt die Beitreibung von Kraftfahrzeugsteuerrückständen bei Arbeitnehmern vielfach durch sog. Lohnpfändungen. Bei dieser Art der Vollstreckung wird die Tatsache eines Steuerrückstands zwangsläufig dem Arbeitgeber bzw. Dienstherrn des Betroffenen bekannt, was sich durchaus negativ auf die weitere Ausgestaltung des Arbeitsverhältnisses auswirken kann. Auch dies spricht für das mildere Mittel der Bekanntgabe der Kontonummer durch den Betroffenen selbst.

– Mittels einer von der Finanzverwaltung elektronisch zur Verfügung gestellten Rückständedatei nehmen die Zulassungsbehörden eine tagesaktuelle Prüfung der Kraftfahrzeugsteuerrückstände vor. Zur Wahrung des in § 30 AO verankerten Steuergeheimnisses bestimmt § 13 Abs. 1 a Satz 6 KraftStG ausdrücklich, dass die Zulassungsbehörden in diesem Fall als Landesfinanzbehörden tätig werden. Durch diese Festlegung sehe ich eine hinreichende Zweckbindung der übermittelten Daten gegeben.

– Aus datenschutzrechtlicher Sicht regelungsbedürftig habe ich die näheren Umstände bei der Zulassung eines Kraftfahrzeugs durch Dritte erachtet:

  Nach § 13 Abs. 1 a Satz 3 Halbsatz 2 KraftStG ist in der Rechtsverordnung zu regeln, dass in Fällen, in denen das Fahrzeug nicht durch den Steuerpflichtigen selbst zugelassen wird, die Zulassung eine Einverständniserklärung des Steuerpflichtigen mit der Bekanntgabe seiner kraftfahrzeugsteuerlichen Verhältnisse an denjenigen, der das Fahrzeug zulässt, voraussetzt.

  In diesem Zusammenhang habe ich es zunächst für wünschenswert gehalten, die Bürger über diese Regelung in geeigneter Form bereits vor dem Gang zur Zulassungsbehörde zu informieren. Für datenschutzrechtlich notwendig habe ich es sogar gehalten, entsprechende Einverständniserklärungsformulare zu konzipieren und auch downloadbar ins Internet einzustellen.

  Zudem habe ich darum gebeten, in der Praxis darauf zu achten, dass bei Vorlage einer Vollmacht, die nicht ausdrücklich auch eine Einverständniserklärung zur Mitteilung der kraftfahrzeugsteuerlichen Verhältnisse an den Dritten enthält, eine Zulassung durch den Dritten nicht erfolgen darf. In den Fällen der Vorlage einer bloßen „Zulassungs-Vollmacht“ darf die Zulassung also nicht erst von einer Abfrage der bestehenden Kraftfahrzeugsteuerrückstände abhängig gemacht werden; sonst würde der Dritte - selbst dann, wenn ihm bei bestehenden Rückständen ohne weitere Erläuterungen die Zulassung verweigert wird - über die grundsätzliche Tatsache bestehender Steuerrückstände (mittelbar) informiert. Dies muss aber auf jeden Fall vermieden werden.

Die „Verordnung über die Mitwirkung der Zulassungsbehörden bei der Verwaltung der Kraftfahrzeugsteuer (MZuKraftStV)“ ist am 01.08.2005 in Kraft getreten. Das Staatsministerium der Finanzen hat das von mir angeregte Einverständnisformular entwickelt. Es liegt in den Zulassungsbehörden und in den Finanzämtern auf und steht auch auf den Internet-Servern der bayerischen Steuerverwaltung zum Download zur Verfügung.

10.5 Datenübermittlung der Finanzämter an die Kirchensteuerämter bei glaubensverschiedenen Ehen

Mehrere Bürgerinnen und Bürger, die im Gegensatz zu ihrem Ehegatten keiner Umlage erhebenden Religionsgemeinschaft angehören, haben sich im Berichtszeitraum an mich gewandt und in einer durch die Finanzverwaltung erfolgten Übermittlung von Steuerdaten an das für ihren Ehegatten zuständige

evangelisch-lutherische Kirchensteueramt ihr informationelles Selbstbestimmungsrecht verletzt gesehen.

Zu dieser Problematik nehme ich aus datenschutzrechtlicher Sicht wie folgt Stellung:

Die derzeitige Praxis der Datenübermittlung zwischen Finanzverwaltung und Kirchensteuerämtern gründet sich auf folgende Rechtsvorschriften:

Nach Art. 140 GG i.V.m. Art. 137 Weimarer Reichsverfassung regeln die Kirchen ihre Angelegenheiten selbst. Ein Ausfluss dieser verfassungsrechtlichen Bestimmungen ist die Einrichtung von Kirchensteuerämtern in Bayern (Art. 17 KirchStG). Die Finanzverwaltung hat den Kirchensteuerämtern gem. § 17 Verordnung zur Ausführung des Kirchensteuergesetzes die für die Festsetzung der Kirchensteuer maßgebenden Besteuerungsgrundlagen mitzuteilen.

Das Steuergeheimnis hindert die Finanzverwaltung an der Mitteilung nicht, da § 31 Abs. 1 AO insoweit ausdrücklich die Datenübermittlung der zur Festsetzung der Kirchensteuer erforderlichen Besteuerungsgrundlagen erlaubt. Die Mitteilung erfolgt im Rahmen eines Datenträgeraustausches. Ein Online-Zugriff der Kirchensteuerämter auf Daten der Finanzämter besteht nicht.

Die Berechnung der Kirchensteuer des Ehegatten, der einer Kirchensteuer erhebenden Religionsgemeinschaft angehört, setzt voraus, dass zunächst errechnet wird, wie viel an der im Rahmen der Zusammenveranlagung festgesetzten Einkommensteuer auf ihn entfällt. Bei gemeinsamer Veranlagung zur Einkommensteuer in glaubensverschiedenen Ehen ist daher nach Art. 9 Abs. 2 KirchStG die gemeinsame Einkommensteuer im Verhältnis der Einkünfte jedes Ehegatten aufzuteilen.

Zur Durchführung dieses Rechenvorgangs teilte in der Vergangenheit die Finanzverwaltung dem jeweiligen Kirchensteueramt die festgesetzte gemeinsame Einkommensteuer und für jeden Ehegatten den Gesamtbetrag seiner Einkünfte mit. Das Kirchensteueramt errechnete daraus den Anteil des Kirchenmitglieds an der gemeinsamen Einkommensteuer und setzte hieraus die Kirchensteuer fest.

Eine Verkomplizierung ist durch das ab dem Veranlagungsjahr 2002 anzuwendende Halbeinkünfteverfahren bei den Einkünften aus Kapitalvermögen entstanden. Der Gesetzgeber hat es in diesem Zusammenhang für erforderlich gehalten, für die so genannten Zuschlagsteuern - also die Steuern, die nach der Einkommensteuer bemessen werden (u.a. die Kirchensteuer) - eine von der im Rahmen der Einkommensteuerveranlagung festgesetzten Einkommensteuer abweichende (fiktive) Bemessungsgrundlage zu definieren. Nähere Einzelheiten finden sich in § 51 a EStG. Das für Veranlagungszeiträume vor 2002 geschilderte Beispiel wird somit, bei Vorliegen entsprechender Kapitaleinkünfte, mit fiktiv errechneten Gesamtbeträgen der Einkünfte und einer fiktiven Einkommensteuer durchgeführt.

Festzustellen ist, dass für die Kirchensteuerberechnung nach wie vor auch Angaben zu dem keiner Religionsgemeinschaft angehörenden Ehegatten erforderlich sind. Eine Datenübermittlung der Finanzverwaltung an die Kirchensteuerämter ließe sich also nur durch einen Antrag auf getrennte Veranlagung vermeiden, was in der Regel aber zu einer höheren Gesamtsteuerbelastung der Ehegatten führen würde.

Einen Sonderfall stellt die Erhebung von Kirchgeld dar. Hierzu bestimmen die Art. 20 ff. KirchStG, dass die Erhebung nach Maßgabe der von den Kirchgeld erhebenden Steuerverbänden erlassenen Steuerordnungen erfolgt. Solche Steuerordnungen sind insbesondere die „Ordnung über die Erhebung von Kirchensteuern in den bayerischen (Erz-) Diözesen“ und das „Kirchengesetz über die Erhebung von Kirchensteuern der Evangelisch-Lutherischen Kirche in Bayern - KirchStErhebG)“.

§ 6 KirchStErhebG bestimmt als Bemessungsgrundlage für die Höhe des so genannten „besonderen Kirchgeldes“ in glaubensverschiedenen Ehen das gemeinsam zu versteuernde Einkommen der zusammenverlangten Ehegatten. Die Erzielung von eigenen Einkünften des der Kirche angehörenden Ehegatten ist dabei nicht Voraussetzung.

In diesem Sonderfall muss von den Finanzbehörden also auch das zu versteuernde Einkommen der zusammenveranlagten Ehegatten an das evangelisch-lutherische Kirchensteueramt übermittelt werden. Die gesetzliche Grundlage für die Datenübermittlung seitens der Finanzverwaltung stellt, wie bereits erwähnt, § 31 Abs. 1 AO dar. Danach sind die Finanzbehörden berechtigt, Besteuerungsgrundlagen u.a. an die Religionsgemeinschaften zur Festsetzung von solchen Abgaben mitzuteilen, die an diese Besteuerungsgrundlagen anknüpfen.

Aufgrund dieser spezialgesetzlichen Regelungen liegt ein Verstoß gegen Datenschutzbestimmungen in den von den Bürgern geschilderten Sachverhalten nicht vor. Allerdings ist auch meiner Auffassung nach die derzeitige Praxis unbefriedigend. Eine Änderung wird allerdings durch die in diesem Zusammenhang ergangene Rechtsprechung erschwert (vgl. nur den Beschluss des Finanzgerichts München vom 31.05.1988, Az.: XIII 277/87 EA, EFG S. 530, und die neueren Urteile des BFH vom 19.10.2005, Az.: I R 76/04, und vom 25.01.2006, Az.: I R 62/05).

10.6 Datenaustausch zwischen der Staatlichen Lotterieverwaltung und den Kommunen zur Untersagung illegaler Sportwetten

Durch eine Eingabe wurde ich auf folgende Praxis der Staatlichen Lotterieverwaltung aufmerksam: Sobald die Staatliche Lotterieverwaltung vom Anbieten illegaler Sportwetten (vgl. insoweit BVerfG, Urteil vom 28.03.2006, Az.: 1 BvR 1054/01) Kenntnis erlangt, wendet sie sich an die jeweils zuständige kommunale Ordnungsbehörde mit der Bitte, umgehend Maßnahmen zur Unterbindung dieses Verhaltens einzuleiten. Zudem bittet die Staatliche Lotterieverwaltung darum, ihr den jeweils aktuellen Verfahrensstand mitzuteilen. Da das entsprechende (Standard-)Schreiben der Staatlichen Lotterieverwaltung durch Gestaltung und Formulierung behördlichen Anschein erweckt, gehen die kommunalen Ordnungsbehörden nach meinen Erkenntnissen davon aus, der Staatlichen Lotterieverwaltung gegenüber zu Amtshilfemaßnahmen verpflichtet zu sein, und entsprechen den geäußerten Bitten.

Nach eingehender Prüfung der Rechtslage habe ich die dargestellte Praxis der Staatlichen Lotterieverwaltung aus datenschutzrechtlicher Sicht wie folgt bewertet:

Zunächst ist festzuhalten, dass sich die Staatliche Lotterieverwaltung im Zuge einer in der Vergangenheit mit mir geführten Diskussion zur datenschutzrechtlichen Einordnung ihrer Geschäftstätigkeit selbst insoweit als Wettbewerbsunternehmen im Sinne des Art. 3 BayDSG bezeichnet hat; sie hat in diesem Zusammenhang wörtlich ausgeführt: „Bei ihrer Geschäftstätigkeit nach außen ist sie nicht Behörde im Sinne des Art. 1 BayVwVfG. … Vielmehr tritt sie hier als staatliches Wirtschaftsunternehmen lediglich im Bereich des allgemeinen Rechts- und Geschäftsverkehrs auf und verfügt dabei über keinerlei öffentlich-rechtliche Befugnisse."

Die Zulässigkeit einer Datenübermittlung von der kommunalen Ordnungsbehörde an die Staatliche Lotterieverwaltung während eines laufenden Verwaltungsverfahrens bemisst sich nach Art. 29 BayVwVfG. Nach Art. 29 Abs. 1 Satz 1 BayVwVfG hat die Behörde den Beteiligten Einsicht in die einzelnen Teile der das Verfahren betreffenden Akten zu gestatten, soweit deren Kenntnis zur Geltendmachung oder Verteidigung ihrer rechtlichen Interessen erforderlich ist.

Da die Staatliche Lotterieverwaltung aber in den geschilderten Verfahren nicht Beteiligte im Sinne des Art. 13 BayVwVfG ist, besteht kein Anspruch auf Akteneinsicht bzw. auf Datenübermittlung gem. Art. 29 Abs. 1 Satz 1 BayVwVfG.

Nach der Rechtsprechung des Bayerischen Verwaltungsgerichtshofs besteht ein Rechtsanspruch eines Nicht-Beteiligten auf Akteneinsicht außerhalb eines Verwaltungsverfahrens zwar grundsätzlich nicht; ein solcher Anspruch kann jedoch in Betracht kommen, wenn der Antragsteller ein berechtigtes Interesse hieran geltend macht. Nach Auffassung des Bayerischen Verwaltungsgerichtshofs ist die Gewährung von Akteneinsicht im Rahmen einer Ermessensentscheidung dabei so zu treffen, dass „unter Berücksichtigung des Grundprinzips des rechtsstaatlichen, fairen Verfahrens eine beiderseits sachgerechte Interessenwahrung möglich ist"; zudem muss die „Kenntnis des Akteninhalts ... Voraussetzung für eine wirksame Rechtsverfolgung sein" (vgl. BayVGH, BayVBl 1998, 693 ff; NVwZ 1999, 889 f. m.w.N.).

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 - hier die Staatliche Lotterieverwaltung - 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 Einzelfalles 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. dazu Wilde/Ehmann/Niese/Knoblauch, Bayerisches Datenschutzgesetz, Kommentar, München, Stand: 2006, Art. 19 BayDSG Rdnr. 15.)

Ein solches berechtigtes Interesse am Fortgang einer gegenüber einer kommunalen Ordnungsbehörde erstatteten Anzeige ist der Staatlichen Lotterieverwaltung zwar grundsätzlich zuzugestehen. Es ist aber darauf hinzuweisen, dass bei einer Datenübermittlung nach den Grundsätzen des Art. 19 Abs. 1 Nr. 2 BayDSG die übermittelnde Stelle eine umfassende Abwägung vorzunehmen hat. Diese Abwägung hat nicht nur das „Ob" einer Datenübermittlung sondern auch deren Umfang zu umfassen. Insbesondere resultiert aus Art. 19 Abs. 1 Nr. 2 BayDSG keine Verpflichtung zu einer Datenübermittlung, also kein Anspruch des potenziellen Datenempfängers. Zudem hat die übermittelnde Stelle den Betroffenen unter Beachtung der Vorgaben des Art. 19 Abs. 3 BayDSG grundsätzlich von der Übermittlung seiner Daten zu unterrichten.

Die erforderliche Abwägung kann in der Praxis allerdings nur dann seriös vorgenommen werden, wenn die Staatliche Lotterieverwaltung in ihren Schreiben an die kommunalen Ordnungsbehörden nicht - zumindest unterschwellig - den Anschein erweckt, ihr gegenüber zu Amtshilfemaßnahmen verpflichtet zu sein.

Ich habe mich deshalb an die Staatliche Lotterieverwaltung mit der Forderung gewandt, entsprechende Umformulierungen in den verwendeten Standardschreiben vorzunehmen. Die Staatliche Lotterieverwaltung hat mir inzwischen ein neu formuliertes Formschreiben übermittelt, das meinen Bedenken Rechnung trägt.

10.7 Datenschutzrechtliche Einordnung der Süddeutschen Klassenlotterie und der Staatlichen Lotterieeinnahmen

Im Berichtszeitraum erreichten mich wieder zahlreiche Eingaben aus dem Lotteriebereich. Die Beschwerden betrafen überwiegend unerwünschte Werbemaßnahmen der im Auftrag der Süddeutschen Klassenlotterie (SKL) tätigen bayerischen Staatlichen Lotterieeinnahmen. Dies habe ich zum Anlass genommen, der bisher offensichtlich ungeprüften Frage der datenschutzrechtlichen Einordnung der SKL und ihrer Vertriebsorganisation nachzugehen.

Losvertriebsverfahren

Die SKL selbst ist nicht mit dem Vertrieb der Lose befasst; vielmehr erfolgt dieser im Namen und für Rechnung der SKL ausschließlich durch die ca. 140 sog. Staatlichen Lotterieeinnahmen und die rund 1.900 sog. Amtlichen Verkaufsstellen. Demzufolge werben die Staatlichen Lotterieeinnahmen und Amtlichen Verkaufsstellen auch selbstständig um Kunden. Zur Durchführung einer Verkaufsaktion mieten Staatliche Lotterieeinnahmen zum Beispiel bei einem privaten Adresshändler Adressen an und beauftragen sodann ein selbstständiges Call Center mit der Durchführung einer Telefonakquise. Aufgrund dieser Sachlage verfügt die SKL selbst nur in geringem Umfang über Kunden- und Werbedateien (im Wesentlichen eine Liste aller Gewinner mit Gewinnen über 50.000 Euro und eine Liste der sog. Showkandidaten - die Bewerber und Teilnehmer an der 5-Millionen-SKL-Show im Fernsehen).

Süddeutsche Klassenlotterie

Nach Art. 1 des „Staatsvertrags zwischen den Ländern Baden-Württemberg, Bayern, Hessen, Rheinland-Pfalz, Sachsen und Thüringen über eine Staatliche Klassenlotterie“ (im Folgenden: SKL-Staatsvertrag) aus dem Jahr 1992 veranstalten die Vertragsländer eine staatliche Klassenlotterie unter der Bezeichnung Süddeutsche Klassenlotterie; diese ist eine rechtsfähige Anstalt des öffentlichen Rechts mit Sitz in München. Organe der Anstalt sind gem. Art. 2 des SKL-Staatsvertrags der Staatslotterieausschuss und die Direktion. Während der aus Vertretern der Trägerländer bestehende Staatslotterieausschuss gem. Art. 4 des SKL-Staatsvertrags vor allem die Geschäftsführung überwacht und die Grundzüge der Geschäftspolitik bestimmt, vertritt die Direktion gem. Art. 5 des SKL-Staatsvertrags die Anstalt gerichtlich und außergerichtlich und führt deren Geschäfte - grob gesagt die Abwicklung der Lotterien. Nach Art. 11 des SKL-Staatsvertrags unterliegt die Anstalt der Aufsicht der Finanzministerien der Vertragsländer, die in zweijährigem Turnus abwechselnd von jedem Vertragsland in alphabetischer Reihenfolge der Länder ausgeübt wird.

Im Gegensatz beispielsweise zum ZDF-Staatsvertrag, nach dessen § 16 das Landesdatenschutzgesetz des Landes Rheinland-Pfalz anzuwenden ist, findet sich im SKL-Staatsvertrag keine Aussage über das anzuwendende Datenschutzgesetz und den zuständigen Landesdatenschutzbeauftragten oder die zuständige Datenschutzaufsichtsbehörde für den nicht-öffentlichen Bereich.

Da es sich bei der SKL um eine Anstalt des öffentlichen Rechts handelt, sind jedenfalls nicht die Datenschutzaufsichtsbehörden der Vertragsländer für den nicht-öffentlichen Bereich zuständig. Zudem gelten gem. Art. 2 Abs. 1 BayDSG die Vorschriften dieses Gesetzes nur für die Erhebung, Verarbeitung und Nutzung personenbezogener Daten durch Behörden, Gerichte und sonstige öffentliche Stellen des Freistaates Bayern, der Gemeinden, Gemeindeverbände und der sonstigen „der Aufsicht des Freistaates Bayern unterstehenden“ juristischen Personen des öffentlichen Rechts. Nach dem Wortlaut des Art. 2 Abs. 1 BayDSG bzw. der entsprechenden Vorschriften der Vertragsländer wäre damit an sich der Landesdatenschutzbeauftragte des jeweils Aufsicht führenden Vertragslandes für die SKL datenschutzrechtlich zuständig; der Bayerische Landesbeauftragte somit erst wieder in den Jahren 2008/2009 und dann 2020/21.

Diese wechselnde Zuständigkeit ist allerdings weder für die Landesdatenschutzbeauftragten der Vertragsländer (Know-How-Verlust; wiederholte Einarbeitung in den aktuellen Sach- und Rechtsstand) einerseits noch für die SKL (ständig wechselnde, erst nach einer Einarbeitungszeit sachkundige Ansprechpartner) andererseits befriedigend. In der Praxis gehen die Landesdatenschutzbeauftragten daher offensichtlich - wie selbstverständlich - von der Zuständigkeit des Datenschutzbeauftragten des Sitzlandes aus. Da ich in der Vergangenheit die SKL datenschutzrechtlich betreut habe, bin ich dazu auch weiterhin bereit.

Zu klären ist, ob auf die SKL das Bayerische Datenschutzgesetz oder das Bundesdatenschutzgesetz anzuwenden ist. Entscheidend ist dabei, ob die öffentliche Stelle SKL als Unternehmen am Wettbewerb teilnimmt. Nach Art. 3 Abs. 1 Satz 1 BayDSG gelten nämlich, soweit öffentliche Stellen als Unternehmen am Wettbewerb teilnehmen, für sie die Vorschriften des BDSG mit Ausnahme des Zweiten Abschnitts; die Kontrollzuständigkeit verbleibt allerdings gem. Art. 3 Abs. 1 Satz 3 BayDSG beim Landesbeauftragten.

Vor dem Hintergrund der Selbsteinschätzung der Staatlichen Lotterieverwaltung als Wettbewerbsunternehmen (siehe hierzu Nr. 10.6 dieses Tätigkeitsberichts), des sinngemäß auch auf die SKL anwendbaren, die Gesellschafter des Deutschen Lotto- und Totoblocks als „Unternehmen“ einordnenden Beschlusses des Kartellsenats des BGH vom 9. März 1999 (KVR 20/97) und der das Lotteriewesen dem Wirtschaftsbereich zuordnenden neueren Rechtsprechung des EuGH ist die SKL in datenschutzrechtlicher Hinsicht als Wettbewerbsunternehmen im Sinne des Art. 3 Abs. 1 BayDSG zu klassifizieren. Schließlich steht die SKL (zumindest auch) im Wettbewerb mit der Norddeutschen Klassenlotterie (NKL).

Für diese Einordnung spricht auch die „Satzung der Süddeutschen Klassenlotterie vom 23. März 1993“ (im Folgenden: Satzung). So bestimmt beispielsweise § 5 Abs. 1 der Satzung, dass der Direktor die Anstalt nach kaufmännischen Grundsätzen leitet. Zudem sind nach § 11 Abs. 1 Satz 2 der Satzung Jahresabschluss und Lagebericht nach den Vorschriften des Dritten Buches des Handelsgesetzbuches für große Kapitalgesellschaften aufzustellen und zu prüfen. Die SKL ist des Weiteren im Handelsregister einzutragen und unterliegt der Umsatzsteuer.

Im Ergebnis sind daher auf die SKL als Wettbewerbsunternehmen gem. Art. 3 Abs. 1 BayDSG grundsätzlich die Vorschriften des BDSG anzuwenden. Soweit die SKL also am Wettbewerb teilnimmt (z.B. hinsichtlich der Kundendaten), gilt das materielle Datenschutzrecht des BDSG für nicht-öffentliche Stellen. In den übrigen Bereichen ist das BayDSG anzuwenden. Die Durchführung und die Kontrolle des Datenschutzes obliegen gem. Art. 3 Abs. 1 Satz 3 BayDSG durchweg dem Bayerischen Landesbeauftragten für den Datenschutz.

Staatliche Lotterieeinnahmen

Die Staatlichen Lotterieeinnahmen sind in Art. 7 des SKL-Staatsvertrags erwähnt. Nach Art. 7 Abs. 2 des SKL-Staatsvertrags werden die staatlichen Lotterieeinnehmer zwar von dem Finanzministerium des Sitzlandes bestellt und abberufen; gem. Art. 7 Abs. 3 Satz 1 des SKL-Staatsvertrags sind die staatlichen Lotterieeinnehmer aber Beauftragte der Süddeutschen Klassenlotterie. Die Lotterieeinnehmer haben nach Art. 7 Abs. 3 Satz 2 des SKL-Staatsvertrags die ihnen obliegenden Geschäfte nach den Weisungen der Anstalt zu besorgen. Zu diesem Zweck werden ihre Rechte und Pflichten gem. Art. 7 Abs. 3 Satz 3 des SKL-Staatsvertrags in einer Geschäftsanweisung festgelegt; zudem übt die SKL nach Satz 4 dieser Vorschrift die Aufsicht über die staatlichen Lotterieeinnehmer aus. Der Begriff des Beauftragten wird allerdings in den folgenden Vorschriften des SKL-Staatsvertrags nicht weiter konkretisiert; offen bleibt somit, ob hiermit ein privat- oder ein öffentlich-rechtliches Auftragsverhältnis gemeint ist. Auch die Begründung des SKL-Staatsvertrags enthält keine Ausführungen zur Rechtsstellung der Staatlichen Lotterieeinnahmen.

Aus dem Wortlaut und dem systematischen Gesamtzusammenhang der „Geschäftsanweisung für die staatlichen Lotterieeinnehmer der Süddeutschen Klassenlotterie vom 15. September 1999“ (im Folgenden: Geschäftsanweisung) ist jedoch zu schließen, dass zwischen dem einzelnen Lotterieeinnehmer und der SKL ein privatrechtliches Vertragsverhältnis vorliegt:

- So handelt es sich bei den in § 5 der Geschäftsanweisung beschriebenen Aufgaben des Lotterieeinnehmers - Verkauf der Lose, Bewerbung des Verkaufs, Betreuung der Spielteilnehmer, Auszahlung der Gewinne, Abführung der Verkaufseinnahmen an die SKL sowie Rechenschaftsablegung gegenüber der SKL - augenscheinlich um keine hoheitlichen Aufgaben. Die Staatlichen Lotterieeinnahmen verfügen auch über keinerlei öffentlich-rechtliche Befugnisse; insbesondere werden ihnen solche hoheitlichen Befugnisse durch den SKL-Staatsvertrag nicht verliehen. An dieser Feststellung vermag auch die ordnungsrechtliche Dimension des Lotteriewesens („Kanalisierung des natürlichen Spieltriebs“) nichts zu ändern. Mangels hoheitlichen Tätigwerdens handelt es sich bei den Staatlichen Lotterieeinnahmen also nicht um Beliehene oder Verwaltungshelfer.

- Zudem ist beispielsweise nach § 20 der Geschäftsanweisung eine Kündigung des Vertragsverhältnisses möglich; auch enthält § 26 der Geschäftsanweisung eine Gerichtsstandsvereinbarung.

- Zu berücksichtigen ist schließlich auch, dass die Staatlichen Lotterieeinnahmen umsatzsteuerpflichtig sind, da sie nach Auffassung des Bundesministeriums der Finanzen in steuerrechtlicher Hinsicht als Unternehmer anzusehen sind.

Im Ergebnis handelt es sich bei den Staatlichen Lotterieeinnahmen somit um - staatlich konzessionierte - Privatunternehmen und damit um nicht-öffentliche Stellen.

Aus dem eben Gesagten ergibt sich, dass eine Zuständigkeit des Landesbeauftragten für die Staatlichen Lotterieeinnahmen als nicht-öffentliche Stellen schon aus Rechtsgründen nicht gegeben ist.

Aber auch aus Sicht des praktischen Datenschutzes ist eine Zuständigkeit der Aufsichtsbehörde für den nichtöffentlichen Bereich (in Bayern also der Regierung von Mittelfranken) für die Staatlichen Lotterieeinnahmen sinnvoll, da

- der Kern der Petitionen zum SKL-Losvertrieb im Umgang der Adresshändler bzw. Call Center mit den personenbezogenen Daten der Eingabeführer liegt (vgl. v.a. die Problematik der Cold Calls) und

- eine effektive datenschutzrechtliche Kontrolle des Geschäftsgebarens der Staatlichen Lotterieeinnahmen nur möglich ist, wenn die datenschutzrechtliche Zuständigkeit sowohl für die Lotterieeinnahmen als auch für die von ihnen beauftragten Adresshändler und Call Center „in einer Hand“ liegt.

Im Ergebnis habe ich mich in Bezug auf die SKL als Anstalt des öffentlichen Rechts mit Sitz in München innerhalb des Kreises der Landesbeauftragten der Vertragsländer dazu bereit erklärt, die datenschutzrechtliche Betreuung weiterhin zu übernehmen. Da es sich bei den bayerischen Staatlichen Lotterieeinnahmen hingegen um nicht-öffentliche Stellen handelt, ist insoweit die Zuständigkeit der Regierung von Mittelfranken als Bayerische Datenschutzaufsichtsbehörde für den nicht-öffentlichen Bereich gegeben. Die betroffenen Datenschutzaufsichtsbehörden haben sich mit diesem Verfahren einverstanden erklärt.

11 Schulen

11.1 Bekanntgabe von Noten im Unterricht

Immer wieder erhalte ich durch Eingaben davon Kenntnis, dass Lehrerinnen und Lehrer Noten - von Bewertungen mündlicher und schriftlicher Leistungen bis hin zu Zeugnisnoten - vor der gesamten Klasse im Unterricht bekannt geben.

Zu dieser Problematik weise ich auf folgendes hin:

In datenschutzrechtlicher Hinsicht handelt es sich bei Schulnoten um personenbezogene Daten im Sinne des Art. 4 Abs. 1 BayDSG. Das Verlesen von Noten vor der versammelten Klasse stellt gem. Art. 4 Abs. 6 Satz 2 Nr. 3 Buchst. a) BayDSG eine Datenübermittlung an Einzelpersonen dar und damit eine Verarbeitung. Nach der den Übermittlungsvorschriften des Bayerischen Datenschutzgesetzes gem. Art. 2 Abs. 7 BayDSG vorgehenden Spezialregelung des Art. 85 Abs. 1 Satz 1 BayEUG sind die Erhebung und die Verarbeitung von Daten nur zur Erfüllung der den Schulen durch Rechtsvorschriften jeweils zugewiesenen Aufgaben zulässig.

Für die Beurteilung der datenschutzrechtlichen Zulässigkeit kommt es also entscheidend darauf an, ob die Bekanntgabe von Noten im Unterricht zur Erfüllung des den Schulen in Art. 1 und 2 BayEUG gesetzlich zugewiesenen Bildungs- und Erziehungsauftrags aus pädagogischen Gründen erforderlich ist. Zu dieser Frage habe ich das Staatsministerium für Unterricht und Kultus um Stellungnahme gebeten. Das Kultusministerium hat insoweit ausgeführt, dass ein Verlesen der Noten aller Schülerinnen und Schüler vor der gesamten Klasse in der Regel pädagogisch weder sinnvoll noch erforderlich sei. Die Bekanntgabe der Noten könne ebenso unter vier Augen stattfinden. Zwar seien Fälle denkbar, in denen dies auch einmal anders zu beurteilen sei, etwa wenn sich einzelne Schüler besonders verbessert hätten im Sinne einer Vorbildwirkung. Aus pädagogischer Sicht sollte eine Verlesung aller Noten aber in den meisten Fällen unterbleiben.

Diese Haltung teile ich. Soll die Notenverkündung aus pädagogischen Gründen erfolgen, ist es ausreichend, einen Notenspiegel - also einen zahlenmäßigen Überblick über die Notenverteilung ohne Namensnennung - einschließlich Notendurchschnitt zu erstellen. Jeder Schüler kann dann unschwer feststellen, wo er leistungsmäßig in der Klasse steht.

Auch das Einholen einer Einwilligung im Sinne des Art. 15 Abs. 1 Nr. 2 BayDSG führt nicht zur Zulässigkeit des Verlesens der Noten im Unterricht. Eine Einwilligung in die Übermittlung personenbezogener Daten kommt nur dann in Betracht, wenn die Übermittlung der Aufgabenerfüllung der Schule dient. Wie eben dargelegt, ist dies bei dem Verlesen der Noten - auch nach Auffassung des Kultusministeriums - aber in der Regel gerade nicht der Fall. Abgesehen davon sind für eine rechtswirksame Einwilligung von der Schule die in Art. 15 Abs. 2 bis 4 BayDSG aufgestellten, strengen formellen Anforderungen (Hinweispflicht, Schriftform etc.) einzuhalten. In diesem Zusammenhang ist insbesondere darauf hinzuweisen, dass das Einholen pauschaler Einwilligungen - etwa bereits bei der Anmeldung der Schülerinnen und Schüler - unzulässig ist. Die Einwilligungen sind vielmehr für jeden Einzelfall einer Datenverarbeitung einzuholen - und zwar grundsätzlich schriftlich bei allen Erziehungsberechtigten. Daher scheitert die - materiell ohnehin unzulässige - Einwil-

ligungslösung in der Praxis bereits an diesen formellen Anforderungen.

11.2 Verpflichtung zur Teilnahme an schulischen Leistungsvergleichen

Im Rahmen einer umfangreichen Änderung des Bayerischen Gesetzes über das Erziehungs- und Unterrichtswesen (BayEUG) hat der bayerische Gesetzgeber mit Wirkung vom 1. August 2006 die Einführung einer Verpflichtung zur Teilnahme an Leistungsvergleichen beschlossen. Nach dem neuen Art. 111 Abs. 4 BayEUG kann das zuständige Staatsministerium nunmehr Schülerinnen, Schüler und Lehrkräfte verpflichten, an Leistungsvergleichen teilzunehmen, die Zwecken der Qualitätssicherung und -steigerung dienen.

In meiner im Verlauf des Gesetzgebungsverfahrens gegenüber dem Staatsministerium für Unterricht und Kultus abgegebenen Stellungnahme habe ich die Einführung dieser Verpflichtung aus datenschutzrechtlicher Sicht kritisiert.

Dabei habe ich nicht bestritten, dass Leistungsvergleiche - sei es auf internationaler, nationaler oder auf Landesebene - wichtige Instrumente zur Sicherung und Steigerung der Qualität der schulischen Bildung darstellen können. Datenschutzrechtlich relevant sind auch meist weniger die eigentlichen Leistungstests selbst als vielmehr die oftmals begleitenden, umfang- und detailreichen Fragebögen für die Lehrkräfte, Schülerinnen und Schüler sowie deren Eltern. Diese greifen teilweise erheblich über das eigentliche schulische Umfeld hinaus und in den privaten Bereich der familiären Lebensgestaltung ein.

Vor diesem Hintergrund bedurfte bislang die Teilnahme an derartigen Leistungsvergleichen der schriftlichen und informierten Einwilligung (im Sinne des Art. 15 Abs. 2 bis 4 BayDSG) aller Betroffenen. Trotz dieser formalen Hürden konnten - wie die im Rahmen von internationalen Leistungsvergleichen wie PISA, DESI oder IGLU gewonnenen Erfahrungen zeigen - jedoch genügend Teilnehmer für die Leistungsvergleiche gefunden werden, um ein zuverlässiges Bild über die Leistungsfähigkeit des schulischen Bildungswesens und dessen Vergleichbarkeit mit anderen Schulsystemen erhalten zu können. Auch aus diesem Grund habe ich gefordert, an der bewährten, datenschutzfreundlichen Praxis festzuhalten.

Darüber hinaus bringt - da bisher die Einwilligungen der Eltern für sie selbst und für ihre Kinder uno actu eingeholt wurden - meiner Einschätzung nach eine Verpflichtung letztlich auch keine nennenswerten Verfahrenserleichterungen mit sich:

- Gerade bei umfangreichen Fragenkatalogen ist es oft zweifelhaft, ob tatsächlich alle Fragen unmittelbar dem Ziel des Projektes - Zwecken der Qualitätssicherung und -steigerung - dienen. Im Hinblick auf die überschießenden Fragen ist somit auch in Zukunft die Einholung einer datenschutzkonformen Einwilligung notwendig.

- In Bezug auf Fragen, die in den privaten Bereich der familiären Lebensgestaltung eingreifen und damit - direkt oder indirekt - personenbezogene Daten der Eltern zum Gegenstand haben, muss zudem weiterhin eine datenschutzkonforme Einwilligung der Eltern eingeholt werden.

- Abgesehen davon werden nicht nur bei internationalen Schülerleistungsvergleichen wie PISA auch die Eltern der Schüler direkt befragt. Eine Teilnahmeverpflichtung der Eltern wurde aber - aus meiner Sicht zu Recht - nicht in das BayEUG eingeführt; daher ist auch insoweit die Einholung der Einwilligung der Eltern weiter erforderlich.

In diesem Zusammenhang weise ich schließlich darauf hin, dass die Verpflichtung der Lehrkräfte, Schülerinnen und Schüler zur Teilnahme an einem Leistungsvergleich nach dem nunmehr geltenden Recht in jedem Einzelfall einen abwägungs- und begründungsintensiven Verpflichtungsakt des zuständigen Staatsministeriums erfordert, der zudem einer gerichtlichen Überprüfung zugeführt werden kann. Auch dieser Umstand trägt nicht zu einer Minimierung des mit der Durchführung von schulischen Leistungsvergleichen verbundenen Verwaltungsaufwandes bei.

Den Auswirkungen der Einführung einer Verpflichtung von Schülerinnen, Schülern und Lehrkräften zur Teilnahme an Leistungsvergleichen auf die schulische Praxis sehe ich daher aus datenschutzrechtlicher Sicht mit Interesse entgegen.

11.3 Schülerbezogene Fragebögen und Steckbriefe im Unterricht

Durch eine Eingabe betroffener Erziehungsberechtigter erhielt ich davon Kenntnis, dass an einer Grundschule im Heimat- und Sachunterricht der 1. Klasse von der Klassleiterin so genannte „Fragebögen“ und „Steckbriefe“ an die Schülerinnen und Schüler verteilt worden waren.

Der zweiseitige Fragebogen enthielt dabei u.a. folgende Fragen:

- „Was waren meine ersten Worte?“

- „Wann trug ich keine Windeln mehr?“
- „Was lag als Baby in meinem Bett?“
- „Was war mein Lieblingsspielzeug als Kindergartenkind?“
- „Das waren meine Freunde/Freundinnen im Kindergarten: ...“
- „Da haben meine Eltern besonders über mich gelacht: ...“

Mit dem einseitigen Steckbrief wurden von den Kindern Geburtstag, Haarfarbe, Augenfarbe, Körpergröße, Gewicht, Lieblingstier, Lieblingssport, Lieblingsspielzeug und Freunde erfragt.

Die Fragebögen und Steckbriefe sollten von den Schülern und deren Eltern zuhause ausgefüllt und mit zwei Fotos (ein Baby- und ein aktuelles Foto) versehen werden. Anschließend sollten die Fragebögen und Steckbriefe - wie auch in den vergangenen Jahren üblich - das ganze Schuljahr über unverschlossen unter den Schülerpulten im Klassenraum aufbewahrt und erst am Schuljahresende den Schülern ausgehändigt werden.

Die betroffenen Erziehungsberechtigten sahen die Persönlichkeitsrechte ihres Kindes verletzt und lehnten die Aushändigung von Fragebogen und Steckbrief an die Klassleiterin ab. Nachdem Gespräche sowohl mit der Klassen- und Schulleitung als auch mit dem Elternbeirat ergebnislos verlaufen waren, baten sie mich um Unterstützung.

Nach Art. 15 Abs. 1 BayDSG sind die Erhebung und die Verarbeitung personenbezogener Daten der Schülerinnen und Schüler durch Fragebogen und Steckbrief mangels schriftlicher Einwilligungserklärungen der Eltern nur zulässig, wenn eine Rechtsvorschrift sie erlaubt oder anordnet. Als gesetzliche Befugnisnorm kommt hier allein Art. 85 Abs. 1 Satz 1 BayEUG in Betracht. Danach sind zur Erfüllung der den Schulen durch Rechtsvorschriften jeweils zugewiesenen Aufgaben die Erhebung und die Verarbeitung von personenbezogenen Daten zulässig.

Datenerhebung durch Fragebogen und Steckbrief

Meiner Auffassung nach war die durch Fragebogen und Steckbrief erfolgte Datenerhebung - über die Schüler, aber auch zum Teil über deren Eltern! - zur Erfüllung des der Schule durch Art. 1 und Art. 2 BayEUG zugewiesenen Bildungs- und Erziehungsauftrages im vorliegenden Fall nicht erforderlich und damit datenschutzrechtlich unzulässig.

Das von mir um Stellungnahme gebetene Staatsministerium für Unterricht und Kultus stellte sich zwar auf den Standpunkt, dass die Fragebögen und Steckbriefe u.a. zur Realisierung des Lernzieles 1.2. des Heimat- und Sachunterrichts - Ich und meine Erfahrungen: „Die Schüler betrachten besondere Ereignisse in ihrem bisherigen Leben. Sie erkennen deren Einmaligkeit und können sich daher auch ihrer eigenen Zeitlichkeit bewusst werden.“ sowie des Lernzieles 1.2.1. - Zeit erleben - Zeiterfahrung: „Zeitlichkeit und Veränderung der eigenen Person wahrnehmen (Einmaligkeit von Ereignissen - lineare Zeit: Das bin ich; Kleinkind, Schulkind...; Einführen einer persönlichen Zeitleiste: Fotografien, Erinnerungsstücke u.ä.)“ eingesetzt worden seien und diese Lernziele auch aus Sicht des Kultusministeriums angemessen umsetzten.

Aus meiner Sicht griff dagegen die durch Fragebogen und Steckbrief erfolgte Datenerhebung tief in die Privat- und Intimsphäre und damit in das verfassungsrechtlich garantierte Recht auf informationelle Selbstbestimmung der Betroffenen ein, ohne dass die Erforderlichkeit der Erhebung dieser Informationen zur Erreichung der genannten Lernziele erkennbar ist. Dies gilt insbesondere für die Fragen „Was waren meine ersten Worte?“, „Wann trug ich keine Windeln mehr?“, „Was lag als Baby in meinem Bett?“ sowie „Da haben meine Eltern besonders über mich gelacht: ...“. Es ist nicht ersichtlich, dass gerade diese Lebensereignisse zur Heranbildung des Bewusstseins der Schüler für Zeit und Zeitlichkeit Verwendung finden müssen. Gleiches gilt für die erheblich in die Privatsphäre gehenden Fragen nach den Freunden/Freundinnen im Kindergarten, dem Lieblingsspielzeug als Kindergartenkind sowie nach Körpergröße und -gewicht.

Erschwerend kam noch hinzu, dass nach Auffassung des Staatsministeriums für Unterricht und Kultus „das Einbringen und Mitteilen persönlicher Vorlieben, Stärken oder Schwächen (im Unterricht) unerlässlich“ sei. Ich vermag auch gegenwärtig unter keinem Aspekt zu erkennen, wozu - pars pro toto - die Kenntnis der Dauer des Windeltragens (!) sowohl bei Staat (Schule) als auch bei außenstehenden Dritten (Mitschülern) gut sein soll. Vielmehr sehe ich hier nach wie vor ein erhebliches Gefährdungspotenzial für den Betroffenen.

Ich habe das Staatsministerium für Unterricht und Kultus daher aufgefordert, den Einsatz solcher oder ähnlicher Fragebögen und Steckbriefe an den Grundschulen künftig zu unterbinden.

Aufbewahrung unter Schülerpulten

Bei dieser Gelegenheit habe ich das Staatsministerium für Unterricht und Kultus zudem allgemein darauf hingewiesen, dass die in der ungesicherten Auf-

bewahrung von Unterlagen mit personenbezogenen Schülerdaten unter den Schülerpulten liegende Datenverarbeitung (in Form der Datenspeicherung, Art. 4 Abs. 6 Satz 2 Nr. 1 BayDSG) datenschutzrechtlich unzulässig ist.

Denn zum Zugriff auf die in solchen Unterlagen (zulässigerweise gespeicherten!) personenbezogenen Daten sind nur der Schüler, seine Erziehungsberechtigten und die jeweils unterrichtende Lehrkraft berechtigt. Ein Zugriff weiterer Personen - etwa Mitschüler, Reinigungskräfte, Hausmeister sowie an außerschulischen Veranstaltungen im Klassenraum teilnehmende Personen usw. - auf diese Daten muss nach Art. 7 BayDSG durch entsprechende technische und organisatorische Maßnahmen ausgeschlossen werden. Dieses Erfordernis der Sicherung der Daten vor unberechtigtem Zugriff gewinnt insbesondere vor dem Hintergrund der Nutzung der Schulräume in den Nachmittags- und Abendstunden durch Einrichtungen der Erwachsenenbildung (etwa Volkshochschulen u.a.) erheblich an Bedeutung (vgl. dazu auch meine Ausführungen unter Nr. 11.7 dieses Tätigkeitsberichts).

Daher ist es aus datenschutzrechtlichen Gründen erforderlich, entweder die jeweiligen Unterlagen den Schülerinnen und Schülern nach dem Ausfüllen nach Hause mitzugeben - und bei Bedarf wieder kurzzeitig in den Unterricht mitbringen zu lassen - oder aber diese in einem geeigneten Behältnis (etwa Schrank im Klassenzimmer o.ä.) durch die (klassleitende) Lehrperson wegzuschließen, so dass ein Zugriff unbefugter Personen dauerhaft und zuverlässig ausgeschlossen wird.

Rundschreiben des Kultusministeriums

In Anbetracht der bayernweiten Bedeutung beider Problemfelder - offenbar ist die Verwendung schülerbezogener Fragebögen und Steckbriefe im Heimat- und Sachunterricht seit mehr als zwei Jahrzehnten geübte Praxis an den Grundschulen - habe ich das Staatsministerium für Unterricht und Kultus gebeten, meine Haltung allen Grundschulen in Bayern in einem Rundschreiben baldmöglichst - noch vor Beginn des neuen Schuljahres - zur Kenntnis zu bringen. Zunächst war das Kultusministerium hierzu überhaupt nicht bereit. Dann beabsichtigte es, meine Rechtsauffassung über Dienstbesprechungen mit den Regierungen und Staatlichen Schulämtern den Schulen in geeigneter Weise sukzessive zur Kenntnis zu bringen. Nach über einjährigen, zähen Verhandlungen auf allen Arbeits- und Leitungsebenen richtete das Staatsministerium für Unterricht und Kultus schließlich doch noch ein entsprechendes Rundschreiben an alle Schulleiterinnen und Schulleiter der bayerischen Grundschulen (KMS Nr. IV.5-5 S 7310. 1-4.22083 vom 17. Mai 2006).

11.4 Modellprojekt „fit & pfundig“

Ebenfalls aufgrund einer Eingabe von betroffenen Erziehungsberechtigten wurde ich auf das Projekt „fit & pfundig“ aufmerksam. Es wurde zunächst als Modellprojekt an allen Grundschulen eines Landkreises von einer privaten (also meiner Kontrollkompetenz nicht unterliegenden) Klinikgruppe in Zusammenarbeit u.a. mit dem zuständigen Staatlichen Schulamt unter Billigung des örtlichen Gesundheitsamtes und mit Genehmigung des Staatsministeriums für Unterricht und Kultus durchgeführt. Ziel des Modellprojektes war es, übergewichtigen Schülern und deren Eltern einen Weg zu einem gesundheitsbewussteren Leben aufzuzeigen. Bei Erfolg sollte das Projekt bayernweit ausgedehnt werden.

Das Projekt umfasste - grob skizziert - drei Phasen: Zunächst wurden alle ca. 5.300 Grundschulkinder in den Schulen gemessen und gewogen. Anhand von Körpergröße, Körpergewicht und Alter wurden dann die Kinder in verschiedene Gefährdungsstufen eingeteilt (erste Phase). Anschließend wurden ca. 50 gefährdete („Gruppe gelb“) und stark gefährdete Kinder („Gruppe rot“) nach Anmeldung durch die Eltern in ein zweijähriges Programm geführt, das die Kinder spielerisch an sportliche Aktivitäten und bewusstes Ernährungsverhalten heranführen sollte; in dieser (zweiten) Phase des Modellprojektes wurden weitere Gesundheitsdaten über die Schüler erhoben und an die am Projekt beteiligten Ärzte weitergeleitet. In der dritten Projektphase wurden schließlich die über ca. 30 Schüler gewonnenen Daten wissenschaftlich ausgewertet.

Meine eingehende datenschutzrechtliche Überprüfung des Modellprojekts „fit & pfundig“ hat ergeben, dass in zahlreichen Punkten Verstöße gegen datenschutzrechtliche Vorschriften vorlagen. Im Einzelnen:

Erste Projektphase

Bereits vor Anmeldung der Kinder zur Projektteilnahme erhoben die Klassenlehrer die für das Projekt relevanten Daten (Alter, Körpergewicht und Körpergröße) in der Unterrichtszeit und gaben diese Daten an die Projektleitung - eine außerschulische Stelle - weiter. In datenschutzrechtlicher Hinsicht lagen damit sowohl Erhebungen als auch Übermittlungen besonders geschützter Gesundheitsdaten der Schüler durch die Schule vor.

Unabhängig von der Frage, ob die genannten Datenerhebungen durch die Klassenlehrer in Erfüllung einer den Schulen gesetzlich zugewiesenen Aufgabe im Sinne des Art. 85 Abs. 1 Satz 1 BayEUG erfolgten, ist jedenfalls die Weitergabe derartiger Gesundheitsdaten an außerschulische Stellen - wie hier die Projektleitung - gem. Art. 85 Abs. 2 Satz 1 BayEUG

ohne ausdrückliche Einwilligung der Erziehungsberechtigten untersagt. Wie das von mir um Stellungnahme gebetene Staatsministerium für Unterricht und Kultus selbst eingeräumt hat, wurde es jedoch hier versäumt, den datenschutzrechtlichen Anforderungen entsprechende, schriftliche Einwilligungen der Eltern einzuholen. In diesem Zusammenhang darf ich noch einmal darauf hinweisen, dass das Schriftformerfordernis des Art. 15 Abs. 3 BayDSG keine bloße Förmelei darstellt. Vielmehr findet die Schriftlichkeit der Einwilligung ihre sachliche Berechtigung darin, dass sie die informierte Freiwilligkeit der Teilnahme in höherem Maße garantiert, als dies im Rahmen einer bloß mündlich oder gar stillschweigend erklärten Einwilligung je der Fall sein könnte.

Das bloße Zusenden von Informationsmaterial an alle betroffenen Eltern konnte die schriftliche Einwilligung daher ebenso wenig ersetzen wie die Teilnahme der Eltern an Informationsveranstaltungen. Zum einen war durch diese Maßnahmen nicht gewährleistet, dass alle betroffenen Eltern vor der ersten Datenerhebung die notwendigen Informationen erhielten. Zum anderen konnte aus einem Nicht-Widerspruch der Eltern - sei es auf das Informationsschreiben, sei es bei der Informationsveranstaltung - nicht zwingend auf ein Einverständnis geschlossen werden. Zur Ausräumung aller Unsicherheiten war deshalb allein die Einholung einer schriftlichen Einwilligung geeignet.

Zudem war zu berücksichtigen, dass es sich vorliegend um sensible Daten bezüglich der körperlichen Konstitution der Schüler handelte, die gem. Art. 15 Abs. 7 Satz 1 Nr. 2 BayDSG nur dann auf der Grundlage einer Einwilligung der Betroffenen erhoben, verarbeitet oder genutzt werden dürfen, wenn sich die Einwilligung ausdrücklich auf diese Daten bezieht.

Zweite Projektphase

Nach Anmeldung der Schüler zur Projektteilnahme durch die Eltern wurden in der zweiten Projektphase weitere Gesundheitsdaten über die Schüler erhoben und an die am Projekt beteiligten Ärzte weitergeleitet. Die im Anmeldeformular enthaltene Einwilligung der Eltern erfüllte zwar jetzt das Schriftformerfordernis des Art. 15 Abs. 3 BayDSG, setzte aber zahlreiche weitere datenschutzrechtliche Vorgaben überhaupt nicht oder zumindest nicht vollständig um.

- So wurde entgegen der Verpflichtung des Art. 15 Abs. 2 BayDSG weder auf die Freiwilligkeit noch auf die Folgen einer Nichtteilnahme hingewiesen. Dagegen wird im Rahmen von Forschungsprojekten und Evaluationsvorhaben in Umsetzung dieser gesetzlichen Vorgabe üblicherweise darauf hingewiesen, dass die Teilnahme an dem Projekt vollkommen freiwillig ist und dass die Nichtteilnahme keinerlei nachteilige Folgen für den Betroffenen hat.

- Auch wurde nicht darauf hingewiesen, dass die Teilnahme an dem Projekt jederzeit ohne Angabe von Gründen widerrufen werden kann und dieser Widerruf keinerlei nachteilige Folgen zeitigt. Im Gegenteil wurde durch Verwendung der Formulierung „verbindlich“ suggeriert, dass ein Widerruf der Teilnahme(bereitschaft) nicht möglich ist.

- Zudem fehlte der Hinweis auf das Recht des Betroffenen, auf Antrag Auskunft (u.a.) über die zu seiner Person gespeicherten Daten verlangen zu können (Art. 10 BayDSG). Ebenso wurde im Anmeldeformular nicht auf die datenschutzrechtlich verantwortliche Stelle (Art. 4 Abs. 9 BayDSG) hingewiesen. Dieser Hinweis erfolgt üblicherweise im Rahmen von Forschungsvorhaben und Evaluationsprojekten unter Angabe eines Ansprechpartners und dessen Telefonnummer, um den Betroffenen eine unkomplizierte und schnelle Möglichkeit der Kontaktaufnahme an die Hand zu geben. Der Hinweis ist auch keineswegs theoretischer Natur, da an diese Stelle (bzw. den betreffenden Ansprechpartner) ein evtl. Widerruf sowie ein evtl. Auskunftsverlangen zu richten sind.

- Soll die Einwilligung zusammen mit anderen Erklärungen schriftlich erteilt werden, ist die datenschutzrechtliche Einwilligungserklärung gem. Art. 15 Abs. 4 BayDSG im äußeren Erscheinungsbild der Erklärung (drucktechnisch) hervorzuheben. Auch diese Anforderung erfüllte das Anmeldeformular nicht.

Dritte Projektphase

In dieser Phase wurden die von den Eltern ausgefüllten, die Ernährungs- und Lebensgewohnheiten ihrer Kinder betreffenden Fragebögen zusammen mit anderen im Rahmen des Projekts gewonnenen Daten an einen Lehrstuhl einer bayerischen Universität zur Evaluierung des Projektes übermittelt. Über die eben dargestellten Mängel hinaus berechtigte die insofern auf dem Anmeldeformular eingeholte Einwilligung der Eltern allerdings ausdrücklich nur zur Übermittlung „anonymisierter Daten“. Da aber tatsächlich keine wirksame und dauerhafte Anonymisierung der Daten vorlag, wurden auch in dieser Projektphase datenschutzrechtliche Bestimmungen verletzt.

Personenbezogene Daten können nur dann als im datenschutzrechtlichen Sinne anonymisiert angesehen werden, wenn sie derart verändert wurden, dass der Empfänger die Einzelangaben über persönliche oder sachliche Verhältnisse entweder überhaupt nicht mehr (sog. absolute Anonymisierung) oder nur noch

mit einem unverhältnismäßig großen Aufwand an Zeit, Kosten und Arbeitskraft (sog. faktische Anonymisierung) einer bestimmten oder bestimmbaren natürlichen Person zuordnen kann (Art. 4 Abs. 8 BayDSG).

Demgegenüber wurde hier von der Projektleitung (zumindest auf den mir zur Überprüfung übermittelten Fragebögen) jeweils auf der ersten Seite der Fragebögen neben einer „Code-Nr." bzw. „Screening-Nr." der Name des Kindes - wenn auch durch weißes Korrekturband überdeckt - vermerkt. Damit lag keine Anonymisierung im datenschutzrechtlichen Sinne vor. Der Fragebogen wäre bereits so zu gestalten gewesen, dass er kein Feld für den Namen des Kindes enthält. Zumindest hätte bei Verwendung des vorliegenden Fragebogens die Unkenntlichmachung des Namens irreversibel erfolgen müssen. Bei einer bloßen Überdeckung mit weißem Korrekturband kann hiervon nicht die Rede sein, da sich solche Überdeckungen nach der allgemeinen Lebenserfahrung unschwer wieder entfernen lassen. Dabei kommt es nicht darauf an, ob der jeweilige Empfänger die Absicht hat, eine solche Reidentifizierung tatsächlich vorzunehmen; ausreichend ist vielmehr bereits die objektive Möglichkeit, dies zu tun.

Beanstandung

Aufgrund der dargestellten Datenschutzverstöße habe ich das Staatsministerium für Unterricht und Kultus förmlich gem. Art. 31 Abs. 1 Satz 1 BayDSG beanstandet. Die Anzahl der Verstöße war so groß und ihre Häufigkeitsverteilung auf die einzelnen Projektphasen derart signifikant - keine Projektphase war fehlerfrei -, dass das Projekt insgesamt als an erheblichen datenschutzrechtlichen Mängeln leidend angesehen werden musste. Bei meiner Entscheidung habe ich auch berücksichtigt, dass es sich hier um sensible Daten von Kindern handelte, die für eine verhältnismäßig lange Zeitspanne einem weiten Personenkreis - darunter auch den Klassenlehrern (!) - bekannt wurden oder jedenfalls bekannt werden konnten.

Ebenso durfte nicht unberücksichtigt bleiben, dass bei der durch die schulrechtliche Vorschrift des § 71 Abs. 1 Satz 1 Volksschulordnung (VSO) vorgeschriebenen Genehmigung des Projektes gegen § 71 Abs. 2 Satz 3 Nr. 1 VSO verstoßen wurde. Nach dieser Bestimmung ist bei „Umfragen und wissenschaftlichen Untersuchungen ... in den Schulen" durch Auflagen insbesondere sicherzustellen, dass „aus der Erhebung keine Rückschlüsse auf einzelne Schüler, Erziehungsberechtigte oder Lehrkräfte gezogen werden können und die Anonymität der betroffenen Personen gewahrt bleibt". Eben diese Vorgaben wurden im Rahmen des Modellprojekts in mehrfacher Hinsicht verletzt.

Gemäß Art. 25 Abs. 1 BayDSG haben die Staatsministerien für ihren Bereich die Ausführung dieses Gesetzes sowie anderer Rechtsvorschriften über den Datenschutz sicherzustellen. Dem Staatsministerium für Unterricht und Kultus war als „Projektpartner" von Beginn an das Projekt bekannt; es hätte - der vorgenannten gesetzlichen Verpflichtung entsprechend - auf die Einhaltung der datenschutzrechtlichen Bestimmungen im Rahmen des Projektes hinwirken müssen. Dies ist leider nicht erfolgt.

Folgen

Die Projektleitung hat in der Folgezeit die von mir beanstandeten, zahlreichen Verstöße gegen datenschutzrechtliche Vorschriften ausdrücklich bedauert und sich für diese Versäumnisse in aller Form entschuldigt.

Das Staatsministerium für Unterricht und Kultus hat mir mitgeteilt, dass die in der ersten Projektphase bei ca. 5.300 Kindern an den Schulen erhobenen Daten nach Auskunft der Projektleitung vollständig vernichtet worden seien. Eine Weitergabe der Daten an Dritte sei nicht erfolgt. Hinsichtlich der in der zweiten Projektphase bei ca. 50 Schülern erfolgten Datenerhebungen und -verarbeitungen seien nachträglich - mittels der mit mir mittlerweile abgestimmten Formulare - von der Projektleitung den datenschutzrechtlichen Anforderungen entsprechende, schriftliche Einwilligungserklärungen bei den betroffenen Eltern eingeholt worden. Die ca. 30 im Rahmen der dritten Projektphase von den Eltern ausgefüllten Fragebögen seien schließlich von der Projektleitung und von dem beteiligten Lehrstuhl den datenschutzrechtlichen Vorschriften entsprechend anonymisiert worden. Nach Abschluss der wissenschaftlichen Auswertung würden die Fragebögen zudem vollständig vernichtet und das Modellprojekt beendet.

Obwohl aufgrund meiner eingehenden datenschutzrechtlichen Überprüfung und Beratung nun eine datenschutzkonforme bayernweite Ausdehnung des Projekts möglich gewesen wäre, hat mich das Staatsministerium für Unterricht und Kultus zuletzt darüber informiert, dass eine landesweite Umsetzung des Projekts „fit & pfundig" aus anderen Gründen nicht mehr vorgesehen sei.

11.5 Teilnutzungsberechtigung des Elternbeirats hinsichtlich der Schülerdatei

Die Weitergabe von bei den Schulen gespeicherten Daten und Unterlagen über Schüler und Erziehungsberechtigte - auch in Form der Gewährung der Einsichtnahme - ist immer wieder Gegenstand von Eingaben und Anfragen betroffener Bürger. Hinsichtlich der Weitergabe an außerschulische Stellen - nach der datenschutzrechtlichen Terminologie also einer

Übermittlung im Sinne von Art. 4 Abs. 6 Satz 2 Nr. 3 BayDSG - sind die gesetzlichen Bestimmungen zwar erfreulicherweise klar und eindeutig: sie ist gem. Art. 85 Abs. 2 BayEUG grundsätzlich unzulässig. Bezüglich der Weitergabe an Stellen innerhalb der Schule - nach der datenschutzrechtlichen Terminologie also einer Nutzung im Sinne von Art. 4 Abs. 7 BayDSG - ist dies jedoch leider noch nicht der Fall.

Aus dem weiten Problemkreis der Nutzung von Schülerdaten möchte ich die immer noch virulente Problematik der Teilnutzungsberechtigung des Elternbeirats hinsichtlich der Schülerdatei besonders hervorheben.

Nach Nr. 6 der Anlage 2 der „Verordnung zur Durchführung des Art. 28 Abs. 2 des Bayerischen Datenschutzgesetzes“ (im folgenden: DSGArt28DV) sind die Einrichtungen zur Mitgestaltung des schulischen Lebens teilnutzungsberechtigt hinsichtlich der Schülerdatei. Die Einrichtungen zur Mitgestaltung des schulischen Lebens sind in Abschnitt IX. des BayEUG aufgeführt; hierzu zählt als Elternvertretung gem. Art. 64 ff. BayEUG auch der Elternbeirat. Die Schülerdatei ist ein zentrales, umfangreiches und grundsätzlich an jeder Schule in Bayern eingesetztes automatisiertes Verfahren zur Unterstützung der schülerbezogenen Verwaltungsarbeiten. Sie enthält u.a. persönliche Daten des Schülers und der Erziehungsberechtigten (wie Anschrift und Telefonnummer), Unterrichtsdaten, Daten zur Schullaufbahn und zu ggf. bestehendem besonderen Förderbedarf sowie Zeugnis- und Abschlussprüfungsdaten.

In Anbetracht des Umfangs und der Sensibilität der in der Schülerdatei gespeicherten Daten ist es aus datenschutzrechtlicher Sicht wesentlich, dass nur Berechtigte ausschließlich bei berechtigten Anliegen auf die Schülerdatei zugreifen dürfen. Durch die datenschutzgerechte Gestaltung der Zugriffsregelungen müssen Missbrauchsmöglichkeiten schon im Ansatz verhindert werden.

An der klaren und eindeutigen Festlegung von - je nach Aufgabenbereich spezifisch ausgestalteten, aber auch beschränkten - Zugriffsbefugnissen fehlt es jedoch bisher. Die spezialgesetzliche Regelung des Art. 85 BayEUG umfasst nur die Fälle der Erhebung und Verarbeitung von Daten, nicht jedoch den Fall der Datennutzung. Daher sind hinsichtlich der Nutzung der Schülerdatei nur die allgemeinen gesetzlichen Datenschutzvorschriften der Art. 15 und 17 BayDSG einschlägig (vgl. Nr. 4.5 Satz 1 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. April 2001, KWMBl I S. 112, geändert durch Bekanntmachung vom 10. Oktober 2002, KWMBl S. 354). Die Nutzung der Schülerdatei durch den Elternbeirat ist demnach gem. Art. 17 Abs. 1 BayDSG nur dann zulässig, wenn sie zur Erfüllung einer dem Elternbeirat obliegenden Aufgabe - siehe insoweit Art. 65 BayEUG - erforderlich ist und für Zwecke erfolgt, für die die Daten erhoben worden sind (vgl. Nr. 4.5 Satz 2 der „Erläuternden Hinweise“). Meines Erachtens wird der gegenständliche Adressatenkreis - Schule und Elternbeirat - durch diese, als allgemeine Datenschutzregelung notwendigerweise sehr abstrakt formulierte Vorschrift nur schwer in die Lage versetzt, mit den in der Schülerdatei enthaltenen personenbezogenen Daten der Schüler und Eltern in schul- und datenschutzrechtlich einwandfreier Weise umzugehen. Auch die in Bezug auf die vorliegende Problematik allein einschlägige Verwaltungsvorschrift der Nr. 4.5 Satz 5 der „Erläuternden Hinweise“ hilft in diesem Zusammenhang nicht wesentlich weiter. Hier findet sich lediglich der - meines Erachtens zudem nicht sehr klare - Hinweis: „Unter dieser Voraussetzung kann es auch zulässig sein, dass Daten an den Elternbeirat, … weitergegeben werden, beispielsweise also dem Elternbeirat der eigenen Schule Adressdaten der Erziehungsberechtigten überlassen werden“.

Aufgrund dieser sowohl für die Schulen als auch für die Einrichtungen zur Mitgestaltung des schulischen Lebens in der Praxis schwierig handhabbaren Rechts- und Weisungslage habe ich das Staatsministerium für Unterricht und Kultus zunächst um nähere Erläuterung des Umfangs der Teilnutzungsberechtigung der Einrichtungen zur Mitgestaltung des schulischen Lebens im Verfahren der Schülerdatei gebeten. Das Kultusministerium hat mir daraufhin mitgeteilt, dass die Weitergabe von Daten der Schüler und Eltern an den Elternbeirat unter äußersten Restriktionen nur für die Erfüllung der Aufgaben der Elternvertretung erfolgen dürfe. Die Daten seien innerhalb der Elternvertretung absolut vertraulich zu behandeln und dürften den Kreis dieser Eltern nicht verlassen. Weitere Vorgaben, um welche Daten es sich zur Erfüllung welcher Aufgabe handeln könnte, würden aber vom Staatsministerium nicht gemacht, da dies der Fülle der Konstellationen im Einzelfall nicht gerecht werden würde. Allgemein gelte, dass hierbei sehr restriktiv zu verfahren sei.

In Anbetracht der beim Kultusministerium sonst zu beobachtenden Normsetzungsbereitschaft haben mich diese Ausführungen erstaunt. Leider hat das Kultusministerium auch (zumindest) eine Information aller Schulen über seine - aus meiner Sicht erfreulich restriktive - Haltung in dieser Frage nicht für erforderlich gehalten. In meinem Antwortschreiben habe ich dem Staatsministerium für Unterricht und Kultus daher vorgeschlagen, zur Klärung der vorliegenden Problematik der Teilnutzungsberechtigung lediglich die Nr. 4.5 der „Erläuternden Hinweise“ um entsprechende Ausführungen zu Nr. 6 der Anlage 2 der DSGArt28DV zu ergänzen. Hier sollten meines Er-

achtens sowohl der Begriff „automatisierte Nutzung“ der Schülerdatei als auch die Begriffe „teilnutzungsberechtigt“ und „Einrichtungen zur Mitgestaltung des schulischen Lebens“ näher erläutert werden. In diesem Rahmen wären zudem - wie beispielsweise in Nr. 4.4 der „Erläuternden Hinweise“ - Beispielsfälle hilfreich. Eine abschließende Aufzählung ist dagegen auch aus meiner Sicht weder machbar noch notwendig. Da die bisherige Regelung Missbrauchsgefahren eröffnet - das derzeit zulässige „Pull-System“ ermöglicht unkontrollierte Zugriffe -, habe ich weiter dem Staatsministerium für Unterricht und Kultus vorgeschlagen, in Nr. 6 der Anlage 2 der DSGArt28DV generell von der Möglichkeit einer automatisierten Teilnutzung der Schülerdatei für Einrichtungen zur Mitgestaltung des schulischen Lebens abzusehen. Datenschutzfreundlich ist allein ein „Push-System“, in dem der Elternbeirat im konkreten Einzelfall die Schulleitung unter näherer Begründung um Mitteilung der benötigten Daten der Eltern und Schüler ersucht. Auf die neue Rechts- und Weisungslage könnte das Kultusministerium die Schulen sodann in einem Rundschreiben aufmerksam machen. Leider hat das Staatsministerium für Unterricht und Kultus meine Anregungen nicht aufgegriffen und insbesondere weitere Hinweise derzeit für nicht erforderlich erachtet. Das Kultusministerium hat aber nochmals festgestellt, dass die Teilnutzungsberechtigung in der Praxis sehr restriktiv gehandhabt werde.

Ob die letzte Aussage bayernweit für sämtliche Schulen zutrifft, mag auch angesichts einer bei mir - fast zeitgleich - eingegangenen weiteren Anfrage eines Elternbeiratsmitglieds (!) dahingestellt bleiben. Es ist jedoch zu hoffen, dass das Staatsministerium für Unterricht und Kultus baldmöglichst - zumindest durch eine entsprechende Überarbeitung der „Erläuternden Hinweise“ - nicht nur die bei allen am Verfahren der Schülerdatei Beteiligten bestehenden Unklarheiten sondern auch die immer noch existierenden Datenmissbrauchsgefahren beseitigt. Ich weise in diesem Zusammenhang nochmals darauf hin, dass eine Schule auch für ein Handeln jedes Mitglieds des Elternbeirats (datenschutz-)rechtlich zur Verantwortung gezogen werden kann.

Spätestens im Rahmen der rechtlichen Umsetzung des eGovernment-Projekts „Amtliche Schuldaten“ (siehe dazu Nr. 21.2 dieses Tätigkeitsberichts) werde ich diese Problematik gegenüber dem Staatsministerium für Unterricht und Kultus wieder aufgreifen.

11.6 Praktikum an der eigenen Schule

Nach § 11 Abs. 5 der Schulordnung für die Fachoberschulen und Berufsoberschulen in Bayern umfasst der Unterricht in der Jahrgangsstufe 11 der Fachoberschule eine fachpraktische Ausbildung. In der Ausbildungsrichtung Wirtschaft, Verwaltung und Rechtspflege absolvieren die Schülerinnen und Schüler daher mehrere Praktika, unter anderem bei Finanzämtern und Banken. Zur Entlastung der angespannten Personalsituation im Sekretariat ist eine Fachoberschule nun auf den Gedanken gekommen, Schülerinnen und Schüler als Praktikanten an der eigenen Schule einzusetzen.

