Bayerischer Landtag
12. Wahlperiode

Drucksache **12/9430**

10. 12. 92

Vierzehnter Tätigkeitsbericht des Landesbeauftragten für den Datenschutz

Berichtszeitraum 1992

Der Landesbeauftragte für den Datenschutz
Nr. DSB/1 – 510 – 15

München, 10. Dezember 1992

An den
Präsidenten
des Bayerischen Landtags
Herrn Dr. Wilhelm Vorndran
München

Vierzehnter Bericht über die Tätigkeit des Landesbeauftragten für den Datenschutz

Sehr geehrter Herr Landtagspräsident!

In der Anlage übersende ich gem. Art. 28 Abs. 4 des Bayerischen Datenschutzgesetzes den vierzehnten Bericht über die Tätigkeit des Landesbeauftragten für den Datenschutz.

Mit vorzüglicher Hochachtung

Sebastian Oberhauser

Inhaltsübersicht

1. Vorbemerkungen

1.1 Kontrolltätigkeit

Wie in den vergangenen Jahren lag auch im Berichtszeitraum ein Schwerpunkt meiner Tätigkeit bei der **Überprüfung bayerischer Behörden**. Datenschutzkontrollen habe ich durchgeführt bei vier Allgemeinen Ortskrankenkassen, einer Betriebskrankenkasse, einem Finanzamt, dem Landeskriminalamt, zwei Polizeipräsidien, zwei Polizeidirektionen, dem Landesamt für Verfassungsschutz, einem Amtsgericht, einer Staatsanwaltschaft, einer Justizvollzugsanstalt, einem Gerichtsvollzieher, einem Landratsamt, drei Städten, einer Verwaltungsgemeinschaft, einer Gemeinde, einer Universität, zwei Schulämtern und einer Umweltbehörde.

Ergänzt wurden die allgemeinen Kontrollen durch zahlreiche **Überprüfungen von Behörden aufgrund von Eingaben, Beschwerden und Presseberichten**. Besonders bedanken möchte ich mich für die Mitarbeit der Bürger, die mich in ihren Eingaben auf Mängel im Datenschutz hinweisen und mir so die Möglichkeit verschaffen, gezielt gegen diese Mängel mit entsprechender Breitenwirkung vorzugehen.

Hinzu kamen **technisch-organisatorische Kontrollen** bei zwanzig öffentlichen Stellen und Rechenzentren sowie Kontrollen der ordnungsgemäßen Entsorgung von Datenträgern bei sechzehn Behörden.

1.2 Datenschutz in Bayern gewährleistet

Auf der Grundlage der durchgeführten Kontrollen und zahlreicher sonstiger Kontakte mit Behörden kann ich auch für das Berichtsjahr 1992 feststellen, daß der Datenschutz in Bayern **grundsätzlich gewährleistet** ist. In einzelnen Bereichen sind freilich noch einige Verbesserungen notwendig, wünschenswert und möglich.

1.3 Inhalt und Schwerpunkte des 14. Tätigkeitsberichts

Den Schwerpunkt bilden die Ergebnisse der durchgeführten **Datenschutzkontrollen**, die dabei gewonnenen **Erfahrungen** und die daraus gezogenen **Konsequenzen**. Zahlreiche **Zweifelsfragen** von Bürgern und Behörden bei der Auslegung und Anwendung des Datenschutzrechts waren wieder zu klären. Soweit die Stellungnahmen von allgemeinem Interesse sind, habe ich sie im Bericht wiedergegeben. Zu einer Reihe von **Gesetzgebungsvorhaben, Richtlinien** und **Dienstanweisungen**, die den Datenschutz betreffen, habe ich Stellung genommen.

- Im Vordergrund standen meine Bemühungen um einen **angemessenen Datenschutz im Sicherheitsbereich**. Allgemeine Querschnittskontrollen ergaben in den meisten Fällen ein **hohes Datenschutzbewußtsein** bei Polizei und Verfassungsschutz und einen **hohen Datenschutzstandard** beim Umgang mit personenbezogenen Daten.

  Bei der **Entrümpelung der Datei Kriminalaktennachweis** konnten Fortschritte erzielt werden: Straftaten von geringerer Bedeutung wie etwa Privatklagedelikte werden künftig in größerem Umfang als bisher nur mehr für einen kürzeren Zeitraum (5 Jahre) gespeichert. Allerdings sollten eine Reihe wenig bedeutungsvoller Verdachtsfälle, z.B. Nachbarquerelen, in denen es nach gegenseitigen Beschuldigungen zu keinen Verurteilungen kommt, überhaupt nicht im Kriminalaktennachweis gespeichert werden. Hier werde ich meine Bemühungen um eine Entrümpelung der Datei fortsetzen. Als besonderer Erfolg des Datenschutzes konnte ferner verbucht werden, daß die Staatsanwaltschaft die Polizei künftig darüber **informiert**, wenn sie einen von der Polizei **Beschuldigten für unschuldig** hält, so daß die kriminalpolizeilichen Unterlagen bereinigt werden können.

  Einen Schwerpunkt meiner Arbeit bildete die Datei **Polizeiliche Sachbearbeitung/Vorgangsverwaltung-Verbrechensbekämpfung (PSV)**, welche die Grundlage des polizeilichen Informationssystems in Bayern bilden wird. Wegen der relativ hohen Mißbrauchsgefahr – in manchen Polizeipräsidien können sich bis zu 5.000 Polizisten der Datei bedienen – ist eine **Protokollierung der Abfragen** unverzichtbar. Auch der Grundsatz, daß ein Verdächtiger nach einer gewissen Zeit gegenüber der Polizei als **unbeschriebenes Blatt** zu gelten hat, muß in der neuen Datei noch effektiver umgesetzt werden.

  Die Forderung nach Abschaffung oder weiterer Einschränkung der **Staatsschutzdatei APIS** ist angesichts der Anschläge rechtsextremistischer Straftäter, die in APIS gespeichert werden, erfreulicherweise verstummt. Die **verlängerte Speicherung sog. Kontaktpersonen** zu Figuren des terroristischen Umfelds ist wegen der konspirativen Vorgehensweise in dieser Szene angemessen.

  Die Dateien **Straftaten bei Sportveranstaltungen und gewalttätigen Jugendgruppen** sowie **Münchner Weltwirtschaftsgipfel 1992**, die beim Polizeipräsidium München geführt werden, befinden sich, wie Querschnittsprüfungen ergaben, auf erfreulich hohem Datenschutzniveau.

- Im **Justizbereich** bemühe ich mich um eine stärkere **Berücksichtigung der Persönlichkeitsrechte beim Briefverkehr der Strafgefangenen in den Haftanstalten**. Von der Kontrolle in der Anstalt sollten Briefe an Behörden, bei denen eine Gefähr-

dung der Sicherheit der Anstalt ausgeschlossen werden kann, wie beispielsweise an den Bundespräsidenten oder den Datenschutzbeauftragten, ausgenommen werden. Von der Anbringung eines Kontrollvermerks (Sichtvermerks) auf den auslaufenden Briefen sollte grundsätzlich Abstand genommen werden. Auf Wunsch sollte der Häftling statt der Adresse der Haftanstalt die Heimatadresse angeben dürfen, wenn keine Anzeichen für eine Gefährdung der Sicherheit oder Ordnung der Anstalt oder der Aufgaben des Strafvollzugs erkennbar sind.

Ausforschungsanzeigen dürfen nicht zum Ziel führen. Werden Strafverfahren eingestellt, die von nicht in ihren Rechten verletzten Anzeigeerstattern ausgelöst worden sind, so sollte in den Mitteilungen der Staatsanwaltschaft an die Anzeigeerstatter auf das Persönlichkeitsrecht des Opfers der angeblichen Straftat wesentlich stärker als bisher Rücksicht genommen werden. Insbesondere dürften Dritten keine Angaben über die Art der Verletzungen des Opfers mitgeteilt werden.

- In gemeindlichen **Adreßbüchern** waren die Namen und Adressen von Bürgern, die in Krankenhäusern, Pflegeheimen oder sonstigen Einrichtungen der Betreuung pflegebedürftiger oder behinderter Menschen, der Rehabilitation oder der Heimerziehung aufgenommen sind, unter der Adresse der Einrichtung abgedruckt. Ich habe daraufhin eine **Durchforstung aller gemeindlichen Adreßbücher** nach unzulässigen Adreßangaben veranlaßt.

- Der Ausbau der in Bayern vorhandenen **klinischen Krebsregister** zu einem **landesweiten auch epidemiologisch nutzbaren System** wird vom Landesbeauftragten für den Datenschutz unterstützt. Bei diesem System bleiben die besonderen Vorteile des klinischen Krebsregisters erhalten, da **alle identifizierenden Patientendaten im Verantwortungsbereich der behandelnden Ärzte und Krankenhäuser** verbleiben und dort den Schutz der ärztlichen Schweigepflicht genießen, sowie alle Daten **gleichzeitig auch zur Behandlung** der Patienten zur Verfügung stehen.

1.4 Neufassung des Bayer. Datenschutzgesetzes

Das Bayerische Datenschutzgesetz wird an die Rechtssprechung des Bundesverfassungsgerichts und an die Erfahrungen der Praxis angepaßt. Nach dem Regierungsentwurf sind folgende Verbesserungen vorgesehen:

- Der Schutzbereich des Gesetzes wird auf die Verarbeitung und Nutzung personenbezogener Daten in **Akten** ausgedehnt. Bisher galt das Gesetz nur für die elektronische Datenverarbeitung und für manuelle Karteien. Für die Betroffenen ist damit insbesondere eine Ausweitung seiner Rechte auf Auskunft, Sperrung und Löschung verbunden.

- Werden Daten benötigt, müssen die öffentlichen Stellen grundsätzlich beim betroffenen Bürger selbst nachfragen. Die **Erhebung** von Daten bei anderen Behörden soll nur aus den im Gesetz näher umschriebenen Gründen möglich sein.

- Daten sollen künftig grundsätzlich nur für den **Zweck** verarbeitet und genutzt werden, für den sie erhoben worden sind. Ausnahmen von diesem Grundsatz sind nur in den gesetzlich bestimmten Fällen zulässig, wenn das Funktionieren der Verwaltung dies zwingend erfordert.

- Die Zulässigkeit **automatisierter Abrufverfahren** wird gesetzlich geregelt.

- Die Verpflichtung öffentlicher Stellen, Bürgern über gespeicherte Daten **Auskunft** zu erteilen, wird erweitert. Auskünfte sollen grundsätzlich kostenfrei erteilt werden.

- Die **Kontrollkompetenz** des Landesbeauftragten für den Datenschutz wird auf **Akten** ausgedehnt, soweit ein **Kontrollanlaß** vorliegt.

- Die schon bisher bestehende **Unabhängigkeit des Landesbeauftragten für den Datenschutz** wird rechtlich zusätzlich abgesichert. Künftig soll der Landesbeauftragte mit Zustimmung des Landtags für einen Zeitraum von **acht Jahren** berufen werden und während seiner Amtszeit nur unter den Voraussetzungen abberufen werden können, die für die Amtsenthebung von Richtern auf Lebenszeit gelten. Ferner wird klargestellt, daß sich der Landesbeauftragte jederzeit an den Landtag und den Senat wenden kann.

- Es wird klargestellt, daß der Landesbeauftragte für den Datenschutz von der Staatskanzlei und den Staatsministerien über **Planungen bedeutender Automationsvorhaben** zu informieren ist, sofern damit personenbezogene Daten verarbeitet werden.

Damit werden die wesentlichen Forderungen des Landesbeauftragten verwirklicht.

1.5 Datenschutz – Innere Sicherheit – Organisierte Kriminalität – extremistische Gewalttaten

Der **Verfall der inneren Sicherheit** in der Bundesrepublik gibt Anlaß zu ernster Sorge. Nach der polizeilichen Kriminalstatistik ist im Jahr 1991 die Kriminalität in den alten Bundesländern um 3,6 % gestiegen. Rauschgiftdelikte haben um 12,0 %, Taschen-

diebstahl und Straßenraub sogar um 30,4 % zugenommen. Im ersten Halbjahr 1992 betrug der Anstieg 9,8 %. Noch gravierender ist die **Zunahme der organisierten Kriminalität**, insbesondere der organisierten Rauschgiftkriminalität, der Kraftfahrzeugverschiebung, der Schutzgelderpressung und des organisierten Diebstahls. Rechtsextremistische Straftaten, insbesondere die „Gewalt der Straße" haben 1992 ein besorgniserregendes Ausmaß angenommen. Der Rechtsstaat präsentiert sich den Bürgern in bedenklicher Schwäche. Um das Vertrauen der Bürger in den Rechtsstaat zu erhalten, muß **der Schutz der inneren Sicherheit vorrangiges Ziel** der Rechtspolitik sein, das angemessene Eingriffe in das informationelle Selbstbestimmungsrecht rechtfertigt.

Breiten Raum in der öffentlichen Diskussion nimmt in diesem Zusammenhang das Verhältnis von Datenschutz und polizeilicher Aufgabenerfüllung ein. Mein Angebot im 13. Tätigkeitsbericht zu einer **unvoreingenommenen Bestandsaufnahme** und Überprüfung angeblicher Behinderungen der Polizei durch den Datenschutz gilt fort.

Während von Seiten der für die innere Sicherheit Verantwortlichen eine **Revision datenschutzrechtlicher Beschränkungen** für notwendig gehalten wird, werden auf der anderen Seite **weitere Verschärfungen des Datenschutzes** gefordert oder effiziente Fahndungsmaßnahmen abgelehnt:

- So sprach sich die Mehrheit der Datenschutzbeauftragten – gegen meine Stimme – dagegen aus, daß alle Asylbewerber erkennungsdienstlich behandelt werden und die abgenommenen Fingerabdrucke und Lichtbilder ohne Einschränkungen auch zur Kriminalitätsbekämpfung, z.B. zur Verhinderung des betrügerischen Mehrfachbezuges von Sozialhilfe, verwendet werden.
- Die Mehrheit der Datenschutzbeauftragten lehnte ferner gegen meinen Widerstand den **Einsatz von Abhörgeräten in Wohnungen zur Bekämpfung schwerster Verbrechen der organisierten Kriminalität** als Verstoß gegen die Menschenwürde ab, obwohl dieses moderne Fahndungsmittel in beinahe allen westlichen Staaten mit langer ungebrochener rechtsstaatlicher Tradition als mit der Menschenwürde vereinbar gehalten und gegen das organisierte Verbrechen erfolgreich angewandt wird. Selbstverständlich ist der Einsatz von elektronischen Observierungsmitteln, als „Großer Lauschangriff" diskriminiert, auch ein angemessenes Mittel zur **Aufklärung rechts- oder linksextremistischer Terrorakte**.

1.6 Beitrag zur Vertrauensbildung oder zur Staatsverdrossenheit

Staatsverdrossenheit resultiert aus der Kluft zwischen zu hohen Erwartungen und der Wirklichkeit, in der diese Erwartungen nicht erfüllt werden können. Tiefsitzende Enttäuschung über den Staat kann aber auch entstehen, wenn **mit dem Argument des Verfassungsbruchs** vor Maßnahmen gewarnt wird, die in Wirklichkeit verfassungsgemäß und sogar unumgänglich notwendig sind.

Die Einrichtung der Datenschutzbeauftragten wurde nicht zuletzt auch zu dem Zweck geschaffen, daß eine unabhängige Instanz durch Kontrolle der Datenverarbeitung der Behörden **zur Stärkung des Vertrauens der Bürger in die Rechtmäßigkeit der Informationsverarbeitung des Staates** beiträgt. Kontraproduktiv wirkt die Mehrheit der Datenschutzbeauftragten jedoch, wenn sie in unabdingbar notwendig gewordenen Maßnahmen wie dem Einsatz von Observationsmitteln in Wohnungen gegen Schwerstverbrecher der organisierten Kriminalität einen Anschlag auf die Menschenwürde sieht, während diese moderne Fahndungsmaßnahme in fast allen westlichen Ländern mit langer ungebrochener rechtsstaatlicher Tradition als selbstverständlich mit der Menschenwürde vereinbar angesehen und erfolgreich praktiziert wird. Woran sollen sich da die Bürger noch halten?

1.7 Ablehnung des Vorsitzes in der Datenschutzkonferenz – Unüberbrückbare Meinungsverschiedenheiten

Wegen **schwerwiegender Differenzen über die Grundsätze der Zusammenarbeit** in der „Konferenz der Datenschutzbeauftragten" habe ich es abgelehnt, für 1993 den auf Bayern fallenden Vorsitz in der Konferenz zu übernehmen. Die Mehrheit der Datenschutzbeauftragten hat in der Vergangenheit bei der Meinungsbildung in der Konferenz immer wieder gegen das **Einstimmigkeitsprinzip** verstoßen. Obwohl nur einstimmig gefaßte Beschlüsse zustande kommen können, wurden immer wieder Mehrheitsmeinungen als Konferenzbeschlüsse verkündet. Auf diese Weise will sich eine Mehrheit unter Verstoß gegen das im **kooperativen Föderalismus** geltende Einstimmigkeitsprinzip für ihre weit überzogenen Forderungen im Datenschutz mehr Gewicht und Aufmerksamkeit verschaffen, als ihr zusteht.

Unüberbrückbare Meinungsverschiedenheiten in Sachfragen entstanden in der Vergangenheit insbesondere, wenn bei der Bewertung von Gesetzesvorhaben oder von Maßnahmen der Behörden das Verhältnis von Datenschutz zu innerer Sicherheit berührt war. Einigkeit besteht zwar darin, daß dabei von der Rechtsprechung des Bundesverfassungsgerichts, vor allem von den Grundsätzen des Volkszählungsurteils von 1983, auszugehen ist. Danach sind **Einschränkungen** des Grundrechts auf informationelle Selbstbestimmung im **überwiegenden Allgemeininteresse** unter Beachtung des Grundsatzes der Verhältnis-

mäßigkeit zulässig. Die Mehrheit räumt jedoch der **inneren Sicherheit, der Ordnung**, in der sich der Einzelne entfalten kann, im Verhältnis zur **Freiheit des Individuums** nur einen relativ **geringen Stellenwert** ein, stellt an den Nachweis der Bedrohung der inneren Sicherheit, der Eignung der Schutzmaßnahme sowie an ihre Zumutbarkeit und Verträglichkeit **zu hohe Anforderungen** mit der Folge, daß die Maßnahmen, die von den für die innere Sicherheit Verantwortlichen gefordert werden, **zu Unrecht als verfassungswidrig abqualifiziert und bekämpft werden**. Den Stellenwert der inneren Sicherheit bestimmen aber nicht die Datenschutzbeauftragten, sondern das Parlament im Rahmen der verfassungsmäßigen Ordnung. Wie stark die innere Sicherheit gefährdet und welche Abwehrmaßnahmen erforderlich sind, bestimmt letztlich ebenfalls das Parlament. Die Datenschutzbeauftragten können in der öffentlichen Diskussion allenfalls die weitgesteckten Grenzen des Ermessens des Gesetzgebers aufzeigen, sollten sich aber nicht zum **beckmesserischen Richter über Parlamente und Regierungen** aufspielen. Unabhängigkeit berechtigt die Datenschutzbeauftragten weder zur Fundamental-Opposition noch stellt sie von der Verantwortung gegenüber dem Gemeinwohl frei.

1.8 Datenschutzregelungen im Bayerischen Petitionsgesetz

Die CSU-Fraktion hat im Bayerischen Landtag einen Gesetzentwurf für ein Bayerisches Petitionsgesetz eingebracht. Dessen Art. 6 Abs. 4 sieht den Schutz personenbezogener Daten des Petenten und dritter Personen vor, die im Zuge der sachlichen Behandlung einer Eingabe dem Landtag übermittelt werden. Die Absicht der Initiatoren, bei der Behandlung von Petitionen im Blick auf die erweiterten Kontrollbefugnisse des Parlaments die Persönlichkeitsrechte der Bürger in einer besonderen Bestimmung klarer und eindeutiger als bisher zu schützen, begrüße ich.

Zu dem Gesetzentwurf habe ich dem Vorsitzenden des Petitionsausschusses noch folgende Vorschläge unterbreitet:

1.8.1 Ausschluß der Öffentlichkeit

Der Ausschluß der Öffentlichkeit bei der Behandlung von Eingaben in Fällen, in denen Umstände aus dem persönlichen Lebensbereich zur Sprache kommen, wird gegenwärtig durch § 29 Abs. 1 und 2 der Geschäftsordnung des Bayerischen Landtags geregelt. Danach **ist** die Öffentlichkeit auszuschließen, wenn Rechtsvorschriften die Bekanntgabe von Daten untersagen. Sie **kann** ausgeschlossen werden, wenn Umstände aus dem persönlichen Lebensbereich des Beschwerdeführers oder eines Dritten zur Sprache kommen, durch deren öffentliche Erörterungen **überwiegende schutzwürdige Interessen** verletzt werden. Zuständig für den Ausschluß der Öffentlichkeit ist der Ausschuß.

Ich habe Zweifel, ob diese Regelung über den Ausschluß der Öffentlichkeit bei der Behandlung von Petitionen der Rechtsprechung des Bundesverfassungsgerichts zum Grundrecht auf informationelle Selbstbestimmung ausreichend Rechnung trägt. Außerdem ist zu bedenken, daß als Folge der Neuregelung des Petitionsrechts über die Stellungnahme der Staatsregierung und die Vorlage von Akten künftig **noch mehr und sensiblere** personenbezogene Daten von Bürgern als bisher dem Parlament übermittelt und bei der Beratung zur Sprache kommen werden.

Ich habe daher vorgeschlagen, § 29 Abs. 2 der Geschäftsordnung so zu ändern, daß der Ausschußvorsitzende auf gemeinsamen Vorschlag der Berichterstatter die Öffentlichkeit ausschließt, wenn **besondere** Rechtsvorschriften die Bekanntgabe von Daten untersagen oder Umstände aus dem persönlichen Lebensbereich des Beschwerdeführers oder eines Dritten zur Sprache kommen, durch deren öffentliche Erörterung überwiegende schutzwürdige Interessen verletzt würden. Selbstverständlich geht ein Beschluß des Ausschusses vor.

Mein Vorschlag beruht darauf, daß einerseits bei wörtlicher Auslegung des § 29 der Geschäftsordnung das Grundrecht auf **informationelle Selbstbestimmung** als „Rechtsvorschrift" bei der Behandlung persönlicher Angelegenheiten grundsätzlich zum Ausschluß der Öffentlichkeit führen müßte, dieser Ausschluß andererseits aber nur zwingend vorgeschrieben werden sollte in den Fällen, in denen **besondere** Rechtsvorschriften, wie z.B. Sozialgeheimnis, Steuergeheimnis, ärztliche Schweigepflicht, einen besonderen Schutz vorschreiben. Außerdem ist für eine Ermessensentscheidung über den Ausschluß der Öffentlichkeit dann kein Raum mehr, wenn durch die Bekanntgabe von Umständen aus dem persönlichen Lebensbereich des Beschwerdeführers oder eines Dritten **überwiegende schutzwürdige Interessen** verletzt würden.

Schließlich halte ich es für praktikabler, wenn nicht der gesamte Ausschuß in öffentlicher Sitzung über den Ausschluß der Öffentlichkeit bei einer Eingabe beraten muß, sondern bereits der Ausschußvorsitzende auf gemeinsamen Vorschlag der Berichterstatter die erforderliche Entscheidung treffen kann. Zur Klärung der Frage, ob überwiegende schutzwürdige Interessen der öffentlichen Erörterung entgegenstehen, kann es dienlich sein, wenn der Landtag in der Bestätigung des Eingangs der Eingabe den Petenten darauf aufmerksam macht, daß Eingaben grundsätzlich öffentlich behandelt werden, wenn der Petent dem nicht widerspricht.

1.8.2 Geheimhaltungsbeschluß zugunsten des Petenten

Der Gesetzentwurf sieht einen Beschluß über die Geheimhaltung, der einen strafrechtlichen Schutz der betreffenden Daten zur Folge hat, nur vor, wenn nichtabtrennbare Daten des Petenten oder Dritter in den vorzulegenden Unterlagen enthalten sind oder, wenn Daten von Dritten dem Landtag vorgelegt werden sollen. Es können jedoch auch **schutzwürdige Interessen des Petenten selbst** einen entsprechenden Geheimhaltungsschutz erfordern. Ich habe deshalb vorgeschlagen, den **Geheimhaltungsbeschluß** stets zu fassen, wenn die **Öffentlichkeit ausgeschlossen** wird.

1.8.3 Klarstellung des Schutzumfangs

Ich habe vorgeschlagen, die bisherige Formulierung des Gesetzentwurfs zum Schutz von „Geheimnissen" zu verdeutlichen und festzulegen, daß durch Gesetz besonders geschützte Geheimnisse wie Patienten- und Sozialgeheimnis nur mit Einwilligung des Betroffenen und nach einem Geheimhaltungsbeschluß dem Landtag übermittelt werden.

2. Gesundheitswesen

2.1 Austausch von HIV-Befunden zwischen Gesundheitsämtern

In einer Eingabe wurde mir folgender Fall zur Beurteilung vorgelegt:
Ein Gesundheitsamt übermittelte unaufgefordert von Drogenabhängigen, die sich in Bayern einer Therapie unterzogen hatten, personenbezogene Daten über die Durchführung eines **HIV-Antikörper-Tests** an ein Gesundheitsamt außerhalb Bayerns, in dessen Zuständigkeitsbereich der Drogenabhängige nun wohnhaft sei. Es erscheine fraglich, ob eine Übermittlungsbefugnis bestehe.

Das Staatsministerium des Innern hat hierzu folgende Auffassung vertreten: Das bayerische Gesundheitsamt habe das außerbayerische Amt darüber informiert, daß der Drogenabhängige die Therapie **vorzeitig** beendigt habe. Diese Mitteilung sei erforderlich zur **Abwehr von Gefahren** für **Leben** und **Gesundheit** Dritter im Sinne von Art. 7 Abs. 1 S. 3 i.V.m. Art. 6 Abs. 2 S.2 des Gesetzes über den öffentlichen Gesundheitsdienst (GDG), da es sich bei den Therapieabbrechern um intravenös Drogenabhängige handle. Dieser Personenkreis gelte gemäß § 2 Nr. 3 BSeuchG als HIV-ansteckungsverdächtig und bilde deshalb eine Gefahr für Leben und Gesundheit Dritter.

Das Gesundheitsamt habe nach § 31 Abs. 1 BSeuchG Fälle von HIV-Ansteckungsverdacht aufzuklären. Um den Therapieerfolg nicht zu gefährden, würden intravenös Drogenabhängige während der Therapie nicht zum Gesundheitsamt vorgeladen. Breche jedoch ein Drogenabhängiger die Therapie ab, müsse das Gesundheitsamt seiner gesetzlichen Aufgabe nachkommen und die Abklärung des Ansteckungsverdachts einleiten.

Da die Ermittlungen bei HIV auf ein möglichst frühzeitiges Erkennen einer Infektion gerichtet sein müßten, um mögliche Übertragungen auf Dritte verhindern zu können, sei die Mitteilung notwendig, um zeitraubende Ermittlungen des nunmehr zuständigen Gesundheitsamtes einzusparen. Angesichts des bisher zum Tode führenden Verlaufs einer HIV-Infektion sei daher die Übermittlung der Daten eines Therapieabbrechers an das zuständige Gesundheitsamt **unbedingt erforderlich**, um diesem die für seine Aufgabenerfüllung notwendigen Informationen zur Verfügung zu stellen.

Diese Auffassung entspricht der Rechtslage.

2.2 Fernwartung eines Klinik-DV-Systems

Bereits im 13. Tätigkeitsbericht habe ich auf die Problematik der Fernwartung von Datenverarbeitungsverfahren in Krankenhäusern hingewiesen. Fernwartung kann zur Folge haben, daß sensible Daten **aus dem Schutzbereich des Krankenhauses** heraus an Dritte gelangen. Es stellt sich daher mit Blick auf die ärztliche Schweigepflicht (§ 203 Abs. 1 Strafgesetzbuch – StGB) sowie auf das Bayerische Krankenhausgesetz (Art. 27 Abs. 4 und 5) die Frage nach der rechtlichen Befugnis von Krankenhäusern zur **Offenbarung** von personenbezogenen Daten. Die bei der Fernwartung tätigen Personen der Wartungsfirma unterliegen nicht der ärztlichen Schweigepflicht. Die Problematik stellt sich freilich nur, wenn im Zuge der Fernwartung mindestens ein Patientendatensatz mit identifizierenden Daten des Patienten der fernwartenden Softwarefirma zur Kenntnis gelangt.

Nach Anhörung der Staatsministerien des Innern, der Justiz und für Arbeit, Familie und Sozialordnung beurteile ich die Fernwartung in öffentlichen Krankenhäusern wie folgt:

- Datenschutzrechtlich handelt es sich **nicht** um eine **Datenübermittlung**, wenn bei der Wartung wie bei der Fernwartung ein personenbezogenes Datum einem Beschäftigten der Wartungsfirma bekannt wird. Bei Wartung wie Fernwartung muß in Einzelfällen die Möglichkeit zur Kenntnisnahme von Patientendaten durch Mitarbeiter der Fernwartungsfirma als Nebenfolge in Kauf genommen werden. Es ist nicht Gegenstand und Zweck der Fernwartung, die Daten mit ihrem Informationsgehalt der Wartungsfirma zu überlassen. Auch wird

der Fernwartungsvertrag ausdrücklich vorsehen, daß der Inhalt von einsehbaren Datenfeldern in keiner Weise verwertet werden darf.

Da sich die Wartungstätigkeit nicht auf den Inhalt der betreffenden Datenfelder bezieht, kann es sich bei Fernwartung auch **nicht** um **Datenverarbeitung im Auftrag** im Sinne von § 11 BDSG bzw. Art. 3 BayDSG handeln. Beide Vorschriften gehen davon aus, daß der Auftragnehmer die **Inhalte** der Datenfelder nach den Weisungen des Auftraggebers **verarbeitet**.

- Nach dem Datenschutzgesetz ist allerdings die **Sicherungsproblematik** sachgerecht zu lösen (s. hierzu unter Nr. 20.1.4).

- Soweit bei der Wartung oder Fernwartung identifizierende Patientendaten den Mitarbeitern der Softwarefirma zur Kenntnis gelangen, liegt jedoch auf jeden Fall **eine Offenbarung** im Sinne von § 203 StGB (ärztliche Schweigepflicht) vor. Eine **gesetzliche** Offenbarungsbefugnis im Sinne dieser Vorschrift ist bei Wartung wie bei Fernwartung durch ein Softwareunternehmen nicht gegeben.

  Denkbar wäre nach Ansicht des Staatsministeriums der Justiz eine Rechtfertigung unter dem Aspekt des **vermuteten Einverständnisses** des Patienten bzw. der zu § 203 StGB entwickelten Grundsätze der Güterabwägung, wenn die erforderlichen und zumutbaren Sicherungsvorkehrungen getroffen sind.

  Im Interesse klarer Verhältnisse für Patienten und Krankenhäuser bei Fremdwartung schlage ich vor, die Einwilligung des Patienten über eine **Klausel im Krankenhaus-Aufnahmevertrag** einzuholen. Durch eine wirksame Einwilligung können die strafrechtlichen Risiken der Software-Fernwartung für Krankenhäuser ausgeräumt werden.

  Voraussetzung dafür, daß den Patienten eine Klausel im Aufnahmevertrag zugemutet werden kann, ist jedoch, daß die Kenntnisnahme von personenidentifizierenden Angaben auf das notwendige Maß **eingeschränkt** wird. Auch bei Aufnahme einer entsprechenden Klausel im Aufnahmevertrag sind daher bei der Fremdwartung alle vertretbaren technisch-organisatorischen Sicherungsmöglichkeiten zu aktivieren, mit denen die Zahl der Fälle reduziert werden kann, in denen personenbezogene Patientendaten überhaupt zur Kenntnis der Wartungsfirma gelangen können (vgl. auch Nr. 20.1.4). Vor allem darf Fernwartung und allgemein Fremdwartung unter Offenbarung personenbezogener Patientendaten nur vorgenommen werden, wenn keine andere Lösung mit vertretbarem Aufwand möglich ist.

2.3 Zentrale zur Weiterverlegung von Patienten

Hochspezialisierte Intensivbetten in Kliniken sind teuer und stehen nur in begrenzter Zahl zur Verfügung. Patienten, die zunächst diese hochwertigen Intensivbetten belegen, müssen sie wieder freimachen, sobald sie in weniger aufwendige Intensivbetten verlegt werden können.

Die einzelnen Kliniken haben jedoch keinen aktuellen Überblick darüber, in welchen Krankenhäusern die benötigten Betten zur Verfügung stehen. Zur besseren Bewirtschaftung ihrer Intensivbetten haben deshalb die Münchner staatlichen und städtischen Kliniken mit der Landeshauptstadt die Einrichtung einer Zentrale zur Weiterverlegung von Patienten – ZWv – vereinbart. Sie soll eine Weiterverlegung von Patienten aus teuren, für sie nicht mehr benötigten Intensivbetten in andere, kostengünstigere Intensivbetten vermitteln.

Verfahren

Wenn ein Patient aus einem hochwertigen Intensivbett verlegt werden kann, informiert der Arzt der Intensivstation die ZWv. Er teilt ihr nähere Angaben über die Erkrankung des Patienten und die Anforderungen an das neue Intensivbett mit. Auch der Name des Patienten wird dabei zur Vermeidung von Verwechslungen genannt. Mit Hilfe dieser Angaben und der Kenntnisse über die fachlichen Betreuungsmöglichkeiten der beteiligten Kliniken sucht die ZWv selbst das passende Intensivbett in einer anderen Klinik. Telefonisch oder per Telefax werden die Patientendaten, welche die ZWv von der abgebenden Klinik erhalten hat, an die aufnehmende Intensivabteilung übermittelt. Der weitere Datenaustausch erfolgt unmittelbar zwischen den Kliniken.