Aus datenschutzrechtlicher Sicht ist dies nicht zulässig:

Nach Art. 17 Abs. 3 Satz 2 BayDSG sind die Verarbeitung und die Nutzung der bei einer öffentlichen Stelle - wie hier der Fachoberschule - gespeicherten personenbezogenen Daten zu Ausbildungszwecken nur zulässig, soweit nicht offensichtlich überwiegende schutzwürdige Interessen der Betroffenen - also der Personen, deren Daten gespeichert sind - entgegenstehen.

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

Im Schulbereich ist typischerweise davon auszugehen, dass jeder Schüler zumindest einen Großteil seiner Mitschüler, deren Erziehungsberechtigter und der Lehrer persönlich kennt. Da im Sekretariat einer Schule aber nahezu ausschließlich die personenbezogenen Daten dieser Personengruppen verarbeitet und genutzt werden, besteht hier eine hohe Gefahr der zweckwidrigen Verwendung. Durch den stark eingeengten Personenkreis, dessen Daten bei einer Schule gespeichert werden, unterscheidet sich ein Praktikum bei der eigenen Schule auch wesentlich von einem Praktikum bei anderen Stellen, wie z.B. bei Finanzämtern und Banken, auch wenn ich diese nicht ganz unkritisch sehe.

Dem Einsatz von Praktikanten an der eigenen Schule stehen daher aus datenschutzrechtlicher Sicht die offensichtlich überwiegenden schutzwürdigen Interessen der Mitschüler, deren Erziehungsberechtigter und der Lehrer, deren personenbezogene Daten an der Schule gespeichert sind, entgegen.

Die zuständige Schulaufsichtsbehörde hat meine Auffassung geteilt und der betroffenen Fachoberschule den Einsatz von Schülerinnen und Schülern als Praktikanten an der eigenen Schule untersagt.

11.7 Volkshochschulkurse in Schulräumen

Nach Art. 12 Abs. 1 Satz 1 Gesetz zur Förderung der Erwachsenenbildung (EBFöG) sollen Staat, Gemeinden und Gemeindeverbände als Sachaufwandsträger von Schulen geeignete Schulräume und geeignete Räume für Veranstaltungen sowie Lehr- und Arbeitsmittel den Einrichtungen der Erwachsenenbildung nach Möglichkeit zur Mitbenutzung überlassen.

Der Vollzug dieser - an sich eindeutigen - gesetzlichen Bestimmung bereitet im Bereich der kommunalen Schulen offenbar immer wieder Schwierigkeiten, worauf der Bayerische Volkshochschulverband e.V. mich aufmerksam gemacht hat. Nach den Erfahrungen des Verbandes versuchten zunehmend mehr Schulleiter, die abendliche Benutzung der Schulräume durch die Volkshochschulen unter Hinweis auf sonst entstehende datenschutzrechtliche Probleme zu verhindern. Da - so die Argumentation der Schulleiter - einige Schülerinnen und Schüler nach Unterrichtsende ihre Schulhefte unter den Pulten liegen ließen, hätten die Teilnehmer von Volkshochschulkursen ansonsten abends die Möglichkeit, unberechtigterweise personenbezogene Daten der Schüler einzusehen.

In Anbetracht dieser Argumentation ist es mir ein Anliegen, in aller Deutlichkeit darauf hinzuweisen, dass datenschutzrechtliche Vorschriften, insbesondere Art. 85 BayEUG, der Überlassung von Schulräumen an Einrichtungen der Erwachsenenbildung zur Mitbenutzung nicht entgegenstehen. Um die von den Schulleitern geäußerten Bedenken auszuräumen, sollten diese die Schülerinnen und Schüler aus datenschutzrechtlichen Gründen vielmehr dazu anhalten, nach Unterrichtsschluss generell keine Schulhefte etc. unverschlossen im Klassenzimmer zu belassen. Daher kann der gem. Art. 14 Abs. 3 Bayerisches Schulfinanzierungsgesetz zur Entscheidung über die Verwendung des Schulvermögens für schulfremde Zwecke im Benehmen mit dem Schulleiter zuständige Sachaufwandsträger der Forderung des Art. 12 Abs. 1 Satz 1 EBFöG gerade dann unproblematisch Folge leisten, wenn die datenschutzrechtlichen Vorgaben von den Schulen ordnungsgemäß und vollständig umgesetzt werden.

Bereits in anderem Zusammenhang (siehe Nr. 11.3 dieses Tätigkeitsberichts) habe ich das Staatsministerium für Unterricht und Kultus darauf hingewiesen, dass die (von der Schule veranlasste) ungesicherte Aufbewahrung von Unterlagen mit personenbezogenen Schülerdaten unter den Schülerpulten datenschutzrechtlich unzulässig ist. Denn zum Zugriff auf solche Unterrichtsmaterialien sind nur der Schüler, seine Erziehungsberechtigten und die jeweils unterrichtende Lehrkraft berechtigt. Ein Zugriff weiterer Personen - etwa Mitschüler, Reinigungskräfte, Hausmeister sowie an außerschulischen Veranstaltungen im Klassenraum teilnehmende Personen usw. - auf diese Daten muss nach Art. 7 BayDSG durch entsprechende technische und organisatorische Maßnahmen zuverlässig ausgeschlossen werden. Dieses Erfordernis der Sicherung der Daten vor unberechtigtem Zugriff gewinnt insbesondere vor dem Hintergrund der Nutzung der Schulräume in den Nachmittags- und Abendstunden durch Einrichtungen der Erwachsenenbildung erheblich an Bedeutung.

Aufgrund der Mitteilung des Bayerischen Volkshochschulverbandes e.V. habe ich das Staatsministerium für Unterricht und Kultus über die im Zusammenhang mit der Überlassung von Schulräumen an Einrichtungen der Erwachsenenbildung zur Mitbenutzung aufgetretenen Probleme informiert. Das Kultusministerium hat sich erfreulicherweise meiner Rechtsauffassung angeschlossen. Auch aus Sicht des Staatsministeriums für Unterricht und Kultus erscheine es pädagogisch nicht unbedingt sinnvoll, Schulhefte in der Schule zurückzulassen. Das Kultusministerium habe die Sachaufwandsträger von Schulen wiederholt daran erinnert, den Einrichtungen der Erwachsenenbildung gem. Art. 12 Abs. 1 Satz 1 EBFöG geeignete Schulräume für Veranstaltungen zur Mitbenutzung zu überlassen. Wie von mir dargelegt, stehen dem die von den Schulleitern vorgebrachten datenschutzrechtlichen Bedenken nicht entgegen.

12 Hochschulen

12.1 „Hochschulreform 2006“

Der Bayerische Landtag hat im Mai 2006 unter dem Begriff „Hochschulreform 2006“ ein Gesetzespaket zur tiefgreifendsten Reform der bayerischen Hochschullandschaft seit 1973 beschlossen. Ziel dieser Reform ist ein neues, grundlegend modernisiertes Hochschulrecht mit den Schwerpunkten Neuordnung der Hochschulorganisationsstruktur, konkrete und überprüfbare Leistungs- und Finanzvereinbarungen, Erprobung von Globalhaushalten, Schärfung des Profils der Hochschulen durch Konzentration auf Schwerpunkte und Ausbau der auf internationale Nachfrage zugeschnittenen Studienangebote mit international vergleichbaren Abschlüssen.

Im Rahmen meiner Beteiligung im Gesetzgebungsverfahren konnte ich bei diesem Reformvorhaben auch zahlreiche Verbesserungen in datenschutzrechtlicher Hinsicht erreichen. Im Einzelnen sind insbesondere folgende Punkte zu erwähnen:

Nach Art. 6 Abs. 2 Satz 1 BayHSchG sind bei der Veröffentlichung von Forschungsergebnissen Personen, die einen eigenen wissenschaftlichen oder wesentlichen sonstigen Beitrag geleistet haben, als Mitautoren oder Mitautorinnen zu nennen; soweit möglich, ist ihr Beitrag zu kennzeichnen. Zwar begegnet

die damit einhergehende Veröffentlichung von personenbezogenen Daten der Mitautoren keinen datenschutzrechtlichen Bedenken, da sie offensichtlich im Interesse der Betroffenen liegt (Rechtsgedanke des Art. 17 Abs. 2 Nr. 3 BayDSG). Allerdings traf Art. 6 BayHSchG in der Fassung des Ressortentwurfs keine Aussage zur datenschutzrechtlichen Zulässigkeit der - in der Praxis bei Forschungsvorhaben bedeutsamen - Veröffentlichung von personenbezogenen Daten anderer Personen als der Mitautoren. Erst auf meine Anregung hin wurde in einem neuen Art. 6 Abs. 2 Satz 2 BayHSchG ein ausdrücklicher Verweis auf Art. 23 Abs. 4 BayDSG aufgenommen; danach ist eine solche Veröffentlichung nur zulässig, wenn der Betroffene eingewilligt hat oder dies für die Darstellung von Forschungsergebnissen über Ereignisse der Zeitgeschichte unerlässlich ist. Durch diesen Verweis kann nun die notwendige Sensibilisierung der Forschenden für diese nach meinen Erfahrungen wichtige Problematik in der Praxis sichergestellt werden.

Art. 10 BayHSchG regelt insbesondere die Bewertung von Forschung und Lehre. Mit dieser Problematik hatte ich mich bereits ausführlich in Nr. 20.2.1 meines 21. Tätigkeitsberichtes 2004 sowie in Nr. 15.4 meines 19. Tätigkeitsberichtes 2000 auseinander gesetzt.

– Nach Art. 10 Abs. 1 Satz 1 BayHSchG soll die Arbeit der Hochschulen in Forschung und Lehre, bei der Förderung des wissenschaftlichen Nachwuchses sowie der Erfüllung des Gleichstellungsauftrags regelmäßig bewertet werden. Die Ergebnisse der Bewertungen sollen gem. Art. 10 Abs. 1 Satz 2 BayHSchG in nicht personenbezogener Form veröffentlicht werden. Dabei wurde die ausdrückliche Festlegung, dass unter den Begriff der „Ergebnisse der Bewertungen“ im Sinne des Art. 10 Abs. 1 Satz 2 BayHSchG keine personenbezogenen Daten zu fassen sind, erst aufgrund meiner Bitte in den Gesetzestext aufgenommen.

– Art. 10 Abs. 2 BayHSchG enthält die Rechtsgrundlagen zur Etablierung eines Qualitätssicherungssystems an den Hochschulen (Datenerhebung und -verarbeitung, Mitwirkungspflicht von Hochschulmitgliedern). Vor allem in Anbetracht der in Art. 10 Abs. 2 Satz 3 BayHSchG insoweit gesetzlich angeordneten Mitwirkungspflicht der Hochschulmitglieder habe ich es für dringend erforderlich gehalten, als Korrelat für die Pflicht zur Angabe personenbezogener Daten ein gesetzliches Verwertungsverbot der gewonnenen Daten und ausgewerteten Ergebnisse zu anderen Zwecken in den Gesetzestext aufzunehmen. Dies ist durch Schaffung des Art. 10 Abs. 2 Satz 4 BayHSchG erfolgt. Meiner Meinung trägt ein solches gesetzliches Verwertungsverbot entscheidend dazu bei, die Akzeptanz der gesetzlichen Mitwirkungspflicht und damit auch die Motivation zur Unterstützung des Qualitätssicherungssystems bei den Mitgliedern der Hochschule - dazu gehören gem. Art. 17 Abs. 1 Satz 1 BayHSchG auch die Studierenden - zu erhöhen.

– Gemäß Art. 10 Abs. 3 Satz 1 BayHSchG können im Rahmen der Bewertung der Lehre die Studierenden als Teilnehmer und Teilnehmerinnen von Lehrveranstaltungen anonym über Ablauf sowie Art und Weise der Darbietung des Lehrstoffs befragt und die gewonnenen Daten verarbeitet werden; eine Auskunftspflicht besteht insoweit nicht. Art. 10 Abs. 3 Satz 2 BayHSchG in der Fassung des Ressortentwurfs erlaubte es sodann grundsätzlich, die dabei gewonnenen personenbezogenen Daten innerhalb der Hochschule zu verwerten.

  Im Gesetzgebungsverfahren habe ich mich diesbezüglich für die Beibehaltung der bisherigen Rechtslage (siehe dazu insbesondere Nr. 20.2.1 meines 21. Tätigkeitsberichtes 2004) ausgesprochen: So durften nach Art. 39 a Abs. 3 Satz 4 Halbsatz 1 BayHSchG a.F. die Bezeichnung der Lehrveranstaltungen, die Namen der Lehrenden und die ausgewerteten Ergebnisse der studentischen Befragungen allein dem Fachbereichsrat und der Hochschulleitung bekannt gegeben und zur Bewertung der Lehre verwendet werden; zuvor war den betroffenen Lehrenden gem. Art. 39 a Abs. 3 Satz 4 Halbsatz 2 BayHSchG a.F. Gelegenheit zur schriftlichen Stellungnahme zu den Bewertungsergebnissen zu geben. Demgegenüber wurden gem. Art. 39 a Abs. 3 Satz 5 BayHSchG a.F. den Mitgliedern des Fachbereichs nur die wesentlichen Ergebnisse der studentischen Befragungen, gegebenenfalls unter Hinzufügung der Stellungnahme des betroffenen Lehrenden, zugänglich gemacht. Die wesentlichen Ergebnisse sind eine personenbezogene Zusammenfassung der Bewertung durch die Studierenden, die auch in Form einer „Benotung“ bestehen kann. Andere Fachbereiche erhielten schließlich insoweit überhaupt keine Informationen.

  Für die Beibehaltung der bisherigen Regelung sprachen meiner Auffassung nach zahlreiche sachliche Gründe: So ist zunächst kein Grund ersichtlich, wieso Detailergebnisse anderen Personen als den Mitgliedern der Hochschulleitung zugänglich gemacht werden sollen. Diese bedürfen dieser Informationen, um die Dienstherrenfunktion der Hochschulleitung wirksam erfüllen zu können. Zur Erfüllung welcher gesetzlichen Aufgabe dritte Personen

die vollständigen Evaluationsergebnisse ebenfalls benötigen sollen, ist nicht erkennbar. Eine Zusammenfassung der Ergebnisse für die Mitglieder der Fakultät ist zur Sicherung und Verbesserung der Qualität der Lehre ebenfalls hinreichend. Eine Verbreitung über alle Fakultäten hinweg ist dagegen sachlich nicht erforderlich; es besteht sogar die Gefahr, dass sie dem Klima innerhalb der Hochschule abträglich sein könnte.

Erfreulicherweise wurden diese Argumente im Gesetzgebungsverfahren großenteils berücksichtigt. So bestimmt nunmehr Art. 10 Abs. 3 Satz 2 Halbsatz 1 BayHSchG, dass die personenbezogenen Daten nur dem Fakultätsrat und der Hochschulleitung bekannt gegeben und für die Bewertung der Lehre verwendet werden dürfen; den betroffenen Lehrpersonen ist dabei gem. Art. 10 Abs. 3 Satz 3 BayHSchG Gelegenheit zur Stellungnahme zu den Bewertungsergebnissen zu geben. Leider hat sich der Gesetzgeber aber dazu entschlossen, die wesentlichen Ergebnisse der studentischen Befragungen nunmehr gem. Art. 10 Abs. 3 Satz 2 Halbsatz 2 BayHSchG nicht nur allen Mitgliedern der Fakultät, sondern allen Mitgliedern der Hochschule, gegebenenfalls unter Hinzufügung der Stellungnahme der betreffenden Lehrperson, zugänglich zu machen. Dies halte ich nach wie vor für sachlich nicht erforderlich.

Art. 30 BayHSchG regelt Stellung und Aufgaben des Studiendekans / der Studiendekanin. So ist er / sie u.a. verantwortlich für die Evaluation der Lehre unter Einbeziehung studentischer Bewertungen (Art. 30 Abs. 2 Nr. 2 BayHSchG) und erstattet dem Fakultätsrat jährlich in nicht personenbezogener Form einen Bericht zur Lehre (Lehrbericht, Art. 30 Abs. 2 Nr. 4 BayHSchG). Dieser Lehrbericht enthält nach Art. 30 Abs. 3 Satz 2 BayHSchG für den Berichtszeitraum auch Angaben über die Bewertung des Lehrangebotes in den einzelnen Studiengängen durch die Studierenden. Da bereits nach bislang geltendem Recht (Art. 39 a Abs. 2 Satz 4 Halbsatz 2, Abs. 3 Satz 1 Halbsatz 2 BayHSchG a.F.) der Lehrbericht keine personenbezogenen Daten der Bewerteten enthalten - und daher auch veröffentlicht werden - durfte (vgl. auch insoweit die Nr. 20.2.1 meines 21. Tätigkeitsberichtes 2004), habe ich im Gesetzgebungsverfahren darum gebeten, diese in datenschutzrechtlicher Hinsicht bedeutsame Klarstellung nunmehr in den Gesetzestext selbst aufzunehmen. Dies ist durch Einfügung der Worte „in nicht personenbezogener Form“ in Art. 30 Abs. 2 Nr. 4 BayHSchG geschehen.

Auch beim Bayerischen Hochschulpersonalgesetz (BayHSchPG) konnte ich eine wesentliche Verbesserung in datenschutzrechtlicher Hinsicht erreichen. Nach der Fassung des Ressortentwurfs des Art. 18 Abs. 4 Satz 6 BayHSchPG durfte bei Berufungen von Professoren, Professorinnen, Juniorprofessoren und Juniorprofessorinnen der Berufungsvorschlag auch die Namen von Personen enthalten, die sich nicht beworben haben. Diese ursprünglich geplante Regelung habe ich als datenschutzrechtlich äußerst bedenklich abgelehnt, da sie das Recht auf informationelle Selbstbestimmung all derer gefährdet, die ohne ihr Wissen und ohne ihr Zutun auf eine Vorschlagsliste gesetzt werden. Davon abgesehen ist es meiner Meinung nach nicht ohne weiteres einsichtig, warum jemand in das Bewerbungsverfahren um eine Hochschullehrerstelle einbezogen werden soll, ohne auch nur im Ansatz eigene Anstrengungen hierzu unternommen zu haben. Schließlich sind auch missbräuchliche Verfahrensweisen - etwa mehrfaches, absichtliches Setzen einer Person, die an den ausgeschriebenen Stellen überhaupt nicht interessiert ist, aus sachfremden Gründen - durchaus denkbar. Erfreulicherweise wurde daraufhin Art. 18 Abs. 4 Satz 6 BayHSchG insoweit ergänzt, als der Berufungsvorschlag nur mit deren Einwilligung auch die Namen von Personen enthalten darf, die sich nicht beworben haben.

12.2 Langzeit-Forschungsprojekt „Bayerisches Absolventenpanel“

In Zusammenarbeit mit den bayerischen Universitäten und Fachhochschulen führt das Staatsinstitut für Hochschulforschung und Hochschulplanung seit 2005 das LangzeitForschungsprojekt „Bayerisches Absolventenpanel“ durch. Ziel dieses für die bayerische Hochschulpolitik bedeutsamen Projektes ist es, eine Absolventenbefragung in Bayern zu etablieren, die sowohl das Staatsministerium für Wissenschaft, Forschung und Kunst als auch die bayerischen Hochschulen in regelmäßigen Abständen über die Qualität der Ausbildung sowie den Arbeitsmarkt- und Berufserfolg bayerischer Absolventen informiert. Auf Länderebene gibt es bislang keine vergleichbare Studie.

Im Rahmen des „Bayerischen Absolventenpanels“ sollen im Zwei-Jahres-Rhythmus zuverlässige Informationen zu Studium, Berufseinstieg und beruflichem Werdegang bayerischer Hochschulabsolventen erhoben werden. Anstelle einer Querschnittsbefragung wird bei diesem Forschungsprojekt ein Längsschnittdesign gewählt, d.h. die gleiche Gruppe von Personen wird zu mehreren aufeinander folgenden Zeitpunkten befragt. Erforderlich ist damit eine Verknüpfung der Befragungsdaten über die einzelnen Erhebungswellen hinweg.

Durch meine Begleitung des Forschungsprojekts konnte ich bereits in der Konzeptionsphase zu einer datenschutzgerechten Gestaltung des „Bayerischen

Absolventenpanels“ beitragen. Im Einzelnen möchte ich insbesondere folgende Punkte erwähnen:

- Zur Erstkontaktierung erhält das Staatsinstitut für Hochschulforschung und Hochschulplanung von den Hochschulen keine Adressdaten der für die Teilnahme an der Befragung in Betracht kommenden Absolventen. Andernfalls hätte dies mit der Zeit zum Aufbau eines bayernweiten, zentralen „Absolventenregisters“ geführt, was ich wegen der damit einhergehenden Datenschutzrisiken grundsätzlich ablehne. Vielmehr wird ein so genanntes „Adressmittlungsverfahren“ eingesetzt.

- Zur Durchführung der Folgebefragungen werden beim Staatsinstitut für Hochschulforschung und Hochschulplanung die Adressdaten der Absolventen erst nach vorheriger, datenschutzgerechter individueller Einwilligung gespeichert. Die Einwilligung kann dabei - worauf in der Teilnehmerinformation ausdrücklich hingewiesen wird - von den Projektteilnehmern jederzeit ohne Angabe von Gründen widerrufen werden.

- Zur Verknüpfung der Befragungsdaten wird von der ursprünglich beabsichtigten Verwendung identifizierender Merkmale - etwa die ersten beiden Buchstaben des Namens - abgesehen. Vielmehr wird bei der Bildung der pseudonymen Kennziffer ein datenschutzkonformes Pseudonymisierungsverfahren gewählt.

Unter Beachtung meiner datenschutzrechtlichen Vorgaben gestaltet sich der Ablauf des Projektes nunmehr wie folgt:

Für die Erstbefragung versenden die Hochschulen im Rahmen eines so genannten „Adressmittlungsverfahrens“ die vom Staatsinstitut für Hochschulforschung und Hochschulplanung vorbereiteten Informationsschreiben und Fragebögen an die ausgewählten Absolventen. Diese erteilen - auf freiwilliger Basis - ihre Einwilligung in die Teilnahme an der Studie und senden die Einwilligungserklärung sowie den ausgefüllten Fragebogen unmittelbar an das Staatsinstitut zurück. Das Staatsinstitut speichert die Adressdaten der Teilnehmer unter einer pseudonymen Kennziffer und wertet den Fragebogen nur unter dieser Kennziffer aus; Adress- und Befragungsdaten werden dabei getrennt gespeichert. Sodann führt das Staatsinstitut - bei fortbestehender Einwilligung - die Folgebefragungen durch; auch hierbei werden Adress- und Befragungsdaten strikt getrennt.

Abweichend von einem „normalen“ Adressmittlungsverfahren tragen die von den Hochschulen für die Erstbefragung versandten Informationsschreiben und Fragebögen allerdings als Absender die Adresse des Staatsinstituts für Hochschulforschung und Hochschulplanung. Auf diese Weise erhält das Staatsinstitut auch die Adressen derjenigen Absolventen, denen die Schreiben nicht zugestellt werden konnten. Auf meine diesbezügliche Nachfrage hin hat das Staatsinstitut ausgeführt, dass es für den Erfolg eines Langzeit-Forschungsprojektes und den Aufbau eines Panels von entscheidender Bedeutung sei, bei der Erstbefragung möglichst viele Absolventen zu erreichen; insbesondere dürfe es nicht zu einem selektiven Ausfall bei bestimmten Gruppen - hier etwa bei den besonders mobilen Absolventen - kommen. Die ohnehin stark belasteten Hochschulverwaltungen sähen sich jedoch - was von den Hochschulen in der Folgezeit bestätigt wurde - nicht in der Lage, die in diesen Fällen erforderlichen, intensiven (u.U. Auslands-)Adressrecherchen zu übernehmen. Vor diesem Hintergrund habe ich schließlich meine datenschutzrechtlichen Bedenken gegen die Übermittlung dieser Adressdaten an das Staatsinstitut mit folgenden Maßgaben zurückgestellt:

- Die Adressen werden beim Staatsinstitut nur zur Ermittlung der aktuellen Anschrift vorübergehend gespeichert.

- Ist diese ermittelt, ist der Absolvent darauf hinzuweisen, auf welche Art und Weise das Staatsinstitut seine aktuelle Anschrift erlangt hat. Selbstverständlich ist für die Projektteilnahme dann auch - wie in den übrigen Fällen - eine datenschutzgerechte Einwilligung des Absolventen erforderlich.

- Verweigert der Absolvent diese Einwilligung, sind die gespeicherten Daten unverzüglich zu löschen.

Abschließend hoffe ich, dass meine datenschutzrechtliche Begleitung des „Bayerischen Absolventenpanels“ exemplarisch zeigt, dass jedenfalls die zu meinem Bedauern aus Unkenntnis nicht nur im Forschungsbereich oftmals beklagten, angeblichen „datenschutzrechtlichen Hindernisse“ der Durchführung und dem Erfolg auch eines Langzeit-Forschungsprojekts nicht entgegen stehen.

12.3 Keine Pflicht zur Veröffentlichung des Lebenslaufes in Dissertationen

Aufgrund einiger Eingaben betroffener Personen befasste ich mich im Berichtszeitraum mit der Frage, ob die in Promotionsordnungen bayerischer Fakultäten enthaltene Pflicht zur Veröffentlichung des Lebenslaufes in Dissertationen in Einklang mit den datenschutzrechtlichen Vorschriften steht.

Die betroffenen Doktoranden wandten sich durchaus nicht dagegen, den zuständigen Stellen der Fakultäten im Rahmen des Promotionsverfahrens ihren aktuellen Lebenslauf vorzulegen. Sie sahen sich jedoch aufgrund der durch die Promotionsordnung ihnen auferlegten Pflicht, auch im Falle der Verbreitung über den Buchhandel die Dissertation in gedruckter Form einschließlich Lebenslauf zu veröffentlichen, in ihrem Recht auf informationelle Selbstbestimmung verletzt. Eine zusätzliche Verschärfung erfuhr die Problematik noch dadurch, dass Universitäten zunehmend mehr Dissertationen als Online-Publikationen (sog. eDissertationen) im Internet veröffentlichen und für den weltweiten Zugriff bereit halten. Insoweit befürchtete ein Doktorand, dass beispielsweise kommerzielle Adresshandelsunternehmen oder Identitätsdiebe mit automatisierten Suchprogrammen auf ihre persönlichen Daten zugreifen könnten. Entsprechende, nicht nur nach Ausbildungsrichtungen aufgeteilte Datenbanken angehender Akademiker seien - so die Petition weiter - durchaus als Ziel von Begehrlichkeiten denkbar.

Ich halte nicht nur die durch die jeweilige Promotionsordnung dem Promovenden im Falle der Verbreitung über den Buchhandel auferlegte Pflicht zur Veröffentlichung seines Lebenslaufes, sondern bereits die in der Promotionsordnung enthaltene Pflicht zur Beifügung des Lebenslaufs zu den bei der Universitätsbibliothek abzuliefernden Pflichtexemplaren für datenschutzrechtlich nicht hinnehmbar. Dies gilt erst recht, wenn der Lebenslauf zusätzlich in einer frei zugänglichen Version der Dissertation auf dem Dokumentenserver der Universität bereit gehalten wird.

Die Übermittlung personenbezogener Daten durch öffentliche Stellen, wozu auch Universitäten gehören, an nicht-öffentliche Stellen - die Leser der Dissertation - ist nach Art. 19 Abs. 1 Nr. 2 BayDSG nur zulässig, wenn die nicht-öffentliche Stelle ein berechtigtes Interesse an der Kenntnis der zu übermittelnden Daten glaubhaft darlegt und der Betroffene (also der Promovierte) kein schutzwürdiges Interesse an dem Ausschluss der Übermittlung hat. Selbst wenn man die regelmäßige Erfüllung der ersten Tatbestandsvoraussetzung unterstellte, kann doch von der regelmäßigen Bejahung auch der zweiten nicht ausgegangen werden.

Für die ordnungsgemäße Erfüllung der der Fakultät im Rahmen des Promotionsverfahrens zugewiesenen Aufgabe - der Prüfung, ob die vorgelegte Arbeit als Nachweis einer eigenständigen wissenschaftlichen Leistung und der Fähigkeit des Bewerbers zur selbstständigen sowie vertieften wissenschaftlichen Arbeit geeignet ist - ist die Veröffentlichung des Lebenslaufes des Bewerbers nicht erforderlich. Auch die Tatsache, dass eine solche Veröffentlichungspraxis akademischem Herkommen entspricht, reicht als Begründung für deren datenschutzrechtliche Zulässigkeit nicht aus.

Nachdem bereits in den Jahren 1995/96 diese Problematik ohne Ergebnis erörtert worden war, habe ich mich im Berichtszeitraum wegen der bayernweiten Bedeutung der Angelegenheit erneut an das Staatsministerium für Wissenschaft, Forschung und Kunst gewandt. Dabei habe ich das Staatsministerium auch gebeten zu berücksichtigen, dass eine Streichung der in Promotionsordnungen bayerischer Fakultäten normierten Pflicht zur Veröffentlichung des Lebenslaufes in Dissertationen einen wichtigen Beitrag zu den von der Staatsregierung besonders betonten Deregulierungsanstrengungen leisten würde.

Um die Auffassung der bayerischen Universitäten zu der von mir angeregten Streichung zu erfahren, hat das Staatsministerium für Wissenschaft, Forschung und Kunst seinerseits Stellungnahmen der Hochschulen sowie der Universität Bayern e.V. - als Verband der bayerischen Universitäten - eingeholt. Eine der betroffenen Universitäten hat daraufhin mitgeteilt, dass sie - in Abkehr von ihrer noch im Jahr 1996 vertretenen Auffassung - im Hinblick insbesondere auf die gesteigerte Bedeutung des Rechts auf informationelle Selbstbestimmung eine Pflicht zur Veröffentlichung des Lebenslaufes in Dissertationen für nicht mehr erforderlich hält. Erfreulicherweise ist in der Folge auch die Universität Bayern e.V. einstimmig zu der Überzeugung gelangt, dass aus ihrer Sicht zukünftig auf die Veröffentlichungspflicht verzichtet werden kann und sollte.

Ebenso wie das Staatsministerium für Wissenschaft, Forschung und Kunst gehe auch ich daher davon aus, dass die Universitäten ihre Promotionsordnungen zeitnah entsprechend anpassen werden.

13 Gesundheitswesen

13.1 Gesundheitsverwaltung und Kassenärztliche Vereinigung

13.1.1 Presseinformationen des Gesundheitsamts zu Infektionskrankheiten

Zwischen den Wünschen der Presse nach umfassender Information und dem informationellen Selbstbestimmungsrecht kann ein Spannungsverhältnis bestehen, wie auch folgender Fall zeigt:

In einem Landkreis ist ein schwerer Fall von Meningitis (Hirnhautentzündung) aufgetreten. Das Landratsamt hat nicht von sich aus die Öffentlichkeit in der Region informiert. Die Presse hat dieses Verhalten des Landratsamts kritisch kommentiert. Das Landratsamt (Gesundheitsamt) hat sich daraufhin mit einer Anfrage an mich gewandt, ob und wie es von

sich aus die Öffentlichkeit beim Vorliegen von Infektionskrankheiten informieren muss, ohne datenschutzrechtliche Grundsätze zu verletzen.

Aufgabe der öffentlichen Stellen ist auch ihre allgemeine Öffentlichkeitsarbeit. In Einklang mit diesem allgemeinen Grundsatz bestimmt Art. 8 des Gesetzes über den öffentlichen Gesundheits- und Veterinärdienst, die Ernährung und den Verbraucherschutz sowie die Lebensmittelüberwachung (Gesundheitsdienst- und Verbraucherschutzgesetz - GDVG), dass die Gesundheitsämter an der Information und Aufklärung der Bevölkerung in allen Fragen des öffentlichen Gesundheitsdienstes und des gesundheitlichen und ernährungsbezogenen Verbraucherschutzes mitwirken. Danach ist also das Gesundheitsamt grundsätzlich berechtigt, von sich aus die Presse bzw. die Medien über relevante Ereignisse aus dem eigenen Zuständigkeitsbereich zu informieren.

Werden Tatsachen festgestellt, die zum Auftreten einer übertragbaren Krankheit führen können oder ist anzunehmen, dass solche Tatsachen vorliegen, so trifft das Gesundheitsamt die notwendigen Maßnahmen zur Abwendung der dem Einzelnen oder der Allgemeinheit hierdurch drohenden Gefahren, vgl. § 16 Abs. 1 Satz 1 des Gesetzes zur Verhütung und Bekämpfung von Infektionskrankheiten bei Menschen (Infektionsschutzgesetz - IfSG). Je nach konkreter Gefährdungslage vor Ort kann sich dadurch die Berechtigung des Gesundheitsamts zur Presseinformation zu einer Verpflichtung verdichten.

Sollen jedoch auch personenbezogene Daten übermittelt werden, so ist auch die Zulässigkeit dieser Übermittlung zu prüfen:

Als Grundvoraussetzung jeder Übermittlung personenbezogener Daten durch die Herausgabe der entsprechenden Presseinformationen muss diese Übermittlung zur Aufgabenerfüllung (also zur Gefahrenabwehr) erforderlich sein. Zwar kommt es insofern jeweils ganz auf die Umstände des Einzelfalls an, allgemein wird sich jedoch sagen lassen, dass die Übermittlung personenbezogener Daten in einer bzw. durch eine Presseinformation sich nur in Ausnahmefällen zur erfolgreichen Abwehr der Gefahr als erforderlich erweisen wird. Denn in den meisten Fällen wird es ausreichen, dass das Gesundheitsamt von sich aus mögliche Kontaktpersonen ermittelt und diese über eine mögliche Infektion informiert und berät.

Eine unbedingte und voraussetzungslose Verpflichtung des Gesundheitsamts, jeden Erkrankungsfall unter namentlicher Nennung des/der Betroffenen aktiv von sich aus der Presse zu melden, wäre mit den gesetzlichen Vorgaben unvereinbar.

13.1.2 Neugeborenen-Screening

Die Neuordnung des Neugeborenen-Screenings in Bayern habe ich seinerzeit auch wegen seiner bundesweiten Vorreiterstellung intensiv in datenschutzrechtlicher Hinsicht begleitet und hierzu ausführlich in meinem 18. Tätigkeitsbericht (Nr. 3.1.1) Stellung genommen. Seither hat sich das Neugeborenen-Screening in Bayern in den vergangenen Jahren - auch und gerade in datenschutzrechtlicher Hinsicht - sehr gut bewährt.

Zusätzlich zu den eigentlichen Untersuchungsverfahren wird in Bayern das so genannte Tracking-Verfahren durchgeführt, mit dessen Hilfe unter Einschaltung der Gesundheits- und Einwohnermeldeämter sichergestellt werden soll, dass die Eltern jedes in Bayern geborenen Kindes die Möglichkeit erhalten haben, ihr Kind (wie ca. 98 % aller in Bayern geborenen Kinder) am Neugeborenen-Screening teilnehmen zu lassen. Zu diesem Zweck melden die Kliniken die Neugeborenen, die am Screening teilgenommen haben, (nur den sog. Stammdatensatz, also Name des Kindes, Geburtsdatum, Name und Anschrift der Eltern - ohne jegliche Aussage zum Ergebnis des Screenings) den Gesundheitsämtern. Daraufhin stellen die Gesundheitsämter an Hand der Meldedaten fest (§ 5 a Bayerische Meldedaten-Übermittlungsverordnung), ob Neugeborene im Amtsbezirk bislang noch nicht am Screening teilgenommen haben und weisen deren Eltern in einem Anschreiben auf die bestehende Möglichkeit des Screenings und seine Vorteile hin und bieten diesbezügliche Beratung an. Abschließend wird die Teilnahmequote am Neugeborenen-Screening mittels einer statistischen Erhebung ermittelt.

Im Berichtszeitraum fragte die Datenschutzbeauftragte eines Landratsamtes an, ob und ggf. zu welchen Zwecken die weitere Speicherung der beim Gesundheitsamt im Rahmen des Neugeborenen-Screenings angefallenen Stammdatensätze (Name des Kindes, Geburtsdatum, Name und Anschrift der Eltern) zulässig sei. Der Anfrage lag folgender Sachverhalt zu Grunde: Beim jugendärztlichen Dienst des Gesundheitsamtes werde das EDV-Modul „Einschulungsuntersuchung mit Screening“ eingesetzt. Dort würden im Rahmen des Neugeborenen-Screenings die von den Kliniken gemeldeten Stammdaten erfasst. Mit diesen Daten sei lediglich die Angabe verknüpft, ob ein Screening stattgefunden habe. Diese Angabe würde nach Abschluss der statistischen Auswertung gelöscht. Der Stammdatensatz (Name des Kindes, Geburtsdatum, Name und Anschrift der Eltern) bliebe aber in der EDV erhalten, um diese Daten bei der Einschulungsuntersuchung nicht erneut erfassen zu müssen. Die Datenschutzbeauftragte des Landratsamtes hielt diese weitere Speicherung der isolierten Stammdatensätze für datenschutzrechtlich unzulässig, obwohl keinerlei weitere Informationen (insbesonde-

re Gesundheitsdaten) damit verknüpft seien und diese Daten auch vom sonstigen Gesundheitsmedizinischen Dienst des Gesundheitsamtes nicht eingesehen oder sonst genutzt werden könnten.

Ich habe in meiner Stellungnahme zunächst daraufhin gewiesen, dass mangels bereichsspezifischer Regelungen das Speichern, Verändern oder Nutzen personenbezogener Daten gemäß Art. 17 Abs. 1 BayDSG nur zulässig ist, wenn es zur Erfüllung der in der Zuständigkeit der speichernden Stelle liegenden Aufgaben erforderlich ist und es für die Zwecke erfolgt, für die die Daten erhoben worden sind. Beide Voraussetzungen waren im vorliegenden Fall nicht erfüllt.

Bereits der Wortlaut des Gesetzes „erforderlich ist“ macht für eine rechtmäßige Datenspeicherung zur Voraussetzung, dass diese auf konkrete und aktuell zur Bewältigung anstehende Aufgaben bezogen ist. Personenbezogene Daten dürfen nicht vorab oder vorsorglich für den Fall erhoben werden, dass sie später einmal (möglicherweise) benötigt werden. Dies wäre eine grundsätzlich unzulässige Speicherung der Daten auf Vorrat.

Überdies ist zu bedenken, dass sich während des zwischen dem Neugeborenen-Screening und der Einschulungsuntersuchung liegenden Zeitraumes aller Voraussicht nach ein nicht unerheblicher Änderungsbedarf (Hin- und Wegzüge) im Datenbestand ergibt, welcher eingepflegt werden muss. Zudem entstünde eine dem Melderegister vergleichbare parallele Datensammlung.

Vor allem aber stellt eine solche Vorgehensweise eine geradezu klassische Durchbrechung des im Datenschutzrecht fundamentalen Grundsatzes der Zweckbindung dar, da die ursprünglich im Rahmen des Neugeborenen-Screenings angefallenen Daten nunmehr für einen anderen Zweck (Durchführung der Einschulungsuntersuchung) genutzt werden sollen. Diese Zweckänderung ist keinesfalls von der Einwilligung der Eltern, welche ihr Kind am Neugeborenen-Screening teilnehmen lassen, abgedeckt. Da zudem keine den verfassungsrechtlichen Anforderungen gerecht werdende, normenklare gesetzliche Befugnisnorm existiert, die diese Zweckänderung erlaubte (insbesondere liegen die Voraussetzungen des Art. 17 BayDSG nicht vor), ist die weitere Speicherung der Stammdatensätze schlichtweg unzulässig.

Ich habe der Datenschutzbeauftragten des Landratsamtes mitgeteilt, dass die geschilderte Vorgehensweise nicht mit den datenschutzrechtlichen Vorschriften zu vereinbaren ist sowie daraufhin gewiesen, dass die unzulässigerweise gespeicherten Daten gem. Art. 12 Abs. 1 Nr. 1 BayDSG unverzüglich zu löschen sind.

13.1.3 Mammographie-Screening

Ein derzeit viel diskutiertes Thema ist die flächendeckende Einführung des Mammographie-Screenings gemäß den Krebsfrüherkennungs-Richtlinien des Bundesausschusses der Ärzte und Krankenkassen. Wie schon in meinem 21. Tätigkeitsbericht unter Nr. 6.2 dargestellt, gab es in Bayern bereits ein Pilotprojekt der Kassenärztlichen Vereinigung Bayerns (KVB) und der gesetzlichen Krankenkassen hierzu, das nunmehr an die neuen Anforderungen angepasst werden muss.

Nach dem neuen Konzept werden die anspruchsberechtigten Frauen nunmehr von einer so genannten zentralen Stelle eingeladen, die in Bayern bei der KVB angesiedelt ist. Diese soll für diesen Zweck von den Meldeämtern die Daten aller in Frage kommenden Frauen erhalten und wird daraus die Einladungen generieren. Die Teilnahme am Screening ist freiwillig. Erscheint die Klientin in der Screening-Einheit, so werden Mammographie-Aufnahmen erstellt und sowohl von einem Erstbefunder, als auch von einem unabhängigen Zweitbefunder beurteilt. In Zweifelsfällen werden weitere Befunder hinzugezogen. Der Klientin wird das Ergebnis schriftlich mitgeteilt.

Für das Mammographie-Screening werden bei der Klientin eine Vielzahl von Daten erhoben, wie z.B. identifizierende Daten (Name, Adresse), medizinische Daten (Befunde, Diagnosen, Vorgeschichte) und Mammographie-Aufnahmen. Die eindeutige Identifikation der Klientinnen erfolgt über eine 10-stellige ScreeningID mit der alle erhobenen Bilder und Daten gekennzeichnet werden. Dennoch stehen dem Arzt für die Befundung auch die identifizierenden Daten der Klientin zur Verfügung, um Verwechslungen zu vermeiden.

Zur Evaluation der Teilnahmequote ist eine Auswertung der Einladungsdaten vorgesehen, die durch gesondert auf den Datenschutz verpflichtete Mitarbeiter der KVB durchgeführt wird. Des Weiteren findet eine Auswertung der medizinischen Daten durch die KVB im Rahmen der Qualitätssicherung statt. Darüber wird mit dem Krebsregister abgeglichen. Dabei werden die Daten jedoch nicht personenbezogen, sondern mit Kontrollnummern versehen an die Registerstelle des Krebsregisters übermittelt. Die Daten aus dem Krebsregister werden nach dem gleichen Prinzip mit Kontrollnummern versehen, so dass ein Abgleich der Daten möglich ist. Ziel ist es, die Qualität des Screenings zu überprüfen und beispielsweise Falschdiagnosen (kein Brustkrebs) zu erkennen.

Um den Dokumentationsaufwand möglichst gering zu halten, soll eine elektronische Dokumentation des Screenings erfolgen. Hierzu hat die KVB eine eigene Softwarelösung MammaSoft entwickelt, die auch in

anderen Bundesländern zum Einsatz kommen soll. Diese Software läuft auf einem von der KVB betriebenen Datenbank-Server und ermöglicht über ein Web-Interface die Eingabe der Daten. In dieser Datenbank sind sowohl die Einladungsdaten der zentralen Stelle, als auch die medizinischen Befunddaten in einer Datenbank gespeichert. Die Mitarbeiter der zentralen Stelle greifen über ein Virtual Private Network (VPN) auf den Server zu, die Screening-Einheiten sind über das KV-Safenet (siehe 21. Tätigkeitsbericht, Nr. 22.2.3.1) angebunden.

Eine zentrale Stelle darf nach meiner Ansicht nicht identisch mit der KVB, sondern allenfalls bei der KVB angesiedelt sein. Der tiefere Grund dafür ist, dass die zentrale Stelle Daten von Personen bekommt, die nicht am System der gesetzlichen Krankenversicherung teilnehmen. Weiter ist es ein Anliegen des Datenschutzes, dass zentrale Datenbestände wegen der damit verbundenen Missbrauchsmöglichkeit möglichst verhindert werden sollen. Auch wenn nur ein bestimmter Teil der Bevölkerung im Datenbestand der KVB verzeichnet ist, wäre eine unmittelbare Aufgabenerfüllung der zentralen Stelle durch die KVB ein weiterer Schritt in diese Richtung. Die KVB hatte nach meiner Intervention keine grundsätzlichen Bedenken gegen eine technische und organisatorische Trennung der zentralen Stelle vom sonstigen KVB-Betrieb.

Jedoch wirft der mir übermittelte Lösungsansatz der KVB insbesondere aus Sicht des technisch-organisatorischen Datenschutzes einige Fragen auf.

Insbesondere soll nach dem neuesten Konzeptentwurf der Datenbank-Server nicht mehr in den Räumen der KVB stehen, sondern bei einem externen Provider. In diesem Fall müssen diverse Sicherheitsmaßnahmen analog zu der im 21. Tätigkeitsbericht unter Nr. 22.2.3.2 dargestellten externen Archivierung ergriffen werden. Dies beinhaltet insbesondere eine verschlüsselte Datenspeicherung, so dass der Provider keine Kenntnis von den bei ihm gespeicherten Daten nehmen kann.

Die aufgeworfenen Probleme werden derzeit noch mit der KVB diskutiert, so dass noch keine abschließende Bewertung des Mammographie-Screenings möglich ist.

13.1.4 Einsichtnahme in Impfbücher und Erstellung einer Impfstatistik durch ein Gesundheitsamt

In vielen Fällen sind Ämter zu ihrer Aufgabenerfüllung auf die Mitwirkung der Bevölkerung angewiesen. Welche datenschutzrechtlichen Grundsätze bei einem Einladungsschreiben zu einer Behördenaktion zu beachten sind, zeigt folgender Beispielsfall:

Die Gesundheitsabteilung eines Landratsamtes bot in einem Rundschreiben an alle Eltern der Schülerinnen und Schüler der 8. Klassen eine „Kontrolle der Impfbücher“ an. Um einen Überblick über die Durchimpfung im Landkreis zu erhalten, würden die Mitarbeiterinnen des Gesundheitsamts an einem bestimmten Tag die Impfbücher der Kinder in der Schule einsehen. Daher würden die Eltern gebeten, ihrem Kind zu diesem Termin das Impfbuch in die Schule mitzugeben. Sie erhielten es umgehend mit der Mitteilung zurück, welche Impfungen bei ihrem Kind fehlten.

Die Eltern eines betroffenen Kindes wandten sich im Wege einer Eingabe an mich und baten um Prüfung, ob dieses Vorgehen mit den geltenden datenschutzrechtlichen Vorschriften zu vereinbaren sei. Grundsätzlich sei die Aktion des Gesundheitsamtes, die Impfbücher auf fehlende Impfungen zu kontrollieren, zu begrüßen. Allerdings sollte dies - so die besorgten Eltern weiter - auf freiwilliger Basis erfolgen. Außerdem hätten sie erhebliche Bedenken gegen die Tatsache, dass Gesundheitsdaten der Kinder für eine Statistik erhoben werden sollten. Ich habe die Angelegenheit in datenschutzrechtlicher Hinsicht wie folgt bewertet:

Einsichtnahme in Impfbücher

Rechtsgrundlage für diese Maßnahme ist Art. 16 Abs. 1 BayDSG. Danach ist das Erheben personenbezogener Daten zulässig, wenn ihre Kenntnis zur Erfüllung der in der Zuständigkeit der erhebenden Stelle liegenden Aufgaben erforderlich ist. Darüber hinaus ist gemäß Art. 15 Abs. 7 Nr. 9 BayDSG das Erheben personenbezogener Daten über die Gesundheit nur zulässig, wenn es zum Zwecke der Gesundheitsvorsorge erforderlich ist und die Verarbeitung dieser Daten durch ärztliches Personal oder durch sonstige Personen erfolgt, die einer entsprechenden Geheimhaltungspflicht unterliegen.

Gemäß § 34 Abs. 10 des Gesetzes zur Verhütung und Bekämpfung von Infektionskrankheiten beim Menschen (Infektionsschutzgesetz - IfSG) sollen die Gesundheitsämter und die in § 33 IfSG genannten Gemeinschaftseinrichtungen - zu denen auch Schulen gehören - die betreuten Personen oder deren Sorgeberechtigte gemeinsam über die Bedeutung eines vollständigen, altersgemäßen, nach den Empfehlungen der Ständigen Impfkommission beim Robert-Koch-Institut ausreichenden Impfschutzes aufklären. Weiter bieten die Gesundheitsbehörden gesundheitliche Beratung und Untersuchung im Kindes- und Jugendalter, insbesondere im Rahmen der schulärztlichen Aufgaben an (Art. 13 Abs. 1 Satz 2 Nr. 3 GDVG). Im vorliegenden Fall handelte also die Gesundheitsabteilung des Landratsamtes im Rahmen seines gesetzlichen Auftrages. Die Einsichtnahme in die Impfbücher erfolgt durch sozialmedizinische Assistentinnen

(Kinderkrankenschwestern) der Gesundheitsbehörde, die der ärztlichen Schweigepflicht gemäß § 203 StGB unterliegen.

Allerdings erfolgt die Einsichtnahme in die Impfbücher der Schülerinnen und Schüler auf freiwilliger Basis, weshalb die Betroffenen auf die Freiwilligkeit hinzuweisen sind (Art. 16 Abs. 3 Satz 2 BayDSG). In dem Elternanschreiben der Gesundheitsbehörde kam der Hinweis auf die Freiwilligkeit lediglich ansatzweise zum Ausdruck („bietet ... an“). Vor der Durchführung solcher Impfbucheinsichten müssen die Gesundheitsbehörden im Elternanschreiben demgegenüber ausdrücklich auf die Freiwilligkeit der Teilnahme und auch auf Verlangen auf die Folgen der Nichtteilnahme hinweisen. Ich habe deshalb das Gesundheitsamt gebeten, die Freiwilligkeit in dem Elternanschreiben stärker herauszustellen.

Erstellung einer Impfstatistik

Die von mir um Stellungnahme gebetene Gesundheitsabteilung des betroffenen Landratsamtes hat ausgeführt, dass die in den vorgelegten Impfbüchern verzeichneten Schutzimpfungen ohne jeden Personenbezug auf eine Strichliste übertragen würden, auf welcher lediglich die entsprechenden Krankheiten und die zu ihrer Vorbeugung (abstrakt) erforderlichen Schutzimpfungen verzeichnet sind. Aus den so gewonnenen Zahlen könne weder auf die an der Impfbucheinsicht teilnehmenden Personen noch auf deren Impfstatus geschlossen werden. Die in den einzelnen Schulen gewonnenen Zahlen würden anschließend auf Landkreisebene zusammengefasst und hieraus die Impfraten in Bezug auf die jeweiligen Schutzimpfungen errechnet.

Aufgrund der landkreisweiten Zusammenfassung der Zahlen ist meiner Auffassung nach ein Rückschluss auf einzelne Schülerinnen und Schüler nicht mehr möglich. Insofern werden durch die Erstellung der solchermaßen beschriebenen Impfstatistik keine personenbezogenen Daten (Einzelangaben über persönliche oder sachliche Verhältnisse bestimmter oder bestimmbarer natürlicher Personen, Art. 4 Abs. 1 BayDSG) erhoben. Allerdings musste ich insoweit feststellen, dass die wünschenswerte Angabe des Zweckes der Statistik sowie eine Erläuterung der Vorgehensweise bei ihrer Aufstellung gegenüber den Erziehungsberechtigten unterlieben ist. Die Gesundheitsabteilung des betroffenen Landratsamtes wird dies künftig im Elternanschreiben tun, wie sie mir in ihrer Stellungnahme versichert hat.

13.1.5 Meldung übertragbarer Krankheiten durch eine Kindertagesstätte an ein Gesundheitsamt

Viele Eltern machen die Erfahrung, dass ihre kleinen Kinder aus dem Kindergarten Kinderkrankheiten wie Masern, Röteln, Windpocken usw. mit nach Hause bringen. Diese Kinder sollen und dürfen zur Vermeidung weiterer Ansteckungen den Kindergarten nicht mehr betreten. In datenschutzrechtlicher Hinsicht stellt sich zum einen die Frage, ob das Gesundheitsamt diesbezüglich Daten erheben darf, zum anderen, ob Erzieherinnen personenbezogene Daten der Kinder an das Gesundheitsamt übermitteln dürfen.

Die Beantwortung der ersten Frage richtet sich nach dem Gesetz zur Verhütung und Bekämpfung von Infektionskrankheiten bei Menschen (Infektionsschutzgesetz - IfSG), das sich nicht nur mit der Bekämpfung meldepflichtiger Krankheiten, sondern auch mit übertragbaren Krankheiten (auch wenn diese nicht der Meldepflicht unterliegen) befasst. Werden Tatsachen festgestellt, die zum Auftreten einer übertragbaren (aber nicht notwendig meldepflichtigen) Krankheit führen können oder ist anzunehmen, dass solche Tatsachen vorliegen, trifft gemäß § 16 Abs. 1 Satz 1 IfSG das Gesundheitsamt die notwendigen Maßnahmen zur Abwehr der dem Einzelnen oder der Allgemeinheit hierdurch drohenden Gefahren. Die Befugnis zur Anordnung der notwendigen Maßnahmen schließt auch die Befugnis zur Erhebung derjenigen personenbezogenen Daten ein, die zur Durchführung der jeweils im Einzelfall gebotenen Maßnahmen erforderlich sind. Ob eine Datenerhebung durch das Gesundheitsamt zur Abwehr der drohenden Gefahren erforderlich ist, ist eine Fragestellung, die in erster Linie medizinisches Fach- und Hintergrundwissen erfordert. Sie ist vom Gesundheitsamt in jedem Einzelfall zu prüfen.

Seitens der Erzieherinnen besteht immer wieder Unsicherheit, ob sie einem Gesundheitsamt im Falle des Auftretens von übertragbaren Krankheiten diese Fälle namentlich melden dürfen. Hier ist darauf hinzuweisen, dass die Kindergartenleitung nach dem Infektionsschutzgesetz (§ 34 Abs. 6 Satz 1 IfSG) nicht nur das Recht, sondern sogar die Pflicht hat, das Gesundheitsamt etwa vom Auftreten von Masern, Windpocken, Keuchhusten, Mumps oder Krätze zu benachrichtigen und dabei krankheits- und personenbezogene Angaben zu machen.

13.2 Krankenhaus

13.2.1 Überwachung eines Aufwachraumes in einem Krankenhaus

Im Berichtszeitraum habe ich aufgrund einer Anfrage geprüft, ob die Überwachung eines Aufwachraumes (in dem sich etwa Patienten nach einer erfolgten ambulanten Operation befinden) durch ärztliches Personal mittels einer Web-Cam (Bild- und Tonüberwachung) aus datenschutzrechtlichen Gründen möglich ist und welche Voraussetzungen hierbei erfüllt sein müssen. Die Ärzte erhofften sich dadurch die Qualität der Betreuung der Patienten zu verbessern.

Datenschutzrechtlich stellen die über das krankenhausinterne Intranet übertragenen Bild- und Tonsignale patientenbezogene Daten im Sinne des Art. 27 Abs. 1 Bayerisches Krankenhausgesetz (BayKrG) dar, da diese Einzelangaben über persönliche oder sachliche Verhältnisse bestimmter oder bestimmbarer Patienten aus dem Bereich der Krankenhäuser enthalten. Für die datenschutzrechtliche Zulässigkeit ist zu unterscheiden, ob die Bild- und Tonsignale (lediglich) zum Zwecke der Beobachtung des Patienten in einen anderen Raum übertragen werden, oder ob darüber hinaus auch eine Aufzeichnung - datenschutzrechtlich gesehen eine Speicherung - der Patientendaten erfolgen soll.

Werden die in einem Aufwachraum mittels einer Web-Cam empfangenen Bild- und Tondaten über das krankenhausinterne Intranet in einen weiteren Raum übertragen, so liegt datenschutzrechtlich eine Erhebung von Patientendaten durch das Krankenhaus vor. Mangels spezieller gesetzlicher Vorschriften ist dies gemäß Art. 27 Abs. 2 Satz 1 BayKrG nur zulässig, soweit dies zur Erfüllung der Aufgaben des Krankenhauses oder im Rahmen des krankenhausärztlichen Behandlungsverhältnisses erforderlich ist oder die betroffene Person eingewilligt hat.

Ohne eine Einwilligungserklärung des Patienten ist eine solche Übertragung patientenbezogener Bild- und Tondaten über das krankenhausinterne Intranet daher nur zulässig, wenn sie im und auf Grund des Behandlungszusammenhanges erforderlich, d.h. aus sachlichen Gründen geboten ist. Ein sachlicher Grund kann in diesem Zusammenhang auch die Verbesserung der Betreuung des Patienten sein.

Unabhängig von der datenschutzrechtlichen Zulässigkeit der Übertragung patientenbezogener Bild- und Tondaten über das krankenhausinterne Intranet muss selbstverständlich durch geeignete technische und organisatorische Maßnahmen jegliche zweckfremde Nutzung der Daten zuverlässig und dauerhaft ausgeschlossen sein. Keinesfalls dürfen die Daten an anderen als den speziell der Beobachtung des Aufwachraumes dienenden Bildschirmarbeitsplätzen abrufbar oder einsehbar sein, ins Internet eingestellt oder sonst veröffentlicht werden; insofern sind auch Vorkehrungen zum Schutz vor missbräuchlicher Benutzung zu treffen.

Sollen - zulässigerweise erhobene - Patientendaten zusätzlich aufgezeichnet - datenschutzrechtlich gesehen also gespeichert - werden, bedarf dieser weitere Datenverarbeitungsvorgang erneuter Prüfung hinsichtlich seiner Zulässigkeit. Auch diese Prüfung hat am Maßstab des Art. 27 Abs. 2 Satz 1 BayKrG zu erfolgen.

In dem der Anfrage offenbar zugrunde liegenden konkreten Einzelfall konnte ich aufgrund der insoweit abstrakt gehaltenen Ausführungen nicht erkennen, warum die Speicherung der entsprechenden Bild- und Tonaufnahmen zur Erfüllung der Aufgaben des Krankenhauses oder im Rahmen des krankenhausärztlichen Behandlungsverhältnisses erforderlich sein sollte. Denn die Überwachung der operierten Patienten in Aufwachräumen dient dem Zweck, bei auftretenden Komplikationen sofort eingreifen zu können. Hierfür reicht aber die bloße Übertragung der entsprechenden Bild- und Tonsignale in einen anderen Raum zunächst vollkommen aus; die Speicherung dieser Signale ist für diesen Zweck grundsätzlich nicht erforderlich.

Schließlich ist zu bedenken, dass im Rahmen der Web-Cam-gestützten Beobachtung eines Aufwachraumes nicht nur Bild- und Tondaten der Patienten, sondern auch der sich dort aufhaltenden Krankenhausmitarbeiter über das krankenhausinterne Intranet übertragen werden. Da es sich bei der Anbringung einer Web-Cam um die Einführung einer technischen Einrichtung handelt, die zumindest geeignet ist, das Verhalten oder die Leistung des Klinikpersonals zu überwachen, besteht hier ein Mitbestimmungsrecht des Personalrats gemäß Art. 75 a Abs. 1 Nr. 1 BayPVG. Der Abschluss einer Dienstvereinbarung gemäß Art. 73 BayPVG ist daher zu empfehlen; ist eine solche zustandegekommen, ist das Klinikpersonal hierauf besonders hinzuweisen.

13.2.2 Getrennte Aufbewahrung von Krankenakten und Sozialdienstakten

An größeren Krankenhäusern, insbesondere Universitätskliniken, wird zum Teil ein eigenständiger Psychosozialer Dienst für die Patienten angeboten. Im Rahmen der Inanspruchnahme dieses Dienstes offenbaren die Betroffenen oftmals sensible Informationen. Um deren Vertraulichkeit zu gewährleisten führt der Psychosoziale Dienst eines Universitätsklinikums eigenständige und von den Krankenakten getrennt aufbewahrte Sozialdienstakten. Die Einrichtung sah sich dazu aus datenschutzrechtlichen Gründen ver-

pflichtet und bat diesbezüglich um meine Einschätzung der Rechtslage. Ich habe der Einrichtung Folgendes mitgeteilt:

Werden im Rahmen eines Psychosozialen Dienstes auch soziale Betreuungsleistungen (z.B. zur Unterstützung bei der Beantragung von Sozialhilfe bzw. Grundsicherung sowie bei der Beantragung von Leistungen aus der Pflegeversicherung) erbracht, sind die hierbei eingesetzten staatlich anerkannten Sozialpädagogen oder staatlich anerkannten Sozialarbeiter nicht Teil des Behandlungsteams und unterliegen daher einer eigenständigen beruflichen Schweigepflicht gemäß § 203 Abs. 1 Nr. 5 StGB.

Wird überdies eine Beratung durch Berufspsychologen mit staatlich anerkannter wissenschaftlicher Abschlussprüfung angeboten, so fallen die diesen anvertrauten oder sonst im Rahmen der Psychosozialen Beratung bekannt gewordenen personenbezogenen Daten gleichfalls unter die Verschwiegenheitspflicht (§ 203 Abs. 1 Nr. 2 StGB).

Dies hat in beiden Fällen zur Folge, dass die betreffenden personenbezogenen Daten nicht unbefugt - auch nicht an behandelnde Ärzte des Klinikums - offenbart werden dürfen. Eine gesetzliche Offenbarungspflicht oder Offenbarungsbefugnis besteht in solchen Fällen grundsätzlich nicht.

Auch ist nicht erkennbar, dass eine erfolgreiche ärztliche Behandlung im Krankenhaus regelmäßig eine Einsichtnahme in Sozialdienstakten erforderte oder dass eine zielführende Psychosoziale Beratung nur nach vorheriger Einsichtnahme in Krankenakten möglich wäre. Ausnahmefälle (insbesondere Notfallsituationen) bleiben allerdings denkbar. Diese stellen jedoch nicht den Regelfall dar, so dass - von Notfallsituation oder Ähnlichem abgesehen - eine Einsichtnahme in den jeweils anderen Vorgang zu unterbleiben hat.

Die Durchsetzung dieser datenschutzrechtlichen Forderung wird in technisch-organisatorischer Hinsicht am besten mit einer vollständigen Trennung von Krankenakten und Sozialdienstakten erreicht. Damit muss freilich eine wirksame und revisionsfähige Zugriffskontrolle einhergehen, da nur so tatsächlich gewährleistet werden kann, dass kein unbefugter Zugriff der jeweils anderen Seite auf die entsprechenden Vorgänge erfolgt (ist).

13.2.3 Akteneinsicht und Patientenkontakt durch Doktoranden

Die Durchführung von medizinischen Forschungsvorhaben ist im Interesse der Weiterentwicklung der Diagnose-, Behandlungs- und Präventionsmöglichkeiten in einem modernen Gesundheitswesen von großer Bedeutung, erfordert aber in nicht wenigen Fällen eine Weitergabe der vom Gesetz besonders geschützten Patientendaten (vgl. § 203 StGB) an Wissenschaftler, die nicht zum Behandlungsteam gehören. In diesen Fällen ist es besonders wichtig, einen Bruch der ärztlichen Schweigepflicht zuverlässig und dauerhaft zu verhindern. Diese Aussage leuchtet zwar unmittelbar ein, ist aber im Alltag der klinischen Praxis schwer umzusetzen, wie der folgende Fall zeigt:

Ein früherer Patient des Klinikums beschwerte sich bei diesem darüber, dass er von einem ihm unbekannten Herrn angerufen und um Beantwortung von Fragen zu seinem Gesundheitszustand gebeten worden sei. Die Recherchen der Klinik ergaben, dass es sich um einen Doktoranden handelte, der beim Klinikum früher als Famulus tätig gewesen war. Zum Schutz der Patientenrechte habe das Klinikum seinerzeit festgelegt, dass die Einsicht in Krankenunterlagen in derartigen Fällen der Genehmigung durch den zuständigen Chefarzt bedarf und der Doktorand sich durch Unterschrift der folgenden Erklärung zu besonderer Verschwiegenheit verpflichten muss:

„Ich verpflichte mich, Daten nur in anonymisierter Form zu erheben und für meine wissenschaftliche Arbeit zu speichern. Ich werde die Daten nur im Rahmen der wissenschaftlichen Arbeit verwenden und nicht an Dritte weiterleiten. Ohne Genehmigung des Klinikums darf ich von dienstlichen Schriftstücken weder Abschriften noch Fotokopien fertigen. Krankenakten, Röntgenbilder oder genehmigte Ablichtungen dürfen nicht aus den Räumen des Klinikums entfernt werden."

Das Klinikum räumte ein, dass der Doktorand im vorliegenden Falle gegen diese Verpflichtung verstoßen habe. In zahlreichen Fällen sei jedoch eine Nachbefragung aufgrund des Forschungsgegenstandes schlichtweg erforderlich, bei anonymisierter Erhebung, Verarbeitung und Nutzung der Patientendaten aber nicht möglich. Daher bat mich das Klinikum anlässlich dieses Vorfalls, die Rechtslage insoweit insgesamt darzulegen. Ich habe dem Klinikum wie folgt geantwortet:

Gemäß Art. 27 Abs. 4 Satz 1 Fall 3 BayKrG dürfen Krankenhausärzte Patientendaten nutzen, soweit dies zu Forschungszwecken im Krankenhaus erforderlich ist.

Folglich darf ein bei einem Klinikum angestellter Arzt zum Zwecke der Anfertigung einer Dissertation Patientendaten nutzen, wenn und soweit die Forschung „im Krankenhaus" stattfindet. Dies bedeutet, dass die Patientendaten das Krankenhaus nicht verlassen dürfen; Grund der Regelung ist die Gewährleistung des Beschlagnahmeschutzes, welchen die Patientenunterlagen gemäß § 97 Abs. 2 Satz 2 StPO

genießen, so lange sie sich „im Gewahrsam einer Krankenanstalt“ befinden.

Voraussetzung ist weiter, dass anhand der Patientendaten nur geforscht werden darf, „soweit“ dies zur Erreichung des Forschungszweckes unbedingt erforderlich ist, der Forschungszweck also mit anonymisierten bzw. jedenfalls pseudonymisierten Daten nicht oder nur mit einem unverhältnismäßigen Aufwand erreicht werden kann.

Forschen Studierende im Krankenhaus und beabsichtigen, zu diesem Zweck Patientendaten nutzen, so ist wie folgt zu unterscheiden:

Forschen sie für Krankenhausärzte, so können diese gemäß Art. 27 Abs. 4 Satz 2 1. Halbsatz BayKrG „andere Personen“ (also auch Studierende) im Krankenhaus mit der Durchführung der entsprechenden Forschungsarbeiten beauftragen.

Forschen die Studierenden hingegen „im eigenen Auftrag“, können jedoch die Krankenhausärzte gemäß Art. 27 Abs. 4 Satz 2 2. Halbsatz BayKrG ihnen die Nutzung von Patientendaten gestatten, wenn dies zur Durchführung des Forschungsvorhabens erforderlich ist und die Patientendaten im Gewahrsam des Krankenhauses verbleiben.

Darüber hinaus sind „diese Personen“ (also unter anderem auch die Studierenden) gemäß Art. 27 Abs. 4 Satz 3 BayKrG zur Verschwiegenheit zu verpflichten, was etwa durch die oben wiedergegebene Erklärung geschehen kann.

Da aber in den zuletzt genannten Fällen die Forschenden nicht zum Behandlungsteam gehören, empfehle ich in diesen Fällen zum effektiven Schutz der Persönlichkeitsrechte der Patienten, eine schriftliche Einwilligung der Patienten vor Beginn des Forschungsprojektes einzuholen.

Dies gilt umso mehr als in vielen Fällen eine Nachbefragung der Patienten erforderlich, bei anonymisierter Datenerhebung aber eben nicht möglich ist. Eine solche Nachbefragung durch eine nicht mehr mit dem Krankenhaus verbundenen Person ist nur noch in Ausnahmefällen von der gesetzlichen Befugnisnorm des Art. 27 Abs. 4 Satz 2 Halbsatz 2 BayKrG gedeckt sein (etwa wenn der Forschende sich zur Durchführung der Nachbefragung in das Krankenhaus begibt, der dort zuständige Krankenhausarzt dem Forschenden die Gestattung im Sinne des Art. 27 Abs. 4 Satz 2 Halbsatz 2 BayKrG erteilt und der Forschende schließlich in den Räumlichkeiten des Krankenhauses die dort aufbewahrten Patientendaten zum Zwecke der Nachbefragung nutzt).

Aus datenschutzrechtlichen, aber auch aus Akzeptanzgründen ist jedenfalls in den Fällen, in denen der Forschungszweck eine Nachbefragung erforderlich macht bzw. machen könnte, dringend die Einholung einer schriftlichen Einwilligungserklärung der Patienten anzuraten.

Eine telefonische Nachbefragung ist durch die genannten datenschutzrechtlichen Vorschriften nicht ausdrücklich ausgeschlossen. Da bei fernmündlichen Nachfragen die Identität des Anrufers unter Umständen nicht ohne weiteres zweifelsfrei geklärt werden kann, sollte jedoch nur in geeigneten Fällen darauf zurückgriffen werden.

Eine solche Einwilligungserklärung in die allgemeinen Vertragsbedingungen des Krankenhauses aufzunehmen, ist datenschutzrechtlich nicht wünschenswert. Denn eine solche Einwilligung wäre in den meisten Fällen gleichsam ins Blaue hinein abgegeben. Demgegenüber verlangt eine rechtswirksame datenschutzrechtliche Einwilligungserklärung eine gezielte, verständliche und umfassende Information und Aufklärung des Betroffenen. Diese sollte mindestens die Angabe der konkreten Studie bzw. des Themas des Forschungsvorhabens bzw. der Promotion, die datenschutzrechtlich verantwortliche Person sowie den ausdrücklichen Hinweis enthalten, dass die Teilnahme an der Studie freiwillig ist und im Falle der Verweigerung oder auch des Widerrufs der Einwilligungserklärung keinerlei Nachteile hieraus entstehen. Diese Anforderungen kann eine Einwilligungserklärung, die in allgemeinen Geschäftsbedingungen enthalten ist, nicht erfüllen.

13.2.4 Übermittlung von Patientendaten für Zwecke der Krankenhausseelsorge (sog. "Pfarrerlisten")

Zu dieser Problematik habe ich bereits im 17. Tätigkeitsbericht (Nr. 3.4.4) ausführlich Stellung genommen. In meinem 18. Tätigkeitsbericht (Nr. 3.3.1) habe ich erneut darauf hingewiesen, dass die Weitergabe von Patientendaten (insbesondere schon die Tatsache des Krankenhausaufenthalts als solche) an die jeweilige Heimatgemeinde bzw. an einen (Laien-) Besuchsdienst der Heimatgemeinde datenschutzrechtlich nur dann zulässig ist, wenn der Patient dieser Datenweitergabe ausdrücklich zugestimmt hat.

Trotzdem erreichte mich im Berichtszeitraum die Eingabe einer betroffenen Bürgerin. Ich habe Ihre Angelegenheit daraufhin datenschutzrechtlich überprüft und das betroffene Krankenhaus auf Folgendes hingewiesen:

Die Weitergabe von patientenbezogenen Daten an die jeweilige Heimatpfarrei bzw. an einen (Laien-) Besuchsdienst der jeweiligen Heimatpfarrei ist datenschutzrechtlich nur zulässig, wenn der Patient dieser Datenweitergabe zuvor ausdrücklich zugestimmt hat.

Aus der Angabe der Konfession im Aufnahmeformular kann nicht geschlossen werden, dass der Patient auch mit dem Besuch eines ehrenamtlich tätigen Besuchsdienstes seiner Heimatpfarrei einverstanden ist. Wie ich bereits in meinem 17. Tätigkeitsbericht (Nr. 3.4.4) ausgeführt habe, kann eine solche Angabe lediglich dahin interpretiert werden, dass der Patient mit der Verständigung eines haupt- oder nebenamtlich am Krankenhaus tätigen Seelsorgers einverstanden ist.

Keine Frage des Datenschutzes ist es, wenn ein Krankenhausseelsorger nach seinem Ermessen Patienten in ihrem Zimmer aufsucht und sich dort als Seelsorger vorstellt. Ein solches Handeln gehört zum rein innerkirchlich zu regelnden Bereich der Krankenhausseelsorge. Eine datenschutzrechtlich relevante Mitwirkung des Krankenhauses erfolgt dabei nicht. Sie läge nur vor, wenn der Krankenhausseelsorger vorher seitens des Krankenhauses Listen von Patienten erhält. In diesem Fall wäre bei der Weitergabe dieser Liste an den Seelsorger nach den oben dargestellten Grundsätzen zu verfahren.

Nach einem längeren Schriftwechsel änderte das Krankenhaus schließlich den Vordruck des Behandlungsvertrages dahingehend, dass nunmehr der Patient ausdrücklich gefragt wird, ob er damit einverstanden ist, dass seine Heimatpfarrei über seinen stationären Aufenthalt informiert wird.

13.2.5 Datenverarbeitung außerhalb eines Krankenhauses

In meinem letzten Tätigkeitsbericht habe ich mich zur Zulässigkeit der verschlüsselten Datenarchivierung von Patientendaten, die in einem Krankenhaus anfallen, bei externen Providern geäußert (dort Nr. 22.2.3.2). Im Berichtszeitraum erreichte mich diesbezüglich eine Vielzahl von Anfragen.

Klarstellend weise ich auf Folgendes hin: Ich halte eine Datenverarbeitung außerhalb eines Krankenhauses nach wie vor nur unter den seinerzeit geschilderten Voraussetzungen für zulässig. Unzulässig wäre es demnach, dass ein privater Unternehmer unverschlüsselt Patientenakten abholt, bei sich digitalisiert und dann extern speichert. Dieses Vorgehen verstieße gegen Art. 27 Abs. 4 Satz 6 Bayerisches Krankenhausgesetz (BayKrG), da die Auftragsdatenverarbeitung von Patientendaten nur in einem anderen Krankenhaus erfolgen darf. Der entscheidende Unterschied zu der im letzten Tätigkeitsberichtsbeitrag geschilderten Fallgestaltung, in dem unter bestimmten Voraussetzungen die Verarbeitung bei einem externen Provider für zulässig erachtet wurde, liegt darin, dass die Verschlüsselung nicht im Krankenhaus erfolgt. Der Dritte erhält somit Kenntnis von den Patientendaten. Eine solche Datenverarbeitung außerhalb eines Krankenhauses wäre unzulässig.

13.3 Medizinische Forschung

13.3.1 Datenschutzrechtliche Begleitung des Aufbaus einer Biomaterialbank - "Biobank der Blutspender"

Die Gewinnung, Aufbewahrung und Verwendung von Blut- und Gewebeproben ist in letzter Zeit zunehmend Gegenstand öffentlicher Erörterungen gewesen. Inzwischen liegen die ersten Ergebnisse der Diskussion hinsichtlich der rechtlichen Rahmenbedingungen und der Verfahrensabläufe bei der Gewinnung, Aufbewahrung und Verwendung von Blut- und Gewebeproben vor. So hat z.B. der nationale Ethikrat in seiner Stellungnahme zum Aufbau und Betrieb von Biobanken (2004) ausgeführt, dass es im Interesse der Patienten und Ärzte, aber auch und gerade der Forschung liege, die künftige Verwendung von Proben für allgemeine Forschungszwecke mittels schriftlicher Einwilligungserklärungen der Betroffenen auf eine klare und verlässliche rechtliche Grundlage zu stellen und die Verfahrensweisen klar zu strukturieren (www.ethikrat.org; Biobanken für die Forschung, Seite 56).

Im Berichtszeitraum plante eine große bayerische Blutspendeeinrichtung die Errichtung einer großen Biomaterialbank („Biobank der Blutspender“). Dabei sollte ein Teil der bei jeder Blutspende anfallenden Blutproben und Daten gesammelt und für medizinische Forschung und Entwicklung verfügbar gemacht werden. Die so gegründete Biomaterialbank könne eine sinnvolle Ergänzung der Proben- und Datensammlungen der Kliniken darstellen (s. Nr. 23.5.3), die oft erst mit der Diagnosestellung beginnen. Durch die Bereitstellung biologischer Proben und verbundener Daten für medizinische Forschung und Entwicklung soll insbesondere ein Beitrag zur Individualisierung von Diagnose und Therapie und zur Verbesserung von Präventionsmaßnahmen geleistet werden.

Ausgewählte Blutspender werden fortlaufend als Teilnehmer in die Biobank der Blutspender aufgenommen und dabei entweder der Fallgruppe oder der Kontrollgruppe zugeordnet. Die Fallgruppe enthält Blutspender, die an einer häufigen chronischen Erkrankung leiden. Die Kontrollgruppe besteht aus gesunden Blutspendern, die der Fallgruppe demographisch vergleichbar sind. Die bereits vorhandenen Proben und Daten beider Gruppen werden systematisch in der „Biobank der Blutspender“ erfasst und pseudonymisiert für medizinische Forschungs- und Entwicklungsprojekte verwendet.

Ich habe im Rahmen meiner Beratungstätigkeit den Aufbau der Biomaterialbank aus datenschutzrechtli-

cher Sicht begleitet. Dabei habe ich zahlreiche Verbesserungen in datenschutzrechtlicher Hinsicht angeregt bzw. gefordert. Folgende Punkte waren zentral:

Eine hinreichende Teilnehmerinformation ist Voraussetzung für eine freiwillige und informierte Einwilligung des Spenders. Sie sollte daher so verständlich wie möglich sein und den nicht vorgebildeten Laien in die Lage versetzen, Aufgabenstellung, Bedeutung und Umfang des in Rede stehenden Projektes in den Grundzügen zu erfassen und auf der Grundlage seiner so gewonnenen Einschätzung freiwillig über seine Teilnahme oder seine Nichtteilnahme an dem Projekt zu entscheiden.

Mindestens zu folgenden Punkten sollte die Teilnehmerinformation klare und verständliche Hinweise enthalten:

- Aufklärung über die für die Proben und Daten dauerhaft verantwortliche Stelle
- Ziel des Projektes
- Dauer sowie Art und Weise der Speicherung/Aufbewahrung der gespeicherten Daten (insbesondere also die Frage nach Anonymisierung bzw. Pseudonymisierung)
- Umfang der gespeicherten Daten
- Kreis der Personen und Stellen, die von den pseudonymisierten Daten bzw. Proben Kenntnis erhalten können
- bei pseudonymer Speicherung/Aufbewahrung: mögliche Anlässe für eine Reidentifizierung der Blutspender
- deutlicher Hinweis auf die Freiwilligkeit der Teilnahme und darauf, dass dem Betroffenen durch eine eventuelle Ablehnung der Einwilligung keinerlei Nachteile entstehen
- Hinweis auf das Recht des Spenders, die Einwilligung für die Zukunft zu widerrufen und eine Herausgabe oder Vernichtung seiner Proben zu verlangen
- Informationen zur eventuellen Unterrichtung des Blutspenders für Forschungsergebnisse
- Hinweis auf grundlegende Datenschutzrechte des Blutspenders (insbesondere Auskunftsanspruch gemäß Art. 10 BayDSG)

Eine Einwilligungserklärung muss vom Blutspender, der an dem Projekt teilnehmen möchte, unterzeichnet werden. Inhaltlich muss die Einwilligungserklärung sich ausdrücklich auf die zuvor ausgehändigte Teilnehmerinformation beziehen und die wesentlichen Punkte erneut aufgreifen (Korrelation zwischen Teilnehmerinformation und Einwilligungserklärung zur Erreichung des „informed consent“).

Erforderlich ist weiter, neben der schriftlichen auch mündliche Information für den Spender anzubieten, wenn dieser eine solche wünscht. Aus diesem Grund muss in der Teilnehmerinformation eine Anlaufstelle für den Teilnehmer (mit vollständiger Postanschrift und Telefon- und Faxdurchwahlnummer) angegeben werden. Auf diese Art und Weise lässt sich der erforderliche „informed consent“ am schnellsten erreichen und am dauerhaftesten aufrechterhalten.

Nach dem vorliegenden Konzept ist beabsichtigt, die Blutproben ganz allgemein zum Zweck der medizinischen Forschung einschließlich genetischer Forschung aufzubewahren und zu verwenden. Aufgrund der besonderen Sensibilität und der vielfältigen Erkenntnismöglichkeiten der genetischen Forschung halte ich es datenschutzrechtlich für erforderlich, die Teilnehmer in der Teilnehmerinformation ausdrücklich darauf hinzuweisen, dass auch der Einsatz der erhobenen personenbezogenen Daten zum Zwecke der genetischen Forschung beabsichtigt ist. Außerdem war das Vorgehen sowie die Erkenntnismöglichkeiten der genetischen Forschung allgemein verständlich darzulegen. Die im Rahmen des Projektes erhobenen Daten zum Zwecke der genetischen Forschung dürfen auf keinen Fall personenbezogen eingesetzt werden.

Zwar können Spender in die Aufbewahrung und Nutzung ihrer Daten und Proben für unbestimmte Dauer einwilligen. Denn die Aufbewahrungsdauer zwingend begrenzende Fristsetzungen würden den wissenschaftlichen Wert von Biobanken erheblich einschränken. Allerdings ist es aus datenschutzrechtlichen Gründen erforderlich, auf den Umstand der zeitlich unbegrenzten Aufbewahrung und Nutzung von Proben und Daten in der Teilnehmerinformation und der Einwilligungserklärung klar und unmissverständlich hinzuweisen.

Wegen der sehr hohen Sensitivität des Datenbestandes bedarf eine Biobank angemessener technisch-organisatorischer Datensicherungsmaßnahmen. Ein wichtiger Aspekt in diesem Zusammenhang ist zunächst die Unabhängigkeit der Biobank von den sonstigen Aufgaben des Blutspendedienstes. Eine personelle und räumliche Trennung der Datenbank-Systeme und Probenlagerung soll erfolgen. Besonderes Augenmerk ist auf die Ausgestaltung der Weisungsbefugnisse zu richten.

Von zentraler Bedeutung ist der Verteilungsgrad der Datenbestände der Biobank-Datenbank. Zur ange-

messenen Wahrung der Belange des Persönlichkeits- und Datenschutzes ist es angesichts der Größe, Zweckbestimmung und Bedeutung der Biomaterialbank nicht akzeptabel, dass alle Daten in einer Datenbank abgelegt werden. Dies ist insbesondere vor dem Hintergrund des Risikos einer unbefugten Depseudonymisierung zu sehen. Denn bei der Ablage aller Daten in einer Datenbank würde u.U. die Kompromittierung der einzelnen Person/Stelle, z.B. des Administrators ausreichen, um Zugriff auf sämtliche Daten der Teilnehmer zu erhalten.

Es ist daher eine physische und organisatorische Trennung zumindest von Personendaten und zur Forschung verwendeten medizinischen Daten erforderlich. Des Weiteren sollte der Pseudonymisierungsvorgang (Ersatz der Personendaten durch ein Pseudonym) weder vom Blutspendedienst noch von den Administratoren der Biobank durchgeführt werden, da die Zuordnung von Pseudonym zu Personen-Daten einem besonderen Schutzbedarf unterliegt. Häufig geeignet ist beispielsweise eine zentrale Patientenliste unter gesonderter Hoheit entsprechend dem generischen Datenschutzkonzept für Biomaterialbanken. Ziel der Verteilung von Datenbeständen muss sein, dass mindestens zwei Stellen kompromittiert sein müssen, bevor eine unbefugte Reidentifizierung der Spender möglich ist.

Beim Export der Daten aus der Datenbank des Blutspendedienstes in der Biobank-Datenbank muss eine wirksame Pseudonymisierung erfolgen. Nähere Ausführungen sind der entsprechenden Orientierungshilfe zu entnehmen: http://www.datenschutz-bayern.de/technik/orient/ohilfe_psn_03.html.

Die üblichen Berechtigungen und Zugriffsmöglichkeiten müssen gemäß den Aufgaben an die Benutzer vergeben werden. Weiter müssen bei einem Export von Daten der Proben an Forscher jeweils eigene Pseudonyme verwendet werden, die nicht Ordnungskriterium der Datenbank sind.

Unter den angesprochenen Voraussetzungen hatte ich gegen den Aufbau einer Biomaterialbank keine datenschutzrechtlichen Bedenken.

13.3.2 Verwendung von Initialen bei medizinischen Forschungsvorhaben

Die wesentlichen Anforderungen an die datenschutzgerechte Ausgestaltung von Forschungsvorhaben habe ich bereits mehrfach in meinen früheren Tätigkeitsberichten dargelegt, etwa im 21. Tätigkeitsbericht (Nr. 20.2.2) und im 19. Tätigkeitsbericht (Nr. 2.3.1).

Im Berichtszeitraum hat mich ein Universitätsklinikum gebeten, ein Forschungsprojekt im Rahmen der bundesweit stattfindenden ESPED-Erhebung in datenschutzrechtlicher Hinsicht zu überprüfen. ESPED (Erfassungssystem seltener pädiatrischer Erkrankungen in Deutschland) ist ein seit längerem etabliertes Erfassungssystem, an dem zahlreiche Universitätskliniken in ganz Deutschland teilnehmen. ESPED teilt der Universitätsklinik, die ein (meist epidemiologisches) Forschungsvorhaben in Bezug auf eine bestimmte (zuvor der ESPED-Zentrale gemeldete) Krankheit durchführt, mit, ob und in welcher Klinik in Deutschland ein Fall dieser Krankheit gemeldet wurde. Daraufhin versendet die forschende Universitätsklinik an die gemeldeten Kliniken Fragebögen. Durch die in dem Fragebogen enthaltenen Informationen wird der Fall hinsichtlich der Schwere des Krankheitsbildes und der etwaiger Komplikationen charakterisiert, er wird freiwillig und ohne Gegenleistung durch Klinikärzte neben deren klinischer Tätigkeit ausgefüllt. Auf dem Fragebogen war eine Klinik-Nummer und eine von der ESPED-Zentrale vergebene fortlaufende Fallnummer angegeben.

Als zusätzlichen Identifikationsmerker haben die Forscher die Initialen, das Geschlecht, der Geburtsmonat und das Geburtsjahr, die ersten drei Ziffern der Postleitzahl des Wohnortes sowie die Nationalität erfasst. Diese Identifikationsmerker seien notwendig, um Doppelmeldungen zu identifizieren und Nachfragen zu ermöglichen. Aufgrund der Erfahrungen mit anderen ESPED-Studien und aufgrund der Unvollständigkeit von Angaben (bei Freiwilligkeit der Teilnahme) sei dies immer wieder erforderlich, um die Daten sinnvoll nutzen zu können.

Nach Ansicht der Forscher ist damit eine ausreichende Pseudonymisierung (vgl. § 3 Abs. 6 a BDSG) erreicht.

Ich habe daraufhin dem Klinikum mitgeteilt, dass die Erhebung, Verarbeitung und Nutzung personenbezogener Daten nur zulässig sind, wenn eine Rechtsvorschrift sie erlaubt oder anordnet oder der Betroffene eingewilligt hat (Art. 15 Abs. 1 BayDSG).Da im vorliegenden Fall die Forscher die Einwilligung der Betroffenen nicht eingeholt haben, setzt die Durchführung des Forschungsvorhabens voraus, dass die in dem Fragebogen erhobenen medizinischen Daten als anonymisiert in datenschutzrechtlichem Sinne (Art. 4 Abs. 8 BayDSG), also als nicht personenbezogen und nicht personenbeziehbar angesehen werden können. Nach meiner Auffassung war dies nicht der Fall, da die Versendung der Initialen, zusammen mit der Angabe des Geschlechtes, des Geburtsmonats und des Geburtsjahres, den ersten drei Ziffern der Postzeitzahl sowie der Angabe der Nationalität - ggf. unter Einsatz von Zusatzwissen - eine Reidentifizierungsmöglichkeit der betroffenen Personen nicht zuverlässig ausgeschlossen werden konnte. Hierbei war ebenfalls zu berücksichtigen, dass es sich vorliegend um sensible medizinische Daten handelte. Ich

habe daher darauf hingewiesen, dass im Rahmen anderer Forschungsvorhaben - insbesondere auch von ESPED-Studien - der Forschungszweck durch den Einsatz von wesentlich datenschutzfreundlicheren Identifikationsmerkern möglich war. So wurde z.B. in einer ESPED-Studie statt der Initialen lediglich der jeweils zweite Buchstabe des Vor- und Nachnamens, das Geschlecht sowie Geburtsmonat und Geburtsjahr erhoben. Im Rahmen einer weiteren ESPED-Studie wurde sogar auf die Erhebung jeglicher Initialen verzichtet; dort wurde an Patientendaten lediglich die drei ersten Ziffern des Wohnortes, das Geschlecht sowie Geburtsmonat und Geburtsjahr erhoben. Vor diesem Hintergrund habe ich um Mitteilung gebeten, warum der Zweck des Forschungsvorhabens die Erhebung des von den Forschern vorgesehenen Datensatzes, insbesondere der Initialen zwingend erfordert.

Daraufhin erklärte sich das Klinikum bereit, auf Initialen sowie Postleitzahlangaben zu verzichten. Es wurden also lediglich Geburtsmonat und -jahr, Geschlecht und Nationalität erhoben. Die Erhebung der Nationalität erfolgt nunmehr ausschließlich in dem - zum Teil neu zu bildenden - Kategorien „deutsch“, „türkisch“ und „andere“ (letztere ohne Freitextfeld).

Ein in der Struktur identisches Problem stellte sich im Zusammenhang mit einer Studie des Robert-Koch-Instituts. Dieses plante eine bundesweite epidemiologische Studie zur Klärung eines möglichen Zusammenhangs zwischen bestimmten Impfungen und plötzlichen Todesfällen bei Kindern im 2. bis 24. Lebensmonat. Für den epidemiologischen Studienteil sollten alle leichenschauärztlichen Angaben sowie Geburts- und Todesdatum durch die öffentlichen Gesundheitsämter an die Studienleitung im Robert-Koch-Institut übermittelt werden. Die personenidentifizierenden Angaben (Name, Anschrift) sollten bis auf die Initialen geschwärzt werden.

Entsprechend meinen obigen Ausführungen habe ich um Mitteilung gebeten, ob nicht auf diese allenfalls pseudonymisierte Übermittlung des Inhalts der Todesbescheinigungen verzichtet werden kann. Das Robert-Koch-Institut hat mir daraufhin mitgeteilt, dass, um die Sicherheit der pseudonymisierten Übermittlung des Inhalts der Todesbescheinigungen zu erhöhen, auf die ursprünglich geplante Übermittlung der Initialen des verstorbenen Kindes auf dem Todesschein verzichtet wird.

13.4 Selbstverwaltungsangelegenheiten

13.4.1 Elektronisches Fortbildungskonto für Ärzte

Die Bayerische Landesärztekammer hat mich über die Fortbildungszertifizierung der Ärztekammer informiert; ich wurde daraufhin sowohl in juristischer als auch in technisch-organisatorischer Sicht beratend tätig.

Vertragsärztinnen und -ärzte müssen gegenüber ihrer Kassenärztlichen Vereinigung den Nachweis kontinuierlicher ärztlicher Fortbildung erbringen. Um den Ärztinnen und Ärzten den Nachweis der Fortbildung zu erleichtern, bietet die Bayerische Landesärztekammer die Möglichkeit eines elektronischen Fortbildungskontos. Aus datenschutzrechtlicher Sicht habe ich gegen dieses Angebot keine Bedenken erhoben. Auf Landesebene ist in Bayern nämlich nach Art. 2 Abs. 1 Heilberufe-Kammergesetz der ärztlichen Berufsvertretung die Aufgabe zu gewiesen, die ärztliche Fortbildung zu fördern und die Erfüllung der ärztlichen Berufspflichten zu überwachen. Im Rahmen dieser Aufgabenzuweisung kann die Bayerische Landesärztekammer zur Erfüllung der gesetzlichen Fortbildungspflicht der Ärzte mittels eines elektronischen Fortbildungspunktekontos grundsätzlich Daten erheben und speichern.

Allerdings habe ich die Bayerische Landesärztekammer darauf aufmerksam gemacht, dass weder aus dem Anschreiben an die Ärzte noch aus den Informationsblättern explizit hervorgeht, dass die Teilnahme am elektronischen Punktekonto freiwillig ist. Im vorliegenden Fall werden nämlich personenbezogene Daten beim Betroffenen mit seiner Kenntnis erhoben, so dass zum einen der Erhebungszweck ihm gegenüber anzugeben ist. Zum anderen ist der Betroffene auf die Freiwilligkeit seiner Angaben hinzuweisen. Denn eine Pflicht, die Daten zu liefern besteht nicht gegenüber der Bayerischen Landesärztekammer, sondern gegenüber der Kassenärztlichen Vereinigung. Die Freiwilligkeit umfasst dabei auch die Wahl des Übermittlungswegs.

Zur Verwirklichung des elektronischen Fortbildungskontos soll eine einheitliche elektronische Fortbildungsnummer (EFN) generiert werden. Die EFN dient ausschließlich der Nutzung im Rahmen des Fortbildungspunktekontos, wodurch eine Verknüpfung verschiedener Datenbestände über den Arzt erschwert wird. Der Veranstalter einer Fortbildung benötigt für die Teilnahmemeldungen an die Ärztekammern nur die EFN, nicht jedoch weitere Nummern des Arztes wie z.B. die Bundeseinheitliche Ärztenummer (BAN). Für die Kommunikation mit der Ärztekammer spielt die EFN nur im Zusammenhang mit der Fortbildung eine Rolle, für andere Bereiche muss sie nicht vorgelegt werden. Ein wichtiger Grund für die Einführung einer gesonderten EFN war, die Nutzung der BAN für eine Vielzahl von Zwecken und somit die Einführung einer einzigen Nummer für die Verwaltung diverser Informationen über den Arzt zu vermeiden.

Ich habe es weiter für sinnvoll erachtet, in einem Informationsblatt einen Überblick darüber zu geben, wo sich welche Daten über den Arzt befinden und was an wen verschickt wird. Dabei sollte dargestellt werden, dass über den Elektronischen Informationsverteiler (EIV) keine personenbezogenen Daten des Arztes, wie Adresse, Name, BAN oder ähnliches übertragen werden, sondern nur seine EFN und die Veranstaltungsnummer/Punktemeldung. Eine Zuordnung zum Arzt geschieht erst in der zuständigen Ärztekammer im dortigen Punktekonto.

Zudem sollte auch noch erwähnt werden, dass die Ärzte auch im elektronischen Verfahren weiterhin vom Veranstalter Papierbescheinigungen über die Teilnahme erhalten, die im Zweifelsfall als Nachweis gegenüber der Ärztekammer gelten (z.B. bei Problemen mit dem elektronischen Punktekonto).

Unter den angesprochenen Bedingungen hatte ich keine Einwände gegen den Betrieb eines elektronischen Fortbildungskontos durch die Bayerische Landesärztekammer.

14 Soziales

14.1 Krankenkassen

14.1.1 Einführung einer elektronischen Gesundheitskarte

Bereits in meinem 21. Tätigkeitsbericht habe ich das Projekt der elektronischen Gesundheitskarte vorgestellt. Die elektronische Gesundheitskarte wirft eine Vielzahl von datenschutzbezogenen Fragen auf. Auch wenn die grundlegenden Richtungsentscheidungen, die auch Vorstellungen des Datenschutzes berücksichtigten, bereits gefallen sind, so muss doch darauf geachtet werden, dass die Detailumsetzung des Projekts der elektronischen Gesundheitskarte möglichst datenschutzfreundlich erfolgt.

Hinsichtlich der Umsetzung des Projekts der elektronischen Gesundheitskarte sind Entwicklungen auf Landes- und auf Bundesebene zu beobachten. Auf Bundesebene wurde eine Gesellschaft namens „Gematik“ gegründet, die die Einführungsstrategien für die elektronische Gesundheitskarte entwickeln soll. Die Gematik baut auf den Arbeiten des im 21. Tätigkeitsbericht erwähnten „Bit4 Health“ Gremiums sowie auf Ergebnissen eines Forschungsprojekts der Fraunhofer Gesellschaft auf. Auf Bundesebene ist der Datenschutz in verschiedenen Gremien der Gematik eingebunden. Diese Ebene ist deshalb besonders wichtig, weil dort die wesentlichen Architekturentscheidungen zur elektronischen Gesundheitskarte fallen werden. Der Bayerische Landesbeauftragte für den Datenschutz nahm an ersten Gesprächen mit Vertretern der Gematik teil.

Die 69. Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat eine Entschließung zur Einführung der elektronischen Gesundheitskarte gefasst (siehe Anlage Nr. 2). Dabei wurde u.a. gefordert, dass die über die Karte erfolgende Datenverarbeitung nach den gesetzlichen Vorgaben weitgehend aufgrund der Einwilligung der Versicherten erfolgen muss. Die Versicherten müssen darüber informiert werden, welche Datenverarbeitungsprozesse mit der Karte durchgeführt werden können, wer hierfür verantwortlich ist und welche Bestimmungsmöglichkeiten sie dabei haben.

Den rechtlichen Rahmen für die Testung gibt die Verordnung über Testmaßnahmen für die Einführung der elektronischen Gesundheitskarte vor. Ich habe mich dafür eingesetzt, dass bereits Einwilligung, Dokumentation auf der Karte, Widerruflichkeit und Beschränkung auf einzelne Anwendungen sowie die gesetzlich geforderten technischen Vorkehrungen zur Zugriffsautorisierung durch den Versicherten zwingende Testgegenstände sein sollen. Die Testung sollte möglichst umfassend erfolgen. Denn nur dadurch kann verhindert werden, dass durch Vorentscheidungen in der Testphase die elektronische Gesundheitskarte einseitig auf datenschutzunfreundliche Konzepte festgelegt wird.

Da die elektronische Gesundheitskarte zunächst auf Länderebene in so genannten Modellprojekten erprobt werden soll, wird es darauf ankommen, die datenschutzrechtlichen Belange bereits bei der Durchführung der Modellprojekte einfließen zu lassen. In Bayern wurde vom Staatsministerium für Arbeit und Soziales, Familie und Frauen und vom BTI (Bayerische Telematikinitiative für das Gesundheitswesen), einer Insitution der Selbstverwaltung, die Modellregion Ingolstadt vorgesehen. Weiter wurde am 01.06.2005 der Verein „Baymatik e.V. Bayerische Modellregion Telematik“ gegründet. Dieser Verein soll insbesondere die Telematik-Infrastruktur zur Einführung der elektronischen Gesundheitskarte testen. Nach seiner Satzung hat der Verein einen beratenden Beirat. In diesem Beirat ist auch der Bayerische Landesbeauftragte für den Datenschutz vertreten. Auf dessen Sitzungen habe und werde ich die datenschutzrechtlichen Belange im Zusammenhang mit der Einführung der elektronischen Gesundheitskarte vertreten.

In Bayern fand im März 2006 weiter ein Workshop statt. Daran haben u.a. Datenschutzbeauftragte der beteiligten gesetzlichen Krankenkassen und der Bayerische Landesbeauftragte für den Datenschutz teilgenommen. In erster Linie war der Bayerische Landesbeauftragte für den Datenschutz hier beratend tätig. Insbesondere galt es, die Teilnahme- und Einwilligungserklärungen für die Versicherten, die an dem Modellprojekt in Ingolstadt teilnehmen wollen, datenschutzkonform auszugestalten. Die Teilnehmer

sollen über die wesentlichen Testszenarien aufgeklärt werden. Erhebungs-, Verarbeitungs- und Nutzungsspektrum der elektronischen Gesundheitskarte sollen anhand abstrakter Fallgestaltungen dargelegt werden. Weiter habe ich darauf hingewiesen, dass die Daten bei einem Widerruf des Betroffenen gelöscht werden müssen. Im Übrigen wurde auch deutlich, dass die weitere Entwicklung des bayerischen Modellprojekts in erster Linie von den Vorgaben der Gematik abhängt. Diesbezüglich dauert die Entscheidungsfindung auf Bundesebene noch an.

14.1.2 Feststellung der Belastungsgrenze durch Krankenkassen

Die Belastungsgrenze für Zuzahlungen in der gesetzlichen Krankenversicherung beträgt gemäß § 62 Sozialgesetzbuch - Fünftes Buch - (SGB V) 2 % der jährlichen Bruttoeinnahmen zum Lebensunterhalt; für chronisch Kranke, die wegen derselben schwerwiegenden Krankheit in Dauerbehandlung sind, beträgt sie 1 % der jährlichen Bruttoeinnahmen zum Lebensunterhalt. Das Nähere zur Definition einer schwerwiegenden chronischen Erkrankung bestimmt der Gemeinsame Bundesausschuss in den von ihm erlassenen Richtlinien. Der Gemeinsame Bundesausschuss wird u.a. von den Kassenärztlichen Bundesvereinigungen und den Bundesverbänden der Krankenkassen gebildet.

Im Zusammenhang mit der Ermittlung der Belastungsgrenze bzw. der Einordnung als chronisch Kranker, der wegen derselben schwerwiegenden Krankheit in Dauerbehandlung ist, habe ich mich mit hierauf bezogenen Erhebungsbögen einer Krankenkasse befasst. Es hatten sich auch einige Versicherte mit diesbezüglichen Fragen bzw. Beschwerden an mich gewandt.

So hat beispielsweise der Antrag auf Befreiung von Zuzahlungen über der Belastungsgrenze einer Krankenkasse eine Einwilligungs- bzw. Schweigepflichtentbindungserklärung enthalten. Dieses Antragsformular wurde allen Antragstellern zur Unterschrift ausgehändigt. Die enthaltene Einwilligungs- bzw. Schweigepflichtentbindungserklärung konnte jedoch allenfalls bei bestimmten Fallgruppen der Antragsteller überhaupt relevant sein. In den Richtlinien des Gemeinsamen Bundesausschusses sind für die Feststellung einer schwerwiegenden chronischen Krankheit unterschiedliche Fallgruppen gebildet.

Das zunächst von der Krankenkasse vorgebrachte Argument, die entsprechenden Erklärungen würden schließlich tatsächlich nur bei der relevanten Fallgruppe in entsprechenden Fällen genutzt, überzeugt nicht. Denn es ist schon nicht zulässig, derartige Erklärungen von allen Antragstellern zu verlangen, wenn diese allenfalls für eine bestimmte Fallgruppe innerhalb der Antragsteller Relevanz haben; dies gilt um so mehr, wenn die Erklärungen unter Hinweis auf eine entsprechende Mitwirkungspflicht und dem Hinweis auf Nachteile bei Nichtabgabe der Erklärung verlangt werden. Weiterhin ist an die Antragsteller aus der Fallgruppe, für die derartige Erklärungen relevant sind, zudem noch jeweils ein gesondertes Formular u.a. eben mit einer entsprechenden Einwilligungs- bzw. Schweigepflichtentbindungserklärung ausgegeben worden, so dass die Erklärung auf dem allgemeinen Formular unter diesem Gesichtspunkt zudem auch schlicht überflüssig war. Die Krankenkasse hat das Formular nach meiner Intervention nunmehr entsprechend abgeändert.

14.1.3 Akteneinsicht bzw. Auskunft

Immer wieder erreichen mich Eingaben von Bürgerinnen und Bürgern, die ihre Rechte im Zusammenhang mit einer Akteneinsicht oder einer Auskunft der zu ihrer Person gespeicherten Sozialdaten beeinträchtigt sehen. Im Anwendungsbereich des Sozialgesetzbuchs - Zehntes Buch - (SGB X) gibt es insoweit zwei wesentliche Vorschriften: Für die Akteneinsicht ist die Regelung des § 25 SGB X maßgeblich, für eine Auskunft über die zur eigenen Person gespeicherten Sozialdaten die des § 83 SGB X. Es hat sich in der Praxis herausgestellt, dass sowohl seitens handelnder (oder eben nicht handelnder) Behörden als auch seitens anfragender Bürgerinnen und Bürger die entsprechenden Voraussetzungen bzw. Rechtsfolgen nicht immer zutreffend eingeordnet werden. Beispielsweise setzt der Anspruch auf Akteneinsicht nach § 25 SGB X ein Verwaltungsverfahren im Sinne des § 8 SGB X voraus.

Aber auch außerhalb eines solchen Verwaltungsverfahrens haben Bürgerinnen und Bürger Möglichkeiten, über die zu ihrer Person gespeicherten Daten Auskunft zu erhalten, etwa gemäß den Regelungen des § 83 SGB X. Bei einer solchen Auskunftserteilung unter den in § 83 SGB X aufgestellten Voraussetzungen bestimmt aber die verantwortliche speichernde Stelle das Verfahren, insbesondere die Form der Auskunftserteilung, nach pflichtgemäßem Ermessen. Eine solche Auskunft kann durch Gewährung von Akteinsicht erfolgen, aber auch auf andere Weise. Es besteht hier beispielsweise auch kein grundsätzlicher Anspruch auf Übersendung von Ablichtungen aus der Akte. Behördlicherseits genügt den Anforderungen an eine Auskunft nach § 83 SGB X jedoch keinesfalls die Mitteilung, man habe nur Daten entsprechend den datenschutzrechtlichen Vorschriften gespeichert. Ebenso wenig kann es angehen, eine Auskunft grundlegend zu verweigern, weil die bzw. der Betroffene bereits zuvor verschiedene Eingaben und Anträge gestellt hat und die Behörde erwartet, bei Gewährung der Auskunft noch mehr derartige Anträge zu erhalten. Den Betroffenen soll

mittels eines Auskunftsanspruchs gerade ermöglicht werden, Kenntnis der zu ihrer Person gespeicherten Sozialdaten zu erhalten, auch um die Richtigkeit dieser Sozialdaten aus ihrer Sicht überprüfen und beispielsweise einen Antrag auf Berichtigung stellen zu können.

14.1.4 Mitgliederwerbung durch gesetzliche Krankenkassen

Immer wieder wird der Ruf nach mehr Wettbewerb zwischen den gesetzlichen Krankenkassen laut. Diese versuchen demgemäß auch oftmals, neue Mitglieder zu werben bzw. an die personenbezogenen Daten potenzieller Neumitglieder zu gelangen. Auch bei der Mitgliedergewinnung muss jedoch auf die Einhaltung der datenschutzrechtlichen Vorschriften geachtet werden. Anlässlich einer Schuleinschreibung hatte eine Krankenkasse einen Informationsstand zum Thema „Gesunde Ernährung von Schulkindern/Gesundes Pausenbrot“ aufgebaut. Dort wurden auch Handzettel mit einem Malspiel mit u.a. dem Aufdruck „Mach mit! Gewinn was!“ ausgegeben. Am Ende des Handzettels waren Felder für den Eintrag folgender Daten vorgesehen: „Dein Name, Dein Geburtsdatum, Name Deiner Eltern und Geburtsdatum, Adresse, Krankenkasse“.

Zumindest in Einzelfällen wurden solche Handzettel nicht an Eltern, sondern auch an ältere Geschwister der ABC-Schützen ausgegeben bzw. von diesen selbstständig an sich genommen.

Ich habe der Krankenkasse mitgeteilt, etwa die Abfrage des Geburtsdatums und der Krankenkasse der Eltern spräche dafür, dass Daten zumindest nicht ausschließlich für ein eventuelles Gewinnspiel genutzt würden. Zudem war weder eine (schriftliche) Einwilligung der Eltern in die Erhebung und Speicherung ihrer Daten ersichtlich noch eine entsprechende Information zum Erhebungs- und Speicherungszweck. Die Krankenkasse hat daraufhin mitgeteilt, dass die personenbezogenen Daten aus dieser Aktion ausschließlich für die Verlosungsaktion verwendet würden, eine weitere Speicherung und Verarbeitung der gewonnenen Daten würde nicht erfolgen. Dieser bedauerliche, fehlerhafte Einzelvorgang - so die Krankenkasse - sei selbstverständlich Anlass, auf die dringende Beachtung der datenschutzrechtlichen Kriterien bei derartigen Vorhaben intern hinzuweisen.

14.2 Jugendamt

14.2.1 Teilnahme von Mitarbeitern der wirtschaftlichen Jugendhilfe an einer Fachteamsitzung im Jugendamt

Immer wieder tauchen datenschutzrechtliche Fragen im Zusammenhang mit der Einschaltung von Fachteams bei der Gewährung von Jugendhilfe auf. Erster Ansprechpartner für junge Menschen oder Eltern, die Jugendhilfe in Anspruch nehmen wollen, ist meistens die zuständige sozialpädagogische Fachkraft beim Jugendamt. In vielen Jugendämtern werden Maßnahmen der Hilfe zur Erziehung, § 27 Sozialgesetzbuch - Achtes Buch - (SGB VIII), in einem so genannten Fachteam erörtert und entschieden. Dabei wird der Fall vom zuständigen Sozialpädagogen vorbereitet und mit den erforderlichen Unterlagen den anderen Teilnehmern der Fachteamsitzung zugeleitet. Ein Fachteam kann etwa bestehen aus dem Leiter des Jugendamts, dem fallverantwortlichen Sozialpädagogen, der Leitung des sozialpädagogischen Dienstes und Mitarbeitern der wirtschaftlichen Jugendhilfe.

In der Sache hängt die Zulässigkeit der Nutzung der personenbezogenen Daten in einer Fachteamsitzung davon ab, ob sie für die Aufgabenerfüllung des Jugendamts erforderlich ist. Für die Beurteilung ist auch wichtig, dass die Mitarbeiter der wirtschaftlichen Jugendhilfe den Bescheid zu erlassen und diesen ggf. auch gegenüber der Widerspruchsbehörde und gegenüber einem Gericht zu vertreten haben. Dies bedingt notwendigerweise eine ganz andere Intensität der Datenverarbeitung/Datennutzung als dies etwa bei einer Kreisrechnungsprüfung der Fall ist.

Ob die Nutzung erforderlich ist, dürfte eine Frage des Einzelfalls sein. In vielen Fällen dürfte es ausreichen, in der Fachteamsitzung entsprechende Fälle ohne Personenbezug zu erörtern. Auch die Belange der wirtschaftlichen Jugendhilfe können dann bereits frühzeitig in die Fachteamsitzung eingebracht werden. Soweit aber in der Fachteamsitzung eine personenbezogene Erörterung des Falles nötig ist, können erforderlichenfalls auch Mitarbeiter der wirtschaftlichen Jugendhilfe von personenbezogenen Daten Kenntnis erlangen. Insofern ist dem Grunde nach eine Teilnahme von Mitarbeitern der wirtschaftlichen Jugendhilfe an Fachteamsitzungen möglich. Zu beachten ist aber immer, dass besondere Geheimhaltungsvorschriften wie etwa § 65 SGB VIII gewahrt werden müssen.

14.3 Unfallversicherungsfragen

14.3.1 Gesetzliche Unfallversicherung und Krisenintervention

Gemäß einem geflügelten Wort ist Vorsorge besser als Nachsorge. Dies gilt auch für den Bereich des Datenschutzes. Dementsprechend bin ich nicht nur im Wege nachträglicher Kontrollen tätig, sondern auch durch Beratungen bereits im Vorfeld von Vorhaben. So ist etwa ein gesetzlicher Unfallversicherungsträger mit der Bitte um Beratung bezüglich der datenschutzrechtlichen Aspekte eines Vertrages zwischen ihm und dem Freistaat Bayern an mich herangetreten. Das Bayerische Staatsministerium für Unterricht und Kultus hat nach den Ereignissen von Erfurt und Freising ein Krisenineterventions- und -bewältigungsteam bayerischer Schulpsychologen (KIBBS-Team) bereitgestellt und koordiniert dessen Einsätze. In einem Vertrag sollte der Einsatz des KIBBS-Teams auch in Zusammenarbeit mit der gesetzlichen Unfallversicherung geregelt werden. Das KIBBS-Team kann etwa in der psychosozialen Notfallversorgung in Krisensituationen an Schulen tätig werden. Durch meine frühzeitige Beteiligung an dem Vorhaben konnte ich maßgeblichen Einfluss auf die - im Zusammenhang mit Einsätzen des KIBBS-Teams und der Aufgabenstellung der Unfallversicherung - verwendeten Einwilligungserklärungen nehmen, die in die Anlage des Vertrags aufgenommen worden sind.

Dabei waren verschiedene Aspekte anzusprechen. Für diese Einwilligungserklärungen gilt im Besonderen, dass die Betroffenen wissen müssen, in welche Datenumgänge sie ggf. einwilligen, wenn sie die Erklärung unterschreiben. Dabei war vor allem auf eine größtmögliche datenschutzrechtliche Transparenz der Einwilligungserklärungen hinzuwirken. Dies konnte beispielsweise durch die textliche Gestaltung der Erklärungen, durch die Erläuterung, welche Stellen sich hinter verwendeten Abkürzungen verbergen und eine deutlichere Trennung von Einverständniserklärungen hinsichtlich unterschiedlicher Datenumgänge bewirkt werden. Letzteres hat den Vorteil, dass Betroffene - die sich gerade in Einsatzfällen des KIBBS-Teams oftmals in einer Ausnahmesituation befinden - ihre Einwilligung einfacher auf bestimmte Datenflüsse beschränken können. So kann etwa eine Einwilligung auf erforderliche Datenumgänge im Zusammenhang mit der Unfallversicherung gesondert abgegeben werden. Weiterhin wurde ein Merkblatt zum Datenschutz für die KIBBS-Mitarbeiter aufgelegt. Dies begrüße ich grundsätzlich. Auch hier konnte ich - da mir das Merkblatt frühzeitig vorgelegt wurde - noch maßgebliche Hinweise geben, die auch entsprechend berücksichtigt wurden.

Der an mich herangetretene Unfallversicherungsträger war ersichtlich darauf bedacht, alle von hier geltend gemachten datenschutzrechtlichen Aspekte zu berücksichtigen. Der Vertrag ist inzwischen auch abgeschlossen. Es entstand damit eine erfolgreiche Abklärung datenschutzrechtlicher Fragestellungen bereits im Vorfeld des Projekts.

14.3.2 Gestaltung von Erhebungsbögen in der gesetzlichen Unfallversicherung

Einem Bürger wurde von einem gesetzlichen Unfallversicherungsträger ein Fragebogen zugesandt, in dem er über seine persönlichen Verhältnisse, u.a. zum Güterstand, Auskunft geben sollte. Der Angeschriebene war jedoch der Auffassung, dass manche der enthaltenen Fragen das erforderliche Maß für eine Sachbearbeitung übersteigen bzw. ganz einfach nicht nötig sind.

Nach meinem Herantreten an den Unfallversicherungsträger hat dieser mitgeteilt, dass tatsächlich Fragen enthalten sind, die nur für bestimmte Fallgruppen relevant sind. Der anfragende Bürger fiel offensichtlich nicht in diese Fallgruppe. Der Sozialversicherungsträger hat weiterhin mitgeteilt, dass eine entsprechende Neugestaltung des Fragebogens erfolgen würde, so dass ich von einer Beanstandung abgesehen habe.

Die Verwendung von Antragsformularen, Frage- bzw. Erhebungsbögen können im Sinne einer effizienten Verwaltung und damit grundsätzlich auch im Sinne aller Verfahrensbeteiligten sinnvoll sein. Maßgeblich bleibt jedoch die datenschutzrechtliche Faustregel, dass nur die zur Aufgabenerfüllung der handelnden Stelle erforderlichen Daten von dieser abgefragt werden dürfen bzw. nur insoweit eine entsprechende Mitwirkungspflicht des betroffenen Bürgers besteht. Dies ist bereits bei der Erstellung eines solchen Fragebogens zu berücksichtigen. Differenzierungen hinsichtlich verschiedener Fallgruppen können beispielsweise durch die Ausgabe spezieller Fragebögen für die jeweilige Fallgruppe oder dadurch erfolgen, dass im Fragebogen oder zumindest in beigelegten Hinweisen allgemein verständlich dargestellt wird, welche Fragen in welchen Fallgruppen beantwortet werden sollen. Weiterhin sind derartige Fragebögen etwa bei Änderungen der Rechtslage von der Stelle, die den Fragebogen einsetzt, daraufhin zu überprüfen, ob die abgefragten Daten noch dem Erforderlichkeitsgrundsatz entsprechen.

14.3.3 Verlängerter Sozialdatenschutz und Zweckbindung

Manche Datenschutzbestimmungen sind - auch bei öffentlichen Stellen - weniger im Bewusstsein der handelnden Personen verankert als andere. Beispielsweise sind die in § 78 SGB X geregelten

Rechtspflichten der Empfänger von Sozialdaten und der darin u.a. enthaltene Grundsatz der Zweckbindung diesen Empfängern nicht immer bzw. nicht in der gesamten Tragweite bewusst. Diese Vorschrift gilt für solche Fallgestaltungen, in denen die empfangende Stelle oder Person nicht zu den in § 35 SGB I aufgezählten Stellen - dort sind insbesondere die Sozialleistungsträger genannt - gehören. Die Problematik wird in folgender an mich herangetragenen Fallgestaltung deutlich:

Ein Unfallversicherungsträger hatte von einer Gemeindebediensteten Daten im Hinblick auf ihren (vermeintlichen) Arbeitsunfall erhalten. Der Unfallversicherungsträger hatte der Gemeinde daraufhin (auch) diese Daten mit der Bitte um Stellungnahme zum Sachverhalt übermittelt. Die diesbezügliche Stellungnahme der Gemeinde hat der Unfallversicherungsträger zur Prüfung des Vorliegens eines Arbeitsunfalls benötigt.

Die Gemeinde hat jedoch diese vom Unfallversicherungsträger übermittelten Daten nicht nur dazu genutzt, gegenüber dem Unfallversicherungsträger Stellung zu nehmen, sondern hat jedenfalls Teile dieser Daten im Rahmen eines Arbeitsgerichtsprozesses im Zusammenhang mit der Kündigung der Gemeindebediensteten genutzt. Gem. § 78 SGB X dürfen jedoch solche Sozialdaten von der Gemeinde, die insofern keine in § 35 SGB I genannte Stelle ist, nur zu dem Zweck verarbeitet oder genutzt werden, zu dem sie der Gemeinde befugt übermittelt worden sind. Mit der Einführung dieser - von der Unfallversicherung im Zusammenhang mit der Prüfung des Vorliegens eines Arbeitsunfalls erhaltenen - Daten in einen Kündigungsschutzprozess wurde die Zweckbestimmung, zu der diese Daten übermittelt wurden, im konkreten Fall jedoch überschritten. Dies ist unzulässig.

Die Gemeinde hat auf mein Tätigwerden hin mitgeteilt, sie bedauere einen Verstoß gegen datenschutzrechtliche Vorschriften und werde künftig dieser Problematik mehr Beachtung schenken. Im Arbeitsgerichtsprozess wurde letztlich durch die Parteien ein Vergleich geschlossen.

14.4 Arbeitsgemeinschaften und Sozialämter

14.4.1 Datenschutz bei Arbeitsgemeinschaften nach § 44 b SGB II

Mit Wirkung vom 01.01.2005 ist das Sozialgesetzbuch - Zweites Buch - (SGB II) in Kraft getreten. Dort sind insbesondere Leistungen zur Eingliederung in Arbeit und Leistungen zur Sicherung des Lebensunterhalts, etwa das Arbeitslosengeld II, geregelt. Im Zusammenhang mit diesen neuen Regelungen und deren verwaltungsmäßiger Umsetzung haben sich eine Vielzahl auch datenschutzrechtlicher Fragestellungen ergeben. Die Beschäftigung mit datenschutzrechtlichen Fragen im Zusammenhang mit der Gewährung von Arbeitslosengeld II machte einen Großteil meiner Tätigkeit im Sozialbereich aus. Auch die Konferenz des Bundesbeauftragten und der Landesbeauftragten für den Datenschutz hat sich verschiedentlich zu grundlegenden datenschutzrechtlichen Aspekten in diesem Zusammenhang geäußert (s. Anlage 7). Außerdem haben die Landesbeauftragten für den Datenschutz und der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit u.a. auf Änderungen in Antragsunterlagen und Erhebungsbögen unter datenschutzrechtlichen Aspekten hingewirkt.

Im Zusammenhang mit der Gewährung von Arbeitslosengeld II erfolgen vielfältige Datenerhebungen von Behörden. Maßgeblich ist wie so oft der Grundsatz der Erforderlichkeit. Die Datenerhebung ist zulässig, wenn ihre Kenntnis zur Erfüllung einer Aufgabe der erhebenden Stelle nach dem Sozialgesetzbuch erforderlich ist. Erforderlich ist eine Datenerhebung dann, wenn die Kenntnis der Daten zur Erreichung des Zwecks objektiv geeignet ist und im Verhältnis zu dem angestrebten Zweck auch angemessen erscheint.

Vor diesem Hintergrund habe ich es beispielsweise für zulässig gehalten, dass in einer auszufüllenden Bewerbungsübersicht danach gefragt wird, wie man von einer zu besetzenden Arbeitsstelle erfahren hat und die Behörde verlangt, dass die jeweiligen schriftlichen Bewerbungen vorgelegt werden. Denn erwerbsfähige Hilfebedürftige und die mit ihnen in einer Bedarfsgemeinschaft lebenden Personen müssen alle Möglichkeiten zur Beendigung oder Verringerung ihrer Hilfebedürftigkeit ausschöpfen. Nicht selten sind schlecht gestaltete oder gar mit Fehlern behaftete Bewerbungsschreiben der Grund für die Ablehnung des Bewerbers. Erhält die Behörde von der Bewerbung Kenntnis, ist es möglich, Defizite zu erkennen und durch entsprechende Angebote (Bewerbungstraining) eine Arbeitsaufnahme zu unterstützen.

Primäres Ziel der Arbeitsgemeinschaften ist es, die Betroffenen wieder in Arbeit zu bringen. In diesem Zusammenhang werden vielfach Profilingbögen verwendet. Diese Profilingbögen enthalten eine Vielzahl von Fragen, etwa zur Ausbildung, Berufspraxis etc. So hat eine Behörde einen Profilingbogen mit dem Hinweis, dass der Profilingbogen wahr und vollständig auszufüllen sei, an den Hilfeempfänger versendet. Weiter wird eine Einwilligungserklärung des Betroffenen eingeholt. Der Betroffene füllt den Bogen aus und dann soll in einem Gespräch geklärt werden, welche Unterstützungsmaßnahmen für den Betroffenen angeboten werden könnten. Dabei würden die Fallmanager nicht in jedem Fall beim Ausfül-

len des Fragebogens auf einer Mitwirkungspflicht des Hilfeempfängers bestehen. Nur wenn begründete Anhaltspunkte im Verhalten des Hilfeempfängers zu sehen seien, die eine Beantwortung einer bestimmten Frage unausweichlich erscheinen ließen, würde man auf der Beantwortung insistieren.

Aus datenschutzrechtlicher Sicht ist darauf zu achten, dass durch das Verfahren abgesichert ist, dass die Datenerhebung nicht unverhältnismäßig wird. Einzelne Fragen des Profilingbogens können für die Aufgabenerfüllung der öffentlichen Stelle durchaus eine Rolle spielen. Der Profilingbogen soll jedoch lediglich als Hilfsmittel für die persönliche Beratung des Betroffenen dienen. Der Umfang der Datenerhebung soll insoweit auf grundsätzliche und allgemeine Fragestellungen, etwa nach der Berufsausbildung und den beruflichen Erfahrungen, nach den speziellen Kenntnissen und Fertigkeiten sowie persönlichen Wünschen und nach den aus der Sicht des Betroffenen möglichen Hindernisgründen, die einer Berufstätigkeit generell oder bei bestimmten Tätigkeiten entgegenstehen, beschränkt werden. Im Übrigen ist immer auf den Einzelfall abzustellen. Die Schwierigkeit besteht darin, dass es der Behörde nicht abgesprochen werden kann, abstrakt generell im Zusammenhang mit der Gewährung von Arbeitslosengeld II Fragen zu stellen. Denn die gesetzgeberische Konzeption läuft darauf hinaus, dass der Betroffene in ein breites Spektrum von potenziellen Arbeitsplätzen zu vermitteln ist.

Vor diesem Hintergrund habe ich jedoch für Zwecke des Profilings etwa die Frage nach der Wohnsituation für unzulässig gehalten. Die Frage, ob man allein, bei den Eltern, mit Ehe- oder Lebenspartner oder in einer Wohngemeinschaft wohnt, kann die Vermittlung des Antragstellers in Arbeit nicht fördern. Zwar mag es sein, dass in bestimmten Fällen eine außergewöhnliche schwierige Wohnsituation zu einem Vermittlungshemmnis führen kann. In den meisten Fällen stellt jedoch nicht die Wohnsituation als solche das Vermittlungshemmnis dar, sondern andere Gründe. Insofern habe ich eine pauschale Abfrage der Wohnsituation bei jedem Antragsteller für unzulässig gehalten.

Unabhängig von derartig grundsätzlichen Fragen haben Bürgerinnen und Bürger ein ganz wesentliches und konkretes Interesse, dass seitens der handelnden Leistungsträger organisatorische Maßnahmen getroffen werden, um die Einhaltung der datenschutzrechtlichen Vorschriften auch beim persönlichen Kontakt vor Ort zu gewährleisten. Dies gilt natürlich auch, soweit die Träger der Leistungen zur einheitlichen Wahrnehmung ihrer Aufgaben Arbeitsgemeinschaften gemäß § 44 b SGB II gebildet haben.

So habe ich mich auch bezüglich dieser Arbeitsgemeinschaften mit an sich alt bekannten Problemen bezüglich der organisatorischen Rahmenbedingungen bei persönlichen Kontakten befassen müssen. Etwa bezüglich offen stehender Verbindungs- und Außentüren bei Gesprächen zwischen einem Antragesteller und einem Sachbearbeiter habe ich auch auf die oben genannten Arbeitsgemeinschaften im Sinne der Ausführungen in meinem 20. Tätigkeitsbericht (dortige Ziffer 17.3.8) eingewirkt. Verschiedentlich wurde seitens Arbeitsgemeinschaften nunmehr auch vorgetragen, die räumliche Situation lasse es etwa nicht zu, Sachbearbeitern immer ein Einzelzimmer zur Verfügung zu stellen. Zu den angesprochenen organisatorischen Maßnahmen gehört es jedoch auch, dass gewährleistet wird, dass Unbefugte nicht von Sozialdaten Kenntnis nehmen können. Diese Gefahr besteht etwa, wenn sich in dem Raum mehrere Personen aufhalten, darunter insbesondere weitere Antragsteller. Grundsätzlich ist der Sozialdatenschutz am besten gewährleistet, wenn sich der Sachbearbeiter mit dem Antragsteller alleine im Raum aufhält. Denn die Antragstellung beschränkt sich oftmals nicht auf die bloße Antragsabgabe, sondern in vielen Fällen muss - gerade bei den komplexen Antragsformularen zu Leistungen nach dem SGB II - mit dem Antragsteller das Formular besprochen werden. Dann ist es unvermeidlich, dass auch Umstände besprochen werden, die dem Sozialgeheimnis unterfallen. Soweit sich diese optimale Situation „ein Antragsteller und ein Sachbearbeiter in einem Raum“ aus tatsächlichen Gründen - ggf. zumindest vorübergehend - nicht erreichen lässt, muss die Behörde jedoch zusätzliche Anstrengungen unternehmen, um den Sozialdatenschutz zu gewährleisten. Soweit seitens der Arbeitsgemeinschaften auf Diskretionsabstände zwischen den Antragstellern verwiesen wird, so ist dabei zu berücksichtigen, dass dieser dann so groß sein muss, dass ein Gespräch in normaler Lautstärke außerhalb der eingerichteten Diskretionszone nicht zu verstehen ist.

Auch in Räumen bzw. an Schaltern, in bzw. an denen üblicherweise nur Antragsunterlagen abgeholt bzw. abgegeben werden, ist darauf zu achten, dass durch ausreichende Diskretionsabstände bzw. ggf. durch die Anbringung von seitlichen Sichtblenden eine Einsichtnahme Dritter in Antragsunterlagen ausgeschlossen wird.

Entscheidend kann ansonsten sein, dass der Antragsteller darauf aufmerksam gemacht wird, dass er sich auch einen Einzeltermin geben lassen bzw. auch in einem geschützten Bereich seine Situation schildern kann. Es ist dann durch geeignete Maßnahmen sicherzustellen, dass die Betroffenen von dieser Möglichkeit auch erfahren. Diesbezüglich können insbesondere Schilder aufgestellt werden. Zudem können Beschäftigte Antragsteller, soweit diese nicht nur einen Antrag abgeben, sondern weitergehende Erläuterungen wünschen, auf die o.g. Möglichkeit eines Einzeltermins hinweisen.

14.4.2 Überweisung der Kosten der Unterkunft direkt an den Vermieter

Bereits in meinem letzten Tätigkeitsbericht (s. Nr. 6.4) habe ich das Problem erörtert, dass das Sozialgeheimnis dann verletzt werden kann, wenn Dritte von der Hilfebedürftigkeit eines Bürgers erfahren. Dabei entsteht dieses Problem nicht nur, wenn wie seinerzeit Formulare verwendet werden, die erkennen lassen, dass die darauf zu bestätigenden Informationen für eine Sozialbehörde bestimmt sind, sondern auch, wenn der Hilfebezug dadurch offen gelegt wird, dass die Hilfe auf das Konto eines Dritten überwiesen wird. Dies zeigt sich anhand des folgenden Falles:

Ein Bürger hat sich bei mir darüber beschwert, dass gegen seinen Willen die angemessenen Kosten der Unterkunft direkt an den Vermieter überwiesen würden. Das datenschutzrechtliche Problem dieser Verfahrensweise besteht darin, dass dadurch der Vermieter erfährt, dass sein Mieter Sozialhilfe bezieht. Aus Datenschutzsicht liegt darin die Übermittlung von Sozialdaten, die nur dann zulässig ist, wenn eine Einwilligung oder eine gesetzliche Übermittlungsbefugnis gegeben ist.

Als gesetzliche Übermittlungsbefugnis kommt allenfalls § 69 Abs. 1 Nr. 1 Alternative 1 und 2 SGB X in Betracht. Danach ist eine Übermittlung von Sozialdaten zulässig, soweit sie erforderlich ist für die Erfüllung der Zwecke, für die sie erhoben worden sind oder für die Erfüllung einer gesetzlichen Aufgabe der übermittelnden Stelle nach dem Sozialgesetzbuch.

Nach den gesetzlichen Bestimmungen ist etwa eine direkte Zahlung an den Vermieter zugelassen, wenn die zweckentsprechende Verwendung durch die Leistungsberechtigten nicht sichergestellt ist. Allein unangemessen hohe Kosten für die Unterkunft reichen nicht aus, damit direkt an den Vermieter geleistet werden kann. Dies ergibt sich bereits aus dem Gesetzeswortlaut. Denn hätte der Gesetzgeber dies gewollt, so hätte er ohne weitere Voraussetzungen für den Fall der unangemessenen hohen Kosten die Direktleistung an den Vermieter für zulässig erklären können.

Der Gesetzgeber knüpft jedoch für die Zulässigkeit der Direktleistung an ein anderes Merkmal an: Nur wenn die zweckentsprechende Verwendung durch den Leistungsberechtigten nicht sichergestellt ist, wäre eine Direktleistung zulässig. Die Behörde muss also Anhaltspunkte dafür haben, dass der Sozialhilfeempfänger das Geld, das eigentlich für die Unterkunft vorgesehen ist, anderweitig verwendet. Diese Anhaltspunkte dürften im Rahmen des seinerzeit geltenden § 15 a BSHG bei Mietrückständen regelmäßig gegeben sein.

Vergleichbares gilt jedoch dann nicht, wenn die Kosten für die Unterkunft im Rahmen der normalen Sozialhilfe übernommen werden. Auch wenn die Kosten für die Unterkunft unangemessen hoch sind, bietet allein die Höhe der Differenz zwischen tatsächlicher und angemessener Miete noch keinen Anhaltspunkt dafür, dass der Mieter die Miete nicht zweckentsprechend verwenden wird. Hier muss meiner Ansicht nach gesondert begründet werden, wieso die Gefahr besteht, dass der Hilfeempfänger die Zahlung nicht zweckentsprechend verwenden wird.

Die Behörde hatte in dem mir vorliegenden Fall die Direktleistung noch damit zu begründen versucht, dass die Wohnung unangemessen sei. Dies kann jedoch nicht dazu führen, dass das Sozialamt hätte annehmen können, dass die zweckentsprechende Verwendung durch die Leistungsberechtigten nicht sichergestellt ist. Denn der Hinweis, dass eine Wohnung unangemessen ist, hat nur die Folge, dass der Hilfeempfänger darüber in Kenntnis gesetzt wird, dass die Unterkunftskosten nicht in tatsächlicher, sondern nur in angemessener Höhe als Bedarf der Hilfe zum Lebensunterhalt anerkannt werden. Aus diesem Hinweis kann nicht der Schluss gezogen werden, dass der Hilfeempfänger den geringeren angemessenen Betrag nicht für die Wohnung aufwenden wird.

Die Behörde hatte jedoch im vorliegenden Fall noch einen weiteren Fehler gemacht. Nach den gesetzlichen Bestimmungen ist der Leistungsberechtigte von der Direktleistung an den Vermieter schriftlich zu unterrichten. Diese Unterrichtung muss vor der Leistung erfolgen, damit der Leistungsberechtigte unter Umständen die Entscheidung des Sozialamts angreifen kann. Wenn eine schriftliche Unterrichtung überhaupt nicht erfolgt, so stellt auch dies einen Verstoß gegen datenschutzrechtliche Bestimmungen dar.

Ich habe daher im vorliegenden Fall die Behörde wegen einer unzulässigen Sozialdatenübermittlung an den Vermieter des Hilfeempfängers und wegen der unterbliebenen Information des Hilfeempfängers beanstandet.

14.5 Heimbereich

14.5.1 Datenerhebung bei Heimen

Im Sozialdatenschutzrecht gilt zum einen die Faustregel, dass Daten nur dann von Sozialleistungsträgern erhoben werden dürfen, wenn sie zur dortigen Aufgabenerfüllung nach dem Sozialgesetzbuch erforderlich sind. Zum anderen hat sich der Gesetzgeber auch dazu geäußert, bei wem die erforderlichen Daten erhoben werden sollen. Nach dem Grundsatz des Vorrangs der Datenerhebung beim Betroffenen hat dies zunächst eben beim Betroffenen selbst zu erfol-

gen. Hintergrund der Vorschrift ist die Transparenz des Verfahrens für den Betroffenen. Außerdem erhält bei Datenerhebungen bei Dritten dieser zwangsläufig allein aufgrund der Tatsache der Datenerhebung durch die Behörde eine Information über den Betroffenen. Letzteres ist auf die gesetzlich geregelten Ausnahmefälle zu beschränken (§ 67 a Abs. 2 Satz 2 SGB X).

An mich ist ein Fall herangetragen worden, in dem ein Sozialhilfeträger im Zusammenhang mit der Prüfung der Beanspruchung des für ein volljähriges Kind zu gewährenden Kindergeldes Daten bei einem Heim bezüglich der Kinder bzw. Eltern erhoben hat. Ein Heim ist hinsichtlich der dort über Kinder bzw. Eltern erhobenen Daten jedoch nicht Betroffener, sondern Dritter. Ich bin daher an den Sozialhilfeträger mit der Bitte um Stellungnahme herangetreten, u.a. inwiefern die Voraussetzungen für eine solche Datenerhebung bei einem Dritten erfüllt sind. Der Sozialhilfeträger hat daraufhin mitgeteilt, meine Anfrage habe ihn veranlasst, die Aktion zu überprüfen, mit dem Ergebnis, sie abzusetzen. Diese Datenerhebungen erfolgen demnach nunmehr nicht mehr bei den Heimen.

14.6 Kindertageseinrichtungen

14.6.1 Bedarfsplanung für Plätze in Kindertageseinrichtungen

Aufgrund von Vorschriften im Sozialgesetzbuch und im Bayerischen Kinderbildungs- und –betreuungsgesetz führen etwa Gemeinden und Städte vor dem Hintergrund ihres Sicherstellungsauftrags Planungen hinsichtlich des Bedarfs an Plätzen in Kindertageseinrichtungen durch.

Es liegt nahe, bezüglich des zu erwartenden Bedarfs - zumindest auch - Betroffene selbst, also Eltern, zu befragen. Eine Befragung kann grundsätzlich zum einen unter Herstellung eines konkreten Personenbezugs (etwa durch Nennung von Name und Vorname), zum anderen ohne Herstellung eines solchen Personenbezugs, also anonym, erfolgen. Die Erhebung personenbezogener Daten ist - unabhängig von weiteren Kriterien - insbesondere am datenschutzrechtlichen Erforderlichkeitsgrundsatz zu messen.

Betroffene Eltern haben mir einen Erhebungsbogen einer Stadt mit der Bitte um datenschutzrechtliche Prüfung vorgelegt. In diesem Erhebungsbogen ist die Abfrage bei den Eltern unter Einbeziehung der Personalien (Name, Vorname) erfolgt. Ich habe daraufhin Stellungnahmen bei der erhebenden Stadt und beim Bayerischen Staatsministerium für Arbeit und Soziales, Familie und Frauen zur Erforderlichkeit dieses Personenbezugs eingeholt. Nach Würdigung der Stellungnahmen bin ich zum Ergebnis gelangt, dass ein solcher Personenbezug datenschutzrechtlich als nicht erforderlich anzusehen ist. Das Bayerische Staatsministerium für Arbeit und Soziales, Familie und Frauen hält im Übrigen eine anonyme Datenerhebung auch aus fachlichen Gründen für geboten. Eltern könnten sich gehindert sehen, ihre wahren Bedürfnisse (etwa im Hinblick auf eine gewünschte besondere pädagogische Ausrichtung) zu artikulieren, wenn ihre Anonymität nicht gewährleistet ist. Inzwischen hat das Bayerische Staatsministerium für Arbeit und Soziales, Familie und Frauen auch einen Praxisleitfaden für die kommunale Bedarfsplanung im Internet veröffentlicht sowie eine Handreichung für die Bedarfsplanung der zuständigen Stellen erarbeitet.

Ich habe die Stadt wegen des unzulässigen Erhebens von personenbezogenen Daten im Zusammenhang mit der Bedarfsplanung nach dem Bayerischen Kinderbildungs- und -betreuungsgesetz beanstandet.

15 Verkehrswesen

15.1 Zulassung von Fahrzeugen nur bei Entrichtung rückständiger Gebühren und Auslagen

Durch das Zweite Gesetz zur Änderung des Straßenverkehrsgesetzes und anderer Gesetze vom 3. Mai 2005 (BGBl I S. 1221) wurde dem § 6 a Straßenverkehrsgesetz (StVG) ein Absatz 8 angefügt, mit dem die Länder ermächtigt werden, die Zulassung von Fahrzeugen von der Entrichtung der dafür bestimmten Gebühren und Auslagen sowie der rückständigen Gebühren und Auslagen aus vorausgegangenen Zulassungsvorgängen abhängig zu machen. Bayern hat in Art. 14 Abs. 4 Kostengesetz (KG) von der Ermächtigung in § 6 a Abs. 8 StVG Gebrauch gemacht und diese Möglichkeit auch für alle anderen Verwaltungsverfahren eröffnet. In der Gesetzesbegründung zu Art. 14 Abs. 4 KG wird allerdings ausdrücklich darauf hingewiesen, dass wegen des verfassungsrechtlich im Rechtsstaatsprinzip verankerten allgemeinen Koppelungsverbots keine Verfahren miteinander verknüpft werden dürfen, die nicht ohnehin in einem inneren Zusammenhang stehen. Die neu geschaffene Befugnis wurde daher auf Verfahren gleicher Art beschränkt. Das bedeutet zum Beispiel, dass eine Gemeinde die Ausstellung eines Personalausweises auch zukünftig nicht von der Bezahlung rückständiger Kommunalabgaben abhängig machen kann.

Im Verfahren zur Umsetzung von § 6 a Abs. 8 StVG in Landesrecht habe ich darauf hingewiesen, dass bei der Kfz-Zulassung in den Fällen, in denen das Fahrzeug nicht durch den Fahrzeughalter selbst, sondern durch einen Dritten zugelassen wird, dem Dritten Angaben über rückständige Gebühren und Auslagen des Fahrzeughalters bekannt werden. Aus daten-

schutzrechtlicher Sicht ist daher eine schriftliche Einverständniserklärung des Fahrzeughalters hinsichtlich der Mitteilung der gebührenrechtlichen Verhältnisse an denjenigen, der das Fahrzeug zulässt, erforderlich.