Bewertung

In einem Gespräch beim Staatsministerium der Justiz habe ich abgeklärt, daß die **Offenbarung** der tatsächlich erforderlichen Daten durch die abgebende Intensivstation an die ZWv als befugt im Sinne von § 203 Abs. 1 StGB anzusehen ist. Dasselbe gilt für die Weitergabe personenbezogener Patientendaten durch die ZWv an die aufnehmende Intensivstation. Die ZWv ist als ärztlicher Gehilfe in der Behandlungskette anzusehen.

Die Übermittlung der Patientendaten aus der Klinik an die ZWv ist nach Art. 27 Abs. 5 Bayer. Krankenhausgesetz zulässig, da sie im **Rahmen des Behandlungsverhältnisses** erfolgt.

Aus datenschutzrechtlicher Sicht bleibt noch abzuklären, ob der Umfang der von der Intensivstation zur ZWv und von dort zur aufnehmenden Intensivstation weitergeleiteten personenbezogenen Informa-

tionen auf das erforderliche Maß beschränkt ist. Mit den aufnehmenden Ärzten wird der tatsächlich benötigte Datenumfang noch genauer überprüft.

2.4 Krebsregister und Datenschutz

Der Bayerische Landtag hat am 01.07.1992 einen Beschluß zur Krebsregistrierung gefaßt. Die Staatsregierung wird darin gebeten, die organisatorischen und finanziellen Voraussetzungen zu schaffen, die derzeitigen Maßnahmen zur Dokumentation der Krebserkrankungen entsprechend den Empfehlungen der Gesundheitsministerkonferenz vom 24./25. Oktober 1991 zu erweitern (Drucksache 12/7085). Dies gab erneut Anlaß, die bestehenden Möglichkeiten für einen effektiven Datenschutz solcher Datensammlungen zu überprüfen.

Von Bundesseite wird an ein **Krebsregistergesetz** gedacht, das für die Einrichtung von Krebsregistern in den Ländern einen Rahmen bilden soll. In den neuen Bundesländern muß die aus der DDR-Zeit vorhandene Sammlung von personenbezogenen Daten über Krebspatienten auf eine neue rechtliche Basis gestellt werden. Außerdem werden dort Konzepte für die Fortführung der Register in den einzelnen Ländern entwickelt. Baden-Württemberg hat, wie schon früher berichtet, ein Modell der **dezentralen Verschlüsselung von Patientendaten** bei den behandelnden Ärzten **vor der Übermittlung** an ein Landesregister entwickelt. In Rheinland-Pfalz gibt es Überlegungen zu einem weiteren Modell, bei dem personenbezogene Meldungen zuerst an eine **zentrale Verschlüsselungsstelle** gegeben werden, welche die verschlüsselten Daten an das eigentliche Register zur Speicherung weiterleitet. In Bayern wird das Modell der behandlungsbezogenen sog. **klinischen Krebsregister** weiter ausgebaut.

2.4.1 Ziel der Krebs-Datensammlung

Krebsregister werden für die Krebsforschung angelegt. Hierfür interessieren vor allem zwei Erkenntnisse:

- Die **Häufigkeit** der verschiedenen Krebs-Erkrankungsarten, ihre regionale Verbreitung und damit die möglichen **Ursachen** der Erkrankung, insbesondere auch regional lokalisierbare, umweltbedingte Ursachen
- Aussagen über Möglichkeiten und Erfolgschancen verschiedener **Therapien** , u.a. durch den Vergleich von Überlebenszeiten.

Die gezielte Datenerhebung zur Ermittlung regionaler Ursachen von Krebserkrankungen begegnet dabei großen Schwierigkeiten. Im Register können nicht alle möglicherweise wichtigen Umweltfaktoren, denen der Patient ausgesetzt war, bevor er erkrankte, gespeichert werden. Schon die Definition solcher Faktoren ist offenbar sehr schwierig. Deshalb ist es unvermeidbar, daß personenbezogene **Nacherhebungen** durchgeführt werden müssen, um möglichen Krebsursachen auf den Grund gehen zu können. Dies macht die **Deanonymisierbarkeit** der Registerspeicherungen erforderlich.

Daten über Therapie und deren Erfolg lassen sich leichter vorab definieren. Um sie im Register in ausreichendem Umfang zu erfassen, ist es nötig, auch die Zusammenführung von Daten verschiedener behandelnder Ärzte zu organisieren. Auch Todesbescheinigungen müssen hierfür zugeordnet und ausgewertet werden können.

2.4.2 Epidemiologisches oder klinisches Krebsregister

Es gibt **zwei grundsätzlich verschiedene Wege**, die für ein Krebsregister benötigten Daten zu sammeln:

- **epidemiologische Register**

  Sie werden unabhängig von behandelnden Ärzten oder Kliniken in selbständigen Forschungszentren eingerichtet und **dienen nur der direkten oder indirekten epidemiologischen Auswertung** (s.o.)

- **klinische Krebsregister**

  Die für das Krebsregister benötigten Daten sind Teil der behandlungsbezogenen Daten einer Klinik und dienen sowohl der **epidemiologischen Auswertung** als auch der **Gewinnung von Hinweisen für Nachsorge und künftige Behandlungen**.

Hinsichtlich der Möglichkeiten, der Forschung einen **einheitlichen Grunddatensatz** zur Verfügung zu stellen, sind rein epidemiologische Register und klinische Register grundsätzlich gleichwertig. Beide Registerarten müssen zwei Voraussetzungen erfüllen: Sie müssen einen ausreichend großen Teil der erkrankten Bevölkerung erfassen, um repräsentative Aussagen zu ermöglichen und sie müssen die erforderlichen Auswertungsmöglichkeiten anbieten.

2.4.3 Einheitlicher Datensatz als Basis des Registers

Bei allen bisher bekannt gewordenen Modellen soll in Krebsregistern zu jedem Patienten ein **einheitlich definierter Datensatz** gespeichert werden, der zwei Arten von **Auswertungen** zuläßt:

- **Unmittelbare Auswertung** der im Datensatz gespeicherten Angaben über die Erkrankung für statistische, einschließlich verlaufsstatistische Aussagen und
- **indirekte Auswertungen**, bei denen die gespeicherten Daten dazu dienen, bestimmte Fälle her-

auszufiltern, denen durch weitere Erhebungen, z.B. beim behandelnden Arzt (ggf. mit Einwilligung) nachgegangen wird, um diejenigen Daten zu gewinnen, die für eine bestimmte wissenschaftliche Fragestellung gebraucht werden, etwa zur Erfassung lokaler Umwelteinflüsse. Diese Fragestellungen und die für die Untersuchungen erforderlichen Daten sind bei Einrichtung des Krebsregisters meist nicht vorhersehbar, so daß hierfür nicht in ausreichendem Maße Daten vorgesehen werden können. Aber auch die Kapazität eines Registers und Kostenfragen setzen dem Umfang der in einem Krebsregister speicherbaren Daten Grenzen. Voraussetzung der effektiven Nutzung ist daher, daß die im Register gespeicherten Informationen, ggf. unter Einschaltung des meldenden Arztes, einem **bestimmten Patienten zugeordnet** werden können, ohne daß dadurch das Patientengeheimnis verletzt wird.

2.4.4 Bewertung aus der Sicht des Datenschutzes

a) **Sensibilität einer Krebsdatensammlung**

Für den Datenschutz ist von besonderer Bedeutung, daß personenbezogene medizinische Daten über Krebspatienten **sehr sensibel** sind. Die Speicherung in zentralen Datensammlungen stellt wegen der damit gegenüber der dezentralen Speicherung beim behandelnden Arzt erleichterten Möglichkeit zur anderweitigen Nutzung ein **erhöhtes Risiko für die Patienten** dar. Es ist deshalb wichtig, daß auch durch die **Art der Organisation** solcher Register die bestmögliche Sicherung der Daten gegen mißbräuchliche Verwendung für andere Zwecke erreicht wird.

Die Sensibilität der Daten ist dabei am stärksten bei denjenigen Patienten ausgeprägt, bei denen die Erkrankung für Dritte **noch nicht erkennbar** und die normale Arbeitsfähigkeit nicht wesentlich eingeschränkt ist. Aus zweckwidriger Verwendung können sich hier besondere Belastungen ergeben. Soweit **Verdachtsdiagnosen** oder **Vorstadien** einbezogen werden, was nicht bei allen Registerkonzepten der Fall ist, sind die Betroffenen in ähnlicher Lage. Verdachtsdiagnosen erweisen sich zum Teil als unzutreffend. Vorstadien, etwa bei Bluterkrankungen, können über viele Jahre andauern, ohne sich auf die berufliche Tätigkeit auszuwirken oder eine Verschlechterung der Kreditwürdigkeit der betreffenden Person zu bewirken.

Da aber **Arbeitgeber, Versicherungen** und **andere Vertragspartner** stets erheblichen Wert darauf legen, möglichst viele Informationen über gesundheitliche Risiken ihrer Vertragspartner zu erfahren, muß ein Krebsregister so eingerichtet werden, daß es für solche und ähnliche Zwecke nicht zur Verfügung steht. Es wäre für Betroffene in der Regel unmöglich, den Einfluß gespeicherter Daten auf ihre Kreditwürdigkeit oder Arbeitsfähigkeit zu widerlegen.

Belastungen für den Betroffenen können sich auch ergeben, wenn der Inhalt eines Krebsregisters zur Beurteilung des vor einem Unfall bestehenden Gesundheitszustandes eines Unfallverletzten ohne weiteres als Beweismittel herangezogen werden könnte. Auch hier könnte der Betroffene bei der Einschätzung der Ursachen für die Entwicklung seiner Gesundheit in eine ausweglose Beweissituation geraten. Der **absolute Schutz der gespeicherten personenbezogenen Daten vor Inanspruchnahme als Beweismittel** im Geschäftsverkehr ist daher eine elementare Forderung an ein Krebsregister. Andernfalls würde die Einrichtung von Krebsregistern – und auch von anderen Krankheitsregistern – in das Recht der gespeicherten Personen auf freie Entfaltung (Art. 2 GG) in unverhältnismäßiger Weise eingreifen.

b) **Klinisches oder epidemiologisches Register – aus Sicht des Datenschutzes**

Aus der **Sicht des Datenschutzes** halte ich den Ausbau der klinischen Register für besonders günstig:

Für klinische Krebsregister spricht, daß hier alle identifizierenden Patientendaten **im Verantwortungsbereich von Krankenhäusern** bleiben, also nicht an außer-klinische Registrierstellen weitergeliefert werden und somit **den erhöhten Schutz von Patientendaten in Krankenhäusern genießen**. Die Registrierung im Krankenhaus entspricht nicht nur der **Vorstellung des Patienten** über den Verbleib seiner Daten, sondern auch dem traditionell in der Ärzteschaft vorhandenen Bewußtsein, daß der ärztliche Bereich gegenüber dritten Interessenten abgeschottet werden muß (ärztliche Schweigepflicht). Außerdem bleibt bei der Registrierung im Krankenhaus auch der **Schutz von Patientendaten** vor Inanspruchnahme als Beweismittel in gerichtlichen Verfahren gemäß § 97 Abs. 2 Strafprozeßordnung in gleichem Umfang wie beim Arzt aufrecht erhalten. Hiervon kann dagegen grundsätzlich nicht ausgegangen werden, wenn Sammlungen von identifizierenden Patientendaten außerhalb von Kliniken eingerichtet werden.

Für selbständige epidemiologische Register, in denen die Patienten in identifizierbarer Weise gespeichert sind, müßte der bei klinischen Registern bereits vorhandene rechtliche Schutz erst aufgebaut werden. Durch Landesgesetze könnte aber ein Schutz entsprechend den Regelungen in § 97 StPO nicht geschaffen werden.

Schließlich dürften klinische Krebsregister, da sie Daten auch für die Nachsorge zur Verfügung stellen, von der Ärzteschaft umfassender mit Patientendaten beliefert werden als bloße epidemiologische Register.

c) **Datenschutzrechtliche Konstruktion der bayerischen klinischen Krebsregister**

Seit Jahren wird in Bayern das Ziel verfolgt, bestehende klinische Krebsregister so auszubauen, daß sie auch die Aufgaben eines epidemiologischen Registers erfüllen. Zu diesem Zweck muß von den Klinikpatienten der sog. epidemiologische „Minimaldatensatz" in einheitlicher Struktur gespeichert werden. Dieser Datensatz ist von verschiedenen Gremien definiert worden (z.B. Arbeitsgemeinschaft der Leitenden Medizinalbeamten – AGLMB).

Um möglichst große Teile der erkrankten Bevölkerung zu erfassen, schließen sich zunehmend **Kliniken aus der Region** an ein Krebsregister bei einer großen Klinik, z.B. einer Universitätsklinik, an, um im Wege der „Datenverarbeitung im Auftrag" dort die Daten ihrer Patienten für ihre eigenen Zwecke (Behandlung, Verlaufsbeobachtung) speichern und auswerten zu lassen.

Wenn angeschlossene Kliniken oder Ärzte Patientendaten im Auftrag verarbeiten lassen, besitzen sie allein den personenbezogenen, also identifizierenden Zugriff zu den Daten ihrer Patienten, nicht aber die Klinik, die für die angeschlossenen Stellen die Auftragnehmerfunktion ausübt. Der **nicht personenbezogene – medizinische – Teil** der Patientendatensätze hingegen kann aufgrund Auftrags der angeschlossenen Kliniken und Ärzte **epidemiologisch ausgewertet** werden wie in einem selbständigen epidemiologischen Krebsregister. Eine Nacherhebung weiterer Daten für besondere epidemiologische Fragestellungen ist über den jeweils auftraggebenden Arzt ebenfalls grundsätzlich möglich.

Die Rechtsform der Auftragsdatenverarbeitung setzt auch bei einer beauftragten Klinik eine **Befugnis zur Offenbarung** von personenbezogenen Patientendaten durch auftraggebende angeschlossene Kliniken an die auftragnehmende Klinik zur Durchführung des Auftrags voraus. Eine solche Offenbarungsbefugnis für „DV im Auftrag" ergibt sich für Kliniken in Bayern, die unter das Bayerische Krankenhausgesetz fallen, aus Art. 27 Abs. 4 Satz 4 und 5 dieses Gesetzes. Das Hinzufügen von Daten aus der Todesbescheinigung wäre aus Datenschutzsicht nach Änderung des Bestattungsrechts grundsätzlich unbedenklich.

Gegenwärtig werden in Bayern Daten von Patienten **niedergelassener Ärzte** bei einem Register der **Bayer. Kassenärztlichen Vereinigung anonym** gesammelt. Sie können nur über die Nummer des Nachsorgekalenders, den der Patient unterschreibt und seinem behandelnden Arzt vorweist, abgerufen oder mit weiteren klinischen Daten verknüpft werden. Auch diese Daten werden zur epidemiologischen Auswertung zur Verfügung stehen.

Datenschutzrechtlich möglich wäre auch, daß **niedergelassene Ärzte** im Wege der „Datenverarbeitung im Auftrag" Patientendaten beim klinischen Krebsregister speichern lassen. Für die damit verbundene „Offenbarung" der Patientendaten im Sinne von § 203 Abs. 1 StGB wäre die Einwilligung der Patienten nötig, da eine Art. 27 Abs. 4 S. 4 und 5 des Bayerischen Krankenhausgesetzes entsprechende Erlaubnis der Auftrags-Datenverarbeitung für **niedergelassene Ärzte** fehlt. Für die Datensammlung der Kassenärztlichen Vereinigung enthält der Nachsorgekalender eine entsprechende Einwilligungsklausel, die der Patient unterschreibt.

Die auftragnehmende Stelle für München/Oberbayern im Klinikum Großhadern weist darauf hin, daß das klinische Krebsregister auch den Vorteil bietet, den angeschlossenen Kliniken und Ärzten für ihre Behandlungstätigkeit unterstützende Auswertungen zu erstellen. Damit entsteht ein **Anreiz zur Speicherung von Patientendaten**. Dies fördert die **Aktualität und Vollständigkeit** der Datensammlung im klinischen Krebsregister und ihren Wert für die wissenschaftliche Forschung. Über einige Krebsarten ist für die Bevölkerung der Münchener Region bereits ein weitgehend vollständiger Datenbestand auswertbar.

d) **Landesweite Auswertung klinischer Krebsregister**

Durch Einrichtung derartiger klinischer Register in allen Landesteilen entsteht die Möglichkeit, **für das ganze Land** epidemiologische Auswertungen vorzunehmen. Die Einrichtung eines zusätzlichen zentralen Krebsregisters kann sich damit in Bayern erübrigen. Aus der Sicht des Datenschutzes wäre dies zu begrüßen.

Das Bayerische Staatsministerium für Unterricht, Kultus, Wissenschaft und Kunst hat festgestellt, daß die Universitätskliniken bereits **denselben epidemiologischen Grunddatensatz in kompatibler Weise speichern**. Da die regionalen Tumorzentren aber nur bei Beteiligung weiterer Kliniken (im Wege der Datenverarbeitung im Auftrag) so viele Patientendaten sammeln können, daß statistisch gesicherte Aussagen möglich sind, müßten auch die **nicht zum Hochschulbereich**

gehörenden Kliniken den einheitlichen Grunddatensatz übernehmen und sich an die regionalen Tumorzentren anschließen, damit die von ihnen gelieferten Daten für landesweite epidemiologische Auswertungen zur Verfügung stehen.

Zu spät einsetzende Koordinierungsversuche könnten u.U. auch wegen erhöhter Anpassungskosten scheitern. Dann könnte sich Bayern einem verstärkten Druck ausgesetzt sehen, neben regionalen klinischen Tumorregistern, die das Land nicht hinreichend abdecken, ein **zusätzliches landeszentrales epidemiologisches Krebsregister** einzurichten. Die gesetzliche Festlegung einer Befugnis aller Ärzte zur personenbezogenen Meldung ihrer Patienten zu diesem Register wäre dafür wohl Bedingung. Ob ein solches rein epidemiologisches Register noch innerhalb des oben beschriebenen rechtlichen Schutzbereichs einer Klinik stünde, ist fraglich.

3. Sozialbehörden

3.1 Gesundheitsstrukturgesetz 1993

Im Gesetzgebungsverfahren hatte ich kurzfristig Gelegenheit, zu einzelnen Vorschriften des Entwurfs mit Datenschutzbezug gegenüber dem Staatsministerium für Arbeit, Familie und Sozialordnung Stellung zu nehmen. Dies betraf im wesentlichen den **Umfang der Datenübermittlung von Krankenhäusern an gesetzliche Krankenkassen**, der nach dem Entwurf stark ausgeweitet wird, und die **Einschaltung privater Abrechnungsstellen** beim Einzug der Vergütung von Krankenhausärzten mit Privatliquidationsrecht. Meine Überlegungen haben in einer Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder zum Gesundheitsstrukturgesetz 1993 Eingang gefunden (Anlage).

Hingegen fanden die Befürchtungen mancher Datenschutzbeauftragter, die Strukturreform sei ein weiterer bedenklicher Schritt auf dem Weg zum „gläsernen Patienten", keine Resonanz. Zwar dürfen künftig versichertenbezogene Angaben über ärztliche Leistungen auch auf Datenbändern oder anderen maschinell verwertbaren Datenträgern erfaßt und den Krankenkassen mitgeteilt werden. Dies gilt jedoch nur, soweit dies für die **Prüfung der Leistungspflicht der Kassen, die Gewährung von Leistungen** an Versicherte, die **Abrechnung** mit den Leistungserbringern und die **Überwachung der Wirtschaftlichkeit** der Leistungen erforderlich ist. Berücksichtigt man, daß es sich hierbei um Datenflüsse handelt, die im Bereich der Privatversicherung eine Selbstverständlichkeit sind, so ist die in der gesetzlichen Krankenversicherung vorgesehene Weitergabe, Speicherung und Nutzung von Gesundheitsdaten angemessen, um insbesondere den wiederholt festgestellten Mißbrauch der Krankenversicherung durch manche Leistungserbringer zu unterbinden. Hinter dem Schlagwort vom „gläsernen Patienten" steht also weniger der Datenschutz der Patienten als vielmehr das Interesse unseriöser Leistungserbringer.

3.2 Zweites Gesetz zur Änderung des Sozialgesetzbuches

Zum Entwurf eines 2. Gesetzes zur Änderung des Sozialgesetzbuches habe ich gegenüber dem Arbeitsministerium Stellung genommen. Folgende Punkte erscheinen mir dabei bedeutsam:

1. **Weitergabe von Daten an andere Leistungsträger**

   Die Mehrzahl der anderen Datenschutzbeauftragten fordert, die **Sozialleistungsträger stärker gegeneinander abzuschotten** und sie durch Einführung einer **Zweckbindung** nach dem Vorbild allgemeiner Datenschutzgesetze stärker dazu zu veranlassen, die Daten unmittelbar beim Betroffenen zu erheben, anstatt sie zwischen Sozialleistungsträgern auszutauschen. Eine solche **Verschärfung der Übermittlungsvoraussetzungen innerhalb der Sozialversicherung** durch Zweckbindungsregelungen habe ich nicht befürwortet. Zum einen, weil dies die Arbeit von Sozialleistungsträgern ohne Notwendigkeit erschweren würde, zum anderen, weil die Zweckbindungsregelungen der allgemeinen Datenschutzgesetze unter anderen Gesichtspunkten geschaffen wurden: Dort sollen Behörden mit ganz heterogenen Aufgaben, mit deren Zusammenwirken die betroffenen Bürger weit weniger rechnen, dazu veranlaßt werden, im stärkeren Umfang als bisher Daten unmittelbar beim Betroffenen zu erheben, anstatt sie gegenseitig auszutauschen. Innerhalb des Sozialleistungsbereichs ist ein Datenaustausch zwischen Leistungsträgern jedoch angemessen.

   Zur Verbesserung der Situation des Betroffenen habe ich vorgeschlagen, ihn **von einer Datenübermittlung zu unterrichten**, soweit er ein schutzwürdiges Interesse hat, es sei denn, die Aufgabenerfüllung des Leistungsträgers würde dadurch gefährdet.

2. **Hinweis auf Rechtsvorschrift bei der Datenerhebung**

   Bei der **Erhebung der Daten** sieht der Gesetzentwurf bisher nicht vor, daß die **Vorschrift** genannt wird, die zur Angabe der Daten verpflichtet. Es genügt aber nicht, daß der Betroffene nur auf das Vorhandensein einer zur Auskunft verpflichtenden Norm hingewiesen wird, ohne diese zu benennen.

Dem Betroffenen muß die Rechtsvorschrift, die ihn zu einer bestimmten Handlung verpflichtet, genannt werden, damit er dies ggf. überprüfen kann, und die Behörde veranlaßt wird, zuverlässig zu prüfen, ob die betreffende Rechtsgrundlage die Anforderung von Daten auch in vollem Umfang abdeckt.

3. **Weitergabe von Sozialdaten an andere Behörden im Wege der Amtshilfe**

§ 68 des X. Buches des Sozialgesetzbuches gestattet derzeit und nach dem Entwurf auch künftig, an **andere Behörden Auskünfte** über Namen, Geburtsdatum, Geburtsort und **derzeitige Anschrift** sowie den Arbeitgeber des Betroffenen zu geben, soweit kein Grund zur Annahme besteht, daß dadurch schutzwürdige Belange des Betroffenen beeinträchtigt werden. Diese Vorschrift hat in der Vergangenheit zu Auslegungsproblemen geführt. So ist der Begriff „derzeitige Anschrift" in Einzelfällen so verstanden worden, daß hierunter auch der momentane Aufenthaltsort (z.B. in einem Amt) fällt. Dahinter verbirgt sich die Problematik, ob z.B. Mitarbeiter eines Sozialleistungsträgers nach vorheriger Bitte der Polizei diese verständigen dürfen, wenn eine bestimmte Person im Amt erscheint. Der Gesetzgeber sollte daher die Gelegenheit der Novellierung nützen, um klarer als bisher zum Ausdruck zu bringen, ob
- nur die Anschrift im Sinne des Melderechts oder
- der davon unabhängige tatsächliche Lebensmittelpunkt oder
- auch der momentane kurzfristige Aufenthalt übermittelt werden darf.

4. **Zweckbindung bei Datenweitergabe zu Forschungszwecken**

Bei Daten, die von einem Sozialleistungsträger an eine dritte Stelle **zum Zwecke wissenschaftlicher Forschung übermittelt** werden, sieht der Entwurf keine weitere **Zweckbindung** für wissenschaftliche Forschung mehr vor. Um die zweckwidrige Nutzung der Daten beim Empfänger zu unterbinden, sollte ein **Zweckbindungsgebot für den Empfänger** wieder aufgenommen werden. Eine gesetzliche Zweckbindung wirkt vor allem bei nichtöffentlichen Empfängern weit stärker als behördliche Auflagen.

3.3 Krankenversicherungskarte als Chipkarte

Nach dem Sozialgesetzbuch (SGB) sollen alle gesetzlich Krankenversicherten eine **maschinenlesbare Krankenversichertenkarte** erhalten (§ 291 SGB V). Hierzu kann entweder eine **Magnetstreifenkarte**, auf der die **Grunddaten** des Versicherten magnetisch gespeichert sind, oder eine moderne **Chipkarte**, bei der diese Daten in einem Mikrochip enthalten sind, verwendet werden.

Für die Einführung der Chipkarte spricht, daß eine wesentlich höhere **Datensicherheit** erreicht wird. Die gespeicherten Daten können durch einen **integrierten Zugriffsschutz** gesichert werden.

Die Chipkarte bietet jedoch rein technisch die Möglichkeit, wesentlich mehr als die vom Sozialgesetzbuch in § 291 Abs. 2 SGB V gesetzlich abschließend festgelegten Daten des Versicherten auf der Karte abzuspeichern.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat deshalb für den Fall, daß die Chipkarte eingeführt wird, gefordert, „daß eine Speicherung auf einer Chipkarte als elektronische Krankenversichertenkarte **auf die gesetzlich festgelegten Grunddaten beschränkt bleiben muß** und nicht auf Gesundheitsdaten ausgedehnt werden darf. Eine technische Sicherung dieser Beschränkung ist zu gewährleisten".

Die Speicherung weiterer Daten, etwa über Risikofaktoren oder besondere Krankheitsinformationen auf einer **anderen Karte**, bleibt davon unberührt. Es mag durchaus sinnvoll und für den Arzt oder Apotheker, insbesondere in Notfällen, eine wertvolle Hilfe sein, wenn auf freiwilliger Basis Gesundheitsdaten des Versicherten wie Risikofaktoren, Krankheitsdaten, Blutgruppe u.ä. auf einer Chipkarte auf freiwilliger Basis gespeichert werden, die der Versicherte bei sich führt. Diese Gesundheitsdaten dürfen jedoch nicht auf der Chipkarte mit den Grunddaten, sondern müssen auf einer **anderen** Karte gespeichert werden.

3.4 Prüfung von Krankenkassen

Im Berichtszeitraum habe ich bei fünf gesetzlichen Krankenkassen, darunter einer Betriebskrankenkasse, allgemeine Datenschutzkontrollen durchgeführt. Den Schwerpunkt bildeten die Erhebung personenbezogener Daten durch **Formulare**, die **Nutzung** der erhobenen Daten sowie **regelmäßige Datenübermittlungen**. Ich konnte feststellen, daß die Kassen den sensiblen Sozialdatenschutz im wesentlichen beachten, und Datenschutzverstöße die seltene Ausnahme sind.

Eine Änderung der bisherigen Verfahrensweise habe ich in folgenden Punkten gefordert:

1. **Unzureichender Datenschutzhinweis auf Erhebungsformularen**

Bei allen geprüften Kassen war der Hinweis auf den Datenschutz auf den verwendeten Formularen oftmals nicht ausreichend.

Notwendig ist: Werden personenbezogene Daten beim Betroffenen mit seiner Kenntnis erhoben, so ist der **Erhebungszweck** ihm gegenüber anzugeben. Werden sie beim Betroffenen aufgrund einer **Rechtsvorschrift** erhoben, die zur Auskunft verpflichtet oder ist die Erteilung der Auskunft Voraussetzung für die Gewährung von Rechtsvorteilen, so ist der Betroffene hierauf, sonst auf die **Freiwilligkeit** seiner Angaben hinzuweisen (§ 13 Abs. 3 BDSG).

Bei einigen Formularen fehlte ein derartiger Hinweis völlig, bei anderen konnte der Versicherte nicht erkennen, ob er zur Mitteilung der Angaben verpflichtet ist bzw. für welchen Zweck Daten erhoben werden. Ich habe daher die Kassen aufgefordert, die Formulare neu zu gestalten und einen Hinweis anzubringen, der (im Falle der Auskunftspflicht) etwa wie folgt lauten könnte:

> „Die Erhebung der Daten beruht auf (Vorschrift, zu deren Vollzug die Daten erhoben werden); zur Mitteilung sind Sie nach (Vorschrift, aus der sich eine Pflicht zur Mitteilung ergibt) verpflichtet."

Der Hinweis sollte in drucktechnisch hervorgehobener Weise **möglichst am Anfang des Fragebogens** angebracht werden, damit der Versicherte vor dem Ausfüllen weiß, welche Angaben freiwillig sind.

2. **Überflüssiges zum Einkommen über der Beitragsbemessungsgrenze**

In der Beitragsabteilung verwenden die Krankenkassen Formulare, in denen vom Versicherten detaillierte Angaben über sein Einkommen verlangt werden. Dabei werden z.B. auch Fragen nach Einnahmen aus Vermietung, Verpachtung, Rente, Sozialhilfebezug sowie nach sonstigen Einnahmen gestellt. Diese Detailangaben benötigt die Kasse jedoch **nur bis zur jeweiligen Beitragsbemessungsgrenze** nach § 232 i.V. mit 239 und 240 des Fünften Buches des Sozialgesetzbuches (SGB V).

Ich habe daher die Kassen aufgefordert, die Versicherten auf die gültige Beitragsbemessungsgrenze hinzuweisen und genauere Angaben zum Einkommen nur zu verlangen, wenn sie unter der Beitragsbemessungsgrenze liegen. Der Versicherte kann sich dann möglicherweise zeitraubende Berechnungen über Einkünfte ersparen, welche die Kasse nicht benötigt. Die Kasse vermeidet dadurch unzulässige – weil nicht erforderliche – Datenerhebungen. Die Kassen waren bereit, die Formulare entsprechend zu ändern.

3. **Interessenkonflikte in der Personalkrankenkasse**

Besonderes Augenmerk habe ich auf die Führung der Personalkrankenkasse gelegt. Nach § 284 Abs. 4 SGB V dürfen Versicherungs- und Leistungsdaten der Beschäftigten einer Krankenkasse einschließlich ihrer mitversicherten Angehörigen den Personen, die kasseninterne **Personalentscheidungen** treffen, nicht zugänglich sein. Bei einer Kasse stellte ich fest, daß die Personalkrankenkasse von einem Mitarbeiter geführt wird, der auch **Personalratsvorsitzender** ist. Bei dieser Doppelfunktion besteht die Gefahr von Interessenkonflikten, wenn ihm bei der Führung der Personalkrankenkasse Krankheiten eines Mitarbeiters bekannt werden, über den eine Personalentscheidung getroffen werden soll, an welcher der Personalrat mitwirkt. Nach Angaben der Kasse war dies jedoch im konkreten Fall die gerechteste Lösung, da der Personalratsvorsitzende das Vertrauen der Beschäftigten genieße. Inwieweit dies tatsächlich und ausnahmslos zutrifft, ist jedoch schwer nachprüfbar.

Zur Lösung dieses Interessenkonfliktes habe ich in Übereinstimmung mit dem Landesprüfungsamt für die Sozialversicherung vorgeschlagen, daß sich der Personalratsvorsitzende durch seinen Vertreter bei Personalentscheidungen vertreten läßt, falls aufgrund seiner Kenntnis aus der Führung der Personalkrankenkasse Interessenkonflikte entstehen können.

4. **Datenübermittlungen an andere Behörden**

Stichprobenartige Überprüfungen von Auskunftsersuchen anderer Behörden haben keine Anhaltspunkte dafür ergeben, daß personenbezogene Daten von den Kassen unzulässigerweise übermittelt werden. Da jedoch insbesondere in der Leistungsabteilung sensible Daten gespeichert werden, habe ich empfohlen, die Mitarbeiter in regelmäßigen Abständen davon zu unterrichten, welche Auskünfte sie erteilen dürfen, bzw. wann der interne Datenschutzbeauftragte einzuschalten ist. In diesem Zusammenhang besonders zu würdigen sind die Bemühungen einer Kasse, die eine umfassende **Datenschutz-Dienstanweisung** erstellt hat: In ihr sind auch die Behörden aufgezählt, denen Daten übermittelt werden dürfen. Ferner ist geregelt, wie bei der Übermittlung zu verfahren ist.

3.5 Offenbarung einer krankheitsbedingten Fahruntauglichkeit an die Führerscheinstelle

Eine Berufsgenossenschaft wandte sich mit der Bitte um Überprüfung folgender Angelegenheit an mich:

Die Berufsgenossenschaft hatte zur Klärung ihrer Leistungspflicht wegen eines Betriebsunfalls mit einem Traktor fachärztliche Gutachten über den Gesundheitszustand ihres Versicherten eingeholt.

In zwei Gutachten hatten die Fachärzte festgestellt, daß der Versicherte nicht fahrtauglich sei. Diese Erkenntnis hatten sie auch dem Versicherten mitgeteilt. Da die Ärzte selbst die Führerscheinstelle von dieser Sachlage nicht in Kenntnis gesetzt hatten, stellte sich nun die Frage, ob die Berufsgenossenschaft die **Führerscheinstelle** benachrichtigen dürfte.

Zwar war zur Erfüllung sozialer Aufgaben nach § 69 SGB X eine solche Datenübermittlung nicht erforderlich. Die Berufsgenossenschaft hatte aber auch zu prüfen, ob eine Information der Führerscheinstelle aufgrund **übergesetzlichen Notstands** entsprechend § 34 StGB in Frage kam. Zwar wird in der Literatur teilweise dessen Anwendbarkeit verneint, weil die Regelungen im SGB X als abschließend anzusehen seien; nach herrschender Auffassung ist aber eine Offenbarung in Fällen des übergesetzlichen Notstands nicht ausgeschlossen, da nicht erkennbar sei, daß der Gesetzgeber im SGB X die Anwendung des übergesetzlichen Notstandes (entsprechend § 34 StGB) ausschließen wollte.

In Übereinstimmung mit dem Staatsministerium für Arbeit, Familie und Sozialordnung habe ich der Berufsgenossenschaft vorgeschlagen, einen „Berufshelfer" zum Versicherten zu schicken, um herauszufinden, ob eine Gefährdung anderer Verkehrsteilnehmer durch den Versicherten besteht. Hätte man eine derartige Gefährdung festgestellt und wäre der Betroffene mit einer Verständigung der Führerscheinstelle nicht einverstanden gewesen, hätte man prüfen müssen, ob es sich um eine „gegenwärtige, nicht anders abwendbare Gefahr" für Leib und Leben Dritter handelt, die eine Offenbarung an die Führerscheinstelle entsprechend § 34 StGB rechtfertigen würde.

Die Berufsgenossenschaft hat daraufhin mitgeteilt, daß nach **Abwägung** sämtlicher Faktoren nach ihrer Auffassung **keine gegenwärtige Gefahr** bestehe. Es bestünde kein Grund, an der Einsichtigkeit und Verläßlichkeit ihres Versicherten zu zweifeln. Die Fahruntauglichkeit des Versicherten sei deshalb der Führerscheinstelle nicht offenbart worden.

3.6 Offenbarungsbefugnis des Jugendamtes gegenüber der Polizei in Fällen von Kindesmißhandlungen

Der Mitarbeiter eines Jugendamtes wandte sich in folgender Angelegenheit an mich:

Er habe eine Familie zu betreuen, deren Kinder derzeit in Pflegefamilien untergebracht seien. Der Vater sei wegen des Verdachts der Kindesmißhandlung zur Zeit in Haft. Die Kriminalpolizei verlange nun vom Jugendamt eine **Aussage** über Einzelheiten aus seiner Betreuungstätigkeit. Darüber hinaus fordere die Polizei die **Einsichtnahme in Akten**, die nach Familienbesuchen erstellt worden seien. Eine richterliche Anordnung, nach der gem. § 73 SGB X die Offenbarung zulässig war, lag nicht vor.

Zur Zulässigkeit der Offenbarung von Sozialgeheimnissen und der Akteneinsicht habe ich in Absprache mit dem Ministerium für Arbeit, Familie und Sozialordnung folgende Auffassung vertreten: Bei den Akten, welche die Polizei einsehen will, handelt es sich um Berichte, die aufgrund von Besuchen und Gesprächen mit der betroffenen Familie erstellt wurden. Die in den Akten enthaltenen Informationen konnten nur mit Einwilligung der Familienmitglieder auf **freiwilliger Basis** gewonnen werden. Nur in Erwartung von Hilfe durch das Jugendamt wurden die Informationen gegeben. Auch die Daten, die der Polizei offenbart werden sollen, sind personenbezogene Daten, die den Mitarbeitern zum Zweck **persönlicher** und **erzieherischer Hilfe** anvertraut wurden.

Für die Daten, die dem Jugendamt in diesem Rahmen mitgeteilt wurden, gilt der **besondere Vertrauensschutz** des § 65 SGB VIII, soweit keine richterliche Anordnung nach § 73 SGB X vorliegt. Nach § 65 SGB VIII dürfen die Daten nur offenbart werden

- mit Einwilligung dessen, der die Daten anvertraut hat, oder
- dem Vormundschafts- oder Familiengericht unter bestimmten Voraussetzungen,
- im übrigen unter den Voraussetzungen, unter denen eine der in § 203 Absatz 1 oder Absatz 3 StGB genannten Personen (z.B. ein Arzt) dazu befugt wäre.

Da die ersten beiden Alternativen ausscheiden, kommt eine Offenbarung also nur unter den Voraussetzungen in Betracht, unter denen eine in § 203 StGB genannte Person befugt wäre.

Zu denken ist zunächst an rechtfertigenden Notstand nach § 34 StGB. Voraussetzung hierfür ist jedoch eine **gegenwärtige,** nicht anders abwehrbare Gefahr für Leib und Leben. Da sich der Beschuldigte in Haft befindet, und das betroffene Kind in einer Pflegefamilie untergebracht ist, liegt eine gegenwärtige Gefahr momentan nicht vor.

Eine Offenbarung kann jedoch nach wohl herrschender Meinung für einen Arzt und damit nach § 65 SGB VIII auch für den Mitarbeiter des Jugendamtes geboten sein „zur Wahrung entgegenstehender berechtigter eigener oder fremder Interessen, soweit die Offenbarung unter Berücksichtigung der widerstreitenden Interessen ein angemessenes Mittel dazu ist". Der Mitarbeiter des Jugendamtes muß daher sorgfältig prüfen, ob nach Abwägung aller Umstände, die für und gegen die Offenbarung sprechen, diese ein angemessenes Mittel ist, die Interessen des Kindes zu wahren.

Zu berücksichtigen ist dabei einerseits, daß das Sozialgeheimnis auch den Sinn und Zweck hat, den Hilfsbedürftigen die Angst zu nehmen, sich an die Sozialbehörden um Hilfe zu wenden. Es dient der sozialen Wohlfahrt. Hilfe wird nur in Anspruch genommen, wenn der Hilfesuchende darauf vertrauen kann, daß sich die Hilfe nicht zu seinem Nachteil verkehrt. Dieses generelle Vertrauen in die Beachtung des Sozialgeheimnisses muß jedoch zurücktreten, wenn im Einzelfall schutzwürdige Interessen Dritter es erfordern. Diese Interessen hat das Jugendamt in jedem konkreten Einzelfall zu ermitteln. Bei schweren Mißhandlungen, völlig zerrütteten Familienverhältnissen und Neigung des Vaters zu roher Gewalt dürfte die Information der Polizei und die daraus folgende Verurteilung selbst mit der Folge noch tieferer Zerrüttung dem Kindesinteresse eher entsprechen als vage Aussichten auf Besserung der Verhältnisse.

3.7 Mitteilung der nichtehelichen Vaterschaft an Arbeitgeber

Ein Bürger hat sich bei mir darüber beschwert, das Jugendamt habe seinem Arbeitgeber mitgeteilt, daß er der Vater eines unehelichen Kindes sei, für das er Unterhalt zu leisten habe. Ein Mitarbeiter des Jugendamtes hatte in seiner Eigenschaft als Amtspfleger beim Leiter der Lohnbuchhaltung seines Arbeitgebers angerufen, um für die Festsetzung des Unterhalts des Kindes Näheres über die Höhe seines Einkommens zu erfahren.

Ich habe die Anfrage des Amtspflegers beim Arbeitgeber des angeblichen Vaters als unzulässige Offenbarung gewertet. Bereits die Tatsache, daß ein Bürger mit der Sozialbehörde in bestimmtem näheren Kontakt steht, fällt unter das Sozialgeheimnis. Dies gilt umso mehr, wenn sich aus der Person des Anfragenden und den sonstigen Umständen ergibt, daß es sich bei dem Betroffenen um einen nichtehelichen Vater handelt, der seinen Zahlungsverpflichtungen nicht nachkommt.

Als Offenbarungsbefugnis für den Amtspfleger kommt nur § 61 Abs. 2 i.V. mit § 68 Abs. 1 SGB VIII in Betracht. Danach ist die Erhebung von personenbezogenen Daten im Rahmen der Tätigkeit als Amtspfleger zulässig, soweit ihre Kenntnis zur Erfüllung der jeweiligen Aufgabe erforderlich ist. Auf die Führung der Amtspflegschaft sind die Bestimmungen des Bürgerlichen Gesetzbuches (BGB) anzuwenden. Dort ist zwar die Aufgabe des Pflegers geregelt, Unterhaltsansprüche für das Kind geltend zu machen. Der Anspruch auf Auskunft gemäß § 1605 BGB kann aber erst geltend gemacht werden, wenn die Vaterschaft rechtskräftig festgestellt ist. Da die rechtskräftige Feststellung der Vaterschaft fehlte, bestand kein Auskunftsanspruch gegen den Betroffenen. Erst recht bestand daher keine rechtliche Grundlage für die Anfrage beim Arbeitgeber.

Die Anfrage beim Arbeitgeber war daher als unzulässige Offenbarung zu rügen. Der Oberbürgermeister hat inzwischen den Mitarbeitern des Jugendamtes entsprechende Weisungen erteilen lassen. Ich habe darüber hinaus gefordert, die Mitarbeiter des Jugendamtes durch wiederholte Schulungen auf die **Sensibilität** der dort gespeicherten Daten hinzuweisen.

3.8 Doppelfunktion eines Mitarbeiters im Sozial- und Jugendamt

Ein Landratsamt bat mich zu überprüfen, ob es zulässig sei, daß ein Bediensteter als Sozialarbeiter zur Hälfte im Sozialamt und zur anderen Hälfte im Jugendamt beschäftigt sei. Während seiner Tätigkeit für das Jugendamt erhalte er gelegentlich auch Informationen, die für das Sozialamt wichtig seien und umgekehrt. Neben der generellen Zulässigkeit einer solchen Doppelfunktion sei auch fraglich, ob derartige Informationen an das jeweilige Amt weitergegeben werden dürfen.

Ich habe dazu die Auffassung vertreten, daß die Bereiche Sozialamt und Jugendamt **organisatorisch strikt getrennt werden sollten**. Daher sind zunächst **alle** organisatorischen Möglichkeiten auszuschöpfen, damit eine solche Doppelfunktion vermieden wird. Sollte eine Trennung dennoch nicht möglich sein, so ist aus der Sicht des Datenschutzes folgendes zu beachten:

1. Die von dem Mitarbeiter betreuten Personen sind vor der Datenerhebung durch einen deutlichen **Hinweis auf die Doppelfunktion** des Beraters hinzuweisen. Ohne diese Information könnten die Betroffenen **freiwillige** Angaben machen, die sie einem Mitarbeiter des anderen Amtes nicht gemacht hätten.

2. Die Frage nach der Zulässigkeit der **Verwertung** der Informationen für die andere Funktion habe ich in Übereinstimmung mit den Staatsministerium für Arbeit, Familie und Sozialordnung wie folgt beurteilt:

   Gibt das Jugendamt personenbezogene Daten an das Sozialamt weiter, so handelt es sich um eine **Offenbarung** im Sinne der § 64 II, 65 SGB VIII, 67 ff. SGB X. Wird daher der Mitarbeiter in Erfüllung von Aufgaben des Jugendamtes tätig, darf das Sozialamt hierbei erlangte Daten nur bei Vorliegen einer Offenbarungsbefugnis nach diesen Bestimmungen verwerten.

3.9 Automatisierte Speicherung von Sozialdaten bei einer kreisangehörigen Gemeinde

Bei der Überprüfung von automatisierten Verfahren einer **kreisangehörigen** Gemeinde stellte ich bei der Speicherung von Sozialdaten folgende Mängel fest:

1. Die Gemeinde plante die **Erfassung** sämtlicher **Wohngeldantragsteller** in einem automatisierten Verfahren. Dabei sollte auch die im Wohngeldantrag angegebene Miete und das Einkommen der zum Haushalt gehörenden Familienmitglieder gespeichert werden, damit bei der Vorprüfung späterer Wohngeldanträge in einem Vergleich mit den früheren Angaben Unstimmigkeiten aufgedeckt werden können.

   Mit dem Staatsministerium des Innern habe ich die Auffassung vertreten, daß zur Erfüllung der Aufgaben einer kreisangehörigen Gemeinde nach § 16 I SGB I, 23 I Wohngeldgesetz zwar die Speicherung gewisser Grunddaten – z.B. Name und Anschrift des Antragstellers, Datum des Antragseingangs und der Weiterleitung an das Landratsamt, Art des Antrags und Wohngeldnummer als erforderlich angesehen werden kann. Dagegen ist die Speicherung der **Miete** und des **Einkommens** der zum Haushalt gehörenden Familienmitglieder nicht erforderlich und damit **unzulässig**.

2. Desweiteren plant die Gemeinde die automatisierte Speicherung von **Antragstellern auf Erwerbsunfähigkeitsrente** sowie von Antragstellern **auf Rente aus der Sozialversicherung**. Die Gemeinde begründete dies mit der Notwendigkeit, bei Rückfragen seitens der Versicherungsträger oder des Versicherten den jeweiligen **Sachstand** schnellstmöglich ersehen zu können.

   Mit dem Staatsministerium für Arbeit, Familie und Sozialordnung habe ich diese Speicherung bei einer kreisangehörigen Gemeinde **nicht für erforderlich** erachtet. Die kreisangehörige Gemeinde hat nach § 16 I 2 SGB I nur die Aufgabe, Anträge auf Sozialleistungen **entgegenzunehmen** und **weiterzuleiten**. Eine Pflicht zur Sachbearbeitung, die eine dateimäßige Erfassung der Anträge erfordern würde, besteht jedoch nicht. Ich habe daher gefordert, soweit die Gemeinde hier freiwillige Unterstützungsarbeit leistet, eine Speicherung nur noch mit **schriftlicher Einwilligung der Betroffenen** vorzunehmen. Die Einwilligungserklärung sollte auch den folgenden Hinweis enthalten: „Die Erteilung dieser Einwilligung ist freiwillig; eine Verweigerung hat auf Leistungen keine Auswirkungen. Nichtankreuzen wird als Verweigerung der Einwilligung behandelt." Die Gemeinde hat diesen Zusatz in die Einverständniserklärung übernommen.

4. Polizei

4.1 Zur Lage des Datenschutzes

Im 13. Tätigkeitsbericht habe ich vom Innenministerium gefordert, die **Richtlinien und Dienstanweisungen** für die polizeiliche Datenverarbeitung an das neue Polizeiaufgabengesetz vom 1.10.1990 anzupassen. Diese **Anpassung** ist eingeleitet. Die Errichtungsanordnung für den **kriminalpolizeilichen Aktennachweis** (KAN) wurde vom Innenministerium überarbeitet, wobei bisher allerdings nur ein Teil meiner Forderungen berücksichtigt worden ist. Der Überprüfung bedürfen u. a. auch die Richtlinien für die Führung kriminalpolizeilicher personenbezogener Sammlungen (KpS).

Innen- und Justizministerium sind nunmehr dem Landtagsbeschluß vom 15.5.1991 nachgekommen, „die Führung kriminalpolizeilicher Sammlungen dadurch zu verbessern, daß bei **Verfahrenseinstellungen** (durch die Justiz) aus der Mitteilung hervorgeht, ob nach Auffassung der Staatsanwaltschaft damit auch der Tatverdacht entfallen ist". Wenn die Polizei über einen Bürger eine Kriminalakte anlegt und bei der Staatsanwaltschaft Strafanzeige erstattet, erhält sie nunmehr nicht nur Kenntnis vom Ausgang des Justizverfahrens, sondern – in den Fällen, in denen Gericht oder Staatsanwaltschaft den Bürger für unschuldig halten – **auch die Gründe dieser Justizentscheidung** mitgeteilt mit der Folge, daß nach einer Überprüfung die Kriminalakte vernichtet und die KAN-Eintragung gelöscht werden kann. Damit wird ein ganz wesentlicher Beitrag zur Löschung unzutreffender belastender Speicherungen in Kriminalakten und im Kriminalaktennachweis geleistet.

Das Innenministerium hat inzwischen die Errichtungsanordnung und die Dienstanweisung für die **Datei „Polizeiliche Sachbearbeitung/Vorgangsverwaltung – Verbrechensbekämpfung (PSV)"** erlassen. Bei dieser neuen Datei, die künftig als Instrument der täglichen Sachbearbeitung die Grundlage der polizeilichen Datenverarbeitung bilden dürfte, sind jedoch noch einige datenschutzrechtliche Anforderungen wie **Protokollierung der Abfragen** und **Beschränkung des Zugriffs** auf Zwecke der Vorgangsverwaltung zu klären.

Die **technische Ausstattung** der Dienststellen mit DV-Geräten ist weitgehend abgeschlossen. Auch im Berichtszeitraum wurden wieder eine Reihe von APC-Anwendungen zum Datenschutzregister angemeldet, die auf ihre datenschutzrechtliche Zulässigkeit zu überprüfen waren.

Das Innenministerium entwickelt derzeit ein Konzept zur **Vernetzung der polizeilichen Dateien** und ein **Zugriffssystem**, das gewährleistet, daß dem jeweiligen Sachbearbeiter aus dem „Integrierten Gesamtverfahren der Polizei" mit seinen zahlreichen Dateien nur die zur Aufgabenerfüllung erforderlichen Daten zur Verfügung gestellt werden. Für den Datenschutz gilt es dabei, den in Art. 38 Abs. 1 PAG normierten Grundsatz der Erforderlichkeit der Datennutzung zur

Geltung zu bringen. An der Konzeptentwicklung werde ich beteiligt.

Mit dem **Gesetz zur Bekämpfung der Rauschgiftkriminalität und anderer Formen der Organisierten Kriminalität (OrgKG)** hat die Polizei eine rechtliche Grundlage für zahlreiche Fahndungsmethoden erhalten, die bisher auf der Grundlage des sog. Übergangsbonus angewandt wurden. Über den **Einsatz von Abhörgeräten in Wohnungen** zur Bekämpfung schwerster Verbrechen der Organisierten Kriminalität muß der Gesetzgeber erst noch entscheiden.

Mit dem **Wegfall der EG-Binnengrenzkontrollen** zum 01.01.1993 stellt sich die Frage, ob und welche **Ausgleichsmaßnahmen** neben dem Schengener Informationssystem und der Nachteile auf dem Gebiet des Nachbarstaates erforderlich sind, um das durch den Wegfall dieser Grenzkontrollen entstehende Sicherheitsdefizit aufzufangen. Nach Ansicht des Staatsministers des Innern wird auf fachlicher Ebene zwischen den Ländern zu erörtern sein, ob die bisher bestehenden Befugnisse für ereignis- und verdachtsunabhängige Fahndungskontrollen im Binnenland noch als ausreichend angesehen werden können oder ob präventive Lücken in der Bekämpfung der organisierten Kriminalität bestehen, so daß auch an eine gesetzgeberische Initiative zu denken wäre. Es bleibt abzuwarten, welche konkreten Vorschläge vorgelegt werden.

In der **Staatsschutzkartei APIS**, die der Abwehr und Aufklärung von Straftaten gegen die innere Sicherheit dient, können künftig sog. **Kontaktpersonen** zu Beschuldigten und Verdächtigen von Straftaten mit staatsfeindlicher Zielsetzung bis zu fünf Jahren gespeichert werden. Die bisherige kürzere Frist hatte sich wegen der für diesen Bereich typischen konspirativen Vorgehensweise nach den Erfahrungen der Polizei für die Aufklärung von Straftaten krimineller, insbesondere terroristischer Vereinigungen als zu kurz erwiesen.

Angesichts zunehmender rechtsextremistischer Verbrechen, von Anschlägen auf Asylbewerberheime, Ausländer und jüdische Einrichtungen werden Überlegungen angestellt, einen polizeilichen **Meldedienst** einzurichten, damit die Polizei umfassende Kenntnis über die verdächtigen Personen erhält, durch Auswertung der Vorgehensweise unbekannte Täter ermitteln und bei geplanten Aktionen rechtzeitig in der erforderlichen Stärke einschreiten kann. Gegen diesen **Sondermeldedienst fremdenfeindliche Straftaten** bestehen genausowenig Bedenken wie gegen den vor Jahren eingerichteten **Meldedienst linksextremistische Straftäter**, der allerdings von einigen Bundesländern auf massive Forderungen der dortigen Datenschutzbeauftragten hin eingestellt worden ist. Keine datenschutzrechtlichen Bedenken bestehen auch gegen die **verstärkte polizeiliche Beobachtung politischer Straftäter**, ein Instrument, das in einigen Bundesländern wegen angeblicher datenschutzrechtlicher Zweifel zur Bedeutungslosigkeit verkümmert ist.

4.2 Schwerpunkte

Schwerpunkte meiner Tätigkeit im Polizeibereich waren

- allgemeine Kontrollen von Dateien und Karteien, insbesondere von Dateien zur Gefahrenabwehr und Strafverfolgung (sog. GAST-Dateien auf Arbeitsplatzcomputern im APC-Verfahren), der Datei „Polizeiliche Sachbearbeitung/Vorgangsverwaltung – Verbrechensbekämpfung (PSV)" der „Arbeitsdatei PIOS – Innere Sicherheit (APIS)" und des Kriminalaktennachweises (KAN),

- die Prüfung von neuen und überarbeiteten polizeilichen Errichtungsanordnungen auf der Grundlage des novellierten Polizeiaufgabengesetzes,

- die Auswertung der Protokolldatei,

- Bürgereingaben.

4.3 Anwendung des Polizeiaufgabengesetzes (PAG)

4.3.1 Verlängerung von Ausschreibungen zur polizeilichen Beobachtung

Die Ausschreibung zur polizeilichen Beobachtung darf nach Art. 36 Abs. 3 PAG i.V.m. Art. 33 Abs. 5 PAG nur vom **Leiter** eines Landespolizeipräsidiums oder einer Polizei- oder Kriminaldirektion, des Grenzpolizeipräsidiums oder des Landeskriminalamtes angeordnet werden. Der Präsident des Landeskriminalamtes kann die Anordnungsbefugnis auf die nachgeordneten Abteilungsleiter übertragen. Die Anordnung ist auf höchstens ein Jahr zu befristen. Zur Verlängerung der Laufzeit bedarf es einer neuen Anordnung. Durch dieses Verfahren soll vermieden werden, daß vom Fahndungsinstrument der polizeilichen Beobachtung zu sorglos und ohne nähere Begründung der Notwendigkeit Gebrauch gemacht wird.

Bei der Prüfung entsprechender Unterlagen einer Polizeibehörde habe ich festgestellt, daß Art. 36 Abs. 3 PAG nicht genügend beachtet war. Die Verlängerung der polizeilichen Beobachtung erfolgte **nicht durch den dazu Berechtigten**. Eine materielle Prüfung der Erforderlichkeit der Verlängerung war in den Unterlagen **nicht dokumentiert**. Ich habe diese Versäumnisse gerügt und die Überprüfung der Verlängerungen veranlaßt.

4.3.2 Einsicht in Paßfotos bei den Paßbehörden zur Verfolgung von Verkehrsordnungswidrigkeiten

Immer wieder beklagen sich Petenten, daß sich die Polizei bei der Aufklärung von Verkehrsverstößen der Paßfotos bei den Paßbehörden bedient. Dies ist zulässig.

Wird ein Verkehrsverstoß durch automatische Kameras registriert, kann der verantwortliche Fahrzeugführer meist nicht an Ort und Stelle angehalten und seine Identität festgestellt werden. Wendet der Fahrzeughalter dann bei seiner Anhörung ein, er habe das Fahrzeug zum fraglichen Zeitpunkt nicht geführt und macht er auch keine Angaben zur Person des verantwortlichen Fahrzeugführers, dann ist für die Polizei der Tatnachweis zumindest erheblich erschwert. Wurde von dem Verkehrsverstoß und dem Fahrzeugführer jedoch ein Frontfoto aufgenommen, so kann durch den Vergleich des Frontfotos mit dem bei der Ausweisbehörde verwahrten Paßfoto die als Fahrzeugführer in Betracht kommende Person häufig ermittelt werden.

Die Beschwerdeführer waren der Meinung, daß die Paßfotos ausschließlich für Zwecke der Paßbehörde, nicht aber für die Verfolgung von Verkehrsordnungswidrigkeiten genutzt werden dürfen. Diese Annahme ist unzutreffend. Die Polizei darf die Paßbehörde nach Art. 42 Abs. 2 PAG um die Übermittlung des Paßbildes ersuchen, wenn sie es zur Erfüllung ihrer Aufgaben benötigt. Die Paßbehörde darf nach § 22 Abs. 2 des Paßgesetzes (PaßG) der Polizei auf Ersuchen das Paßfoto übermitteln. Diese darf es bei ihren Ermittlungen verwenden, Abzüge anfertigen etc.

Die Heranziehung des Paßfotos ist nicht wegen des Grundsatzes der Verhältnismäßigkeit auf die Aufklärung besonders gravierender Verkehrsverstöße beschränkt. Im Hinblick auf die geschwundene Verkehrsmoral und die Gefahren des Straßenverkehrs besteht auch bei Verkehrsverstößen, die nicht zu einer Eintragung im Verkehrszentralregister führen, ein **gesteigertes öffentliches Interesse an Aufklärung und Ahndung**. Diese dürfen bei leichteren Verstößen nicht zusätzlich erschwert werden, da sonst die Polizei wegen unverhältnismäßigen Aufwandes die Verfolgung einstellt. Im übrigen ist die Heranziehung des Paßfotos ein relativ geringer Eingriff.

4.3.3 Videoabstandsmessungen

In Bayern wird die Einhaltung des notwendigen Mindestabstands zwischen Fahrzeugen im fließenden Verkehr mit Hilfe einer **Video-Kamera** überwacht. Zur Identifizierung des Fahrers, der den Mindestabstand unterschreitet und zur Feststellung des amtlichen Kennzeichens des zu dicht auffahrenden Fahrzeugs wird eine **Frontfotoanlage** eingesetzt.

Die Videokamera wird beispielsweise auf einer Brücke so aufgestellt, daß der anlaufende Verkehr von der Kameraoptik im Bereich der Meßstrecke von oben erfaßt und das Verkehrsgeschehen ständig aufgezeichnet wird.

Dieses Verfahren ist aus datenschutzrechtlicher Sicht nicht zu beanstanden, da Fahrer und Kennzeichen der an Verkehrsverstößen **unbeteiligten Fahrzeuge** in der Videoaufnahme normalerweise nicht zu erkennen sind. Selbst wenn im Einzelfall personenbezogene Daten Unbeteiligter festgehalten werden, ist die Aufnahme des fließenden Verkehrs ohne konkrete Anhaltspunkte für eine Straftat oder Ordnungswidrigkeit durch Art. 33 Abs. 2 PAG gedeckt: Die Erfüllung der polizeilichen Aufgabe, den fließenden Verkehr auf Geschwindigkeitsverstöße und Verstöße gegen das Abstandsgebot zu überwachen, würde sonst erheblich erschwert.

4.3.4 Information von Privaten über polizeiliche Erkenntnisse

Die Polizei kann nach näherer Maßgabe des Art. 41 PAG personenbezogene Daten über Bürger von Amts wegen oder auf Antrag an Private weitergeben.

Bei meinen **Querschnittskontrollen** habe ich diesbezüglich keine Anhaltspunkte für eine unzulässige Weitergabe an Dritte gefunden.

Bei einigen **Beschwerdefällen** hatte ich allerdings den Verdacht, daß personenbezogene Daten von Bürgern in unzulässiger Weise zu **privaten Zwecken** verwendet wurden. Die meisten Fälle ließen sich freilich nicht vollständig aufklären. In einem Fall steht zwar fest, daß die Halterdaten von Unfallfahrzeugen von einem Polizeibeamten unbefugt abgefragt und an Kfz-Händler weitergegeben wurden. Der Täter konnte jedoch von der Justiz nicht zweifelsfrei ermittelt werden.

Nur folgender Fall konnte geklärt werden: Ein Dienststellenleiter hat im Kriminalaktennachweis **gespeicherte Erkenntnisse zur Person eines Bankkunden an den Leiter des Kreditinstituts** weitergegeben. Der Vorfall hatte seinen Ausgangspunkt in einer dienstlichen Beobachtung eines Polizeibeamten. Dieser überprüfte ein ihm verdächtig erscheinendes Fahrzeug in der Nähe der Bank und stellte den Fahrzeughalter durch Abfrage im Zentralen Verkehrsinformationssystem (ZEVIS) fest. Die anschließende Abfrage des Fahrzeughalters im Kriminalaktennachweis ergab, daß gegen den Halter ein Strafverfahren wegen eines Wirtschaftsdelikts geführt, aber eingestellt worden war. Diese Erkenntnis teilte der Beamte seinem Dienststellenleiter mit. Dieser setzte sich daraufhin mit dem Filialleiter der Bank in Verbindung und machte ihn auf die „Vorbelastung" seines Besuchers aufmerksam.

Die Weitergabe polizeilicher Erkenntnisse an den Zweigstellenleiter der Bank war unzulässig, weil die Voraussetzungen des Art. 41 Abs. 1 PAG nicht vorlagen. Es würde entschieden zu weit gehen, die Warnung einer Bank vor einem möglichen Betrüger als polizeiliche Aufgabe anzusehen, wenn gegen diese Person ein Strafverfahren wegen Betrugs gelaufen ist. KAN-Speicherungen allein dürfen nicht dazu verwendet werden, möglicherweise gefährdete Dritte vor dem Gespeicherten zu warnen. Dies wäre allenfalls bei einer **konkreten Gefährdung** zulässig, die sich aus zusätzlichen Umständen ergeben müßte. Es kann auch keine Rede davon sein, daß, wie das PAG verlangt, die Warnung zur Wahrung schutzwürdiger Interessen Einzelner erfolgte und kein Grund zu der Annahme bestand, daß der Betroffene ein schutzwürdiges Interesse an dem Ausschluß der Übermittlung hatte. Denn der Bankkunde hatte umgekehrt ein Interesse daran, daß Eintragungen zu seiner Person im KAN, von denen er übrigens gar nichts wußte, nicht an Dritte weitergeben werden. Im übrigen wurden die KAN-Eintragungen auf die Beschwerde des Petenten gelöscht.

Ich habe diese grobe Verletzung des informationellen Selbstbestimmungsrechts des Betroffenen beanstandet und das zuständige Polizeipräsidium gebeten, solchen Verstößen durch entsprechende Belehrungen der Polizeibeamten entgegenzuwirken.

4.4 Allgemeine Prüfungen

Allgemeine Querschnittsprüfungen habe ich bei folgenden Polizeibehörden vorgenommen:
- Landeskriminalamt
- Polizeipräsidium Mittelfranken mit dem Ballungsraum Nürnberg/Fürth/Erlangen
- Polizeipräsidium Niederbayern/Oberpfalz mit der Polizeidirektion Landshut
- Polizeipräsidium Oberbayern mit der Polizeidirektion Ingolstadt
- Polizeipräsidium München

Die Ergebnisse der Kontrollen lassen den Schluß zu, daß die Polizei die gesetzlichen und polizeiinternen Bestimmungen zur Datenerhebung und Datenverarbeitung **im wesentlichen beachtet**, und Datenschutzverstöße die Ausnahme sind. Verstöße beruhen in erster Linie auf der unzutreffenden Beurteilung von Einzelsachverhalten, auf früheren Organisationsmängeln, auf erst zum Ende des Berichtszeitraums gelösten Einzelproblemen (Berücksichtigung des Ausgangs des Justizverfahrens) und auf technischen und fachlichen Umstellungsschwierigkeiten (z.B. Einführung der Datei „PSV").

4.4.1 Kriminalaktennachweis (KAN)

Meine Prüfungen des KAN haben gezeigt, daß die Polizei die in früheren Tätigkeitsberichten dargestellten datenschutzrechtlichen Erfordernisse bei der Führung der Datei und der Kriminalakten **weitgehend beachtet**.

Im Berichtszeitraum habe ich insbesondere folgende Bereiche des KAN vor Ort stichprobenartig geprüft:
- Beleidigung
- Ladendiebstahl
- Betrug
- Straftaten eines ausgewählten Monats
- bestimmte Straftatenschlüssel (z.B. 000005 = sonstige polizeiliche Gefahrenabwehr)
- bestimmte Zeitpunkte für Aussonderungsprüfung
- bestimmte Erfassungszeiträume
- Speicherungen mit sog. personenbezogenen Hinweisen (z.B. Prostitution)
- Speicherungen mit sog. KAN-Merkern (z.B. gewohnheitsmäßige Tatbegehung)
- Speicherungen von Kindern
- Speicherungen von über 70jährigen Tatverdächtigen

Die einzelnen Speicherungen, die nach den o.g. Kriterien ausgewählt wurden, habe ich nach folgenden **Maßstäben** geprüft:

- Sind die Speicherungen im KAN zur Gefahrenabwehr oder Strafverfolgung **erforderlich**? Läßt sich die Erforderlichkeit aus den polizeilichen Unterlagen nachvollziehen?
- Ist die gewählte **Speicherungsebene** (Regional-, Landes-, Bundes-KAN) erforderlich?
- Ist die **Dauer** der Speicherung auf das erforderliche Maß beschränkt? Insbesondere: Sind die durch Art. 38 Abs. 2 Satz 3 PAG vorgegebenen Prüfungstermine eingehalten? Sind in Fällen geringerer Bedeutung kürzere Fristen festgesetzt?
- Wurden die Prüfungstermine durch automatisierte Vergabe oder – wie von mir gefordert – durch **Sachbearbeiterentscheidung** festgesetzt?
- Wurde der **Ausgang des Strafverfahrens** berücksichtigt, insbesondere in Fällen, in denen der Tatverdacht entfallen war, eine Straftat nicht vorlag oder sich der Tatvorwurf geändert hatte? Ist die Prüfung durch den Sachbearbeiter **dokumentiert** und ist ggf. die Löschung, Fristverkürzung oder Aktualisierung des Tatvorwurfs vorgenommen worden?
- Sind bei der Speicherung von **Kindern** und über **70jährigen** Tatverdächtigen die besonderen Anforderungen an die Speicherung berücksichtigt?
- Sind die Vergabe von **KAN-Merkern** und die damit verbundene Speicherung im Bundes-KAN sowie die Vergabe **personengebundener Hinweise** zutreffend und in den polizeilichen Unterlagen nachvollziehbar **dokumentiert**?