16 Gewerbe und Handwerk

16.1 Information über unlautere Geschäftspraktiken durch eine Innung

Eine Kfz-Innung hat in einem Rundschreiben ihre Mitglieder über das Urteil eines Oberlandesgerichts unterrichtet, das festgestellt hatte, dass die Vorgehensweise einer Rechtsanwaltskanzlei im Zusammenhang mit kostenpflichtigen Serienabmahnungen zum Thema Unfallschadenabwicklung als rechtsmissbräuchlich zu qualifizieren war. Die Rechtsanwaltskanzlei, die in dem Rundschreiben namentlich erwähnt wird, hat sich bei mir über die Innung beschwert. Aus datenschutzrechtlicher Sicht habe ich den Vorgang wie folgt bewertet:

Nach § 54 Abs. 4 der Handwerksordnung (HandwO) kann die Innung neben ihren Pflichtaufgaben auch sonstige Maßnahmen zur Förderung der gemeinsamen gewerblichen Interessen der Innungsmitglieder durchführen. Zu diesen sonstigen freiwilligen Aufgaben der Innung zählt auch, dass die Innung z.B. vor unlauteren oder gefährlichen Geschäftspraktiken Dritten warnt. Dabei ist nach einer entsprechenden Interessenabwägung auch nichts dagegen einzuwenden, wenn die Innung die Angelegenheit deutlich zur Sprache bringt und dabei ihren subjektiven Standpunkt in einer für die Innungsmitglieder verständlichen Weise vertritt (vgl. Honig, Kommentar zur Handwerksordnung, 3. Auflage 2004, § 54 Rdnr. 51). Auch das von mir in der Angelegenheit beteiligte Bayerische Staatsministerium für Wirtschaft, Infrastruktur, Verkehr und Technologie vertritt die Auffassung, dass es zu den satzungsmäßigen Aufgaben der Innung gehört, ihre Mitglieder über missbräuchliche Geschäftspraktiken Dritter zu unterrichten. Im vorliegenden Fall hatte das Oberlandesgericht festgestellt, dass die Abmahntätigkeit der Anwaltskanzlei in den Jahren 2000 und 2001 als rechtsmissbräuchlich zu qualifizieren war. Die Information der Innungsmitglieder hierüber in einem Rundschreiben, das lediglich den Mitgliedern der Innung zugänglich war, lag somit im Rahmen der Aufgabenerfüllung der Kfz-Innung und war datenschutzrechtlich nicht zu beanstanden.

16.2 Prüfung des elektronischen Verteildienstes beim Verfahren GEWAN

Im Berichtszeitraum habe ich den elektronischen Verteildienst des Verfahrens Gewerbeanzeigen im Netz (GEWAN) datenschutzrechtlich geprüft. Beim elektronischen Verteildienst handelt es sich um eine Teilfunktion des Verfahrens GEWAN, das vom Bayerischen Landesamt für Statistik und Datenverarbeitung entwickelt wurde, um die Kommunen bei der Erfassung und Pflege von Gewerbeanzeigen (An-, Ab- und Ummeldung) elektronisch zu unterstützen. Bereits im vorletzten Berichtszeitraum hatte ich das Verfahren GEWAN umfassend geprüft (siehe 20. Tätigkeitsbericht 2002 Nr. 14.3) und mir dabei eine spätere Prüfung des elektronischen Verteildienstes vorbehalten, da dieser zum damaligen Zeitpunkt noch nicht im Echtbetrieb durchgeführt worden war. Mit Hilfe des elektronischen Verteildienstes können Daten aus der Gewerbeanzeige medienbruchfrei an alle beteiligten Stellen übermittelt werden: Das Verfahren sieht zunächst eine Weiterleitung der anfallenden Daten aus der Gewerbeanzeige durch das Bayerische Landesamt für Statistik und Datenverarbeitung an neun zentrale Verteilstellen (sog. Kopfstellen) in Bayern vor. Diese Kopfstellen übernehmen die Weiterleitung der Daten an die jeweils gesetzlich vorgeschriebene örtliche Empfangsstelle (z.B. die örtlich zuständige Handwerkskammer, das örtlich zuständige Finanzamt etc.) in eigener Verantwortung.

Im Rahmen der datenschutzrechtlichen Prüfung habe ich festgestellt, dass bei der Weiterleitung der Daten von den Kopfstellen an die Empfangsstellen nicht ausgeschlossen werden kann, dass die Daten von der Kopfstelle möglicherweise unverschlüsselt an die örtlich zuständige Empfangsstelle weitergeleitet werden. Ich habe das Bayerische Landesamt für Statistik und Datenverarbeitung daher aufgefordert, die Kopfstellen darauf hinzuweisen, dass die Daten nur verschlüsselt über öffentliche Netze übertragen werden dürfen. Da auch für die Leitungen des bayerischen Behördennetzes nicht ausgeschlossen werden kann, dass Sicherheitsprobleme beim Provider der Leitungen einen Zugriff auf die Daten ermöglichen, halte ich auch eine Verschlüsselung der Daten bei einer Übertragung innerhalb des Bayerischen Behördennetzes für erforderlich. Das Bayerische Landesamt für Statistik und Datenverarbeitung hat daraufhin alle neun Kopfstellen über die Verschlüsselungspflicht bei der Übermittlung von Gewerbedaten im Verfahren GEWAN informiert.

17 Umweltfragen

17.1 Bayerisches Umweltinformationsgesetz

Nach Art. 11 EU-Richtlinie 2003/4/EG vom 28. Januar 2003 über den Zugang der Öffentlichkeit zu Umweltinformationen ist die Umweltinformationsrichtlinie 90/131/EWG zum 14. Februar 2005 aufgehoben worden. In Art. 10 der neuen Umweltinformationsrichtlinie wurden die Mitgliedsstaaten verpflichtet, die Richtlinie bis zu diesen Zeitpunkt umzuset-

zen. Da der Anwendungsbereich des Bundes-Umweltinformationsgesetzes vom 22. Dezember 2004 (BGBl I S. 3704) sich im Hinblick auf die Gesetzgebungskompetenz des Bundes nur noch auf informationspflichtige Stellen des Bundes bezieht, war eine Regelung auf Landesebene erforderlich. Das Bayerische Staatsministerium für Umwelt, Gesundheit und Verbraucherschutz hat daher einen Entwurf eines Bayerischen Umweltinformationsgesetzes (BayUIG) erarbeitet, der mir im Rahmen der Ressortabstimmung vorgelegt wurde.

Der inzwischen von der Bayerischen Staatsregierung in den Landtag eingebrachte Gesetzentwurf (LT-Drucksache 15/5627 vom 23.05.2006) sieht eine inhaltsgleiche Umsetzung des Europarechts vor und geht nicht über die Vorgaben der EU-Richtlinie hinaus. Er enthält im Vergleich zum bisher geltenden Informationsrecht folgende Neuerungen: Nunmehr werden alle Stellen der öffentlichen Verwaltung zur Herausgabe von Umweltinformationen verpflichtet, unabhängig davon, ob sie spezifisch Aufgaben im Bereich des Umweltrechts wahrnehmen. In den Kreis der Informationspflichtigen werden ausdrücklich auch Personen des privaten Rechts aufgenommen, soweit sie unter der Kontrolle einer Stelle der öffentlichen Verwaltung stehen und im Zusammenhang mit der Umwelt öffentliche Aufgaben wahrnehmen oder öffentliche Dienstleistungen erbringen. Der Begriff der „Umweltinformation“ wird inhaltlich erweitert und erfasst damit z.B. auch Aspekte der Gentechnik und der menschlichen Gesundheit und Sicherheit. Die Fristen für die Beantwortung von Anfragen dürfen in der Regel einen Monat nicht überschreiten. Die öffentlichen Verwaltungen werden außerdem angehalten, unter Nutzung elektronischer Medien Umweltinformationen aktiv zu verbreiten.

Dem Recht auf informationelle Selbstbestimmung bei der Veröffentlichung von Umweltinformationen wird insbesondere durch die Vorschrift des Art. 8 Abs. 1 Satz 1 Nr. 1 des Gesetzentwurfs Rechnung getragen. Diese Regelung sieht eine Abwägung zwischen dem Informationsanspruch des Antragsstellers und den schutzwürdigen Interessen des davon betroffenen Bürgers vor. So ist ein Antrag auf Erteilung von Umweltinformationen abzulehnen, soweit durch das Bekanntgeben der Informationen personenbezogene Daten offenbart und dadurch schutzwürdige Interessen der Betroffenen beeinträchtigt würden, es sei denn, die Betroffenen haben zugestimmt oder das öffentliche Interesse an der Bekanntgabe überwiegt. Das Umweltministerium hat damit einem Vorschlag von mir entsprochen. Im Interesse eines einheitlichen Sprachgebrauchs hatte ich vorgeschlagen, Art. 8 Abs. 1 Satz 1 Nr. 1 BayUIG sowie die Gesetzesbegründung an den Wortlaut des Art. 19 Abs. 1 Nr. 2 Bayerisches Datenschutzgesetz (BayDSG) anzupassen, der bei einer Herausgabe personenbezogener Daten an eine nicht-öffentliche Stelle ebenfalls eine Abwägung zwischen dem berechtigten Interesse des potenziellen Empfängers an den zu übermittelnden Daten und den schutzwürdigen Belangen des Betroffenen an dem Ausschluss der Übermittlung vorsieht.

18 Landwirtschaft

18.1 Datenschutzgerechte Gestaltung des Berichtshefts im Lehrberuf Landwirt

Nach § 7 Satz 1 der Verordnung über die Berufsausbildung zum Landwirt / zur Landwirtin (LwAusbV) hat der Auszubildende ein Berichtsheft in Form eines Ausbildungsnachweises zu führen. Im Rahmen einer Eingabe wurde mir nun vorgetragen, dass der Auszubildende seine dreijährige Ausbildungszeit in der Regel - um die gesamte Breite des Berufsbildes abzudecken - in verschiedenen Betrieben absolviere. Da in dem Berichtsheft der Gang der Ausbildung zu dokumentieren sei, würden dort auch wirtschaftliche und persönliche Daten des jeweiligen Betriebsinhabers eingetragen, wie etwa Ein- und Verkaufspreise, Anbautechniken und Darlehenskonditionen bis hin zu Privatausgaben. Während jedoch früher für jedes Lehrjahr ein gesondertes Heft zu führen gewesen sei, sei neuerdings - angeblich sogar bundeseinheitlich - ein zusammengefasstes Berichtsheft für alle drei Lehrjahre zu führen. Dies habe aber zur Folge, dass die Betriebsleiter des dritten Lehrjahres zahlreiche wirtschaftliche und persönliche Daten der Vorbetriebe über dieses Berichtsheft zu Gesicht bekämen, was wettbewerbsrechtlich fragwürdig und datenschutzrechtlich nicht hinnehmbar sei.

Meine Prüfung der einschlägigen Vorschriften hat zunächst ergeben, dass § 7 LwAusbV die Führung eines zusammengefassten Berichtsheftes nicht ausdrücklich vorschreibt. Die Auferlegung einer solchen Pflicht durch eine bundes- oder landesrechtliche Rechts- oder Verwaltungsvorschrift wäre meiner Auffassung nach auch datenschutzrechtlich bedenklich, da ihre ordnungsgemäße Erfüllung jedenfalls mittelbar zu Übermittlungen von sensiblen Daten der Betriebsinhaber vorausgegangener Ausbildungsabschnitte zwingen würde, ohne dass dies offensichtlich zur Erreichung des Ausbildungszweckes erforderlich wäre. Ich habe daher das Staatsministerium für Landwirtschaft und Forsten um Stellungnahme zu dem geschilderten Sachverhalt gebeten.

Das Staatsministerium für Landwirtschaft und Forsten hat in seiner Antwort ausgeführt, dass ein Wechsel des Ausbildungsbetriebes im Rahmen der Berufsausbildung zum Landwirt / zur Landwirtin ausdrücklich gewünscht sei. Folglich habe nach § 14 Abs. 1 Nr. 4 des Berufsbildungsgesetzes (BBiG) der jeweilige Ausbildende den Auszubildenden zur Führung von schriftlichen Ausbildungsnachweisen anzuhalten. Im bundeseinheitlichen Berichtsheft seien

zwar eindeutig festgelegte betriebliche Daten in vorgedruckte Formulare einzutragen. Für zusätzliche Angaben - wie etwa Darlehenskonditionen oder Privatausgaben des Betriebsleiters - seien allerdings keine Datenfelder vorgesehen. Die geforderten Angaben umfassten zum einen die natürlichen Verhältnisse (Boden, Geländegestalt, Klima), zum anderen die Ausstattung des Betriebes (Viehhaltung, Gebäude und Maschinen). Neben Angaben, die sich auf eher technische und natürliche Kapazitäten, wie Tierzahl, Stallplätze und ähnliches bezögen, seien dabei auch jeweils ein Blatt für Einkaufspreise sowie für Verkaufserlöse im Berichtsheft vorgegeben. Die Angaben in diesen beiden Blättern bezögen sich jedoch nur auf die jeweiligen technischen Einheiten (wie Euro je Kilogramm, je Doppelzentner, je Liter usw.); ein Schluss auf die betrieblichen Einnahmen und Kosten insgesamt sei bei diesen Angaben nicht möglich.

Bei den Formblättern handele es sich um Einlegeblätter, die vom Auszubildenden in einen Ringordner eingeordnet würden. Daher sei es technisch unschwer möglich, bestimmte betriebliche Daten, die ein Ausbilder dem nachfolgenden Ausbildungsbetrieb nicht offenbaren wolle, zu entfernen. Überdies verpflichte sich der Auszubildende mit der Unterzeichnung des (Muster-) Berufsausbildungsvertrages dazu, Stillschweigen „über Betriebs- und Geschäftsgeheimnisse“ zu wahren.

Um besser auf diese Möglichkeit hinzuweisen und um die Problematik auch in datenschutzrechtlicher Hinsicht für alle Beteiligten transparenter zu gestalten, beabsichtigt das Staatsministerium für Landwirtschaft und Forsten, in Bayern zukünftig wie folgt zu verfahren:

In einem speziellen Einlegeblatt soll der Ausbilder nun aufgefordert werden, mit Unterschrift zu erklären, ob

- das Berichtsheft in vorliegender Form dem nachfolgenden Ausbilder vorgelegt werden kann oder

- welche eigens gekennzeichneten Seitenblätter aus dem Berichtsheft vor der Weitergabe zu entfernen und vom Auszubildenden gesondert aufzubewahren sind.

Das Staatsministerium für Landwirtschaft und Forsten hat angekündigt, sich beim Arbeitskreis der zuständigen Stellen nach dem BBiG dafür auszusprechen, dass bundesweit eine derartige Erklärung des Ausbilders zur Weitergabe von Daten des Berichtsheftes aufgenommen wird. Die zuständigen Stellen in Bayern erhielten bereits im Vorgriff auf die anzustrebende bundeseinheitliche Regelung das beschriebene zusätzliche Einlegeblatt.

Die vom Staatsministerium für Landwirtschaft und Forsten beabsichtigte Verfahrensweise ist aus meiner Sicht - insbesondere aufgrund der nunmehr schriftlich zu erteilenden (beschränkten) Einwilligung des Ausbilders in die Datenübermittlung - geeignet, die bei der Führung des Berichtsheftes auftretenden datenschutzrechtlichen Probleme einer praxisgerechten Lösung zuzuführen. Für seine Bereitschaft, auch bundesweit auf die Aufnahme einer derartigen Erklärung des Ausbilders in das Berichtsheft hinzuwirken, habe ich dem Staatsministerium für Landwirtschaft und Forsten ausdrücklich meinen Dank ausgesprochen.

19 Personalwesen

19.1 Bedienstetennamen im Publikumsverkehr

Mit dem spezifischen Problem des Tragens von Namensschildern im öffentlichen Dienst hatte ich mich bereits in Nr. 12.4 meines 16. Tätigkeitsberichts 1994 befasst. Auch im vergangenen Berichtszeitraum erreichten mich immer wieder Anfragen zu der übergreifenden Problematik der Angabe der Namen von Bediensteten in Behörden mit Publikumsverkehr - sei es u.a. in Form der Namensnennung der Sachbearbeiter in amtlichen Schreiben oder auch der Angabe von Vor- und Nachnamen auf Türschildern.

Zu der Frage, in welchem Umfang sich Amtsträger in diesem Zusammenhang auf das Recht auf informationelle Selbstbestimmung berufen können, vertrete ich folgende Auffassung:

Als Grundrecht stellt das Recht auf informationelle Selbstbestimmung in erster Linie ein Abwehrrecht des Bürgers gegenüber dem Staat dar. Soweit der öffentlich Bedienstete also dem Staat als eigenständiger Träger von Rechten und Pflichten gegenübersteht, kann er sich gegenüber seinem Dienstherrn selbstverständlich auf dieses Grundrecht berufen. In seiner Eigenschaft als Amtsträger - also als handelndes Organ des Staates - kann der öffentlich Bedienstete jedoch schon begrifflich nicht Grundrechtsträger sein. Dies bedeutet aber nicht, dass der Dienstherr in diesem Verhältnis uneingeschränkt dienstliche Kommunikationsdaten des Amtsträgers - wie Name, Vorname, Zuständigkeitsbereich, dienstliche Telefonnummer oder Zimmernummer - an Dritte übermitteln darf. Hier ist vielmehr eine Abwägung erforderlich. Dabei ist einerseits natürlich die Funktionsfähigkeit des Behördenapparates ein gewichtiges Entscheidungskriterium. Gerade in den letzten Jahren spielt auch der Gesichtspunkt der Service- oder Kundenorientierung, d.h. der Bürgerfreundlichkeit der Verwaltung, eine immer wichtigere Rolle. So gehört es heutzutage zur ordnungsgemäßen Aufgabenerfüllung insbesondere einer Behörde mit Publikumsver-

kehr, die Bürger darüber zu informieren, welche Bediensteten die richtigen Ansprechpartner für ihre Anliegen sind. Andererseits kann im Rahmen der Abwägungsentscheidung die Fürsorgepflicht des Dienstherrn zu einer Geheimhaltung bestimmter Informationen über den Bediensteten führen.

Die Rechtsgrundlage für die Übermittlung von Kommunikationsdaten der öffentlich Bediensteten an Dritte stellt Art. 19 Abs. 1 Nr. 1 i.V.m. Art. 17 Abs. 1 Nr. 2 BayDSG dar. Im datenschutzrechtlichen Sinne liegt hier eine Datenübermittlung an nicht-öffentliche Stellen vor. Da es sich aufgrund der Verwendung zu Organisationszwecken bei den gegenständlichen Bedienstetendaten um Sachaktendaten handelt, sind die Vorschriften des Personalaktenrechts (Art. 100 a ff. BayBG) insoweit nicht einschlägig. Im Rahmen der Prüfung dieser Rechtsgrundlage ist entscheidend, ob die Übermittlung der konkreten Kommunikationsdaten zur Aufgabenerfüllung der Behörde erforderlich ist. Dabei kommt es im Rahmen der Erforderlichkeitsprüfung 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.

Bei der Abwägung, ob die Pflicht des Dienstherrn zur ordnungsgemäßen und bürgerfreundlichen Aufgabenerfüllung oder die Fürsorgepflicht des Dienstherrn gegenüber dem Bediensteten höher zu werten sind, dürfte eine völlige Geheimhaltung der Identität eines Bediensteten nur in extremen Einzelfällen in Betracht kommen, etwa bei absehbaren Lebens- oder Gesundheitsgefährdungen. Gegen die Anordnung eines Dienstherrn, Bedienstetennamen im Publikumsverkehr zu verwenden - etwa Namensschilder zu tragen, Türschilder mit Namen zu versehen oder die Namen der Sachbearbeiter in amtlichen Schreiben zu nennen - erhebe ich daher grundsätzlich keine datenschutzrechtlichen Bedenken.

Allerdings hat der Dienstherr seiner Pflicht zur Information der Bürger in der Regel bereits durch die Bekanntgabe des Familiennamens der Bediensteten Genüge getan. Dennoch ist die in letzter Zeit mir gegenüber vermehrt geäußerte Auffassung, dass die Nennung des vollständigen Namens der Bediensteten die Bürgerfreundlichkeit der Behörde besonders unterstreiche, in gewissen Grenzen für mich nachvollziehbar. Wenn aber nun ein Dienstherr ein berechtigtes Interesse an der zusätzlichen Nennung des Vornamens vorträgt, muss es eine Möglichkeit geben zu überprüfen, ob schutzwürdige Interessen der Betroffenen am Ausschluss der Datenübermittlung bestehen. Daher ist den Bediensteten in diesen Fällen ein Widerspruchsrecht einzuräumen. So legt Art. 15 Abs. 5 Satz 1 BayDSG fest, dass personenbezogene Daten insoweit nicht übermittelt werden dürfen, als Betroffene schriftlich einer bestimmten Übermittlung widersprechen und eine Abwägung im Einzelfall ergibt, dass das schutzwürdige Interesse eines Betroffenen wegen seiner besonderen persönlichen Situation das Interesse der öffentlichen Stelle an der Übermittlung dieser Daten überwiegt. Um diese Abwägung zu ermöglichen, muss der Bedienstete also dem Dienstherrn seine persönliche Situation und seine damit verbundenen schutzwürdigen Interessen näher schriftlich darlegen.

Meiner Erfahrung nach kann insbesondere bei folgenden Fallkonstellationen die erforderliche Abwägung zu einer Nichtangabe des Vornamens führen: Im Bereich der Eingriffsverwaltung befürchten Bedienstete oftmals private Belästigungen bis hin zu persönlichen Bedrohungen für sich selbst und ihre Familie. Anlässe sind hier in der Regel der Erlass von - für den Adressaten sicherlich meist auch persönlich - belastenden Verwaltungsakten, etwa im Ordnungsrecht, aber vor allem im Sozial(hilfe)- und Ausländerrecht. Hier wird es den von belastenden Verwaltungsakten Betroffenen durch die zusätzliche Angabe des Vornamens wesentlich erleichtert, unter Nutzung weiterer, frei zugänglicher (elektronischer) Datenbestände - wie Adressbücher, Telefonverzeichnisse usw. - den oder (in der Praxis meist) die Sachbearbeiterin auch außerhalb der Behörde als Privatperson zu identifizieren und zu belästigen. Generell problematisch kann darüber hinaus beispielsweise auch die Angabe von Vornamen wie Achmed oder Moses sein, die auf die Religionszugehörigkeit eines Bediensteten schließen lassen.

Im - gewissermaßen umgekehrten - praxisrelevanten Fall eines Krankenhauses gelten diese Ausführungen natürlich entsprechend für die zusätzliche Angabe des Nachnamens. So hatte sich beispielsweise im Rahmen einer Eingabe eine Krankenschwester an mich gewandt, um die von der Klinikleitung verfügte Angabe auch des Nachnamens auf den von den Schwestern zu tragenden Namensschildern zu verhindern. Ihre Kolleginnen und sie befürchteten, dass Patienten bei Angabe des vollständigen Namens vermehrt private Kontakte zu knüpfen versuchten.

Ergänzend möchte ich darauf aufmerksam machen, dass auch der Personalrat die Interessen der Bediensteten in diesem Zusammenhang im Mitwirkungsverfahren nach Art. 76, 72 BayPVG gegenüber dem Dienstherrn zum Ausdruck bringen kann.

Abschließend darf ich noch darauf hinweisen, dass der Bayerische Landkreistag (Schreiben vom 28. Mai 2004, Az.: I-047-305/st) meine Auffassung zur Problematik der Namensangabe von Bediensteten in Behörden mit Publikumsverkehr teilt.

19.2 Postöffnung in Behörden

Mit dem datenschutzrechtlichen Dauerbrenner der Postöffnung in Behörden hatte ich mich zuletzt in Nr. 12.2.1 meines 19. Tätigkeitsberichts 2000 und in Nr. 13.3.1 meines 20. Tätigkeitsberichts 2002 auseinander gesetzt. Auch im Berichtszeitraum erreichten mich zu diesem Problemkreis wieder zahlreiche Anfragen und Eingaben. Auffällig war dabei vor allem, dass oftmals immer noch Unklarheit darüber besteht, wann Post als „dienstlicher Eingang" von der zentralen Eingangsstelle zu öffnen ist und wann ein Eingang an den Beschäftigten persönlich gerichtet und diesem daher ungeöffnet zuzuleiten ist. Problematisch gestaltete sich überdies teilweise auch die Behandlung von Poststücken mit erkennbar sensiblem Inhalt, wie Beihilfeunterlagen oder Personalsachen.

Trennung persönliche und dienstliche Eingänge

Nach § 12 Abs. 1 AGO ist es Aufgabe der in jeder Behörde vorzuhaltenden zentralen Eingangsstelle, die an die Behörde gerichteten Sendungen entgegenzunehmen, zu bearbeiten und in den Geschäftsgang zu geben. Unproblematisch sind dabei die allein an die Behörde adressierten Sendungen; hier handelt es sich immer um dienstliche Eingänge. Problematisch sind dagegen die Eingänge, die als Adressierung nicht nur die Behördenanschrift, sondern auch den Namen eines Bediensteten aufweisen. Hier steht die Eingangsstelle vor der Schwierigkeit, dienstliche von privater Post zu trennen. Zusätzlich verschärft wird diese Problematik dadurch, dass die Öffnung von Privatpost eine (strafbewehrte) Verletzung des in Art. 10 GG verankerten Briefgeheimnisses darstellt.

In der Vergangenheit wurden bereits mehrere Versuche unternommen, dieses Problem befriedigend zu lösen. So bestimmte § 9 Abs. 1 Satz 2 Halbsatz 1 der mit Ablauf des 31.12.2000 außer Kraft getretenen Allgemeinen Dienstordnung (ADO), dass Sendungen mit der „persönlichen Anschrift eines Behördenangehörigen" diesem ungeöffnet auszuhändigen sind. Der Wortlaut dieser Vorschrift führte jedoch zu vielfältigen Unklarheiten und Abgrenzungsschwierigkeiten, die durch die Formulierung des ab dem 01.01.2001 geltenden § 12 Abs. 4 Satz 1 AGO behoben werden sollten. Nunmehr waren „Eingänge, die an Beschäftigte persönlich gerichtet sind", diesen unmittelbar und ungeöffnet zuzuleiten. Es zeigte sich jedoch, dass Eingangsstellenmitarbeiter aus dieser Formulierung in der Praxis vielfach - irrtümlich - schlossen, dass unter diese Bestimmung nur Eingänge fallen, die ausdrücklich mit dem Zusatz „persönlich" versehen waren. Nach dem Sinn und Zweck der Regelung des § 12 Abs. 4 Satz 1 AGO war aber neben dem Namen des Beschäftigten ein besonderer Zusatz (wie „persönlich", „vertraulich", „privat" o.ä.) gerade nicht erforderlich.

Um die in der Praxis offenbar einschränkende Wirkung des Wortes „persönlich" zu relativieren, habe ich im Rahmen des Anhörungsverfahrens zur Änderung der AGO dem Staatsministerium des Innern vorgeschlagen, in § 12 Abs. 4 Satz 1 AGO vor dem Wort „persönlich" das Wort „erkennbar" einzufügen. Dieser Vorschlag wurde erfreulicherweise in der ab dem 31.12.2005 geltenden Fassung übernommen. Entscheidend ist nunmehr, ob das Poststück bei einer Gesamtwürdigung aller Umstände als dienstlich oder privat einzustufen ist. So liegt eine persönliche Adressierung zwar grundsätzlich immer dann vor, wenn der Name eines Behördenangehörigen vor der Behördenbezeichnung angeführt ist; im umgekehrten Fall ist allerdings nicht immer auf einen dienstlichen Inhalt zu schließen. In Zweifelsfällen ist daher eher von Privatpost auszugehen. Dies ist auch letztlich aus Sicht des Dienstherrn hinnehmbar, da die Empfänger bei dezentral - also beim Mitarbeiter - eingehenden Sendungen, die dienstliche Mitteilungen enthalten, gemäß § 12 Abs. 4 Satz 3, Abs. 6 Satz 1 AGO die Verantwortung für die ordnungsgemäße Bearbeitung der Eingänge, die Registrierung vorgangsrelevanter Dokumente und die Weitergabe in den Geschäftsgang tragen.

Ich hoffe, dass mit dieser Regelung in Zukunft die meisten Auslegungsprobleme gelöst werden können.

Um die Handhabung dieser Vorschrift in der Praxis zu erleichtern, möchte ich noch beispielhaft folgende Einzelfälle beleuchten:

Adressierung unter Funktionsnennung oder Amtsbezeichnung

Zu dieser Thematik vertrat eine Dienststelle mir gegenüber die Auffassung, dass Briefe, die unter der Nennung der Funktion oder der Amtsbezeichnung an Mitarbeiter gerichtet sind, immer Dienstpost darstellen. Meines Erachtens kann jedoch allein aufgrund der zusätzlichen Nennung der Funktion oder der Amtsbezeichnung des Empfängers eine persönliche Adressierung nicht ausgeschlossen werden. Im Gegenteil kann Grund für die Angabe der Funktion oder der Amtsbezeichnung - vor allem bei häufig vorkommenden Namen, aber auch bei (vermuteten) Namensgleichheiten - gerade sein, den persönlichen Erhalt durch einen bestimmten, möglichst konkret bezeichneten Mitarbeiter sicherzustellen.

Adressierung „zu Händen von"

Die Adressierung mit der Behördenanschrift und dem Zusatz „zu Händen von" ist in der AGO eindeutig geregelt; diese Eingänge stellen Dienstpost dar. Allerdings ist in diesen Fällen gem. § 12 Abs. 4 Satz 4 AGO sicherzustellen, dass die bezeichneten Personen von ihnen Kenntnis erhalten.

Beihilfeunterlagen

In diesem Zusammenhang ist es mir auch ein Anliegen, auf die besonders sorgfältige Behandlung von Eingängen mit sensiblen Daten aufmerksam zu machen. So erreichten mich im Berichtszeitraum einige Beschwerden über die Öffnung von Beihilfeunterlagen durch die Dienststelle. Nach § 17 Abs. 4 Satz 1 der Allgemeinen Verwaltungsvorschrift für Beihilfen in Krankheits-, Pflege- und Geburtsfällen (Beihilfevorschriften - BhV) sind die Beihilfeanträge unter Beifügung der Belege der Festsetzungsstelle vorzulegen. Gemäß den zu dieser Vorschrift erlassenen Vollzugsbestimmungen (VB-BhV) ist eine Vorlage der Beihilfeanträge über die Beschäftigungsdienststelle zwar nicht mehr erforderlich; der Beihilfeberechtigte kann sie jedoch dort in einem verschlossenen Umschlag einreichen und als solche kenntlich machen. Sie sind dann ungeöffnet an die Festsetzungsstelle weiterzuleiten, wo sie nur von dem hierfür besonders bestimmten Bediensteten geöffnet werden dürfen. Entsprechend ist bei der Versendung des Bescheides und der Belege zu verfahren.

Vor dem Hintergrund dieser Bestimmungen dürfen an einen Beihilfeberechtigten gerichtete - als solche nicht nur erkennbare, sondern in der Regel auch mit dem Zusatz „vertraulich“ versehene - Sendungen keinesfalls von der Eingangsstelle geöffnet werden. Kann der Brief der Beihilfestelle im Einzelfall einem konkreten Beschäftigten nicht zugeordnet werden, ist er vielmehr ungeöffnet - mit einem entsprechenden Hinweis versehen - an die Beihilfestelle zurückzuleiten. Eigene Nachforschungen - durch Öffnen der Sendung - darf die Dienststelle dagegen nicht anstellen. Ich weise auch darauf hin, dass Beihilfesendungen in der Dienstelle nicht unberechtigtem Zugriff offen ausgesetzt werden dürfen; sie sind vielmehr dem Empfänger unmittelbar zuzuleiten.

Personalsachen

Besonderes Augenmerk ist bei der Eingangsbehandlung auch auf den Umgang von Personalsachen zu legen. Dabei handelt es sich zwar um Post mit dienstlichem Inhalt; nach Art. 100 a Abs. 1 Satz 1 Halbsatz 2 BayBG sind Personalaktendaten jedoch vertraulich zu behandeln und vor unbefugter Einsicht zu schützen. Eingänge mit gekennzeichnet personalaktenrechtlich relevantem Inhalt dürfen deshalb nur von den dafür zuständigen Bediensteten geöffnet werden.

Vor diesem Hintergrund habe ich dem Staatsministerium des Innern im Rahmen des Anhörungsverfahrens zur Änderung der AGO vorgeschlagen, eine entsprechende Regelung in § 12 Abs. 4 AGO aufzunehmen. In § 12 Abs. 4 Satz 5 AGO ist nunmehr ausdrücklich festgelegt, dass Eingänge, die als Personalsache gekennzeichnet sind, nur von den zuständigen Personal verwaltenden Stellen, nicht aber von der Eingangsstelle geöffnet werden dürfen. Die Behörde hat zudem durch geeignete organisatorische Maßnahmen sicherzustellen, dass eine unbefugte Einsichtnahme durch Dritte unterbleibt.

19.3 Datenschutz bei Zeiterfassungsdaten

Zum Problemkreis des Datenschutzes bei Zeiterfassungsdaten hatte ich mich zuletzt in den Nrn. 13.1.2 und 13.1.3 meines 20. Tätigkeitsberichts 2002 geäußert. Auch im Berichtszeitraum erreichten mich insoweit wieder zahlreiche Anfragen und Eingaben. Meinem Eindruck nach bestehen in der Praxis vor allem Unklarheiten bei der Einführung und Anwendung von elektronischen Zeiterfassungssystemen sowie im Hinblick auf die Einsichtsberechtigungen und die Aufbewahrungsfristen für Zeiterfassungsdaten.

Allgemeines

Unterlagen und Dateien zur Zeiterfassung sind gemäß Art. 100 a Abs. 1 Satz 2 Halbsatz 1 BayBG grundsätzlich den Personalaktendaten zuzuordnen; sie können gem. Art. 100 a Abs. 2 Sätze 1 und 2 BayBG in einem eigenen Teilakt bei der für diesen Aufgabenbereich zuständigen Stelle der Behörde geführt werden. Nach Art. 100 a Abs. 1 Satz 1 Halbsatz 2 BayBG sind sie vertraulich zu behandeln und vor unbefugter Einsicht zu schützen. Personalaktendaten dürfen gemäß Art. 100 a Abs. 1 Satz 3 BayBG nur für Zwecke der Personalverwaltung oder der Personalwirtschaft verwendet werden, es sei denn, der Beamte willigt in die anderweitige Verwendung ein; diese Verwendungsbeschränkung gilt gem. Art. 100 h Abs. 1 Satz 1 BayBG auch bei der automatisierten Verarbeitung und Nutzung von Personalaktendaten.

In diesem Zusammenhang weise ich darauf hin, dass meiner Auffassung nach die den allgemeinen datenschutzrechtlichen Vorschriften gem. Art. 2 Abs. 7 BayDSG vorgehenden Regelungen über das Personalaktenrecht der Beamten (Art. 100 ff. BayBG) entsprechend auch auf die nicht verbeamteten Beschäftigten des öffentlichen Dienstes anzuwenden sind, da sie allgemein gültige Schutzprinzipien für alle öffentlichen Bediensteten enthalten.

Einführung eines elektronischen Zeiterfassungssystems

Die Einführung eines Datenverarbeitungssystems zur Erfassung und Auswertung von Arbeitszeitdaten berührt neben datenschutzrechtlichen auch personalvertretungsrechtliche Fragen. So hat der Personalrat gem. Art. 75 a Abs. 1 Nr. 1 BayPVG bei Einführung, Anwendung und erheblicher Änderung technischer Einrichtungen zur Überwachung des Verhaltens oder der Leistungen des Beschäftigten mitzubestimmen.

Hierbei ist zunächst allgemein darauf hinzuweisen, dass nach der Rechtsprechung eine Leistungs- oder Verhaltenskontrolle der Beschäftigten nicht beabsichtigt sein muss; vielmehr reicht es aus, dass die technische Einrichtung zu diesen Kontrollen an sich geeignet ist. Im vorliegenden Zusammenhang ist festzustellen, dass die in elektronischen Zeiterfassungssystemen erfolgenden Aufzeichnungen jedenfalls zur Verhaltens- und Leistungskontrolle der Bediensteten (zumindest) geeignet sind; die Einführung eines solchen Datenverarbeitungssystems unterliegt somit der zwingenden Mitbestimmung des Personalrats.

Nicht nur um einer unverhältnismäßigen Beeinträchtigung der Persönlichkeitsrechte der Betroffenen schon von vornherein entgegenzuwirken, sondern vor allem um die wünschenswerte innerbehördliche Transparenz bei allen Beteiligten herzustellen, empfehle ich in derartigen Fallgestaltungen, eine Dienstvereinbarung zwischen der Dienststelle und dem Personalrat abzuschließen (vgl. Art. 73 BayPVG). In dieser Dienstvereinbarung sollte insbesondere geregelt werden, welche Daten aufgezeichnet werden, wie lange die aufgezeichneten Daten gespeichert werden, welche Personen Zugriff auf die gespeicherten Zeiterfassungsdaten haben und wer welche Auswertungen wann veranlassen kann.

Nicht vergessen werden sollte auch, rechtzeitig vor dem Einsatz eines elektronischen Zeiterfassungssystems für die datenschutzrechtliche Freigabe des Verfahrens gem. Art. 26 BayDSG zu sorgen.

Zugang zu Zeiterfassungsdaten

Vorweg ist festzuhalten, dass die Einsichtnahme in Zeiterfassungsdaten eine Datennutzung im Sinne des Art. 4 Abs. 7 BayDSG darstellt, da es sich um die Weitergabe von Daten innerhalb der speichernden Stelle (vgl. Art. 4 Abs. 9 BayDSG) handelt.

Nach Art. 100 a Abs. 3 BayBG dürfen Zugang zum Personalakt - hier zu den Zeiterfassungsdaten - nur Beschäftigte haben, die im Rahmen der Personalverwaltung mit der Bearbeitung von Personalangelegenheiten beauftragt sind und nur soweit dies zu Zwecken der Personalverwaltung oder der Personalwirtschaft erforderlich ist; dies gilt auch für den Zugang im automatisierten Abrufverfahren. Zur Wahrung der Vertraulichkeit des Personalakts und damit zum Schutz des Persönlichkeitsrechtes der Beschäftigten wird also durch diese gesetzliche Regelung der Zugang zu Personalaktendaten innerhalb der personalaktenführenden Stelle in doppelter Hinsicht beschränkt: Zum einen dürfen Personalaktendaten nur bestimmten Personen überhaupt zugänglich gemacht werden, und zum anderen dürfen diese Personen den Personalakt nur seinem bestimmungsgemäßen Gebrauch entsprechend nutzen.

In Ausfüllung dieses gesetzlichen Rahmens bestimmt Nr. 7 der Verwaltungsvorschriften zu Art. 80 BayBG - Gleitende Arbeitszeit - (Bekanntmachung des Staatsministeriums der Finanzen betreffend Verwaltungsvorschriften zum Bayerischen Beamtengesetz - VV-BayBG - vom 21.02.2002, StAnz. Beil. Nr. 4/2002), dass der Dienststellenleiter die Arbeitszeiterfassung und die Einhaltung der Dienstvereinbarung durch geeignete Maßnahmen zu überwachen hat. Er kann sich hierzu jederzeit Buchungsübersichten oder Arbeitszeitkarten vorlegen lassen. Eine wirksame Kontrolle der handschriftlichen Aufzeichnungen ist sicherzustellen.

Nach Nr. 9 VV zu Art. 80 BayBG kann der Dienststellenleiter die ihm nach den vorstehenden Verwaltungsvorschriften zugewiesenen Befugnisse und Verpflichtungen allgemein oder im Einzelfall delegieren, soweit dies zweckmäßig erscheint. In der Praxis wird hierzu meist ein Bediensteter zum sog. Arbeitszeitbeauftragten bestellt. Aus datenschutzrechtlicher Sicht zwar nicht unbedingt wünschenswert, aber möglich und zulässig ist es auch, dem (unmittelbaren) Vorgesetzten die Aufgabe der Kontrolle der Arbeitszeiterfassung zu übertragen.

Soweit Datennutzungen über den dargestellten Umfang hinausgehen, sind sie nur mit der freiwilligen und informierten Einwilligung der Bediensteten (Art. 100 a Abs. 1 Satz 3 BayBG, Art. 15 Abs. 2 bis 4 BayDSG) zulässig.

Ergänzend darf ich zur Nutzung von Personaldaten im Rahmen der Budgetierung auf die Nr. 12.2 meines 18. Tätigkeitsberichts 1998 hinweisen.

Einsichtnahme durch den Personalrat

Aus datenschutzrechtlicher Sicht habe ich mich bereits allgemein zu den Informations- und Einsichtsrechten der Personalvertretung in Nr. 13.4 meines 20. Tätigkeitsberichts 2002 geäußert. Bereits dort habe ich festgestellt, dass der Personalrat im Verhältnis zur Dienststelle kein „Dritter“ im Sinne des Art. 4 Abs. 10 BayDSG, sondern ein datenschutzrechtlich unselbstständiger Teil der speichernden Stelle ist (vgl. Art. 4 Abs. 9 BayDSG). Dies bedeutet aber nicht, dass dem Personalrat schrankenlos Zugang zu sämtlichen in der Behörde verarbeiteten personenbezogenen Daten einzuräumen ist. Vielmehr ist jegliche Datennutzung an den einschlägigen Bestimmungen des BayDSG oder vorgehenden spezialgesetzlichen Regelungen (vgl. Art. 2 Abs. 7 BayDSG) zu messen.

Der Informationsanspruch des Personalrats nach Art. 69 Abs. 2 BayPVG ist als „besondere Rechtsvorschrift über den Datenschutz“ im Sinne des Art. 2 Abs. 7 BayDSG anzusehen. Nach Art. 69 Abs. 2 Sätze 1 und 2 BayPVG ist der Personalrat zur Durchführung seiner Aufgaben rechtzeitig und umfassend

zu unterrichten; ihm sind die hierfür erforderlichen Unterlagen zur Verfügung zu stellen. Ein Anspruch der Personalvertretung auf umfassende und rechtzeitige Information besteht also nur insoweit, als sie Auskünfte und dergleichen von Seiten der Dienststelle benötigt, um die ihr obliegenden Aufgaben erfüllen und ihre Beteiligungsrechte rechtzeitig und uneingeschränkt wahrnehmen zu können. Die Personalvertretung ist aber kein Kontrollorgan der Verwaltung, dem es obliegt, die Aufgabenerfüllung und den inneren Betrieb der Dienststelle allgemein zu überwachen. Daher ist ein generelles Einsichtsrecht des Personalrats in die Zeiterfassungsdaten der Beschäftigten aus datenschutzrechtlicher Sicht abzulehnen. Ein pauschales Auskunftsverlangen unabhängig von einem bestimmten Anlass und ohne Bezug zu einer konkreten Aufgabe ist vom Informationsrecht des Personalrats nicht gedeckt.

Einer generellen Einsichtnahme in die Zeiterfassungsunterlagen durch den Personalrat liegen auch keine Zwecke der Personalverwaltung oder der Personalwirtschaft zugrunde. Zudem ist die Personalvertretung nicht im Sinne von Art. 100 a Abs. 3 BayBG „mit der Bearbeitung von Personalangelegenheiten“ beauftragt. Darüber hinaus ist in diesem Zusammenhang auf Art. 69 Abs. 2 Satz 4 BayPVG hinzuweisen, nach dem Personalakten nur mit schriftlicher Zustimmung der Beschäftigten und nur von einem von ihm bestimmten Mitglied des Personalrats eingesehen werden dürfen.

Der Personalrat ist deshalb verpflichtet, bei Inanspruchnahme seines Informationsrechts den Dienststellenleiter jeweils darüber zu unterrichten, aus welchem bestimmten Anlass er die Vorlage welcher Unterlagen verlangt und aus welchen Gründen er dies zur Erfüllung seiner Aufgaben für erforderlich hält, soweit sich die Notwendigkeit der Information nicht schon aus der Sache selbst ergibt. Jedenfalls verlangt es der Grundsatz der Verhältnismäßigkeit, an einen - im Rahmen der Erforderlichkeit der Unterrichtung zu fordernden - sachlich berechtigten Anlass für ein Informationsbegehren des Personalrats strenge Anforderungen zu stellen, wenn der Persönlichkeitsschutz nach der Intensität der Betroffenheit dies erfordert.

(Vgl. zum Ganzen auch Ballerstedt/Schleicher/Faber/Eckinger, Bayerisches Personalvertretungsgesetz, Kommentar, München, Stand: 2006, Art. 69 BayPVG Rdnr. 32 und 113 bis 117 sowie Wilde/Ehmann/Niese/Knoblauch, Bayerisches Datenschutzgesetz, Kommentar, München, Stand: 2006, Teil C Handbuch XIII.7.)

Aufbewahrungsfristen

Nach Nr. 3.5.1 der VV zu Art. 80 BayBG ist das im Zusammenhang mit der Zeiterfassung anfallende Zahlenmaterial längstens zwei Jahre vorzuhalten, sofern im Einzelfall nicht eine längere Frist erforderlich ist. Die Frist beginnt mit Ablauf des jeweiligen Abrechnungsmonats. Art. 12 BayDSG ist zu beachten; danach sind personenbezogene Daten in Dateien oder Akten zu löschen, wenn ihre Kenntnis zur rechtmäßigen Erfüllung der im Zuständigkeitsbereich der Beschäftigungsbehörde liegenden Aufgaben nicht mehr erforderlich ist. Soweit im Rahmen der Zeiterfassung erhobene Daten auch für Zwecke der Verwaltung von Fehlzeiten verwendet werden, ist für die Aussonderung dieser Daten die Fünf-Jahres-Frist des Art. 100 g Abs. 2 Satz 1 BayBG zu beachten.

Abschließend hoffe ich, mit diesen Hinweisen zu einem datenschutzgerechten Umgang mit Zeiterfassungsdaten in der Praxis beitragen zu können.

19.4 Neuordnung des Bayerischen Disziplinarrechts

Im Herbst 2005 hat der Landtag eine Neuordnung des Bayerischen Disziplinarrechts beschlossen. In Ablösung der Bayerischen Disziplinarordnung (BayDO) ist so am 1. Januar 2006 das Bayerische Disziplinargesetz (BayDG) in Kraft getreten. Nachdem der Oberste Rechnungshof in seinem Jahresbericht 2003 eine übermäßige Dauer förmlicher Disziplinarverfahren festgestellt und bemängelt hatte, ist es Ziel dieser Neuordnung, das Disziplinarrecht zu vereinfachen und die Verfahren zu straffen. In allen Verfahrensstadien gilt nun der Grundsatz der Beschleunigung, der durch entsprechende verfahrensrechtliche Erleichterungen umgesetzt wird.

Im Rahmen meiner Beteiligung im Gesetzgebungsverfahren konnte ich bei diesem Reformvorhaben auch zahlreiche Verbesserungen in datenschutzrechtlicher Hinsicht erreichen. Im Einzelnen sind insbesondere folgende Punkte zu erwähnen:

Die der personalaktenrechtlichen Tilgungsvorschrift des Art. 100 f BayBG als gesetzliche Spezialvorschrift vorgehende, bisher in Art. 109 BayDO enthaltene disziplinarrechtliche Regelung des Verwertungsverbots und der Entfernung aus der Personalakte ist nun Gegenstand des Art. 17 BayDG.

Es ist zwar bedauerlich, dass der Gesetzgeber von der ursprünglich in Anlehnung an § 16 Bundesdisziplinargesetz beabsichtigten teilweisen Verkürzung der Fristen zur Verwertung einer verhängten Disziplinarmaßnahme wieder Abstand genommen hat. Da jedoch in Art. 17 Abs. 1 BayDG die Disziplinarmaßnahme der „Zurückstufung“ - so die Begründung des Gesetzentwurfs - „auch mit Blick auf den Schutz des Persönlichkeitsrechts und des informationellen Selbstbestimmungsrechts des Beamten oder der Beamtin erstmalig in das Verwertungsverbot aufge-

nommen worden“ ist, stellt die Neuregelung des Art. 17 Abs. 1 BayDG insgesamt eine durchaus beachtliche Verbesserung in datenschutzrechtlicher Hinsicht dar.

Die in Art. 17 Abs. 3 BayDG normierte Abkehr vom bisherigen Antragsverfahren hin zur Entfernung und Vernichtung von Eintragungen in der Personalakte über die Disziplinarmaßnahme nach Eintritt des Verwertungsverbots von Amts wegen (bei Einräumung eines Widerspruchsrechts für den Beamten oder die Beamtin) habe ich ebenso wie den generellen Wegfall der gesonderten Aufbewahrung von Disziplinarunterlagen außerhalb des Personalakts aus datenschutzrechtlicher Sicht ausdrücklich begrüßt. Erfreulich ist zudem, dass es künftig - im Gegensatz zur bisherigen Regelung - auch möglich sein wird, Eintragungen über die Disziplinarmaßnahme „Kürzung der Dienstbezüge“ aus dem Personalakt zu entfernen und zu vernichten, anstatt diese Unterlagen dauerhaft gesondert vorzuhalten.

Nach Art. 17 Abs. 3 Satz 2 Halbsatz 1 BayDG verbleiben allerdings Rubrum und Tenor eines eine „Zurückstufung“ aussprechenden Urteils aus besoldungs- und versorgungsrechtlichen Gründen (so die Begründung des Gesetzentwurfs) auch nach Eintritt des Verwertungsverbots im Personalakt. Diesbezüglich habe ich im Gesetzgebungsverfahren darauf aufmerksam gemacht, dass ausweislich des klaren Wortlautes des Art. 17 Abs. 1 Satz 2 BayDG der Beamte oder die Beamtin nach Eintritt des Verwertungsverbots als von der „Zurückstufung“ nicht betroffen gilt. Da aber im Falle eines Widerspruchs des Beamten oder der Beamtin das Verwertungsverbot gem. Art. 17 Abs. 3 Satz 4 Halbsatz 2 BayDG bei den Eintragungen zu vermerken ist, habe ich schon aus Gründen der Transparenz, aber nicht zuletzt um Fehlinterpretationen aufgrund der Systematik - kein Vermerk = kein Verwertungsverbot - von vornherein auszuschließen, vorgeschlagen, auf das Verwertungsverbot auch im Falle des Art. 17 Abs. 3 Satz 2 BayDG noch einmal ausdrücklich im Gesetz selbst hinzuweisen. Aus datenschutzrechtlicher Sicht hat der Gesetzgeber diesem Vorschlag erfreulicherweise durch die Einfügung des Art. 17 Abs. 3 Satz 2 Halbsatz 2 BayDG Rechnung getragen.

Schließlich wird durch die neue Regelung des Art. 17 Abs. 5 BayDSG im Wege einer Verweisung auf Art. 100 f Abs. 1 Satz 1 Nr. 2 BayBG sichergestellt, dass die auf Grund eines Disziplinarvorgangs in die Personalakte aufgenommenen missbilligenden Äußerungen unter den gleichen Voraussetzungen entfernt und vernichtet werden wie diejenigen, die ohne einen vorherigen Disziplinarvorgang aufgenommen wurden. Dass im Rahmen der Neuordnung des Bayerischen Disziplinarrechts die maßgebliche Frist von drei auf zwei Jahre verkürzt wurde, habe ich aus datenschutzrechtlicher Sicht ausdrücklich befürwortet.

Bei Einleitung oder Ausdehnung eines Disziplinarverfahrens ist der Beamte oder die Beamtin nach Art. 22 Abs. 1 Satz 3 BayDG u.a. auch darauf hinzuweisen, dass es ihm oder ihr freisteht, sich mündlich oder schriftlich zu äußern oder nicht zur Sache auszusagen und sich jederzeit eines Bevollmächtigten oder Beistands zu bedienen. In Art. 22 Abs. 3 Satz 1 BayDG ist nun erstmals ein Verwertungsverbot für den Fall normiert, dass diese Belehrung unterblieben oder unrichtig erfolgt ist. Dies habe ich aus datenschutzrechtlicher Hinsicht begrüßt.

Nach der Begründung des Gesetzentwurfs zu Art. 31 BayDG (Innerdienstliche Informationen) werden in dieser Vorschrift „im Lichte des Grundrechts auf informationelle Selbstbestimmung erstmals die Vorlage von Personalakten im Disziplinarverfahren sowie die Weitergabe von Mitteilungen zwischen den Dienststellen über Disziplinarvorgänge in Abwägung der widerstreitenden Interessen umfassend geregelt. Im Verhältnis zu Art. 100 e BayBG ist Art. 31 BayDG die speziellere Norm.“

In Anbetracht der Vertraulichkeit von Personalakten wie von Disziplinarunterlagen, die sich auch auf den Verkehr der Behörden untereinander bezieht, sowie der in Art. 100 a Abs. 3 und Art. 100 e Abs. 1 und 4 BayBG getroffenen Regelungen über den Zugang zum Personalakt, die Vorlage von Personalakten und die Auskunft daraus halte ich die in Art. 31 Abs. 1 und 2 BayDG für den Informationsaustausch vorgesehene Maßgabe der Erforderlichkeit zur Durchführung des Disziplinarverfahrens grundsätzlich mit dem Recht auf informationelle Selbstbestimmung für vereinbar. Denn auch Art. 100 a Abs. 3 und Art. 100 e Abs. 1 BayBG beschränken die Nutzung bzw. die Vorlage auf die erforderlichen Zwecke.

In Art. 31 Abs. 2 Fall 3 BayDG wird aber neben den für mich nachvollziehbaren Fällen einer künftigen Übertragung von Aufgaben oder Ämtern an den Beamten oder die Beamtin (Art. 31 Abs. 2 Fall 2 BayDG) ein Informationsaustausch zwischen den Dienststellen eines oder verschiedener Dienstherren sowie zwischen den Teilen einer Dienststelle auch zugelassen, wenn dieser „im Einzelfall aus besonderen dienstlichen Gründen unter Berücksichtigung der Belange des Beamten oder der Beamtin oder anderer Betroffener erforderlich ist“. Ich habe Zweifel, ob in Anbetracht der in Art. 31 Abs. 2 Fall 2 BayDG bereits geregelten Fälle für die Regelung des Art. 31 Abs. 2 Fall 3 BayDG in der Praxis überhaupt noch ein eigenständiger Anwendungsbereich verbleibt. Jedenfalls muss diese Regelung im Hinblick auf das Recht auf informationelle Selbstbestimmung sehr eng ausgelegt werden. Ich habe mich im Gesetzgebungsverfahren daher dafür ausgesprochen, die Regelung

des Art. 31 Abs. 2 Fall 3 BayDG entweder ganz zu streichen oder jedenfalls deren restriktive Interpretation in der Begründung klarzustellen sowie - zumindest in der Begründung - einen derartigen Einzelfall (beispielhaft) zu konkretisieren. Der Gesetzgeber hat darauf immerhin durch Aufnahme folgender Hinweise in die Gesetzesbegründung reagiert: „Die Weitergabe von Mitteilungen nach Absatz 2 „aus besonderen dienstlichen Gründen“ ist unter datenschutzrechtlichen Gesichtspunkten restriktiv zu handhaben. Sie kann z.B. aus Gründen der Dienstaufsicht erforderlich sein.“

Insgesamt bin ich zuversichtlich, dass die Neuordnung des Bayerischen Disziplinarrechts auch in datenschutzrechtlicher Sicht ihr Ziel erreicht, das Disziplinarrecht zu vereinfachen, zu straffen und insgesamt transparenter zu gestalten.

20 Medien und Telekommunikation

20.1 Richtlinie über die Nutzung von Internet und E-Mail in der bayerischen Staatsverwaltung

Internet und E-Mail gehören inzwischen zu den unverzichtbaren Arbeitsmitteln in der täglichen Verwaltungspraxis. Sie fördern insbesondere eine effiziente interne und externe Kommunikation sowie eine breite und beschleunigte Informationsbeschaffung. Ohne diese elektronischen Informations- und Kommunikationsdienste könnten heute zahlreiche Aufgaben der Staatsverwaltung nicht mehr sach- und termingerecht erledigt werden. Die Nutzung von Internet und E-Mail am Arbeitsplatz führt allerdings nicht nur zur Erleichterung der täglichen Arbeit, sondern auch zu neuen Problemen im Verhältnis Mitarbeiter und Dienststelle. Diese (arbeits-)tägliche Problematik bildet nach wie vor einen Schwerpunkt meiner Beratungstätigkeit. Ich weise darauf hin, dass ich hierzu bereits in Nr. 21.1 meines 21. Tätigkeitsberichtes 2004 aus datenschutzrechtlicher Sicht umfangreiche Hinweise gegeben habe.

Im Berichtszeitraum hat die Zentrale IuK-Leitstelle im Staatsministerium des Innern die „Richtlinie über die Nutzung von Internet und E-Mail in der bayerischen Staatsverwaltung“ (BayITR-05) erlassen und im Behördennetz bekannt gemacht (abrufbar unter http://www.bybn.de/RBIS/IUK/IUK-RICHTLINIEN/bayitr-05.pdf). Ziel dieser Richtlinie ist es, einheitliche, ressortübergreifende Rahmenbedingungen für den Einsatz des Internet zur Abfrage von Web-Diensten sowie zur Nutzung von E-Mail-Diensten am Arbeitsplatz in der Staatsverwaltung festzulegen. Im wesentlichen regelt die Richtlinie die allgemeinen Voraussetzungen, unter denen die entscheidungsbefugten Stellen die Privatnutzung gestatten dürfen.

Im Rahmen meiner Beteiligung im Erlassverfahren konnte ich zahlreiche Verbesserungen in datenschutzrechtlicher Hinsicht erreichen. Im Einzelnen sieht die Richtlinie insbesondere Folgendes vor:

Der dienstlich bereitgestellte Internetzugang darf zur Nutzung von Angeboten im World-Wide-Web (WWW-Dienst) sowie zum Senden und Empfangen von E-Mails (E-Mail-Dienst) grundsätzlich nur für dienstliche Zwecke verwendet werden (Nr. 3 Abs. 1 der Richtlinie).

Allerdings können gem. Nr. 3 Abs. 2 der Richtlinie die obersten Dienstbehörden oder die von ihnen ermächtigten Behörden die Nutzung des WWW-Dienstes auch für private Zwecke erlauben, sofern sie diese von der Einhaltung nachfolgender Nutzungsbedingungen abhängig machen:

- Die Beschäftigten, die den Internetzugang privat nutzen wollen, haben eine eigenhändig unterzeichnete Einwilligungserklärung gemäß dem der Richtlinie beigefügten Muster abzugeben; diese ist zum Personalakt zu nehmen. Mit Unterzeichnung dieser Erklärung erteilt der Bedienstete - jederzeit widerruflich - sein Einverständnis mit der Protokollierung auch seiner privaten Internetzugriffe zur Durchführung einer stichprobenartigen oder missbrauchsverdachtsabhängigen Kontrolle seiner Netzaktivitäten.

- Die Privatnutzung ist auf einen geringfügigen Umfang zu beschränken. Hiervon umfasst ist auch die Speicherung privater Daten und Downloads, sofern nicht die Sicherheit der IT-Systeme gefährdet ist.

- Die Privatnutzung darf nicht zur Verfolgung gewerblicher oder geschäftsmäßiger Interessen erfolgen; die Privatnutzung für Rechtsgeschäfte des täglichen Lebens kann zugelassen werden.

- Die Privatnutzung darf nicht zu Zwecken erfolgen, die die Interessen oder das Ansehen einer Behörde oder des Freistaates Bayern in der Öffentlichkeit oder die Sicherheit des Behördennetzes beeinträchtigen können. Insbesondere haben der Abruf kostenpflichtiger Internetseiten, das Abrufen, Verbreiten oder Speichern von Inhalten, die gegen persönlichkeitsrechtliche, datenschutzrechtliche, lizenz- und urheberrechtliche oder strafrechtliche Bestimmungen verstoßen, das Abrufen, Verbreiten oder Speichern von beleidigenden, verleumderischen, verfassungsfeindlichen, rassistischen, sexistischen, gewaltverherrlichenden oder pornografischen Äußerungen oder Abbil-

dungen sowie Aktivitäten, die sich gegen die Sicherheit von IT-Systemen richten (z.B. Angriffe auf externe Webserver), zu unterbleiben.

In diesem Zusammenhang habe ich bereits im Ressortanhörungsverfahren meine Zweifel zum Ausdruck gebracht, inwieweit mit dem bloßen Abruf von für den Privatnutzer kostenpflichtigen, den übrigen Nutzungsbedingungen aber entsprechenden Internetseiten Zwecke verfolgt werden sollten, die die Interessen oder das Ansehen einer Behörde oder des Freistaates Bayern in der Öffentlichkeit beeinträchtigen könnten. Aus personaldatenschutzrechtlicher Sicht besteht hier vielmehr die Gefahr, dass eine wörtliche Anwendung dieser Verbotsbestimmung mit dem Sinn und Zweck der Richtlinie nicht mehr in Einklang zu bringen ist. So stellt beispielsweise das Herunterladen eines kostenpflichtigen, privat interessierenden und privat bezahlten, wissenschaftlichen Artikels von www.spiegel.de vom Wortlaut her einen Verstoß gegen dieses Nutzungsverbot dar, der aber sicherlich nicht dem Sinn und Zweck der Richtlinie widerspricht.

Die Privatnutzung darf ferner nur gestattet werden, solange und soweit die uneingeschränkte Verfügbarkeit der betroffenen IT-Systeme für dienstliche Zwecke vorrangig gewährleistet bleibt und keine haushaltsrechtlichen Belange entgegenstehen (Nr. 3 Abs. 3 der Richtlinie).

Wird die Privatnutzung des Internet erlaubt, so stellt dies eine freiwillige Leistung des Dienstherrn dar. Aus der Gestattung der Privatnutzung kann kein Rechtsanspruch der Beschäftigten hergeleitet werden. Die Gestattung der Privatnutzung kann jederzeit durch einseitige Erklärung widerrufen werden. (Nr. 3 Abs. 4 der Richtlinie)

Für die Nutzung des dienstlich bereitgestellten E-Mail-Dienstes zu privaten Zwecken gelten diese Bestimmungen entsprechend. Generell unzulässig sind die Verwendung des intern genutzten Anmeldenamens (Benutzerkennung) und Anmeldepasswortes im Internet und der dienstlichen E-Mail-Adresse in öffentlichen Chat-Räumen und ähnlichen öffentlichen Meinungsforen. Es ist sicherzustellen, dass die Interessen oder das Ansehen einer Behörde oder des Freistaats Bayern in der Öffentlichkeit oder die Sicherheit des Behördennetzes durch die Privatnutzung nicht beeinträchtigt werden. Die Privatnutzung von E-Mail-Diensten über private Webmail-Angebote ist im Rahmen der erlaubten Privatnutzung der Web-Dienste möglich. (Nr. 3 Abs. 5 der Richtlinie)

Das zunächst im Richtlinienentwurf vorgesehene ausnahmslose Verbot der Privatnutzung der dienstlichen E-Mail-Adresse wurde erfreulicherweise auch aufgrund meiner Kritik fallengelassen. Ein solches Verbot ist nämlich aus datenschutzrechtlicher Sicht problematisch: So kann beispielsweise der Bedienstete mangels Einflussmöglichkeit nicht verhindern, dass ihm ein Dritter - anlasslos und/oder sogar ohne sein Einverständnis - eine private E-Mail an seine dienstliche - zudem meist leicht erschließbare ! - E-Mail-Adresse sendet. Mit Eingang der E-Mail liegt aber bereits eine Nutzung der dienstlichen E-Mail-Adresse zu privaten Zwecken vor. Abgesehen davon würde ein solches Nutzungsverbot auch nicht für den Dritten gelten. Somit unterliegen beim Bediensteten eingehende private E-Mails in jedem Fall dem in §§ 88 ff. TKG normierten Fernmeldegeheimnis - über das der Bedienstete auch nicht verfügen kann. Eingehende E-Mails können damit letztlich von der Behörde nicht überprüft werden.

Weiter können nach Nr. 4 Abs. 1 Satz 1 der Richtlinie zur Überwachung der Einhaltung der Nutzungsregelungen zu dienstlichen und privaten Zwecken unter Beachtung des Verhältnismäßigkeitsprinzips sowie der personalvertretungs- und datenschutzrechtlichen Vorschriften und Vereinbarungen Missbrauchskontrollen (Stichproben- und Verdachtskontrollen) durchgeführt werden.

(Rahmen-)Regelungen über die Protokollierung der Internetzugriffe enthielt der Richtlinienentwurf allerdings zunächst nicht. Damit war insbesondere unklar, welche Daten protokolliert werden sollen, wie lange die protokollierten Daten gespeichert werden sollen und wer Zugriff auf diese gespeicherten Daten hat; hierauf habe ich auch im Ressortanhörungsverfahren hingewiesen. In diesem Zusammenhang habe ich zudem darauf aufmerksam gemacht, dass die Protokollierung der Internetzugriffe an der zentralen Firewall des Behördennetzes beim Landesamt für Statistik und Datenverarbeitung vom Staatsministerium des Innern mit Schreiben vom 22. Februar 2001 datenschutzrechtlich freigegeben wurde (im Behördennetz abrufbar unter http://www.stmi.bybn.de/datenschutz/Internetfreigabe-Landesamt.pdf). Aufgrund meiner Anregung erfolgte schließlich sowohl in Nr. 4 Abs. 1 Satz 2 der Richtlinie als auch in der Muster-Einwilligungserklärung ein ausdrücklicher Hinweis auf die Bestimmungen dieser Freigabe.

Die Behörden, die die Privatnutzung erlauben, tragen gem. Nr. 4 Abs. 2 der Richtlinie die Verantwortung für die Einhaltung der Regelungen der Richtlinie; die persönliche Verantwortlichkeit der Beschäftigten bleibt hiervon allerdings unberührt. Werden Vorkommnisse bekannt, die geeignet sind, die Interessen oder das Ansehen des Freistaats Bayern zu beeinträchtigen, so hat die verantwortliche Stelle umgehend geeignete Maßnahmen zur Aufklärung der Vorkommnisse zu ergreifen und erforderlichenfalls un-

verzüglich für Abhilfe zu sorgen (Nr. 4 Abs. 3 der Richtlinie).

Im Rahmen der Ressortanhörung habe ich zuletzt darauf aufmerksam gemacht, dass in jedem Falle - gleich ob Privatnutzung erlaubt wird oder nicht - die Durchführung von Protokollierungsmaßnahmen nach Art. 75 a Abs. 1 Nr. 1 BayPVG zwingend der Mitbestimmung des Personalrats unterliegt. Aus datenschutzrechtlicher Sicht ist hierzu der Abschluss einer Dienstvereinbarung gem. Art. 73 Abs. 1 Satz 1 BayPVG empfehlenswert, in der die Fragen der Protokollierung, Auswertung und Durchführung von Kontrollen eindeutig geregelt werden. Erfreulicherweise wird aufgrund meiner Anregung nunmehr in Nr. 4 Absatz 4 der Richtlinie ausdrücklich auf diesen personalvertretungsrechtlichen Aspekt hingewiesen.

In diesem Zusammenhang darf ich nochmals darauf hinweisen, dass ich auf meiner Homepage umfangreiche Hinweise zur privaten Internet- und E-Mail-Nutzung eingestellt habe.

20.2 Kein Auskunftsanspruch gegen Internet-Provider

Das Bundesministerium der Justiz hat am 6. Januar 2006 den Referentenentwurf eines „Gesetzes zur Verbesserung der Durchsetzung von Rechten des geistigen Eigentums“ vorgelegt, der in Umsetzung der „Richtlinie 2004/48/EG des Europäischen Parlaments und des Rates vom 29. April 2004 zur Durchsetzung der Rechte des geistigen Eigentums“ (IPR-Enforcement-Richtlinie) stärkere Instrumente zum Schutz des Urheberrechts und anderer gewerblicher Schutzrechte in das nationale Recht einführen soll. Der Gesetzentwurf gesteht den Rechteinhabern in bestimmten Fällen Auskunftsansprüche auch gegenüber unbeteiligten Dritten zu, die selbst keine Urheberrechtsverletzungen begangen haben. So sollen etwa Internet-Provider auch über - durch das Fernmeldegeheimnis gem. Art. 10 GG geschützte - Daten ihrer Nutzerinnen und Nutzer zur Auskunft verpflichtet werden. Damit sollen beispielsweise Anbieter und Nutzer illegal kopierter Musik- oder Videodateien oder Software leichter ermittelt werden können.

Gegen die Einräumung derartiger Auskunftsansprüche gegenüber unbeteiligten Dritten hat sich die 71. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 16./17. März 2006 in Magdeburg mit der einstimmig gefassten Entschließung „Keine Aushöhlung des Fernmeldegeheimnisses im Urheberrecht“ (siehe Anlage Nr. 16) gewandt. Nach Auffassung der Datenschutzkonferenz lassen die europarechtlichen Vorgaben den Mitgliedstaaten zugunsten des Datenschutzes so viel Spielraum, dass Eingriffe in das Fernmeldegeheimnis vermieden werden können. Nachdem das grundrechtlich geschützte Fernmeldegeheimnis in den letzten Jahren immer stärker und in immer kürzeren Abständen für Zwecke der Strafverfolgung und der Geheimdienste eingeschränkt wurde, soll es nun auch erstmals zugunsten privater wirtschaftlicher Interessen nicht unerheblich weiter eingeschränkt werden. Die Datenschutzkonferenz befürchtet, dass damit ähnliche Begehrlichkeiten weiterer privater Interessengruppen geweckt werden. Sie appelliert deshalb an den Gesetzgeber, auf eine weitere Einschränkung des Fernmeldegeheimnisses - erstmals zur Durchsetzung privater wirtschaftlicher Interessen - zu verzichten. Es wäre völlig unakzeptabel, wenn Daten, deren zwangsweise Speicherung mit der Abwehr terroristischer Gefahren begründet wurde, nun auf breiter Basis für die Verfolgung von Urheberrechtsverletzungen genutzt würden.

IPR-Enforcement-Richtlinie

Die Mitgliedstaaten müssen zwar nach Art. 8 Abs. 1 lit. c) der IPR-Enforcement-Richtlinie sicher stellen, dass die Gerichte unter bestimmten Voraussetzungen die Erteilung von Auskünften u.a. durch Personen anordnen können, die nachweislich für rechtsverletzende Tätigkeiten genutzte Dienstleistungen in gewerblichem Ausmaß erbringen.

Weder Art. 8 noch eine andere Vorschrift der IPR-Enforcement-Richtlinie schreibt jedoch den Mitgliedstaaten zwingend vor, zur Erfüllung dieses Auskunftsanspruches Verkehrsdaten heranzuziehen und damit einen Eingriff in das Fernmeldegeheimnis vorzusehen. Das deutsche Umsetzungsgesetz muss daher keinen auf die Übermittlung von Verkehrsdaten abzielenden Auskunftsanspruch gegen Internet-Provider vorsehen, weshalb auch ein Verzicht auf diesen Auskunftsanspruch keinen Verstoß gegen die IPR-Enforcement-Richtlinie darstellt. Dies ist auch nicht weiter überraschend, da es nie Sinn und Zweck der IPR-Enforcement-Richtlinie war, internetspezifische Probleme zu lösen; sie hat vielmehr, wie aus der Begründung des Kommissionsentwurfs hervorgeht, alle Formen von Produktpiraterie im Auge (so auch Spindler/Dorschel, Vereinbarkeit der geplanten Auskunftsansprüche gegen Internet-Provider mit EU-Recht, CR 2006, 341, 346/7).