In Einzelfällen war die Erforderlichkeit der Speicherung nicht nachvollziehbar. Die Nachprüfung durch

die speichernde Polizeibehörde führte teilweise zur Löschung der personenbezogenen Daten. So in einem Fall, in dem sich beide Beschuldigte wegen Beleidigung, Bedrohung und Verleumdung gegenseitig angezeigt hatten. Zu den Auseinandersetzungen war es im Rahmen von Mietstreitigkeiten gekommen. Die Ermittlungsverfahren wurden von der Staatsanwaltschaft gemäß §§ 374, 376 StPO eingestellt, da **kein öffentliches Interesse** an der Erhebung der öffentlichen Klage wegen der Privatklagedelikte bestand.

Grundsätzlich bin ich der Auffassung, daß die Speicherung von Privatklagedelikten, insbesondere von Beleidigungen, im KAN nur dann in Betracht kommt, wenn nach den besonderen Umständen der Tat nach kriminalpolizeilicher Erfahrung mit einer gewissen Wahrscheinlichkeit anzunehmen ist, daß die Angelegenheit in der Zukunft für die Gefahrenabwehr oder Strafverfolgung eine Rolle spielen wird. Diesen Grundsatz hat die Polizei in den von mir geprüften Fällen nicht immer in ausreichendem Maße berücksichtigt, mit der Folge, daß beispielsweise Bürger aufgrund von gegenseitigen Anzeigen fünf Jahre und länger als potentielle Straftäter gespeichert waren.

Bei einer Polizeidirektion besteht die Anweisung, **Ladendiebstähle im Wert unter 10,- DM** (ohne erschwerende Umstände und beim „Ersttäter") nicht im KAN zu erfassen. Die Stichproben aus dem KAN zu Ladendiebstählen bestätigten dies. Ich halte diese Praxis für sachgerecht. Eine Speicherung solcher Vorgänge in der Datei PSV erscheint mir ausreichend.

Die Speicherungen mit sog. **personengebundenen Hinweisen** (z.B. Prostitution) und die Speicherungen mit sog. **KAN-Merkern** (z.B. gewohnheitsmäßige Tatbegehung) waren aus datenschutzrechtlicher Sicht nicht zu beanstanden. In einigen Fällen fehlte die Prüfung der Erforderlichkeit der weiteren Speicherung unter Berücksichtigung des Verfahrensausgangs. Eine ausreichende Begründung für die weitere Speicherung durch die Polizei steht noch aus.

Speicherungen zur **sonstigen polizeilichen Gefahrenabwehr** (Straftatenschlüssel 000005) habe ich bei der von mir daraufhin überprüften Polizeidirektion nicht festgestellt.

Bei einer Polizeidirektion war die **Festlegung des Aussonderungsprüfdatums** überwiegend nur aus dem KAN selbst, nicht aber auch aus der Kriminalakte ersichtlich. Nur in wenigen Fällen war eine **Sachbearbeiterentscheidung** vorgenommen und in der Kriminalakte dokumentiert worden. Auf Nachfrage wurde mir erklärt, daß die sog. Sachbearbeiterentscheidung bei der Polizeidirektion erst seit ca. 1990 praktiziert werde. Vorher sei statt dessen eine zentrale Prüfung durch Bedienstete der Aktensammlung durchgeführt worden. Dieses Verfahren erklärt den bei der Prüfung gewonnenen Eindruck, daß bis 1990 **nicht in ausreichendem Umfang von der Möglichkeit der Fristverkürzung Gebrauch gemacht,** vielmehr bei Fristvergabe mitunter zu schematisch verfahren wurde. Allein richtig ist es, die Entscheidung über die Festlegung des Aussonderungsprüfdatums dem Sachbearbeiter zu übertragen. Nur der Sachbearbeiter hat die erforderliche Sachnähe und damit die ausreichende Kenntnis des konkreten Einzelfalles, die es ihm erlaubt, die Dauer der Speicherung sachgerecht und einzelfallbezogen festzulegen.

Bei der Hälfte der Vorgänge, die von einer Polizeidirektion im **Regional-KAN** erfaßt waren, wurde eine 10jährige Aussonderungsprüffrist vergeben. Dieser Anteil ist, berücksichtigt man die Tatsache, daß es sich um Regional-KAN-Speicherungen handelt, relativ hoch. Im Regional-KAN werden nach den Grundsätzen des KAN-Systems im wesentlichen nur „Fälle von geringerer Bedeutung" gespeichert, für die nach Art. 38 Abs. 2 PAG eine verkürzte Prüffrist zu vergeben ist. Vor diesem Hintergrund ist zu vermuten, daß bei dieser Polizeidirektion nicht im ausreichenden Maße von der Vergabe **verkürzter Aussonderungsprüffristen** Gebrauch gemacht wird.

Vermutlich ist dies auf die oben beschriebenen **früheren Organisationsmängel** zurückzuführen. Die Polizeidirektion hat mir auf meinen Vorhalt hin zugesagt, die Regional-KAN-Bestände auf die Verkürzung der Aussonderungsprüffristen hin zu überprüfen. 10-jährige Aussonderungsprüffristen für Vorgänge von „geringerer Bedeutung" werden auf fünf Jahre verkürzt. Die nachgeordneten Dienststellen wurden angewiesen, die Erforderlichkeit der Vergabe verkürzter Aussonderungsprüffristen für die o.g. Vorgänge stärker zu berücksichtigen oder evtl. ganz auf eine Einstellung solcher Vorgänge in den Regional-KAN zu verzichten. Das Ergebnis der Überprüfung durch die Polizeidirektion liegt mir noch nicht vor.

In Einzelfällen fehlte in der Kriminalakte **die Mitteilung des Verfahrensausgangs** durch die Staatsanwaltschaft. Bei einer Polizeidirektion, die zum Überprüfungszeitpunkt 253 Vorgänge mit Tatzeit Januar 1990 gespeichert hatte, habe ich das Fehlen der Mitteilung in 5 Fällen festgestellt. Dies ist zum Teil darauf zurückzuführen, daß einzelne Verfahren zum Prüfungszeitpunkt noch nicht abgeschlossen waren. Warum die Mehrzahl der Vorgänge ohne Hinweis blieb, konnte noch nicht abschließend geklärt werden.

Soweit sich die Mitteilung über den Verfahrensausgang in der Kriminalakte befand, waren zum Teil **die Kenntnisnahme** von der Mitteilung und die **Entscheidung über die weitere Speicherung** durch den

Sachbearbeiter **nicht dokumentiert**. Es ist daher nicht auszuschließen, daß bei dieser Polizeidirektion die Mitteilungen der Staatsanwaltschaft über den Verfahrensausgang unbesehen zur Kriminalakte gelegt werden und keinerlei Überprüfungen stattfinden.

Bei einer Polizeidirektion habe ich die Speicherung von 209 **Kindern** im KAN festgestellt. Das sind 0,72 % der Gesamtspeicherung im KAN. Von besonderem Interesse für meine Prüfung waren Speicherungen von Kindern, die zum Zeitpunkt der ersten Tat noch nicht 10 Jahre alt waren. Nach Nr. 3.4.1 der Dienstanweisung KAN werden **Kinder unter 10 Jahre** grundsätzlich nicht in den KAN aufgenommen. Die Speicherung eines 7jährigen Mädchens war aufgrund der besonderen Umstände des Einzelfalles nicht zu beanstanden. Ein 7jähriger Junge wurde wegen eines gemeinsam mit einem 17jährigen verübten Fahrraddiebstahls gespeichert. Sowohl sein Verhalten während der Tat als auch seine Angaben während seiner Anhörung durch den sachbearbeitenden Beamten hatten nach dessen Einschätzung eine für dieses Alter ungewöhnliche Dreistigkeit erkennen lassen. Es sei deshalb zum Erfassungszeitpunkt zu erwarten gewesen, daß der Junge erneut auffällig werden würde. Wegen der besonderen Umstände des Einzelfalls erscheinen diese Speicherungen angesichts der nachvollziehbar negativen Prognosen für das weitere Verhalten vertretbar.

4.5 Prüfung der Rechtmäßigkeit von Abfragen im Informationssystem der Bayer. Polizei (Protokolldatei)

Die bei der Polizei gespeicherten Daten unterliegen wegen ihrer besonderen Sensibilität strengen Sicherheitsvorkehrungen, die unbefugte Abfragen ausschließen sollen. In Bayern werden **alle Abfragen der Polizei** in einer polizeilichen Landes- (IBP) oder Bundes- (INPOL)datei, wie z.B. Kriminalaktennachweis, Fahndungsdatei, Haftdatei, Erkennungsdienstdatei, sowie in den über IBP erschließbaren nichtpolizeilichen Dateien (derzeit: Einwohnerdateien, Ausländerzentralregister, Zentrales Verkehrsinformationssystem) in einer beim Landeskriminalamt geführten **Protokolldatei** für ein Jahr festgehalten. Gespeichert werden die persönliche Kennung des abfragenden Polizeibeamten (soweit dieser nur Datenübermittler ist wie bei Telefon- oder Funkanfragen, zusätzlich die Identifizierungsdaten des die Abfrage Veranlassenden), der Suchbegriff (z.B. Namen und/oder Geburtsdatum der abgefragten Person), die Kennung der abgefragten Datei, der Zeitpunkt der Abfrage, die Nummer des Datenendgerätes und bei Abfragen in ZEVIS der Grund der Abfrage.

Die Protokolldatei dient u.a. dem **Zweck**, innerhalb eines Jahres die Rechtmäßigkeit der Abfragen kontrollieren zu können und so einem möglichen Mißbrauch von Bürgerdaten durch unbefugte Abfragen und anschließende Nutzung zu unzulässigen Zwecken vorzubeugen.

Zu diesem Zweck ist die Protokolldatei **in unregelmäßigen Zeitabständen ohne konkreten Anlaß stichprobenartig auszuwerten**: Die protokollierten Dateiabfragen, die als Online-Abfragen getätigt werden, sind im nachhinein auf ihre Rechtmäßigkeit zu überprüfen. Darüber hinaus können **bei Verdacht des Datenmißbrauchs weitere Kontrollen** notwendig werden.

4.5.1 Anlaßabhängige Auswertungen der Protokolldatei

In einigen Fällen war es erforderlich, verdachtsbezogene Kontrollen durchzuführen:

1. Presseveröffentlichungen legten den Verdacht nahe, daß ein ehemaliger Parteifunktionär, der als Polizeibeamter tätig ist, nach parteiinternen Auseinandersetzungen verschiedene polizeiliche Auskunftssysteme nach Speicherungen über seine Kontrahenten ohne dienstliche Veranlassung abgefragt hat, um sich weitere „Munition" zu verschaffen. Ich bin diesem Verdacht nachgegangen und habe hierzu die beim Landeskriminalamt geführte Protokolldatei auswerten lassen. Die Auswertung führte zum Ergebnis, daß unter der persönlichen Kennung des Polizeibeamten Personen im Kriminalaktennachweis sowie im polizeilichen Fahndungsbestand abgefragt worden waren. Die datenschutzrechtliche Prüfung, ob die Abfragen dienstlich veranlaßt waren oder mißbräuchlich durchgeführt wurden, konnte ich im Hinblick auf ein in diesem Zusammenhang gegen den Polizeibeamten eingeleitetes staatsanwaltschaftliches Ermittlungsverfahren wegen Weitergabe von Dienstgeheimnissen noch nicht abschließen.

2. Auf einen weiteren Fall, bei dem der Verdacht der unzulässigen Nutzung polizeilicher Informationssysteme bestand, bin ich bereits in meinem 13. Tätigkeitsbericht kurz eingegangen:

   Ein Autohändler hatte vermutet, die Polizei liefere unzulässigerweise Daten an seine Konkurrenten, weil diese nach Verkehrsunfällen immer wieder Daten über Halter und Kraftfahrzeuge erhalten hätten und diese für Geschäftsanbahnungen (Kaufangebote) nutzen würden.

   Die Auswertung der Protokolldatei ergab in diesem Fall, daß unter der Stammnummer eines Polizeibeamten innerhalb von etwa 20 Minuten neun ZEVIS-Abfragen durchgeführt worden waren. Dienstliche Gründe für die Abfrage waren nicht ersichtlich. Im Ermittlungsverfahren wegen Verstoßes gegen Art. 34 BayDSG ließ sich der Be-

amte dahingehend ein, daß ein anderer Polizeibeamter unter seiner Stammnummer die Abfragen vorgenommen haben müsse. Er selbst sei während der fraglichen Zeit nicht im Dienst gewesen. Die Staatsanwaltschaft stellte das Verfahren – auch wegen fehlenden Strafantrags – nach § 170 Abs. 2 StPO ein. Da die Abfragen über Fernschreiber (nicht über APC) durchgeführt worden waren, wozu neben der Stammnummer nur ein allen Polizeivollzugsbeamten bekanntes Kennwort einzugeben war, nicht hingegen ein persönliches Paßwort, habe diese Einlassung nach Auffassung der Staatsanwaltschaft nicht widerlegt werden können.

Dieses Ergebnis ist aus Sicht des Datenschutzes unbefriedigend. Wenn gegen Protokollierungen mit Erfolg eingewandt werden kann, daß die persönliche Stammnummer von unbefugten Dritten mißbraucht worden sei, dann sind Protokollierungen von ZEVIS-Abfragen weitgehend wertlos, weil sich jeder Polizeibeamte gegen den Vorwurf einer unzulässigen ZEVIS-Abfrage solcher Ausreden bedienen und damit der Nachweis einer unzulässigen ZEVIS-Abfrage nicht geführt werden kann.

Auf meine Einwände hin hat die Staatsanwaltschaft das Ermittlungsverfahren gegen den Beamten wieder aufgenommen, inzwischen aber erneut eingestellt, weil der Einwand des Beschuldigten, ein Dritter habe unter seiner Stammnummer abgefragt, nicht zu widerlegen sei. Wenn auch der Täter nicht mit einer für die Anklageerhebung ausreichenden Sicherheit ermittelt werden konnte, so ist doch der **objektive Verstoß gegen Datenschutzvorschriften durch unberechtigte Abfragen** aus dem polizeilichen Informationssystem festzustellen. Dieser Verstoß wurde **erleichtert** durch das bereits beschriebene, unter dem Gesichtspunkt der Datensicherheit unzureichende, damalige Anmeldeverfahren. In Kenntnis dieser **Sicherheitslücke** wäre es geboten gewesen, einen Mißbrauch durch organisatorische Maßnahmen soweit wie möglich auszuschließen. Solche Maßnahmen waren bei der betroffenen Polizeiinspektion nicht in ausreichendem Umfang getroffen.

Den Verstoß gegen den Datenschutz durch unberechtigte Abfragen des polizeilichen Informationssystems und unzureichende Maßnahmen der Datensicherung habe ich beanstandet. Inzwischen ist bei der betroffenen Polizeiinspektion, wie übrigens auch bei den übrigen bayerischen Polizeiinspektionen, der Fernschreiber durch einen APC ersetzt worden. **Abfragen erfordern nun zusätzlich die Eingabe eines persönlichen Kennwortes** und sind damit zuverlässiger einem bestimmten Polizeibeamten zuzuordnen.

4.5.2 Anlaßunabhängige Auswertungen der Protokolldatei in verschiedenen DV-Anwendungen (EWO, AZR, KAN, Fahndung, ZEVIS)

Wie mehrmals angekündigt, habe ich im Berichtszeitraum mehrere Auswertungen vorgenommen.

Vom Landeskriminalamt habe ich mir hierzu für einzelne Präsidialbereiche Ausdrucke der Protokolldaten der ersten 1000 Abfragen eines aktuellen Datums der Dateien
- Einwohnermeldeamtsverfahren (EWO)
- Ausländerzentralregister (AZR)
- Kriminalaktennachweis (KAN)
- Fahndung
- Zentrales Verkehrsinformationssystem (ZEVIS)

fertigen lassen. Aus den protokollierten Abfragen habe ich stichprobenartig einzelne Datensätze an die Polizeipräsidien mit der Bitte weitergegeben, die mit Hilfe der individuellen Stammnummer identifizierten Polizeibeamten nach dem Grund der Abfrage in der Datei zu befragen. Die Befragung sollte klären, ob die gesetzlichen Voraussetzungen für die Dateiabfrage vorgelegen haben, und der jeweilige Polizeibeamte die Daten zur Erfüllung polizeilicher Aufgaben verwendet hat.

Bei der Protokollauswertung zeigte sich, daß von der nachträglichen Befragung der Polizeibeamten nur dann genaue Auskünfte erwartet werden können, wenn die Beamten **innerhalb kürzester Zeit nach der Computerabfrage**, etwa innerhalb einer Woche, zur Stellungnahme aufgefordert werden. Andernfalls können sie sich an einen Vorgang, z.B. eine Abfrage nach dem Halter eines Kraftfahrzeuges im Zentralen Verkehrsinformationssystem ZEVIS, mitunter nicht mehr hinreichend genau erinnern.

Die Auswertung der Protokollierung hat keinen Anhalt für einen Datenmißbrauch durch die kontrollierten Stellen ergeben.

Bei der Auswertung hat sich allerdings auch gezeigt, daß das Protokollierungssystem den Veranlasser einer Abfrage nicht sicher ausweist, wenn die Abfrage über eine sog. Terminalzentrale erfolgt. In diesem Fall wird das persönliche Kennwort des in der Zentrale arbeitenden Bediensteten in das System eingegeben, außerdem die Stammnummer des Veranlassenden oder eine entsprechende Kennung. Eine Identifizierung des die Abfrage über Telefon oder Funk Veranlassenden ist damit nicht sicher gewährleistet. Ich habe das Innenministerium gebeten, für derartige Fälle geeignete Sicherungsmaßnahmen vorzusehen.

Die Protokollauswertungen sind nicht nur für den Landesbeauftragten für den Datenschutz, sondern auch für die zur Kontrolle ausgewählten Polizeidienststellen mit gewissem **Arbeits- und Zeitaufwand** verbunden. Deshalb habe ich die Polizeipräsi-

denten gebeten, ihren Mitarbeitern den Sinn und Zweck solcher Auswertungen zu verdeutlichen, insbesondere daß solche Auswertungen von keinem konkreten Mißbrauchsverdacht ausgelöst werden, sondern als Routinekontrollen zu verstehen sind.

4.6 Bayerisches Landeskriminalamt (BLKA)

Wie in den Vorjahren habe ich wieder eine mehrtägige Prüfung der „Arbeitsdatei PIOS Innere Sicherheit" (APIS) durchgeführt. Nach mehrjähriger Pause habe ich auch wieder die Arbeitsdatei „Organisierte Kriminalität" (ADOK) überprüft.

4.6.1 Arbeitsdatei PIOS Innere Sicherheit (APIS)

Ansatzpunkte der Kontrolle waren wie in den letzten Jahren bestimmte Erfassungszeiträume, Aussonderungsprüfdaten, bestimmte Personengruppen, verschiedene Straftatbestände wie z.B. **Beleidigung, Sachbeschädigung, Nötigung** und andere Suchbegriffe wie Golfkrise, Palästinenser, Rechtsanwälte, Weltwirtschaftsgipfel, Kernenergie, Wiederaufbereitung und Volkszählung. Ferner wurde eine Liste mit ausgewählten Namen auf Bestand in APIS überprüft.

Besonderes Augenmerk habe ich im Hinblick auf die Schwierigkeit der Bewertung der APIS-Relevanz auf die Speicherung sog. **anderer Personen** (Kontaktpersonen) und sog. **anderer Straftaten** (keine typischen Staatsschutzdelikte) gerichtet.

Die Prüfung führte zu folgendem Ergebnis:
- In einigen Fällen war auch mit Hilfe der dazugehörigen Unterlagen die **APIS-Relevanz** einzelner Speicherungen nicht zu erkennen.
- Die **Speicherungsdauer** war in minderschweren Fällen auf drei oder fünf Jahre verkürzt worden. Dies ist zu begrüßen.

Speicherung sog. anderer Straftaten

Einer Übersicht des BLKA konnte ich für das Jahr 1991 einen Anteil der sog. anderen Straftaten am Gesamtbestand der Datei APIS von 51,72 % entnehmen. „Andere Straftaten", also nichttypische Staatsschutzdelikte, können u.a. wegen des Motivs des Täters gespeichert werden, wenn
- über die aus dieser Straftat gewonnenen Erkenntnisse hinaus **Anhaltspunkte für eine staatsfeindliche Zielsetzung** des Täters vorliegen oder
- Anhaltspunkte dafür vorliegen, daß der Täter **weitere** Straftaten zum Erreichen staatsfeindlicher Ziele begehen wird.

Dabei handelt es sich um Straftaten, die u.a. gegen die freiheitliche demokratische Grundordnung, den Bestand und die Sicherheit des Bundes oder eines Landes gerichtet sind oder die eine ungesetzliche Beeinträchtigung der Amtsführung von Mitgliedern verfassungsmäßiger Organe des Bundes oder eines Landes zum Ziele haben (im einzelnen vgl. 12. TB Nr. 4.5).

Diese Voraussetzungen lagen bei den geprüften Speicherungen wegen Hausfriedensbruchs und Sachbeschädigung vor: So war z.B. die Teilnehmerin an einer „Fortbildungsveranstaltung" von Rechtsextremisten in einer leerstehenden Scheune wegen Hausfriedensbruchs in APIS gespeichert. Eine Speicherung wegen Sachbeschädigung betraf einen Beschuldigten, der zur Tatzeit zusammen mit drei Mittätern vor einer Sammelunterkunft für Asylbewerber bei zwei abgestellten Pkw mit Steinen die Scheiben eingeworfen hatte.

Speicherung von Kontaktpersonen

Die von mir geprüften Speicherungen „anderer Personen" betrafen **Kontaktpersonen** zu Personen, die zur polizeilichen Beobachtung ausgeschrieben waren. Die näheren Umstände des Kontaktes rechtfertigen die Annahme, daß die Speicherung zur Aufklärung oder vorbeugenden Bekämpfung der in § 138 StGB genannten Straftaten oder einer Straftat nach § 129 StGB erforderlich ist.

Ausgewählte Suchbegriffe

Zu den Begriffen „Volkszählung" und „Palästinenser" waren zum Überprüfungszeitpunkt keine Datensätze in APIS gespeichert. Zu den Begriffen Golfkrise, Weltwirtschaftsgipfel, Kernenergie, Wiederaufbereitung waren Speicherungen vorhanden, die aber – mit Ausnahme des fehlenden Verfahrensausgangs – den datenschutzrechtlichen Anforderungen genügten. Unbedenklich waren auch die von mir geprüften Personendatensätze, die unter dem Begriff „Rechtsanwälte" gespeichert waren. Die Speicherungen betrafen in allen Fällen „Gefährdete".

Die Prüfung bestätigte erneut, daß sich die Datei APIS in datenschutzrechtlicher Hinsicht in einem guten Zustand befindet. Dies ist nicht zuletzt auf den zentralen Einsatz von erfahrenen Sachbearbeitern im BLKA bei der Bewertung der APIS-Relevanz von Vorgängen zurückzuführen.

4.6.2 Arbeitsdatei „Organisierte Kriminalität – ADOK"

Vor dem Hintergrund der wachsenden Bedrohung durch die verschiedenen Erscheinungsformen der Organisierten Kriminalität (OK) richtete das BLKA 1990 die Arbeitsdatei „Organisierte Kriminalität – ADOK" ein. Mit der Datei sollen **Anhaltspunkte** für **Zusammenhänge** zwischen einzelnen Straftaten bzw. Tätern und **Verbindungen** mit dem dazugehörenden Umfeld aus den Deliktsbereichen organisierter Krimi-

nalität, z.B. Rauschgifthandel und -schmuggel, Falschgeldherstellung und -vertrieb, Waffenhandel und -schmuggel, Erpressung, erkannt und aufgezeigt werden. Die Datei soll
- das Erkennen von ok-relevanten Personen, Personen- gruppierungen, Institutionen, Objekten und Sachen,
- das Erkennen von Verflechtungen/Zusammenhängen,
- das Erkennen krimineller Organisationen,
- das Zusammenführen von Erkenntnissen zu gleichgelagerten Tätergruppen und Straftaten sowie
- das Ausscheiden unbedeutender Informationen

unterstützen. Es handelt sich um eine beim BLKA eingerichtete zentrale **Arbeitsdatei**, die dem frühzeitigen Erkennen von ok-relevantem Täterverhalten (sog. Indikatoren) schon im Vorfeld strafbarer Handlungen und somit auch der Verhütung von Straftaten dient.

In ADOK werden nach der Errichtungsanordnung neben **Beschuldigten** und **Verdächtigen** auch Personen gespeichert, die mit dem vorgenannten Personenkreis **in Verbindung** stehen **und** deren Verhalten den Verdacht begründet, strafbare Handlungen dieses Personenkreises zu fördern oder zu unterstützen. Ferner werden auch **gefährdete** und **geschädigte** Personen gespeichert, wenn ok-verdächtige Tatsachen bzw. Sachverhalte vorliegen.

In Stichproben habe ich daher insbesondere
- die Relevanz der Speicherungen – mit Schwerpunkt „andere Personen" – im Hinblick auf Zugehörigkeit oder Bezug zum sog. OK-Milieu,
- die Speicherungsdauer sowie
- die Dokumentation der Verlängerung von Speicherungen in den schriftlichen Unterlagen geprüft.

Verstöße gegen den Datenschutz habe ich, abgesehen von geringfügigen **Mängeln bei der Dokumentation** der Begründung der Fristverlängerung einer Speicherung, nicht festgestellt. Betroffene wurden nur dann als „andere Personen" gespeichert, wenn zwar keine ausreichenden tatsächlichen Anhaltspunkte für eine aktive Beteiligung an einer ok-relevanten Straftat vorlagen, die Umstände des Einzelfalles aber ihre Verbindung zu dem Kreis der „Verdächtigen" nahelegten.

4.7 Polizeipräsidium München

Beim Polizeipräsidium München habe ich
- die Datei „Münchner Wirtschaftsgipfel 1992 – MWG'92" und
- die Datei „Straftäter bei Sportveranstaltungen und gewalttätige Jugendgruppen" geprüft.

Ferner hat der Datenschutzbeirat die Datei „Polizeiliche Sachbearbeitung/Vorgangsverwaltung-Verbrechensbekämpfung (PSV)" des Polizeipräsidiums besichtigt.

4.7.1 Datei Münchner Wirtschaftsgipfel 1992 – MWG'92

Aus Anlaß des Weltwirtschaftsgipfels 1992 in München richtete das Polizeipräsidium München eine Datei ein, in der die für die Bewältigung der polizeilichen Aufgaben im Zusammenhang mit diesem Großereignis erforderlichen Daten gespeichert wurden. Die Datei wird im automatisierten Verfahren „Besondere Einsatzlagen" (BELA) betrieben.

BELA dient zur Unterstützung der polizeilichen Tätigkeit bei besonderen Einsatzlagen, insbesondere
- zur Sammlung und Verknüpfung von Erkenntnissen für die Beurteilung der Lage, z.B. über geplante Störungen des MWG,
- zum Erkennen von Zusammenhängen bei der Planung und Durchführung von Einsätzen und sonstigen Maßnahmen,
- zur Strafverfolgung und Gefahrenabwehr,
- zur Dokumentation von Vorgängen und
- zur Bereitstellung logistischer und einsatztaktischer Daten.

Folgende Personengruppen können in eine BELA-Datei aufgenommen werden:
- Beschuldigte im Strafverfahren,
- Betroffene im Ordnungswidrigkeitenverfahren,
- einer Straftat oder Ordnungswidrigkeit Verdächtige,
- potentielle Störer,
- gefährdete und geschädigte Personen,
- Anzeigeerstatter,
- Zeugen,
- Hinweisgeber,
- Auskunftspersonen,
- Adressaten von polizeilichen Maßnahmen,
- Beschäftigte der Polizei und
- Verantwortliche/Beauftragte.

Besondere Einsatzlagen wie der Münchner Wirtschaftsgipfel, bei denen mit Störungen und Zwischenfällen zu rechnen ist, erfordern besondere Vorbereitungen. Im Vorfeld eines Einsatzes sind auch diejenigen Informationen zu sammeln, denen aufgrund einer Einzelbetrachtung zunächst nur geringe Bedeutung zugemessen wird, die aber in der Gesamtschau durch die Verknüpfung mit anderen Erkenntnissen mögliche polizeirelevante Auswirkungen mit Handlungsbedarf, insbesondere zur Gefahrenabwehr, erkennen lassen. Beispielsweise kann erst die Kenntnis vom mehrfachen Auftreten einer bestimmten Person zu verschiedenen Gelegenheiten und Anlässen Rückschlüsse auf eine mögliche Störereigenschaft zulassen. Aber auch die Speicherung von Nichtstörern, wie z.B. Verantwortliche bestimmter Beherbergungs-

betriebe, kann zur Lagebeurteilung und Dokumentation notwendig sein, wenn ihnen aufgrund von Informationen sicherheitsrelevante Bedeutung zukommen kann.

Aus datenschutzrechtlicher Sicht können deshalb an die Speicherungen in dieser Datei nicht die gleichen Anforderungen bezüglich Erforderlichkeit und polizeilicher Relevanz gestellt werden wie z.B. an Aktennachweissysteme. Zum Ausgleich ist der Datenbestand nach der Errichtungsanordnung grundsätzlich **spätestens 6 Monate nach Beendigung des Einsatzes zu löschen**. Eine einmalige Verlängerung der Aufbewahrung um 6 Monate ist möglich, wenn Tatsachen die Annahme rechtfertigen, daß die Daten für die polizeiliche Aufgabenerfüllung weiter benötigt werden. In Fällen von geringerer Bedeutung werden Daten auch bereits vor Fristablauf gelöscht.

Bei meiner Prüfung habe ich mich im wesentlichen auf die Kontrolle der **Erforderlichkeit der Speicherungen für die polizeiliche Aufgabenerfüllung** beschränkt. Diese war bei den von mir stichprobenweise geprüften Datensätzen gegeben. In einem Fall war eine Person nach einem mißverständlichen Katalogschlagwort bewertet. Die entsprechende Speicherung wurde berichtigt.

Nach Ablauf der Speicherungsfrist werde ich mich von der **Löschung** des Datenbestandes der Datei überzeugen und eine eventuelle weitere Nutzung der gespeicherten Daten auf ihre Zulässigkeit hin überprüfen.

Es ist davon auszugehen, daß **Teilmengen der Datei in andere polizeiliche Dateien oder Karteien übernommen** werden, wenn sie für die weitere polizeiliche Aufgabenerfüllung benötigt werden. In erster Linie kommt die Aufnahme von Vorgängen in den Kriminalaktennachweis (KAN) in Betracht, beispielsweise wenn wegen eines bestimmten Ereignisses Strafanzeige bei der Staatsanwaltschaft erstattet wurde.

Personen, gegen die wegen des Verdachts von Straftaten im Zusammenhang mit dem Weltwirtschaftsgipfel Ermittlungsverfahren eingeleitet und deren Verfahren nach § 170 Abs. 2 StPO eingestellt werden, werden nach Mitteilung des Polizeipräsidiums nur dann im KAN oder anderen INPOL-Anwendungen gespeichert werden, wenn die Prüfung des Einzelfalles die Notwendigkeit der Speicherung ergibt. Dabei werde ein entsprechend strenger Maßstab angelegt.

4.7.2 Datei „Straftäter bei Sportveranstaltungen und gewalttätige Jugendgruppen"

Die Datei, die ich im 13. Tätigkeitsbericht (Nr. 4.11) bereits kurz dargestellt habe, wurde im Berichtsjahr geprüft. Sie ersetzt eine bisher beim Polizeipräsidium München im Kommissariat für gruppen- und jugendtypische Gewaltdelikte (K 124) geführte Handkartei, die dem polizeilichen Informationsbedürfnis wegen fehlender Auswertungsmöglichkeit nicht mehr genügte.

Die Datei dient als überregionale aktuelle Informationssammlung,
- der Aufklärung und Aufhellung des relevanten Tätermilieus, des Täterverhaltens und der Täterabsichten sowie dem Erkennen von Brennpunkten, um Straftaten und sonstige Störungen der öffentlichen Sicherheit oder Ordnung zu verhindern (Gefahrenabwehr);
- der Erfassung von Straftätern, verdächtigen und gewaltbereiten Gruppenmitgliedern, deren Aufenthaltsorten und Tatbegehungsweisen, um **Zusammenhänge** zu erkennen und so **Ermittlungsansätze** zur Straf- und Ordnungswidrigkeitenverfolgung zu gewinnen.

Neben dem zuständigen Kommissariat des Polizeipräsidiums München sind seit kurzem auch Dienststellen des Polizeipräsidiums Oberbayern, welche die gleiche Aufgabe haben, eingabe- und zugriffsberechtigt. Dieser erweiterte Zugriff ist wegen der hohen Mobilität des betroffenen Personenkreises, insbesondere im Großraum München, aus datenschutzrechtlicher Sicht nicht zu beanstanden.

Gespeichert werden Personen,
- gegen die wegen Straftaten und Ordnungswidrigkeiten im Zusammenhang mit **Ausschreitungen bei Sportveranstaltungen ermittelt** wurde,
- die unter das Jugendgerichtsgesetz (JGG) fallen und gegen die wegen **jugend- und gruppentypischer Aggressionsdelikte** (insbesondere Vandalismus, alle Formen der vorsätzlichen Körperverletzung, Sittlichkeitsdelikte, Raub und räuberische Erpressung, Tötungsdelikte) **ermittelt** wurde,
- die aufgrund glaubwürdiger Hinweise oder polizeilicher Ermittlungen **gewalttätigen Gruppierungen** oder deren engerem Umfeld zuzuordnen, aber in strafrechtlicher Hinsicht noch nicht in Erscheinung getreten sind.