Im Gegenteil dürfte der im Referentenentwurf eines „Gesetzes zur Verbesserung der Durchsetzung von Rechten des geistigen Eigentums“ enthaltene Auskunftsanspruch gegen Internet-Provider sogar selbst europarechtswidrig sein. Nach Art. 15 Abs. 1 der „Richtlinie 2002/58/EG des Europäischen Parlaments und des Rates vom 12. Juli 2002 über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation“ (TK-Datenschutzrichtlinie) ist nämlich eine Verarbeitung von Verkehrsdaten über die in Art. 6 dieser Richtlinie normierten Erlaubnistatbestände hinaus nur

zulässig, soweit diese „für die nationale Sicherheit, (d.h. die Sicherheit des Staates), die Landesverteidigung, die öffentliche Sicherheit sowie die Verhütung, Ermittlung, Feststellung und Verfolgung von Straftaten oder des unzulässigen Gebrauchs von elektronischen Kommunikationssystemen in einer demokratischen Gesellschaft notwendig, angemessen und verhältnismäßig ist.“ Die Erfüllung von Auskunftspflichten im Interesse privater Dritter, die nicht etwa auf die Verfolgung strafbarer, sprich vorsätzlicher Schutzrechtsverletzungen beschränkt ist, dürfte diesen Anforderungen schwerlich genügen (so auch Spindler/Dorschel, Vereinbarkeit der geplanten Auskunftsansprüche gegen Internet-Provider mit EU-Recht, CR 2006, 341, 346 m.w.N.). Dabei stellt Art. 8 Abs. 3 lit. e) der IPR-Enforcement-Richlinie ausdrücklich klar, dass die Auskunftstatbestände der IPR-Enforcement-Richtlinie die Verpflichtungen nach der TK-Datenschutzrichtlinie nicht zu relativieren vermögen.

Abgesehen von dieser europa- und verfassungsrechtlichen Problematik ist auch zu bedenken, dass der beabsichtigte Auskunftsanspruch gegen Internet-Provider aus praktischen Gründen ins Leere führt.

De lege lata sind nämlich die beim Provider gespeicherten Verkehrsdaten gem. § 96 Abs. 2 Satz 2 TKG nach Beendigung der Verbindung grundsätzlich unverzüglich zu löschen; die gespeicherten Verkehrsdaten dürfen gem. § 96 Abs. 2 Satz 1 TKG nur in den dort enumerativ aufgeführten, eng begrenzten Ausnahmefällen über das Ende der Verbindung hinaus verwendet werden. Bedeutsamster Ausnahmefall ist dabei die in § 97 TKG normierte Entgeltermittlung und Entgeltabrechnung, wozu die entsprechenden Verkehrsdaten gem. § 97 Abs. 3 Satz 3 TKG höchstens sechs Monate nach Versendung der Rechnung gespeichert werden dürfen.

Zu beachten ist in diesem Zusammenhang aber, dass die Internet-Provider nach einer aktuellen Entscheidung des für die T-Online AG zuständigen und somit insoweit deutschlandweit maßgeblichen Landgerichts Darmstadt (Urteil vom 25. Januar 2006, Az.: 25 S 118/05, MMR 2006, 330, 331, bestätigt durch Entscheidung des BGH vom 26. Oktober 2006, Az.: III ZR 40/06) bei einem Flatrate-Tarif verpflichtet sind, die dem Kunden jeweils zugeordnete dynamische IP-Adresse unmittelbar nach dem Ende der jeweiligen Verbindung zu löschen. Das Landgericht Darmstadt hat insoweit ausgeführt, dass insbesondere eine Speicherung nach § 97 Abs. 2 TKG nicht in Betracht kommt, da die IP-Adresse weder für die Entgeltermittlung noch für die Entgeltabrechnung erforderlich ist.

Berücksichtigt man nun vor dem Hintergrund dieser Rechtslage, dass Flatrate-Tarife wie geschaffen zum Download der für Musik oder Filme benötigten großen Datenvolumina sind, die Preise für Flatrates seit kurzer Zeit aber rapide fallen - es werden sogar bereits kostenlose Flatrates angeboten -, so spricht vieles dafür, dass der beabsichtigte Auskunftsanspruch gegen Internet-Provider schon im Zeitpunkt seiner Verkündung im Bundesgesetzblatt wertlos ist. Darin waren sich auch die Urheberrechts- und Informationstechnologieexperten auf der Tagung „Auskunftsanspruch gegen Internetprovider“ am 7. April 2006 im Institut für Urheber- und Medienrecht in München einig.

Für den - in Zukunft zunehmend unwahrscheinlichen - Fall, dass beim Internet-Provider zum Zeitpunkt der Erhebung eines Auskunftsanspruchs überhaupt noch Verkehrsdaten gespeichert sind, möchte ich darauf hinweisen, dass der Drittauskunftsanspruch nach der Begründung des Referentenentwurfs (Seite 78) nicht nur voraussetzt, dass die Mitwirkungshandlungen des Dritten ein gewerbliches Ausmaß erreicht haben; vielmehr muss auch die Rechtsverletzung selbst in gewerblichem Ausmaß begangen worden sein, also in einem Ausmaß, das den üblichen Konsum überschreitet. Hiervon geht auch Erwägungsgrund 14 der IPR-Enforcement-Richtlinie aus.

Nach der Lebenserfahrung ist nun davon auszugehen, dass ein Rechteverletzer, der in so definiertem gewerblichem Ausmaß illegale Downloads vornimmt, mit den technischen Möglichkeiten des Internet besonders vertraut ist. Dem Rechteverletzer wird es daher unschwer möglich sein, durch informationstechnische Maßnahmen wie beispielsweise durch die Nutzung verteilter (Anonymisierungs-)Systeme, bei denen mehrere Provider hintereinander geschaltet sind, die Verwirklichung des Auskunftsanspruchs über die Höchstspeicherungsdauer des § 97 Abs. 2 Satz 3 TKG von sechs Monaten hinauszuzögern und damit letztlich ganz zu verhindern.

Vorratsspeicherungs-Richtlinie

Die Frage, ob die Internet-Provider auch über Vorratsdaten Auskunft erteilen müssen, wird in dem Referentenentwurf nicht geregelt. Darüber kann erst mit dem Gesetz zur Umsetzung der „Richtlinie 2006/24/EG des Europäischen Parlaments und des Rates vom 15. März 2006 über die Vorratsspeicherung von Daten, die bei der Bereitstellung öffentlich zugänglicher elektronischer Kommunikationsdienste oder öffentlicher Kommunikationsnetze erzeugt oder verarbeitet werden, und zur Änderung der Richtlinie 2002/58/EG“ (Vorratsspeicherungs-Richtlinie) entschieden werden. Erfreulicherweise hat Deutschland bereits gem. Art. 15 Abs. 3 der Vorratsspeicherungs-Richtlinie erklärt, die Anwendung dieser Richtlinie auf die Speicherung von Kommunikationsdaten betreffend Internetzugang, Internet-Telefonie und Internet-E-Mail bis zum 15. März 2009 aufzuschieben.

Nach Art. 1 Abs. 1 der Vorratsspeicherungs-Richtlinie sollen mit dieser Richtlinie 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“. Erwägungsgrund 9 Satz 3 der Vorratsspeicherungs-Richtlinie bezeichnet als schwere Fälle ausdrücklich „organisierte Kriminalität und Terrorismus“.

In seiner Sitzung vom 16. Februar 2006 hat der Deutsche Bundestag den Antrag der Koalitionsfraktionen vom 7. Februar 2006 „Speicherung mit Augenmaß - Effektive Strafverfolgung und Grundrechtswahrung“ (BT-Drs. 16/545) angenommen und damit in Abschnitt II. Nr. 2 a) die Bundesregierung aufgefordert, „hinsichtlich der Speicherungsdauer und der erfassten Datenarten keine über die Mindestanforderungen der Richtlinie hinausgehenden Pflichten“ zu regeln. Dies, insbesondere die im Folgenden getroffene Festlegung auf die Mindestspeicherungsfrist von sechs Monaten, begrüße ich aus datenschutzrechtlicher Sicht ausdrücklich. Obwohl der Antrag in Abschnitt I. mehrmals darauf abstellt, dass die Vorratsspeicherung zur Bekämpfung des internationalen Terrorismus und der organisierten Kriminalität als Ermittlungsinstrument unverzichtbar sei, soll nach Abschnitt II Nr. 2 a) die Datenabfrage zu Zwecken der Strafverfolgung nicht auf die Ermittlung, Aufdeckung und Verfolgung erheblicher Straftaten beschränkt, sondern auch auf bloß „mittels Telekommunikation begangene Straftaten“ erstreckt werden.

Diese Ausweitung der Datenabfrage ist nicht nur datenschutzrechtlich problematisch, sondern steht auch in dieser Allgemeinheit zu der in Art. 1 Abs. 1 der Vorratsspeicherungs-Richtlinie europarechtlich vorgeschriebenen Beschränkung auf schwere Straftaten in Widerspruch. Der Deutsche Bundestag kann sich dabei auch nicht auf eine im Rahmen der 2709. Tagung des Rates der Europäischen Union (Justiz und Inneres) am 21. Februar 2006 in Brüssel gefasste Erklärung des Rates zu Art. 1 der Vorratsspeicherungs-Richtlinie stützen. Nach dem genauen Wortlaut dieser Erklärung haben nämlich lediglich „bei der Definition des Begriffs „schwere Straftat“ im einzelstaatlichen Recht … die Mitgliedstaaten … Straftaten unter Einsatz von Telekommunikationseinrichtungen angemessen zu berücksichtigen.“ Der Rat selbst stellt damit nicht in Frage, dass die mittels Telekommunikation begangenen Straftaten selbstverständlich die Qualität schwerer Straftaten erreichen müssen.

Bezogen auf die Problematik des Auskunftsanspruchs gegen Internet-Provider darf ich überdies darauf hinweisen, dass gem. Art. 4 der Vorratsspeicherungs-Richtlinie die Mitgliedstaaten sicherstellen müssen, dass die gemäß dieser Richtlinie auf Vorrat gespeicherten Daten nur an die für die Strafverfolgung zuständigen nationalen Behörden weitergegeben werden; ebenso wie andere staatliche Stellen dürfen auch private Dritte keinen Zugang zu den Daten erhalten.

In diesem Zusammenhang darf ich auch auf die Stellungnahme der Datenschutzbeauftragten der EU-Mitgliedstaaten (Artikel 29-Gruppe) zur Vorratsspeicherungs-Richtlinie vom 25. März 2006 hinweisen (im Internet abrufbar unter http://ec.europa.eu).

Im Übrigen wäre auch eine - europarechtswidrige - Erstreckung der Datenabfrage zur Strafverfolgung nicht schwerer, aber mittels Telekommunikation begangener Straftaten - selbst bei Ausschöpfung der von der Vorratsspeicherungs-Richtlinie vorgegebenen Höchstspeicherfrist von zwei Jahren - aus tatsächlichen Gründen nicht geeignet, dem hier in Rede stehenden Auskunftsanspruch gegen Internet-Provider zur Wirkung zu verhelfen.

Wie beispielsweise Prof. Dr. Hannes Federrath vom Lehrstuhl Management der Informationssicherheit der Universität Regensburg auf der Tagung „Auskunftsanspruch gegen Internetprovider“ vom 7. April 2006 im Institut für Urheber- und Medienrecht in München eindrucksvoll dargelegt hat, kann die Verwirklichung des Auskunftsanspruchs durch die Nutzung verteilter Systeme, bei denen mehrere Provider hintereinander geschaltet sind, über die nach der Vorratsdatenspeicherungs-Richtlinie vorgesehene Maximalspeicherdauer von zwei Jahren unschwer hinausgezögert werden. Auch in diesem Falle würde also der Auskunftsanspruch ins Leere laufen.

Vor diesem Hintergrund hoffe ich, dass der Gesetzgeber im Zuge der Umsetzung sowohl der IPR-Enforcement-Richtlinie als auch der Vorratsspeicherungs-Richtlinie den aufgezeigten datenschutzrechtlichen Aspekten die notwendige Bedeutung beimisst. Dafür werde ich mich auch weiterhin persönlich einsetzen.

20.3 Datenschutzkonforme Befreiung von der Rundfunkgebührenpflicht

Nach den Bestimmungen des Rundfunkgebührenstaatsvertrages werden u.a. die Empfänger bestimmter Sozialleistungen - insbesondere von Sozialhilfe, Grundsicherung, Sozialgeld und Arbeitslosengeld II - auf Antrag von der Rundfunkgebührenpflicht befreit. In Bayern war der Antrag bisher dezentral bei der jeweiligen Heimatgemeinde zu stellen, so dass der Antragsteller die für die Befreiung erforderlichen Nachweise nach Übernahme der relevanten Daten sofort wieder an sich nehmen konnte.

Mit dem In-Kraft-Treten des Achten Rundfunkänderungsstaatsvertrages im Jahr 2005 wurde auch das Verfahren zur Befreiung von der Rundfunkgebührenpflicht geändert: Nach dem neuen § 6 Abs. 2 Rundfunkgebührenstaatsvertrag (RGebStV) hat nun der Antragsteller die Voraussetzungen für die Befreiung von der Rundfunkgebührenpflicht durch Vorlage des - vollständigen - Sozialleistungsbescheides im Original oder in beglaubigter Kopie zentral bei der GEZ nachzuweisen.

Dies halte ich für datenschutzrechtlich äußerst problematisch. Aufgrund des Zwangs zur Vorlage des vollständigen Sozialleistungsbescheids muss der Betroffene in erheblichem Umfang sensible Sozialdaten offenbaren, die zum überwiegenden Teil für die Entscheidung über die Befreiung von der Rundfunkgebührenpflicht nicht erforderlich sind (z.B. umfangreiche Daten über die Einkommens-, Vermögens- und Wohnsituation des Antragstellers und nicht selten auch seiner Familienangehörigen). So verfügt die GEZ inzwischen über die umfangreichste - und zudem ständig aktualisierte - Sammlung von Sozialleistungsbescheiden in Deutschland.

Unmittelbar nach dem In-Kraft-Treten des Achten Rundfunkänderungsstaatsvertrags haben meine Kollegen und ich zusammen mit den Datenschutzbeauftragten der Rundfunkanstalten nach Wegen zur Beseitigung dieses datenschutzrechtlich unbefriedigenden Zustands gesucht. Da die Sozialleistungsbehörden auf der Basis der derzeitigen Rechtslage - aber auch aus Kostengründen - bisher nicht bereit sind, das Vorliegen der Befreiungsvoraussetzungen auf einem Formblatt schriftlich zu bestätigen, kann ein den Grundsätzen der Erforderlichkeit und Datensparsamkeit entsprechendes datenschutzfreundliches Befreiungsverfahren nur durch eine erneute Änderung des Rundfunkgebührenstaatsvertrages eingeführt werden. Um diesbezüglich einheitliche Vorschläge in die politische Diskussion einbringen zu können, wurde aus Vertretern der Rundfunkreferenten der Länder, der Rundfunkdatenschutzbeauftragten und der Landesdatenschutzbeauftragten eine gemeinsame Arbeitsgruppe gebildet.

Nach intensiven Vorarbeiten im Kreis der Landesdatenschutzbeauftragten konnte in dieser Arbeitsgruppe eine Einigung erreicht werden: Dem Sozialleistungsempfänger soll künftig durch eine entsprechende Änderung des § 6 Abs. 2 RGebStV eine Wahlmöglichkeit eingeräumt werden. Der Antragsteller soll die Voraussetzungen für die Befreiung von der Rundfunkgebührenpflicht entweder durch Vorlage (lediglich) einer Bestätigung des Sozialleistungsträgers über die Gewährung und die Dauer der Sozialleistung (im Original) oder durch Vorlage des Sozialleistungsbescheides (im Original oder in beglaubigter Kopie) nachweisen. Es ist geplant, die Änderung in den 10. Rundfunkänderungsstaatsvertrag aufzunehmen.

Die Rundfunkanstalten und die GEZ haben sich bereit erklärt, im Vorgriff auf diese staatsvertragliche Regelung entsprechende Bestätigungen anzuerkennen. Es ist aber darauf hinzuweisen, dass eine Verpflichtung aller Sozialleistungsbehörden zur Ausstellung dieser Bestätigungen aus kompetenziellen Gründen im Rundfunkgebührenstaatsvertrag nicht begründet werden kann. Als Vorsitzender der Rundfunkkommission hat deshalb der Ministerpräsident des Landes Rheinland-Pfalz - auch im Namen der Rundfunk- und der Landesdatenschutzbeauftragten - bei der Bundesagentur für Arbeit und bei den betroffenen kommunalen Spitzenverbänden für die Bestätigungslösung geworben. Erfreulicherweise haben sich in Bayern bereits der Bayerische Rundfunk und die GEZ auf der einen Seite und die bayerischen kommunalen Spitzenverbände (Gemeindetag, Landkreistag, Städtetag) auf der anderen Seite unter Vermittlung der Bayerischen Staatskanzlei auf diese datenschutzgerechte Lösung verständigt. Schließlich möchte ich nicht unerwähnt lassen, dass die GEZ derzeit intensiv an der Konzeption eines datenschutzfreundlichen Online-Verfahrens arbeitet, das den betroffenen Sozialleistungsbehörden zur weiteren Verfahrensvereinfachung die elektronische Übermittlung der Bestätigungen ermöglichen soll.

20.4 Übermittlung von Grundsteuerdaten an die GEZ

Im Berichtszeitraum haben mich mehrere Kommunen zu der Frage um Stellungnahme gebeten, ob es datenschutzrechtlich zulässig ist, Beauftragten der GEZ auf Anfrage Adressdaten von Zweitwohnungseigentümern aus der kommunalen Grundsteuerdatei bekannt zu geben. Hintergrund der Fragestellung ist offensichtlich, dass einerseits Zweitwohnungseigentümer nicht immer melderechtlich erfasst sind und die gem. Art. 31 MeldeG grundsätzlich zulässige Übermittlung von Meldedaten an die GEZ somit ins Leere läuft, andererseits Zweitwohnungseigentümer aber durchaus rundfunkgebührenpflichtig sein können.

Grundlegend ist festzustellen, dass die GEZ im Auftrag der Landesrundfunkanstalten tätig ist. Der Rundfunkgebührenstaatsvertrag enthält allerdings keine Bestimmung, die eine Offenbarung der dem in § 30 AO verankerten Steuergeheimnis unterliegenden Grundsteuerdaten ermöglicht. Insoweit kommt daher nur § 31 Abs. 3 AO in Betracht.

Nach § 31 Abs. 3 AO sind die für die Verwaltung der Grundsteuer zuständigen Behörden berechtigt, die nach § 30 AO geschützten Namen und Anschriften von Grundstückseigentümern, die bei der Verwaltung

der Grundsteuer bekannt geworden sind, zur Verwaltung anderer Abgaben sowie zur Erfüllung sonstiger öffentlicher Aufgaben zu verwenden oder den hierfür zuständigen Gerichten, Behörden oder juristischen Personen des öffentlichen Rechts auf Ersuchen mitzuteilen, soweit nicht überwiegende schutzwürdige Interessen des Betroffenen entgegenstehen.

Das von mir diesbezüglich um Stellungnahme gebetene Staatsministerium der Finanzen hat eine Datenübermittlung an die GEZ aufgrund der Vorschrift des § 31 Abs. 3 AO grundsätzlich für zulässig erachtet. Es hat jedoch ausdrücklich meiner Auffassung zugestimmt, dass § 31 Abs. 3 AO die Datenübermittlung in das Ermessen der Kommune stellt und damit keine Verpflichtung zu einer Übermittlung besteht. Schließlich hat das Staatsministerium den in der genannten Vorschrift normierten Verhältnismäßigkeitsgrundsatz als gewahrt angesehen, wenn seitens der Kommune sichergestellt wird, dass nur Daten von Zweitwohnungseigentümern weitergegeben werden.

Meiner Meinung nach muss die Zulässigkeit einer Übermittlung von Grundsteuerdaten an die GEZ aus datenschutzrechtlicher Sicht allerdings an weitere Voraussetzungen geknüpft werden:

- So regelt Art. 31 Abs. 1 Satz 3 MeldeG die Zulässigkeit von Gruppenauskünften. Da der Gesetzgeber aber in § 12 a BayMeldeDÜV bereits die Möglichkeit einer regelmäßigen Datenübermittlung an die GEZ vorgesehen hat, ist an die Prüfung von - zusätzlichen - Gruppenauskunftsbegehren der GEZ gem. Art. 31 Abs. 1 Satz 3 MeldeG ein strenger Maßstab anzulegen. Mit dem Staatsministerium des Innern vertrete ich daher die Auffassung, dass die GEZ, soweit eine Datenübermittlung grundsätzlich in Frage kommt, besondere Gesichtspunkte vortragen muss, die über das grundsätzlich bestehende öffentliche Interesse am Rundfunkgebühreneinzug hinausgehen. Dies können beispielsweise von vergleichbaren anderen Gemeindeteilen oder anderen Gemeinden signifikant abweichende statistische Daten über Rundfunkanmeldungen sein (vgl. VGH Baden-Württemberg, Urteil vom 14.11.1994, Az.: 1 S 310/94).

- Unter dem Gesichtspunkt der Verhältnismäßigkeit ist meiner Auffassung nach auch zu berücksichtigen, dass die Tatsache an die GEZ übermittelt werden soll, dass ein Steuerbürger Eigentümer eines bestimmten Zweitwohnsitzes ist, und zwar ohne dass bereits feststeht, ob der betroffene Steuerbürger in der Zweitwohnung zum einen überhaupt Rundfunkgeräte vorhält und zum anderen diese unzulässigerweise nicht angemeldet hat.

  Von der Qualität der Datenübermittlung her geht damit die Bekanntgabe des Merkmals „Zweitwohnungseigentümer“ weit über die Bekanntgabe der melderechtlichen Gegebenheiten hinaus. § 31 Abs. 3 AO sieht dementsprechend auch ausdrücklich vor einer Datenübermittlung aus der Grundsteuerdatei die Prüfung der schutzwürdigen Interessen des Betroffenen vor.

Im Ergebnis halte ich eine Datenübermittlung aus der kommunalen Grundsteuerdatei an die GEZ bei Anlegung eines strengen Maßstabes nur dann für zulässig, wenn die GEZ nachvollziehbare Gesichtspunkte darlegt, die die Schlussfolgerung erlauben, dass Zweitwohnungseigentümer - im konkreten Fall einer bestimmten Kommune oder generell - ihrer Meldepflicht nach dem Rundfunkgebührenstaatsvertrag nicht nachgekommen sind. In jedem Einzelfall muss die Kommune zudem überprüfen, ob nicht überwiegende schutzwürdige Interessen der Betroffenen dem Auskunftsersuchen entgegenstehen. Seitens der Kommune muss zudem sichergestellt werden, dass nur die Angaben der Zweitwohnungseigentümer und keinesfalls die Angaben aller Grundsteuerpflichtigen übermittelt werden.

Im Übrigen weise ich nochmals ausdrücklich darauf hin, dass § 31 Abs. 3 AO die Mitteilung an die GEZ lediglich gestattet, aber nicht dazu verpflichtet, die kommunale Finanzbehörde also nach ihrem eigenen Ermessen zu entscheiden hat. In diesem Zusammenhang ist zu beachten, dass die Beauftragten der GEZ - worauf mich einige Kommunen aufmerksam gemacht haben - vor Ort Straßenbegehungen durchführen. Melderechtlich nicht erfasste Zweitwohnungseigentümer können der GEZ also auch auf diesem Weg bekannt werden mit der Folge, dass die GEZ diese Zweitwohnungseigentümer unter der Adresse der Zweitwohnung selbst um Auskunft bitten kann. Dies erscheint zwar ein umständlicher aber dennoch durchaus gangbarer Weg zu sein, die Meldepflicht nach dem Rundfunkgebührenstaatsvertrag zu überprüfen. Jedenfalls sollte die Kommune diese Möglichkeit im Rahmen ihrer Ermessensabwägung im Fall einer von der GEZ erbetenen Auskunft über Zweitwohnungseigentümer aus der kommunalen Grundsteuerdatei berücksichtigen.

21 Statistik

21.1 eGovernment-Projekt „Amtliche Schuldaten“

Die Erhebung der „Amtlichen Schuldaten“ (ASD) war bereits in der Vergangenheit Gegenstand einer intensiven Diskussion zwischen dem Staatsministerium für Unterricht und Kultus und mir. Dabei ging es zum einen um die Frage einer tragfähigen Rechts-

grundlage und zum anderen um die Frage, um welche Art von Statistik es sich handelt.

Das Kultusministerium geht derzeit vom Vorliegen einer Geschäftsstatistik aus, obwohl bei einer derartigen Statistik an sich nur im Verwaltungsvollzug bereits angefallene Daten verarbeitet werden können. Zudem stützt das Staatsministerium das Verfahren auf die - unspezifisch formulierte - Vorschrift des Art. 113 BayEUG („Die Schulaufsichtsbehörden haben in Erfüllung ihrer Aufgaben insbesondere das Recht, ... Berichte, Nachweise und statistische Angaben zu fordern."). Das Verfahren ist bisher arbeitsteilig angelegt: Das Staatsministerium bereitet die Lehrer- und Unterrichtsdaten auf, das Landesamt für Statistik und Datenverarbeitung die Schülerdaten. Dem Landesamt werden dabei nur aggregierte Klassendaten geliefert.

Im Rahmen der eGovernment-Initiative der Staatsregierung hat das Staatsministerium für Unterricht und Kultus im Jahr 2005 eine vollständige Neukonzeption des Verfahrens „Amtliche Schuldaten" in Angriff genommen. Dieses Vorhaben wurde sicherlich auch durch ein nahezu identisches, inzwischen weitgehend realisiertes Projekt in Baden-Württemberg (dort kurz „E-Stat" genannt) sowie durch den Beschluss der Kultusministerkonferenz (KMK) zur Einführung eines „Kerndatensatzes der Länder für schulstatistische Individualdaten" befördert. Der Landesbeauftragte für den Datenschutz Baden-Württemberg hat zu dem dortigen Projekt in seinem 25. Tätigkeitsbericht 2004 ausführlich Stellung genommen; die dortige Landesregierung hat bezüglich der Rechtsgrundlagen einen umfangreichen Gesetzentwurf vorgelegt.

Nach Darstellung des Staatsministeriums für Unterricht und Kultus ist Gegenstand dieser Neukonzeption eine umfassende Restrukturierung der Geschäftsprozesse der Kultusverwaltung unter Ausschöpfung der heute verfügbaren informationstechnischen Möglichkeiten - kurz gesagt: ein effektives, netzbasiertes Schulverwaltungsverfahren.

Das Projekt geht im Wesentlichen davon aus, dass (web-browser-basiert) die (Schul-)Daten dort erfasst werden, wo sie anfallen. Durch die Einrichtung von zentralen Datenbanken (z.B. für Dienststellen, Schüler, Unterrichtseinheiten) und den Zugriff auf bereits bestehende Datenspeicher (z.B. Personaldatenbanken der Lehrer) soll die Mehrfachhaltung von Daten vermieden werden. Zudem soll mittels einer Verbindung mit den im Melderegister über die Schulpflichtigen gespeicherten Daten der Erfassungsaufwand innerhalb der Kultusverwaltung reduziert werden. Die Rationalisierung von Arbeitsprozessen soll die rechtzeitige Verfügbarkeit der aufbereiteten Daten sowie deren benutzerfreundliche Auswertbarkeit im Rahmen eines modernen Führungsinformationssystems (einschließlich eines Data Warehouse) ermöglichen. Die Statistikdaten sollen dann quasi als „Abfallprodukt" der vorgehaltenen Verwaltungsdaten anfallen. Im Rahmen einer Benutzerverwaltung soll schließlich festgelegt werden, welche Funktionen die einzelnen Benutzer ausüben dürfen und welche Zugriffsrechte diese erhalten.

Festzuhalten ist, dass die Implementierung eines derart umfangreichen, multifunktionalen eGovernment-Projekts mit vielfältigen Nutzungsmöglichkeiten von den bestehenden gesetzlichen Grundlagen, insbesondere von Art. 85 BayEUG, nicht mehr gedeckt ist. Notwendig ist daher - wie in Baden-Württemberg - die Schaffung einer umfassenden und normenklaren gesetzlichen Rechtsgrundlage.

Bei meinem derzeitigen Kenntnisstand halte ich in diesem Zusammenhang allerdings insbesondere die Vorhaltung einer Vielzahl von Daten aller bayerischen Schüler in personenbezogener Form in zentralen Datenbanken für datenschutzrechtlich problematisch. Durch die beabsichtigte Vergabe von Schüler-Identifikationsnummern wird die Gefahr der Erstellung von Persönlichkeitsprofilen sogar noch verstärkt. Dies gilt in gleicher Weise hinsichtlich der geplanten Vergabe von Lehrer-Identifikationsnummern zur Ermöglichung von (lediglich pseudonymisierten?) Verlaufsuntersuchungen.

Aus datenschutzrechtlicher Sicht sollte im Rahmen der notwendigen Rechtsgrundlage jedenfalls auch die Erhebung der Schulstatistik auf eine tragfähige, rechtssichere und normenklare gesetzliche Basis gestellt werden. Die von der KMK beschlossene Umstellung auf Schülerindividualdatensätze lässt für die bisher vom Kultusministerium vertretene Auffassung, dass es sich bei den schulstatistischen Erhebungen um die bloße Aufbereitung einer Geschäftsstatistik handelt, keinen Raum mehr. Vor allem im Hinblick auf die fehlende Normenklarheit verfehlt zudem der oben zitierte Art. 113 BayEUG die an eine derartige Rechtsgrundlage zu stellenden Anforderungen.

Aus diesen Gründen habe ich beim Staatsministerium für Unterricht und Kultus mehrfach die Übermittlung eines umfassenden Gesetzentwurfs für das Projekt „Amtliche Schuldaten" angemahnt. Gegenüber dem Kultusministerium habe ich zum Ausdruck gebracht, dass eine verlässliche datenschutzrechtliche Beurteilung von Seiten des Landesbeauftragten nur auf der Basis eines klaren und eindeutigen Sachverhalts erfolgen kann. Dies setzt voraus, dass die mit dem Gesamtprojekt „Amtliche Schuldaten" - ebenso wie mit den jeweiligen Teilprojekten - konkret verfolgten Ziele, beabsichtigten Datenaustausche und zu schaffenden Funktionalitäten im Einzelnen dargelegt werden. Als maßgeblichen Schritt hierzu sehe ich weiterhin die Erarbeitung eines Entwurfs einer Rechtsgrundlage für das Gesamtprojekt „Amtliche Schuldaten" einschließlich eingehender, detaillierter Begrün-

dung an. Dabei sollte insbesondere auch die Rechtsnatur des Statistikteils des Projekts „Amtliche Schuldaten“ einer endgültigen, rechtssicheren Klärung zugeführt werden.

Im November 2006 hat mir das Staatsministerium für Unterricht und Kultus die baldige Übermittlung eines umfassenden Gesetzentwurfs für das Gesamtprojekt „Amtliche Schuldaten“ zugesagt. Ich werde diesen Gesetzentwurf einer kritischen datenschutzrechtlichen Prüfung unterziehen.

Auch die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat zu der genannten Thematik in Form der Entschließung „Keine Schülerstatistik ohne Datenschutz“ kritisch Stellung bezogen (siehe Anlage Nr. 21).

21.2 Speicherung von Lehrerdaten auf dem Server eines Privatunternehmens

Im Jahr 2005 wurde ich durch eine Eingabe darauf aufmerksam, dass das Staatsministerium für Unterricht und Kultus die Übermittlung der für die Erhebung der „Amtlichen Schuldaten“ benötigten Lehrerdaten von den Schulen über das Internetportal eines privaten Schulverwaltungssoftware-Anbieters an das jeweilige Schulamt duldete. Zu diesem Zweck wurden die Lehrerdaten auf dem Server des Privatunternehmens (zumindest zwischen-)gespeichert.

In diesem Zusammenhang stellten sich mir aus datenschutzrechtlicher Sicht mehrere Fragen. So war vor allem zu klären,

- ob es sich hier um Auftragsdatenverarbeitung im Sinne des Art. 6 BayDSG handelte, wer jeweils Auftraggeber war und welche vertraglichen Bindungen bestanden,

- ob die (zumindest zeitweilige) Vorhaltung von Personalaktendaten außerhalb der Kultus(-personal-)verwaltung in dem privaten Internetportal mit den Bestimmungen der Art. 100 a ff. BayBG über das Personalaktengeheimnis zu vereinbaren war und

- ob und von wem das Verfahren gem. Art. 26 BayDSG datenschutzrechtlich freigegeben worden war.

Mit diesen Fragen wandte ich mich an das Staatsministerium für Unterricht und Kultus.

- Das Kultusministerium brachte zur Frage des Vorliegens einer Auftragsdatenverarbeitung vor, dass der private Anbieter „für die AKDB im Auftrag der Staatlichen Schulämter“ arbeite und somit der Tatbestand der datenschutzrechtlich zugelassen Auftragsdatenverarbeitung vorliege.

  Selbst wenn man sich diese Rechtsauffassung zu eigen machte, hätte jedoch gemäß Art. 6 Abs. 2 Satz 2 BayDSG ein derartiger Auftrag von jedem einzelnen Schulamt schriftlich erteilt werden müssen; dabei wären Datenerhebung, -verarbeitung und -nutzung sowie die technischen und organisatorischen Maßnahmen einschließlich etwaiger Unterauftragsverhältnisse auch jeweils schriftlich festzulegen gewesen. Dies war jedoch offensichtlich nicht geschehen. In diesem Zusammenhang musste ich das Kultusministerium auf Art. 25 Abs. 1 BayDSG hinweisen, der die gesetzliche Verantwortlichkeit für die Sicherstellung des Datenschutzes den fachlich zuständigen Staatsministerien jeweils für ihren Geschäftsbereich auferlegt.

- Zur Frage der (zumindest zeitweiligen) Vorhaltung von Personalaktendaten außerhalb der Kultus(-personal-)verwaltung stellte das Kultusministerium lediglich unter Zitierung des Wortlauts von Art. 100 a Abs. 3 BayBG fest, dass die Zugriffsrechte hinsichtlich des Internetportals des privaten Anbieters so geregelt seien, dass nur diejenigen Bediensteten der Kultusverwaltung Zugang hätten, die im Rahmen der Personalverwaltung ohnehin mit der Bearbeitung von Personalangelegenheiten beauftragt seien, und dies nur soweit, wie es zu Zwecken der Personalverwaltung erforderlich sei.

  Die Zugriffsberechtigungen von Bediensteten waren von mir aber nicht problematisiert worden. Vielmehr war vom Kultusministerium allein zu klären, in welchem Umfang, wie lange und ggf. mittels welcher Verschlüsselung Personalaktendaten des Lehrpersonals auf EDV-Einrichtungen des privaten Anbieters (zwischen-)gespeichert wurden und welche Einsichtsmöglichkeiten für Beschäftigte des privaten Anbieters in diesem Zusammenhang bestanden.

- Aus seiner Darstellung, dass der private Anbieter „für die AKDB“ arbeite, zog das Kultusministerium den Schluss, dass damit eine datenschutzrechtliche Freigabe durch die das Verfahren einsetzende öffentliche Stelle gem. Art. 26 Abs. 1 Satz 2 Halbsatz 1 BayDSG nicht erforderlich sei, da das Verfahren von der AKDB bereits datenschutzrechtlich freigegeben worden sei.

Nach Auskunft der von mir daraufhin angeschriebenen AKDB bestand allerdings hinsichtlich der Schulverwaltungssoftware des privaten Anbieters lediglich eine Zusammenarbeit bezüglich des Produktvertriebs; Vereinbarungen hinsichtlich der Fortentwicklung des Verfahrens habe es jedoch nicht gegeben. Insbesondere das in Rede stehende Internetportal sei ohne Auftrag und ohne datenschutzrechtliche Freigabe der AKDB entwickelt und den Anwendern zur Verfügung gestellt worden.

Nach mehrmonatiger, intensiver Diskussion hat das Staatsministerium für Unterricht und Kultus Folgendes veranlasst:

- Alle Schulämter haben mit dem privaten Anbieter Einzelverträge im Sinne des Art. 6 BayDSG zu Art und Umfang der (Auftrags-) Datenverarbeitung abgeschlossen. Danach darf das Internetportal nur im Rahmen der Klassenbildung zum Einsatz kommen; für die Erhebung der „Amtlichen Schuldaten“ im Oktober 2006 wurde die Nutzung des Portals allerdings untersagt.

- Auf explizite Nachfrage hat der private Anbieter dem Kultusministerium versichert, dass die Personalaktendaten des Lehrpersonals in dem Internetportal pseudonymisiert gespeichert seien und somit die Mitarbeiter nicht in der Lage seien, diese Daten einer bestimmten Lehrkraft zuzuordnen.

- Das Kultusministerium hat den privaten Anbieter aufgefordert, die zur Erteilung der datenschutzrechtlichen Freigabe gem. Art. 26 BayDSG erforderlichen Unterlagen zeitnah einzureichen.

Ich werde die weitere Entwicklung kritisch begleiten. Meiner Meinung nach unterstreicht dieser Vorgang exemplarisch die Bedeutung einer frühzeitigen, umfassenden datenschutzrechtlichen Beurteilung eines Verfahrens im Rahmen der datenschutzrechtlichen Freigabe. Dies umso mehr, als jedes Staatsministerium gem. Art. 25 BayDSG in seinem Geschäftsbereich für die Einhaltung datenschutzrechtlicher Vorgaben verantwortlich ist.

21.3 CEUS^{HB} - Computerbasiertes EntscheidungsUnterstützungsSystem für die Hochschulen in Bayern

Zur Stärkung von Effizienz und Wirtschaftlichkeit des Hochschulmanagements wird derzeit mit dem Projekt CEUS^{HB} ein Führungsinformationssystem für die Hochschulen und das Staatsministerium für Wissenschaft, Forschung und Kunst auf der Grundlage eines hierarchisch aufgebauten Data-Warehouse-Systems entwickelt.

Die Systemarchitektur von CEUS^{HB} besteht aus folgenden (Teil-)Data-Warehouse-Systemen:

- einem hochschulinternen Data-Warehouse-System für jede einzelne Hochschule mit aus den operativen Systemen der jeweiligen Hochschule extrahierten, bei Personenbezug faktisch anonymisierten Daten,

- einem hochschulübergreifenden Data-Warehouse-System für alle Hochschulen mit ausgewählten landes- und bundesweiten Vergleichsdaten aus der Amtlichen Statistik und

- einem Data-Warehouse-System für das Staatsministerium für Wissenschaft, Forschung und Kunst mit Daten aus der Amtlichen Statistik.

In die Planungen wurde ich von Anfang an eingebunden. Erfreulicherweise besteht sowohl seitens des Staatsministeriums für Wissenschaft, Forschung und Kunst als auch seitens des projektentwickelnden Wissenschaftlichen Instituts für Hochschulsoftware der Universität Bamberg großes Interesse an einer datenschutzrechtlich einwandfreien Umsetzung von CEUS^{HB}: Zu begrüßen ist insbesondere, dass sowohl das hochschulübergreifende Data-Warehouse-System als auch das Data-Warehouse-System des Staatsministeriums für Wissenschaft, Forschung und Kunst beim Landesamt für Statistik und Datenverarbeitung - und nicht beim Staatsministerium selbst - betrieben werden sollen.

Datenschutzrechtliche Probleme können sich vor allem im Bereich von einelementigen Abfrageergebnissen - so genannten Tabelleneinsen - ergeben, da diese einen Personenbezug ermöglichen können. Insoweit vertrete ich folgenden Standpunkt:

Aufgrund der Bestimmung des § 6 Abs. 2 HStatG, nach der die Statistischen Landesämter ausdrücklich ermächtigt werden, auch einelementige Abfrageergebnisse an die obersten Landesbehörden zu liefern, erscheint der Nachweis von Tabelleneinsen im Data-Warehouse-System des Staatsministeriums für Wissenschaft, Forschung und Kunst selbst datenschutzrechtlich hinnehmbar.

Allerdings ist zu beachten, dass im Bereich der Amtlichen Statistik die Bekanntgabe von einelementigen Abfrageergebnissen an die obersten Landesbehörden in der Praxis regelmäßig mit der Auflage versehen wird, dass diese nur für Zwecke der Planung, nicht jedoch für die Regelung von Einzelfällen erfolgt.

Dies ist Ausfluss der verfassungsrechtlichen Trennung von Statistik und Verwaltungsvollzug.

Bei Auswertungen aus dem hochschulübergreifenden Data-Warehouse-System können - entgegen ursprünglichen Aussagen - ebenfalls Tabelleneinsen entstehen. Dies ist von der Bestimmung des § 6 Abs. 2 HStatG jedoch nicht mehr gedeckt, da die Datenempfänger keine obersten Landesbehörden sind.

Im Hinblick auf das Personalaktengeheimnis sind hier aus datenschutzrechtlicher Sicht insbesondere Auswertungen von Personal- und Stellendaten als kritisch anzusehen. Durch eine Reduzierung der auswertbaren Merkmale im Zusammenspiel mit einem neu überdachten Berechtigungskonzept könnten nach Aussage der Projektleitung jedoch kritische Tabellenfelder nahezu ausgeschlossen werden. Es wurde vereinbart, mich von diesbezüglichen Überlegungen zu unterrichten.

Für das hochschulinterne Data-Warehouse-System gilt in Bezug auf Personal- und Stellendaten das eben Gesagte entsprechend. Auch hier könnte ein differenziertes und einschränkendes Berechtigungskonzept zur Problemlösung beitragen.

Generell habe ich die Projektverantwortlichen auf die Notwendigkeit einer Protokollierung sämtlicher Zugriffe auf das Führungsinformationssystem - und auch einer entsprechenden Kontrolle - hingewiesen. Sobald mir das Berechtigungskonzept vorgelegt wird, werde ich es einer kritischen datenschutzrechtlichen Prüfung unterziehen.

21.4 eSTATISTIK.core

Unter Vorlage umfangreicher Unterlagen hat mich der Präsident des Landesamts für Statistik und Datenverarbeitung im Berichtszeitraum um eine datenschutzrechtliche Bewertung des bundesweiten Statistikprojekts eSTATISTIK.core gebeten.

Das Verfahren eSTATISTIK.core soll den auskunftspflichtigen Unternehmen ermöglichen, statistische Daten automatisiert unmittelbar aus dem betrieblichen Rechnungswesen zu entnehmen und an einen zentralen gemeinsamen Internet-Dateneingang der Statistischen Ämter elektronisch zu übermitteln. Die dazu erforderlichen Programmpakete sollen die Softwarehersteller direkt in die jeweils von ihnen entwickelte Unternehmenssoftware integrieren. Mit dem Verfahren wird das Ziel verfolgt, durch Optimierung der Datengewinnung und des Datenaustausches die auskunftspflichtigen Unternehmen, aber auch die Statistischen Ämter zu entlasten. Der gemeinsame Internet-Dateneingang soll zumindest während einer Pilotphase vom Statistischen Bundesamt betrieben werden. Der Pilotbetrieb soll alle Aktivitäten umfassen, die für die automatisierte Übermittlung der statistischen Daten vom Absender bis zum originär zuständigen Statistischen Landesamt als Empfänger erforderlich sind. Die eingehenden Datenpakete sollen durch das Statistische Bundesamt entschlüsselt, auf formale Richtigkeit geprüft und anschließend an das jeweils zuständige Statistische Landesamt weitergeleitet werden.

Aus datenschutzrechtlicher Sicht stellt sich vor allem die Frage, ob hier eine Datenverarbeitung im Auftrag vorliegt oder eine Funktionsübertragung angenommen werden muss. Abhängig von dieser Frage sind Überlegungen zur Rechtsgrundlage anzustellen.

Grundsätzlich ist zu bemerken, dass für die Erhebung und Aufbereitung einer Bundesstatistik bis hin zum Landesergebnis - entsprechend der föderativen Gliederung der Bundesrepublik Deutschland - die Länder und damit die Statistischen Landesämter zuständig sind. Vor diesem Hintergrund erscheint die im Verfahren eSTATISTIK.core zunächst vorgesehene Entschlüsselung - und damit auch die Kenntnisnahme der von den Berichtspflichtigen übermittelten Datensätze - durch das Statistische Bundesamt als problematisch. Nach Durchsicht der Unterlagen scheinen die dem Statistischen Bundesamt zu übertragenden Aufgaben jedoch in der Hauptsache „Poststellencharakter“ - einschließlich einer wohl weitgehend maschinell erfolgenden formalen Vorabkontrolle - zu haben. Die Auffassung, dass es sich hierbei um eine Datenverarbeitung im Auftrag handelt, ist deshalb aus meiner Sicht nicht von der Hand zu weisen.

Um Rechtsunsicherheiten und damit eine Gefährdung des seitens der Statistik als sehr wichtig eingestuften Projekts zu vermeiden, erscheint mir aber auch der Abschluss einer vom Statistischen Bundesamt und der überwiegenden Mehrheit der Statistischen Landesämter favorisierten, auf dem mit Gesetz vom 09.06.2005 in das Bundesstatistikgesetz eingefügten § 3 a BStatG basierenden Verwaltungsvereinbarung als rechtlich zulässig. Der mir vorgelegte Entwurf einer Verwaltungsvereinbarung geht in seiner Zielrichtung von einer Funktionsübertragung aus. Dabei ist jedenfalls positiv zu bemerken, dass der Entwurf sowohl eine Zweckbindungs- als auch eine Löschungsregelung enthält.

In diesem Zusammenhang möchte ich darauf hinweisen, dass die Vorschrift des § 3 a BStatG zwar keine Differenzierung nach dem Regelungsgegenstand - z.B. Pilotprojekt ja/nein - vorsieht. Ich bin aber der Meinung, dass der derzeitige Pilotcharakter des Verfahrens aus der Verwaltungsvereinbarung - durch eine entsprechende Formulierung - ersichtlich sein sollte. Folgerichtig sollten in der Vereinbarung dann aber auch die Dauer der Pilotphase und eine etwaige

Auswertung der gewonnenen Erfahrungen geregelt werden.

Entscheidend für eine abschließende Beurteilung dürfte allerdings der Umfang der auf das „Poststellenamt“ übertragenen Plausibilisierungsarbeiten sein.

Im Hinblick auf die eingangs erwähnte, grundsätzliche bundesstaatliche Aufgabenverteilung wäre es meiner Meinung nach wünschenswert, die endgültige „Poststelle“ für das Verfahren eSTATISTIK.core bei einem Statistischen Landesamt einzurichten. Es liegt allerdings allein in der Verfügungsmacht der eine Verwaltungsvereinbarung abschließenden Beteiligten, eine derartige Regelung zu treffen. Bei meinem derzeitigen Kenntnisstand sehe ich aus datenschutzrechtlicher Sicht - zumindest für die Pilotphase - keine Ansatzpunkte für eine grundsätzliche Ablehnung des Projekts.

21.5 Volkszählung 2010/2011

Das Bundeskabinett hat am 29. August 2006 beschlossen, dass sich Deutschland an der kommenden Volkszählungsrunde der Europäischen Union 2010/2011 mit einem registergestützten Zensus beteiligt. Bei einem registergestützten Zensus werden die für die Zählung benötigten Daten vorwiegend aus Verwaltungsregistern zusammengeführt - hier insbesondere aus den Melderegistern und den Registern der Bundesagentur für Arbeit. Neben den Gebäude- und Wohnungseigentümern sollen aufgrund dieser Verfahrensweise nur etwa 10 % der Bevölkerung im Rahmen ergänzender Stichproben befragt werden.

Aus datenschutzrechtlicher Sicht bestehen gegen einen derartigen registergestützten Zensus keine grundsätzlichen Bedenken. Die vom Bundesverfassungsgericht im sog. Volkszählungsurteil (BVerfGE 65, 1) im Jahr 1983 aufgestellten Prinzipien zum Schutz des Grundrechts auf informationelle Selbstbestimmung müssen jedoch strikt beachtet werden. Es dürfen nur erforderliche Daten erhoben und verwendet werden; Datenerhebung und Datenverwendung sind gesetzlich zu regeln. Insbesondere dürfen die gewonnenen Statistikdaten nicht für Zwecke des Verwaltungsvollzugs verwendet werden. Darüber hinaus ist eine möglichst frühzeitige Anonymisierung anzustreben.

Ich werde die Vorbereitung und die Durchführung des Zensus aus datenschutzrechtlicher Sicht kritisch begleiten.

22 Spezielle datenschutzrechtliche Themen

22.1 Datenschutz bei Verwendungsnachweisen

Öffentliche Stellen, die Fördermittel aus öffentlichen Haushalten erhalten, müssen regelmäßig die zweckentsprechende und sparsame Verwendung der ihnen zur Verfügung gestellten Mittel gegenüber dem Zuwendungsgeber mittels sog. Verwendungsnachweise belegen. Datenschutzrechtliche Probleme können sich insbesondere dann ergeben, wenn nach den Förderbedingungen vom Zuwendungsempfänger zum Nachweis von Personalkosten auch Personaldaten, vor allem Gehaltsdaten, erhoben und übermittelt werden sollen.

Den folgenden Fall habe ich zum Anlass genommen, mich eingehend mit dieser Problematik auseinanderzusetzen:

Zur Durchführung verschiedener Forschungsvorhaben erhielt ein Lehrstuhl einer bayerischen Universität im Rahmen der Forschungsförderung von einer Einrichtung des Bundes öffentliche Mittel. Als Fördervoraussetzung war dabei im jeweiligen Zuwendungsbescheid u.a. festgelegt, welcher Eigenanteil vom Zuwendungsempfänger - in Form von Arbeitsleistung - erbracht werden musste. Zur genauen Überprüfung dieser Fördervoraussetzung forderte die Mittel gewährende Einrichtung vom Lehrstuhl nun, die in den jeweiligen Verwendungsnachweisen abgerechneten Personalkosten durch Beifügung der Gehaltsmitteilungen der am jeweils geförderten Projekt beteiligten Bediensteten zu belegen. Ohne den Nachweis des Eigenanteils, d.h. also ohne die Einwilligung der betroffenen Mitarbeiter in die Erhebung und Übermittlung ihrer Gehaltsdaten, würden die Zuwendungen zurückgezogen, so dass den über die fördernde Einrichtung finanzierten wissenschaftlichen Mitarbeitern des Lehrstuhls unverzüglich gekündigt werden müsste. Ein betroffener (nichtwissenschaftlicher) Lehrstuhlmitarbeiter, dessen Gehalt - wie bei Hochschulmitarbeitern üblich - von der damaligen Bezirksfinanzdirektion abgerechnet wurde, war nun einerseits trotz Aufforderung nicht geneigt, seine - auch zahlreiche persönliche, sensible Daten enthaltende - Gehaltsmitteilung zu diesem Zweck dem Lehrstuhl auszuhändigen. Da er andererseits aber auch die Zuwendung der Fördermittel und damit letztlich den Arbeitsplatz seiner Kollegen nicht gefährden wollte, sah er sich einer „Nötigungssituation“ ausgesetzt und wandte sich im Rahmen einer Eingabe an mich.

Meiner Auffassung nach ist eine Beifügung der Gehaltsmitteilungen der am jeweiligen Projekt beteiligten Mitarbeiter zu den Verwendungsnachweisen aus datenschutzrechtlicher Sicht nicht hinnehmbar.

In den Gehaltsmitteilungen sind nämlich neben den Angaben über Besoldungsgruppe, Alter und Familienstand beispielsweise auch Angaben über Lohnsteuerklasse, Religions(nicht)zugehörigkeit, Lohn- und Kirchensteuerbeträge und u.U. auch Angaben über den Arbeitgeberanteil zur Sozialversicherung, über Freibeträge und vermögenswirksame Leistungen, aber ggf. auch über Lohnpfändungen enthalten. Bei all diesen Gehaltsdaten handelt es sich somit um sensible Personalaktendaten, die nach den gesetzlichen Bestimmungen der Art. 100 ff. BayBG besonderen Schutz genießen. Diese Bestimmungen sind meiner Auffassung nach analog auch auf die nicht verbeamteten Beschäftigten des öffentlichen Dienstes anzuwenden, da sie allgemein gültige Schutzprinzipien für Arbeitnehmer enthalten.

Soweit der Zuwendungsempfänger nun - wie hier - in Bezug auf die Gehaltsabrechnungen seiner Mitarbeiter nicht speichernde Stelle im Sinne des Art. 4 Abs. 9 BayDSG ist, stellt das Einfordern der Gehaltsmitteilungen eine Erhebung von Personalaktendaten dar. Nach Art. 100 Satz 1 BayBG darf der Dienstherr personenbezogene Daten über Beamte jedoch nur erheben, soweit dies zur Begründung, Durchführung, Beendigung oder Abwicklung des Dienstverhältnisses oder zur Durchführung organisatorischer, personeller und sozialer Maßnahmen, insbesondere auch zu Zwecken der Personalplanung und des Personaleinsatzes, erforderlich ist oder eine Rechtsvorschrift dies erlaubt. Eine Erhebung sämtlicher in den Gehaltsmitteilungen enthaltenen Personalaktendaten durch den Dienstherrn zum Nachweis der Fördervoraussetzungen gegenüber einer dritten Stelle ist danach jedenfalls nicht zulässig.

Aber auch falls der Zuwendungsempfänger die Gehälter der bei ihm beschäftigten Mitarbeiter selbst abrechnet, ist jedenfalls die ihm angesonnene Übermittlung der Gehaltsmitteilungen an den Zuwendungsgeber unzulässig:

Die vorgesehenen Übermittlungen sind als (Sammel-)auskünfte aus den Personalakten der betroffenen Bediensteten zu werten. Abgesehen von seltenen, hier nicht einschlägigen Ausnahmefällen dürfen solche Auskünfte an Dritte nach Art. 100 e Abs. 2 Satz 1 BayBG nur mit Einwilligung der Beamten erteilt werden. Da bei einer Verweigerung der Einwilligung jedoch die Gefahr der Streichung von Fördermitteln und damit letztlich u.U. auch des Wegfalls von Arbeitsplätzen besteht, unterliegen in Fallgestaltungen wie der vorliegenden die um Erteilung der Einwilligung angegangenen Mitarbeiter einem erheblichen faktischen Zwang. Eine in dieser Situation den Beschäftigten abverlangte Einwilligung ist aber rechtlich nicht wirksam, da die vom Gesetz vorausgesetzte, im Dienst- oder Arbeitsverhältnis ohnehin problematische Freiwilligkeit der Einwilligung (Art. 15 Abs. 2 BayDSG) gerade nicht vorliegt.

Darüber hinaus sei noch darauf hingewiesen, dass die fördernde Einrichtung in dem zu Grunde liegenden Fall vor dem Hintergrund vielfach fehlerhafter Gehaltsabrechnungen in der Vergangenheit darauf bestand, auch die Höhe der in Ansatz gebrachten Gehaltszahlungen an die betroffenen Lehrstuhlmitarbeiter im Einzelnen zu überprüfen. Die von mir üblicherweise bevorzugte Heranziehung aktueller Personalkostendurchschnittswerte (vgl. nur Nr. 12.2 meines 18. Tätigkeitsberichtes 1998) kam daher zur Lösung der vorliegenden Problematik nicht in Betracht.

In Verhandlungen mit dem Staatsministerium der Finanzen, der fördernden Einrichtung und dem Datenschutzbeauftragten der betreffenden Universität konnte mittlerweile ein neues Verfahren entwickelt werden, das den Schutz der personenbezogenen Daten der Mitarbeiter gewährleistet; es wird gleichzeitig den Belangen der Forschung und der Forschungsförderung einerseits und dem berechtigten Interesse an einer effektiven Überprüfung der Fördervoraussetzungen andererseits in bestmöglichem Umfang gerecht. Im Einzelnen gestaltet sich das Verfahren wie folgt:

Bereits bisher werden - im staatlichen Bereich - von der Bezügestelle die jeweils aufgelaufenen Beträge der Bezüge-Haushaltsbelastung der „Haushalt führenden Stelle“ im Wege eines HÜL-Auszuges (Haushaltsüberwachungsliste; Art. 34 BayHO und Nr. 7, 7.1.1, 7.1.2 und 7.2.2 VV-BayHO) in Papierform bereitgestellt. Diese Daten sind bestimmten Beschäftigten (Name, Geburtsdatum) zuordnenbar und enthalten - neben der Buchungsstelle - den Gesamtbetrag der Haushaltsbelastung, unterteilt nach Bruttobezügen sowie ggf. Arbeitgeber-Sozialversicherungsanteilen und Arbeitgeber-Aufwendungen für die Zusatzversorgung. Angaben über die konkrete Nettoberechnung (Steuerbeträge usw.) sowie zusätzliche persönliche Angaben (Lohnsteuerklasse usw.) sind in diesen Unterlagen nicht enthalten.

Die routinemäßige Übermittlung eines HÜL-Auszuges durch die Bezügestelle an die „Haushalt führende Stelle“ ist datenschutzrechtlich gemäß Art. 18 Abs. 1 i.V.m. Art. 17 Abs. 1 Nr. 2 BayDSG zulässig. Denn die damit verbundene Übermittlung personenbezogener Daten ist zur Erfüllung der gesetzlichen Verpflichtung der „Haushalt führenden Stelle“ zur Überwachung des Haushalts (Art. 34 Abs. 2 BayHO) in Bezug auf die Personalausgaben erforderlich und die personenbezogenen Daten sind (auch) für diesen Zweck zuvor durch die Bezügestelle gespeichert worden.

Die „Haushalt führende Stelle“ - im wissenschaftlichen Bereich sind Teile der Haushaltsführung den Lehrstühlen übertragen (Projektmittelfinanzierung) - bittet nun künftig in einem ersten Schritt die zustän-

dige Bezügestelle um Auskunft über die in konkreten Zeiträumen (z.B. April bis Juni 2006) aufgelaufene Haushaltsbelastung bezüglich der Mitarbeiter, die für das jeweils geförderte Projekt Arbeitsleistungen erbracht haben. In einem zweiten Schritt bildet sie - etwa nach den dort vorliegenden Stundenaufschreibungen - die dem jeweiligen Arbeitsanteil entsprechenden anteiligen Summen und leitet diese sodann in einem dritten Schritt pseudonymisiert dem Mittelgeber zur Rechungslegung zu.

Im Rahmen der Pseudonymbildung durch die betreffende öffentliche Stelle ist darauf zu achten, dass die Verwendung von Pseudonymen, die personenbezogene Bestandteile enthalten, unterbleibt. So ist insbesondere die Verwendung der Organisations- und Stammnummer des jeweiligen Beschäftigten als Pseudonym datenschutzrechtlich unzulässig, da die Stammnummer das Geburtsdatum des Beschäftigten enthält.

Die Übermittlung der Auskünfte über die in konkreten Zeiträumen aufgelaufenene Haushaltsbelastung bezüglich der für das geförderte Projekt tätigen Mitarbeiter durch die Bezügestelle an die Lehrstuhlverwaltung zum Nachweis der ordnungsgemäßen Verwendung der Fördermittel ist gemäß Art. 18 Abs. 1 i.V.m. Art. 17 Abs. 3 Satz 1 Fall 3 BayDSG zulässig, da diese Datenübermittlung für Zwecke der Rechnungsprüfung erfolgt. Ebenfalls aufgrund dieser Rechtsgrundlage ist die Übermittlung der pseudonymisierten Daten durch die Lehrstuhlverwaltung an die betreffende Einrichtung der Forschungsförderung zum Nachweis des Eingenanteils zulässig.

Ich habe den Datenschutzbeauftragten der betreffenden Hochschule gebeten, dieses neue Verfahren allen mit der Erstellung von Verwendungsnachweisen befassten Lehrstühlen zur Kenntnis zu bringen und dafür Sorge zu tragen, dass umgehend von einer ggf. bisher abweichenden Verfahrenspraxis Abstand genommen wird. Zudem habe ich gebeten, dieses Verfahren den Datenschutzbeauftragten der bayerischen Universitäten und Fachhochschulen vorzustellen. Der betroffene universitäre Datenschutzbeauftragte hat mir beides zugesagt.

Schließlich möchte ich noch darauf hinweisen, dass dieses Verfahren auch in vergleichbaren Fallgestaltungen außerhalb des Hochschulbereichs, in denen eine öffentliche Stelle die ordnungsgemäße Erbringung des Eigenanteils zur Erlangung von Fördermitteln oder die ordnungsgemäße Verwendung von Fördermitteln (insbesondere Personalkostenzuschüssen) gegenüber dem Zuwendungsgeber mitarbeiterbezogen und Euro-genau nachzuweisen hat, Anwendung finden sollte. So kann dieses Verfahren sinngemäß auch im kommunalen Bereich angewandt werden, da die Inanspruchnahme der Ausgabemittel dort gem. § 26 Abs. 2 Satz 1 der Kommunalhaushaltsverordnung ebenfalls in Haushaltsüberwachungslisten oder auf andere geeignete Weise zu überwachen ist.

22.2 Referentendatenbanken bei Erwachsenenbildungseinrichtungen

Eine betroffene Referentin machte mich darauf aufmerksam, dass das Bildungswerk eines meiner Kontrollkompetenz unterliegenden, bayernweit tätigen Berufsverbandes gerade im Begriff war, eine zentrale, landesweite Datenbank über die mehr als 300 für das Bildungswerk nebenberuflich tätigen Referenten einzurichten. Ziel des Bildungswerks war es, die bereits bisher sowohl in der Zentrale als auch in den Außenstellen vorgehaltenen Referentenvorschlagslisten mit sehr uneinheitlichen Datenbeständen in einer einzigen, einheitlichen Referentendatenbank zusammenzuführen. Damit sollte auch eine der Voraussetzungen für die Zertifizierung des Bildungswerkes erfüllt werden, die das Staatsministerium für Unterricht und Kultus im Jahr 2003 allen Trägern von Erwachsenenbildungseinrichtungen in Bayern empfohlen hatte.

Vor diesem Hintergrund hatte das Bildungswerk seine Referenten darum gebeten, einen „Lebenslauf“ mit Angaben zu Schul- und Weiterbildung und Berufs- und sonstiger Tätigkeit sowie mit einem Foto und Kopien von Qualifikationsnachweisen (Zeugnisse, Zertifikate u.ä.) einzureichen. Weiter war ein „Datenblatt“ von den Referenten auszufüllen und zu unterschreiben, worin u.a. um Angabe von Geburtstag, Bankverbindung und regionalem Einsatzgebiet gebeten worden war. Durch Unterzeichnung einer „Erklärung zum Datenschutz“ sollten die Referenten ihr Einverständnis mit der Speicherung, Nutzung und Weitergabe - auch an nicht näher bezeichnete außenstehende Dritte - ihrer persönlichen Daten einschließlich ihres Fotos erklären. Zudem war von ihnen ein „Fragebogen über Beziehungen zur Scientology-Organisation“ auszufüllen. In dem zugehörigen Anschreiben hatte das Bildungswerk schließlich erklärt, dass auch die Referenten, die nicht in die Datenbank aufgenommen werden wollten, alle Unterlagen zurücksenden müssten.

Die betroffene Referentin verweigerte die Rücksendung der Unterlagen und bat mich um datenschutzrechtliche Überprüfung der Angelegenheit.

In seiner ausführlichen Stellungnahme wies der Berufsverband zunächst darauf hin, dass die Angabe der persönlichen Daten nur mit Einwilligung der Referenten erfolge. Aufgrund der angestrebten Zertifizierung setze allerdings die weitere Ausübung ebenso wie die Neubegründung einer Referententätigkeit voraus, dass dem Bildungswerk die notwendigen, in den Vordrucken als Pflichtangaben bezeichneten Daten mitgeteilt würden. Zudem sei nach Art. 10

Abs. 2 Erwachsenenbildungsförderungsgesetz (EBFöG) der Einsatz geeigneter Lehrkräfte Voraussetzung für die Gewährung von staatlichen Fördermitteln. Sodann begründete der Berufsverband die durch die versandten Unterlagen beabsichtigten Datenerhebungen im einzelnen: So sei es, um die Qualifikation der Referenten feststellen zu können, erforderlich, einen Lebenslauf einschließlich Qualifikationsnachweisen zu erhalten. Die Angabe des Geburtsdatums diene als Unterscheidungsmerkmal bei Namensgleichheit. Die Angabe der Kontoverbindung sei für die Honorarzahlung notwendig; eine andere Zahlungsart scheide künftig aus. Schließlich sollten aufgrund der Angabe des regionalen Einsatzgebietes zukünftig unnötige Anfragen bei den Referenten vermieden werden.

Im Verlaufe eines umfangreichen Schriftwechsels habe ich den Aufbau der gegenständlichen Referentendatenbank gegenüber dem Berufsverband aus datenschutzrechtlicher Sicht wie folgt bewertet:

Eine Einwilligung ist nur dann datenschutzrechtlich wirksam, wenn sie den in Art. 15 Abs. 2 bis 4 BayDSG aufgestellten Anforderungen entspricht. Dabei räumt der bayerische Gesetzgeber insbesondere der Freiwilligkeit der Einwilligung einen hohen Stellenwert ein.

Im Hinblick auf die formalen Datenschutzanforderungen an Einwilligungen wies die den Referenten zugesandte „Erklärung zum Datenschutz“ zahlreiche Mängel auf:

Das Schriftformerfordernis des Art. 15 Abs. 3 Satz 1 BayDSG war zwar erfüllt. Auch kam der Berufsverband der Anforderung des Art. 15 Abs. 4 BayDSG nach, die Einwilligungserklärung im äußeren Erscheinungsbild hervorzuheben. Der in Art. 15 Abs. 2 BayDSG aufgestellten Verpflichtung, die Betroffenen auf den Zweck der Erhebung, Verarbeitung oder Nutzung hinzuweisen, wurde aber nur im Anschreiben entsprochen. Aus Transparenzgründen hätte dieser Hinweis jedoch unmittelbar in die zu unterzeichnende „Erklärung zum Datenschutz“ aufgenommen werden müssen; zumindest hätte in der „Erklärung zum Datenschutz“ insoweit ausdrücklich auf das Anschreiben Bezug genommen werden müssen. Des weiteren enthielt die „Erklärung zum Datenschutz“ keinen ausdrücklichen Hinweis auf die Freiwilligkeit; diese ergab sich nur mittelbar aus dem Gesamtzusammenhang der Unterlagen. Um der gesetzlichen Verpflichtung des Art. 15 Abs. 2 BayDSG zum Hinweis auf die Empfänger vorgesehener Datenübermittlungen nachzukommen, genügte es auch nicht, in der „Erklärung zum Datenschutz“ lediglich pauschal auf „Dritte“ zu verweisen. Nicht nur aus Gründen einer vermutlich erhöhten Akzeptanz bei den betroffenen Referenten wäre zumindest der Kreis der in Betracht kommenden Dritten genau zu bezeichnen gewesen. Schließlich wies zwar der Berufsverband in der „Erklärung zum Datenschutz“ darauf hin, dass die Referenten die Einwilligung jederzeit widerrufen können. Im Gegensatz zu der gesetzlichen Verpflichtung des Art. 15 Abs. 2 BayDSG wurden die Referenten aber nicht ausdrücklich unter Darlegung der Rechtsfolgen darauf aufmerksam gemacht, dass sie die Einwilligung verweigern können. Da jedoch im Falle der Verweigerung oder des Widerrufs der Einwilligung eine Aufnahme oder Fortsetzung der Referententätigkeit nicht möglich war, hätte diese Rechtsfolge den Betroffenen klar vor Augen geführt werden müssen.

Ich habe den Berufsverband daher aufgefordert, die „Erklärung zum Datenschutz“ unverzüglich in einen datenschutzkonformen Zustand zu bringen.

Bereits nach einer Woche sandte mir der Berufsverband eine entsprechend meinen Forderungen überarbeitete „Erklärung zum Datenschutz“ zu. Diese Überarbeitung enthielt nun einen deutlichen Hinweis auf die Freiwilligkeit der Einwilligung. In einem eigenen Absatz wurde nun auch in der „Erklärung zum Datenschutz“ auf den Zweck der Datenerhebung, -verarbeitung und -nutzung ausdrücklich hingewiesen. Auf die Weitergabe von Daten an Dritte wurde erfreulicherweise ganz verzichtet; nach Aussage des Berufsverbands würden in Zukunft die Referenten über entsprechende Anfragen von Interessenten informiert, sodass sie selbst entscheiden könnten, ob sie sich mit den Interessenten in Verbindung setzen wollten oder nicht. Zusätzlich wurde in einen weiteren Absatz der Hinweis aufgenommen, dass bei Verweigerung oder Widerruf der Einwilligung die personenbezogenen Daten des Betroffenen nicht in der zentralen Referentendatenbank erfasst oder wieder gelöscht werden.

Diese erheblich überarbeitete „Erklärung zum Datenschutz“ habe ich akzeptiert, von dem Berufsverband aber gefordert, die neue „Erklärung zum Datenschutz“ auch all den Referenten, die die ursprüngliche Fassung bereits unterzeichnet hatten, erneut vorzulegen. Dies sagte der Berufsverband zu.

Bezüglich des Anschreibens habe ich den Berufsverband darauf hingewiesen, dass im Falle der Verweigerung der Einwilligung gerade keine Pflicht besteht, die zugesandten Unterlagen auszufüllen und an das Bildungswerk zurückzusenden. Der Berufsverband sagte zu, diese Passage künftig zu streichen.

Um die Voraussetzungen sowohl für die vom Kultusministerium empfohlene Zertifizierung als auch für die weitere Förderung gem. Art. 10 Abs. 2 EBFöG zu erfüllen, aber zum Teil auch aus praktischen Erwägungen habe ich die mit den Vordrucken „Lebenslauf“ und „Datenblatt“ erfolgende Erhebung der als „Pflichtangaben“ gekennzeichneten Daten in

Anbetracht der eingehenden Erläuterungen des Berufsverbands als erforderlich angesehen. Maßstab meiner Prüfung war dabei der Grundsatz, dass eine bayerische öffentliche Stelle auch auf der Grundlage einer Einwilligung nur diejenigen personenbezogenen Daten erheben, verarbeiten oder nutzen darf, die sie zur ordnungsgemäßen Erfüllung ihrer gesetzlichen - d.h. auch satzungsgemäßen - Aufgaben tatsächlich benötigt. So verzichtete der Berufsverband schließlich auch auf die Einreichung von Fotos.