Während die Speicherung von Personen der beiden erstgenannten Gruppen an den konkreten Verdacht einer Straftat oder Ordnungswidrigkeit und damit an ein förmliches Verfahren anknüpft, hängt die Speicherung von Personen der letztgenannten Gruppe **von wesentlich vager formulierten Voraussetzungen ab**. Wegen der dabei möglicherweise auftretenden Schwierigkeiten und im Hinblick darauf, daß es sich um Vorgänge im mehr oder weniger weiten Vorfeld strafrechtlich relevanten Verhaltens handelt, habe ich diese Speicherungen zum Schwerpunkt meiner Prüfung gemacht.

Die Kontrolle ergab, daß die gespeicherten Personen **nachvollziehbar gewalttätigen Gruppierungen zuzuordnen** sind. Ich habe festgestellt, daß die für die Speicherung notwendigen Erkenntnisse ausreichend waren, um eine Zuordnung der Betroffenen zu gewalttätigen Gruppierungen oder deren engerem Umfeld zuzulassen. Die Erkenntnisse waren in Einsatzberichten von polizeilichen Fan-Betreuern festgehalten. Ergänzend standen diese Rede und Antwort. Die Speicherungen stützten sich ausnahmslos auf konkrete polizeiliche Feststellungen. Die Fundstellen sollten allerdings zur Erleichterung der Nachvollziehbarkeit der Speicherung in der Datei nachgewiesen werden.

Wer sich immer wieder an berüchtigten Örtlichkeiten eines Fußballstadions aufhält und sich dort mit als gewalttätig bekannten Schlägern trifft, denen Fußball in einem Fußballstadion Nebensache ist, kann nachvollziehbar dem Umfeld gewalttätiger Gruppierungen zugerechnet werden. Gleiches gilt für diejenigen „Fans", die sich bei Auswärtsspielen ihrer Mannschaft bei der Anreise und während des Aufenthalts inmitten von gewalttätig bekannten Gruppen bewegen. Dabei konnte ich mich davon überzeugen, daß die Fan-Betreuer der Polizei bei ihrer Bewertung einen strengen Maßstab anlegen.

Gespeichert waren auch zwei Brüder, die vom Fenster der elterlichen Wohnung aus einen Bierfahrer mit dem Luftgewehr beschossen und ihn verletzten. Auch wenn es sich hier um eine recht kleine „Gruppierung" handelt, habe ich die Annahme der Polizei, daß in der Tat Ansätze zu jugend- und gruppentypischer Aggression zu erkennen seien, für noch vertretbar gehalten.

Ferner gespeichert waren drei jugendliche Räuber, die einer alten Frau die Handtasche geraubt hatten. Wegen des besonders raffinierten Vorgehens hat die Polizei zu Recht angenommen, daß die Speicherung dieses Vorgangs zur Aufklärung künftiger Überfälle beitragen kann.

4.8 Kriminalaktennachweis (KAN) und Polizeiaufgabengesetz (PAG)

Wie im 13. Tätigkeitsbericht (Nr. 4.7) dargestellt, muß der KAN als eine der wichtigsten Informationssammlungen für die Bewältigung der polizeilichen Aufgaben an die Vorgaben des neuen Polizeiaufgabengesetzes angepaßt werden. Ich habe deshalb mit dem Innenministerium verhandelt mit dem Ziel

- der Reduzierung der im KAN zu speichernden Vorgänge,
- der Verkürzung der Speicherungsfristen in Fällen geringerer Bedeutung und
- der Einschränkung der sog. Fristverlängerungsautomatik.

4.8.1 Reduzierung der im KAN zu speichernden Vorgänge

Ich hatte unter eingehender Begründung (13. TB 4.7.1) vorgeschlagen, zur **Entschlackung des KAN von nicht erforderlichen Speicherungen** nachfolgende Delikte künftig nicht mehr in die Datei aufzunehmen:

- Privatklagedelikte, soweit von der Staatsanwaltschaft das öffentliche Interesse an der Anklageerhebung verneint wird,
- alle Fahrlässigkeitsdelikte,
- Ordnungswidrigkeiten, die bisher nur auf der Ebene der Polizeidirektionen, also regional gespeichert wurden.

Das **Innenministerium** hat sich gegen den völligen Verzicht auf die Speicherung dieser Straftaten und Ordnungswidrigkeiten ausgesprochen.

1. **Privatklagedelikte**

   Das Innenministerium hat die Beibehaltung der Speicherung von Privatklagedelikten im KAN in den Fällen, in denen die Staatsanwaltschaft das öffentliche Interesse an der Anklageerhebung verneint hat, wie folgt begründet:

   Die Privatklagedelikte, insbesondere Körperverletzung (auch gefährliche Körperverletzung), Bedrohung sowie Sachbeschädigung, gehörten zu den relevanten Delikten der **Straßenkriminalität.** Es handle sich auch um **Gewaltdelikte**, die in bedeutendem Maße die **öffentliche Sicherheit und Ordnung** und das **individuelle Sicherheitsgefühl** der Bevölkerung berührten. Die Begehung solcher Straftaten sei häufig aufsehenerregend und ziehe nicht selten ein erhebliches **Medienecho** nach sich. Der Speicherung im KAN komme deshalb unter dem Aspekt der Gefahrenabwehr eine wichtige Rolle zu. Sie sei häufig das entscheidende **Hilfsmittel für die Polizei zur Verdachtsgewinnung gegen Aggressionstäter**.

   Das Innenministerium war nur bereit, für die Privatklagedelikte als Straftaten von geringerer Bedeutung generell eine fünfjährige Aussonderungsprüffrist festzulegen.

   Diese Argumente betreffen spezielle Privatklagedelikte, deren Nichtspeicherung ich aber nicht gefordert habe.

   Es geht bei meinem Vorschlag nicht darum, die gesamten als Privatklagedelikte bezeichneten Delikte von der Speicherung im KAN auszunehmen. Selbstverständlich sollen auch künftig die Delikte der Straßenkriminalität und die Gewaltdelikte, die in bedeutendem Maße die öffentliche Sicherheit und Ordnung und das Sicherheitsgefühl der Be-

völkerung berühren, im KAN gespeichert werden. Denn ich gehe davon aus, daß in den Fällen der Straßenkriminalität und der die öffentliche Sicherheit berührenden Gewaltkriminalität die Staatsanwaltschaft das öffentliche Interesse an der Anklageerhebung stets bejahen wird. Bagatelldelikte hingegen, deren Verfolgung die Staatsanwaltschaft nicht der Mühe wert findet und dem Verletzten überläßt, wie Nachbarquerelen, kleinliche Auseinandersetzungen, die die Betroffenen unter sich ausmachen können und den das öffentliche Wohl vertretenden Staatsanwalt nicht interessieren, sind kaum geeignete Anhaltspunkte zur Verdachtsgewinnung. Im übrigen werden auch bisher schon Privatklagedelikte nicht im KAN gespeichert, wenn der Verletzte nach Belehrung durch die Polizei und Hinweis auf den Privatklageweg auf eine Anzeigenerstattung verzichtet. Vorgänge, die von Polizei oder Staatsanwaltschaft unter dem Gesichtspunkt des öffentlichen Interesses, das die öffentliche Sicherheit umfaßt, als Lappalien bewertet werden, sollten gleich behandelt und in beiden Fällen nicht in den KAN aufgenommen werden. Ich werde deshalb meine Forderung weiterhin vertreten.

2. **Fahrlässigkeitsdelikte**

Das Innenministerium verteidigt die Speicherung aller Fahrlässigkeitsdelikte (ausgenommen die Antragsdelikte) im KAN mit dem Hinweis, hinter manchen Fahrlässigkeitsdelikten würden sich **vorsätzliche Delikte verbergen**. Würden die Speicherungen unterbleiben, so gingen Fahndungsansätze bei künftigen vorsätzlichen Straftaten verloren.

Dieser mögliche Ausnahmefall rechtfertigt es aber nicht, Fahrlässigkeitsdelikte generell zu speichern, sondern nur in den Fällen, in denen nach den Erfahrungen der Polizei die Speicherung für die Aufklärung späterer vorsätzlicher Straftaten von Bedeutung sein kann.

Die Begründung des Innenministeriums ist, berücksichtigt man, daß Antragsdelikte nicht gespeichert werden, auch **nicht folgerichtig**. Würde sie zutreffen, müßten auch Antragsdelikte gespeichert werden, auf deren Speicherung die Polizei jedoch bereits verzichtet, weil sie im KAN als unnützer Ballast empfunden werden. Fahrlässigkeitsdelikte haben im übrigen im Regelfall so wenig kriminellen Gehalt, daß sie kaum als Ansatzpunkt für spätere Ermittlungen wegen vorsätzlicher Taten geeignet erscheinen. Zu begrüßen ist, daß Fahrlässigkeitsdelikte nunmehr in der Regel nur noch als Straftaten von geringerer Bedeutung mit einer Aussonderungsprüffrist von fünf Jahren gewertet werden. Meine Forderung, die Fahrlässigkeitsdelikte im KAN künftig nicht mehr zu speichern, erhalte ich aufrecht.

3. **Speicherung von Ordnungswidrigkeiten**

Das Innenministerium begründet die Beibehaltung der Speicherung von Ordnungswidrigkeiten, die bisher im regionalen KAN erfaßt werden, mit den Erfahrungen der Praxis. Danach sei in gefahrgeneigten und sicherheitssensiblen Bereichen wie z.B. Umweltschutz, Brandschutz, Gewerberecht, Waffen- und Sprengstoffrecht die Speicherung von vorsätzlich begangenen Ordnungswidrigkeiten für präventive und repressive Zwecke unverzichtbar. Häufig hänge es von Zufällen ab, ob eine schwerwiegende Folge einer gefährlichen Handlung eintrete oder nicht und damit ein Ordnungswidrigkeiten- oder Straftatbestand verwirklicht werde. Angesichts dieser Gegebenheiten möchte ich den Vorschlag nicht weiterverfolgen.

4.8.2 Verkürzung der Aussonderungsprüffristen

Für den KAN sind Termine festzulegen, an denen spätestens überprüft werden muß, ob die suchfähige Speicherung von Daten weiterhin erforderlich ist (Prüfungstermine). In Fällen von geringerer Bedeutung sind **kürzere Fristen** festzusetzen (Art. 38 Abs. 2 Satz 4 PAG). Diese Regelung ist Ausfluß des Grundsatzes der Verhältnismäßigkeit.

Ich hatte gefordert, in der Errichtungsanordnung zum KAN oder in der Dienstanweisung **weitere Fallgruppen** zu bilden, die in der Regel als solche von geringerer Bedeutung anzusehen seien. Dabei kämen neben Straftaten von geringem Unrechtsgehalt auch kriminologische Gesichtspunkte wie geringe kriminelle Energie, Ersttäter, geringe Wiederholungsgefahr in Betracht.

Das Innenministerium hat neben den bereits bisher in der Dienstanweisung KAN als Straftaten von geringerer Bedeutung bezeichneten Privatklagedelikte alle Fahrlässigkeitsdelikte in dieser Weise eingestuft und bei diesen Delikten eine fünfjährige Aussonderungsprüffrist vorgesehen. Im übrigen hat es jedoch meine Forderung nicht aufgegriffen: In der Dienstanweisung KAN sei bereits unter Zugrundelegung einer verallgemeinernden Interessenabwägung festgelegt, daß alle **Privatklagedelikte**, Speicherungen von Fällen der **Gefahrenabwehr** und alle **Ordnungswidrigkeiten** als Fälle geringerer Bedeutung zu behandeln seien.

Diese Ausführungen lassen keine Bereitschaft des Innenministeriums erkennen, den polizeilichen Sachbearbeitern zur Auslegung des Begriffs „Fall von geringerer Bedeutung" ausreichende Hinweise an die Hand zu geben. Denn es kann keinem Zweifel unterliegen, daß dieser Begriff mit den oben erwähnten

Privatklage- und Fahrlässigkeitsdelikten sowie den Fällen der Gefahrenabwehr und den Ordnungswidrigkeiten nicht ausgeschöpft ist. Ich werde deshalb bei künftigen KAN-Prüfungen besonders darauf achten, ob das Gebot kürzerer Speicherung in Fällen geringerer Bedeutung beachtet wird.

4.8.3 Einschränkung der Fristverlängerungsautomatik

Die Prüfungsfrist, nach deren Ablauf spätestens überprüft werden muß, ob die suchfähige Speicherung der KAN-Eintragung weiterhin erforderlich ist, beginnt regelmäßig mit dem Ende des Jahres, in dem das letzte Ereignis erfaßt worden ist (Art. 38 Abs. 2 Satz 5 PAG). Die Speicherungsdauer bereits gespeicherter Ereignisse kann sich bei Zuspeicherung eines weiteren Ereignisses verlängern.

Ich hatte vorgeschlagen, daß zumindest bei **Vermißtenfällen** oder **Suizidversuchen** von einer Verlängerung der Speicherungsdauer bereits gespeicherter Erkenntnisse abgesehen wird.

Das **Innenministerium** ist dem Vorschlag nicht gefolgt. Die Fristenautomatik ergebe sich aus Art. 38 Abs. 2 Satz 5 PAG. Für eine Sonderregelung bei Vermißtenfällen und Suizidversuchen sah es keinen Anlaß.

Ich halte es hingegen nach wie vor für unverhältnismäßig, wenn beispielsweise ein im KAN gespeicherter Diebstahl, der wenige Monate vor der Löschung steht, nur deshalb um weitere 5 Jahre länger gespeichert wird, weil der Betroffene zwischenzeitlich vermißt war oder einen Selbstmordversuch unternommen hat. Außerdem betrifft Art. 38 Abs. 2 Satz 5 PAG nur die Speicherung von Straftaten, nicht aber von Vermissungen oder Suizidversuchen.

4.9 Verlängerung der Speicherfristen bei Kontaktpersonen in der Arbeitsdatei PIOS Innere Sicherheit (APIS)

Die Datei APIS soll als Hilfsmittel zur **Verhütung oder Aufklärung von Straftaten mit staatsfeindlicher Zielsetzung** dienen. Dabei handelt es sich u.a. um Straftaten, die gegen die freiheitliche demokratische Grundordnung, dem Bestand und die Sicherheit des Bundes oder eines Landes gerichtet sind oder die eine ungesetzliche Beeinträchtigung der Amtsführung von Mitgliedern verfassungsmäßiger Organe des Bundes oder eines Landes zum Ziele haben.

Neben Beschuldigten im Rahmen eines strafrechtlichen Ermittlungsverfahrens und verdächtigen Personen werden auch **andere Personen** in APIS gespeichert, wenn sie **in Verbindung mit den erstgenannten stehen und zureichende tatsächliche Anhaltspunkte die Annahme rechtfertigen**, daß die Erfassung **zur Aufklärung oder vorbeugenden Bekämpfung der in § 138 des Strafgesetzbuches (StGB) genannten Straftaten oder einer Straftat nach § 129 StGB erforderlich ist.**

Die Dauer der Speicherung von Daten solcher „anderen Personen" betrug in Fällen der §§ 129 und 129 a StGB bisher 3 Jahre. Die Erfahrungen in den vergangenen Jahren haben jedoch gezeigt, daß diese Speicherdauer nicht ausreicht, die kriminellen Lebensläufe von Mitgliedern krimineller Vereinigungen, insbesondere von Terroristen, frühzeitig zu erkennen. Die Innenministerkonferenz hat deshalb beschlossen, daß die Speicherungsdauer „anderer Personen" in Fällen der §§ 129 und 129 a StGB (Bildung einer kriminellen bzw. terroristischen Vereinigung) längstens 5 Jahre beträgt. Die Nutzung dieser 5-Jahresfrist bleibt den Ländern und dem Bund unbenommen. Bayern macht von der Verlängerung der Speicherungsfrist Gebrauch.

Die von der Innenministerkonferenz beschlossene Verlängerung der Speicherungsfrist halte ich für angemessen und verhältnismäßig. Angesichts der Fahndungsdefizite bei der Aufklärung insbesondere terroristischer Straftaten, die auf die für diesen Bereich typische konspirative Vorgehensweise zurückzuführen sind, ist die Notwendigkeit einer Verlängerung der Speicherungsfrist nachvollziehbar. Die **Erfahrungen der Polizei** bei der Bekämpfung von Straftaten nach §§ 129, 129 a StGB müssen in die Regelungen zu APIS einfließen können und dürfen nicht durch einen überzogenen Datenschutz unberücksichtigt bleiben.

4.10 Datei „Polizeiliche Sachbearbeitung/Vorgangsverwaltung-Verbrechensbekämpfung" (PSV)

Im 13. Tätigkeitsbericht (Nr. 4.9) habe ich die PSV als künftige Grundlage des Informationssystems der bayerischen Polizei (IBP) vorgestellt, die Maßstäbe aufgezeigt, an denen die Datei zu messen ist und eine vorläufige Bewertung abgegeben.

Die PSV dient
- der innerdienstlichen Verwaltung des Vorgangs,
- als Ermittlungshilfe für Zwecke der Verbrechensbekämpfung,
- der Gewinnung von Entscheidungshilfen für innerbetriebliche Aufgaben,
- der Bereitstellung von einsatztaktischen und logistischen Daten,
- der Bereitstellung von Informationselementen für andere IBP-Anwendungen,
- der Dokumentation.

Das Innenministerium hat die Errichtungsanordnung PSV inzwischen in **überarbeiteter Fassung** bekannt-

gegeben. Im Berichtsjahr habe ich die PSV eines Polizeipräsidiums kontrolliert.

Zur Errichtungsanordnung (EA) in der geltenden Fassung und zu den Kontrollfeststellungen ist folgendes anzumerken:

1. **Fehlende Umsetzung der Errichtungsanordnung vom 28.11.1991**

   Die Kontrolle der PSV des Polizeispräsidiums gestaltete sich deshalb schwierig, weil das Präsidium wegen Gegenvorstellungen beim Innenministerium die Errichtungsanordnung noch nicht umgesetzt hatte.

2. **Fehlende Protokollierung**

   Die aus der Sicht des Datenschutzes erforderliche **Protokollierung von Abfragen** in der Datei PSV findet derzeit nicht statt. Sie ist zwar in der Errichtungsanordnung noch nicht vorgesehen, jedoch wegen der umfangreichen Zugriffsmöglichkeiten aus prophylaktischen Gründen, aber auch zur effektiven Datenschutzkontrolle aus meiner Sicht unverzichtbar. Es ist deshalb dringend notwendig, daß die technischen Voraussetzungen für eine Protokollierung mit Nachdruck geschaffen werden und die Protokollierung realisiert wird.

   Das Innenministerium hat gegen die Protokollierung eingewandt, sie erfordere entweder leistungsfähigere Hardware und damit erheblichen Aufwand oder die Leistungsfähigkeit lasse wegen der für die Protokollierung benötigten Speicherkapazität spürbar nach. Es hat aber angekündigt, daß es dazu demnächst einen Lösungsvorschlag unterbreiten wird.

3. **Fehlende Löschung**

   Die EA PSV sieht vor, daß die Speicherungen personenbezogener Daten in der Datei PSV nach bestimmten Fristen zu überprüfen und zu löschen sind. Nach Auskunft des Innenministeriums wird die polizeiliche Vorgangsverwaltung in Bayern derzeit entsprechend den Bestimmungen der Errichtungsanordnung umgestellt.

   Bei dem von mir geprüften Polizeipräsidium wurde zum Zeitpunkt der Prüfung eine solche Löschung nicht vorgenommen. Die Daten der Datei PSV werden 18 bis 36 Monate nach ihrer Speicherung auf ein sog. Archivband überspielt und abgelegt. Die so „archivierten" Daten stehen zwar in der Regel für Auskünfte im sog. Online-Verfahren nicht mehr zur Verfügung. Nur mit besonderem Aufwand ist es möglich, die „archivierten" Daten wieder einzuspielen und auszuwerten. Dies kommt – wie mir erklärt wurde – allenfalls zur Aufklärung von Kapitalverbrechen in Betracht. Für diese „Archivierung" sehe ich jedoch im Polizeiaufgabengesetz keine Grundlage. Es sind deshalb sobald wie möglich die erforderlichen Löschungen durchzuführen. Die Behörde hat die Löschung ab 1993 zugesagt.

   Das Innenministerium hat darauf hingewiesen, daß es sich bei der „Archivierung" der Vorgangsdaten nach 18 bis 36 Monaten um eine rein technisch und organisatorisch bedingte Übergangsmaßnahme gehandelt habe. Die nach der Errichtungsanordnung für die Datei PSV vorgeschriebenen Aussonderungsprüffristen von 5 bzw. 10 Jahren seien durch die Übergangsmaßnahme nicht berührt gewesen. Die fristgerechte Aussonderung von Vorgangsakten sei nach den geltenden Richtlinien gewährleistet gewesen.

4. **Aussonderung der schriftlichen Unterlagen**

   Nach der EA PSV sind die zu den in der Datei PSV gespeicherten Daten bestehenden schriftlichen Unterlagen **mit der Löschung der Daten in der PSV auszusondern**. Da eine Löschung von Daten der Datei PSV derzeit nicht stattfindet, werden auch keine Unterlagen ausgesondert.

5. **Verbindung zwischen PSV und KAN**

   Eine Verbindung dergestalt, daß bei einer Löschung der personenbezogenen Daten zu einer bestimmten Person im KAN auch die entsprechende Qualifizierung der Person als Beschuldigter **in der Datei PSV automatisch gelöscht** wird, gibt es nicht.

   Nach der EA/DA PSV sind Strafanzeigen gegen bekannte Täter und andere Vorgänge, die für Zwecke der Verbrechensbekämpfung aufgenommen wurden und bei denen der Vorgang oder Tatverdächtige/Betroffene in der Datei PSV und im KAN nachgewiesen wurden, entsprechend der für den KAN festzulegenden Aussonderungsfristen (Art. 38 Abs. 2 PAG) zu löschen, im Regelfall nach 10 Jahren, bei Jugendlichen nach 5 Jahren, bei Kindern nach 2 Jahren seit dem Ende des Erfassungsjahres. Es ist deshalb **sicherzustellen, daß diese Fristen auch für die Löschung in der PSV eingehalten werden**, soweit nicht eine längere Aufbewahrung zum Zwecke der Vorgangsverwaltung und Dokumentation geboten ist. Während dieser längeren Aufbewahrung darf die Speicherung nur mehr für Zwecke der Vorgangsverwaltung und Dokumentation zur Verfügung stehen. Jedenfalls muß bei Löschung im KAN auch die Qualifizierung der Person als Beschuldigter in der Datei PSV gelöscht werden – entwe-

der automatisch oder durch Organisation gesichert. Der Betroffene darf danach bei Recherchen in der PSV nicht mehr als Beschuldigter angezeigt werden.

6. **Statusänderung bei entfallenem Tatverdacht ohne praktische Folgen**

Ist der Tatverdacht gegen eine Person entfallen, so sind die Daten nach Art. 38 Abs. 2 Satz 2 PAG zu löschen. Dies gilt für den KAN wie für die PSV. Werden die Daten aber zum Zwecke der Vorgangsverwaltung oder Dokumentation in der PSV weiter gespeichert, darf sich aus der weiteren Speicherung zumindest die bisherige, inzwischen aber weggefallene Eigenschaft als Beschuldigter oder Verdächtiger, **nicht** mehr ergeben.

In diesem Fall wird beim kontrollierten Polizeipräsidium der Zusatz: „Keine Straftat" eingegeben.

Dieses Verfahren bedarf noch einer abschließenden datenschutzrechtlichen Überprüfung. Ich habe Zweifel, ob die Interessen des weiterhin Gespeicherten ausreichend geschützt sind. Von der Möglichkeit, die nach Art. 38 Abs. 2 Satz 2 PAG zu löschenden Daten, die jedoch noch für Zwecke der Vorgangsverwaltung/Dokumentation gebraucht werden, für Zwecke der Verbrechensbekämpfung zu sperren und den Zugriff nur noch für Zwecke der Vorgangsverwaltung und Dokumentation zu erlauben, wird kein Gebrauch gemacht noch ist diese Möglichkeit in der EA vorgesehen mit der Folge, daß diese Daten jederzeit nach wie vor in der PSV auch zur Verbrechensbekämpfung bereitstehen.

Da mit der Datei PSV verschiedene Zwecke gleichzeitig oder nacheinander verfolgt werden (Vorgangsverwaltung, Dokumentation, Verbrechensbekämpfung), entwickelt sie sich zu einem wirksamen Instrument der polizeilichen Informationsverarbeitung. Dies bedeutet aber auch gleichzeitig, daß die Auswirkungen dieser Datei auf die darin gespeicherten Personen auch weiterhin einer intensiven Kontrolle bedürfen.

4.11 Sonstige polizeiliche Dateien

GAST-Dateien

GAST-Dateien (Dateien zur Gefahrenabwehr und Verfolgung von Straftaten und Ordnungswidrigkeiten) stellen eine der Anwendungen des APC-Verfahrens der bayerischen Polizei dar.

Die Dateien dienen der Erleichterung der polizeilichen Aufgabenerfüllung. In eine GAST-Datei können personenbezogene Daten von Beschuldigten, Verdächtigen, Betroffenen, Verantwortlichen (Art. 7 PAG), Verursachern (Art. 8 PAG) und Geschädigten aufgenommen werden, soweit dies zur **Abwehr von Gefahren** für die öffentliche Sicherheit oder Ordnung oder zur **Durchführung und Dokumentation von Straf- und Bußgeldverfahren** erforderlich ist. Diese Daten werden nach polizeilicher Beurteilung zur **Feststellung von Tatzusammenhängen** und zur **Zuordnung sichergestellter Gegenstände** benötigt. Art und Umfang der zu speichernden Daten richten sich nach den Erfordernissen des jeweiligen Verfahrens.

Die Polizei machte im Berichtszeitraum von der Möglichkeit, Dateien auf der Grundlage der Errichtungsanordnung GAST einzurichten, regen Gebrauch. Es handelt sich dabei um folgende lokale Anwendungen, die bei verschiedenen Polizeidienststellen eingesetzt sind:
- Fahrraddateien
- Dateien für Gaststätten und Beherbergungsbetriebe
- Dateien zur Überwachung der Prostitution
- Dateien zur Bekämpfung der Rauschgiftkriminalität
- Dateien zur Erfassung von Nachtlokalen
- Dateien zur Bekämpfung des Kfz-Diebstahls
- verschiedene Dateien zur Bekämpfung von Erscheinungsformen der Organisierten Kriminalität.

Die **Genehmigung** zur Einrichtung der Dateien im Einzelfall ist den Polizeipräsidenten übertragen worden. In meinem 12. Tätigkeitsbericht habe ich bereits darauf hingewiesen, daß mit der allgemein gehaltenen Beschreibung des Dateizweckes eine **unüberschaubare und damit letztlich unkontrollierbare Anzahl von Dateien** entstehen kann. Da die Dateien jedoch zum Datenschutzregister gemeldet werden, bin ich über ihren Einsatz unterrichtet und habe die Möglichkeit zur datenschutzrechtlichen Prüfung der Dateien.

Bei einer Polizeidirektion habe ich eine **Überprüfung von GAST-Dateien** durchgeführt:

Karteikasten AG-Pkw

Mit Hilfe dieser Datei werden von einer Arbeitsgruppe Pkw-Diebstähle durch unbekannte Täter erfaßt. Gespeichert werden nur Kfz-Kennzeichen, Fahrzeugdaten und Modus-Operandi-Daten, nicht hingegen Geschädigten- oder evtl. Täterdaten. Datenschutzrechtliche Bedenken gegen die Speicherungen in dieser Datei haben sich nicht ergeben.

Rauschgiftdatei (GIFTI)

In dieser Datei wurden nur „KAN-relevante" Sachverhalte und Personen gespeichert. Neben personenbezogenen Daten und Angaben zur Begehungsweise der jeweiligen Straftat besteht zusätzlich ein Feld

„Konsumentenart", in dem festgelegt wird, in welchen Bereichen der Rauschgiftkriminalität die jeweilige Person aufgetreten ist (z.B. Haschisch).

Nachdem bei der Polizeidirektion die Arbeitsdatei Rauschgift (ADR) betriebsbereit ist, wurde die Datei GIFTI gelöscht.

Prostituiertendatei (PROSI)

Gespeichert werden
- Personen, die im KAN im Zusammenhang mit Prostitution erfaßt sind,
- Prostituierte, deren Gesundheitszeugnisse kontrolliert wurden und
- Frauen (Modelle), die sich kurzzeitig zur Ausübung der Prostitution im Direktionsbereich aufhalten und ihren Aufenthalt der Polizei mitteilen.

Datenschutzrechtliche Bedenken gegen Speicherungen in dieser Datei haben sich nicht ergeben. Insbesondere ist die **Doppelspeicherung** im KAN und in PROSI zulässig, weil in PROSI zusätzliche Daten gespeichert werden können, die für die Aufgabenerfüllung der Polizei erforderlich sind.

Datei Gaststättenbetriebe (GASTS)

In dieser Datei wird jede **Gaststättenerlaubnis** erfaßt, die der Polizei vom Gewerbeamt mitgeteilt wird. Erfaßt werden insbesondere **Erlaubnis- und Konzessionsdaten** (Sperrstunde etc.). Ein entsprechendes Feld „Vermerk", in dem **freitextliche Begriffe** eingegeben werden können, ist nicht recherchierbar. Nach Darstellung der Polizeidirektion enthält dieses Feld keine „belastenden Vermerke". Stichproben ergaben nichts Gegenteiliges.

Eine **Grundlage** für die Datei „Gaststättenbetriebe" sehe ich für den Normalfall in der Errichtungsanordnung GAST nicht. Zur Bereitstellung von Daten zur Überprüfung der Sperrstunde oder der Erlaubnisauflagen steht die Datei „Polizeiliche Sachbearbeitung/Vorgangsverwaltung-Verbrechensbekämpfung (PSV)" zur Verfügung. Ziffer 3.1.4 der Errichtungsanordnung PSV sieht ausdrücklich die Aufnahme von Daten über Gaststätten vor. Das zuständige Polizeipräsidium hat mir zugesagt, eine Umstellung der Datenbestände zu prüfen, wenn im Präsidialbereich die Datei PSV eingerichtet ist.

Datei Nachtlokal (NACHA)

Mit Hilfe dieser APC-Anwendung sollen Zusammenhänge zwischen Konzessionsinhabern, Betreibern, Pächtern und Beschäftigten von Nachtlokalen im Bereich der Polizeidirektion hergestellt werden, soweit die Zusammenhänge für Zwecke der Verbrechensbekämpfung bedeutsam sind. Bisher war erst ein Nachtlokal erfaßt und personenbezogene Daten des Konzessionsinhabers und von Beschäftigten eingegeben worden.

Das zuständige Polizeipräsidium hat mir auf Nachfrage mitgeteilt, daß die Datei „NACHA" wegen zu geringen Datenaufkommens wieder gelöscht wurde. Aus diesem Vorgang ist für die Polizeipräsidien die Empfehlung abzuleiten, die Notwendigkeit und Zweckmäßigkeit von GAST-Dateien in regelmäßigen Abständen zu überprüfen.

4.12 Karteien

Prostituiertenkartei aktualisieren

Prostituierte werden im Kriminalaktennachweis unter der Rubrik „sonstige Gefahrenabwehr", in der Datei „Polizeiliche Sachbearbeitung/Vorgangsverwaltung-Verbrechensbekämpfung" und/oder in sonstigen Dateien des lokalen APC-Verfahrens automatisiert gespeichert.

Bei einzelnen Polizeidirektionen wird dieser Personenkreis auch noch in Karteiform erfaßt, insbesondere vom Sachgebiet „Sitte". Es ist nichts dagegen einzuwenden, wenn, wie ich bei der Kontrolle einer Polizeidirektion festgestellt habe, ein Sachgebiet, dessen spezielle Aufgabe die Überwachung der Prostitution ist, eine Prostituiertenkartei anlegt. Die Kartei dient der Sammlung und Auswertung von Erkenntnissen zur Überwachung der weiblichen Prostitution, der Bekämpfung der Begleitdelinquenz der Prostitution und der Bekämpfung von Geschlechts- und anderen übertragbaren Krankheiten, der Aufrechterhaltung der öffentlichen Sicherheit und Ordnung sowie der Unterbindung und Verfolgung von Straftaten und Ordnungswidrigkeiten. Die Kartei war allerdings seit längerem nicht mehr auf **Aussonderung nicht mehr benötigter Vorgänge** überprüft worden. Wenn eine Person fünf Jahre nicht mehr bei Ausübung der Prostitution angetroffen wird, ist die Karteikarte auszusondern. Meine Aufforderung, die gesamte Kartei zu aktualisieren, hat die Polizeidirektion zum Anlaß genommen, die Kartei aufzulösen und den aktuellen Bestand in die Datei „Polizeiliche Sachbearbeitung/Vorgangsverwaltung-Verbrechensbekämpfung" zu übernehmen.

Auch eine mehrfache Speicherung in verschiedenen Dateien/Karteien ist unter dem Gesichtspunkt der Gefahrenabwehr grundsätzlich zulässig, soweit es der spezielle Dateizweck zuläßt. Andererseits sollen aber unnötige **Doppelspeicherungen** unterbleiben, da hierbei die Gefahr besteht, daß die eine oder andere Datei nicht aktualisiert wird. Dies zeigte sich auch bei der kontrollierten Prostituiertenkartei.

4.13 Berücksichtigung des Verfahrensausgangs

Wie ein roter Faden zieht sich durch die Tätigkeitsberichte die Forderung des Datenschutzes nach **Berücksichtigung des Verfahrensausgangs** durch die Polizei bei der KAN-Speicherung. Wenn die Polizei eine Kriminalakte über eine Person anlegt, diese Person in die „Verdachtsdatei KAN" einstellt und dadurch für die Polizei landes- bzw. bundesweit abrufbar hält, dann ist der **Ausgang des Ermittlungsverfahrens** bei der Justiz für die weitere Speicherung im KAN und für die Fortführung der Kriminalakte von **erheblicher Bedeutung**. Die Polizei muß sich fragen, ob ihr **Verdacht** angesichts der Entscheidung der Justiz **noch berechtigt** und die weitere Speicherung zulässig ist.

Deshalb muß die Polizei von der Staatsanwaltschaft über den Ausgang des Strafverfahrens unterrichtet werden. Diese Forderung – die nicht nur für Strafsachen, sondern sinngemäß **auch für Ordnungswidrigkeiten** gilt – ist bei neueren Speicherungen berücksichtigt. Die Polizei fügt der an die Staatsanwaltschaft übersandten Strafakte ein Strafmitteilungsblatt bei, das nach Beendigung des Strafverfahrens ausgefüllt an die Polizei zurückgesandt wird.

Nach wie vor ungelöst war jedoch bisher die Frage: Was macht die Polizei, wenn die Staatsanwaltschaft mitteilt, das Ermittlungsverfahren sei von ihr nach **§ 170 Abs. 2 StPO** eingestellt worden, weil kein hinreichender Grund zur Erhebung der Klage vorliege. Diese Mitteilung kann bedeuten, die Staatsanwaltschaft habe zwar auch Anhaltspunkte für einen Tatverdacht gesehen, halte ihn aber zur Klageerhebung nicht für ausreichend. Hinter der Einstellung nach § 170 Abs. 2 StPO **kann aber auch** die Auffassung der Staatsanwaltschaft stehen, es bestehe **überhaupt kein Tatverdacht**. Jedenfalls im letzteren Fall muß die Polizei ihre Speicherung im KAN überprüfen, ob ihr polizeilicher Tatverdacht trotz der gegenteiligen Auffassung der Staatsanwaltschaft begründet ist. Wenn sie daran festhält, muß sie es **nachvollziehbar** begründen. Dies gilt insbesondere dann, wenn das Ermittlungsverfahren fast ausschließlich von der Staatsanwaltschaft geführt worden ist.

Um diese Überprüfung durchführen zu können, benötigt die Polizei über die Mitteilung des Ausgangs des Verfahrens hinaus einen **Hinweis, wenn der Tatverdacht entfallen ist**. Erst durch diesen Hinweis wird die Polizei in die Lage versetzt, mit vertretbarem Aufwand das Ergebnis des Justizverfahrens bei der Entscheidung über die weitere Speicherung personenbezogener Daten in polizeilichen Dateien und Akten zu berücksichtigen.

Dieser Auffassung hat sich der Bayerische Landtag angeschlossen. Mit Beschluß vom 15.05.1991 hat er die Staatsregierung gebeten, die Führung kriminalpolizeilicher Sammlungen dadurch zu verbessern, daß bei Verfahrenseinstellungen aus der Mitteilung hervorgeht, ob nach Auffassung der Staatsanwaltschaft damit auch der Tatverdacht entfallen ist.

Wie ich in meinem 13. Tätigkeitsbericht ausgeführt habe, zeichnete sich zu dieser Forderung zunächst keine Lösung ab. Ich habe mich deshalb im Zusammenhang mit der Eingabe eines Bürgers direkt an den Ministerpräsidenten gewandt mit der Bitte, mit Nachdruck darauf hinzuwirken, daß der Beschluß von der Staatsregierung zügig umgesetzt wird.

Aufgrund meiner nachhaltigen Vorstöße hat das Innenministerium am 3. September 1992 in Absprache mit dem Justizministerium eine Dienstanweisung über „Berichtigung, Löschung und Sperrung von Daten im Zusammenhang mit Entscheidungen der Justiz" erlassen, die den datenschutzrechtlichen Erfordernissen weitgehend Rechnung trägt. Danach hat die Polizei eine **Einzelfallprüfung der Notwendigkeit der weiteren Aufbewahrung der polizeilichen Unterlagen/Speicherung der Daten** stets vorzunehmen in Fällen der Verfahrensbeendigung

- durch Einstellung nach § 170 Abs. 2 StPO, wenn sich für die Justiz die **Unschuld des Beschuldigten** ergeben hat oder jeglicher begründete **Verdacht entfallen** ist, **und** dies dem Beschuldigten von der Staatsanwaltschaft nach Nr. 88 Satz 2 der Richtlinien für das Strafverfahren und das Bußgeldverfahren (RiStBV) **mitgeteilt** wurde. Ein Abdruck dieser Mitteilung mit Einstellungsbegründung wird der Polizei mit dem Strafmitteilungsblatt übersandt.

- durch **Einstellung nach § 206 b StPO**, weil sich während des Verfahrens das Strafrecht geändert hat und danach die Tat nicht mehr strafbar ist. In diesen Fällen ist auszusondern und zu löschen, es sei denn, daß ein Sachzusammenhang zu anderen Straftaten die weitere Aufbewahrung bzw. Speicherung rechtfertigt.

- durch ein **freisprechendes Urteil**. Ein Abdruck des Urteils wird der Polizei mit dem Strafmitteilungsblatt übersandt.

Wird in den vorgenannten Fällen von der aktenführenden Polizeidienststelle nach Prüfung entschieden, daß die

Aufbewahrung der Unterlagen/Speicherung der Daten weiterhin notwendig ist, so sind die hierfür maßgebenden Gründe kurz und formlos (z.B. „Tatverdacht besteht fort, weil ....." oder „Restverdacht weiterhin gegeben, weil .....") in der Kriminalakte zu vermerken (**Dokumentation der Gründe für weitere Speicherung**).

Durch die Dienstanweisung ist auch **ohne Antragstellung** des Beschuldigten gewährleistet, daß die Polizei die Informationen, die sie für ihre Entscheidung über den Wegfall des Tatverdachts (Art. 38 Abs. 2 PAG) benötigt, künftig erhalten wird. Dies gilt allerdings nur für die Fälle, in denen der Beschuldigte als solcher vernommen worden ist oder ein Haftbefehl gegen ihn erlassen worden war; dasselbe gilt, wenn er um einen Bescheid gebeten hat oder wenn ein besonderes Interesse an der Bekanntgabe ersichtlich ist (§ 170 Abs. 2 Satz 2 StPO). Ich habe deshalb das Innenministerium um Mitteilung gebeten, ob in der polizeilichen Praxis Fälle bekannt sind, in denen eine Speicherung personenbezogener Daten im Kriminalaktennachweis erfolgt, der Beschuldigte aber nicht als solcher vernommen worden ist oder aus anderen Gründen über die Einstellung nach § 170 Abs. 2 StPO nicht informiert wird. Gegebenenfalls sollte auch in diesen Fällen sichergestellt werden, daß die Polizei nach Abschluß des Verfahrens die notwendigen Informationen erhält, um die Erforderlichkeit der weiteren Speicherung überprüfen zu können.

4.14 Bürgereingaben

Ein Schwerpunkt meiner Tätigkeit im Polizeibereich war im Berichtszeitraum wieder die Beantwortung von Bürgeranfragen. Die Anzahl der Anfragen entsprach in etwa der des Vorjahres.

Die meisten Petenten befürchteten, sie könnten in **polizeilichen Auskunftssystemen gespeichert** sein. Grund für diese Annahme war vielfach die bloße Kontrolle beim Grenzübertritt oder im Straßenverkehr. Daneben wurde die **Löschung polizeilicher Speicherungen** und die **Vernichtung der Unterlagen** verlangt.

Soweit sich die Petenten nicht selbst unmittelbar an die Polizei wenden wollten, habe ich ihre Anliegen entweder durch schriftliche Anfragen bei den zuständigen Polizeidienststellen oder durch Kontrollen bzw. Einsichtnahmen vor Ort geklärt. In vielen Fällen erwiesen sich die Befürchtungen, daß Speicherungen vorhanden seien, als unbegründet. Soweit polizeiliche Speicherungen vorlagen, waren sie in den meisten Fällen datenschutzrechtlich nicht zu beanstanden. Nur in Einzelfällen mußte ich die Löschung von Daten und die Vernichtung von polizeilichen Unterlagen wegen fehlerhafter Bewertung durch die Polizei verlangen.

Als ein Beispiel für die nach meinen Prüfungserfahrungen meist unbegründeten Vorwürfe, die Polizei würde im Rahmen ihrer Aufgabenerfüllung in rechtlich unzulässiger Weise personenbezogene Daten erheben und nutzen sowie zuviele Daten in ihrem Informationssystem speichern, möchte ich folgenden Fall anführen: Bei der Beobachtung einer Demonstration, bei der aufgrund polizeilicher Erkenntnisse davon auszugehen war, daß das Schwerpunktthema dieser Veranstaltung der „Gegenkongreß" zum Münchner Weltwirtschaftsgipfel sein sollte, stellte ein Beamter in der näheren Umgebung des Kundgebungsortes einen Pkw fest, in dem sich von außen sichtbar ein Zettel befand, auf dem handschriftlich eine Reihe von Namen mit Vornamen und Telefonnummern stand. Neben den Namen befand sich auf dem Zettel noch eine handschriftliche Notiz, aus der sich ein Bezug zur laufenden Veranstaltung ableiten ließ. Es bestand also offensichtlich ein Zusammenhang zu der zu diesem Zeitpunkt an der genannten Örtlichkeit stattfindenden Veranstaltung und dem sich dort treffenden Personenkreis, der zumindest teilweise in Verdacht stand, Gewaltaktionen gegen den Weltwirtschaftsgipfel vorzubereiten. Da mit Störaktionen zum Weltwirtschaftsgipfel gerechnet werden mußte und eine Beteiligung von sog. links-extremen militanten Gruppierungen an der genannten Veranstaltung nicht auszuschließen war, notierte sich der Beamte die auf dem Zettel stehenden Namen.

Diese **Datenerhebung** war nicht zu beanstanden, da sie auf der Grundlage des geltenden Polizeirechts erfolgte. Die Polizei kann Daten von Personen erheben, wenn dies zur Gefahrenabwehr, insbesondere zur vorbeugenden Bekämpfung von Straftaten erforderlich ist. Aufgrund vorliegender Informationen konnte die Polizei davon ausgehen, daß an der Demonstration Sympathisanten von Extremisten teilnehmen würden. Sie konnte daher eine Gefahrensituation annehmen, deren Abwehr Aufgabe der Polizei (Art. 2 Abs. 1 PAG) ist. Dabei ist es für die polizeiliche Datenerhebung ausreichend, wenn vom Vorliegen einer abstrakten Gefahr ausgegangen werden kann. Zur Vorbereitung und Durchführung von vorbeugenden Maßnahmen gegen die Gefährdung der Sicherheit des Münchner Weltwirtschaftsgipfels war die Erhebung von Informationen im Vorfeld des Gipfels **notwendig**. Die Polizei mußte damit rechnen, daß sich unter den auf dem Zettel notierten Namen Personen befanden, die mit der Vorbereitung von schweren Störungen des Weltwirtschaftsgipfels befaßt waren. Die Sammlung von Informationen über die mögliche Teilnahme gewaltbereiter Gruppierungen an Aktionen am Rand des Weltwirtschaftsgipfels war im Hinblick auf die Erheblichkeit der zu befürchtenden Gefahren auch **verhältnismäßig**.

Die auf der Liste stehenden Namen wurden von der Polizei im Bundes-, Landes- und Regional-Kriminalaktennachweis (KAN) einschließlich Fahndungs- und Erkennungsdienstdateien **überprüft**. Dies konnte ich durch eine Auswertung der beim BLKA geführten Protokolldatei feststellen. Der **Abgleich** der festgestellten Namen mit den polizeilichen Dateien wurde auf der Grundlage des Art. 43 Abs. 1 PAG vorgenommen. Danach kann die Polizei Daten von

Personen mit dem Inhalt polizeilicher Dateien abgleichen, wenn Tatsachen die Annahme rechtfertigen, daß dies zur Erfüllung einer bestimmten polizeilichen Aufgabe erforderlich ist. Der Datenabgleich war hier erforderlich, um festzustellen, ob über die auf der Liste stehenden Personen, die als Teilnehmer von Aktionen am Rande des Weltwirtschaftsgipfels in Frage kamen, Erkenntnisse vorlagen, die für die Gefahrenabwehr von Bedeutung hätten sein können.

Die **Notizen** wurden nach dem Bericht des Innenministeriums **vernichtet**, nachdem die Namen überprüft worden waren. Ich habe mich selbst davon überzeugt, daß die auf dem Zettel im Auto enthaltenen Namen – abgesehen von der Protokolldatei – in keiner Datei oder Kartei im Zusammenhang mit der Veranstaltung von der Polizei gespeichert wurden.

5. Verfassungsschutz

5.1 Vorbemerkung

Die trotz Rückgangs der Bedeutung des orthodoxen Kommunismus fortbestehende Bedrohung durch den Linksextremismus, die zunehmende Militanz rechtsextremistischer Gruppierungen und unorganisierter Gruppentäter sowie Aktivitäten ausländischer extremistischer und terroristischer Gruppen belegen die Unverzichtbarkeit des Verfassungsschutzes für die Erhaltung der freiheitlichen demokratischen Grundordnung. Auch die nachrichtendienstliche Bedrohung besteht, trotz der Umwälzungen im Osten, fort.

Die Diskussion darüber, ob und ggf. welche Aufgaben der Verfassungsschutz bei der Bekämpfung der organisierten Kriminalität, insbesondere des organisierten Drogenhandels, übernehmen könnte, ist noch nicht beendet. Angesichts der bestehenden Befugnisse der Polizei in der vorbeugenden Verbrechensbekämpfung bedürfte eine Aufgabenerweiterung allerdings einer überzeugenden Begründung.

5.2 Richtlinien über den Informationsaustausch in Angelegenheiten des Verfassungsschutzes (IVS-Richtlinien)

Das Landesamt für Verfassungsschutz ist als Behörde ohne Unterbau zur Erfüllung seiner gesetzlichen Aufgaben auf den Informationsaustausch mit anderen Behörden angewiesen. Demgemäß schreibt das Bayer. Verfassungsschutzgesetz vor, **daß alle bayerischen Behörden dem Landesamt die notwendigen Informationen zu übermitteln haben, und das Landesamt seinerseits das Ergebnis seiner Auswertung den für die Aufrechterhaltung der öffentlichen Sicherheit und Ordnung zuständigen Stellen übermitteln darf.**

Die zwangsläufig generalklauselartige Regelung im Gesetz soll durch die Richtlinien über den Informationsaustausch in Angelegenheiten des Verfassungsschutzes erläutert werden.

Mein Anliegen war es dabei, eine extensive Auslegung des Gesetzes zu verhindern. Für Behörden besteht eine Berichtspflicht an das LfV über Planung oder Begehung von Straftaten sowie anderen Störungen der öffentlichen Sicherheit oder Ordnung nicht schon dann, wenn Vermutungen für eine extremistische Motivation bestehen, sondern erst, **wenn tatsächliche Anhaltspunkte dafür bestehen, daß mit den Straftaten oder Störungen extremistische Bestrebungen** verfolgt werden.

Die Richtlinien nennen eine Reihe von **Vorschriften, die der Befolgung von Auskunfts- und Einsichtsersuchen entgegenstehen**. Hier forderte ich eine **Ergänzung** der Aufzählung, damit die Einhaltung dieser besonderen Schutzvorschriften besser gewährleistet ist.

Die endgültige Fassung der Richtlinien liegt mir noch nicht vor. Eine abschließende Bewertung behalte ich mir deshalb vor.

5.3 Generelle Prüfung 1992

Im Berichtszeitraum habe ich beim Landesamt für Verfassungsschutz wieder eine mehrtägige Prüfung verschiedener **Dateien und Karteien** vorgenommen.

Prüfungsschwerpunkte waren insbesondere Speicherungen
- im Nachrichtendienstlichen Informationssystem NADIS der Verfassungsschutzbehörden
- in Dateien und Karteien der Bereiche „Extremismus links", „Extremismus rechts" und
- in der Vorgangsverwaltung (REGA).

Wesentliche Verstöße gegen datenschutzrechtliche Bestimmungen habe ich dabei **nicht festgestellt**.

Neben einer systematischen Kontrolle von **NADIS** habe ich die dort gespeicherten Daten auch anhand einer Personenliste, die ich aus offen zugänglichen Quellen zusammengestellt habe, durchgeführt. In einem Fall war die Verlängerung einer Speicherung nicht nachvollziehbar. Erkenntnisse, welche die Festsetzung einer erneuten Speicherungsfrist gerechtfertigt hätten, waren den schriftlichen Unterlagen nicht zu entnehmen. Anlaß für Beanstandungen bestand im übrigen nicht.

Eingehend habe ich Speicherungen in der Datei **REGA** überprüft. Bei REGA handelt es sich um ein EDV-unterstütztes Registratur- und Schriftgutverwaltungsverfahren. Das Verfahren erleichtert die Zuordnung des eingehenden Schriftgutes zu den einzelnen

internen Arbeitsbereichen, gewährleistet den Nachweis der Schriftstücke und unterstützt bei Wiedervorlage und Aussonderung von Schriftstücken, Vorgängen und Akten ausschließlich im Rahmen der Schriftgutverwaltung.

Um festzustellen, ob Personen gespeichert sind, die Angehörige nichtextremistischer Organisationen sind, habe ich ausgewählte Organisationen, Adressen/Örtlichkeiten und Ereignisse/Kampagnen auf Datenbestand in REGA abgefragt. Dabei habe ich mich davon überzeugen können, daß in der Datei im wesentlichen nur die personenbezogenen Daten gespeichert werden, die zur Erfüllung der Aufgaben des Landesamtes für Verfassungsschutz erforderlich sind. In wenigen Fällen war die Notwendigkeit der Speicherung und der Aufbewahrung von Unterlagen für mich nicht erkennbar. Das LfV hat aufgrund meiner Prüfung eine Bereinigung vorgenommen.

Für eine Querschnittsprüfung wurde eine Auswertung von Speicherungen im extremistischen Bereich vorgenommen. Dabei habe ich festgestellt, daß bei einigen Personendatensätzen das Wiedervorlagedatum nicht den gesetzlichen Vorgaben entsprach. Dies habe ich beanstandet.

5.4 Weitergabe von Erkenntnissen bei der Ermittlung

Personenbezogene Daten, die er über Bürger gesammelt hat, darf der Verfassungsschutz **an Private** nicht übermitteln, es sei denn, daß dies zum Schutz der freiheitlichen demokratischen Grundordnung oder der Sicherheit des Bundes oder eines Landes erforderlich ist und das Innenministerium seine Zustimmung erteilt hat; die Zustimmung kann auch für eine Mehrzahl von gleichartigen Fällen vorweg erteilt werden (Art. 14 Abs. 4 Satz 1 BayVSG).

Gegenstand der Erörterung unter den Datenschutzbeauftragten war die Frage, ob zur Datenübermittlung im Sinne von § 19 Abs. 4 BVerfSchG (entspricht Art. 14 Abs. 4 BayVSG) auch die Übermittlung personenbezogener Informationen an eine nichtöffentliche Stelle zur **Durchführung von Informationsbeschaffungsmaßnahmen** zu rechnen ist.

Der **Bundesminister des Innern** und das **Bayerische Innenministerium** sehen in der Weitergabe personenbezogener Daten im Rahmen konkreter Ermittlungsmaßnahmen keine Datenübermittlung im Sinne des § 19 Abs. 4 BVerfSchG (Art. 14 Abs. 4 BayVSG), sondern einen nichttrennbaren Teil der Informationsbeschaffung, der im 2. Abschnitt des BVerfSchG bzw. BayVSG (§§ 8 ff BVerfSchG, Art. 4 ff BayVSG) geregelt sei. Der Wortlaut des § 19 Abs. 4 Satz 1 des BVerfSchG sei nur scheinbar einschlägig. Der Gesetzgeber wolle damit nicht den Fall der Ermittlungen regeln, sondern – als Ausnahmevorschrift und mit einer wesentlich anderen Zielsetzung – nur den Fall der **selbständigen Übermittlung** an Private. Hätte der Gesetzgeber insofern auch Operativbefragungen erfassen wollen, dann hätte er wohl nicht die Notwendigkeit der Zustimmung des Bundesministers des Innern in jedem einzelnen Fall vorgesehen, weil es nicht Aufgabe des Ministeriums sein könne, sich mit jedem Ermittlungsfall zu befassen.

Es entspricht der Erfahrung, daß Ermittlungsmaßnahmen mit Hilfe einer anderen Person in der Regel eine zumindest teilweise Weitergabe personenbezogener Informationen an diese voraussetzen, um sie überhaupt in die Lage zu versetzen, Auskünfte über einen Dritten zu erteilen. Bei der **Befragung von Privatpersonen** gemäß Art. 4 ff BayVSG, die **notwendigerweise auch Informationen für den Befragten** enthält, handelt es sich um einen **einheitlichen natürlichen Lebensvorgang**. Eine andere Beurteilung würde dazu führen, daß ein natürlicher Sachverhalt künstlich in zwei Vorgänge aufgespalten würde. Eine Befragung ohne lenkende Hinweise auf ein bestimmtes Befragungsziel würde regelmäßig zu keinem sinnvollen Ergebnis führen. Es erscheint deshalb vertretbar, das Gesetz dahingehend auszulegen, daß die **Ermächtigungsnormen für operative Befragungen** – seien sie offen oder verdeckt durchgeführt – **abschließend in Art. 4 ff BayVSG geregelt** sind und die für die Ermittlungsmaßnahme **erforderlichen** Hinweise an den Befragten **mitumfassen**. Ein Fall der Weitergabe von Erkenntnissen an private Dritte im Sinne des § 19 Abs. 4 BVerfSchG bzw. Art. 14 Abs. 4 BayVSG liegt also bei der Ermittlung nicht vor.

5.5 Identitätsprüfung bei Auskunftsersuchen

Das LfV hatte mir mitgeteilt, daß es künftig „zur Erreichung einer höheren Datensicherheit bei Auskunftsersuchen über beim LfV gespeicherte Daten" die **Vorlage einer Ablichtung des Personalausweises** des Petenten für erforderlich halte. Dadurch solle die Identität des Antragstellers mit der Person, über die Auskunft begehrt wird, festgestellt und Abfragen von Nichtberechtigten ausgeschlossen werden.

Gegen dieses Verfahren habe ich Bedenken geäußert, da die Zusendung einer Ablichtung des Personalausweises als Voraussetzung für die Behandlung des Auskunftsantrags möglicherweise manchen Bürger von einer Antragstellung hätte abhalten können. Darüber hinaus ist im Bayer. Verfassungsschutzgesetz – im Gegensatz zu anderen Gesetzen, wie z.B. dem sog. Stasi-Unterlagengesetz – keine entsprechende Regelung enthalten. Ich halte auch die Gefahr, daß sich jemand Einsicht in Stasi-Akten dritter Personen erschleichen will, für wesentlich größer als bei Daten des LfV.

Aufgrund meiner Einwendungen hat das LfV seine Praxis geändert und verfährt nunmehr wie folgt: Sofern die Kombination von Name und Vorname des Antragstellers weder in NADIS noch in einer Datei des LfV erfaßt ist, erfolgt **keine Rückfrage** bei dem Antragsteller zur Klärung der Identität. Gleiches gilt, wenn der Antragsteller eindeutig mit einer beim LfV gespeicherten Person identisch ist.

Bestehen Speicherungen zu der Kombination Name und Vorname des Antragstellers, sind aber gleichzeitig wegen unterschiedlicher Adressen oder aus anderen Gründen **Zweifel an der Identität des Antragstellers** mit der gespeicherten Person vorhanden, so wird beim Antragsteller nach entsprechenden Daten nachgefragt, die eine Identifizierung ermöglichen. Die Bitte um Übermittlung beispielsweise des Geburtsdatums und des Geburtsortes kann verknüpft werden mit der Empfehlung, zur Arbeitserleichterung statt der erbetenen Auskünfte eine Ablichtung des Personalausweises zu übersenden. Keinesfalls wird die Übersendung einer Ablichtung des Personalausweises zur Voraussetzung für die Bearbeitung des Auskunftsantrags erklärt.

Mit dieser Regelung bin ich einverstanden.

5.6 Kontrolle von Einzelvorgängen und Bürgereingaben

5.6.1 Dokumentation der Sicherheitsüberprüfung

Im Berichtszeitraum wandte sich ein Bürger an mich mit der Bitte um Auskunft über die zu seiner Person vermuteten Speicherungen beim LfV.

Grund für diese Vermutung war, daß ihm von seinem Arbeitgeber, der auch Produkte für sicherheitsempfindliche Bereiche fertigt, gekündigt worden war. Er glaubte, daß diese Kündigung aufgrund einer Sicherheitsüberprüfung beim LfV, die für Angestellte in sensiblen Bereichen vorgeschrieben ist, erfolgt sei. Dem Petenten, der sich zunächst direkt an das LfV wandte, war von dort mitgeteilt worden, daß über ihn beim LfV keine Speicherungen in Dateien bzw. Unterlagen vorhanden und keine Sicherheitsüberprüfung vom LfV durchgeführt worden sei.

Wie sich erst später herausstellte, war der Petent sehr wohl einer routinemäßigen Sicherheitsüberprüfung beim LfV mit negativem Ergebnis, d. h. ohne nachteilige Erkenntnisse, unterzogen worden. Da jedoch bei negativen Überprüfungsergebnissen die Anfragen im Original direkt an die anfragende Stelle zurückgesandt wurden und keine Speicherung beim LfV vorgesehen war, wurde die Eingabe vom LfV zunächst nicht korrekt beantwortet, weil die Sicherheitsüberprüfung nicht dokumentiert war. Erst als sich der Petent an mich wandte und ich entsprechende Nachprüfungen durchführte, kam die Sicherheitsüberprüfung an den Tag. Der Petent erhielt dann die richtige Auskunft.

Um derartigen Fehlinformationen künftig vorzubeugen, habe ich beim LfV angeregt, auch die Sicherheitsüberprüfungen ohne nachteilige Erkenntnisse zu dokumentieren und die entsprechende Unterlage zur Dokumentation der Sicherheitsüberprüfung bei eventuellen Nachprüfungen und Nachfragen zwei Jahre aufzubewahren.

Das LfV hat sein Verfahren in diesem Sinn geändert.

5.6.2 Keine Auskunft über G-10-Maßnahmen

In einer Eingabe wollte ein Bürger Auskunft über evtl. gegen seine Person gerichtete Abhörmaßnahmen im Rahmen des sog. G-10-Gesetzes. Ich habe ihn darauf hingewiesen, daß ich für derartige Auskünfte nicht zuständig bin. Über die Zulässigkeit von G-10-Maßnahmen entscheidet die G-10-Kommission des Bayerischen Landtags. Über die Mitteilung an den Betroffenen entscheidet das Innenministerium. Hält die Kommission eine Mitteilung für geboten, so ist diese unverzüglich zu veranlassen.

6. Justiz

6.1 Gesetzgebungsverfahren

6.1.1 Justizmitteilungsgesetz

Die Bundesregierung hat dem Bundesrat den Entwurf eines Gesetzes über Mitteilungen der Justiz von Amts wegen in Zivil- und Strafsachen (JuMittG) zur Stellungnahme zugeleitet. Durch den Entwurf, der mittlerweile dem Bundestag vorliegt, soll die **Übermittlung personenbezogener Daten innerhalb der Justiz und an andere öffentliche Stellen** auf die erforderliche gesetzliche Grundlage gestellt werden. Bisher stützt sich die Übermittlung auf bundeseinheitliche Verwaltungsvorschriften (MiZi und MiStra).

Für die Beratungen im Bundesrat habe ich zum Gesetzesentwurf gegenüber dem Staatsministerium der Justiz Stellung genommen. Von den neuen Regelungen zur Datenübermittlung erscheinen mir folgende besonders erwähnenswert:

1. Die Staatsanwaltschaft unterrichtet die Polizei über den **„Ausgang des Verfahrens"**, wobei erforderlichenfalls auch die Übermittlung einer mit Gründen versehenen Einstellungsentscheidung zulässig ist. Soweit ein Urteil, das angefochten worden ist, der Polizei übersandt wird, ist von der Staatsanwaltschaft auch anzugeben, wer es angefochten hat.

Ich habe in meiner Stellungnahme darauf hingewiesen, daß in der Begründung der Gesetzesvorlage ausgeführt ist, daß unter dem Begriff „Ausgang des Verfahrens" der **rechtskräftige** Abschluß des Verfahrens gemeint ist. Darunter fallen **Verfahrenseinstellungen** nach § 170 Abs. 2 StPO nicht. Ich habe daher angeregt, klarzustellen, daß auch diese Einstellungen – die Auswirkung auf die Datenspeicherung bei der Polizei haben können (vgl. 4.13) – von der Mitteilungspflicht erfaßt werden.

Ein Erfordernis für eine Zwischenmitteilung an die Polizei durch Übermittlung eines nicht rechtskräftigen Urteils habe ich nicht gesehen. Ich halte es für ausreichend, wenn der Polizeibehörde der **Abschluß** des Verfahrens mitgeteilt wird.

2. Soweit eine **Klage auf Räumung von Wohnraum** im Falle der Kündigung eines Mietverhältnisses wegen Zahlungsverzuges des Mieters bei Gericht eingegangen ist, teilt das Gericht dem zuständigen Träger der Sozialhilfe u.a. den Tag des Eingangs der Klage, die Höhe des monatlich zu entrichtenden Mietzinses und die Höhe des geltend gemachten Mietzinsrückstandes mit, es sei denn, der Zahlungsverzug beruht offensichtlich nicht auf einer Zahlungsunfähigkeit. Dadurch wird sichergestellt, daß der Träger der Sozialhilfe entsprechend seiner Amtspflicht Maßnahmen zur Sicherung der Unterkunft des Mieters bei drohender Obdachlosigkeit ergreifen kann. Eine Kündigung eines Mietverhältnisses über Wohnraum wird nämlich unwirksam, wenn sich bis zum Ablauf eines Monats nach Eingang der Klage der Träger der Sozialhilfe zur Befriedigung des fälligen Mietzinses verpflichtet.

   Gegen die Aufnahme einer solchen Regelung im Bundessozialhilfegesetz haben bei vielen Datenschutzbeauftragten starke Vorbehalte bestanden. Sie haben im Zusammenhang mit der Übersendung der Klageschrift an den Mieter die **Beifügung eines Hinweisblattes** an den Mieter, in dem er über die Möglichkeit unterrichtet wird, bei Mittellosigkeit Unterstützung durch den Träger der Sozialhilfe zu erhalten, für ausreichend gehalten.

   Demgegenüber habe ich gegen eine solche **Mitteilungspflicht der Gerichte** keine grundsätzlichen Bedenken erhoben. Die Unterrichtung des Sozialamtes liegt im wohlverstandenen Interesse des Mieters. Für Haarspalterei ist hier kein Platz. Die Übersendung eines Hinweisblattes halte ich weder für hilfreich noch aus der Sicht des Datenschutzes für geboten. Die Erfahrungen zeigen, daß viele betroffene sozialschwache Mieter nicht von sich aus tätig werden und deshalb das Sozialamt nicht rechtzeitig in eine evtl. bestehende Zahlungspflicht eintreten kann.

   Nach einem Pressebericht ist in dem vom Sozialreferat der Landeshauptstadt München in Auftrag gegebenen „Armutsbericht '90" der Vorwurf erhoben worden, der Datenschutz behindere gegenwärtig Sozialarbeit dadurch, daß er dem Richter verbiete, dem Sozialamt den Eingang von Räumungsklagen gegen säumige Mieter mitzuteilen. In einem Leserbrief bin ich diesem Vorwurf entgegengetreten und habe deutlich gemacht, daß bereits nach den geltenden Verwaltungsvorschriften eine Mitteilung von Räumungsklagen durch die Gerichte an den Träger der Sozialhilfe zulässig ist, wenn der Richter nach Aktenlage zur Auffassung kommt, daß die Säumigkeit des Mieters auf dessen Mittellosigkeit beruht.

6.1.2 Gewinnaufspürungsgesetz

Zur wirksamen Bekämpfung der organisierten Kriminalität ist es unerläßlich, die Weiterverwendung der aus den begangenen Straftaten erzielten Gewinne zu unterbinden und das „Waschen von Geld", d.h. die Rückführung illegal erworbenen Vermögens in den legalen Finanzkreislauf, unter Strafe zu stellen. Zu diesem Zweck müssen Strafverfolgungsbehörden in der Lage sein, solche „Geldwaschtransaktionen" zu enttarnen, die hieran Beteiligten zu ermitteln und auf die entsprechenden Unterlagen zuzugreifen.

Der dazu von der Bundesregierung vorgelegte Entwurf eines Gesetzes über das Aufspüren von Gewinnen aus schweren Straftaten (Gewinnaufspürungsgesetz) regelt

1. die Pflichten der Banken und anderer Gewerbetreibenden zur
   - **Identifizierung** ihrer Kunden sowie zur Aufzeichnung und Aufbewahrung der Identifizierungsangaben sowie zur
   - Ermittlung der **wirtschaftlich Berechtigten** einer Finanztransaktion,
2. eine Pflicht für Kredit- und Finanzierungsinstitute sowie Spielbanken, den Strafverfolgungsbehörden Fälle zu **melden**, in denen sie den Verdacht einer Geldwäsche feststellen,
3. die **Schaffung von internen Sicherungsmaßnahmen** zum Schutz gegen Geldwäsche und zur Erleichterung der Strafverfolgung bei solchen Unternehmen, die für Geldwäsche in Betracht kommen.

Ich habe den Gesetzentwurf geprüft und keinen Verstoß gegen datenschutzrechtliche Grundsätze festgestellt.

6.1.3 Gesetzliche Regelung zum genetischen Fingerabdruck (Genomanalyse)

Die Bundesministerin der Justiz hat einen neuen Entwurf für eine gesetzliche Regelung über den Einsatz

der Genomanalyse zur Täterfeststellung (genetischer Fingerabdruck) vorgelegt.