Da zahlreiche bayerische Beamte eine dem „Fragebogen über Beziehungen zur Scientology-Organisation“ entsprechende Erklärung bereits im Rahmen ihrer Einstellung unterzeichnet haben, habe ich die erneute Abgabe einer solchen Erklärung bei diesen Personen als datenschutzrechtlich bedenklich angesehen. Der Berufsverband erklärte sich insofern dazu bereit, in solchen Fällen auf die Unterzeichnung des Fragebogens zu verzichten. Ein entsprechender Hinweis wurde daraufhin in diesen Vordruck aufgenommen.

Zuletzt möchte ich ausdrücklich festhalten, dass die von mir hier allgemein aufgestellten Datenschutzanforderungen an Referentendatenbanken selbstverständlich auch von sämtlichen Erwachsenenbildungseinrichtungen anderer bayerischer öffentlicher Träger zu beachten sind.

23 Technischer und organisatorischer Bereich

23.1 Allgemeine Anmerkungen

Die Aufgaben im technisch-organisatorischen Bereich waren in diesem Berichtszeitraum im Wesentlichen geprägt von der Erbringung telefonischer und schriftlicher Beratungsleistungen für Bürger und verschiedenste öffentliche Einrichtungen, von beratender Unterstützung im Rahmen des Bayerischen Behördennetzes und dortiger zentraler Komponenten sowie von der Beschäftigung mit aktuellen Fragestellungen und Vorhaben aus dem Bereich der Medizin und der medizinischen Forschung.

Trotz des nach wie vor steigenden Bedarfs an Beratungsleistungen wurden auch Kontrollen auf Stichprobenbasis und aus aktuellem Anlass durchgeführt. Bezüglich der Einzelheiten hierzu verweise ich auf die nachfolgenden Ausführungen.

23.2 Bayerisches Behördennetz (BayKOM)

In Nr. 22.1.1 meines 21. Tätigkeitsberichts habe ich berichtet, dass mit Bekanntmachung vom 15.06.2004 die Bayerische Staatsregierung die „Richtlinie für den koordinierten Einsatz der Informations- und Kommunikationstechnik (IuK) in der bayerischen Staatsverwaltung (IuK-KoordR)“ erlassen und gleichzeitig damit der Zentralen IuK-Leitstelle (ZIL) im Staatsministerium des Innern die Aufgabe zugewiesen hat, eine IuK-Strategie zu erstellen und fortzuschreiben.

IuK-Strategie

Diese IuK-Strategie für die Bayerische Staatsverwaltung (BayIuKS) liegt nunmehr seit Ende 2005 vor und legt Ziele, Prioritäten und Strukturen des IuK-Einsatzes für alle staatlichen bayerischen Behörden, Gerichts- und Hochschulverwaltungen verbindlich fest. In der IuK-Strategie werden neben den zu erreichenden drei Hauptzielen der Qualitätssteigerung, der kontrollierten Modernisierung und der Einsparung von Ausgaben in Ziffer 1.5 in der nachfolgenden Ziffer 1.7 sieben grundlegende und zu beachtende Anforderungen beim Einsatz der IuK-Technik beschrieben.

Als eine dieser sieben Anforderungen wird explizit die Gewährleistung von Sicherheit und Datenschutz genannt (Ziffer 1.7 Buchstabe g) BayIuKS). Eigentlich handelt es sich dabei um eine Selbstverständlichkeit, dennoch will ich in Anbetracht der Größe und Komplexität der gesteckten Aufgabe die Benennung dieser Grundanforderung in der IuK-Landesstrategie positiv erwähnen und hervorheben.

Umgesetzt werden soll diese Anforderung im Bereich eGovernment insbesondere durch „eine ganzheitliche Lösung der Sicherheitsanforderungen hinsichtlich Authentifizierung, Signierung und Verschlüsselung“ (Ziffer 1.8.3 BayIuKS).

Im Rahmen der fortschreitenden Arbeiten der Zentralen IuK-Leitstelle wurden von dieser mittlerweile eine ganze Reihe grundlegender Vorgaben in Form von

- verbindlichen IuK-Standards (bestehend aus derzeit 17 Einzeldokumenten),
- verbindlichen allgemeinen Richtlinien (bestehend aus derzeit fünf Einzeldokumenten) und
- verbindlichen Richtlinien für die IuK-Sicherheit (bestehend aus derzeit 15 Einzeldokumenten) erlassen.

Eine Liste all dieser Einzeldokumente wurde in der Bekanntmachung des Bayerischen Staatsministeriums des Innern vom 10. Dezember 2004, Az.: IZ7-1073-5, geändert mit Bekanntmachung vom 7. September 2005 (AllMBl, S. 331) und Bekanntmachung vom 27. Juni 2006 (AllMBl, S. 235) mit der Bezeichnung „Standards und Richtlinien für die Informations- und Kommunikationstechnik (IuK) in der

bayerischen Verwaltung (IuKSR)“ veröffentlicht. Diese Bekanntmachung sowie die zugehörigen Einzeldokumente stehen im Bayerischen Behördennetz zum Abruf bereit.

Basiskomponenten

Darüber hinaus wurden auch Basiskomponenten bestimmt. Dabei handelt es sich um eine einheitliche IuK-Infrastruktur, also um Einrichtungen und Verfahren, die von der Staatskanzlei und den Geschäftsbereichen der Staatsministerien gemeinsam genutzt werden (sollen). Mit Hilfe der Definition und Realisierung dieser Basiskomponenten soll u.a. die in der bayerischen Verwaltung bestehende Vielzahl unterschiedlicher Verfahren für im Grunde die gleiche grundlegende Aufgabe erheblich reduziert werden. Dazu zählen beispielsweise Verfahren für die Verschlüsselung und Signatur samt zugehöriger Public Key Infrastructure (PKI), die Dokumenten- und Schriftgutverwaltung, die Personalverwaltung und ein Integriertes Zeitmanagementsystem. Eine Liste der Basiskomponenten (BayITB) ist ebenfalls im Bayerischen Behördennetz abrufbar.

Auf die Basiskomponente „Dokumenten- und Schriftgutverwaltung“ gehe ich in Nr. 23.5.5, Datenschutzanforderungen an ein Dokumentenmanagementsystem, und auf die Basiskomponente „Zeitmanagementsystem (ZES)“ sowie die damit in Zusammenhang stehenden datenschutzrechtlichen Aspekte gehe ich in Nr. 19.3 näher ein.

Elektronische Signatur, Verschlüsselung und Public Key Infrastructure (PKI)

Bereits seit meinem 19. Tätigkeitsbericht, 2000, habe ich immer wieder diese Themenbereiche behandelt und die zügige flächendeckende Einführung geeigneter Verfahren zu Signatur und Verschlüsselung sowie der zugehörigen Infrastruktur angemahnt. Ich halte diese Verfahren für eine ganz grundlegende Voraussetzung für datenschutzgerechtes Verwaltungshandeln im Rahmen des eGovernment.

Als erforderlich betrachte ich dabei nicht nur die Absicherung des E-Mail-Verkehrs von Behörden mit Behörden und von Behörden mit dem Bürger, sondern auch die Absicherung von Datenverkehr jeglicher anderen Art, also z.B. von Online-Anwendungen, Filetransfer und auch von Speicherungen elektronischer Dokumente. Bei jeder elektronischen Datenverarbeitung und Übertragung personenbezogener Daten sind geeignete Maßnahmen zur Sicherstellung von Integrität, Authentizität und Vertraulichkeit zu ergreifen.

– Die geeignete Maßnahme zur Sicherstellung der Integrität und Authentizität ist die elektronische Signatur - in jeder Form ihrer Ausprägung, d.h. als einfache, fortgeschrittene oder als qualifizierte elektronische Signatur. Die jeweils anzuwendende Form von elektronischer Signatur wird bestimmt durch die Art und Schutzwürdigkeit der personenbezogenen Daten und durch entsprechende Rechtsvorschriften. Eine pauschal gültige Aussage, z.B. über die kategorische Anwendung einer bestimmten Form von elektronischer Signatur, lässt sich nicht treffen.

– Die geeignete Maßnahme zur Sicherstellung der Vertraulichkeit personenbezogener Daten bei Übertragung und Speicherung ist deren Verschlüsselung. Hierbei ist grundsätzlich danach zu unterscheiden, auf welcher Ebene die Verschlüsselung der Daten erfolgt - auf Anwendungsebene oder den darunterliegenden Sitzungs- und Transportebenen.

  Es soll hier nicht auf alle technisch verfügbaren Formen der Verschlüsselung, sondern nur auf die durch den Anwender initiierte asymmetrische Verschlüsselung eingegangen werden. Dazu sei auch lediglich angemerkt, dass tunlichst streng zwischen Verschlüsselungs- und Signaturschlüssel zu unterscheiden ist - insbesondere in deren Verwendung.

– Diese Art der Datenverschlüsselung setzt wie die Verwendung der elektronischen Signatur eine entsprechende leistungsfähige Public Key Infrastruktur (PKI) voraus. In Anbetracht der Vielzahl an Beschäftigten im öffentlichen Dienst sowie der unterschiedlichen Arten an zu generierenden und verwaltenden Schlüssel sind Aufbau, Bereitstellung und vor allem Betrieb einer solchen Einrichtung zweifelsohne eine ausgesprochen schwierige Aufgabe. Ohne Bewältigung der damit einhergehenden mannigfachen Schwierigkeiten ist aber eine gesicherte elektronische Kommunikation nicht möglich.

– Auf Transportebene ist das SSL-Protokoll die derzeit bekannteste Methode (Transportverschlüsselung) und wird auch im Behördennetz mehrfach angewendet. Sie verschlüsselt jeglichen Datenverkehr zwischen einem Web-Server und dem anfragenden Arbeitsplatz-PC. Sie setzt voraus, dass der Web-Server über ein Zertifikat (im Rahmen einer PKI) verfügt, welches der Benutzer bzw. sein Arbeitsplatz-PC als vertrauenswürdig akzeptiert. Auf die damit verbundenen Problematiken gehe ich in Nr. 23.6.4 näher ein.

  Eine weitere Methode der Verschlüsselung bezieht sich nicht auf die gesamte Verbindungsstrecke zwischen einem Arbeitsplatz-PC

und einem Server, sondern nur auf Teilstrecken in dieser gesamten Wegstrecke. Auch hier wird jeglicher Datenverkehr verschlüsselt. Diese Methode wird üblicherweise als Leitungsverschlüsselung bezeichnet und es ist geplant, diese auch im Bayerischen Behördennetz einzusetzen. Mit dieser Verschlüsselungstechnik werden dann Teilstrecken des Behördennetzes zwischen den jeweiligen Anschlussstellen (Eingangsroutern) der Behörden geschützt.

Ich halte dies für einen erheblichen Schritt in Richtung Sicherheit bei der Datenübertragung. Leider kann aber nicht davon ausgegangen werden, dass in naher Zukunft alle Teilstrecken des Bayerischen Behördennetzes derart abgesichert sind, so dass sich der Benutzer des Behördennetzes trotz der zentral bereitgestellten und sicherlich begrüßenswerten Maßnahme nicht sicher sein kann, dass seine Kommunikation zumindest ab Verlassen des eigenen Behördenbereiches und bis zum Eingang bei der angewählten Behörde in jedem Fall geschützt durch Verschlüsselung und somit vertraulich erfolgt. Auch diese Maßnahme gilt es konsequent und zügig umzusetzen und weiter auszubauen.

Zusammenfassung

In Nr. 22.1.1.1 meines 21. Tätigkeitsberichts habe ich die Vermutung geäußert, dass mit Schaffung der Zentralen IuK-Leitstelle eine Grundlage für eine kompetente und geschäftsübergreifend bindende Instanz für die Sicherheit der elektronischen Kommunikation innerhalb des Bayerischen Behördennetzes geschaffen würde. Diese Annahme hat sich im Berichtszeitraum vollauf bestätigt.

Die bisher in Form der entsprechenden Richtlinien und Standards geschaffenen organisatorischen Grundlagen müssen aber gepflegt, zügig vervollständigt und fortentwickelt werden.

Die eingeleiteten Realisierungsschritte und ergriffenen praktischen Umsetzungsmaßnahmen bzgl. Anwendung der elektronischen Signatur, Einsatz von Verschlüsselungstechniken und Schaffung von Basiskomponenten weisen in die richtige Richtung und müssen trotz aller vielfältigen Schwierigkeiten und Hemmnisse konsequent weiter beschritten und ausgebaut werden.

Nur dann ist im und mit dem Bayerischen Behördennetz datenschutzgerechtes Verwaltungshandeln möglich. Um dieses gemeinsame Ziel schnellstmöglich und treffsicher zu erreichen, steht meine Geschäftsstelle auch weiterhin gerne beratend zur Verfügung.

23.3 Behandlung von Spam-Mails

Die Themen Nutzung von E-Mail und anderen Internetdiensten am Arbeitsplatz sowie die Viren- und Spam-Filterung wurden zwar bereits unter Nr. 21.1 und Nr. 22.1.2 meines 21. Tätigkeitsberichts 2004 ausführlich behandelt. Wie meine Mitarbeiter aber im Rahmen von Prüfungen, Beratungen und Vorträgen immer wieder feststellen müssen, herrscht gerade bezüglich der Behandlung von Spam-Mails immer noch große Unsicherheit bei vielen Behörden. Deshalb gehe ich hier nochmals auf dieses Thema ein.

Um die Arbeitsbelastung der Mitarbeiter für das Erkennen und Aussortieren von Spam-Mails zu reduzieren, sind viele Behörden dazu übergegangen, vermeintliche Spam-Mails - soweit wie möglich - anhand verschiedener Kriterien automatisch als solche zu erkennen, um sie sodann zu kennzeichnen oder auszufiltern. Dabei sind sie sich durchaus im Klaren darüber, dass Spam-Filter zum einen nicht jede Spam-Mail zuverlässig identifizieren und zum anderen auch wichtige Nachrichten fälschlicherweise als vermeintliche Spam-Mails kennzeichnen.

Erkennung von Spam-Mails

Spam-Filter unterscheiden sich vor allem darin, welche Merkmale sie zur Filterung heranziehen.

Häufig wird auf Grund der IP-Adresse des Absenders gefiltert - das einzige Datum, das ein Spammer nicht ohne weiteres fälschen kann. Dabei können beispielsweise Nachrichten basierend auf einer Liste der bekannten IP-Adressen der Versender von E-Mail-Werbung oder von E-Mail-Nachrichten mit strafbarem bzw. nicht jugendfreiem Inhalt gefiltert werden. Mit Hilfe so genannter White- und Blacklists können sowohl bei den Mail-Servern als auch bei den Mail-Clients die „guten" und „schlechten" IP-Adressen erfasst werden, die sich zur Filterung nutzen lassen. Bei jedem Empfang einer Nachricht überprüft das Mail-Programm automatisch, ob der Absender in einer dieser Listen eingetragen ist. Findet das Programm beispielsweise den Absender in der Blacklist, wird die E-Mail als Spam eingestuft. Mit Hilfe der IP-Filterung werden in der Regel aber nicht nur einzelne E-Mail-Adressen identifiziert, sondern ganze Hosts und damit u.U. eine Vielzahl von Domains. Dabei ist zu bedenken, dass der Eintrag eines Hosts einer Domain in eine „schwarze Liste" dazu führt, dass alle E-Mails dieser Domain als Spam-Mail eingestuft werden - wodurch dann auch seriöse E-Mails von dieser Domain als Spam-Mail eingestuft werden. Außerdem ist zu berücksichtigen, dass Spammer mittlerweile in immer kürzeren Abständen ihre IP-Adresse wechseln, um damit die Erkennung ihrer E-Mails durch IP-Filter zu umgehen, so dass eine IP-Filterung letztlich häufig nur für Stunden oder Tage das leistet, was sie soll.

Eine weitere Möglichkeit zur Erkennung von Spam-Mails ist die Verwendung von Verfahren mit inhaltsbasierter Filterung. Dabei wird automatisch nach in den Nachrichten allgemein verwendeten Phrasen gesucht (z.B. „kostenlos“ oder „billig“). Verwendet werden dabei Listen mit Ausdrücken und Stichwörtern, die bekanntermaßen häufig in Spam-Mails vorkommen. Inhaltsbasierende Verfahren sind zwar aufwendiger, dafür ist aber die Qualität der Erkennung oft besser als die der IP-Filter. Man unterscheidet zwischen Verfahren, die mittels vorgegebener Muster (Heuristik) bekannte Spam-Inhalte erfassen, und statistischen Verfahren, die laufend anhand erkannter Spam-Mails trainiert werden und dabei selbstständig typische Kennzeichen von Spam erlernen.

Neben diesen beiden Filterkriterien gibt es noch eine Vielzahl von für sich alleine genommen relativ wenig aussagender Kriterien, die ein Anzeichen für Spam sein können. Deshalb verwenden viele Filtersysteme eine Kombination aller dieser Kriterien, in dem sie jedes Kriterium bewerten. Überschreitet die Summe dieser Bewertungen in einer E-Mail einen vordefinierten Schwellwert, so wird davon ausgegangen, dass es sich um eine Spam-Mail handelt.

Die aufgezeigten Filterkriterien stehen teilweise auch in den eingesetzten Mail-Programmen zur Verfügung. So bietet beispielsweise Outlook die Möglichkeit, eine erkannte Spam-Mail per vorab definierter Regel entsprechend dem individuellen Wunsch des Nutzers weiterzubehandeln. Diese eingebauten Filter der Mail-Programme können auch jederzeit um eigene Adressen und Begriffe erweitert werden. Die Nutzung der mit dem Mail-Programm mitgelieferten Filter stellt zwar eine einfache Lösung, aber sicherlich nicht die effektivste Anti-Spam-Lösung dar. Serverbasierte Produkte zur Spam-Bekämpfung sind in der Regel (noch) effektiver.

Technisch mögliche Behandlung von Spam-Mails

Nachdem eine E-Mail durch eines der o.g. Verfahren als Spam-Mail eingestuft wurde, ist es vor dem Hintergrund der Arbeitsersparnis für die Bediensteten sinnvoll, diese E-Mail auch einer möglichst automatischen Behandlung zuzuführen.

Rein technisch gesehen sind mehrere Vorgehensmöglichkeiten zur Spam-Behandlung gegeben:

Auf einem zentralen Mail-Server/Spam-Filter:

- Markierung der E-Mail als Spam-Mail und Weiterleitung an den Empfänger
- Blockung der E-Mail und damit einhergehende Unterdrückung der Weiterleitung der Original-E-Mail an den Empfänger
- Verweigerung der Annahme der E-Mail (Bounce)
- Löschung der E-Mail

Auf dem Mail-Client:

- Farbliches Kennzeichnen der E-Mail zur Unterscheidung von „regulärer“ E-Mail im Posteingangsfach
- Verschieben der E-Mail in einen speziellen Unterordner im eigentlichen Posteingangsfach
- Automatisches Löschen der E-Mail

Auch wenn diese vorgenannten Behandlungsformen technisch möglich sind, so sind diese jedoch nicht oder nicht ohne weiteres rechtlich zulässig.

Rechtlich zulässige Behandlung von Spam-Mails

Die Reichweite des Fernmeldegeheimnisses erstreckt sich auf den gesamten Übertragungsweg zwischen Absender und Empfänger einer E-Mail. Damit stellt jede automatische Maßnahme auch bereits zur Erkennung von Spam-Mail auf einem zentralen Mail-Server/Spam-Filter einen Eingriff in das Fernmeldegeheimnis dar.

Setzen die Maßnahmen zur Spam-Erkennung und anschließenden Spam-Behandlung dagegen erst auf dem Mail-Client des Bediensteten an und kann dieser selbst über deren Ausprägung und Anwendung bestimmen, so ist das Fernmeldegeheimnis nicht berührt.

Im Falle des Verbotes der privaten E-Mail-Nutzung kann die zentrale Erkennung, Blockung, Markierung oder Löschung offensichtlicher Spam-Mails aus datenschutzrechtlicher Sicht zur Gewährleistung der Aufrechterhaltung des Dienstbetriebes akzeptiert werden. Die damit einhergehende Kontrolle der E-Mail-Nutzung halte ich im Rahmen der Erforderlichkeit für zulässig (vgl. Nr. 21.1 meines 21. Tätigkeitsberichts), wobei eine Blockung oder Löschung auf Grund der Möglichkeit des Verlusts von fälschlicherweise als Spam erkannten E-Mails aus meiner Sicht nicht sinnvoll ist.

Eine weitergehende manuelle inhaltliche Kontrolle durch den Arbeitgeber von gekennzeichneten Spam-Mails darf im Einzelfall nur dann erfolgen, wenn ein begründeter Missbrauchsverdacht, insbesondere bezüglich strafrechtlicher Handlungen oder hinsichtlich des Verrats von Dienstgeheimnissen, besteht.

Gestattet eine Dienststelle ihren Bediensteten die private Nutzung des E-Mail-Dienstes, ist sie ihnen

gegenüber Telekommunikations- bzw. Teledienste-Anbieter und zur Wahrung des Fernmeldegeheimnisses gemäß § 88 Telekommunikationsgesetz (TKG) verpflichtet. Dabei spielt es keine Rolle, ob der Arbeitgeber diese Dienste direkt selbst anbietet oder sich dazu eines Anderen (z.B. des Netzbetreibers oder des Mail-Providers) bedient. Dem Arbeitgeber ist es somit untersagt, sich oder anderen über das für die geschäftsmäßige Erbringung der Telekommunikationsdienste erforderliche Maß hinaus Kenntnis vom Inhalt oder den näheren Umständen der Telekommunikation zu verschaffen (§ 88 Abs. 3 TKG).

Eine zentrale Erkennung, Markierung, Blockung oder Löschung vermeintlicher Spam-Mails ist in diesem Fall ohne diesbezügliche Einwilligung der Betroffenen rechtlich nicht zulässig.

Nach Art. 75 a Abs. 1 Nr. 1 BayPVG hat der Personalrat sowohl im Fall der rein dienstlichen als auch im Fall der zugelassenen privaten Nutzung über Kontrollmaßnahmen zur E-Mail-Nutzung am Arbeitsplatz (hier Spam-Erkennung und Spam-Behandlung) mitzubestimmen. Ich empfehle daher aus datenschutzrechtlicher Sicht, über die Nutzung von E-Mail eine Dienstvereinbarung mit der Personalvertretung abzuschließen, in der auch die Maßnahmen zur Spam-Erkennung und -Behandlung eindeutig geregelt werden. Diese Dienstvereinbarung sollte dann genau regeln, welche Maßnahmen auf welchem Rechner zur Spam-Bekämpfung von Seiten des Arbeitgebers ergriffen werden sollen, welche personenbezogenen Daten dabei anfallen und ob und wofür diese Daten genutzt werden.

Die Bediensteten sind über zentrale Maßnahmen zur Spam-Erkennung und -bekämpfung vorab zu unterrichten.

Bei zugelassener privater E-Mail-Nutzung ist überdies die Einwilligung jedes einzelnen Bediensteten erforderlich. Diese Einwilligung muss ausdrücklich und insbesondere vor Beginn der Spam-Erkennungs- und Bekämpfungsmaßnahmen von allen Bediensteten schriftlich und freiwillig erteilt werden. Eine mutmaßliche Einwilligung genügt den rechtlichen Anforderungen nicht. Die Mitarbeiter sind dabei umfassend darüber zu unterrichten, welche Daten im Rahmen der Spam-Bekämpfung über sie erhoben, verarbeitet oder genutzt werden.

Der Dienstherr kann die Gestattung der privaten Nutzung von dem Vorliegen der o.g. Einwilligung abhängig machen (vgl. Nr. 21.1 meines 21. Tätigkeitsberichts).

Fazit

Die Bekämpfung von Spam-Mails ist eine sachliche Notwendigkeit. Dazu stellen sich aber nicht nur technische Aufgaben und Herausforderungen. Vor dem Hintergrund des Fernmeldegeheimnisses und der Mitbestimmungsrechte sind vorrangig die komplexen rechtlichen Probleme zu bewältigen.

Dabei hilft auch die durch die Zentrale IuK-Leitstelle am 01.06.2006 für die bayerische Staatsverwaltung erlassene verbindliche „Richtlinie für die Nutzung von Internet und E-Mail in der bayerischen Staatsverwaltung“ (BayITR-05) mit der Anlage: „Vorschlag für ein Begleitschreiben der Behörde zur Einwilligungserklärung“. Diese Richtlinie ist auch im Bayerischen Behördennetz zum Abruf bereitgestellt worden. In Nr. 20.1 gehe ich näher auf diese Richtlinie ein.

23.4 Erkenntnisse aus Prüfungen

23.4.1 Vorbemerkungen

Aus den nachgenannten Prüfungen ergaben sich wieder eine Reihe von Erkenntnissen bzgl. der praktischen Schwierigkeiten in der Umsetzung von technisch-organisatorischen Datenschutz- und Datensicherheitsmaßnahmen. Bedauerlicherweise handelt es sich dabei nicht um grundlegend neue Probleme, sondern um Mängel, auf die meine Mitarbeiter seit vielen Jahren unmittelbar aufmerksam machen und auf die auch in zurückliegenden Tätigkeitsberichten immer wieder hingewiesen wurde. Im Nachfolgenden werden einige näher beschrieben:

Individuelle Benutzerkennungen und -passworte

Obwohl die IuK-Technik nun schon seit vielen Jahren im öffentlichen Bereich wie selbstverständlich im Einsatz ist, ist es leider immer noch nicht selbstverständlich, dass jeder berechtigte Benutzer auch über eine eigene Benutzerkennung zur Anmeldung am DV-System bzw. an einer spezifischen Anwendung und über ein nur ihm bekanntes persönliches Passwort verfügt. Dieses persönliche Passwort muss der Benutzer auch jederzeit selbst ändern können. Nach vordefiniertem Zeitablauf von ca. drei Monaten soll die IuK-Technik den Anwender zwingen, sein Passwort auch tatsächlich zu ändern, wenn er es nicht von sich aus getan hat.

Einbindung des behördlichen Datenschutzbeauftragten

Obwohl in Art. 26 Abs. 3 BayDSG klar und unmissverständlich bestimmt ist, dass Öffentliche Stellen ihren behördlichen Datenschutzbeauftragten rechtzeitig vor dem Einsatz oder der wesentlichen Änderung eines automatisierten Verfahrens eine Verfahrensbeschreibung mit den zur Bewertung erforderlichen Unterlagen zur Verfügung zu stellen haben, gibt es hier leider immer wieder Versäumnisse festzustellen.

So wird der behördliche Datenschutzbeauftragte mitunter gar nicht oder viel zu spät eingebunden. Die auf seine Anregungen unter Umständen erforderlichen Änderungen an der Konzeption oder gar an der bereits erfolgten Realisierung werden dann eventuell sehr aufwändig oder können im Extremfall angeblich nicht mehr berücksichtigt werden. Derartige Erschwernisse und unnötigen Kosten können bei einer frühzeitigen Beteiligung des behördlichen Datenschutzbeauftragten in aller Regel ohne großen Aufwand vermieden werden.

Datenschutzrechtliche Freigabe von Verfahren

Mit der vorgenannten rechtzeitigen Beteiligung des eigenen behördlichen Datenschutzbeauftragten geht einher die nach Art. 26 Abs. 3 Satz 2 BayDSG gesetzlich vorgeschriebene datenschutzrechtliche Freigabe durch diesen. Bei dieser Freigabe handelt es sich nicht nur um einen formalen Akt, der einfach mal so abgehakt wird. Es soll vielmehr damit sichergestellt und dokumentiert werden, dass nicht nur funktionale Aspekte bei automatisierten Verfahren Berücksichtigung gefunden haben, sondern auch datenschutzrechtliche Rahmenbedingungen und Aspekte angemessen geprüft und realisiert wurden. Auch hier ist aber leider immer noch mangelndes Bewusstsein festzustellen.

Internet-Datenschutz-Erklärung

Nahezu jede öffentliche Einrichtung verfügt mittlerweile über einen eigenen Internet-Auftritt. Dabei werden zum Teil große Anstrengungen unternommen, um diese Homepage möglichst informativ, benutzerfreundlich und ansprechend zu gestalten. Dennoch fehlen zum Teil elementarste Bestandteile, wie eben die nach § 4 Abs. 1 Teledienstedatenschutzgesetz (TDG) vorgeschriebene Datenschutzerklärung, eine vollständige Anbieterkennzeichnung/ Impressum nach § 6 Teledienstegesetz (TDG) oder das Angebot zur verschlüsselten Kommunikation per E-Mail. Der Kürze halber verweise hier auf meine detaillierten Ausführungen zu Rechtsgrundlagen und Inhalten in den Nrn. 22.2.2.2 und 22.2.2.3 meines 20. Tätigkeitsberichts.

Verschluss personenbezogener Unterlagen und Papierentsorgung

Mit zunehmender Verbreitung der IuK-Technik scheint das Erfordernis nach datenschutzgerechtem Umgang mit Papier im allgemeinen Bewusstsein in den Hintergrund zu rücken. Dies ist mir nicht nachvollziehbar, denn gerade mit dem Einsatz der IuK-Technik hat die Produktion von schriftlichen Unterlagen auch mit personenbezogenen Daten enorm zugenommen.

Dabei wird anscheinend auch übersehen, dass nicht nur die elektronisch gespeicherten Daten vor unbefugter Kenntnisnahme u.a. zu schützen sind, sondern auch und nach wie vor gedruckte oder geschriebene personenbezogene Daten. Die besten und aufwändigsten Schutzmechanismen im Bereich der IuK-Technik relativieren sich hinsichtlich ihrer Wirksamkeit sofort, wenn andererseits personenbezogene Unterlagen/Akten in frei zugänglichen Diensträumen oder Gebäudeteilen offen gelagert werden oder wenn Fehlablichtungen, Fehldrucke, Zwischenmaterial oder korrigierte Schreiben u.ä. lediglich über normalen Hausmüll oder das allgemeine Altpapier entsorgt werden.

So fehlt es oftmals an Vorschriften und Regelungen zum Verschluss von Diensträumen, zum Verschluss von personenbezogenen Unterlagen und zur datenschutzgerechten Entsorgung von Papierunterlagen. Sind solche vorhanden, fehlt es gelegentlich an der nötigen internen Kontrolle.

Teilweise fehlen auch geeignete Behältnisse oder Aktenvernichter gänzlich oder sind zumindest nicht in ausreichender Anzahl vorhanden. Auch wenn dies in Zeiten knapper Haushaltsmittel schwierig ist, so müssen doch dafür die erforderlichen Mittel unbedingt aufgebracht werden.

In den folgenden Abschnitten gehe ich auf weitere ausgewählte Prüfungsergebnisse im Einzelnen näher ein.

23.4.2 Geprüfte Einrichtungen

Im Berichtszeitraum habe ich bei folgenden Dienststellen die Einhaltung der gebotenen technischen und organisatorischen Datensicherheits- und Datenschutzmaßnahmen überprüft:

- Klinikum Großhadern der Ludwig-Maximilian-Universität München - TempoBy
- Klinikum Großhadern der Ludwig-Maximilian-Universität München - Biomaterialbanken
- Klinikum rechts der Isar der Technischen Universität München - Biomaterialbanken
- Klinik und Poliklinik für Psychiatrie und Psychotherapie des Universitätsklinikums München
- Universitätsklinikum Regensburg
- Stadtwerke Erding

- Landratsamt Dachau
- Landratsamt Traunstein
- Georg-Simon-Ohm-Fachhochschule Nürnberg
- Sigmund-Schuckert-Gymnasium Nürnberg
- Gymnasium München-Moosach
- Münchenstift GmbH - Hauptverwaltung -
- Landeshauptstadt München Zentralbibliothek Gasteig

Die Überprüfungen erstreckten sich neben den klassischen Ansätzen der Daten- und Netzwerksicherheit sowie der organisatorischen Aspekte insbesondere auf dortige spezielle Prozesse oder Anwendungen. Schwerpunkte der Prüfungen im Berichtszeitraum waren der Umgang mit Biomaterial und Biomaterialbanken an den Universitätskliniken, medizinische Forschungsvorhaben und damit zusammenhängende landesweite oder -übergreifende Netzwerkanwendungen sowie der Einsatz von RFID-Technik (Remote Frequency Identification) im öffentlichen Bereich.

Zu den daraus gewonnen Erkenntnissen verweise ich auf die nachfolgenden Abschnitte.

23.4.3 Verfahrensfreigabe lokal betriebener Systeme in Universitätsklinika

Im Rahmen von technisch-organisatorischen Prüfungen im Berichtszeitraum wurde insbesondere im Bereich der Universitätsklinika folgende Problematik deutlich:

Neben den zentral durch die IT-Abteilung betriebenen IT-Systemen wie Krankenhausinformationssystemen (KIS) und Radiologiesystemen sind insbesondere im Rahmen der Forschungstätigkeit eine Vielzahl von lokal aufgesetzten und administrierten IT-Systemen in den einzelnen Kliniken und Abteilungen vorhanden. Dies sind beispielsweise Datenbanken für klinische Studien, in denen die studienrelevanten medizinischen Daten der Patienten erfasst werden, oder aber abteilungsbezogene elektronische Patientenakten, die eine schnelle Auswertung der sonst nur auf Papier vorhandenen Dokumentation ermöglichen. Diese lokal betriebenen Systeme enthalten daher häufig sensible personenbezogene Patientendaten, die mit einem automatisierten Verfahren verarbeitet werden.

Dazu gelangen neben kommerziellen Produkten häufig auch eigen entwickelte Software-Produkte zum Einsatz, die z.T. von Studenten programmiert und gewartet werden. Die Dateneingabe erfolgt durch an den Studien beteiligtes Personal (Ärzte, Pflegekräfte, Study Nurses etc.), aber auch durch Studenten, die teilweise selbst nur wenige Monate am Klinikum arbeiten.

Diese Situation genügt nicht den Anforderungen des Bayerischen Datenschutzgesetzes. Sie ist in mehreren Punkten unbefriedigend:

- Der behördliche Datenschutzbeauftragte ist in die Verfahrenskonzeption nicht eingebunden. Auch der zentralen IT-Abteilung sind die Systeme samt deren Nutzung in der Regel nicht bekannt, selbst wenn die Beschaffung der Rechner häufig über die IT-Abteilung abgewickelt wird.
- Es wird daher nicht immer inhaltlich geprüft, welche Daten auf diesen Systemen gespeichert werden sollen und ob hierbei allgemeine, hausweite oder auch spezifische Mindeststandards an Sicherheit einzuhalten sind.
- Es ist nicht sichergestellt, dass vor Einführung derartiger Verfahren geprüft wird, ob sie den technisch-organisatorischen Sicherheitsanforderungen des Art. 7 BayDSG genügen, d.h. ob z.B. ausreichende Maßnahmen zum Schutz gegen unbefugte Kenntnisnahme der Patientendaten getroffen werden.
- Insbesondere wird nicht immer überprüft, unter welchen Umständen beispielsweise Daten aus diesen IT-Systemen das Haus verlassen können. Es kann dadurch der Fall eintreten, dass unter Umgehung der zentralen Firewall Verbindungen zu externen Netzen geschaffen werden, die weder der IT-Abteilung noch dem Datenschutzbeauftragten bekannt sind, und ggf. Risiken für das restliche Netzwerk des Hauses entstehen lassen.
- Auch die Einhaltung gesetzlicher Aufbewahrungs- bzw. Löschfristen kann nur sehr schwer kontrolliert werden.
- Es sind mehrfach parallele Datenbestände zu Patienten vorhanden, von denen jeweils nur die betreffende Abteilung weiß.
- Da dem Datenschutzbeauftragten diese Verfahren nicht bekannt und diese auch nicht datenschutzrechtlich gemäß Art. 26 BayDSG freigegeben sind, ist das nach Art. 27 BayDSG vorgeschriebene Verfahrensverzeichnis zwangsläufig unvollständig.

– Damit ist auch keine vollständige Auskunft an einen Patienten möglich, wo welche Daten über ihn gespeichert, verändert oder wohin sie übermittelt werden.

Eine derartige Konstellation ist jedoch weder im Sinne des behördlichen Datenschutzbeauftragten noch im Sinne der IT-Abteilung oder der Klinikumsleitung, da die Datenflüsse nicht mehr kontrolliert werden können.

Es empfiehlt sich daher, klinikumsweite Regelungen zur Nutzung medizinischer Daten für die Forschung und zum Eigenbetrieb von IT-Systemen festzulegen. Hierzu müssen u.a. folgende Punkte geregelt werden:

– Festlegung von Randbedingungen, unter denen personenbezogene Patientendaten in selbst betriebenen Systemen genutzt werden dürfen. Hierunter fällt insbesondere auch der Regelungsgegenstand, auf welche Daten Studenten unter welchen Umständen Zugriff haben dürfen und wie diese zur Verschwiegenheit verpflichtet werden.

– Vorgehensweise zur Meldung von durch Abteilungen und andere Organisationseinheiten selbst betriebener Systeme sowie frühzeitiger und umfassender Einbindung des behördlichen Datenschutzbeauftragten.

– Definition von hausweiten Mindestsicherheitsanforderungen, die von allen Systemen eingehalten werden müssen und Festschreibung eines systematischen Überprüfungsverfahrens hierfür. Hierunter fallen z.B. die Punkte personenbezogene Benutzerkennungen, differenzierte Zugriffsrechte, Protokollierung der Zugriffe, Verpflichtung der Mitarbeiter.

– Regelungen zur Einbindung selbst gewarteter Systeme in die internen Netze des Klinikums.

– Regelungen zur Anbindung selbst gewarteter Systeme an externe Netze und zu Datenübermittlungen an externe Partner.

Eine datenschutzrechtliche Freigabe nach Art. 26 BayDSG ist auch für lokal betriebene Verfahren zwingend nötig. Nur wenn diese beantragt und vom behördlichen Datenschutzbeauftragten nach Prüfung erteilt wird, ist sichergestellt, dass den datenschutzrechtlichen Belangen auch im Vorfeld ausreichend Rechnung getragen wird. Die Freigabe muss vor dem erstmaligen Einsatz des Verfahrens erfolgen, andernfalls darf das Verfahren nicht betrieben werden.

23.4.4 Aufbewahrung schulärztlicher Unterlagen

Aufgrund einer Eingabe eines Bürgers habe ich mich im Berichtszeitraum mit der Aufbewahrung schulärztlicher Unterlagen befasst. Hierzu ist Folgendes zu berücksichtigen:

Schulärztliche Unterlagen enthalten über einen längeren Zeitraum hinweg erfasste medizinische Daten wie z.B. Angaben zu Krankheiten, Diagnosen, körperlicher und geistiger Entwicklung der Schüler. Diese Daten unterliegen aus Datenschutzsicht einem besonderen Schutzbedarf sowie der ärztlichen Schweigepflicht und müssen daher für Schüler, aber auch für Schulleitung, Lehrer, Reinigungsdienst etc. unzugänglich aufbewahrt werden. Dies liegt in der Verantwortung des zuständigen öffentlichen Gesundheitsdienstes, der die schulärztlichen Untersuchungen durchführt. Gemäß Art. 80 Abs. 3 BayEUG (Bayerisches Gesetz über das Erziehungs- und Unterrichtswesen) ist dieser für die gesicherte Verwahrung der anfallenden Daten verantwortlich.

Werden Unterlagen in der Schule aufbewahrt, ist sicherzustellen, dass dies in abgeschlossenen Schränken / Räumen erfolgt, so dass sie nur dem Schularzt und seiner Hilfskraft zugänglich sind. Der Schlüssel zu den Schränken darf sich somit nur in der Obhut des schulärztlichen Dienstes befinden. Ein Deponieren des Schlüssels an mehr oder weniger frei zugänglichen Stellen ist keinesfalls statthaft. Die Schränke und deren Schlösser müssen stabil sein, zusätzlich sollte der Raum nach Möglichkeit nicht der breiten Öffentlichkeit zugänglich sein.

Die generell jedoch vorzuziehende Variante ist eine Lagerung der schulärztlichen Unterlagen in den Räumen des Gesundheitsdienstes. Hier ist einerseits der Beschlagnahmeschutz besser gewährleistet, da die Unterlagen in einer medizinischen Einrichtung aufbewahrt werden, andererseits kann der Gesundheitsdienst den Zugang durch die direkte Obhut besser kontrollieren. Gleichzeitig muss aber auch hier sichergestellt werden, dass nur die zuständigen Schulärzte Zugriff auf ihre jeweiligen Unterlagen haben und nicht beispielsweise ein Vielzahl von Mitarbeitern des Gesundheitsdienstes.

Auch bei der Aktenaussonderung und Vernichtung müssen die üblichen Anforderungen des Datenschutzes berücksichtigt werden. Insbesondere darf es zu keiner Durchbrechung der Sicherheitsmaßnahmen kommen, in dem z.B. Akten ungesichert zwischengelagert oder über den Papiermüll / normalen Reinigungsdienst der Schule entsorgt werden. Auch diesbezüglich ist der Gesundheitsdienst für den korrekten Umgang mit den Daten verantwortlich.

23.4.5 Einsatz von RFID in der Münchner Stadtbibliothek

Seit Anfang 2006 führt die Stadtbibliothek München in ihrer Zentralbibliothek im Gasteig sowie nach und nach in allen Stadtteilsbibliotheken die RFID-basierte Selbstverbuchung von Medien ein. Dabei steht RFID für Remote Frequency Identification, d.h. Identifikation und Lokalisierung von Objekten mittels Einsatzes von Funktechnik. Dazu werden alle Medien mit einem RFID-Chip ausgestattet und Terminals aufgestellt, an denen der Benutzer selbstständig Medien ausleihen und zurückgeben kann. Auch andere Bibliotheken in Deutschland befassen sich mit diesem Thema, da man sich von der RFID-basierten Selbstverbuchung Effizienzsteigerungen, besseren Service für die Kunden und Kosteneinsparungen erwartet.

Die eingesetzten RFID-Chips arbeiten auf einer Frequenz von 13,56 MHz, bei der normalerweise von einer Reichweite bis zu maximal 1 Meter - je nach Bauform und Umgebungsbedingungen - ausgegangen werden kann. Nach den praktischen Erfahrungen der Münchner Stadtbibliothek beträgt dort die Reichweite sogar nur 45 cm. Diese Entfernung ermöglicht einen Diebstahlschutz beim Durchschreiten von Schleusen, erschwert jedoch ein unbefugtes Auslesen der Daten durch Dritte.

Auf den Chips werden keine personenbezogenen Daten oder Angaben zum Buch gespeichert, sondern nur organisatorische Daten wie Mediennummer und besitzende Bibliothek. Diese Daten werden erst im IuK-System der Stadtbibliothek mit Angaben zu z.B. Autor, Titel etc. des Buches sowie den Entleihdaten des Benutzers verknüpft. Ein potentieller Angreifer erhielte dadurch selbst bei einem erfolgreichen Auslesen des Chips keine Informationen über den Entleiher.

Die Benutzerausweise sind derzeit noch Karten mit einem Barcode. Die Benutzernummer ist eine laufende Nummer, die keine Aussagen zum Bibliotheksbenutzer macht (z.B. codiertes Geburtsdatum). Zukünftig soll ein Ausweis mit einem RFID-Chip eingeführt werden; dies ist derzeit in der Planungsphase. Auch dann sollen jedoch keine personenbezogenen Daten auf dem Chip gespeichert werden.

Die Ausleihterminals sind so gestaltet, dass die Bücher in ein markiertes Feld gelegt werden müssen, so dass ein ungewolltes Ausleihen „im Vorbeigehen“ nicht möglich ist. Analog müssen bei der Rückgabe die Bücher einzeln in den entsprechenden Automaten gelegt werden. Das jeweilige Benutzerkonto ist an den Terminals nach dem Einlesen des Barcodes einsehbar, angezeigt werden die ausgeliehenen Medien sowie eventuell fällige Gebühren. Eine Historie früher bereits entliehener Bücher ist nicht vorhanden, sie ist auch für die Mitarbeiter der Bibliothek nicht abrufbar, da nur die letzten drei Entleiher eines Buches in den zugehörigen Exemplardaten gespeichert werden.

Unter der Voraussetzung, dass für das IuK-System der Bibliothek, mit dem die Benutzerkonten verwaltet werden, die üblichen Sicherheitsanforderungen gemäß Art. 7 BayDSG erfüllt sind, habe ich angesichts dieser Ausgestaltung des Verfahrens keine datenschutzrechtlichen Bedenken beim Einsatz von RFID in den Münchner Stadtbibliotheken. Die weiteren Entwicklungen, wie z.B. die Einführung des RFID-basierten Benutzerausweises, werde ich auch in Zukunft verfolgen.

23.4.6 Telefondatenerfassung bei Privatgesprächen und von Berufsgeheimnisträgern

Bezüglich der Telefondatenerfassung in Behörden werden im Rahmen von technisch-organisatorischen Prüfungen immer wieder die gleichen Verstöße festgestellt. So werden häufig detaillierte Verbindungsdaten (z.B. vollständige Zielnummer) von ausgehenden Telefongesprächen erfasst und ausgewertet, auch wenn es sich dabei um Privatgespräche handelt.

Bei Privatgesprächen, die vorab z.B. durch Eingabe einer PIN (Persönliche Identifikationsnummer) als solche gekennzeichnet wurden, dürfen die gespeicherten Daten aber ausschließlich für Abrechnungszwecke verwendet werden. Dazu ist gemäß Nr. 3.2.2.3 der Bekanntmachung des Bayerischen Staatsministeriums der Finanzen zur „Einrichtung und Benutzung dienstlicher Telekommunikationsanlagen“ (Dienstanschlussvorschriften-BayDAV; Bekanntmachung des Bayer. Staatsministeriums der Finanzen vom 07.11.1997, Nr. 63-H4700-1/418-73038, FMBl 1997, S. 280 ff. zuletzt geändert durch Bekanntmachung vom 27.11.2001, FMBl 2002, S. 471) lediglich die Auswertung folgender Daten erforderlich:

- Name des jeweiligen Bediensteten
- Nummer der rufenden Nebenstelle
- Datum, Anzahl, Dauer und Kosten der geführten Privatgespräche

Lediglich auf ausdrücklichen Wunsch des Betroffenen sind den Ausdrucken die Rufnummern der Angerufenen hinzuzufügen. Die erstellten Ausdrucke sind in verschlossener Form den Bediensteten zuzuleiten. Eine Kenntnisnahme durch Dritte ist grundsätzlich unzulässig.

Die gespeicherten Daten der Privatgespräche sind nach der Abrechnung unverzüglich, spätestens aber 3 Monate nach Ablauf des Abrechnungszeitraums, zu löschen. Maschinelle Ausdrucke und handschriftlich aufgezeichnete Daten sind zu vernichten.

Da es sich bei Telekommunikationsanlagen um technische Einrichtungen handelt, die zur Überwachung des Verhaltens oder der Leistung der Beschäftigten geeignet sind, unterliegen sie der Mitbestimmung der Personalvertretung. Daher sollte über die getroffenen Modalitäten eine schriftliche Dienstvereinbarung abgeschlossen werden.

Obwohl bereits in Nr. 13.3.2. meines 20. Tätigkeitsberichtes darauf hingewiesen wurde, welche Anforderungen an die Erfassung der Telefondaten von Berufsgeheimnisträgern zu stellen sind, sind nach wie vor viele Behörden unsicher darüber, welche Aufzeichnungen und Auswertungen bei Gesprächen von Personen erstellt werden dürfen, die einer besonderen Verschwiegenheitspflicht unterliegen. Daher gehe ich an dieser Stelle nochmals kurz auf die diesbezüglichen Regelungen der Nr. 3.1.5 der BayDAV ein:

Bei Telefonaten von Stellen und Personen, deren Telefonverkehr nicht der Aufsicht (z.B. Personalvertretungen in Personalangelegenheiten) oder im Rahmen einer freiwilligen Beratung (z.B. Drogen-, Gesundheits-, Ehe- und Familienberatung) einer besonderen Verschwiegenheitspflicht unterliegen, dürfen grundsätzlich nur die Leistungsentgelte festgehalten werden. Für die praktische Umsetzung bedeutet dies, dass derartige Gespräche entweder nur mit speziell dafür vorgesehenen Telefonapparaten oder nach spezifischer Kennzeichnung solcher Gespräche durch z.B. vorangehende Eingabe einer PIN geführt werden sollen.

23.4.7 Protokollierung von lesenden Zugriffen

Unter Protokollierung ist die Aufzeichnung von Daten zu verstehen, die einzelne Aktionen in einem System (Rechner, Netzwerk etc.) oder die Zustände eines Systems beschreiben. Zur Sicherstellung und zum Nachweis der Ordnungsmäßigkeit der Datenverarbeitung ist eine Protokollierung insbesondere von Datenzugriffen unerlässlich.

Dieser Verpflichtung zur Protokollierung kommen auch die meisten Behörden nach. Dabei wird allerdings häufig über das Ziel hinausgeschossen, indem jeder Datenzugriff (gleich welcher Art) protokolliert wird. Da es sich aber bei Protokolldaten um personenbezogene Daten handelt, dürfen bei einer Protokollierung nur diejenigen Daten erhoben, verarbeitet und genutzt werden, deren Kenntnis, Speicherung und Nutzung zur Aufgabenerfüllung der betreffenden Stelle notwendig sind. So ist eine Protokollierung lesender Zugriffe in der Regel nur erforderlich, wenn es sich beispielsweise um sehr sensible Anwendungen und Daten, um Zugriffe über öffentliche Netze sowie um Übermittlungen im Rahmen der Einrichtung automatisierter Abrufverfahren (Art. 8 BayDSG) handelt oder wenn eine bestimmte Rechtsnorm oder Vorschrift diese Protokollierung vorschreibt.

Protokolldaten unterliegen zudem nach dem Datenschutzrecht einer strikten Zweckbindung und dürfen daher nur zum Nachweis der fehlerfreien und ordnungsgemäßen Datenverarbeitung oder zur Aufdeckung von missbräuchlichen Zugriffen oder Zugriffsversuchen, keinesfalls jedoch für Zwecke der Verhaltens- oder Leistungskontrolle der Mitarbeiter verwendet oder ausgewertet werden. Genau solches Fehlverhalten von Behördenleitern und Mitarbeitern wird jedoch gelegentlich in Rahmen von technisch-organisatorischen Prüfungen festgestellt. Häufig ist dieses auch Gegenstand von Eingaben Betroffener an mich.

Die Dauer der Aufbewahrung von Protokolldateien muss geregelt werden. Da es sich bei Protokolldaten um personenbezogene Daten handelt, unterliegen sie den allgemeinen Löschungsregeln der Datenschutzgesetze - soweit keine spezielle gesetzliche Aufbewahrungsvorschrift vorhanden ist. Maßgeblich ist hier der Grundsatz der Erforderlichkeit zur Aufgabenerfüllung. Gibt es keinen zwingenden Grund für das weitere Vorhalten von Protokolldateien, besteht eine Löschungspflicht (z.B. gemäß Art. 12 Abs. 1 Nr. 2 BayDSG) und diese Daten sind zu löschen.

Eine generell gültige und exakte Bestimmung des zulässigen Aufbewahrungszeitraums für Protokolldaten, deren Auswertung zeitlich nicht konkretisiert ist, ist nicht möglich. Als Anhaltspunkte können aber dienen:

- die Wahrscheinlichkeit, dass Unregelmäßigkeiten (noch) aufgedeckt werden können und
- die Möglichkeit und Notwendigkeit, die Gründe von Unregelmäßigkeiten anhand der Protokolle und anderer Unterlagen aufdecken zu können.

Erfahrungsgemäß sollte eine Frist von höchstens einem halben Jahr nicht überschritten werden.

Soweit Protokolle zum Zwecke gezielter Kontrollen angefertigt werden, z.B. Überprüfung der Eindringversuche an einer Firewall, kommen auch mitunter wesentlich kürzere Speicherungsfristen in Betracht. In der Regel reicht hier eine Aufbewahrung bis zur tatsächlichen Kontrolle. Gerade bei diesem Beispiel kommt es auf eine sehr zeitnahe Auswertung mit entsprechenden Reaktionen an.

Häufig fehlt auch eine Vereinbarung mit dem Personalrat, in der die zulässigen Protokollierungen, ihre Aufbewahrungsdauer sowie die Art ihrer Auswertung genau definiert sind. Da die Protokollierung eine technische Einrichtung zur Überwachung des Verhaltens der Beschäftigten der speichernden Stelle darstellt, hat der Personalrat gemäß Art. 75a Abs. 1 BayPVG ein Mitbestimmungsrecht. Durch eine Vereinbarung mit dem Personalrat sollte daher sichergestellt sein, dass das Instrument der Protokollierung nicht zweckentfremdet verwendet wird.

23.4.8 Elektronische Gästebücher und Internet-Foren

Elektronische Gästebücher und Internet-Foren auf der eigenen Homepage erfreuen sich insbesondere bei Kommunen immer größerer Beliebtheit, dienen sie doch dazu, Kontakte mit den Bürgern zu pflegen. So können diese beispielsweise Kommentare zu aktuellen politischen Themen oder auch nur ihr Lob bzw. Kritik bezüglich der Gestaltung der Homepage kundtun.

Allerdings werden diese Gästebücher und Foren gelegentlich auch dazu missbraucht, politisch radikalen Inhalt einzutragen, andere Personen (insbesondere Politiker) zu beleidigen und sonstige strafrechtlich relevanten Eintragungen vorzunehmen. Aus diesem Grunde sind verschiedene Kommunen mit der Frage an mich herangetreten, ob und wie sie gegen derartiges Fehlverhalten vorgehen könnten, ohne dabei den Datenschutz zu verletzen. Insbesondere das Mitloggen der IP-Adressen und die Erfassung personenbezogener Daten der Gästebuchnutzer spielten bei diesen Überlegungen eine große Rolle.

Elektronische Gästebücher und Internet-Foren stellen Teledienste im Sinne des § 2 Abs. 1 Teledienstegesetz (TDG) dar, da sie elektronische Informations- und Kommunikationsdienste sind, die für eine individuelle Nutzung von kombinierbaren Daten, wie Zeichen, Bilder oder Töne bestimmt sind und ihnen eine Übermittlung mittels Telekommunikation zugrunde liegt.

Die Betreiber einer entsprechenden Homepage sind sowohl im Sinne des Teledienstegesetzes als auch des Teledienstedatenschutzgesetzes (TDDSG) sog. Diensteanbieter, da sie als juristische Personen einen eigenen Teledienst zur Nutzung bereithalten bzw. den Zugang zu dessen Nutzung vermitteln (§ 3 Nr. 1 TDG, § 2 Nr. 1 TDDSG).

Gemäß § 3 Abs. 1 TDDSG dürfen personenbezogene Daten vom Diensteanbieter zur Durchführung von Telediensten nur erhoben, verarbeitet und genutzt werden, soweit dieses Gesetz oder eine andere Rechtsvorschrift es erlaubt oder der Nutzer eingewilligt hat. Weiter bestimmt § 4 Abs. 6 TDDSG, dass der Diensteanbieter dem Nutzer die Inanspruchnahme von Telediensten und ihre Bezahlung anonym oder unter Pseudonym zu ermöglichen hat, soweit dies technisch möglich und zumutbar ist.

Unter Pseudonymisieren ist dabei das Verändern personenbezogener Daten durch eine Zuordnungsvorschrift dergestalt zu verstehen, dass die Einzelangaben über persönliche oder sachliche Verhältnisse ohne Kenntnis oder Nutzung der Zuordnungsvorschrift nicht mehr einer natürlichen Person zugeordnet werden können. Ein Pseudonym kann beispielsweise ein erfundener Name oder eine Kurzbezeichnung sein, die aus sich heraus die Identität des Nutzers nicht preisgeben, aber z.B. über eine Referenzliste beim Diensteanbieter mit der tatsächlichen Identität des Nutzers zusammengeführt werden können.

So setzt auch § 4 Abs. 7 Satz 1 TDDSG voraus, dass der Diensteanbieter Daten zu dem Pseudonym des Nutzers speichert. Dies bedeutet, dass ein Diensteanbieter entweder selbst die Pseudonyme vergibt oder ihm zumindest bekannt sein muss, wer sich dahinter verbirgt. In beiden Fällen sind ihm somit die Identitäten des Besuchers seiner Internetseiten bekannt.

Ein Pseudonym schützt einen Nutzer von Gästebüchern oder Foren somit nicht vor der Kenntnis durch den Diensteanbieter, wohl aber muss dieser durch entsprechende technische und organisatorische Vorkehrungen sicherstellen, dass die wahre Identität des Nutzers anderen Nutzern gegenüber nicht bekannt wird.

Diensteanbieter sind gemäß § 8 Abs. 2 Satz 1 TDG nicht verpflichtet, die von ihnen übermittelten oder gespeicherten Informationen zu überwachen oder nach Umständen zu forschen, die auf eine rechtswidrige Tätigkeit hinweisen. Hat ein Betreiber einer Homepage allerdings Kenntnis von entsprechenden Einträgen und entfernt sie nicht, so haftet er für diese Inhalte (vgl. § 11 TDG).

Kommunale Internet-Foren und Gästebücher können als eine öffentliche Einrichtung der Gemeinde i.S.d. Art. 21 Gemeindeordnung (GO) angesehen werden. Die Gemeinden dürfen keine rechtswidrigen (oder gar strafbaren) Benutzungen ihrer öffentlichen gemeindlichen Einrichtungen dulden. Sie sind als Körperschaften des öffentlichen Rechts in besonderer Weise Gesetz und Recht verpflichtet und somit dazu aufgerufen, derartige rechtswidrige oder strafbare Benutzung zu unterbinden. Sie können faktisch auch nicht dazu gezwungen werden, strafrechtlich relevante oder sogar verfassungsfeindliche Inhalte in ihren Foren und Gästebüchern zu dulden.

Für ein datenschutzgerechtes Betreiben von Gästebüchern und Internet-Foren empfehle ich daher folgende Vorgehensweise:

- Eintragungen im Gästebuch bzw. Forum werden nicht anonym, sondern nur unter einem selbst gewählten Pseudonym - nach vorheriger Anmeldung mit personenbezogenen Daten - zugelassen.

- Die wahren Identitäten der Nutzer werden nicht veröffentlicht, können aber vom Betreiber der Homepage ermittelt und bei strafbaren Handlungen den Ermittlungsbehörden übergeben werden.

- Darauf sollte in den Nutzungsbedingungen des Gästebuches bzw. des Forums hingewiesen werden. Soweit technisch möglich, sollte einem Nutzer zusätzlich bei der Vornahme seines Eintrages ein entsprechender Hinweis eingeblendet werden.

- Bei einer relativ geringen Anzahl von Einträgen pro Tag empfiehlt es sich, eine Moderation des Gästebuches bzw. des Forums mit Vorbehalt einer Freischaltung der einzelnen Einträge erst nach Sichtung durch den Betreiber der Homepage vorzunehmen. Darauf sind die Eintragswilligen vorab bereits bei ihrer Registrierung hinzuweisen.

- Ist eine Vorabkontrolle aufgrund des hohen Aufkommens von Einträgen nicht möglich, so sollte zumindest einmal täglich der Inhalt des Gästebuches bzw. der Foren auf strafrechtlich relevante Inhalte durchgesehen werden. Derartige Inhalte sind natürlich unverzüglich zu entfernen.

Eine vorsorgliche Protokollierung von IP-Adressen ist nur wegen sicherheitsrelevanter Ereignisse (im Sinne von Gefährdung der technisch-organisatorischen Sicherheit - also z.B. zur Abwehr oder Nachverfolgung von Angriffen über das Internet) zulässig.

Nicht zulässig ist aber eine vorsorgliche Protokollierung von IP-Adressen zum Zwecke einer evtl. späteren Strafverfolgung, weil möglicherweise zukünftig ein Besucher des Gästebuches oder des Forums dort strafrechtlich relevante Eintragungen vornehmen könnte.

Über die Protokollierung der IP-Adressen aus Gründen der Datensicherheit sind die Besucher der Homepage im Rahmen der Online-Datenschutzerklärung zu unterrichten (siehe Nr. 22.2.2.2 meines 21. Tätigkeitsberichts und die Orientierungshilfe „Online-Datenschutz-Prinzipien (ODSP)“ - abrufbar auf meiner Homepage im Bereich Technik/Grundsätze/ Allgemein).

23.5 Beratungsleistungen

23.5.1 Allgemeine Anmerkungen

Wie im vorletzten hat auch in diesem Berichtszeitraum der Umfang an nachgefragter Beratungsleistung stark zugenommen und beanspruchte im technisch-organisatorischen Bereich wieder einen ganz wesentlichen Teil meiner personellen Kapazitäten. Neben lokalen und landesweiten Projekten wurde erhebliche Beratungsleistung auch in bundesweiten Projekten, die teilweise bereits seit mehreren Jahren meine Dienststelle und auch meine Kollegen in Bund und Ländern intensiv beschäftigen, erbracht.

Dabei hat es sich - wie bereits in meinen früheren Tätigkeitsberichten ausgeführt - erneut gezeigt, dass die sich im Zusammenhang mit den Projekten ergebenden Datenschutzfragen und -aspekte längst nicht mehr nach Recht und Technik getrennt betrachtet werden können. Die erreichten umfassenden Beratungsergebnisse konnten nur erzielt werden durch die von meinen Mitarbeitern praktizierte enge Zusammenarbeit zwischen Technikern und Juristen.

Auf einige dieser sehr arbeitsintensiven Projekte bin ich in den Kapiteln Einführung einer elektronischen Gesundheitskarte (vgl. Nr. 14.1.1), Mammographie-Screening (vgl. Nr. 13.1.3), Elektronisches Fortbildungskonto für Ärzte (vgl. Nr. 13.4.1) und Datenschutzrechtliche Begleitung des Aufbaus einer Biomaterialbank - Biobank der Blutspender (vgl. Nr. 13.3.1) bereits eingegangen.

Weitere Projekte mit ebenfalls technisch-organisatorischem Beratungsbedarf sind wegen des derzeitigen Schwerpunktes im rechtlichen Bereich in den entsprechenden rechtlichen Abschnitten dargestellt, z.B. in den Kapiteln Polizei, Justiz, Gemeinden, Städte und Landkreise, Steuer- und Finanzverwaltung, Personalwesen, Statistik, Medien und Telekommunikation.

Auf einige, wegen ihrer gravierenden technisch-organisatorischen Bedeutung ausgewählte Projekte gehe ich in den folgenden Abschnitten näher ein.

23.5.2 JobCard-Verfahren / ELENA

Wie schon unter Nr. 22.2.3.3 meines 21. Tätigkeitsberichts 2004 dargestellt, habe ich auch in diesem Berichtszeitraum die Weiterentwicklung des JobCard-Verfahrens, mittlerweile umbenannt in ELENA-Verfahren (Elektronischer Einkommensnachweis), begleitet.

Projektstand

Am 31.12.2005 wurde das Projekt JobCard-Verfahren Stufe 2 mit einem Abschlussbericht beendet. In diesem Projekt wurde die Machbarkeit von Erweiterungen des JobCard-Verfahrens Stufe 1 untersucht, so z.B. die Einbindung von 17 weiteren Bescheinigungen neben der ursprünglichen Arbeitgeberbescheinigung für das Arbeitslosengeld, wie z.B. Mutterschaftsgeld, Krankengeld, Kindergeld, Wohngeld, Rentenbescheinigung, Verdienstbescheinigung für Gerichte (Prozesskostenhilfe), Arbeitgeberbescheinigung zum Erziehungsgeldantrag, Bescheinigungen im Rahmen des Unterhaltssicherungsgesetzes. Damit sollen ca. 90% des Bescheinigungswesens abgedeckt werden.

Das Grundprinzip des Verfahrens hat sich dennoch nicht fundamental geändert. Nach wie vor übermitteln die Arbeitgeber monatlich einen multifunktionalen Datensatz an die Zentrale Speicherstelle (ZSS). Dort werden sie entsprechend der Aufbewahrungsfristen der einzelnen Verfahren verschlüsselt aufbewahrt. Die Verschlüsselung geschieht mittels eines Masterkey-Verfahrens, also nicht mit dem Schlüssel des Betroffenen. Der Abruf erfolgt durch die Leistungsgewährende Stelle, nachdem sowohl der Betroffene als auch der Sachbearbeiter eine entsprechende Vollmacht elektronisch signiert haben. Da die Teilnahme am Verfahren für alle Arbeitnehmer in Deutschland verpflichtend ist, müssen diese im Besitz einer Signaturkarte sein.

Die Bedingungen des Jobcard-Verfahrens sollen per Gesetz geregelt werden. Ein Gesetzesentwurf hierzu soll noch im Herbst 2006 in das parlamentarische Verfahren eingebracht werden. 2008 sollen nach jetzigem Planungsstand die Arbeitgebermeldungen beginnen, 2009 dann der Bescheinigungsabruf.

Mittlerweile wurde die Projektstufe 3 gestartet, in der zum einen die Details zur Einbindung der Entgeltersatzleistungen erarbeitet werden sollen. Entgeltersatzleistungen sind Leistungen öffentlicher Einrichtungen, die in die Berechnung oben genannter Bescheinigungen miteinbezogen werden müssen, wie z.B. der Bezug von Arbeitslosengeld. Aus Sicht der Effizienzsteigerung ist es sinnvoll, wenn auch diese Daten von den entsprechenden Stellen elektronisch geliefert werden.

Zum anderen soll in dieser Phase die reale Einführung des Verfahrens vorbereitet werden. In diesem Zusammenhang wird beispielsweise an einem so genannten Migrationskonzept gearbeitet, das festlegt, wie die Zeitspanne gehandhabt werden soll, in der noch nicht alle Betroffenen eine Signaturkarte besitzen.

Diskussionspunkte

Aus Datenschutzsicht ist nach wie vor die Frage der verfassungsrechtlichen Zulässigkeit des Verfahrens nicht vollständig geklärt. Ein Großteil der Bevölkerung wird an dem Verfahren teilnehmen müssen. Ein Teil davon wird vermutlich zumindest für bestimmte Zeitabschnitte überhaupt keine Sozialleistungen beantragen. Bisher wurden von den zuständigen Stellen noch keine belastbaren Zahlen oder Argumente vorgelegt, die untermauern könnten, dass die Grundsätze der Erforderlichkeit und Verhältnismäßigkeit eingehalten werden. Somit kann derzeit nicht abschließend geklärt werden, ob es sich um eine unverhältnismäßige, verfassungswidrige Datenspeicherung handelt. Die Gesetzesbegründung soll hierzu Aussagen enthalten.

Zudem besteht bei großen Datenbeständen immer die Gefahr, dass Begehrlichkeiten geweckt werden und auch das Risiko des Missbrauchs ist nicht zu unterschätzen.

Neben diesen grundsätzlichen, noch offenen Fragen wurden auch technische Einzelheiten des Verfahrens diskutiert. Zum einen war dies die Frage der Ende-zu-Ende-Verschlüsselung der Datensätze mit dem Schlüssel des Betroffenen, um der Möglichkeit der Entschlüsselung durch die ZSS zu begegnen. Hierzu wurde ein Gutachten durch das Bundesamt für Sicherheit in der Informationstechnik (BSI) erstellt, das zu dem Ergebnis kam, dass die Ende-zu-Ende-Verschlüsselung zwar möglich wäre, jedoch Probleme bezüglich der praktischen Handhabbarkeit aufwerfe, da sich der technische und organisatorische Aufwand für viele Vorgänge erhöhen würde. Insbesondere problematisiert wurde das Thema Verlust bzw. Defekt der Signaturkarte des Betroffenen, die eine Entschlüsselung der in der ZSS gespeicherten Daten unmöglich machen würden. Die entsprechenden Daten müssten somit beim Arbeitgeber wiederbeschafft werden, was dort komplexe Methoden zur Bereithaltung erfordern würde.

Als Kompromiss wurde eine Lösung festgelegt, bei der der Masterkey des Verfahrens aus der Hoheit der ZSS ausgelagert und in die Hände eines unabhängigen Dritten gelegt wird. Dieser kontrolliert, ob die Zugriffe auf den Masterkey und damit die Datenabrufe zulässig sind.

Ein weiteres Thema sind die Entgeltersatzleistungen, welche weitere Daten Datenlieferanten und abrufende Stellen in das Verfahren einbringen. Hieran zeigt sich zum einen die Tendenz des JobCard-Verfahrens, einen umfassenden, zentralen Datenpool zu Sozialdaten fast der gesamten Bevölkerung aufzubauen, der unter Umständen Begehrlichkeiten aus anderen Bereichen weckt. Dieser Effekt konnte bereits beobachtet werden: So wurde z.B. im Rahmen der Diskussion

um die Schwarzarbeitsbekämpfung die Anforderung gestellt, den Ermittlungsbehörden Zugriff auf die Datenbestände ohne Wissen des Betroffenen zu gewähren. Dies wurde zwar von allen Beteiligten abgelehnt, es stellt sich jedoch die Frage, welche Wünsche zukünftig noch an das Verfahren herangetragen werden. Da auf die Ende-zu-Ende-Verschlüsselung verzichtet wurde, ist ein derartiger Zugriff technisch betrachtet realisierbar. Es könnten somit allein durch eine Gesetzesänderung neue Nutzungsmöglichkeiten für vorhandene Daten erschlossen werden.

Zum anderen stellt sich die Frage der datenschutzgerechten technischen Umsetzung der Entgeltersatzleistungen. Hierbei ist insbesondere darauf zu achten, dass die Daten nicht in der ZSS und somit unter der gleichen Obhut wie die Arbeitgeberdaten und mit dem gleichen Schlüssel verschlüsselt gespeichert werden. Dies würde z.B. auch bei Angriffen auf die ZSS-Systeme die Menge der potentiell unbefugt offenbarten Daten deutlich erhöhen. Angedacht ist derzeit, eine eigene ZSS für die Entgeltersatzleistungsdaten einzuführen.

Gerade wegen der Vielzahl der im Verfahren gesammelten Daten ist die Transparenz ein wichtiger Aspekt. Hierzu wurden von Seiten des Datenschutzes Maßnahmen gefordert, damit der Betroffene jederzeit nachvollziehen kann, welche Daten über ihn gespeichert sind und welche Datenübertragungen an welche Stellen stattgefunden haben. Es wären z.B. Online-Terminals denkbar.