Bei dem sog. DNA-Fingerprinting werden Genomstrukturen von Körperzellen, die am Tatort oder am Opfer gefunden wurden, mit den entsprechenden Genomstrukturen aus Körperzellen des vermuteten Spurenlegers verglichen. Dabei werden DNA-Bereiche herangezogen, die **außerhalb des kodierenden Teils** des menschlichen Genoms liegen und damit nach bisheriger Erkenntnis **keinen Rückschluß auf Persönlichkeitsmerkmale** zulassen. Im Vergleich zu den herkömmlichen Untersuchungsmethoden kann durch diese Methode eine Person mit wesentlich höherer Wahrscheinlichkeit als Täter festgestellt oder ausgeschlossen werden.

Obwohl die Anwendung dieser Ermittlungsmethode – wie der Bundesgerichtshof im Jahre 1990 entschieden hat – in §§ 81 a und 81 c der Strafprozeßordnung eine **ausreichende Rechtsgrundlage** findet, sollen die geplanten gesetzlichen Vorschriften die Voraussetzungen und Beschränkungen für die Anwendung des DNA-Fingerprinting in normenklarer Weise festlegen. So sieht der Entwurf u.a. vor:

- **Verwendungsbeschränkung** für das Vergleichsmaterial auf Strafverfahren sowie die Verpflichtung zur **Vernichtung** des Materials, soweit es nicht mehr erforderlich ist,
- **Untersuchungsbeschränkung** auf den Teil der DNA, der keine genetischen Anlagen enthält,
- **Richtervorbehalt** für die Entnahme von Vergleichsmaterial sowie für die Anordnung der Untersuchung.

Gegen den Entwurf habe ich zwar keine grundsätzlichen Bedenken erhoben, jedoch zur Klarstellung gefordert, daß molekulargenetische Untersuchungen nur für die eine konkrete Straftat, zu deren Aufklärung das Material entnommen wurde, zulässig sind, da der Richter nur für diese konkrete Tat die Untersuchung angeordnet hat. Die Auswertung des untersuchten Materials für eine andere Straftat bedarf einer erneuten richterlichen Anordnung.

6.2 Automatisierte Datenverarbeitung bei Gerichten und Staatsanwaltschaften

1. Die im 9. und 10. Tätigkeitsbericht beschriebene **Entwicklung zur automatisierten Datenverarbeitung** im Justizbereich hat sich im Berichtszeitraum fortgesetzt. Mittlerweile sind dort 26 Datenverarbeitungsverfahren im Einsatz. Personenbezogene Daten, die bisher manuell in Karteikarten, Lose-Blatt- oder Buchform erfaßt wurden, werden nun in erheblichem Umfang in automatisierten Dateien zum Zwecke der Verwaltung und Bearbeitung (z.B. Erstellung von Texten) gespeichert.

   In zahlreichen **Amtsgerichten** werden **Familien-** und **Zivilrechts-, Nachlaß-, Grundbuch-** und **Strafverfahren** in automatisierten Verfahren verarbeitet.

   Bei 12 **Staatsanwaltschaften** wird das **Zentrale Namensverzeichnis** automatisiert geführt.

2. **Bereichsspezifische gesetzliche Grundlagen** für die Verarbeitung personenbezogener Daten in den einzelnen Verfahrensordnungen fehlen derzeit.

   Die Aktenverwaltung findet bisher ihre Grundlage in einer bundeseinheitlichen Verwaltungsvorschrift „**Aktenordnung** für die Geschäftsstellen der Gerichte der ordentlichen Gerichtsbarkeit und der Staatsanwaltschaften (AktO)". An der Aktenordnung orientieren sich auch die einzelnen DV-Verfahren.

   Der Referentenentwurf eines Strafverfahrensänderungsgesetzes aus dem Jahre 1989 sieht für den **Strafrechtsbereich** Regelungen über die Verarbeitung personenbezogener Daten in Dateien vor. Für die anderen Justizbereiche liegen bisher keine Gesetzesinitiativen vor. Solange der Bund von seiner Regelungskompetenz keinen Gebrauch macht, haben die Länder die Möglichkeit, die Datenverarbeitung im Justizbereich zu regeln. Das Land Berlin hat von dieser Möglichkeit im Ausführungsgesetz zum Gerichtsverfahrensgesetz Gebrauch gemacht. Nach der Novellierung des Bayerischen Datenschutzgesetzes, das auch für die Justiz gelten soll, wird zu prüfen sein, ob zusätzliche bereichsspezifische Regelungen erforderlich sind.

6.3 Aufbewahrung von Akten und Aktennachweisen

Zur Aufgabenerfüllung von Gerichten, Staatsanwaltschaften und sonstigen Justizbehörden wird Schriftgut (Akten) angelegt, das mit Hilfe von Registern und Verzeichnissen in Karteiform, Lose-Blatt-Sammlungen oder in Buchform geführt und erschlossen wird. Nicht nur die Datenspeicherung in automatisiert geführten Dateien, sondern auch die Aufbewahrung der Akten, in denen personenbezogene Daten erfaßt sind, greift in das informationelle Selbstbestimmungsrecht der davon betroffenen Personen ein. Nach den Ausführungen des Bundesverfassungsgerichtes im sog. Volkszählungsurteil sind Einschränkungen des Rechts auf informationelle Selbstbestimmung nur im überwiegenden Allgemeininteresse und aufgrund einer **verfassungsgemäßen gesetzlichen Grundlage**, die dem rechtsstaatlichen Gebot der Normenklarheit und dem Grundsatz der Verhältnismäßigkeit entsprechen muß, zulässig.

Eine bereichsspezifische gesetzliche Grundlage für die Aufbewahrung von Schriftgut **fehlt** bisher. Der Referentenentwurf eines Strafverfahrensänderungsgesetzes sieht zwar Regelungen über die Verarbeitung personenbezogener Daten in Dateien, nicht jedoch über die Dauer der Aufbewahrung von Schriftgut vor.

Bisher erfolgt die Aufbewahrung von Akten auf der Grundlage von bundeseinheitlich geltenden **Verwaltungsvorschriften,** den „Bestimmungen über die Aufbewahrungsfristen für das Schriftgut der ordentlichen Gerichtsbarkeit, der Staatsanwaltschaften und der Justizvollzugsbehörden". Die Aufbewahrungsfristen betragen zwischen 5 und 30 Jahre, wobei sich die Frist im einzelnen nach Art der Erledigung bemißt.

Ich habe im Einklang mit den Datenschutzbeauftragten des Bundes und der Länder die **Schaffung einer gesetzlichen Grundlage für die Aufbewahrung von Schriftgut** gefordert. Die bisher geltenden Aufbewahrungsfristen sind unter dem Gesichtspunkt der Erforderlichkeit zu überprüfen. Solange der Bundesgesetzgeber von seiner Regelungsbefugnis keinen Gebrauch macht, können auch die Länder die erforderlichen Grundlagen schaffen. In Bayern wäre etwa an eine Verordnungsermächtigung im neuen Bayerischen Datenschutzgesetz zu denken. Die Diskussion mit dem Staatsministerium der Justiz hierüber ist noch nicht abgeschlossen.

6.4 Einsatz privater Personal Computer durch Richter und Staatsanwälte

Im Zuge der in allen Lebensbereichen festzustellenden Entwicklung zum Einsatz von Personal Computern verwenden auch Richter und Staatsanwälte private Personal Computer zur Vorbereitung ihrer Entscheidungen und Verfügungen sowie teilweise zur Textbearbeitung.

1. Für die **richterliche** Tätigkeit ergibt sich die Zulässigkeit aus dem verfassungsrechtlich verankerten Gebot der richterlichen Unabhängigkeit (Art. 97 Abs. 1 Grundgesetz). Diese umfaßt nicht nur die richterliche Entscheidung als solche, sondern auch alle Sach- und Verfahrensentscheidungen, die den eigentlichen Richterspruch vorbereiten und ihm mittelbar dienen, somit auch die Wahl der Arbeitsmittel. Im Hinblick auf die richterliche Unabhängigkeit ist es mir daher verwehrt, beim Einsatz von privaten Personal Computern zur Vorbereitung von Entscheidungen die Einhaltung datenschutzrechtlicher Bestimmungen zu überwachen. Vielmehr hat der Richter selbst die Verantwortung für die Einhaltung des Datenschutzes und der Datensicherheit zu tragen.

2. Hinsichtlich der **staatsanwaltschaftlichen** Tätigkeit vertritt das Staatsministerium der Justiz die Auffassung, daß eine Ungleichbehandlung von Staatsanwälten und Richtern nicht gerechtfertigt sei. Im Hinblick auf den praktizierten Laufbahnwechsel zwischen richterlichem und staatsanwaltschaftlichem Amt müsse es auch dem Staatsanwalt überlassen bleiben, wie er seine Entscheidungen vorbereite.

   Demgegenüber bin ich der Auffassung, daß die aus der richterlichen Unabhängigkeit zu ziehenden Folgerungen nicht für Staatsanwälte gelten können. § 146 Gerichtsverfassungsgesetz bestimmt, daß Beamte der Staatsanwaltschaft den dienstlichen Anweisungen ihres Vorgesetzten nachzukommen haben. Eine sachliche oder persönliche Unabhängigkeit des Staatsanwaltes, wie sie Art. 97 Abs. 1 Grundgesetz dem Richter einräumt, ist daher nicht gegeben.

   Der Behördenleiter, dem die Dienstaufsicht über den einzelnen Staatsanwalt obliegt, hat nach meiner Auffassung durch geeignete Maßnahmen dafür Sorge zu tragen, daß der Datenschutz durch den einzelnen Staatsanwalt eingehalten wird. Ich habe deshalb gefordert, daß private Personal Computer durch Staatsanwälte zu dienstlichen Zwecken nur nach Anzeige an den Behördenleiter und auf der Grundlage von behördeninternen Datenschutzhinweisen für den konkreten Anwendungsbereich verwendet werden dürfen.

6.5 Einzelne EDV-Verfahren der Gerichte und Staatsanwaltschaften

1. Das EDV-System **SIJUS-Strafsachen** ist ein DV-Verfahren zur Unterstützung der Automation des Geschäftsstellenbetriebes und der Kanzleitätigkeiten bei den Staatsanwaltschaften und den Strafgerichten. Als Anwender kommen somit die Strafverfolgungsbehörden und die Strafvollstreckungsabteilungen der Staatsanwaltschaften in Frage. Mittlerweile befindet sich das DV-Verfahren bei sieben Staatsanwaltschaften in der Erprobung. Ein ähnliches Verfahren befindet sich für die Strafgerichte in der Entwicklung.

   Das „SIJUS-Strafsachen" ist konzipiert nach der bundeseinheitlichen Verwaltungsvorschrift „Aktenordnung für die Geschäftsstellen der Gerichte der ordentlichen Gerichtsbarkeit und der Staatsanwaltschaften (AktO)". Es bietet neben der automatisierten Bearbeitung von Verwaltungsaufgaben auch die Möglichkeit der Textbe- und verarbeitung unter Verwendung von Textbausteinen. Der staatsanwaltschaftliche Verfahrensteil des DV-Verfahrens unterstützt die im Bereich der Strafverfol-

gung tätigen Geschäftsstellen der Staatsanwaltschaften bei der Verfahrensregistrierung, der Aktenverwaltung (Aktenkontrolle, Wiedervorlage u.ä.) und der Zählkartenbearbeitung; bei der Erstellung von Schriftgut kann auf die in den Dateien gespeicherten Personen- und Verfahrensdaten zurückgegriffen werden.

Die Verarbeitung personenbezogener Daten erfolgt derzeit auf der Grundlage der §§ 160, 152 StPO i.V.m. Art. 16 Abs. 1 BayDSG. Der vierte Entwurf eines Strafverfahrensänderungsgesetzes aus dem Jahre 1989 sieht hierzu bereichsspezifische Regelungen vor.

Die Entwicklung des DV-Verfahrens ist noch nicht abgeschlossen. Es fehlen noch ein **Konzept zur Löschung** von Daten aus dem DV-System sowie eine **Dienstanweisung für den Verfahrenseinsatz und eine Verfahrensbeschreibung für den technischen Bereich**. Der staatsanwaltschaftliche Verfahrensteil des DV-Verfahrens war bisher Gegenstand zweier datenschutzrechtlicher Prüfungen bei Staatsanwaltschaften. Eine abschließende Beurteilung des Verfahrens habe ich für Anfang 1993 vorgesehen. Zu diesem Zwecke habe ich beim Staatsministerium der Justiz ausstehende Verfahrensunterlagen angefordert.

2. Über die Entwicklung des DV-Verfahrens SIJUS-Strafsachen hinaus werden vom Staatsministerium der Justiz Überlegungen angestellt, ein **zentrales landesweites Aktennachweissystem (Landes-Sissy)** auf der Grundlage des vierten Entwurfes des Strafverfahrensänderungsgesetzes einzuführen. Bei diesem System geben alle Staatsanwaltschaften, die „SIJUS-Strafsachen" einsetzen, Personaldatensätze und zum Teil auch die zur Erschließung der Akten erforderlichen Verfahrensdaten an eine zentrale Stelle weiter. Nach Mitteilung des Staatsministeriums der Justiz ist jedoch nicht daran gedacht, sämtliche Verfahren an die Zentralstelle zu übermitteln. So soll z.B. auf die Übermittlung von Verkehrsdelikten verzichtet werden. Ich habe das Staatsministerium der Justiz aufgefordert, mich rechtzeitig an der Entwicklung des Systems zu beteiligen.

3. Zur Unterstützung der Tätigkeit der Vormundschaftsgerichte wurde nunmehr ebenfalls ein DV-Verfahren, **VORMTEXT**, entwickelt und nach Art. 26 BayDSG freigegeben. Bei dem DV-Verfahren handelt es sich um ein Anwenderprogramm für Vormundschaftssachen sowie für sämtliche sonstigen Angelegenheiten der Freiwilligen Gerichtsbarkeit, die traditionell der Vormundschaftsabteilung eines Amtsgerichtes zugeordnet werden. Dies sind z.B. Pflegschaften, Beistandschaften, Unterbringungssachen, Adoptionssachen, ab 01.01.92 Betreuungssachen. Das Verfahren unterstützt dabei die Tätigkeit des Vormundschaftsgerichtes durch eine **Verfahrensbank**, welche die nach der Aktenordnung vorgeschriebenen, in Kartei- oder Buchwerken geführten Register und Verzeichnisse ersetzt, sowie durch eine größere Zahl von programmierten **Textbausteinen**, die auf die in der Datenbank gespeicherten Informationen zugreifen.

   In meiner Stellungnahme gegenüber dem Staatsministerium der Justiz habe ich eine stärkere Berücksichtigung des Grundsatzes der Erforderlichkeit bei der **Speicherdauer** von Daten gefordert sowie ergänzende Vorschläge zur Datensicherheit gemacht. Im übrigen begegnet das DV-Verfahren – wie ich mich auch bei einer datenschutzrechtlichen Kontrolle eines Amtsgerichts überzeugen konnte – keinen datenschutzrechtlichen Bedenken.

6.6 Kontrolle eines Amtsgerichtes

An einem Amtsgericht habe ich die Datenverarbeitung in familien- und vormundschaftsgerichtlichen Angelegenheiten überprüft. Im Hinblick auf die Neuentwicklung des DV-Verfahrens „VORMTEXT" lag der Schwerpunkt der Kontrolle bei der vormundschaftsgerichtlichen Abteilung, die das DV-Verfahren in der Praxis erprobt. Wegen der richterlichen Unabhängigkeit mußte sich meine Kontrolle auf die Verwaltungstätigkeit beschränken.

Als Ergebnis der Prüfung konnte ich feststellen, daß das Amtsgericht dem Datenschutz einen hohen Stellenwert beimißt. Wesentliche datenschutzrechtliche Mängel waren nicht festzustellen.

6.6.1 Vormundschaftsgericht

Beim Vormundschaftsgericht kommt das DV-Verfahren „VORMTEXT" zum Einsatz, das die früher zur Register- und Verzeichnisführung entsprechend der AktO verwendeten Karteikarten ablöste. Zur Prüfung der Erforderlichkeit der **Datenerhebung** und **Speicherung** habe ich einige Datenfelder in einzelnen Datenbanken sowie deren Inhalte gesichtet. Daten, die für die Verfahrensbearbeitung nicht erforderlich sind, habe ich nicht festgestellt.

Alle **Vormundschaftsverfahren, die noch nicht abgeschlossen** sind werden in das DV-Verfahren übertragen. Die Karteikarten der übertragenen Verfahren wurden bisher nicht vernichtet, sondern werden weiter aufbewahrt. Für eine **Weiteraufbewahrung der Karteikarten** besteht keine Notwendigkeit, da durch die Erfassung der Verfahren in der Datei die Karteikarten zur Erschließung der Akten nicht mehr

benötigt werden. Ich habe daher die Vernichtung der Karteikarten übertragener Verfahren gefordert.

Da das DV-Verfahren erst seit wenigen Jahren angewandt wird, waren **Löschungen** von Daten in Registern noch nicht veranlaßt. Für mit Hilfe der EDV erstellte Texte ist kein spezielles Löschprogramm vorhanden. Die Texte, die in dem System gespeichert werden, werden durch die Schreibkanzlei gefertigt und nach Erstellung, in der Regel spätestens nach zwei Monaten, von der Schreibkraft gelöscht, wobei einzelne Texte bei Bedarf aufgrund besonderer Anordnung des Sachbearbeiters länger gespeichert werden können.

Die letzte **Aussonderung** von **Akten** erfolgte nach Auskunft des zuständigen Sachbearbeiters im Jahre 1987, wobei die zu den ausgesonderten Akten gehörenden **Karteikarten** nicht mitvernichtet wurden. Die Aktenaussonderung wird nicht jährlich, sondern in einem Abstand von ca. fünf Jahren durchgeführt. Diese Verfahrensweise entspricht der Bekanntmachung des Staatsministeriums der Justiz über die Abgabe von Archivgut an die Staatsarchive und Aussonderung des übrigen Schriftgutes (Archivsachenbekanntmachung). Danach ist nach Ablauf der in den Aufbewahrungsbestimmungen festgesetzten Fristen das Schriftgut in den vom Behördenleiter zu bestimmenden Zeiträumen (etwa alle 5 bis 10 Jahre) auszusondern und entweder als Archivgut an die Staatsarchive abzugeben oder zu vernichten. Archivgut, d.h. Akten und sonstiges Schriftgut, das für die Feststellung von Rechtsverhältnissen oder für die wissenschaftliche Forschung von Bedeutung sein kann, wird in den jeweiligen Staatsarchiven weiter aufbewahrt.

Diese Verfahrensweise der Aktenaussonderung hält nach meiner Auffassung datenschutzrechtlichen Anforderungen nicht Stand. Die Aufbewahrungsbestimmungen regeln, wie lange Akten und Aktenbestandteile aufzubewahren sind. Daraus ist aber im Umkehrschluß zu folgern, daß die Akten etc. nach Ablauf der Frist nicht mehr für die Sachbearbeitung erforderlich sind. Aus datenschutzrechtlichen Gründen sind sie daher nach Ablauf der Aufbewahrungsfristen zu vernichten, soweit sie nicht zu archivieren sind. Einen besonderen Arbeitsaufwand, der einer jährlichen Aktenaussonderung entgegensteht, vermag ich nicht zu erkennen. Vom Arbeitsaufwand her kann es keinen entscheidenden Unterschied machen, ob einmal im Jahr eine geringere Menge Akten oder alle fünf Jahre eine größere Menge Akten auf Aussonderung durchzusehen ist.

Da es sich bei den Karteikarten um eine Vorgangsverwaltung handelt, ist aus datenschutzrechtlicher Sicht zu fordern, daß mit der Vernichtung der Verfahrensakte auch die dazugehörige Karteikarte vernichtet wird.

Die Erörterung dieser Fragen mit dem Staatsministerium der Justiz ist noch nicht abgeschlossen.

6.6.2 Familiengericht

Das **Register** wird in Buchform geführt, darin sind alle seit 1977 anhängigen Verfahren fortlaufend verzeichnet. Das **Namensverzeichnis** wurde bis 01.01.1992 manuell mittels Karteikarten geführt. Nunmehr ist es im DV-Verfahrens FAMTEXT enthalten.

Die Durchführung **der Akten- und Karteikartenaussonderung** entspricht dem in der vormundschaftsgerichtlichen Abteilung.

6.7 Kontrolle einer Staatsanwaltschaft

Wie im Vorjahr habe ich auch im Berichtszeitraum eine Staatsanwaltschaft geprüft, bei der das Datenverarbeitungsverfahren **„Sijus-Strafsachen"** eingeführt ist.

Als Ergebnis der Prüfung konnte ich feststellen, daß die Staatsanwaltschaft trotz eines erheblich gestiegenen Geschäftsanfalles – die Verfahrenseingänge haben sich bei gleichbleibendem Personalbestand verdoppelt – auf die Einhaltung datenschutzrechtlicher Bestimmungen achtet.

6.7.1 Manuelle Zentrale Namenskartei

Bis zur Einführung des DV-Verfahrens „Sijus-Strafsachen" im Frühjahr 1991 wurden Ermittlungsverfahren in der manuellen Zentralen Namenskartei erfaßt. Sie enthält den Namen, das Geburtsdatum des Beschuldigten, den Tatvorwurf und das Aktenzeichen.

Im 13. Tätigkeitsbericht habe ich darauf hingewiesen, daß **Karteikarten als Hilfsmittel zum Auffinden von Verfahrensakten zusammen mit diesen zu vernichten sind** und eine weitere Aufbewahrung von Karteikarten nach Aussonderung der Akten datenschutzrechtlichen Anforderungen nicht genügt.

Bei der Prüfung der Staatsanwaltschaft habe ich festgestellt, daß eine **Aussonderung und Vernichtung von Karteikarten** seit Ende der 60er Jahre nicht mehr erfolgt ist. Die Staatsanwaltschaft hat in den zurückliegenden Jahren dafür keine Notwendigkeit gesehen. Die Karteikarten seien bisher nicht zu Lasten von Beschuldigten verwendet worden. Im Einzelfall habe man vielmehr im Interesse eines Betroffenen, z.B. wegen versicherungs- bzw. rentenrechtlicher Fragen, noch nach Vernichtung der Akte belegen können, daß ein Verfahren bei der Behörde anhängig war.

Allein die Möglichkeit, daß sich die weitere Aufbewahrung der Karteikarten in ganz besonderen Einzelfällen einmal vorteilhaft für den Betroffenen auswirken kann, rechtfertigt nicht den Eingriff in das Recht auf informationelle Selbstbestimmung bei einer Vielzahl von Betroffenen.

Das Staatsministerium der Justiz teilt meine Auffassung, da es die weitere Aufbewahrung der Karteikarten nach Vernichtung der entsprechenden Verfahrensakten zur Erfüllung staatsanwaltschaftlicher Aufgaben nicht für erforderlich hält. Es hat jedoch darauf hingewiesen, daß die derzeit geltenden bundeseinheitlichen Aufbewahrungsbestimmungen eine fünfjährige Aufbewahrung der Karteikarten **nach** Vernichtung der Akten bzw. deren Ablieferung an die Staatsarchive vorsehen. Die Anpassung der Aufbewahrungsbestimmungen an die Erfordernisse des Datenschutzes wird derzeit mit den anderen Justizverwaltungen abgestimmt.

Ich habe gegenüber dem Staatsministerium der Justiz darauf hingewiesen, daß mit der Bereinigung der Karteikarten nicht bis zum Abschluß der sich erfahrungsgemäß über Jahre hinziehenden Verhandlungen der Justizverwaltungen gewartet werden sollte. In der Zwischenzeit sollte zumindest – beginnend mit den ältesten Jahrgängen – die Aussonderung der Karteikarten in Angriff genommen werden, die bereits nach den geltenden Bestimmungen zu vernichten sind. Das Staatsministerium der Justiz stellte in Aussicht, daß dies entsprechend den personellen Möglichkeiten geschehen werde.

6.7.2 Automatisierte Zentrale Namenskartei

Seit Frühjahr 1991 werden neu eingehende Ermittlungsverfahren nur noch in der automatisiert geführten Zentralen Namenskartei im Verfahren „**Sijus-Strafsachen**“ erfaßt. Frühere, im manuellen Zentralen Namensverzeichnis eingetragene Verfahren werden bis einschließlich 1989 in „SIJUS“ übernommen. Die Karteikarten der übernommenen Verfahren werden vernichtet.

Bei der Übernahme der sog. „Altverfahren“ wird im Anschluß an die Referatskennung ein behördenintern entwickeltes **Deliktskürzel** eingegeben, das dem Sachbearbeiter beim Ausdruck des Vorverfahrensverzeichnisses Aufschluß über die Deliktsart des „Alt-Verfahrens“ gibt.

Die generelle Übernahme der Verfahren der letzten drei Jahre in die automatisiert geführte Namensdatei führt jedoch auch dazu, daß **Kinder** erfaßt werden. Ich habe darauf hingewiesen, daß der Strafverfahrensänderungsentwurf 1989 eine Regelspeicherdauer für Kinder von 2 Jahren vorsieht, und demgemäß die Speicherfrist für Kinder in der automatisiert geführten Zentralen Namenskartei ebenfalls nur zwei Jahre nach Eingang des Verfahrens bei der Staatsanwaltschaft betragen sollte. Ich habe gefordert, auf diese Besonderheit bei der retrograden Erfassung zu achten und die bereits erfaßten Ermittlungsverfahren daraufhin zu überprüfen. Dem Anliegen wird Rechnung getragen werden.

6.7.3 Speicherregelungen in Sijus-Strafsachen

Das DV-Verfahren „Sijus-Strafsachen“ bietet die Möglichkeit, das Zentrale Namensverzeichnis in automatisierter Form zu führen. Regelungen für die Speicherdauer der im **Register** gespeicherten personenbezogenen Daten sind bisher noch nicht festgelegt worden.

Wie mir das Staatsministerium der Justiz mitgeteilt hat, bereitet die zur Entwicklung des DV-Verfahrens „Sijus-Strafsachen“ eingesetzte Arbeitsgruppe zur Zeit ein Löschungskonzept vor, das differenzierte Löschungsfristen für die Register vorsieht. Mit einer Realisierung sei im Jahre 1993 zu rechnen. Die Erforderlichkeit der im Konzept vorgesehenen Speicherungsdauer wird von mir überprüft werden.

Das DV-Verfahren „Sijus-Strafsachen“ bietet in seinem staatsanwaltschaftlichen Anwendungsbereich neben der Führung des Zentralen Namensverzeichnisses auch die Möglichkeit, Texte mit vorgegebenen Textbausteinen zu erstellen. Dabei verwenden die Schreibkanzleien im Regelfall die im DV-Verfahren hierfür vorgesehenen **Textverzeichnisse** und Programmabläufe. Darüber hinaus können die Schreibkanzleien mit einem gesonderten Textsystem Schriftstücke eigenständig und ohne Verwendung vorgegebener Textbausteine fertigen und diese in einer individuell festzulegenden Ablagestruktur speichern.

Wegen der unterschiedlichen technischen Möglichkeiten können automationsunterstützte Routinen zur Löschung von Textdateien **(Löschungsprogramme)** nicht bereitgestellt werden. Hinzu kommt, daß die Texte – abhängig vom Gang des Ermittlungsverfahren – unterschiedlich lange gespeichert werden müssen, was eine individuelle Entscheidung über die Löschungsdauer bedingt. In der Praxis werden daher bisher Textdateien nach drei Monaten individuell gelöscht, soweit keine Gründe für eine längere Speicherungsdauer vorliegen.

6.7.4 Mitteilung des Verfahrensausganges an die Polizei (Nr. 11 MiStra)

Anhand mehrerer Verfahrensakten habe ich mich über den Vollzug von Nr. 11 der Anordnung über Mitteilungen in Strafsachen (MiStra) durch die Staatsanwaltschaft unterrichtet. Nach dieser Vor-

schrift hat die Staatsanwaltschaft das Aktenzeichen und den **Ausgang des Verfahrens** der Polizei mitzuteilen, sofern diese um die Mitteilung gebeten hat. Dazu leitet die Staatsanwaltschaft das von der Polizei in der Regel der Ermittlungsakte beigefügte **Formblatt** an diese zurück. Die Mitteilung des Verfahrensausganges – je nachdem, ob die Justiz den der polizeilichen Anzeige zugrundeliegenden Tatverdacht bestätigt oder nicht – hat erhebliche Bedeutung für die polizeiliche Datenspeicherung.

Verstöße gegen Nr. 11 MiStra konnte ich bei der Staatsanwaltschaft nicht feststellen. In bereits erledigten, weggelegten Verfahren konnten in keinem Fall im Akt verbliebene Formblätter aufgefunden werden. Ob die Formblätter tatsächlich versandt worden waren, konnte ich jedoch nicht überprüfen, da in den **Einstellungsformblättern** der Staatsanwaltschaft **keine Anordnungsziffer bezüglich Nr. 11 MiStra vorgesehen** ist. Eine Verfügung durch den Sachbearbeiter oder Staatsanwalt erfolgt nicht. Ich habe vorgeschlagen, die Einstellungsformblätter hinsichtlich einer Anordnung „MiStra Nr. 11" zu ergänzen. Dies ist mittlerweile geschehen.

6.7.5 Beiziehen von nichtanonymisierten gerichtlichen Musterentscheidungen

In einem Verfahren stellte ich fest, daß auf Antrag des Verteidigers des Beschuldigten eine gerichtliche Musterentscheidung beigezogen wurde, ohne daß vorher die Personalien des Verurteilten oder der übrigen Prozeßbeteiligten unkenntlich gemacht worden wären.

Dies hält datenschutzrechtlichen Anforderungen nicht Stand: Die Kenntnis der Namen der im beigezogenen Urteil beteiligten Personen war in dem von der Staatsanwaltschaft betriebenen Ermittlungsverfahren nicht erforderlich. Die Namen waren daher unkenntlich zu machen. Auch wenn die das Urteil übermittelnde Stelle in erster Linie für die Anonymisierung Sorge zu tragen hat, so muß die Staatsanwaltschaft als Übermittlungsempfänger die Anonymisierung vor dem Einheften der Entscheidung in die Akte nachholen, um eine weitere unzulässige Kenntnisnahme personenbezogener Daten zu verhindern. Ich habe diese Unterlassung gerügt und die Staatsanwaltschaft aufgefordert, das Versäumte nachzuholen. Dies ist mittlerweile geschehen.

6.7.6 Vorverfahrensverzeichnis

Nach Eintrag einer Neuanzeige gegen einen Beschuldigten in das Zentrale Namensverzeichnis durch die Geschäftsstelle wird dem Staatsanwalt die Akte mit einem sog. „Vorverfahrensverzeichnis" des Beschuldigten vorgelegt. Bei diesem Verzeichnis handelt es sich um einen Ausdruck der früher gegen den Beschuldigten anhängigen Verfahren aus dem Zentralen Namensverzeichnis.

Bei Gewährung von Akteneinsicht wird das Vorverfahrensverzeichnis, wie Stichproben ergaben, **aus dem Akt entnommen**. Nach Auskunft der Staatsanwaltschaft wird das Vorverfahrensverzeichnis auch bei Anklageerhebung aus dem Akt genommen und vernichtet. Eine Übermittlung an Gerichte erfolge nicht. Bei Überprüfung des Auslaufes an die Amtsgerichte konnte ich jedoch in einem Verfahren den Verbleib des Verzeichnisses in der Akte feststellen; den übrigen Akten war das Verzeichnis entnommen worden. Ich habe die Staatsanwaltschaft aufgefordert, sicherzustellen, daß das Verzeichnis zuverlässig vor Auslauf entnommen wird.

Wird das Ermittlungsverfahren von der Staatsanwaltschaft eingestellt, so verbleibt das Vorverfahrensverzeichnis uneingeheftet im Akt. Dadurch ist es möglich, bei späterer Beiziehung des Vorgangs früher anhängige Verfahren, deren Akten bereits vernichtet wurden, festzustellen. Ich habe daher die Vernichtung des Vorverfahrensverzeichnisses nach Verfahrensabschluß gefordert.

Bei der Staatsanwaltschaft wurde mittlerweile eine Dienstanweisung getroffen, wonach das Verzeichnis bei Anklageerhebung vor dem Auslauf der Akte an das Gericht und im übrigen nach Verfahrensabschluß aus dem Akt zu entnehmen und zu vernichten ist.

6.8 Kontrolle einer Justizvollzugsanstalt

Um für die Novellierung des Strafvollzugsgesetzes weitere Erfahrungen zu sammeln, habe ich im Berichtszeitraum erneut eine datenschutzrechtliche Kontrolle bei einer Justizvollzugsanstalt durchgeführt. Als Ergebnis konnte ich feststellen, daß die JVA dem Datenschutz einen hohen Stellenwert beimißt.

6.8.1 Gefangenenpersonalakten

Die Personalakte enthält weitgehende Informationen über den Gefangenen, aber auch personenbezogene Daten über Dritte (z.B. Eltern, Geschwister, Ehefrau). Sie ist deshalb besonders sorgfältig vor unberechtigtem Zugriff zu schützen. Trotzdem hat **jeder Bedienstete** der Anstalt **jederzeit Zugriff** auf die **vollständige** Akte eines **jeden** Gefangenen. Wird die Akte nicht unmittelbar in der Geschäftsstelle eingesehen, so verbleibt nur ein Fehlblatt im Karteikasten, auf dem das entnehmende Referat und der Entnahmetag einzutragen sind. Der entnehmende Sachbearbeiter selbst ist jedoch nicht erkennbar.

Ich habe geltend gemacht, daß die Einsicht in die Gefangenenpersonalakte nur in dem Umfang erfolgen

sollte, wie sie zur jeweiligen Aufgabenerfüllung erforderlich ist. Angesichts der Sensibilität der in der Akte enthaltenen Daten sollte die **Einsichtnahme dokumentiert** werden, damit nachvollziebar ist, wer zu welchem Zeitpunkt vom Akteninhalt Kenntnis genommen hat und ob die Kenntnisnahme notwendig war. Auch habe ich erneut angeregt, für hochsensible Daten (z.B. angehaltene Briefe) **Sonderhefte** anzulegen.