Derzeit diskutiert wird die Frage, wie der Datenabruf während der Übergangsphase bei der Einführung des JobCard-Verfahrens erfolgen soll, in der noch nicht alle Arbeitnehmer eine Signaturkarte besitzen. Ein der Arbeitsgruppe JobCard zur Kommentierung vorgelegtes Migrationskonzept sieht vor, in dieser Phase den Datenabruf ohne die Signaturkarte des Antragstellers über eine Art PIN/TAN-Verfahren zu ermöglichen. Dies wird sehr kritisch gesehen, da damit die Sicherheitshürden deutlich reduziert würden und zudem vom Zwei-Karten-Prinzip abgewichen werden soll, das bisher die Grundlage der Akzeptierbarkeit des Verfahrens aus Datenschutzsicht war. Aus diesen Gründen wurde daher das Migrationskonzept von der Projektleitung wieder verworfen und zum Zwei-Karten-Prinzip auch für die Migrationsphase zurückgekehrt.

Fazit

Das JobCard-Verfahren wurde zeitweise sehr intensiv von Seiten des Datenschutzes begleitet, dennoch konnten bisher die Befürchtungen nicht endgültig ausgeräumt werden. Einerseits konnten juristische Fragen zur Vorratsdatenspeicherung bisher nicht geklärt werden, andererseits ist das Verfahren nach wie vor im Fluss und erfährt ständig neue Ergänzungen. Das zeitweise vorgeschlagene Migrationskonzept mit seiner Abweichung vom Zwei-Karten-Prinzip ließ die Besorgnis aufkommen, dass hiermit das Sicherheitsniveau für Datenzugriffe reduziert wird und dass diese als Provisorium gedachte Maßnahme zur Dauereinrichtung werden könnte, weswegen von dieser Lösung nach kritischer Beurteilung durch die Datenschutzbeauftragten wieder Abstand genommen wurde. Es erscheint daher angezeigt, die Entwicklung des JobCard-Verfahrens und insbesondere auch die zu erstellenden gesetzlichen Regelungen genau zu beobachten.

23.5.3 Umgang mit Biomaterialien in Universitätsklinika

Der Umgang mit menschlichen Biomaterialien (z.B. Blut, Gewebe, Liquor, Urin) gewinnt mit der zunehmenden Verbreitung genetischer Analysen eine besondere Brisanz. Insbesondere an den Universitätsklinika wird eine breite Forschung an Biomaterialien betrieben. Zur Gewinnung eines Überblicks über die üblichen Praktiken habe ich an alle bayerischen Universitätsklinika einen detaillierten Fragebogen versandt. Zusätzlich wurden von meinen Mitarbeitern im Prüfungszeitraum zwei Klinika besucht, um die jeweils üblichen Verfahrensweisen unmittelbar vor Ort kennen zu lernen.

Dabei hat sich ergeben, dass im Großen und Ganzen die Anforderungen des Datenschutzes eingehalten werden. Es bestehen jedoch teilweise große Unterschiede zwischen einzelnen Abteilungen und Projekten innerhalb eines Klinikums, da jeweils eigene Konzepte und Lösungen Anwendung finden. Deshalb erscheint es sinnvoll, an dieser Stelle die Mindestanforderungen aus Sicht des Datenschutzes an die Verarbeitung von Biomaterialen in Krankenhäusern festzulegen. Zu unterscheiden ist hierbei zwischen den Bereichen Patientenversorgung und Forschung.

Patientenversorgung

Im Rahmen der medizinischen Versorgung werden für die Diagnose und Therapie beim Patienten Biomaterialien genutzt. Diese Nutzung ist im Allgemeinen vom Behandlungsvertrag gedeckt. Die Proben werden üblicherweise auf der behandelnden Station entnommen, dort mit dem Patientennamen, Geburtsdatum, Geschlecht und evtl. internen Verwaltungsnummern beschriftet und so an interne wie auch an externe Labore weitergegeben. Die Ergebnisse der Untersuchung werden im Labor zusammen mit den identifizierenden Daten des Patienten zumeist einerseits in den speziellen Laborsystemen elektronisch abgespeichert und von dort an das Krankenhausinformationssystem (KIS) und die anfordernde Abteilung weitergegeben, zum anderen auf Papier zur Patientenakte genommen. Die Proben werden nach

der Auswertung vernichtet. Nur für sehr schwer zu erlangendes Material wird dieses bei Bedarf mit Einwilligung des Betroffenen für die Forschung weitergenutzt.

Die Beschriftung der Proben und Daten mit den identifizierenden Daten des Patienten ist im direkten Behandlungszusammenhang akzeptabel. Auch wenn theoretisch betrachtet eine pseudonymisierte Nutzung möglich erscheint, steigt in der Praxis die Verwechslungsgefahr dadurch deutlich, die u.U. zu lebensbedrohlichen Situationen für den Patienten führen kann.

Für die Nutzung von Biomaterialien im Behandlungszusammenhang sind folgende Anforderungen zu beachten, die sowohl den Schutz der Patientendaten als auch der Proben sicherstellen sollen:

- Für das Laborsystem und seine Anbindung an sonstige im Klinikum vorhandenen Systeme (z.B. KIS) gelten die üblichen Anforderungen des Datenschutzes wie z.B. personenbezogene Benutzerkennungen und differenzierte Zugriffsrechte, Integrität der Daten, Nachverfolgbarkeit von Datenzugriffen und -änderungen, gesicherte Datenübermittlung. Details hierzu finden sich u.a. in der Orientierungshilfe zu Krankenhausinformationssystemen, die von meiner Homepage abrufbar ist.

- Bezüglich der Proben ist zum einen eine durchgängige Sicherung gegen Verlust oder Diebstahl erforderlich: Proben sollten nach ihrer Erhebung eindeutig, z.B. per Nummer, identifizierbar sein und in der Bestandsverwaltung, z.B. Laborsystem, erfasst werden. Hierüber sollte auch nachvollziehbar sein, wo sich die Probe gerade befindet.

  Für den Transport der Proben muss sichergestellt werden, dass dieser über diebstahlgeschützte Wege erfolgt und eine unbefugte Kenntnisnahme der personenbezogenen Beschriftungen nicht möglich ist. Insbesondere bei einem Transport nach außen durch externe Dienstleister muss gewährleistet werden, dass diese keine Kenntnis von der Beschriftung der Proben nehmen können.

- Die Verwahrung von Proben auf Station und in den Labors muss in abgeschlossenen Räumen oder Schränken erfolgen und auch für zu vernichtende Proben muss sichergestellt werden, dass hierbei kein Entwenden des Materials möglich ist. Es darf grundsätzlich nur das Personal Zugang haben, das mit der Behandlung des Patienten bzw. der Analyse der Proben betraut ist.

Forschung

In der Forschung wird in vielen Fällen bereits heute mit anonymisierten oder pseudonymisierten Daten und Proben gearbeitet. An dieser Stelle sollen nur Fälle betrachtet werden, bei denen Universitätsklinika definierte und zeitlich begrenzte Forschungsprojekte betreiben. Biomaterialbanken, bei denen Daten und Proben längerfristig und eventuell auch zu derzeit noch unbestimmten Zwecken gesammelt werden, werden in Nr. 13.3.1 genauer dargelegt.

Die für die Forschung relevanten Daten werden in der Regel getrennt von identifizierenden Daten elektronisch gespeichert und aufbewahrt. Zunehmend handelt es sich bei den Forschungsprojekten um sog. Multicenter-Studien, bei denen Daten und Proben mehrerer Stellen gesammelt und auch von allen oder von einigen dann genutzt werden. Die verwendeten Verfahren zur Anonymisierung / Pseudonymisierung und auch die Sicherheitsmaßnahmen zum Schutz vor einer unbefugten Depseudonymisierung fallen jedoch sehr unterschiedlich aus. Daher sollen im Folgenden gewisse Mindeststandards an die Nutzung von Biomaterialien für die Forschung dargelegt werden.

- Die Forschung mit Patientendaten und Proben ist nur unter der Voraussetzung der Einwilligung des Patienten möglich. Hierzu sind eine Patienteninformation, welche die Einzelheiten der Studie in verständlicher Form darstellt, und eine Einwilligungserklärung nötig.

- Forscher dürfen in jedem Fall nur auf pseudonymisierte oder anonymisierte medizinische Patientendaten zugreifen, da ein Personenbezug für Forschungsfragen in aller Regel nicht erforderlich ist. Dies bedeutet, dass sowohl Daten als auch Proben, die zu Forschungszwecken genutzt werden, nur mit einem Code (Pseudonym) versehen sein dürfen, d.h. Namensangaben etc. dürfen nicht enthalten sein. Detaillierte Hinweise zum Thema Pseudonymisierung sind von meiner Homepage mit der entsprechenden Orientierungshilfe abrufbar.

- Die Pseudonymisierung / Anonymisierung muss zu einem möglichst frühen Zeitpunkt nach der Erhebung von Daten und Proben vorgenommen werden, also insbesondere vor der Herausgabe von Daten / Proben an Partner. Das Pseudonym sollte hierbei nicht sprechend sein, so dass daraus keine Rückschlüsse auf den Patienten möglich sind, also beispielsweise nicht aus Initialen und Geburtsdatum bestehen.

- In gewissen Fällen kann eine Reidentifizierung des Patienten nötig sein. Zu diesem

Zweck kann die Zuordnung Pseudonym - identifizierende Daten aufbewahrt werden. Wichtig ist hierbei jedoch die gesicherte Verwahrung, getrennt von den Forschungsdaten und Proben, z.B. unter gesonderter organisatorischer Obhut. Auch sollten Maßnahmen ergriffen werden, um den Beschlagnahmeschutz zu gewährleisten.

- Wie im Falle der Nutzung für die Patientenversorgung müssen eventuell verwendete IT-Systeme den üblichen Anforderungen des Datenschutzes genügen und sicherstellen, dass nur Befugte Zugriff auf die Daten erhalten. Ebenso müssen die Proben gesichert gelagert werden.

- Forschungsergebnisse dürfen nur in anonymisierter oder aggregierter Form veröffentlicht werden.

- Je nach Größe und Bedeutung der Proben kann auch eine organisatorische Trennung der verschiedenen Funktionen erforderlich sein, so dass für eine unbefugte Depseudonymisierung mehrere Stellen kompromittiert werden müssten. Es kann z.B. sinnvoll sein, Proben, identifizierende Daten und medizinische Daten jeweils an einer anderen Stelle und unter getrennter Obhut aufzubewahren. Diese Fragen sind insbesondere für große Biomaterialbanken von Interesse, wie sie in Nr. 13.3.1 behandelt werden.

- Für jedes Forschungsprojekt ist auch die Frage zu klären, wie die datenschutzrechtliche Freigabe gemäß Art. 26 BayDSG erfolgt. Insbesondere bei Multicenter-Studien ist festzulegen, wer verantwortlich im Sinne des Datenschutzes ist.

23.5.4 Zusammenlegung von Kfz-Zulassungsbehörden

Im Berichtszeitraum sind verschiedene Städte und Landratsämter mit der Bitte an mich herangetreten, zu prüfen, in wieweit es möglich wäre ihre Kfz-Zulassungsbehörden zusammenzulegen. Dazu ist aufgrund der derzeitigen Rechtslage Folgendes zu sagen:

Für eine Zusammenlegung von Kfz-Zulassungsbehörden eines Landratsamtes und einer kreisfreien Stadt und die dabei vorgesehene wechselseitige Bearbeitung von Anträgen nach der Straßenverkehrs-Zulassungs-Ordnung (StVZO) ist § 68 Absatz 2 Satz 2 StVZO maßgeblich. Danach dürfen Anträge (z.B. auf Zulassung und Stilllegung) mit Zustimmung der örtlich zuständigen Behörde von einer gleichgeordneten auswärtigen Behörde behandelt und erledigt werden. Voraussetzung ist eine entsprechende Vereinbarung der beteiligten Kfz-Zulassungsbehörden. Die Anwendbarkeit der Vorschrift ist außerdem auf Vorgänge beschränkt, für die ein Antrag erforderlich ist. Unzulässig wäre es auch, eine gemeinsame Behörde zu schaffen, d.h. die Behörden müssen eigenständig bleiben und auch das Personal muss in der Hoheit der jeweiligen Behörde verbleiben.

Nicht vom § 68 Abs. 2 StVZO erfasst ist die Übertragung von Aufgaben einer Kfz-Zulassungsbehörde an kreisangehörige Gemeinden. Soll dies geschehen, muss ein entsprechender Antrag gemäß § 15 der Verordnung über Zuständigkeiten im Verkehrswesen (ZustVVerk) an das Staatsministerium für Wirtschaft, Infrastruktur, Verkehr und Technologie (StMWIVT) gerichtet werden, das dafür seine Zustimmung erteilen muss.

Die Eigenständigkeit der Kfz-Zulassungsbehörden einer kreisfreien Stadt und eines Landratsamtes muss auch durch die Ergreifung entsprechender technisch-organisatorischer Datensicherheitsmaßnahmen gewährleistet werden. So ist es zwar möglich, dass sich beide Stellen einer gemeinsamen physikalischen Datenbank bedienen, allerdings muss dabei zwingend eine logische Trennung der beiden Datenbestände erfolgen. Die Verantwortlichkeiten für die Datensicherung und die Gewährleistung der Verfügbarkeit der erforderlichen Daten und Datenbankserver müssen bei einer gemeinsamen Datenbank vertraglich geregelt werden.

Außerdem müssen die beiden Datenbestände gegen unberechtigte Zugriffsversuche - auch von der jeweils anderen Stelle - abgesichert werden; z.B. durch strikte Rechtevergabe, Authentisierung und Identifizierung mittels Benutzerkennung und Passwort, Protokollierung der Zugriffsversuche und Auswertung der Protokolldateien hinsichtlich Schutzverletzungen. Sollten im Rahmen der Datenverarbeitung öffentliche Leitungen genutzt werden, sind die Installation einer Firewall zur jeweiligen Netzwerkabsicherung, eventuell die Einrichtung eines VPN und eine verschlüsselte Datenübertragung erforderlich. Auch zur Abschottung der Netzteilnehmer untereinander ist der Einsatz einer Firewall empfehlenswert.

§ 6 des vom Bayerischen Ministerrat im September 2006 beschlossenen Gesetzes zur Erweiterung und Erprobung von Handlungsspielräumen der Kommunen sieht vor, dass kreisfreie Gemeinden und der Freistaat Bayern, vertreten durch das jeweilige staatliche Landratsamt, sich zu einem Zweckverband gemäß dem Gesetz über die kommunale Zusammenarbeit zusammenschließen und ihm die Aufgaben der unteren Verwaltungsbehörden für die Fahrzeugzulassung übertragen können. Diese Regelung soll dem

Art. 8 des Gesetzes über die Zuständigkeit im Verkehrswesen als Abs. 3 angefügt werden.

23.5.5 Datenschutzanforderungen an ein Dokumentenmanagementsystem

Insbesondere größere Kommunen und Behörden planen seit einiger Zeit, ein Dokumentenmanagementsystem (DMS) zur Verwaltung ihrer elektronischen Dokumente einzusetzen. So entwickelt beispielsweise ein Softwareunternehmen für den Freistaat Bayern das einheitliche Dokumentenmanagement- und Vorgangsbearbeitungssystem ELDORA (Elektronische Dokumentenverarbeitung mit Recherche und Aktenverwaltung), das im Laufe des Jahres 2007 möglichst flächendeckend im staatlichen Bereich eingeführt werden soll.

Im Rahmen einer Landeslizenz soll ELDORA auch kommunalen Stellen und sonstigen rechtlich selbstständigen Körperschaften, Anstalten und Stiftungen, die unter der Aufsicht des Freistaates Bayern stehen, möglich sein, dieses DMS kostengünstig zu erwerben.

In die Spezifikation und Feinkonzeption des Systems wurde ich eingebunden. Die Gespräche über einzelne grundlegende datenschutzrechtliche Anforderungen an dieses Projekt waren zum Redaktionsschluss noch nicht abgeschlossen.

Ein Dokumentenmanagementsystem dient der zentralen und medienbruchfreien Verwaltung elektronischer Dokumente sowie ihrer Wiederauffindbarkeit und spart damit Zeit und Kosten. Andererseits entsteht durch die elektronische Abbildung der Tätigkeiten der Mitarbeiter eine große Menge von zusätzlichen Informationen, die gezielt zur Ausforschung und zur permanenten Verhaltens- und Leistungskontrolle von einzelnen oder allen Mitarbeitern genutzt werden können.

Daher sollte in einer Dienstvereinbarung mit dem Personalrat genau festgelegt werden, für welche Zwecke das DMS eingeführt werden soll, welche Protokolldaten im DMS erzeugt werden, wer zu welchen Zwecken darauf zugreifen und diese auswerten darf. Eine Nutzung dieser Daten für Verhaltens- und Leistungskontrollen ist dabei natürlich auszuschließen.

Aber auch Akteneinsichtsrechte (z.B. Art. 29 BayVwVfG) und Rechte der Betroffenen auf Berichtigung, Sperrung und Auskunft bezüglich der über sie gespeicherten Daten müssen in einem DMS sichergestellt und praktisch umgesetzt werden.

So ist bei der Einführung eines DMS darauf zu achten, dass insbesondere folgende datenschutzrechtliche Anforderungen umgesetzt werden:

- Dokumente dürfen nicht unzulässig im DMS gespeichert werden oder bleiben.
- Unzulässige Zugriffe auf die Dokumente sind zu verhindern.
- Dokumente dürfen nicht manipuliert oder gelöscht werden können.
- Der Zugriff auf Protokolldaten der Beschäftigten zu Zwecken der Leistungs- und Verhaltenskontrolle ist zu untersagen.

Gemäß Art. 26 Abs. 1 Satz 1 BayDSG bedarf der erstmalige Einsatz von automatisierten Verfahren, mit denen personenbezogene Daten verarbeitet werden, der vorherigen schriftlichen datenschutzrechtlichen Freigabe durch die das Verfahren einsetzende öffentliche Stelle. Eine solche Freigabe muss natürlich auch für ein DMS vorliegen.

Selbstverständlich müssen auch in einem DMS Maßnahmen zur Gewährleistung der Vertraulichkeit, der Authentizität, der Integrität, der Revisionsfähigkeit und der Verfügbarkeit ergriffen werden.

So muss z.B. die Möglichkeit bestehen, sensible personenbezogene Daten zur Wahrung der Vertraulichkeit verschlüsselt abspeichern zu können. Die Übertragung personenbezogener Daten hat immer verschlüsselt zu erfolgen.

Für die Gewährleistung der Authentizität und der Integrität ist der Einsatz der elektronischen Signatur anzuraten.

Bezüglich der Revisionsfähigkeit ist darauf zu achten, dass jederzeit nachträglich überprüfbar und feststellbar ist (z.B. durch eine entsprechende Protokollierung), ob und von wem personenbezogene Daten eingegeben, verändert oder entfernt worden sind. Vermerke und Änderungen an Dokumenten sind so zu dokumentieren, dass die Wiederherstellung des ursprünglichen Zustandes jederzeit möglich ist. Dabei ist zu beachten, dass auch Zugriffe der Administratoren gespeichert und ausgewertet werden müssen, da diese im Regelfall Zugriff auf alle Dokumente haben, wodurch sie eventuell unbefugt Informationen zur Kenntnis nehmen oder Dokumente manipulieren bzw. löschen könnten. Festzulegen ist auch, auf welche Weise die Protokolldateien ausgewertet werden und wer diese Auswertung vornimmt. Diese Auswertung sollte nicht oder zumindest nicht ausschließlich durch die Systemadministration erfolgen. Hier gilt es, das Vier-Augen-Prinzip anzuwenden, also z.B. Aus-

wertung nur gemeinsam durch Systemverwalter und behördlichem Datenschutzbeauftragten.

Der Verlust der Verfügbarkeit der Daten ist dadurch zu verhindern, dass die Dokumentenverwaltung technisch so gestaltet wird, dass alle Unterlagen während der Dauer der Aufbewahrungsfrist verfügbar sind. Diese müssen innerhalb einer angemessenen Zeit so lesbar gemacht werden können, dass sie dem Original entsprechen.

Ein Dokumentenmanagementsystem wird häufig als ein Informations- und Wissenstool für alle Beschäftigten angesehen. Dabei wird nicht selten übersehen, dass auch bei einem DMS ein Berechtigungskonzept zu erstellen ist, das detailliert regelt,

- welche Personen im Rahmen ihrer jeweiligen Aufgabe
- welche Funktionen (z.B. Suchmasken nur über Metadaten oder über alle Daten, Recherchemöglichkeiten) und
- welche Daten auf
- welche Art und Weise (Lese- bzw. Schreibzugriff)

nutzen dürfen.

Dabei dürfen immer nur so viele Zugriffsrechte vergeben werden, wie es für die Aufgabenwahrnehmung notwendig ist. So ist sicherzustellen, dass ein Nutzer nur die Dokumente sehen kann, die seiner jeweiligen Verfügungsberechtigung unterliegen. Eintragungen bzw. Änderungen an den Unterlagen und Bearbeitungsvermerken dürfen nur im Rahmen dieser Zuständigkeiten möglich sein und ein unbefugtes Lesen, Kopieren oder Löschen von Daten ist zu verhindern.

Insbesondere ist zu beachten, dass die Zugriffsrechte bei einer elektronischen Aktenführung denen bei der Führung einer herkömmlichen Akte in Papierform entsprechen müssen und keinesfalls darüber hinausgehen dürfen. Ob eine Akte in herkömmlicher Papierform oder in elektronischer Form geführt wird, ist lediglich eine Frage des gewählten Mediums. Hinsichtlich der Zugriffsberechtigungen können sich aus dieser Entscheidung keine unterschiedlichen Folgerungen ergeben.

Die Zugriffsbefugnisse sowohl für eine Akte in Papierform wie auch in elektronischer Form bestimmen sich nach den einschlägigen gesetzlichen und organisatorischen Aufgabenzuweisungen. Dabei ist auch der Grundsatz der informationellen Gewaltenteilung zu beachten. In diesem Zusammenhang weise ich darauf hin, dass der Behördenleiter zur Wahrnehmung der Dienstaufsicht, der Behördenleitung und der Vertretung der Behörde nach außen einen direkten Zugriff auf die Datenbestände seiner Behörde nicht benötigt (Nr. 8.13 meines 18. Tätigkeitsberichts 1998).

Bereits für das Einscannen des Papiergutes ist festzulegen, welche Personen zum Scannen welcher Dokumente berechtigt und für diesen Vorgang verantwortlich sind. Dies gilt insbesondere für das Einscannen von Dokumenten mit sensiblem Inhalt. Hierbei sind spezifische Vorkehrungen gegen unbefugte Kenntnisnahme erforderlich.

Durch das Ergreifen technischer und organisatorischer Maßnahmen sollte nicht nur ein unvollständiges Scannen sondern auch ein fehlerhaftes Zusammenführen einzelner Dokumente und eine falsche Zuordnung zu Vorgängen möglichst vermieden werden.

Die Aufbewahrungs- und Löschungsfristen der Dokumente sollten vorab und generell geregelt werden, wobei natürlich die einschlägigen gesetzlichen Bestimmungen zu beachten sind. Alle elektronischen Dokumente müssen während ihrer gesamten Archivierdauer zuordenbar und gegen Manipulationen und zufälliger Zerstörung geschützt sein. Andererseits sind Maßnahmen festzulegen, die eine Löschung unzulässig gespeicherter sowie nicht mehr benötigter und nicht archivwürdiger Dokumente sicherstellen.

Weitere Informationen zum „Datenschutz bei Dokumentenmanagementsystemen“ enthält die gleichnamige Orientierungshilfe, welche von einer Arbeitsgruppe des Arbeitskreises eGovernment der Konferenz der Datenschutzbeauftragten des Bundes und der Länder erarbeitet wurde und auf meiner Homepage im Bereich Technik/Orientierungshilfen/Sonstiges abrufbar ist.

23.6 Technisch-organisatorische Einzelprobleme

23.6.1 OK.FIS

Im Jahre 2001 traten mehrere Städte mit der Bitte an mich heran, zu prüfen, ob das Finanzinformationssystem OK.FIS der Anstalt für Kommunale Datenverarbeitung in Bayern (AKDB) datenschutzrechtlich unbedenklich sei. Hauptkritikpunkt war, dass alle Anordnungsdienststellen einer Stadt Zugriff auf alle Finanzadressen (FAD) dieser Kommune hatten. So konnten alle Mitarbeiter neben der Wohnanschrift auch alle anderen Daten - wie Bankverbindungen oder Immobilienobjekte - sowohl von Bürgern als auch von Bediensteten einsehen.

Aufgrund dieser Erkenntnisse führten Mitarbeiter meiner Geschäftsstelle ein Gespräch mit Vertretern

der AKDB bezüglich einer möglichen Neugestaltung des OK.FIS-Verfah-rens, bei der die notwendigen Datenschutz- und Datensicherheitsmaßnahmen berücksichtigt werden sollten (siehe Nr. 17.3.4 meines 20. Tätigkeitsberichts).

Diese Programmänderungen wurden von der AKDB sukzessive bis zum Sommer 2004 durchgeführt und eine entsprechende neue Programmversion an die Kunden ausgeliefert.

Im Rahmen meiner Nachfrage bei mehreren Kommunen, die das OK.FIS-Verfahren nutzen, stellte sich im Jahre 2006 jedoch heraus, dass nahezu keine öffentliche Stelle die neuen Programmkomponenten zum Schutz der Finanzadressen einsetzte. Insbesondere wurden dafür folgende Gründe angegeben:

- zu hohe Kosten, weil die Einstellung zusätzlichen Personals für die Pflege der Datenbank erforderlich sei
- Erhöhung des Arbeitsaufwandes für die Stadtkassen, da mit verschiedenen Finanzadressen gearbeitet werden müsse
- hoher administrativer Aufwand für die Pflege der Rechtevergabe
- Kompatibiltätsprobleme mit anderen AKDB-Verfahren (z.B. OK.FEN)

In einer daraufhin erfolgten Besprechung mit der AKDB erklärte diese jedoch, dass alle bereits vorhandenen Objekte und Finanzadressen ohne großen Aufwand und ohne Neuerfassung in das neue OK.FIS transportiert werden könnten. Somit müsste keineswegs mit verschiedenen Finanzadressen gearbeitet werden. Auch der Aufwand für die Pflege der Rechtevergabe (wer auf welche Daten in welcher Weise zugreifen darf) würde nicht höher liegen als bei vergleichbaren Verfahren.

Um den Kommunen den Umstieg auf die datenschutzgerechtere Programmversion von OK.FIS zu erleichtern, sagten mir die Vertreter der AKDB zu, die bestehende Bedienungsanleitung für das Verfahren zu überarbeiten und gezielter auf die dabei möglichen und notwendigen Schritte hinzuweisen.

Inwieweit durch den Einsatz von OK.FIS tatsächlich Probleme mit anderen AKDB-Ver-fahren auftreten, wird ebenfalls von der AKDB geklärt. Falls dies der Fall sein sollte, würden durch die AKDB eventuell erforderliche Programmanpassungen vorgenommen werden.

Aufgrund dieser Erkenntnisse besteht aus meiner Sicht nun kein Grund mehr, noch länger mit dem Umstieg auf die neue Programmversion zu warten. Ich fordere daher die betroffenen Stellen auf, so schnell wie möglich die neue datenschutzgerechte Version von OK.FIS einzusetzen.

23.6.2 Verlinkung auf der Homepage

Nahezu jede Behörde bietet die Möglichkeit, von ihrer Homepage aus auf die Web-Sei-ten anderer Anbieter zu verlinken. Das Setzen so genannter (Hyper-)Links auf fremde Web-Seiten ist aber ohne Einwilligung des davon betroffenen Homepage-Betreibers rechtlich umstritten. Einerseits wird argumentiert, dass, wer eine Homepage betreibt, damit rechnen muss (und wohl auch will), dass seine Webseiten aufgerufen werden, andererseits kann eine (ungewünschte) Verlinkung u.U. zu Problemen mit dem

- Zivilrecht (z.B. Schadensersatzforderungen),
- Urheberrecht (eine verlinkte Webseite kann Werke im Sinne des § 1 UrhG enthalten),
- Wettbewerbsrecht (evtl. sittenwidrige Leistungsübernahme, Herkunftstäuschung beim so genannten Framing) usw.

führen.

Einige Firmen sind inzwischen sogar dazu übergegangen, Rechnungen für die „unerlaubte Nutzung von Leistungen“ an Betreiber von Webseiten zu versenden, die Links auf die Webseite dieser Firmen gesetzt haben. Auf immer mehr Webseiten finden sich auch Hinweise darauf, unter welchen Voraussetzungen ein Verlinken auf ihre Seite erlaubt bzw. verboten ist. Diese Hinweise sind zumeist im Impressum, in der Datenschutzerklärung oder einer eigenen „Linking Policy“ integriert.

Ich kann daher nur raten, vor dem Setzen eines Links zu einer Webseite die schriftliche Einwilligung des betreffenden Homepage-Betreibers einzuholen oder sich zumindest davon zu vergewissern, dass diese Webseiten keine Erklärung beinhalten, die eine Verlinkung verbieten.

Da es auch Behörden gibt, die das Setzen von Links regulieren, empfehle ich bezüglich der Verlinkung zu anderen Behörden die gleiche Vorgehensweise. Gleiches gilt für die Veröffentlichung nicht anklickbarer Internetadressen der eigenen Homepage, da auch diese Adressen mittels Abtippen oder Kopieren sofort in den Browser eines Homepage-Besuchers übernommen werden können.

23.6.3 Voice over IP (VoIP)

Immer mehr Behörden ersetzen ihre bisherigen Telefonanlagen durch VoIP-Anlagen, um neue Anwendungen nutzen zu können oder auch die Kosten zu senken. Unter IP-Telefonie versteht man das Telefonieren über Computernetzwerke, die nach Internet-Standards aufgebaut sind. Allerdings ist eine Umstellung auf VoIP aus Datenschutzgründen nicht ganz unbedenklich, da VoIP-Verbindungen in den meisten Fällen noch wesentlich unsicherer sind als ein Telefongespräch über das herkömmliche Festnetz und somit eine Bedrohung für das Fernmeldegeheimnis darstellen.

Vorteile von VoIP

VoIP bietet seinen Nutzern viele Vorteile. So ermöglicht es beispielsweise drastische Kosteneinsparungen beim Telefonieren, wenn z.B. ohnehin vorhandene Hochgeschwindigkeitsverbindungen zwischen verschiedenen Standorten der gleichen Behörde genutzt werden. Auch die Zusammenlegung bereits vorhandener Daten- und Telefonnetze verspricht Kostensenkungen, da bei reinen IP- zu IP-Telefonaten für das Telefonieren über Computer und Internet sowie die hierfür benötigte Software keine Extrakosten anfallen. Wichtige Voraussetzung hierfür ist aber, dass die Telefongespräche zu keiner Zeit über das öffentliche Telefonnetz geführt werden.

Allerdings können im Zuge der Umstellung auf IP-Telefonie zusätzliche Kosten dadurch entstehen, dass neben dem Erwerb einer VoIP-Telefonanlage beispielsweise auch das vorhandene IT-Netzwerk für den Einsatz von Voice over IP unter Geschwindigkeitsaspekten aufgerüstet werden muss. Auch für die Gewährleistung der Verfügbarkeit fallen in der Regel zusätzliche Kosten an, da VoIP immer noch relativ störanfällig ist und VoIP-Telefonate beim Ausfall der Internetanbindung nicht möglich sind.

Ein weiterer Vorteil von VoIP besteht darin, dass neue, attraktive Dienste genutzt werden können, die einen erheblichen Mehrwert gegenüber den herkömmlichen Angeboten (z.B. ISDN-Anlagen) schaffen. So ist mit Voice over IP - ähnlich wie bei einer E-Mail - die gleichzeitige Übertragung von Sprache, Texten und Bildern über eine einzige Leitung möglich. Dabei wird die Sprache - genauso wie andere Daten - in Form von IP-Paketen in und über Netzwerke transportiert. Auch die Integration von VoIP in computergestützte Anwendungen wie Personal Information-Clients (beispielsweise Outlook) ist möglich. So können alle Kommunikationsvorgänge einheitlich und nahtlos abgewickelt und dokumentiert werden. Eingehende Anrufe können mittels Voice-Mailbox aufgezeichnet oder eigene Gespräche direkt aus der Anwendung gestartet werden. Sicher werden zukünftig Gespräche mittels Videokonferenzen geführt werden können. Weitere Dienste sind in der Planung. Auch das Handy wird zukünftig vermutlich immer mehr für VoIP genutzt werden.

Die Arbeitsplatzflexibilität kann ebenfalls mittels Voice over IP drastisch gesteigert werden. So kann der Arbeitsplatz zukünftig an jeden beliebigen Ort - ob in der Behörde, zu Hause oder unterwegs - verlegt werden und der Mitarbeiter ist trotzdem immer unter der gleichen Rufnummer erreichbar. Er benötigt lediglich einen Internet-Anschluss und einen Zugang zum behördeneigenen Netzwerk. Dies erleichtert natürlich auch die Kommunikation mit Telearbeitern und spart Kosten beim Umzug einer Telefonanlage.

Große Sicherheitsrisiken beim Internet-Telefonieren

Die Nutzung von Voice over IP birgt neben den Risiken, die für alle auf Basis des Internet bestehenden Kommunikationsformen bestehen (z.B. grundsätzlich unverschlüsselte Datenübertragung), noch zusätzliche Gefahren für den Datenschutz und die Datensicherheit. So ist es grundsätzlich jedem, der Zugang zum Netzwerk hat, möglich, mittels so genannter Sniffer (Schnüffelprogramme) neben den Daten-Paketen auch die Voice-Pakete abzuhören und aufzuzeichnen. Letztendlich handelt es sich in beiden Fällen lediglich um IP-Pakete. Auf diese Art sind für die gesprochene Kommunikation eine Reihe von neuen Angriffsformen denkbar, die derzeit nur aus dem konventionellen Internet-Datenverkehr bekannt sind, z.B. in Form von Replay-Attacken, call hijacking, Virenbefall, Denial-of-Service-Attacken oder Spam-Angriffen.

So stellt Voice Spam (auch Spit = Spam over Internet Telephony genannt) wohl derzeit die größte Gefahr für Voice over IP dar. Unter Voice Spam versteht man das massenhafte Beschicken von IP-basierten Telefonanschlüssen z.B. mit Klingelrundrufen oder mit einer ungeheuren Menge von Sprachpaketen. Dies kann zu einer erheblichen Belastung der Netz-Ressourcen und im Extremfall zu einem Zusammenbruch der Kommunikationsverbindungen führen.

Die Zusammenlegung des Datenverkehrs und der Telekommunikation ermöglicht Systemverwaltern neue, bisher ungeahnte Möglichkeiten, sich ein umfangreiches Wissen über die Nutzer zuzulegen, indem deren gesamter Netzverkehr (auch die Sprachübertragung) aufgezeichnet und ausgewertet bzw. manipuliert werden kann. Diesen Missbrauchsmöglichkeiten muss soweit wie möglich entgegengewirkt werden. So sollte beispielsweise die Aufbewahrdauer der Protokolldaten zeitlich beschränkt werden.

Die vielfältigen Anwendungsmöglichkeiten von VoIP-Anlagen können natürlich auch für eine Leistungs- und Verhaltenskontrolle (bezüglich des Telefonverhaltens) der Mitarbeiter genutzt werden. Es muss daher - in Zusammenarbeit mit dem Perso-

nalrat - darauf hingewirkt werden, dass die Persönlichkeitsrechte der Bediensteten im gleichen Umfang wie bei der bisherigen TK-Anlage gewahrt bleiben. Insbesondere darf im Regelfall der Inhalt der Kommunikation ohne Wissen oder gegen den Willen der Betroffenen nicht zur Kenntnis genommen werden. Ausnahmen von diesem Verbot der Kenntnisnahme sind grundsätzlich nur erlaubt, wenn dies im konkreten Einzelfall beispielsweise zur Verhinderung oder Aufdeckung einer Straftat erforderlich ist, dabei ein konkreter Tatverdacht gegen einen Mitarbeiter und keine andere Möglichkeit zur Aufklärung besteht.

Diese Gefahren sind vielen Verantwortlichen in den Behörden häufig zu wenig bewusst oder werden manchmal sogar ignoriert. So wird häufig argumentiert, dass der Einsatz von Sicherheitskomponenten wie Firewalls und Verschlüsselungssystemen eine schlechtere Sprachqualität sowie Gesprächsabbrüche verursachen könnten. Dieses kann durchaus zutreffen. Aber das darf in keinem Fall zu einem Verzicht auf die notwendigen Sicherheitsmaßnahmen führen.

Unbedingt notwendige Schutzmaßnahmen

Beim Einsatz von VoIP müssen insbesondere folgende Datensicherheitsmaßnahmen getroffen werden, um eine sichere und datenschutzgerechte Nutzung zu ermöglichen:

- Wird VoIP für Gespräche zwischen zwei bekannten behördlichen Teilnehmern verwendet, so ist die Verbindung wie alle anderen personenbezogenen Datenübertragungen über externe Netze zu verschlüsseln (z.B. mittels IPSEC oder Einsatz eines VPN). Dies gilt natürlich auch für eine eventuelle Fernwartung der VoIP-Soft- und -Hardware.

- Sowohl der Verbindungsaufbau wie der Verbindungsabbau müssen über eine Firewall kontrolliert erfolgen.

- Auch im Rahmen von Voice over IP müssen die gängigen Netzwerksicherheitsmaßnahmen wie der Einsatz von Virenscanner und die Vergabe differenzierter Zugangs- und Zugriffsrechte genutzt werden. Dazu ist unter Umständen eine Umkonfiguration dieser Systeme nötig.

- Die Endgeräte sind durch den Einsatz starker Zugangskontroll- und Authentifizierungsmechanismen zu schützen.

- Alle vorhandenen VoIP-Sicherheits-Features (wie etwa die Verschlüsselung der Sprachdaten mittels Secure Real-time Transport Protocol (SRTP)) sind konsequent zu nutzen und bekannt gewordene Sicherheitslücken unverzüglich durch Einspielen entsprechender Patches zu beseitigen.

- Die Administration des VoIP-Netzes sollte zwecks Missbrauchsbegrenzung in verschiedene Funktionen getrennt werden.

- Zur Erhöhung der Ausfallsicherheit des Internetzugangs muss ein entsprechendes Backup-Konzept entwickelt werden.

Der Arbeitskreis Technik der Datenschutzbeauftragten des Bundes und der Länder hat zu diesem Thema eine Arbeitsgruppe eingerichtet, um eine Orientierungshilfe zu VoIP zu erstellen. Sobald diese Orientierungshilfe vorliegt, kann sie auch über meine Homepage abgerufen werden.

23.6.4 Verschlüsselung von Webseiten mit selbstsignierten Zertifikaten

Um die Übertragung von Daten zwischen einem Webserver und seinem Besucher zu verschlüsseln und den Webserver gegenüber dem Besucher zu authentifizieren, wird in der Regel HTTPS verwendet. HTTPS steht für Hyper Text Transfer Protocol Secure und ist ein URL-Schema, das eine zusätzliche Schicht der Kommunikation zwischen Web-Server und Browser definiert. Ohne Verschlüsselung wären alle Web-Daten für jeden, der Zugang zu einem Netz hat, durch das die IP-Pakete laufen, im Klartext lesbar. HTTPS stellt das einzige Verschlüsselungsverfahren dar, das ohne gesonderte Softwareinstallation von allen aktuellen Browsern unterstützt wird.

Damit ein Server HTTPS anbieten kann, muss er ein Zertifikat, also einen öffentlichen und einen privaten Schlüssel, besitzen. Er teilt den öffentlichen Schlüssel dem Besucher mit. Dieser generiert einen zufälligen Sitzungsschlüssel und schickt diesen, mit dem öffentlichen Schlüssel des Servers verschlüsselt, an den Server. Dieser entschlüsselt den Sitzungsschlüssel mit seinem privaten Schlüssel und fortan verwenden beide Kommunikationsteilnehmer diesen Sitzungsschlüssel zur Verschlüsselung ihrer Kommunikation, so dass damit ein abhörsicherer Secure Sockets Layer (SSL) Tunnel zur Übertragung der Daten aufgebaut wird.

Somit kann zwar eine sichere Verbindung zur Abwehr von Abhörversuchen (etwa Man-In-The-Middle Angriffe) aufgebaut werden, es ist damit aber noch nicht sichergestellt, dass es sich bei dem Webserver auch um den richtigen und authentischen Webserver und nicht etwa um den eines Betrügers, z.B. für Phishing-Angriffe, handelt.

Damit ein Benutzer prüfen kann, mit welchem Server er gerade kommuniziert, wird das Serverzertifikat von einer dritten Stelle, der der Benutzer vertrauen können sollte, digital unterschrieben. Jeder Browser enthält von sich aus schon eine Liste von kommerziellen Zertifizierungsstellen, so dass alle von diesen Stellen unterschriebenen Zertifikate vom Browser als vertrauenswürdig eingestuft werden. Bei Aufruf einer so gesicherten Webseite erscheint beim Besucher keine Warnmeldung bzgl. des Serverzertifikates.

Neben diesen bereits vorinstallierten Zertifizierungsstellen kann es aber gerade in der Kommunikation zwischen Behörden sinnvoll sein, etwa Zertifikaten der PKI Verwaltung des Freistaates Bayern zu vertrauen. Dazu installiert die abrufende Behörde nach einer einmaligen, manuellen Echtheitsprüfung das Zertifikat der PKI im Browser und kann dann genau so sicher und komfortabel mit dem Webserver kommunizieren wie mit einem Standardzertifikat.

Anders verhält es sich mit selbst signierten Zertifikaten oder mit der Kommunikation von Behörden mit dem Bürger:

Über Websites von Behörden werden nicht mehr nur allgemeine Informationen angeboten, sondern zunehmend auch schutzwürdige Dialoge abgewickelt. Besucht ein Bürger nun eine Website einer Behörde, so ist es zwar erfreulich festzustellen, dass die Behörde die Kommunikation über https geschützt abwickeln will. Ich halte es aber nicht für anwenderfreundlich und auch nicht für zumutbar, dass der Benutzer für diesen unter Umständen einmaligen Besuch das von der Behörde selbst erstellte Zertifikat des Webservers manuell überprüft - soweit ihm dies überhaupt möglich ist. Im Normalfall wird er das vermutlich unterlassen, so dass die gute Intention der Behörde eigentlich ins Leere geht. Dass damit der Sache Bürgerfreundlichkeit und eGovernment wegen unsachgemäßer Anwendung von Datenschutz- und Datensicherheitsmaßnahmen auch kein Gefallen getan wird, liegt auf der Hand. Hier sollten also m.E. von den Behörden Zertifikate einer bereits im Browser vorinstallierten Zertifizierungsstelle verwendet werden, um so mit dem Komfort auch die Akzeptanz beim Benutzer zu erhöhen - auch wenn solche Zertifikate Geld kosten.

23.6.5 Sicheres WLAN

Mit neueren Verschlüsselungstechniken stehen im Vergleich zu den in Nr. 17.3.7 meines 21. Tätigkeitsberichts beschriebenen und damals vorhandenen IEEE-Standards 802.11 Wired Equivalent Privacy (WEP) in aktuellen Geräten nun Sicherheitsmassnahmen zu Verfügung, die bei richtiger Verwendung eine Übertragung von Daten bis mittleren Schutzbedarf über ein wireless local area network (WLAN) erlauben.

Bei Anwendung lediglich der WEP Verschlüsselung kann durch Aufzeichnung und Analyse größerer Datenmengen der Netzwerkschlüssel ermittelt werden, so dass eine Übertragung von personenbezogenen Daten über ein solchermaßen nur mittels WEP gesichertes WLAN nicht als datenschutzgerecht betrachtet werden kann.

Zur Verbesserung von WEP wurde ein Teil des IEEE-Standards 802.11i als Wi-Fi Protected Access (WPA) als Pseudostandard etabliert. Dieser beseitigt die Angriffsmöglichkeiten auf das WEP Protokoll und bietet bei sicher gewählten Passwörtern zumindest im Moment noch ausreichend Schutz.

Geräte, die den neuesten Standard WPA2 unterstützen, müssen sich vollständig an IEEE 802.11i halten und bieten somit den zur Zeit besten Schutz für die WLAN-Übertragung. Als Verschlüsselung wird hier in der Regel der Advanced Encryption Standard (AES) mit 128 Bit Schlüssellänge verwendet.

Bei der Beschaffung von neuer Hardware oder dem Ersatz von alter Hardware und der Planung von neuen Infrastrukturen sollte aus diesem Grund darauf geachtet werden, dass lediglich Geräte, die dem aktuellen Sicherheitsstandard (WPA2, IEEE 802.11i) genügen, verwendet werden.

Zur Authentifizierung des Clients am Access Point und umgekehrt kann sowohl bei WPA als auch bei WPA2 ein geheimer Text, der "Pre-Shared-Key", oder ein RADIUS-Server verwendet werden. Die Authentifizierung mit einem Pre-Shared-Key empfiehlt sich lediglich für kleinere Installationen, also z.B. für ein Funknetz mit wenigen Geräten z.B. im privaten Heimbereich.

In größeren Netzen ermöglicht die Verwendung des RADIUS Protokolls mit einem oder mehreren RADIUS-Servern eine zentrale Benutzeradministration. Der Access Point leitet in diesem Fall die Authentifizierungsanfrage des Clients an den RADIUS-Server weiter und lässt - je nach Erfolg - den Zugriff zu. Somit gibt es für die Sperrung oder Neueinrichtung einer Kennung eine zentrale Instanz.

WPA und WPA2 per RADIUS ermöglichen zusätzliche Authentifizierungsmethoden durch die Verwendung des Extensible Authentication Protocols (EAP) in Verbindung mit Tunneled Transport Layer Security (TTLS). EAP-TTLS erlaubt die Verwendung von Zertifikaten für die Authentifizierung. Dies ist für größere Installationen mit einem erhöhten Schutzbedarf zu bevorzugen, vor allem, wenn schon eine Public Key Infrastruktur (PKI) vorhanden oder geplant ist.

Es können entweder Benutzerzertifikate vergeben werden, so dass ein Benutzer dieses Zertifikat auf mehreren WLAN Geräten verwenden kann. Oder es werden Maschinenzertifikate verwendet, die es beispielsweise einem Laptop erlauben, sich in das WLAN einzubuchen - unabhängig davon, ob der Benutzer eine spezielle WLAN Berechtigung hat. Dies ist vor allem für „Abteilungs-Laptops“ von Vorteil, die etwa von unterschiedlichen Personen z.B. für Vorträge benutzt werden. Der Benutzer meldet sich am Laptop dann lediglich mit seiner normalen Kennung an, die vom Laptop dann transparent an den Betriebssystem-Anmeldeserver weitergegeben und dort geprüft wird. Dies funktioniert auch dann, wenn sich der Benutzer vorher noch nie an diesem Laptop angemeldet hatte.

Trotz aller mittlerweile in den Protokollen erfolgten Verbesserungen bleibt festzuhalten, dass WLANs ohne zusätzliche Schutzmassnahmen etwa auf der Anwendungsebene für einen datenschutzgerechten Einsatz und somit zur Verarbeitung von sensiblen personenbezogenen Daten nicht ausreichend sicher sind.

Nähere Hinweise zum datenschutzgerechten Einsatz von WLANs enthält Kapitel 2 der Orientierungshilfe „Datenschutz in drahtlosen Netzen“ - abrufbar auf meiner Homepage im Bereich Technik/Grundsätze/ Vernetzung.

23.6.6 Digitale Kopiersysteme

Nahezu alle zur Zeit im Einsatz befindlichen Kopiersysteme fallen unter die Kategorie digitale Kopiersysteme. Sie vereinen die Funktion eines Scanners mit der eines Druckers und bieten das Kopieren von Papierseiten an. Damit Funktionen wie Vergrößern, mehrere Seiten auf eine Seite kopieren etc. möglich werden, müssen die Geräte über ein Speichermedium verfügen, das die gescannten Seiten zwischenspeichert. In der Regel sind dies Festplatten in den heute zur Verfügung stehenden Größen, so dass dort ohne Probleme mehrere tausend Seiten gespeichert werden können.

Neben der Kopierfunktion stellen viele der modernen Multifunktionsgeräte auch noch Dienste wie Fax- und E-Mail-Versand zur Verfügung. Auch hier werden die eingescannten Daten zwischengespeichert. Das Gerät ist i.d.R. mit dem internen Netz verbunden und stellt so unter Umständen Daten zum Abruf bereit. Ebenso gibt es für solche Geräte oft eine Konfigurationsoberfläche, die mit Hilfe eines Webservers realisiert ist.

Zum einen ergibt sich hieraus die Gefahr, dass Mitarbeiter aus dem internen Netz unbefugt auf die im Kopiersystem gespeicherten Daten zugreifen können, etwa weil die Datenschnittstelle nicht sicher konfiguriert oder weil die Software des Druckers fehlerhaft ist (hier gibt es in der Regel keine Security Patches). Deshalb sollte genau überlegt werden, ob ein Kopiersystem an das interne Netz angeschlossen werden muss. Ist dies unbedingt nötig, sollte eine kleine Firewall den Zugriff darauf schützen und die Dienste des Kopierers sind restriktiv zu konfigurieren. Der Kopierer ist damit wie ein Server im eigenen Netz zu sichern und zu betreiben.

Die andere Gefahr, die unabhängig von einer Netzwerkschnittstelle besteht, liegt in der Weitergabe des Kopierers und damit der eingebauten Festplatte, etwa im Rahmen eines endenden Leasing-Vertrages oder bei Reparaturarbeiten. Es dürfte die Regel sein, dass zurückgegebene Festplatten erneut an andere Kunden weitergegeben werden. Hier ist darauf zu achten, dass alle personenbezogenen Daten vorher sicher gelöscht werden. Da das eventuell nur von der Wartungsfirma erledigt werden kann, ist dies in die Verträge aufzunehmen und auch stichprobenartig zu kontrollieren, indem man sich beispielsweise die Funktion des Löschens demonstrieren lässt.

24 Informationsmaterial und Orientierungshilfen

24.1 Aktuelle Datenschutznormen im Internet

Nachdem es vor allem für Bürger schwierig ist, aktuelle und verlässliche Quellen für Gesetzestexte und Normen im Internet zu finden, biete ich in Zusammenarbeit mit der Juris GmbH seit Juni 2005 auf meiner Hompage über vierzig einschlägige Vorschriften an - teils vollständig, teils in Auszügen mit den datenschutzrelevanten Teilen.

Die Gesetzes- und Vorschriftentexte sind abrufbar unter der Rubrik „Recht & Normen“ gruppiert nach den Kategorien

- Allgemeines Datenschutzrecht z.B. mit dem Bayerischen Datenschutzgesetz (BayDSG) sowie dem Bundesdatenschutzgesetz (BDSG),
- Verfassungsrecht,
- Sicherheitsrecht z.B. mit dem Polizeiaufgabengesetz (PAG),
- Gesundheitsrecht z.B. mit dem Bayerischen Krankenhausgesetz (BayKrG) und dem Gesundheitsdienst- und Verbraucherschutzgesetz (GDVG),

- Sozialrecht mit Auszügen aus den Sozialgesetzbüchern,
- Schul- und Hochschulrecht,
- Recht des öffentlichen Dienstes z.B. mit dem Bayerischen Beamtengesetz (BayBG) und dem Bayerischen Personalvertretungsgesetz (BayPVG),
- Recht der Medien und Telekommunikation z.B. mit dem Teledienstedatenschutzgesetz (TDDSG) und dem Telekommunikationsgesetz (TKG) sowie
- Sonstiges z.B. mit der Bayerischen Meldedaten-Übermittlungsverordnung (BayMeldeDÜV), der Abgabenordnung (AO) und dem Bundesstatistikgesetz (BStatG).

Die Texte werden im täglichen Turnus aktuell gehalten. Neueste Gesetzes- und Vorschriftenänderungen stehen somit zeitnah zur Verfügung. Ebenso wird eine Volltextsuche angeboten, sodass das Finden von Informationen erheblich erleichtert wird.

24.2 Neue Orientierungshilfen

Im Berichtszeitraum hat meine Geschäftsstelle folgende neue Ausarbeitungen und Orientierungshilfen erstellt:

- Private Internet- und E-Mail-Nutzung
- Einrichtung eines Benutzerservices
- PGP-Verschlüsselung - auch wenn man nichts zu verbergen hat!
- Anbindung externer Partner an Krankenhäuser zum Austausch patientenbezogener medizinischer Daten
- Pseudonymisierung in der medizinischen Forschung

Der Arbeitskreis Technik, der Arbeitskreis Medien bzw. der Arbeitskreis eGovernment der Datenschutzbeauftragten des Bundes und der Länder haben folgende Orientierungshilfen erstellt bzw. waren zum Redaktionsschluss noch mit den Arbeiten zu deren Fertigstellung befasst:

- Broschüre Datenschutzgerechtes eGovernment
- Datenschutz bei Dokumentenmanagementsystemen
- Datenschutz in drahtlosen Netzen
- Datenschutzgerechter Einsatz von RFID
- E-Mail und Internet am Arbeitsplatz
- Voice over IP (VoIP)

Alle Dokumente können von meiner Homepage abgerufen werden.

25 Die Datenschutzkommission

Der Datenschutzkommission beim Bayerischen Landtag gehörten in den vergangenen zwei Jahren folgende Mitglieder bzw. stellvertretende Mitglieder an:

Für den Landtag:

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

Für die Staatsregierung:

Hubert Kranz	Ministerialrat im Bayerischen Staatsministerium der Finanzen	Christian Peter Wilde	Ministerialrat im Bayerischen Staatsministerium des Innern

Für die Sozialversicherungsträger:

Werner Krempl	Erster Direktor und Geschäftsführer der Deutschen Rentenversicherung Ober- und Mittelfranken	Dr. Helmut Platzer	Vorstandsvorsitzender der AOK Bayern

Für die Kommunalen Spitzenverbände:

Wolfgang Kellner	Abteilungsleiter bei der AKDB	Klaus Laumer	Abteilungsleiter bei der AKDB

Für den Verband freier Berufe e.V.:

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

Den Vorsitz in der Datenschutzkommission führt Herr Prof. Dr. Gerhard Stockinger, MdL. Stellvertretende Vorsitzende ist Frau Bärbel Narnhammer, MdL.

Die Datenschutzkommission beim Bayerischen Landtag tagte im vergangenen Berichtszeitraum neun Mal. Dabei befasste sie sich u.a. mit folgenden Themen:

- Vorberatung des 21. Tätigkeitsberichtes
- Berichte über Beanstandungen
- Berichte von Datenschutzkonferenzen
- Kontenabfragen nach § 93 Absätze 7 und 8 der Abgabenordnung
- Änderung des Bayerischen Polizeiaufgabengesetzes (PAG)
- Berichte zum Sachstand Gesundheitskarte.

Anlage 1: **Entschließung der Datenschutzbeauftragten des Bundes und der Länder vom 17.02.2005**
Keine Gleichsetzung der DNA-Analyse mit dem Fingerabdruck

Die strafprozessuale DNA-Analyse ist - insbesondere in Fällen der Schwerstkriminalität wie bei Tötungsdelikten - ein effektives Fahndungsmittel. Dies hat zu Forderungen nach der Ausweitung ihres Anwendungsbereichs zur Identitätsfeststellung in künftigen Strafverfahren geführt. So sieht ein Gesetzesantrag mehrerer Bundesländer zum Bundesratsplenum vom 18. Februar 2005 die Streichung des Richtervorbehalts und der materiellen Erfordernisse einer Anlasstat von erheblicher Bedeutung sowie der Prognose weiterer schwerer Straftaten vor.

Das zur Begründung derartiger Vorschläge herangezogene Argument, die DNA-Analyse könne mit dem herkömmlichen Fingerabdruck gleichgesetzt werden, trifft jedoch nicht zu:

Zum einen hinterlässt jeder Mensch permanent Spurenmaterial z.B. in Form von Hautschuppen oder Haaren. Dies ist ein Grund für den Erfolg des Fahndungsinstruments „DNA-Analyse“, weil sich Täter vor dem Hinterlassen von Spuren nicht so einfach schützen können, wie dies bei Fingerabdrücken möglich ist. Es birgt aber - auch unter Berücksichtigung der gebotenen vorsichtigen Beweiswürdigung - in erhöhtem Maße die Gefahr, dass Unbeteiligte aufgrund zufällig hinterlassener Spuren am Tatort unberechtigten Verdächtigungen ausgesetzt werden oder dass sogar bewusst DNA-Material Dritter am Tatort ausgestreut wird.

Zum anderen lassen sich bereits nach dem derzeitigen Stand der Technik aus den sog. nicht-codierenden Abschnitten der DNA über die Identitätsfeststellung hinaus Zusatzinformationen entnehmen (Verwandtschaftsbeziehungen, wahrscheinliche Zugehörigkeit zu ethnischen Gruppen, aufgrund der räumlichen Nähe einzelner nicht-codierender Abschnitte zu codierenden Abschnitten möglicherweise Hinweise auf bestimmte Krankheiten). Die Feststellung des Geschlechts ist bereits nach geltendem Recht zugelassen. Nicht absehbar ist schließlich, welche zusätzlichen Erkenntnisse aufgrund des zu erwartenden Fortschritts der Analysetechniken zukünftig möglich sein werden.

Mit gutem Grund hat daher das Bundesverfassungsgericht in zwei Entscheidungen aus den Jahren 2000 und 2001 die Verfassungsmäßigkeit der DNA-Analyse zu Zwecken der Strafverfolgung nur im Hinblick auf die derzeitigen Voraussetzungen einer vorangegangenen Straftat von erheblicher Bedeutung, einer Prognose weiterer schwerer Straftaten und einer richterlichen Anordnung bejaht. Es hat besonders gefordert, dass diese Voraussetzungen auch nach den Umständen des Einzelfalls gegeben sein müssen und von der Richterin oder dem Richter genau zu prüfen sind.

Eine Prognose schwerer Straftaten und eine richterliche Anordnung müssen im Hinblick auf diese Rechtsprechung und den schwerwiegenden Eingriff in das Recht auf informationelle Selbstbestimmung, den die DNA-Analyse darstellt, auch zukünftig Voraussetzung einer derartigen Maßnahme bleiben.

Die besondere Qualität dieses Grundrechtseingriffs muss auch im übrigen bei allen Überlegungen, die derzeit zu einer möglichen Erweiterung des Anwendungsbereichs der DNA-Analyse angestellt werden, den Maßstab bilden; dies schließt eine Gleichsetzung in der Anwendung dieses besonderen Ermittlungswerkzeugs mit dem klassischen Fingerabdruckverfahren aus.

Anlage 2: **Entschließung der 69. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 10./11.03.2005**
Einführung der elektronischen Gesundheitskarte

Die Datenschutzbeauftragten des Bundes und der Länder begleiten aufmerksam die Einführung der elektronischen Gesundheitskarte. Sie weisen darauf hin, dass die über die Karte erfolgende Datenverarbeitung nach den gesetzlichen Vorgaben weitgehend auf Grund der Einwilligung der Versicherten erfolgen muss. Um die hierfür nötige Akzeptanz bei den Versicherten zu erlangen, sind neben den rechtlichen auch die tatsächlichen - technischen wie organisatorischen - Voraussetzungen zu schaffen, dass sowohl das Patientengeheimnis als auch die Wahlfreiheit bei der Datenspeicherung und -übermittlung gewahrt sind.

Die Versicherten müssen darüber informiert werden, welche Datenverarbeitungsprozesse mit der Karte durchgeführt werden können, wer hierfür verantwortlich ist und welche Bestimmungsmöglichkeiten sie hierbei haben. Das Zugriffskonzept auf medizinische Daten muss technisch so realisiert werden, dass in der Grundeinstellung das Patientengeheimnis auch gegenüber und zwischen Angehörigen der Heilberufe umfassend gewahrt bleibt. Die Verfügungsbefugnis der Versicherten über ihre Daten, wie sie bereits in den Entschließungen zur 47. und 50. Datenschutzkonferenz gefordert wurde, muss durch geeignete Maßnahmen sichergestellt werden, um die Vertrau-

lichkeit der konkreten elektronischen Kommunikationsbeziehungen unter Kontrolle der Betroffenen entsprechend dem gegenwärtigen technischen Stand zu gewährleisten.

Vor der obligatorischen flächendeckenden Einführung der elektronischen Gesundheitskarte sind die Verfahren und Komponenten auf ihre Funktionalität, ihre Patientenfreundlichkeit und ihre Datenschutzkonformität hin zu erproben und zu prüfen. Die Tests und Pilotversuche müssen ergebnisoffen ausgestaltet werden, damit die datenschutzfreundlichste Lösung gefunden werden kann. Eine vorzeitige Festlegung auf bestimmte Verfahren sollte deshalb unterbleiben.

Für die Bewertung der Gesundheitskarte und der neuen Telematikinfrastruktur können unabhängige Gutachten und Zertifizierungen förderlich sein, wie sie ein Datenschutz-Gütesiegel und ein Datenschutz-Audit vorsehen. Vorgesehene Einführungstermine dürfen kein Anlass dafür sein, dass von den bestehenden Datenschutzanforderungen Abstriche gemacht werden.

Anlage 3: **Entschließung der 69. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 10./11.03.2005 Datenschutzbeauftragte plädieren für Eingrenzung der Datenverarbeitung bei der Fußball-Weltmeisterschaft 2006**

Die Datenschutzbeauftragten des Bundes und der Länder betrachten das Vergabeverfahren für die Eintrittskarten zur Fußball-Weltmeisterschaft 2006 mit großer Sorge. Bei der Bestellung von Tickets müssen die Karteninteressentinnen und -interessenten ihre persönlichen Daten wie Name, Geburtsdatum, Adresse, Nationalität sowie ihre Ausweisdaten angeben, um bei der Ticketvergabe berücksichtigt zu werden. Die Datenschutzbeauftragten befürchten, dass mit der Personalisierung der Eintrittskarten eine Entwicklung angestoßen wird, in deren Folge die Bürgerinnen und Bürger nur nach Preisgabe ihrer persönlichen Daten an Veranstaltungen teilnehmen können.

Es wird deshalb gefordert, dass nur die personenbezogenen Daten erhoben werden, die für die Vergabe unbedingt erforderlich sind. Rechtlich problematisch ist insbesondere die vorgesehene Erhebung und Verarbeitung der Pass- bzw. Personalausweisnummer der Karteninteressentinnen und -interessenten. Der Gesetzgeber wollte die Gefahr einer Nutzung der Ausweis-Seriennummer als eindeutige Personenkennziffer ausschließen. Die Seriennummer darf damit beim Ticketverkauf nicht als Ordnungsmerkmal gespeichert werden. Zur Legitimation der Ticketinhaberin bzw. -inhabers beim Zutritt zu den Stadien ist sie nicht erforderlich. Das Konzept der Ticket-Vergabe sollte daher überarbeitet werden. Eine solche Vergabepraxis darf nicht zum Vorbild für den Ticketverkauf auf Großveranstaltungen werden. Solche Veranstaltungen müssen grundsätzlich ohne Identifizierungszwang besucht werden können.

Anlage 4: **Entschließung der Datenschutzbeauftragten des Bundes und der Länder vom 01.06.2005 Einführung biometrischer Ausweisdokumente**

Obwohl die Verordnung Nr. 2252/2004 des Europäischen Rates vom 13. Dezember 2004 die Mitgliedstaaten verpflichtet, bis Mitte 2006 mit der Ausgabe biometriegestützer Pässe für die Bürgerinnen und Bürger der Europäischen Union zu beginnen, sollen in Deutschland noch im laufenden Jahr die ersten Pässe ausgegeben werden.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder ist der Auffassung, dass mit der Ausgabe von elektronisch lesbaren biometrischen Ausweisdokumenten erst begonnen werden kann, wenn die technische Reife, der Datenschutz und die technische und organisatorische Sicherheit der vorgesehenen Verfahren gewährleistet sind. Diese Voraussetzungen sind bisher jedoch noch nicht in ausreichendem Maße gegeben.

Daher sind in einem umfassenden Datenschutz- und IT-Sicherheitskonzept zunächst technische und organisatorische Maßnahmen zur Wahrung des Rechts auf informationelle Selbstbestimmung festzulegen. Darüber hinaus sind im Passgesetz Regelungen zur strikten Zweckbindung der Daten erforderlich.

Die Konferenz begrüßt das Eintreten des Europäischen Parlaments für verbindliche Mindestanforderungen biometriegestützter Pässe zur Verhinderung des Missbrauchs, insbesondere des heimlichen Auslesens und der Manipulation der Daten. Die Konferenz bedauert es jedoch, dass die Einführung dieser Pässe beschlossen wurde, ohne dass die Chancen und Risiken der Technik ausreichend diskutiert wurden. Besonders problematisch ist es, dass die Entscheidung durch den Europäischen Rat der Regierungsvertreter entgegen der entsprechenden Stellungnahme des Europäischen Parlaments und der nationalen Gesetzgeber der EU-Mitgliedstaaten getroffen wurde.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder stellt fest, dass die Einführung biometrischer Merkmale nicht automatisch zur Verbesserung der Sicherheit führt. Noch immer weisen manche biometrische Identifikationsverfahren

hohe Falscherkennungsraten auf und sind oft mit einfachsten Mitteln zu überwinden. Scheinbar besonders sichere Ausweisdokumente werden durch den Einsatz unsicherer biometrischer Verfahren somit plötzlich zu einem Risikofaktor. Fehler bei der Erkennung von Personen haben zudem erhebliche Konsequenzen für die Betroffenen, weil sie einem besonderen Rechtfertigungsdruck und zusätzlichen Kontrollmaßnahmen ausgesetzt werden.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder fordert daher eine objektive Bewertung von biometrischen Verfahren und tritt dafür ein, die Ergebnisse entsprechender Untersuchungen und Pilotprojekte zu veröffentlichen und die Erkenntnisse mit der Wissenschaft und der breiten Öffentlichkeit zu diskutieren. Mit der Ausgabe von elektronisch lesbaren, biometrischen Ausweisdokumenten darf erst begonnen werden, wenn durch rechtliche, organisatorische und technische Maßnahmen gewährleistet wird,

- dass die biometrischen Merkmale ausschließlich von den für die Passkontrollen zuständigen Behörden für hoheitliche Zwecke genutzt werden,
- dass die in Ausweisen gespeicherten Daten mit den biometrischen Merkmalen nicht als Referenzdaten genutzt werden, um Daten aus unterschiedlichen Systemen und Kontexten zusammenzuführen,
- dass die für die Ausstellung und das Auslesen verwendeten Geräte nach internationalen Standards von einer unabhängigen Stelle zertifiziert werden,
- dass die verwendeten Lesegeräte in regelmäßigen zeitlichen Intervallen durch eine zentrale Einrichtung authentisiert werden,
- dass eine verbindliche Festlegung der zur Ausgabe oder Verifikation von Dokumenten zugriffsberechtigten Stellen erfolgt,
- dass vor der Einführung biometrischer Ausweise Verfahren festgelegt werden, die einen Datenmissbrauch beim Erfassen der Referenzdaten (sicheres Enrollment), beim weiteren Verfahren und bei der Kartennutzung verhindern,
- dass diese Verfahrensfestlegungen durch eine unabhängige Stelle evaluiert werden. Darüber hinaus muss sichergestellt sein, dass keine zentralen oder vernetzten Biometriedatenbanken geschaffen werden. Die biometrischen Identifizierungsdaten dürfen ausschließlich auf dem jeweiligen Ausweisdokument gespeichert werden. Durch international festzulegende Standards sowie Vorschriften und Vereinbarungen ist anzustreben, dass die bei Grenzkontrollen erhobenen Ausweisdaten weltweit nur gemäß eines noch festzulegenden einheitlichen hohen Datenschutz- und IT-Sicherheitsstandards verarbeitet werden.

Anlage 5: **Entschließung der 70. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 27./28.10.2005 Appell der Datenschutzbeauftragten des Bundes und der Länder: Eine moderne Informationsgesellschaft braucht mehr Datenschutz**

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder sieht für die 16. Legislaturperiode des Deutschen Bundestags großen Handlungsbedarf im Bereich des Datenschutzes. Der Weg in eine freiheitliche und demokratische Informationsgesellschaft unter Einsatz modernster Technologie zwingt alle Beteiligten, ein verstärktes Augenmerk auf den Schutz des Rechts auf informationelle Selbstbestimmung zu legen. Ohne wirksameren Datenschutz werden die Fortschritte vor allem in der Informations- und der Biotechnik nicht die für Wirtschaft und Verwaltung notwendige gesellschaftliche Akzeptanz finden.

Es bedarf einer grundlegenden Modernisierung des Datenschutzrechtes. Hierzu gehört eine Ergänzung des bisher auf Kontrolle und Beratung basierenden Datenschutzrechtes um Instrumente des wirtschaftlichen Anreizes, des Selbstdatenschutzes und der technischen Prävention. Es ist daher höchste Zeit, dass in dieser Legislaturperiode vom Deutschen Bundestag ein Datenschutz-Auditgesetz erarbeitet wird. Datenschutzkonforme Technikgestaltung als Wettbewerbsanreiz liegt im Interesse von Wirtschaft, Verwaltung und Bevölkerung. Zugleich ist die ins Stocken geratene umfassende Novellierung des Bundesdatenschutzgesetzes mit Nachdruck voranzutreiben. Eine Vereinfachung und Konzentration der rechtlichen Regelungen kann Bürokratie abbauen und zugleich den Grundrechtsschutz stärken.

Die Bürgerinnen und Bürger müssen auch in Zukunft frei von Überwachung sich informieren und miteinander kommunizieren können. Nur so können sie in der Informationsgesellschaft ihre Grundrechte selbstbestimmt in Anspruch nehmen. Dem laufen Bestrebungen zuwider, mit dem Argument einer vermeintlich höheren Sicherheit immer mehr alltägliche Aktivitäten der Menschen elektronisch zu registrieren und für Sicherheitszwecke auszuwerten. Die längerfristige Speicherung auf Vorrat von Verkehrsdaten bei der

Telekommunikation, die zunehmende Videoüberwachung im öffentlichen Raum, die anlasslose elektronische Erfassung des Straßenverkehrs durch Kfz-Kennzeichenabgleich, die Erfassung biometrischer Merkmale der Bevölkerung oder Bestrebungen zur Ausdehnung der Rasterfahndung betreffen ganz überwiegend völlig unverdächtige Bürgerinnen und Bürger und setzen diese der Gefahr der Ausforschung ihrer Lebensgewohnheiten und einem ständig wachsenden Anpassungsdruck aus, ohne dass dem immer ein adäquater Sicherheitsgewinn gegenübersteht. Freiheit und Sicherheit bedingen sich wechselseitig Angesichts zunehmender Überwachungsmöglichkeiten kommt der Freiheit vor staatlicher Beobachtung und Ausforschung sowie dem Grundsatz der Datensparsamkeit und Datenvermeidung eine zentrale Bedeutung zu.

Den Sicherheitsbehörden steht bereits ein breites Arsenal an gesetzlichen Eingriffsbefugnissen zur Verfügung, das teilweise überstürzt nach spektakulären Verbrechen geschaffen worden ist. Diese Eingriffsbefugnisse der Sicherheitsbehörden müssen einer umfassenden systematischen Evaluierung durch unabhängige Stellen unterworfen und öffentlich zur Diskussion gestellt werden. Unangemessene Eingriffsbefugnisse, also solche, die mehr schaden als nützen, sind wieder zurückzunehmen.

Die Kontrolle der Bürgerinnen und Bürger wird auch mit den Argumenten der Verhinderung des Missbrauchs staatlicher Leistungen und der Erhöhung der Steuerehrlichkeit vorangetrieben. So richtig es ist, in jedem Einzelfall die Voraussetzungen für staatliche Hilfen zu prüfen und bei hinreichenden Anhaltspunkten Steuerhinterziehungen nachzugehen, so überflüssig und rechtsstaatlich problematisch ist es, alle Menschen mit einem Pauschalverdacht zu überziehen und Sozial- und Steuerverwaltung mit dem Recht auszustatten, verdachtsunabhängig Datenabgleiche mit privaten und öffentlichen Datenbeständen vorzunehmen. Es muss verhindert werden, dass mit dem Argument der Leistungs- und Finanzkontrolle die Datenschutzgrundsätze der Zweckbindung und der informationellen Gewaltenteilung auf der Strecke bleiben.

Die Entwicklung in Medizin und Biotechnik macht eine Verbesserung des Schutzes des Patientengeheimnisses notwendig. Telemedizin, der Einsatz von High-Tech im Gesundheitswesen, gentechnische Verfahren und eine intensivierte Vernetzung der im Gesundheitsbereich Tätigen kann zu einer Verbesserung der Qualität der Gesundheitsversorgung und zugleich zur Kosteneinsparung beitragen. Zugleich drohen die Vertraulichkeit der Gesundheitsdaten und die Wahlfreiheit der Patientinnen und Patienten verloren zu gehen. Diese bedürfen dringend des gesetzlichen Schutzes, u.a. durch ein modernes Gendiagnostikgesetz und durch datenschutz- und patientenfreundliche Regulierung der Computermedizin.

Persönlichkeitsrechte und Datenschutz sind im Arbeitsverhältnis vielfältig bedroht, insbesondere durch neue Möglichkeiten der Kontrolle bei der Nutzung elektronischer Kommunikationsdienste, Videotechnik, Funksysteme und neue biotechnische Verfahren. Schranken werden bisher nur im Einzelfall durch Arbeitsgerichte gesetzt. Das seit vielen Jahren vom Deutschen Bundestag geforderte Arbeitnehmerdatenschutzgesetz muss endlich für beide Seiten im Arbeitsleben Rechtsklarheit und Sicherheit schaffen.

Die Datenschutzkontrolle hat mit der sich fast explosionsartig entwickelnden Informationstechnik nicht Schritt gehalten. Immer noch findet die Datenschutzkontrolle in manchen Ländern durch nachgeordnete Stellen statt. Generell sind Personalkapazität und technische Ausstattung unzureichend.. Dem steht die europarechtliche Anforderung entgegen, die Datenschutzaufsicht in völliger Unabhängigkeit auszuüben und diese adäquat personell und technisch auszustatten.

Die Europäische Union soll ein „Raum der Freiheit, der Sicherheit und des Rechts“ werden. Die Datenschutzbeauftragten des Bundes und der Länder sind sich bewusst, dass dies zu einer verstärkten Zusammenarbeit der Strafverfolgungsbehörden bei der Verbrechensbekämpfung in der Europäischen Union führen wird.

Die grenzüberschreitende Zusammenarbeit von Polizei- und Justizbehörden darf jedoch nicht zur Schwächung von Grundrechtspositionen der Betroffenen führen. Der vermehrte Austausch personenbezogener Daten setzt deshalb ein hohes und gleichwertiges Datenschutzniveau in allen EU-Mitgliedstaaten voraus. Dabei ist von besonderer Bedeutung, dass die Regelungen in enger Anlehnung an die Datenschutzrichtlinie 95/46/EG erfolgen, damit ein möglichst einheitlicher Datenschutz in der Europäischen Union gilt, der nicht zuletzt dem Ausgleich zwischen Freiheitsrechten und Sicherheitsbelangen dienen soll.

Die Datenschutzbeauftragten des Bundes und der genannten Länder appellieren an die Fraktionen im Bundestag und an die künftige Bundesregierung, sich verstärkt für den Grundrechtsschutz in der Informationsgesellschaft einzusetzen.

Anlage 6: **Entschließung der 70. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 27./28.10.2005 Keine Vorratsdatenspeicherung in der Telekommunikation**

Die Europäische Kommission hat den Entwurf einer Richtlinie über die Vorratsspeicherung von Daten über die elektronische Kommunikation vorgelegt. Danach sollen alle Telekommunikationsanbieter und Internet-Provider verpflichtet werden, systematisch eine Vielzahl von Daten über jeden einzelnen Kommunikationsvorgang über einen längeren Zeitraum (ein Jahr bei Telefonaten, sechs Monate bei Internet-Nutzung) für mögliche Abrufe von Sicherheitsbehörden selbst dann zu speichern, wenn sie diese Daten für betriebliche Zwecke (z.B. zur Abrechnung) gar nicht benötigen. Die Annahme dieses Vorschlags oder des gleichzeitig im Ministerrat beratenen, weiter gehenden Entwurfs eines Rahmenbeschlusses und ihre Umsetzung in nationales Recht würde einen Dammbruch zulasten des Datenschutzes unverdächtiger Bürgerinnen und Bürger bedeuten. Sowohl das grundgesetzlich geschützte Fernmeldegeheimnis als auch der durch die Europäische Menschenrechtskonvention garantierte Schutz der Privatsphäre drohen unverhältnismäßig eingeschränkt und in ihrem Wesensgehalt verletzt zu werden.

Die Datenschutzbeauftragten des Bundes und der Länder bekräftigen ihre bereits seit 2002 geäußerte grundsätzliche Kritik an jeder Pflicht zur anlassunabhängigen Vorratsdatenspeicherung. Die damit verbundenen Eingriffe in das Fernmeldegeheimnis und das informationelle Selbstbestimmungsrecht lassen sich auch nicht durch die Bekämpfung des Terrorismus rechtfertigen, weil sie unverhältnismäßig sind. Insbesondere gibt es keine überzeugende Begründung dafür, dass eine solche Maßnahme in einer demokratischen Gesellschaft zwingend notwendig wäre.

Die anlassunabhängige Vorratsdatenspeicherung aller Telefon- und Internetdaten ist von großer praktischer Tragweite und widerspricht den Grundregeln unserer demokratischen Gesellschaft. Erfasst würden nicht nur die Daten über die an sämtlichen Telefongesprächen und Telefax-Sendungen beteiligten Kommunikationspartner und -partnerinnen, sondern auch der jeweilige Zeitpunkt und die Dauer der Einwahl ins Internet, die dabei zugeteilte IP-Adresse, ferner die Verbindungsdaten jeder einzelnen E-Mail und jeder einzelnen SMS sowie die Standorte jeder Mobilkommunikation. Damit ließen sich europaweite Bewegungsprofile für einen Großteil der Bevölkerung für einen längeren Zeitraum erstellen.

Die von einigen Regierungen (z.B. der britischen Regierung nach den Terroranschlägen in London) gemachten Rechtfertigungsversuche lassen keinen eindeutigen Zweck einer solchen Maßnahme erkennen, sondern reichen von den Zwecken der Terrorismusbekämpfung und der Bekämpfung des organisierten Verbrechens bis hin zur allgemeinen Straftatenverfolgung. Alternative Regelungsansätze wie das in den USA praktizierte anlassbezogene Vorhalten ("Einfrieren" auf Anordnung der Strafverfolgungsbehörden und „Auftauen“ auf richterlichen Beschluss) sind bisher nicht ernsthaft erwogen worden.

Mit einem Quick-freeze Verfahren könnte man dem Interesse einer effektiven Strafverfolgung wirksam und zielgerichtet nachkommen.

Der Kommissionsvorschlag würde zu einer personenbezogenen Datensammlung von beispiellosem Ausmaß und zweifelhafter Eignung führen. Eine freie und unbefangene Telekommunikation wäre nicht mehr möglich. Jede Person, die in Zukunft solche Netze nutzt, würde unter Generalverdacht gestellt. Jeder Versuch, die zweckgebundene oder befristete Verwendung dieser Datensammlung auf Dauer sichern zu wollen, wäre zum Scheitern verurteilt. Derartige Datenbestände würden Begehrlichkeiten wecken, aufgrund derer die Hürde für einen Zugriff auf diese Daten immer weiter abgesenkt werden könnten. Auch aus diesem Grund muss bereits den ersten Versuchen, eine solche Vorratsdatenspeicherung einzuführen, entschieden entgegengetreten werden. Zudem ist eine Ausweitung der Vorratsdatenspeicherung auch auf Inhaltsdaten zu befürchten. Schon jetzt ist die Trennlinie zwischen Verkehrs- und Inhaltsdaten gerade bei der Internetnutzung nicht mehr zuverlässig zu ziehen. Dieselben - unzutreffenden - Argumente, die jetzt für eine flächendeckende Speicherung von Verkehrsdaten angeführt werden, würden bei einer Annahme des Kommissionsvorschlags alsbald auch für die anlassfreie Speicherung von Kommunikationsinhalten auf Vorrat ins Feld geführt werden.

Die Konferenz appelliert an die Bundesregierung, den Bundestag und das Europäische Parlament, einer Verpflichtung zur systematischen und anlasslosen Vorratsdatenspeicherung auf europäischer Ebene nicht zuzustimmen. Auf der Grundlage des Grundgesetzes wäre eine anlasslose Vorratsdatenspeicherung verfassungswidrig.

Anlage 7: **Entschließung der 70. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 27./28.10.2005 Gravierende Datenschutzmängel beim Arbeitslosengeld II endlich beseitigen**

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder stellt fest, dass bei der Um-

setzung der Zusammenlegung von Arbeitslosenhilfe und Sozialhilfe weiterhin erhebliche datenschutzrechtliche Mängel bestehen. Die Rechte der Betroffenen werden dadurch stark beeinträchtigt. Zwar ist das Verfahren der Datenerhebung durch die unter Beteiligung der Datenschutzbeauftragten des Bundes und der Länder überarbeiteten Antragsvordrucke auf dem Weg, datenschutzkonform ausgestaltet zu werden. Bei der Leistungs- und Berechnungssoftware A2LL gibt es jedoch entgegen den Zusagen des Bundesministeriums für Wirtschaft und Arbeit (BMWA) und der Bundesagentur für Arbeit (BA) immer noch keine erkennbaren Fortschritte.

Weder ist ein klar definiertes Zugriffsberechtigungskonzept umgesetzt, noch erfolgt eine Protokollierung der lesenden Zugriffe. Damit ist es über 40.000 Mitarbeiterinnen und Mitarbeitern in der BA und den Arbeitsgemeinschaften nach SGB II (ARGEn) nach wie vor möglich, voraussetzungslos auf die Daten aller Leistungsempfänger und -empfän-gerinnen zuzugreifen, ohne dass eine Kontrolle möglich wäre.

Dies gilt auch für das elektronische Vermittlungsverfahren coArb, das ebenfalls einen bundesweiten lesenden Zugriff erlaubt. Äußerst sensible Daten, wie z.B. Vermerke über Schulden-, Ehe- oder Suchtprobleme, können so eingesehen werden. Den Datenschutzbeauftragten sind bereits Missbrauchsfälle bekannt geworden. Einzelne ARGEn reagieren auf die Probleme und speichern ihre Unterlagen wieder in Papierform. Es muss sichergestellt sein, dass das Nachfolgesystem VerBIS, das Mitte 2006 einsatzbereit sein soll, grundsätzlich nur noch einen engen, regionalen Zugriff zulässt und ein detailliertes Berechtigungs- und Löschungskonzept beinhaltet. Der Datenschutz muss auch bei der Migration der Daten aus coArb in VerBIS beachtet werden.

Mit Unterstützung der Datenschutzbeauftragten des Bundes und der Länder hat die BA den Antragsvordruck und die Zusatzblätter überarbeitet. Soweit die Betroffenen auch die ergänzenden neuen Ausfüllhinweise erhalten, wird ihnen ein datenschutzgerechtes Ausfüllen der Unterlagen ermöglicht und damit eine Erhebung von nicht erforderlichen Daten vermieden. Doch ist immer noch festzustellen, dass die bisherigen Ausfüllhinweise nicht überall verfügbar sind. Es ist daher zu gewährleisten, dass allen Betroffenen nicht nur baldmöglichst die neuen Antragsvordrucke, sondern diese gemeinsam mit den Ausfüllhinweisen ausgehändigt werden („Paketlösung“).

Es handelt sich bei den ARGEn um eigenverantwortliche Daten verarbeitende Stellen, die uneingeschränkt der Kontrolle der Landesbeauftragten für Datenschutz unterliegen. Dies haben die Bundesanstalt und die ARGEn zu akzeptieren. Es ist nicht hinnehmbar, dass über die Verweigerung einer Datenschutzkontrolle rechtsfreie Räume entstehen und damit in unzumutbarer Weise in die Rechte der Betroffenen eingegriffen wird.

Die Datenschutzbeauftragten des Bundes und der Länder fordern die BA und die sonstigen verantwortlichen Stellen auf Bundes- und Länderebene auf, selbst und im Rahmen ihrer Rechtsaufsicht die Datenschutzmissstände beim Arbeitslosengeld II zu beseitigen. Für den Fall einer völligen Neugestaltung des Systems A2LL wegen der offenbar nicht zu beseitigenden Defizite erwarten die Datenschutzbeauftragten ihre zeitnahe Beteiligung. Es ist sicherzustellen, dass die datenschutzrechtlichen Vorgaben, wie die Protokollierung der lesenden Zugriffe und ein klar definiertes Zugriffsberechtigungs- und Löschungskonzept, ausreichend berücksichtigt werden, um den Schutz des informationellen Selbstbestimmungsrechts zu gewährleisten.

Anlage 8: **Entschließung der 70. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 27./28.10.2005 Telefonieren mit Internettechnologie (Voice over IP - VoIP)**

Die Internet-Telefonie verbreitet sich rasant. Mittlerweile bieten alle großen Provider in Deutschland das Telefonieren über das Internet an. Dabei ist den Kunden und Kundinnen oft nicht bekannt, dass diese Verbindungen in den meisten Fällen noch wesentlich unsicherer sind als ein Telefongespräch über das herkömmliche Festnetz.

Bei Telefongesprächen über das Internet kommt die Internet-Technologie Voice over IP (VoIP) zum Einsatz. In zunehmendem Maße wird angeboten, Telefongespräche mit Hilfe der Internet-Technologie VoIP zu führen. Das Fernmeldegeheimnis ist auch für die Internettelefonie zu gewährleisten. Während jedoch bei separaten, leitungsvermittelten Telekommunikationsnetzen Sicherheitskonzepte vorzulegen sind, ist dies bei VoIP bisher nicht die Praxis. Vielmehr werden diese Daten mit Hilfe des aus der Internetkommunikation bekannten Internet-Protokolls (IP) in Datenpakete unterteilt und paketweise über bestehende lokale Computernetze und/oder das offene Internet übermittelt.

Eine derartige Integration von Sprache und Daten in ein gemeinsames Netzwerk stellt den Datenschutz vor neue Herausforderungen. Die aus der Internetnutzung und dem Mail-Verkehr bekannten Unzulänglichkeiten und Sicherheitsprobleme können sich bei der Integration der Telefonie in die Datennetze auch auf die Inhalte und näheren Umstände der VoIP-Kommunikation auswirken und den Schutz des Fernmeldegeheimnisses beeinträchtigen. Beispiels-

weise können VoIP-Netzwerke durch automatisierte Versendung von Klingelrundrufen oder Überflutung mit Sprachpaketen blockiert, Inhalte und nähere Umstände der VoIP-Kommunikation mangels Verschlüsselung ausgespäht, kostenlose Anrufe durch Erschleichen von Authentifizierungsdaten geführt oder Schadsoftware wie Viren oder Trojaner aktiv werden. Darüber hinaus ist nicht auszuschließen, dass das Sicherheitsniveau der vorhandenen Datennetze negativ beeinflusst wird, wenn sie auch für den VoIP-Sprachdaten-Verkehr genutzt werden. Personenbezogene Daten der VoIP-Nutzenden können außerdem dadurch gefährdet sein, dass Anbieter von VoIP-Diensten ihren Sitz mitunter im außereuropäischen Ausland haben und dort möglicherweise weniger strengen Datenschutzanforderungen unterliegen als Anbieter mit Sitz in der Europäischen Union (EU).

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder fordert deshalb Hersteller und Herstellerinnen, Anbieter und Anbieterinnen sowie Anwender und Anwenderinnen von VoIP-Lösungen auf, das grundgesetzlich geschützte Fernmeldegeheimnis auch bei VoIP zu wahren und hierfür

- angemessene technische und organisatorische Maßnahmen zu treffen, um eine sichere und datenschutzgerechte Nutzung von VoIP in einem Netzwerk zu ermöglichen,
- Verschlüsselungsverfahren für VoIP anzubieten bzw. angebotene Verschlüsselungsmöglichkeiten zu nutzen,
- Sicherheits- und Datenschutzmängel, die die verwendeten Protokolle oder die genutzte Software bisher mit sich bringen, durch Mitarbeit an der Entwicklung möglichst schnell zu beseitigen,
- auf die Verwendung von offenen, standardisierten Lösungen zu achten beziehungsweise die verwendeten Protokolle und Algorithmen offenzulegen,
- VoIP-Kunden über die Gefahren und Einschränkungen gegenüber dem klassischen, leitungsvermittelten Telefondienst zu informieren und
- bei VoIP alle datenschutzrechtlichen Vorschriften genauso wie bei der klassischen Telefonie zu beachten.

In den benutzten Netzen, auf den beteiligten Servern und an den eingesetzten Endgeräten müssen angemessene Sicherheitsmaßnahmen umgesetzt werden, um die Verfügbarkeit, die Vertraulichkeit, die Integrität und die Authentizität der übertragenen Daten zu gewährleisten.

Anlage 9: Entschließung der 70. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 27./28.10.2005 Unabhängige Datenschutzkontrolle in Deutschland gewährleisten

Anlässlich eines von der Europäischen Kommission am 5. Juli 2005 eingeleiteten Vertragsverletzungsverfahrens gegen die Bundesrepublik Deutschland zur Unabhängigkeit der Datenschutzkontrolle fordert die Konferenz erneut eine völlig unabhängige Datenschutzkontrolle.

Die Richtlinie 95/46/EG zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (EG-Datenschutzrichtlinie) verlangt, dass die Einhaltung datenschutzrechtlicher Vorschriften in den Mitgliedstaaten von Stellen überwacht wird, die die ihnen zugewiesenen Aufgaben in völliger Unabhängigkeit wahrnehmen. In Deutschland ist indessen die Datenschutzkontrolle der Privatwirtschaft überwiegend in den Weisungsstrang der jeweiligen Innenverwaltung eingebunden. Diese Aufsichtsstruktur bei der Datenschutzkontrolle der Privatwirtschaft verstößt nach Ansicht der Europäischen Kommission gegen Europarecht.

Die Datenschutzbeauftragten des Bundes und der Länder können eine einheitliche Datenschutzkontrolle des öffentlichen und privaten Bereichs in völliger Unabhängigkeit sicherstellen. Sie sollten dazu in allen Ländern und im Bund als eigenständige Oberste Behörden eingerichtet werden, die keinen Weisungen anderer administrativer Organe unterliegen.

Demgegenüber ist die in Niedersachsen beabsichtigte Rückübertragung der Datenschutzkontrolle des privatwirtschaftlichen Bereichs vom Landesdatenschutzbeauftragten auf das Innenministerium ein Schritt in die falsche Richtung. Die Konferenz wendet sich entschieden gegen diese Planung und fordert den Bund sowie alle Länder auf, zügig europarechtskonforme Aufsichtsstrukturen im deutschen Datenschutz zu schaffen.

Anlage 10: Entschließung der 70. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 27./28.10.2005 Schutz des Kernbereichs privater Lebensgestaltung bei verdeckten Datenerhebungen der Sicherheitsbehörden

Aus dem Urteil des Bundesverfassungsgerichts vom 27. Juli 2005 zur präventiven Telekommunikations-

überwachung nach dem niedersächsischen Polizeigesetz folgt, dass der durch die Menschenwürde garantierte unantastbare Kernbereich privater Lebensgestaltung im Rahmen aller verdeckten Datenerhebungen der Sicherheitsbehörden uneingeschränkt zu gewährleisten ist. Bestehen im konkreten Fall Anhaltspunkte für die Annahme, dass eine Überwachungsmaßnahme Inhalte erfasst, die zu diesem Kernbereich zählen, ist sie nicht zu rechtfertigen und muss unterbleiben (Erhebungsverbot). Für solche Fälle reichen bloße Verwertungsverbote nicht aus.

Die Gesetzgeber in Bund und Ländern sind daher aufgerufen, alle Regelungen über verdeckte Ermittlungsmethoden diesen gerichtlichen Vorgaben entsprechend auszugestalten.

Diese Verpflichtung erstreckt sich auch auf die Umsetzung der gerichtlichen Vorgabe zur Wahrung des rechtsstaatlichen Gebots der Normenbestimmtheit und Normenklarheit. Insbesondere im Bereich der Vorfeldermittlungen verpflichtet dieses Gebot die Gesetzgeber auf Grund des hier besonders hohen Risikos einer Fehlprognose, handlungsbegrenzende Tatbestandselemente für die Tätigkeit der Sicherheitsbehörden zu normieren.

Im Rahmen der verfassungskonformen Ausgestaltung der Vorschriften sind die Gesetzgeber darüber hinaus verpflichtet, die gerichtlichen Vorgaben im Hinblick auf die Wahrung des Verhältnismäßigkeitsgrundsatzes - insbesondere die Angemessenheit der Datenerhebung -und eine strikte Zweckbindung umzusetzen.

In der Entscheidung vom 27. Juli 2005 hat das Gericht erneut die Bedeutung der - zuletzt auch in seinen Entscheidungen zum Großen Lauschangriff und zum Außenwirtschaftsgesetz vom 3. März 2004 dargelegten - Verfahrenssicherungen zur Gewährleistung der Rechte der Betroffenen hervorgehoben. So verpflichtet beispielsweise das Gebot der effektiven Rechtsschutzgewährung die Sicherheitsbehörden, Betroffene über die verdeckte Datenerhebung zu informieren.

Diese Grundsätze sind sowohl im Bereich der Gefahrenabwehr als auch im Bereich der Strafverfolgung, u.a. bei der Novellierung der §§ 100a und 100b StPO, zu beachten.

Die Konferenz der DSB erwartet, dass nunmehr zügig die erforderlichen Gesetzgebungsarbeiten in Bund und Ländern zum Schutz des Kernbereichs privater Lebensgestaltung bei allen verdeckten Ermittlungsmaßnahmen aufgenommen und die Vorgaben des Bundesverfassungsgerichts ohne Abstriche umgesetzt werden.

Anlage 11: **Entschließung der 70. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 27./28.10.2005 Telefonbefragungen von Leistungsbeziehern und Leistungsbezieherinnen von Arbeitslosengeld II datenschutzgerecht gestalten**

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder weist anlässlich von durch die Bundesanstalt mit Hilfe privaten Callcentern durchgeführten Telefonbefragungen bei Leistungsbeziehern und Leistungsbezieherinnen von Arbeitslosengeld II darauf hin, dass es den Betroffenen unbenommen ist, sich auf ihr Grundrecht auf informationelle Selbstbestimmung zu berufen. Da die Befragung freiwillig war, hatten sie das Recht, die Beantwortung von Fragen am Telefon zu verweigern.

Die Ablehnung der Teilnahme an einer solchen Befragung rechtfertigt nicht den Verdacht auf Leistungsmissbrauch. Wer seine Datenschutzrechte in Anspruch nimmt, darf nicht deshalb des Leistungsmissbrauchs bezichtigt werden.

Die Konferenz fordert daher das Bundesministerium für Wirtschaft und Arbeit und die Bundesanstalt für Arbeit dazu auf, die Sach- und Rechtslage klarzustellen und bei der bereits angekündigten neuen Telefonaktion eine rechtzeitige Beteiligung der Datenschutzbeauftragten sicherzustellen.

Anlage 12: **Entschließung der Datenschutzbeauftragten des Bundes und der Länder vom 15.12.2005**
Sicherheit bei eGovernment durch Nutzung des Standards OSCI

In modernen eGovernment-Verfahren werden personenbezogene Daten zahlreicher Fachverfahren zwischen unterschiedlichen Verwaltungsträgern in Bund, Ländern und Kommunen übertragen. Die Vertraulichkeit, Integrität und Zurechenbarkeit der übertragenen Daten kann nur gewährleistet werden, wenn dem Stand der Technik entsprechende Verschlüsselungs- und Signaturverfahren genutzt werden.

Mit dem Online Services Computer Interface (OSCI) steht bereits ein bewährter Sicherheits-Standard für eGovernment-Anwendungen zur Verfügung. Verfahren, die diese Standards berücksichtigen, bieten die Gewähr für eine durchgehende Sicherheit bei der Datenübermittlung vom Versand bis zum Empfang (Ende-zu-Ende-Sicherheit) und erlauben somit auch

rechtsverbindliche Transaktionen zwischen den beteiligten Kommunikationspartnerinnen und -partnern.

Die durchgehende Sicherheit darf nicht dauerhaft durch Vermittlungs- und Übersetzungsdienste, die nicht der OSCI-Spezifikation entsprechen, beeinträchtigt werden. Werden solche Dienste zusätzlich in die behördlichen Kommunikationsströme eingeschaltet, wird das mit OSCI-Transport erreichbare Sicherheitsniveau abgesenkt. Der Einsatz von sogenannten Clearingstellen, wie sie zunächst für das automatisierte Meldeverfahren vorgesehen sind, kann daher nur eine Übergangslösung sein.

Werden Programme und Schnittstellen auf der Basis derartiger Standards entwickelt, ist sichergestellt, dass die Produkte verschiedener Anbieterinnen und Anbieter im Wettbewerb grundlegende Anforderungen des Datenschutzes und der Datensicherheit in vergleichbar hoher Qualität erfüllen. Gleichzeitig erleichtern definierte Standards den öffentlichen Verwaltungen die Auswahl datenschutzkonformer, interoperabler Produkte.

Vor diesem Hintergrund begrüßt die Konferenz der Datenschutzbeauftragten des Bundes und der Länder die vom Koordinierungsausschuss Automatisierte Datenverarbeitung (KoopA ADV), dem gemeinsamen Gremium von Bund, Ländern und Kommunalen Spitzenverbänden, getroffene Festlegung, in eGovernment-Projekten den Standard OSCI-Transport für die Übermittlung von personenbezogenen Daten einzusetzen. Um die angestrebte Ende-zu-Ende-Sicherheit überall zu erreichen, empfiehlt sie einen flächendeckenden Aufbau einer OSCI-basierten Infrastruktur.

Anlage 13: **Entschließung der 71. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 16./17.03.2006 Keine kontrollfreien Räume bei der Leistung von ALG II**

Die Datenschutzbeauftragten des Bundes und der Länder haben die Bundesagentur für Arbeit (BA) und die sonstigen verantwortlichen Stellen auf Bundes- und Länderebene in ihrer Entschließung vom 27./28. Oktober 2005 aufgefordert, die Datenschutzmissstände beim Arbeitslosengeld II zu beseitigen. Zu diesen Missständen gehört die wiederholte Weigerung der BA, Landesbeauftragten für den Datenschutz zu ermöglichen, ihre Kontrollaufgaben bei den Arbeitsgemeinschaften nach dem SGB II (ARGEn) zu erfüllen. Mit einer „Weisung“ vom 31. Januar 2006 versucht die BA, nunmehr alle ARGEn auf diese Linie zu verpflichten. Den Landesdatenschutzbeauftragten soll der für Kontrollzwecke notwendige Zugriff auf die zentralen automatisierten Verfahren verwehrt werden.

Der Bundesbeauftragte für den Datenschutz und die Landesdatenschutzbeauftragten bekräftigen ihre gemeinsame Auffassung, dass es sich bei den ARGEn um eigenverantwortliche Daten verarbeitende Stellen der Länder handelt, die uneingeschränkt der Kontrolle der Landesbeauftragten für den Datenschutz unterliegen. Dass die BA Ressourcen für die Arbeitsgemeinschaften bereitstellt, ändert nichts an diesem Ergebnis.

Es muss gewährleistet sein, dass die Verarbeitung von Sozialdaten in den ARGEn von den jeweils zuständigen Landesbeauftragten umfassend und ohne inhaltliche Beschränkungen datenschutzrechtlich überprüft werden kann. Eine rechtliche Konstellation, durch die die Landesbeauftragten für den Datenschutz von der Kontrolle der ARGEn ausgeschlossen würden, würde gegen die bundesstaatliche Kompetenzordnung verstoßen und wäre einer effektiven Datenschutzkontrolle abträglich. Sie würde den Grundrechtsschutz der betroffenen Bürgerinnen und Bürger empfindlich beeinträchtigen.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder fordert die Bundesregierung dazu auf, umgehend einen rechtskonformen Zustand herzustellen.

Anlage 14: **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**

Auf europäischer Ebene wird verstärkt über die Ausweitung des grenzüberschreitenden Informationsaustauschs für Zwecke der Polizei und Justiz mit dem Ziel diskutiert, einen Raum der Freiheit, der Sicherheit und des Rechts zu schaffen. Der Austausch personenbezogener Informationen zwischen den Strafverfolgungsbehörden der Mitgliedstaaten setzt ein hohes und gleichwertiges Datenschutzniveau bei allen beteiligten Stellen voraus.

Die Datenschutzbeauftragten des Bundes und der Länder begrüßen, dass die EU-Kommission einen Rahmenbeschluss zur Harmonisierung und zum Ausbau des Datenschutzes bei den Polizei- und Justizbehörden vorgelegt hat. Sie betonen, dass die Regelungen in enger Anlehnung an die allgemeine Datenschutzrichtlinie (95/46/EG) erfolgen müssen, damit der Datenschutz in der EU auf einem einheitlich hohen Niveau gewährleistet wird.

Die Datenschutzbeauftragten des Bundes und der Länder unterstützen die Forderungen der Europäischen Datenschutzkonferenz in ihrem Beschluss vom 24. Januar 2006. Auch sie treten dafür ein, den Datenschutz im Zusammenarbeitsbereich der sog. „Dritten Säule“ der EU im Sinne der EU-Grundrechte-Charta zu gestalten.

Dies bedeutet u.a., dass Eingriffe in Freiheitsrechte nur im überwiegenden öffentlichen Interesse und im Rahmen der Verhältnismäßigkeit zulässig sind. Die Rahmenrichtlinie muss die Voraussetzungen der Datenverarbeitung und -übermittlung nach den jeweiligen Rollen der Verfahrensbeteiligten (Beschuldigte, Verdächtigte, Zeugen und Zeuginnen, Opfer) normenklar und differenziert regeln. Zudem müssen die Rechte der Betroffenen auf Auskunft, Berichtigung und Löschung gewährleistet werden. Die Datenverarbeitung muss umfassend durch unabhängige Datenschutzbehörden kontrolliert werden können. Die Datenschutzkontrollrechte müssen - unter Beachtung der richterlichen Unabhängigkeit - gewahrt werden. Sie dürfen nicht mit der Begründung eingeschränkt werden, dass ein laufendes Verfahren vorliege oder die Gefahrenabwehr bzw. die Strafverfolgung behindert werde. Einheitliche Datenschutzregelungen müssen zudem alle Formen der Datenverarbeitung - auch sofern sie in Akten erfolgt - einbeziehen.

Daten von europäischen Polizei- und Justizbehörden dürfen an Drittstaaten außerhalb der EU nur übermittelt werden, wenn ihre Verarbeitung im Zielland nach rechtsstaatlichen Grundsätzen erfolgt und ein angemessener Datenschutz sichergestellt ist. Bei der polizeilichen und justiziellen Zusammenarbeit in Strafsachen muss ferner der Grundsatz der Zweckbindung beachtet werden. Abweichungen des ersuchenden Staates vom angegebenen Verwendungszweck müssen auf Ausnahmefälle von besonderem Gewicht beschränkt bleiben. Die Ausnahmen müssen für den ersuchten Staat umfassend und zeitnah kontrollierbar sein.

Zur Schaffung eines hohen und einheitlichen Datenschutzstandards in der Dritten Säule der EU gibt es keine Alternative. Es darf nicht dazu kommen, dass auf europäischer Ebene weitere Eingriffsbefugnisse für die Sicherheitsbehörden mit immer tieferen Einschnitten in die Grundrechte beschlossen werden, ohne dass gleichzeitig die Freiheitsrechte der hier lebenden Bürgerinnen und Bürger gestärkt und geschützt werden. Aus diesem Grund hält es die Konferenz für dringend erforderlich, entsprechende Datenschutzbestimmungen zügig zu verabschieden und umzusetzen, bevor der Datenaustausch weiter ausgebaut wird.

Anlage 15: Entschließung der 71. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 16./17.03.2006 Listen der Vereinten Nationen und der Europäischen Union über Terrorverdächtige

In den vergangenen Monaten sind die vom Sanktionsausschuss der Vereinten Nationen (VN) erstellten Listen über terrorverdächtige Personen und Organisationen, die von der Europäischen Gemeinschaft durch entsprechende Verordnungen umgesetzt worden sind, in den Blickpunkt der Öffentlichkeit gerückt. Personen, die auf diesen Listen erscheinen, unterliegen umfangreichen Beschränkungen, die von Wirtschafts- und Finanzsanktionen über Einreiseverbote bis hin zum Einfrieren ihrer Gelder und anderer Vermögenswerte reichen.

Ein Eintrag in den genannten Listen greift in das informationelle Selbstbestimmungsrecht der betreffenden Personen ein und kann darüber hinaus gravierende existentielle Folgen haben, die z.B. die Verweigerung von Sozialleistungen umfassen können. Vielfach sind diese Personen nicht eindeutig bezeichnet. Auch in Deutschland lebende Personen sind von entsprechenden Maßnahmen betroffen. In jüngster Zeit gab es Verwechslungen mit schwer wiegenden Folgen für völlig unverdächtige Personen. Besonders kritisch ist zu werten, dass gegen die Aufnahme in die Listen kein Rechtsschutz besteht.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder fordert daher die Bundesregierung auf, bei den Vereinten Nationen und in der Europäischen Union auf die Einhaltung der rechtsstaatlich gebotenen Standards zu dringen. Dazu gehören insbesondere ein transparentes Listing-Verfahren, Entscheidungen auf einer gesicherten Tatsachenbasis, ein zweifelsfreier Identitätsnachweis und effektiver Rechtsschutz.

Anlage 16: Entschließung der 71. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 16./17.03.2006 Keine Aushöhlung des Fernmeldegeheimnisses im Urheberrecht

Das Bundesministerium der Justiz hat den Referentenentwurf eines „Gesetzes zur Verbesserung der Durchsetzung von Rechten des geistigen Eigentums“ vorgelegt, das in Umsetzung einer europäischen Richtlinie stärkere Instrumente zum Schutz des Urheberrechts und anderer gewerblicher Schutzrechte einführen soll.

Der Gesetzentwurf gesteht den Rechteinhabenden in bestimmten Fällen Auskunftsansprüche auch gegenüber unbeteiligten Dritten zu, die selbst keine Urheberrechtsverletzungen begangen haben. So sollen etwa Internet-Provider auch über - durch das Fernmeldegeheimnis geschützte - Daten ihrer Nutzerinnen und Nutzer zur Auskunft verpflichtet werden. Damit sollen beispielsweise Anbietende und Nutzende illegal kopierter Musik- oder Videodateien oder Software leichter ermittelt werden können.

Die Datenschutzbeauftragten des Bundes und der Länder warnen vor der hiermit eingeleiteten Entwicklung. Zwar sind die vorgesehenen Eingriffe in das Fernmeldegeheimnis in dem Entwurf an formale Hürden geknüpft; insbesondere müssen Rechteinhabende eine richterliche Anordnung erwirken. Jedoch lassen die europarechtlichen Vorgaben den Mitgliedstaaten zugunsten des Datenschutzes so viel Spielraum, dass Eingriffe in das Fernmeldegeheimnis vermieden werden können. Das Bundesverfassungsgericht hat betont, dass gemeinschaftsrechtliche Spielräume zu nutzen sind.

Nachdem das grundrechtlich geschützte Fernmeldegeheimnis in den letzten Jahren immer stärker und in immer kürzeren Abständen für Zwecke der Strafverfolgung und der Geheimdienste eingeschränkt wurde, soll es nun auch erstmals zugunsten privater wirtschaftlicher Interessen nicht unerheblich weiter eingeschränkt werden. Es ist zu befürchten, dass damit ähnliche Begehrlichkeiten weiterer privater Interessengruppen geweckt werden. Dem grundrechtlich geschützten Fernmeldegeheimnis unterliegende Daten stünden am Ende der Entwicklung für kaum noch zu übersehende Zwecke zur Verfügung.

Es ist zu befürchten, dass durch die Auskunftsansprüche gegen Internet-Provider die gerade für die Verfolgung schwerer Straftaten beschlossene Verpflichtung zur Vorratsdatenspeicherung von Verkehrsdaten für die Durchsetzung privater Interessen genutzt wird. Angesichts der Tendenz, die Internet-Anbietenden in immer stärkerem Maße für die Kommunikationsinhalte ihrer Kunden verantwortlich zu machen, ist zudem zu befürchten, dass die Firmen vorsichtshalber weitere Verkehrsdaten speichern, um im Falle von Rechtsverletzungen Auskünfte erteilen zu können.

Die Datenschutzbeauftragten des Bundes und der Länder appellieren deshalb an die Bundesregierung und an den Gesetzgeber, auf eine weitere Einschränkung des Fernmeldegeheimnisses - erstmals zur Durchsetzung wirtschaftlicher Interessen - zu verzichten. Es wäre völlig unakzeptabel, wenn Daten, deren zwangsweise Speicherung mit der Abwehr terroristischer Gefahren begründet wurde, nun auf breiter Basis für die Verfolgung von Urheberrechtsverletzungen genutzt würden. Musik- und Filmindustrie müssen selbst dafür Sorge tragen, dass durch technische Maßnahmen und neue Geschäftsmodelle unrechtmäßigen Nutzungen die Grundlage entzogen wird.

Anlage 17: **Entschließung der Datenschutzbeauftragten des Bundes und der Länder vom 11.10.2006 (bei Enthaltung von Schleswig-Holstein) Sachgemäße Nutzung von Authentisierungs- und Signaturverfahren**

Die Datenschutzbeauftragten des Bundes und der Länder beobachten einen Trend, abweichend von den bislang geltenden Vorgaben zur Nutzung der qualifizierten elektronischen Signatur in der öffentlichen Verwaltung zunehmend ungeeignete oder weniger sichere Verfahren zuzulassen. So soll beispielsweise infolge des Gesetzentwurfes der Bundesregierung zum Jahressteuergesetz 2007 (BR-Drs. 622/06) beim Verfahren Elster Online der Finanzverwaltung das in § 87a AO Abs. 3 geforderte Verfahren zur qualifizierten elektronischen Signatur durch ein Verfahren ersetzt werden, das lediglich zur Authentisierung der Datenübermittler geeignet ist. Auch die Planungen zum Verfahren für den elektronischen Einkommensnachweis ELENA sehen zumindest für einen Übergangszeitraum den Verzicht auf die qualifizierte elektronische Signatur vor. Einer derartigen Fehlentwicklung muss mit Nachdruck entgegengetreten werden.

Obwohl Signatur- und Authentisierungsverfahren mit der asymmetrischen Verschlüsselung vergleichbare technische Verfahren nutzen, unterscheiden sie sich im Inhalt ihrer Aussagen und müssen unterschiedliche Rechtsfolgen für die Nutzenden nach sich ziehen. Der grundlegende Unterschied dieser Verfahren muss sowohl bei der Planung als auch bei ihrem Einsatz in Verwaltungsverfahren berücksichtigt werden.

Elektronische Signaturen liefern Aussagen über elektronische Dokumente, insbesondere über deren Authentizität und Integrität. Ausschließlich die qualifizierte elektronische Signatur ist durch rechtliche Regelungen der eigenhändigen Unterschrift in weiten Bereichen gleichgestellt und dient dem Nachweis der Echtheit elektronischer Dokumente. Zudem sind nur Verfahren zur Erzeugung elektronischer Signaturen rechtlich geregelt und sicherheitstechnisch genau definiert.

Authentisierungsverfahren liefern hingegen lediglich eine Aussage über die Identität einer Person oder einer Systemkomponente. Solche Verfahren sind beispielsweise zur Authentifizierung einer Person oder eines IT-Systems gegenüber Kommunikations-

partnern oder zur Anmeldung an einem IT-System geeignet. Die hierbei ausgetauschten Informationen unterliegen in der Regel nicht dem Willen und dem Einfluss der Rechnernutzenden bzw. der Kommunikationspartner und beziehen sich ausschließlich auf den technischen Identifizierungsprozess. Daher dürfen an die Authentizität und Integrität solcher Daten nicht die gleichen Rechtsfolgen geknüpft werden wie an eine qualifizierte elektronische Signatur.

Die Aufrechterhaltung der unterschiedlichen Funktionalität und Verbindlichkeit von Signatur und Authentisierung liegt sowohl im Interesse von Bürgerinnen und Bürgern als auch der Verwaltung und ist rechtlich geboten. Die unsachgemäße Anwendung oder in Kauf genommene Funktionsvermischung dieser Verfahren mindert die Transparenz, die Sicherheit und die Verlässlichkeit bei der elektronischen Datenverarbeitung. Darüber hinaus sind erhebliche Nachteile für die Nutzenden zu erwarten.

Wird ein Authentisierungsschlüssel zum Signieren verwendet,

- kann fälschlicher Weise behauptet werden, dass Nutzende elektronische Dokumente signiert haben; da sie das Gegenteil nicht beweisen können, müssen sie befürchten, die damit verbundenen Rechtsfolgen tragen zu müssen,
- besteht die Möglichkeit, dass Authentisierungsverfahren (Single Sign On, Challenge Response etc.) gezielt missbräuchlich verwendet werden,
- wird den Nutzenden keine „Warnfunktion“ mehr angeboten wie bei der ausschließlichen Verwendung des Signaturschlüssels zum Signieren und
- sind die Verfahren und die daraus resultierenden Konsequenzen für die Nutzenden nicht mehr transparent.

Vor diesem Hintergrund fordert die Konferenz der Datenschutzbeauftragten des Bundes und der Länder, dass der Gesetzgeber weder ungeeignete noch weniger sichere Verfahren zulässt. Dies bedeutet, dass

- Nutzenden die Möglichkeit eröffnet werden muss, die elektronische Kommunikation mit der Verwaltung durch eine qualifizierte elektronische Signatur abzusichern,
- immer dann Signaturverfahren eingesetzt werden müssen, wenn Aussagen über Dokumente oder Nachrichten gefordert sind und Authentisierungsverfahren nur dort verwendet werden dürfen, wo es um Aussagen über eine Person oder eine Systemkomponente geht,
- die Transparenz der Verfahren und die Nutzbarkeit der Authentisierungsfunktion erhalten bleiben müssen.

Die Datenschutzbeauftragten appellieren darüber hinaus an die Verantwortlichen in der Verwaltung und bei den Projektträgern, gemeinsam die offenen Fragen beim Einsatz der qualifizierten elektronischen Signatur zu lösen und insbesondere die Entwicklung interoperabler, ökonomischer Verfahren zur Prüfung qualifizierter elektronischer Signaturen zu unterstützen. Hierfür ist die konstruktive Zusammenarbeit der Verantwortlichen von großen Anwendungsverfahren wie Elster Online, ELENA und Elektronische Gesundheitskarte unabdingbar.

Die Bundesregierung sollte verstärkt die Einführung von Verfahren mit qualifizierter elektronischer Signatur unterstützen, weil diese Verfahren für die sichere und authentische Kommunikation zwischen Bürgerinnen und Bürgern und der Verwaltung besonders geeignet sind. Die qualifizierte elektronische Signatur muss eine zentrale Komponente in eGovernment-Anwendungen sein, und darf nicht durch ungeeignete oder weniger sichere Verfahren ersetzt werden. Die Bundesregierung sollte daher die Verbreitung von Chipkarten mit qualifiziertem Zertifikat fördern. Erst der flächendeckende Einsatz von qualifizierten elektronischen Signaturen ermöglicht niedrige Kosten bei der Bereitstellung der Karten und führt darüber hinaus zu rationellen und somit kostengünstigen Verwaltungsabläufen.

Anlage 18: **Entschließung der 72. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 26./27.10.2006 Das Gewicht der Freiheit beim Kampf gegen den Terrorismus**

Seit dem 11. September 2001 wandelt sich der Staat immer mehr zu einem Präventionsstaat, der sich nicht darauf beschränkt, Straftaten zu verfolgen und konkrete Gefahren abzuwehren. Der Staat verlagert seine Aktivitäten zunehmend in das Vorfeld der Gefahrenabwehr. Sicherheitsbehörden gehen der abstrakten Möglichkeit von noch nicht einmal geplanten Taten nach. Immer mehr Daten werden auf Vorrat gesammelt und damit eine Vielzahl unverdächtiger Menschen erfasst. Auch unbescholtene Bürgerinnen und Bürger werden als Risikofaktoren behandelt, ohne dass diese dafür Anlass gegeben haben. Dieses neue Verständnis von innerer Sicherheit führt zu gravierenden Einschränkungen der Freiheitsrechte. Beispiele sind die von der Europäischen Union beschlossene

Speicherung der Telekommunikationsverkehrsdaten oder die im Jahr 2002 verfassungswidrig durchgeführten Rasterfahndungen.

In diesem Zusammenhang ist auch der "Entwurf eines Gesetzes zur Ergänzung des Terrorismusbekämpfungsgesetzes" kritisch zu bewerten. Die ursprünglich zur Terrorismusbekämpfung geschaffenen Befugnisse werden immer weiter ausgedehnt und nicht mehr nur auf Terrorverdächtige beschränkt.

Bei allen Gesetzen und Maßnahmen zur Terrorbekämpfung stellt sich die Frage nach deren Eignung und Verhältnismäßigkeit. Mehr Überwachung führt nicht automatisch zu mehr Sicherheit, aber stets zu weniger Freiheit. Es gibt keine absolute Sicherheit.

Die verfassungsrechtlich notwendige wissenschaftliche Evaluation der bisherigen Vorschriften zur Terrorismusbekämpfung durch eine unabhängige Stelle fehlt bislang. Der „Bericht der Bundesregierung zu den Auswirkungen des Terrorismusbekämpfungsgesetzes" ist keine vollwertige Evaluation der bisherigen Vorschriften. Damit steht sowohl die Notwendigkeit einer Verlängerung als auch die Erforderlichkeit der Schaffung neuer Befugnisse in Zweifel.

Zunehmende Befugnisse verlangen nach zusätzlichen Kontrollen. Daher ist es unerlässlich, einen angemessenen Ausgleich zwischen den Befugnissen der Sicherheitsbehörden und den Kompetenzen der Kontrollorgane zu schaffen. Insbesondere müssen die Handlungsmöglichkeiten der parlamentarischen Kontrollorgane entsprechend ausgestaltet sein.

Anlage 19: **Entschließung der 72. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 26./27.10.2006 Verfassungsrechtliche Grundsätze bei Antiterrordatei-Gesetz beachten**

Mit dem Entwurf eines Gesetzes zur Errichtung gemeinsamer Dateien von Polizeibehörden und Nachrichtendiensten des Bundes und der Länder (Gemeinsame-Dateien-Gesetz-BT-Drs. 16/2950) - verschärft durch Forderungen aus dem Bundesrat - sollen in der Bundesrepublik Deutschland erstmals die rechtlichen Grundlagen für die Errichtung gemeinsamer Dateien von Polizeibehörden und Nachrichtendiensten geschaffen werden. Von besonderer Bedeutung ist die beim Bundeskriminalamt zur Aufklärung und Bekämpfung des internationalen Terrorismus einzurichtende Antiterrordatei, in welcher umfangreiches Datenmaterial der beteiligten Sicherheitsbehörden zusammengeführt werden soll.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder verkennt nicht die zur Begründung des Gesetzentwurfs geltend gemachte hohe Bedrohung durch den internationalen Terrorismus und die Notwendigkeit zur Optimierung des Informationsaustauschs. Jede Intensivierung der informationellen Zusammenarbeit zwischen Polizeibehörden und Nachrichtendiensten muss jedoch den verfassungsrechtlichen Vorgaben, insbesondere dem Recht auf informationelle Selbstbestimmung, dem Grundsatz der Verhältnismäßigkeit und dem - in einigen Landesverfassungen ausdrücklich genannten - Trennungsgebot zwischen Polizei und Nachrichtendiensten entsprechen. Der vorliegende Entwurf zur Antiterrordatei enthält schwerwiegende verfassungs- und datenschutzrechtliche Risiken.

Insbesondere den folgenden brisanten Aspekten wird im Rahmen der anstehenden parlamentarischen Beratungen besondere Beachtung zu schenken sein:

- Die Anti-Terror-Datei sieht gravierende Erweiterungen des Datenaustauschs vor. Deshalb ist zumindest eine weitergehende Präzisierung der zu erfassenden Personen erforderlich. Insoweit ist insbesondere zu berücksichtigen, dass die Nachrichtendienste in der Antiterrordatei auch Personen erfassen, bei denen nur auf weichen Informationen beruhende tatsächliche Anhaltspunkte für eine Zuordnung zum internationalen Terrorismus bestehen. Diese Anhaltspunkte können auf legalem Verhalten beruhen, mit der Folge, dass auch unbescholtene Personen in der Antiterrordatei erfasst werden und deren Daten allen zugriffsberechtigten Behörden zur Verfügung stehen. Dass im Bereich der Vorfeldermittlungen ein besonders hohes Risiko einer Fehlprognose besteht, ist auch bereits verfassungsgerichtlich festgestellt.

- Die Definition der in der Datei zu erfassenden sog. Kontaktpersonen muss präzisiert werden und der Kreis der Betroffenen ist einzuschränken. Dies gilt insbesondere für solche Kontaktpersonen, gegen die keinerlei belastende Erkenntnisse vorliegen. Es muss sichergestellt werden, dass nicht bereits unverdächtige soziale Kontakte zu einer Erfassung von Personen aus dem Umfeld Verdächtigter führen.

- Die Aufnahme besonderer Bemerkungen, ergänzender Hinweise und Bewertungen in Freitextform eröffnet den am Verbund teilnehmenden Behörden die Möglichkeit, eine Vielzahl, auch weicher personenbezogener Informationen (z.B. nicht überprüfte Hinweise oder Vermutungen) ohne Bindung an hinreichend konkrete Festlegungen des Gesetzge-

bers in der Datei zu erfassen. Deshalb sollte darauf verzichtet werden.

– In diesem Zusammenhang ist auch der Zugriff von Polizeibehörden auf Vorfelderkenntnisse der Nachrichtendienste im Hinblick auf das Trennungsgebot kritisch zu hinterfragen. Besonders bedenklich erscheint dabei die Zulassung von Ausnahmen vom verfassungsrechtlichen Trennungsgebot in den sog. Eilfällen, in welchen den beteiligten Behörden ein unmittelbarer Online-Zugriff auf alle Daten gestattet wird.

– Die zugriffsberechtigten Sicherheitsbehörden sind nicht klar genug bezeichnet. Aufgrund der Speicherung auch höchst sensibler personenbezogener Vorfelddaten muss der Gesetzgeber aus rechtsstaatlichen Gründen selbst festlegen, welche Stellen zugriffsberechtigt sein sollen.

– Im Übrigen sind auch die bereits jetzt erkennbaren Tendenzen zu einer Erweiterung der Antiterrordatei über die Terrorismusbekämpfung hinaus nicht akzeptabel. Dies gilt insbesondere für die im Gesetzentwurf vorgesehene Nutzung der Datei im Rahmen der Strafverfolgung. Es darf nicht zu einer immer niedrigeren Eingriffsschwelle kommen.

Anlage 20: **Entschließung der 72. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 26./27.10.2006 Verbindliche Regelungen für den Einsatz von RFID-Technologien**

Der Einsatz von RFID-Tags (Radio Frequency Identification) hält unaufhaltsam Einzug in den Alltag. Schon jetzt werden sowohl im öffentlichen als auch im privatwirtschaftlichen Bereich viele Gegenstände mit diesen miniaturisierten IT-Systemen gekennzeichnet. Es ist zu erwarten, dass neben bereits jetzt mit RFID-Technik gekennzeichneten Lebensmitteln künftig auch Personalausweise, Geldscheine, Kleidungsstücke und Medikamentenpackungen mit RFID-Tags versehen werden. In wenigen Jahren könnten somit praktisch alle Gegenstände des täglichen Lebens weltweit eindeutig gekennzeichnet sein.

Die flächendeckende Einführung derart gekennzeichneter Gegenstände birgt erhebliche Risiken für das Recht auf informationelle Selbstbestimmung in sich. Die RFID-Kennungen verschiedenster Gegenstände können sowohl miteinander als auch mit weiteren personenbezogenen Daten der Nutzenden - in der Regel ohne deren Wissen und Wollen - zusammengeführt werden. Auf diese Weise werden detaillierte Verhaltens-, Nutzungs- und Bewegungsprofile von Betroffenen ermöglicht.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder erwartet von allen Stellen, in deren Verantwortungsbereich RFID-Tags verwendet werden, insbesondere von Herstellern und Anwendern im Handels- und Dienstleistungssektor, alle Möglichkeiten der datenschutzgerechten Gestaltung dieser Technologie zu entwickeln und zu nutzen, und vor allem die Prinzipien der Datensparsamkeit, Zweckbindung, Vertraulichkeit und Transparenz zu gewährleisten. Der schnellen Umsetzung dieser Forderungen kann auch eine verbindliche Selbstverpflichtung von Herstellern und Anwendern der RFID-Technologie im Handels- und Dienstleistungssektor dienen.

Das Bundesverfassungsgericht hat den Gesetzgeber mehrfach darauf hingewiesen, dass wegen des schnellen und für den Grundrechtsschutz riskanten informationstechnischen Wandels die technischen Entwicklungen aufmerksam zu beobachten sind und notfalls durch ergänzende Rechtsetzung korrigierend einzugreifen ist. Daher sind die besonderen Gegebenheiten, die mit dem Einsatz der RFID-Technologie verbunden sind, vom Gesetzgeber daraufhin zu untersuchen, ob für alle Risiken adäquate und rechtliche Schutzmechanismen vorhanden sind. In den Bereichen, in denen diese fehlen, hat der Gesetzgeber einzugreifen. Dies gilt insbesondere für den Fall, dass die Hersteller und Anwender sich auf eine verbindliche Selbstverpflichtung nicht einlassen.

Für den Schutz der Persönlichkeitsrechte Betroffener sind generell folgende Forderungen zu berücksichtigen:

– Transparenz

  Alle Betroffenen müssen umfassend über den Einsatz, Verwendungszweck und Inhalt von RFID-Tags informiert werden.

– Kennzeichnungspflicht

  Nicht nur die eingesetzten RFID-Tags selbst, sondern auch die Kommunikationsvorgänge, die durch die Chips ausgelöst werden, müssen für die Betroffenen leicht zu erkennen sein. Eine heimliche Anwendung darf es nicht geben.

– Keine heimliche Profilbildung

  Daten von RFID-Tags aus verschiedenen Produkten dürfen nur so verarbeitet werden, dass personenbezogene Verhaltens-, Nutzungs- und

Bewegungsprofile ausschließlich mit Wissen und Zustimmung der Betroffenen erstellt werden können. Soweit eine eindeutige Identifizierung einzelner Gegenstände für einen bestimmten Anwendungszweck nicht erforderlich ist, muss auf eine Speicherung eindeutig identifizierender Merkmale auf den RFID-Tags verzichtet werden.

– Vermeidung der unbefugten Kenntnisnahme

  Das unbefugte Auslesen der gespeicherten Daten muss beispielsweise durch Verschlüsselung bei ihrer Speicherung und Übertragung unterbunden werden.

– Deaktivierung

  Es muss vor allem im Handels- und Dienstleistungssektor die Möglichkeit bestehen, RFID-Tags dauerhaft zu deaktivieren, bzw. die darauf enthaltenen Daten zu löschen, insbesondere dann, wenn Daten für die Zwecke nicht mehr erforderlich sind, für die sie auf dem RFID-Tag gespeichert wurden.

Anlage 21: Entschließung der 72. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 26./27.10.2006 Keine Schülerstatistik ohne Datenschutz

Seit einigen Jahren arbeitet die Kultusministerkonferenz an der Einführung eines bundesweit einheitlichen Schulstatistiksystems, in dem weit über das bisherige Maß hinaus Daten aus dem Schulbereich personenbezogen verarbeitet werden sollen. Es soll auf Landesebene in einer Datei für jede Schülerin und jeden Schüler sowie für jede Lehrerin und jeden Lehrer für das gesamte "Schulleben" ein umfangreicher Datensatz angelegt werden. Hierzu erhält jede Person eine Identifikationsnummer, was auf ein pseudonymisiertes Register hinausläuft. Die Länderdateien sollen überdies zu einer bundesweiten Datenbank zusammengefasst werden. Die spätere Ergänzung des Schülerdatensatzes mit so genannten sozialökonomischen Daten über das Elternhaus sowie eine Einbeziehung der Kindergarten- und Hochschulzeit ist beabsichtigt. Eine präzise und einheitliche Zweckbestimmung lässt sich den bisherigen Äußerungen der Kultusministerkonferenz nicht entnehmen.

In datenschutzrechtlicher Hinsicht sind folgende Vorgaben zu beachten:

Wie das Bundesverfassungsgericht festgestellt hat, ist eine Totalerhebung nur zulässig, wenn der gleiche Erfolg nicht mit weniger einschneidenden Maßnahmen erreicht werden kann. Im Hinblick auf die bereits gewonnenen Ergebnisse aus stichprobenartigen und weitgehend auf Freiwilligkeit beruhenden wissenschaftlichen Untersuchungen (wie PISA, IGLU oder TIMSS) erscheint die Notwendigkeit der geplanten Einrichtung eines bundesweiten zentralen schüler- bzw. lehrerbezogenen "Bildungsregisters" nicht dargetan. Ein solches Register wäre ein nicht erforderlicher und damit unverhältnismäßiger Eingriff in das informationelle Selbstbestimmungsrecht.

Deshalb fordern die Datenschutzbeauftragten von der Kultusministerkonferenz bei diesem Vorhaben nachdrücklich den Verzicht auf eine ID-Nummer. Jede Möglichkeit einer Reidentifizierung von Individualdatensätzen ist durch geeignete Verfahren auszuschließen (kein schüler- oder lehrerbeziehbares Bildungsregister!).

Im Übrigen sind folgende verfassungsrechtliche Vorgaben und Grenzen unabdingbar:

– Der Umfang des Erhebungsprogramms ist auf den für die Statistikzwecke dienlichen Umfang zu beschränken.

– Bei allen Festlegungen sind die Grundsätze der Erforderlichkeit und Verhältnismäßigkeit zu beachten.

– Bei der Datenverarbeitung ist das Gebot der personellen, organisatorischen, räumlichen und verfahrensmäßigen Trennung von Verwaltungsvollzug und Statistik einzuhalten und das Statistikgeheimnis zu gewährleisten.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder begrüßt, dass Schulministerien in mehreren Ländern das bisherige, datenschutzrechtlich bedenkliche Konzept nicht mehr weiter verfolgen, und strebt dies auch als Gesamtergebnis der mit der Kultusministerkonferenz zu führenden Gespräche und des angekündigten Workshops an.

Abkürzungsverzeichnis

a.a.O. ..... am angegebenen Ort
Abs. ..... Absatz
ADV ..... Automatisierte Datenverarbeitung
AES ..... Advanced Encryption Standard
AGO ..... Allgemeine Geschäftsordnung für die Behörden des Freistaates Bayern
AKDB ..... Anstalt für Kommunale Datenverarbeitung in Bayern
AKE-AD ..... Arbeitsdatei automatisierte Kennzeichenerkennung
AllMBl ..... Allgemeines Ministerialamtsblatt
AO ..... Abgabenordnung
AOK ..... Allgemeine Ortskrankenkasse
Art. ..... Artikel
ASD ..... Amtliche Schuldaten
ATDG ..... Antiterrordateigesetz
Az. ..... Aktenzeichen
BAN ..... Bundeseinheitliche Ärztenummer
BayBG ..... Bayerisches Beamtengesetz
BayDG ..... Bayerisches Disziplinargesetz
BayDO ..... Bayerische Disziplinarordnung
BayDSG ..... Bayerisches Datenschutzgesetz
BayEUG ..... Bayerisches Gesetz über das Erziehungs- und Unterrichtswesen
BayHO ..... Bayerische Haushaltsordnung
BayHSchG ..... Bayerisches Hochschulgesetz
BayITB ..... Basiskomponenten
BayITR ..... Bayerische IT-Richtlinie
BayIuKS ..... IuK-Strategie für die Bayerische Staatsverwaltung
BayKOM ..... Bayerisches Kommunikationsnetz
BayKrG ..... Bayerisches Krankenhausgesetz
BayMeldeDÜV .... Verordnung zur Durchführung von regelmäßigen Datenübermittlungen der Meldebehörden; Bayerische Meldedaten-Übermittlungsverordnung
BayPVG ..... Bayerisches Personalvertretungsgesetz
BayUIG ..... Bayerisches Umweltinformationsgesetz
BayVBl ..... Bayerische Verwaltungsblätter
BayVGH ..... Bayerischer Verwaltungsgerichtshof
BayVSG ..... Bayerisches Verfassungsschutzgesetz
BayVwVfG ..... Bayerisches Verwaltungsverfahrensgesetz
Bcc ..... Blind-Copy-Funktion / blind carbon copy
BDSG ..... Bundesdatenschutzgesetz
BFH ..... Bundesfinanzhof
BGB ..... Bürgerliches Gesetzbuch
BGBl ..... Bundesgesetzblatt
BGH ..... Bundesgerichtshof
BrV ..... Ballungsraumverfahren
BSHG ..... Bundessozialhilfegesetz
BSI ..... Bundesamt für Sicherheit in der Informationstechnik
BStatG ..... Gesetz über die Statistik für Bundeszwecke (Bundesstatistikgesetz)
BT-Drs. ..... Bundestagsdrucksache
BTI ..... Bayerische Telematikinitiative für das Gesundheitswesen
BV ..... Bayerische Verfassung
BVerfG ..... Bundesverfassungsgericht
BVerfGE ..... Entscheidungen des Bundesverfassungsgerichts (zitiert nach Band und Seite)
BVerfSchG ..... Bundesverfassungsschutzgesetz
BWG ..... Bundeswahlgesetz
bzw. ..... beziehungsweise
CD ..... Compact Disc
CEUS ^{HB} ..... Computerbasiertes EntscheidungsUnterstützungsSystem für die Hochschulen in Bayern
CSU ..... Christlich Soziale Union
d.h. ..... das heißt
DM ..... Deutsche Mark
DMS ..... Dokumentenmanagementsystem
DNA-Analyse ..... Molekulargenetische Untersuchung
DSB ..... Datenschutzbeauftragter
EA ..... Errichtungsanordnung für Dateien
EAP ..... Extensible Authentication Protocol
EFG ..... Sammlung der Entscheidungen der Finanzgerichte
EFN ..... Elektronische Fortbildungsnummer
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
EG-PassVO ..... Verordnung (EG) Nr. 2252/2004 des Rates vom 13. Dezember 2004 über Normen für Sicherheitsmerkmale und biometrische Daten in von den Mitgliedstaaten ausgestellten Pässen und Reisedokumenten
EIV ..... Elektronischer Informationsverteiler

ELDORA ..... Elektronische Dokumentenverarbeitung mit Recherche und Aktenverwaltung
ELENA..... Elektronischer Einkommensnachweis
ELSTER..... Elektronische Steuererklärung
ESPED ..... Erfassungssystem seltener pädiatrischer Erkrankungen in Deutschland
EStG..... Einkommensteuergesetz
etc. ..... et cetera
EU ..... Europäische Union
EuGH ..... Europäischer Gerichtshof
FAD..... Finanzadressen
ff. ..... folgende
FMBl ..... Amtsblatt des Bayerischen Staatsministeriums der Finanzen
GAST-Dateien ..... Dateien zur Gefahrenabwehr und Verfolgung von Straftaten
GDVG ..... Gesundheitsdienst- und Verbraucherschutzgesetz
gem. ..... gemäß
GEWAN..... Gewerbeanzeigen im Netz
GEZ..... Gebühreneinzugszentrale der öffentlich-rechtlichen Rundfunkanstalten Deutschlands
GG..... Grundgesetz
ggf. ..... gegebenenfalls
GLKrWG ..... Gemeinde- und Landkreiswahlgesetz
GmbH..... Gesellschaft mit beschränkter Haftung
GO..... Gemeindeordnung
GVBl ..... Gesetz- und Verordnungsblatt
Gz. ..... Geschäftszeichen
HandwO ..... Gesetz zur Ordnung des Handwerks; Handwerksordnung
HStatG..... Hochschulstatistikgesetz
HTTPS ..... Hyper Text Transfer Protocol Secure
i.d.F. ..... in der Fassung vom
i.d.R. ..... in der Regel
i.S.d. ..... im Sinne des
i.V.m. ..... in Verbindung mit
IEEE..... Institute of Electrical and Electronics Engineers
IfSG..... Infektionsschutzgesetz
IGVP ..... Integrationsverfahren Polizei
INPOL..... Informationssystem der Polizei (bundesweit)
IP ..... Internet Protocol
IPSEC..... IP Security
ISDN ..... Integrated Services Digital Network
ISIS ..... bayerische Staatsschutzdatei
IuK ..... Informations- und Kommunikationstechnik
IuK-KoordR ..... Richtlinie für den koordinierten Einsatz der Informations- und Kommunikationstechnik (IuK) in der Bayerischen Staatsverwaltung
IuKSR..... Standards und Richtlinien für die Informations- und Kommunikationstechnik (IuK) in der Bayerischen Verwaltung
IuK-Systeme..... Informations- und Kommunikationssysteme
JGG ..... Jugendgerichtsgesetz
JVA ..... Justizvollzugsanstalt
KAG ..... Kommunalabgabengesetz
KAN ..... Kriminalaktennachweis
KG ..... Kostengesetz
KIBBS ..... Kriseninterventions- und -bewältigungsteam bayerischer Schulpsychologen
KirchStG ..... Kirchensteuergesetz
KIS ..... Krankenhausinformationssystem
KMS ..... Schreiben des Bayerischen Staatsministeriums für Unterricht und Kultus
KraftStG ..... Kraftfahrzeugsteuergesetz
KVB ..... Kassenärztliche Vereinigung Bayerns
KVR ..... Kreisverwaltungsreferat
KWMBl..... Kultus- und Wissenschaftsministerialblatt
LfD ..... Landesbeauftragter für Datenschutz
lit. ..... Buchstabe
LVA..... Landesversicherungsanstalt
LWG..... Landeswahlgesetz
m.E. ..... meines Erachtens
MdL..... Mitglied des Landtages
MeldeG..... Bayerisches Gesetz über das Meldewesen
MHz..... Megahertz
NJW..... Neue Juristische Wochenschrift
NPD..... National-Sozialistische Partei Deutschlands
Nr. ..... Nummer
NVwZ..... Neue Zeitschrift für Verwaltungsrecht
o.g. ..... oben genannt
ODSP..... Online-Datenschutz-Prinzipien
OK.FIS ..... Finanzinformationssystem
PAG..... Bayerisches Polizeiaufgabengesetz
PaßG..... Passgesetz
PAuswG ..... Gesetz über Personalausweise
PC..... Personalcomputer
PFAD..... Personen- und Fall-Auskunftsdatei
PGP ..... Pretty Good Privacy
PIN ..... Personell Identification Number
PKI ..... Public Key Infrastructure

PSV ..... Polizeiliche Sachbearbeitung/Vorgangsverwaltung-Verbrechensbekämpfung
RADIUS..... Remote Authentication Dial-In User Service
Rdnr..... Randnummer
RFID ..... Radio Frequency Identification
RGIS ..... Rauschgiftinformationssystem
S. ..... Seite
SGB..... Sozialgesetzbuch
SIKO ..... Sicherheitskonferenz
sog. ..... sogenannt
SPD ..... Sozialdemokratische Partei Deutschlands
Spit ..... Spam over Internet Telephony
SRTP ..... Secure Real-time Transport Protocol
SSL..... Secure Sockets Layer
StGB..... Strafgesetzbuch
StMWIVT ..... Staatsministerium für Wirtschaft, Infrastruktur, Verkehr und Technologie
StPO ..... Strafprozessordnung
StVG ..... Straßenverkehrsgesetz
StVollzG..... Strafvollzugsgesetz
StVZO ..... Straßenverkehrs-Zulassungs-Ordnung
TAN ..... Transaktionsnummer
TK ..... Telekommunikation
TKG..... Telekommunikationsgesetz
TKÜ..... Telekommunikationsüberwachung
TTLS ..... Tunneled Transport Layer Security
u.a. ..... unter anderem
u.U. ..... unter Umständen
UrhG..... Urheberrechtsgesetz
URL..... Uniform Resource Locator
UStG..... Umsatzsteuergesetz
VermKatG ..... Vermessungs- und Katastergesetz
VersammlG ..... Versammlungsgesetz
VGH ..... Verwaltungsgerichtshof
vgl. ..... Vergleiche
VoIP ..... Voice over IP
VPN..... Virtual Private Network / Virtuelles Privates Netz
VV ..... Verwaltungsvorschriften
WEP ..... Wired Equivalent Privacy
WLAN..... Wireless Local Area Network
WPA..... Wi-Fi Protected Access
z.B. ..... zum Beispiel
z.T. ..... zum Teil
ZES..... Zeitmanagementsystem
ZIL ..... Zentrale IuK-Leitstelle
ZSS..... Zentrale Speicherstelle
ZustVVerk..... Verordnung über Zuständigkeiten im Verkehrswesen
ZVD..... Zentrale Vollzugsdatei

Stichwortverzeichnis