Das Staatsministerium der Justiz ist dagegen der Auffassung, daß die Dokumentation der Einsichtnahme nicht erforderlich, die **Vergabe von differenzierten Zugriffsberechtigungen** und die Anlegung von **Sonderheften** nicht durchführbar sei. Da alle im Vollzug Tätigen zusammenarbeiten und daran mitwirken, die Aufgaben des Vollzugs zu erfüllen, und zur Aufstellung und Überprüfung des Vollzugsplanes für den Gefangenen sowie zur Vorbereitung wichtiger Entscheidungen Konferenzen mit den an der Behandlung maßgeblich Beteiligten durchgeführt werden, sei eine umfassende Information über den Gefangenen notwendig. Eine Einsichtnahme aus vollzugsfremden Gründen ließe sich durch eine Dokumentation der Einsichtnahme nicht nachweisen. Fehlentscheidungen durch Informationsdefizite wären daher vorprogrammiert, wenn sensible Aktenteile abgesondert und dafür differenzierte Zugriffberechtigungen vergeben würden. Zudem würde die Anlegung von Sonderheften zu einem unvertretbaren Verwaltungsaufwand führen.

Demgegenüber meine ich jedoch, daß keine sachlichen Gründe dafür bestehen, hochsensible Daten, die nicht ständig für die laufende Gefangenenbehandlung benötigt werden (z.B. Erkenntnisse über Dritte im Rahmen der Besuchsüberwachung oder Besucherüberprüfung, angehaltene Briefe des Gefangenen) jedem Vollzugsbediensteten ohne Kontrolle der dienstlichen Notwendigkeit zugänglich zu machen. Diese Daten sollten in **Sonderheften** gesammelt werden, auf die nur solche Bedienstete zugriffsberechtigt sein sollten, die im Rahmen ihrer konkreten Tätigkeit diese Daten benötigen. Im übrigen halte ich die Dokumentation der Einsichtnahme in die Personalakte und die damit gegebene Möglichkeit der Datenschutzkontrolle für ein geeignetes Mittel der Einsichtnahme aus vollzugsfremden Gründen vorzubeugen. Einen unvertretbaren Verwaltungsmehraufwand durch Anlegen von Sonderheften erkenne ich nicht.

6.8.2 Gesundheitsakten

Die Gesundheitsakten der Gefangenen, die bisher nicht ausgesondert wurden, werden im Aufnahmezimmer der Krankenabteilung der Anstalt, die von den Vollzugsabteilungen räumlich getrennt ist, **aufbewahrt.** Zugang zu den Akten hat der Arzt sowie das Sanitätspersonal. Nach der Entlassung aus der Justizvollzugsanstalt werden die Akten von den Personalakten des Gefangenen getrennt weiteraufbewahrt. Eine Aussonderung hat bisher noch nicht stattgefunden. Die Aussonderung der Gesundheitsakten und der dazugehörigen Karteikarten habe ich angemahnt. Bei der Übermittlung personenbezogener medizinischer Daten von Gefangenen durch das Personal der Krankenabteilung an die Anstaltsleitung wird die ärztliche Schweigepflicht beachtet.

6.8.3 Manuelle Karteikarten

Die alphabetisch geführte **Gefangenenkartei** enthält die Personengrunddaten, die Vorstrafen, den Haftgrund, das Bekenntnis, die Staatsangehörigkeit, Familienstand, Kinderzahl, Name und Wohnung der nächsten Angehörigen, den erlernten Beruf sowie die Tatgenossen der Gefangenen.

Ich habe gefordert, die Karteien gleichzeitig mit den Akten zu vernichten, da die Erforderlichkeit einer weiteren Aufbewahrung nicht ersichtlich ist.

Die **Kartei der psychologischen Problemfälle** wird von einem der Anstaltspsychologen von solchen Patienten angelegt, die ihn entweder freiwillig aufsuchen oder die besondere psychische Auffälligkeiten aufweisen. Zu Beginn der Behandlung weist der Psychologe den Gefangenen darauf hin, daß alle Angaben, die der Gefangene ihm anvertraut, der **Vertraulichkeit** unterliegen, soweit nicht die Sicherheit oder Ordnung der Anstalt betroffen ist.

Ich habe deutlich gemacht, daß die Angaben der Gefangenen, die den Anstaltspsychologen freiwillig als Patienten aufsuchen, dem Arztgeheimnis gem. § 203 Abs. 1 Nr. 2 StGB unterliegen. Eine Offenbarung solcher Angaben ist daher – auch wenn sie die Sicherheit und Ordnung der Anstalt betreffen – nur nach Abwägung der betroffenen Rechtsgüter im Einzelfall zulässig.

6.8.4 Listen

Die **Grunddaten** des Gefangenen, insbesondere Name und Wohnung der nächsten Angehörigen, Vorstrafen, werden nicht nur in der Gefangenenpersonalakte und der Gefangenenkartei gespeichert, sondern auf Bögen auch einer Reihe von Stellen (z.B. Lehrkräften, Werkdienstleitung) innerhalb der Vollzugsanstalt bekanntgegeben.

Eine Notwendigkeit, daß diese Stellen **sämtliche** Grunddaten der Gefangenen erhalten, kann ich nicht erkennen. So ist z.B. nicht ersichtlich, zu welchen Zwecken die Werkdienstleitung im Rahmen ihrer Aufgabenerfüllung Angaben über den nächsten Angehörigen, letzte Entlassung, Tatgenossen oder Vor-

strafen des Gefangenen bedarf. Ich habe daher gefordert, die Datenübermittlung auf das zur Aufgabenerfüllung erforderliche Maß zu beschränken.

In der **Kartei der Entlassungsnachrichten für Bewährungshelfer** befinden sich Entlassungsnachrichten des Sozialdienstes der Anstalt an den nach Entlassung des Gefangenen zukünftig zuständigen Bewährungshelfer. In der Entlassungsnachricht ist u.a. der Name des Gefangenen, der letzte Wohnort, Entlassung, Entlassungstag, Anschrift, der künftige Arbeitgeber, Bewährungsauflagen, Vorstrafen, verbüßte Strafe, Beruf/jetzige Tätigkeit, Führung und Arbeitsleistung im Vollzug sowie Hinweise zur Person, Bezugsperson, Angehörige des Gefangenen aufgeführt. Darüber hinaus wird der Bewährungshelfer jedoch auch um die Zusendung eines Durchschlages der regelmäßigen Berichte an die Anstalt gebeten. Letzteres soll es der Anstalt ermöglichen, sich bei auftretenden Schwierigkeiten des Probanden mit diesem in Verbindung zu setzen und ihn zu unterstützen.

Datenschutzrechtliche Bedenken hinsichtlich der von der Sozialabteilung übermittelten Daten bestehen nicht. Bedenken habe ich jedoch bezüglich der Bitte um **Übersendung eines Durchschlages der Bewährungsberichte** erhoben. Eine Rechtsgrundlage hierfür ist für mich nicht ersichtlich. Nach Entlassung des Gefangenen ist die Zuständigkeit der Anstalt für diesen beendet, so daß auch eine Erforderlichkeit für solche Berichte nicht gegeben ist. Ich habe daher die JVA aufgefordert, das Formblatt diesbezüglich zu berichtigen. Die Änderung des Formblattes ist mittlerweile veranlaßt.

6.8.5 Überwachung des Schriftverkehrs Gefangener

6.8.5.1 Schriftwechsel mit Datenschutzbeauftragten

Der Schriftwechsel Gefangener wird in der überprüften JVA – wie auch in anderen Vollzugsanstalten – **grundsätzlich überwacht**.

Das Staatsministerium der Justiz hält eine generelle Überwachung des Schriftwechsels, auch soweit es sich um Briefe des Gefangenen mit dem Bundesbeauftragten für die Unterlagen des Staatssicherheitsdienstes der ehemaligen DDR oder mit dem Datenschutzbeauftragten handelt, für zulässig:

Nach der einheitlichen Rechtsprechung des Bundesverfassungsgerichts und der Oberlandesgerichte könne der Schriftwechsel sämtlicher Gefangener, die sich im geschlossenen Vollzug befinden, ohne Einzelfallprüfung generell überwacht werden, zumindest soweit dies auf besondere Sicherheitsbedürfnisse der jeweiligen Justizvollzugsanstalten gestützt werde. Von der Überwachung seien gemäß § 29 Abs. 2 StVollzG nur ausgenommen Schreiben des Gefangenen an Volksvertretungen des Bundes und der Länder sowie an deren Mitglieder, soweit die Schreiben an die Anschriften dieser Volksvertretungen gerichtet sind und den Absender zutreffend wiedergeben, sowie an die Europäische Kommission für Menschenrechte. Der Gesetzgeber habe den Schriftverkehr mit anderen Stellen, wie z.B. mit Gerichten, Justizbehörden und auch mit dem Datenschutzbeauftragten, bewußt nicht von der Überwachung ausgenommen, um jedes Risiko, insbesondere durch mißbräuchliche Manipulation auf dem Transportweg oder durch Fehlleitungen, auszuschließen. Ein Mißtrauensvotum gegenüber bestimmten Adressaten von Gefangenenpost habe dem Gesetzgeber fern gelegen. Ein Anlaß, von der gesetzlichen Regelung abzuweichen, bestehe nicht.

Demgegenüber bin ich der Auffassung, daß nach § 29 Abs. 3 Strafvollzugsgesetz (StVollzG) zwar der Schriftwechsel Gefangener – soweit er nicht mit dem Verteidiger oder einem Abgeordneten geführt wird – aus **Gründen der Behandlung oder der Sicherheit oder Ordnung** der Anstalt überwacht werden darf. Ein Eingriff in das auch einem Gefangenen zustehende grundgesetzlich geschützte Briefgeheimnis ist daher nur zulässig, soweit er aus den in § 29 Abs. 3 StVollzG geregelten Überwachungsgründen notwendig ist. Dies schließt eine **generelle** Überwachung des Schriftwechsels aus. Die JVA hat vielmehr im Einzelfall zu prüfen, ob diese Überwachungsgründe vorliegen, wobei ein generalisierender Maßstab bei der Beurteilung angelegt werden kann. Das Vorliegen solcher Überwachungsgründe beim Schriftwechsel des Gefangenen mit dem Bundesbeauftragten für die Unterlagen des Staatssicherheitsdienstes der ehemaligen DDR oder mit mir vermag ich nicht zu erkennen.

6.8.5.2 Briefkontrollen

Die **Briefkontrolle** wird dokumentiert, indem auf das auslaufende Schreiben des Strafgefangenen ein Datumsstempel mit Handzeichen des kontrollierenden Bediensteten als **Sichtvermerk** angebracht wird. Davon wird abgesehen, wenn der Gefangene dies unter Darlegung eines berechtigten Interesses beantragt oder aus dem Inhalt des Schreibens ersichtlich ist, daß die Anbringung des Sichtvermerkes untunlich ist.

Das Staatsministerium der Justiz hält die Anbringung von Sichtvermerken für eine notwendige Maßnahme zur Aufrechterhaltung der Sicherheit und Ordnung einer Justizvollzugsanstalt:

Der Sichtvermerk diene der Feststellung, ob und ggf. von welchem Bediensteten ein Schreiben in der Anstalt überprüft worden sei. Die Anbringung eines Sichtvermerks könne z.B. von Bedeutung sein, wenn ein Gefangener im Rahmen seines Schriftwechsels

erneut eine Straftat begangen oder die Sicherheit der Allgemeinheit in sonstiger Weise beeinträchtigt habe. Sollte die Briefüberwachung übergangen worden sein, so könnten die erforderlichen Maßnahmen getroffen werden, um dies künftig zu vermeiden. Darüber hinaus diene der Sichtvermerk dem Nachweis der ordnungsgemäßen Weiterleitung des Briefes durch die Anstalt. Beschwerden und Rückfragen in diesem Zusammenhang könnten ohne weiteres nachgegangen werden.

Demgegenüber bin ich der Auffassung, daß die generelle Anbringung eines Sichtvermerkes keine hinreichende Rechtsgrundlage in § 29 Abs. 3 StVollzG findet. Diese Vorschrift ermächtigt nur zur Kontrolle des Schriftverkehrs. Das Anbringen eines Sichtvermerkes führt darüber hinaus zu einem Eingriff in das allgemeine Persönlichkeitsrecht des Gefangenen, da die Empfänger des Schriftstückes aufgrund des Sichtvermerkes den Schluß ziehen können, daß sich der Absender in Haft befindet. Diesen Rechtseingriff halte ich auch nicht für erforderlich, da es der Anbringung eines Sichtvermerkes auf den ausgehenden Schreiben des **Strafgefangenen** zur Überwachung des Schriftwechsels nicht bedarf. Wie die Durchführung der **Kontrolle von Briefen der Untersuchungsgefangenen** zeigt, ist eine Überwachung des Schriftwechsels durchaus ohne Anbringung eines Sichtvermerkes möglich.

Bei Untersuchungsgefangenen werden nämlich ausgehende Schreiben in einem **Begleitumschlag** dem Untersuchungsrichter vorgelegt, der seine Vermerke auf einem Begleitbrief und nicht auf dem Schreiben des Gefangenen anbringt. Die Begleitumschläge werden in Sammelakten bei den Gerichten aufbewahrt und nach einem Jahr nach Weglegung der Akte ausgesondert.

Ein vergleichbares Verfahren wäre daher – ohne erheblichen Verwaltungsmehraufwand – bei der Briefkontrolle in Justizvollzugsanstalten denkbar.

In Betracht kommt auch die **Anlegung von Listen**, in der die ausgehende Post des Gefangenen zum Nachweis der Kontrolle dokumentiert sind.

6.8.5.3 Privatanschrift des Gefangenen

In den Justizvollzugsanstalten sind die Gefangenen grundsätzlich gehalten, bei ausgehenden Schreiben nicht ihre **Privatanschrift**, sondern die **Adresse der Anstalt** anzugeben, wobei dem Gefangenen gestattet wird, die Bezeichnung „JVA" wegzulassen. Zudem wird dem Gefangenen die Möglichkeit gegeben, das **Postfach der Anstalt** ohne Angabe des Straßennamens zu verwenden. Die Angabe der Privatanschrift ist nur dann möglich, wenn der Gefangene ein berechtigtes Interesse darlegt oder ein solches sonst ersichtlich ist.

Die JVA begründet diese Praxis damit, daß sie den Gefangenen bei der Täuschung des Empfängers über seine postalische Anschrift nicht unterstützen wolle. Zudem wolle man vermeiden, daß der Gefangene seine Heimatanschrift zur Begehung neuer Straftaten mißbrauche.

Das Staatsministerium der Justiz teilt die Auffassung der JVA. Wohnsitz und gewöhnlicher Aufenthaltsort seien begrifflich nicht deckungsgleich. Nach der Lebenserfahrung sehe der Empfänger eines Schreibens die Absenderadresse als den gewöhnlichen Aufenthaltsort an, so daß der Gefangene sehr wohl eine Täuschungshandlung bei Verwendung seiner Heimatanschrift begehe. Da eine lückenlose Briefkontrolle nicht durchführbar sei, bestünde durchaus die Gefahr, daß die Wohnsitzadresse zur Begehung neuer Straftaten mißbraucht werde.

Demgegenüber bin ich der Auffassung, daß eine Täuschung durch den Gefangenen dann nicht vorliegt, wenn er seine Heimatanschrift verwendet, soweit er dort noch einen Wohnsitz begründet. Eine Notwendigkeit, die Adresse der JVA vorzuschreiben, um neuen Straftaten vorzubeugen, sehe ich nicht, da bereits durch die Kontrolle des Schriftverkehrs Vorbereitungshandlungen für Straftaten entdeckt werden können. Nach meiner Ansicht sollte daher dem Gefangenen grundsätzlich gestattet sein, seine Heimatanschrift zu verwenden, soweit keine Anhaltspunkte für einen Mißbrauch vorliegen. Sollte die JVA aber Wert darauf legen, daß sie das Antwortschreiben des Emfängers kontrollieren kann, so besteht diese Möglichkeit auch bei der Angabe der Heimatadresse, wenn der Brief von einem Besucher in die Anstalt gebracht wird.

6.8.6 Besucherverkehr

Soweit der Besucher eines Gefangenen nicht hinreichend bekannt ist, und eine polizeiliche Überprüfung angezeigt erscheint, werden **Besucher** polizeilich **überprüft**. Dabei ersucht die Anstalt die Polizei im Wege der Amtshilfe schriftlich um Feststellung, ob die vom Gefangenen angegebenen Daten des Besuchers zutreffen und ob über diesen polizeiliche Erkenntnisse vorliegen, die gegen einen Besuch des Gefangenen sprechen. Sind dabei Erhebungen erforderlich, bittet die Anstalt, diese „vertraulich, so schonend wie möglich und vor allem ohne jede Bloßstellung der zu überprüfenden Person durchzuführen". Der Gefangene oder der überprüfte Besucher werden von der Justizvollzugsanstalt über die Überprüfung nicht unterrichtet.

Die Besucher von Gefangenen werden derzeit auf der Grundlage der §§ 24 und 25 Strafvollzugsgesetz

überprüft. Diese Vorschriften stellen jedoch mangels Normenklarheit keine ausreichende Rechtsgrundlage für die Überprüfung dar. Die Überprüfung von Besuchern kann daher allenfalls auf den sog. Übergangsbonus gestützt werden. Rechtseingriffe durch die Polizei sind nur unter den Voraussetzungen des Polizeiaufgabengesetzes zulässig.

Nach dem vorläufigen Referentenentwurf zum Vierten Gesetz zur Änderung des Strafvollzugsgesetzes soll § 24 Abs. 3 StVollzG ein Satz 2 angefügt werden, wonach aus Sicherheitsgründen ein Besuch von einer Zustimmung des Besuchers zur Einholung von Auskünften über ihn bei anderen Behörden abhängig gemacht werden darf.

Bis zur Novellierung des Strafvollzugsgesetzes sollte daher der Besucher, bevor er auf die Besucherliste gesetzt und zu diesem Zwecke überprüft wird, erfahren, daß der Gefangene beantragt hat, ihn auf die Liste zu setzen, und seine Person überprüft werden soll. Dem **Besucher** sollte damit die **Möglichkeit** gegeben werden, zu **entscheiden**, ob er den Gefangenen besuchen und sich deswegen überprüfen lassen will.

6.8.7 Vernichtung erkennungsdienstlicher Unterlagen

Nach § 86 Abs. 3 StVollzG sind Gefangene spätestens bei Entlassung darüber zu belehren, daß sie nach der Entlassung aus dem Vollzug verlangen können, daß die gewonnenen erkennungsdienstlichen Unterlagen vernichtet werden, sobald die Vollstreckung der richterlichen Entscheidung, die dem Vollzug zugrundegelegen hat, abgeschlossen ist. Diese **Belehrung** geschieht in der JVA bereits **bei** der **Aufnahme des Gefangenen**.

Soweit ein Gefangener die Vernichtung dieser Unterlagen verlangt, werden die Lichtbilder in der JVA vernichtet. Bei Strafgefangenen und Sicherheitsverwahrten mit einer Vollzugsdauer von mehr als drei Jahren wird dem Landeskriminalamt jedoch trotz des Antrages auf Vernichtung der Unterlagen neben der Entlassungsnachricht nach Nr. 51 Abs. 2 der Vollzugsgeschäftsordnung (VGO) ein Abzug des zuletzt gefertigten Lichtbildes beigefügt. Die übrigen Unterlagen werden vernichtet.

Aufgrund der relativ langen Verweildauer der Gefangenen in der geprüften JVA habe ich angeregt, den Gefangenen bei der **Entlassung** (erneut) darauf hinzuweisen, daß sie einen Antrag auf Vernichtung der erkennungsdienstlichen Unterlagen stellen können. Die Praxis, trotz des Antrages des Gefangenen auf Vernichtung der erkennungsdienstlichen Unterlagen ein Lichtbild dem Landeskriminalamt zu übermitteln, hält nach meiner Auffassung datenschutzrechtlichen Anforderungen nicht stand:

Zum einen geht der Gefangene irrtümlich davon aus, daß sämtliche Unterlagen auf seinen Antrag hin vernichtet worden sind. Er hat keine Kenntnis davon, daß ein Lichtbild dem Landeskriminalamt übersandt wird. Zum anderen findet diese Handhabung in § 51 Abs. 2 VGO keine Rechtsgrundlage. Die VGO hat lediglich den Rechtscharakter einer Verwaltungsvorschrift. § 86 Abs. 3 StVollzG bestimmt demgegenüber, daß erkennungsdienstliche Unterlagen nach der Entlassung auf Antrag des Gefangenen zu vernichten sind. Ich habe daher gefordert, daß in Zukunft eine Weitergabe eines Lichtbildes an das Landeskriminalamt unterbleibt, soweit der Gefangene einen Antrag auf Vernichtung der erkennungsdienstlichen Unterlagen gestellt hat. Eine andere Beurteilung wäre allenfalls dann denkbar, wenn die Polizei nach der Strafprozeßordnung oder dem Polizeiaufgabengesetz befugt ist, über den Gefangenen erkennungsdienstliche Unterlagen zu besitzen. Das Staatsministerium der Justiz hat mir mitgeteilt, daß die Weitergabe des Lichtbildes in Zukunft unterbleibt, wenn der Gefangene nach Beendigung des Vollzugs die Vernichtung der erkennungsdienstlichen Unterlagen beantragt.

6.9 Protokollierung der Einsicht im Grundbuch

Bereits im 10. Tätigkeitsbericht habe ich die Protokollierung der Einsichtnahme Dritter in das Grundbuch gefordert.

Das Grundbuch enthält eine Vielzahl sensibler personenbezogener Daten wie Eigentumsverhältnisse oder Belastungen, Gläubiger von Geldforderungen etc.

Nach § 12 Grundbuchordnung (GBO) ist deshalb die Einsicht in das Grundbuch nur demjenigen gestattet, der ein berechtigtes Interesse darlegt. Nur unter dieser Voraussetzung darf das Grundbuchamt einem Dritten Einsicht gewähren. Es hat also bei jedem Antrag auf Einsichtnahme zu prüfen, ob beim Antragsteller die gesetzlichen Voraussetzungen für eine Einsichtnahme vorliegen. Nur wenn sie im Einzelfall gegeben sind, muß der Eigentümer die Einsichtnahme und den damit verbundenen Eingriff in sein informationelles Selbstbestimmungsrecht hinnehmen. Das Grundbuchamt ist für die Beachtung des Grundrechts des Eigentümers verantwortlich. Zum Schutz des Grundrechts gehört aber auch, daß der Eigentümer nachprüfen kann, ob Dritten zu Recht Einsicht in seine persönlichen Verhältnisse gewährt worden ist. Mindestvoraussetzung einer Nachprüfungsmöglichkeit ist aber, daß die Einsichtnahme protokolliert wird. Obwohl also durch die Einsicht sensible, personenbezogene Daten bekannt werden können, wird bisher in Bayern die Einsichtnahme nicht protokolliert. Dadurch kann – wie bereits im 10. Tätigkeitsbericht geschildert – nicht einmal bei einem offenkundigen Mißbrauch der Einsicht die Person des Einsichtnehmenden festgestellt werden. Gleichwohl hat

das Staatsministerium der Justiz eine solche Protokollierung weder für zweckmäßig noch für geboten gehalten.

In Berlin sieht das vor kurzem in Kraft getretene Ausführungsgesetz zum Gerichtsverfassungsgesetz (AGGVG) vor, daß bei einer Einsichtnahme eines Dritten in Akten die Tatsache der Datenweitergabe in den Akten zu vermerken oder in der jeweiligen Datei aufzuzeichnen ist. Dementsprechend besteht dort nunmehr auch eine Pflicht der Grundbuchämter, Einsichtnahmen zu protokollieren. Nach der Verfügung der Präsidentin des Kammergerichtes an die Direktoren der Amtsgerichte zur Umsetzung der Protokollierungspflicht bei Grundbuchämtern werden **in einem lose bei den Akten befindlichen Verzeichnis Tag der Einsicht sowie Name und Anschrift** des Einsehenden handschriftlich eingetragen.

Unter Hinweis auf die Berliner Lösung habe ich mich erneut an das Staatsministerium der Justiz gewandt und eine **Protokollierungspflicht der Grundbuchämter** in Bayern gefordert. Das Ministerium hält jedoch wegen des zu erwartenden ganz erheblichen Aufwandes weiter an seiner ablehnenden Auffassung fest. Es weist außerdem darauf hin, daß der Bundesminister der Justiz Zweifel geäußert habe, ob eine Regelung über die Protokollierung der Grundbucheinsicht durch Landesrecht möglich sei.

Ich verkenne nicht, daß mit einer Protokollierung der Einsicht in das Grundbuch ein geringer Verwaltungsmehraufwand verbunden ist. Gleichwohl erscheint mir eine solche Protokollierung zum Schutz der in dem Grundbuch enthaltenen personenbezogenen Daten unerläßlich. Dabei kann es dahingestellt bleiben, ob die datenschutzrechtliche Forderung durch Ergänzung des Bundes- oder des Landesrechts umgesetzt wird. Das Grundrecht auf informationelle Selbstbestimmung beinhaltet das Recht des Bürgers zu wissen, wer, was, wann und bei welcher Gelegenheit über ihn weiß. Nach § 12 GBO braucht sich der in das Grundbuch Eingetragene nicht jegliche Einsichtnahme gefallen zu lassen, sondern nur wenn ein berechtigtes Interesse dargelegt wird. Dieses Recht muß organisatorisch ausreichend gesichert sein. Ist das Grundbuchamt aber wegen der **hohen Zahl der Einsichtnahmen** nicht mehr in der Lage, den Einzelfall nachzuvollziehen, so ist es für den Bürger nicht mehr möglich, den Kreis der Einsichtnehmenden festzustellen und die Rechtmäßigkeit einer Einsichtnahme zu überprüfen. Dies stellt eine Beeinträchtigung seines Grundrechtes dar. Die spätere Identifizierungsmöglichkeit der Person des Einsichtnehmenden mittels der Protokollierung der Grundbucheinsicht würde zudem einem Mißbrauch der Einsichtnahme vorbeugen.

6.10 Datenschutzbestimmungen im gerichtlichen und staatsanwaltschaftlichen Verfahren

6.10.1 Gewährung von Akteneinsicht durch die Staatsanwaltschaft

Durch die Gewährung von Akteneinsicht in die Ermittlungsakte können sensible personenbezogene Daten des Beschuldigten und sonstiger am Verfahren beteiligter Dritter dem Opfer sowie nicht verfahrensbeteiligten Dritten, die ein berechtigtes Interesse am Akteninhalt darlegen, offenbart werden. Der Staatsanwalt hat daher bei seiner Entscheidung über den Antrag auf Akteneinsicht das Interesse des Antragstellers und das Persönlichkeitsrecht der Betroffenen gegeneinander abzuwägen.

1. Nach § 406 e Abs. 2 Strafprozeßordnung ist den durch die Tat **Verletzten** die Einsicht in die Akte zu versagen, soweit überwiegende schutzwürdige Interessen des Beschuldigten oder anderer Personen entgegenstehen. Eine **schriftliche Niederlegung** der Gründe für die **Gewährung** der Akteneinsicht als Grundlage für die Überprüfung der staatsanwaltschaftlichen Entscheidung halte ich nicht für erforderlich. Ob die Akteneinsicht gerechtfertigt war, kann auch noch nachträglich aus dem Antrag in Verbindung mit den Verfahrensakten nachvollzogen werden. Ein Ermessen steht dem Staatsanwalt nicht zu.

2. Die Gewährung von Akteneinsicht für **nicht am Verfahren Beteiligte**, die jedoch ein berechtigtes Interesse für eine Akteneinsicht darlegen, ist bisher gesetzlich nicht geregelt. Sie hat ihre Grundlage derzeit noch in bundeseinheitlichen Verwaltungsvorschriften, nämlich den Richtlinien für das Straf- und Bußgeldverfahren (RiStBV) sowie den Richtlinien zum Jugendgerichtsgesetz (RiJGG). Da die Staatsanwaltschaften eingehende Schreiben fortlaufend in die Akten einheften, kann dies dazu führen, daß nicht verfahrensbeteiligten Dritten bei einer Akteneinsichtsgewährung auch solche **Aktenteile** offenbart werden, die **besonders sensible personenbezogene Daten** beinhalten (so z.B. Berichte der Jugendhilfe, der Bewährungshilfe und der Führungsaufsicht sowie medizinische Sachverständigengutachten) und für deren Kenntnisnahme kein berechtigtes Interesse besteht.

   Ich habe das Staatsministerium der Justiz darauf hingewiesen, daß die Akteneinsicht Dritter in Ermittlungsakten dringend einer gesetzlichen Regelung bedarf. Für eine gewisse Übergangszeit kann die Gewährung von Akteneinsicht ohne ausreichende Rechtsgrundlage hingenommen werden, sofern sie auf solche Aktenteile beschränkt wird, für deren Kenntnisnahme der Antragsteller ein **berechtigtes Interesse nachvollziehbar dargelegt**

hat. Die Gründe der Einsichtgewährung sind zu dokumentieren.

Das Staatsministerium der Justiz hat mir mitgeteilt, daß auch nach seiner Auffassung die Einsicht in Ermittlungs- und Strafakten einer gesetzlichen Regelung bedarf. Für die Übergangszeit sei beabsichtigt, den Landesjustizverwaltungen und der Bundesministerin der Justiz eine Ergänzung der bisher geltenden Richtlinien vorzuschlagen, wonach bestimmte Schriftstücke, durch welche Belange des Persönlichkeitsschutzes **typischerweise** in besonderem Umfang berührt werden, von der Akteneinsicht durch nicht am Verfahren beteiligte Dritte **grundsätzlich** auszunehmen seien. Zur praktikablen Handhabung sei geplant, **Sonderhefte** anzulegen, in denen solche Schriftstücke abzulegen seien. **Im übrigen** müsse nach den Umständen des Einzelfalles abgewogen werden, ob einer Akteneinsichtsgewährung schutzwürdige Interessen des Betroffenen entgegenstünden.

3. Die Gewährung von Akteneinsicht für **Anzeigenerstatter, die nicht zugleich Verletzte sind**, ist gesetzlich nicht geregelt und findet ebenfalls ihre Grundlage in den Verwaltungsvorschriften der RiStBV und RiJGG. So wird gemäß § 185 III RiStBV dem nicht verletzten Anzeigenerstatter über seinen bevollmächtigten Rechtsanwalt Akteneinsicht gewährt, wenn er ein **berechtigtes Interesse** darlegt und wenn **sonst Bedenken nicht bestehen**.

   Nach meiner Auffassung rechtfertigt **allein der Umstand**, daß der Anzeigenerstatter **Beschwerde** gegen den Einstellungsbescheid einlegt, **keine Akteneinsicht**. Durch die Akteneinsicht ist der Anzeigenerstatter nämlich in der Lage, personenbezogene Daten über den Beschuldigten zu erfahren, obwohl er durch die behauptete Tat des Beschuldigten selbst nicht unmittelbar in seinen Rechtsgütern verletzt ist.

   Das formelle Beschwerderecht kann nicht mehr Akteneinsicht vermitteln als die Position des Anzeigeerstatters. Voraussetzung muß stets ein überwiegendes berechtigtes materielles Interesse sein.

   Diesem Umstand trägt auch die Strafprozeßordnung insofern Rechnung, als der nicht verletzte Anzeigenerstatter zwar die Möglichkeit der Dienstaufsichtsbeschwerde und der Gegenvorstellung gegen den Einspruchsbescheid hat, nicht jedoch das gerichtliche Klageerzwingungsverfahren nach § 171 StPO durchführen kann. Der nicht verletzte Anzeigenerstatter, der außer dem Umstand seiner Anzeige und Beschwerde kein sonstiges Interesse am Ermittlungsverfahren darlegen kann, sollte daher keine Akteneinsicht durch die Staatsanwaltschaft erhalten.

6.10.2 Einstellungsbescheid der Staatsanwaltschaft an nicht verletzte Anzeigenerstatter

Stellt die Staatsanwaltschaft ein Ermittlungsverfahren ein, hat sie nach § 171 StPO den Anzeigeerstatter unter Angabe der Gründe zu bescheiden. Dies gilt auch dann, wenn der Anzeigeerstatter durch die behauptete Straftat nicht in seinen Rechten verletzt ist.

Ich habe gegenüber dem Staatsministerium der Justiz darauf hingewiesen, daß die Staatsanwaltschaft insbesondere in diesem Fall bei der Abfassung der Begründung des Einstellungsbescheides das Persönlichkeitsrecht der von dem Ermittlungsverfahren Betroffenen stärker als bisher berücksichtigen sollte.

Inhalt und Umfang der Begründung müssen neben dem Interesse des Anzeigeerstatters auch das Recht der Betroffenen auf informationelle Selbstbestimmung berücksichtigen. Dies gilt um so mehr, je schutzwürdiger die personenbezogenen Daten sind, von denen der Anzeigeerstatter durch die Begründung Kenntnis erhält. Ist der Anzeigeerstatter nicht zugleich auch Verletzter, sehe ich bei Abwägung der beiderseitigen Interessen keine Erforderlichkeit, dem Anzeigeerstatter z.B. besonders schutzwürdige Gesundheitsdaten im Wege des Einstellungsbescheides zu übermitteln. Auch die Strafprozeßordnung sieht in § 172 StPO nur für den Anzeigeerstatter, der zugleich Verletzter ist, die Möglichkeit der Beschwerde und des Klageerzwingungsverfahrens vor.

Das Staatsministerium der Justiz teilt grundsätzlich meine Auffassung. Die Mitteilung an den Anzeigenerstatter müsse diesem stets eine Entscheidung darüber ermöglichen, ob er als Nichtverletzter Gegenvorstellung oder Dienstaufsichtsbeschwerde gegen die Einstellung erheben will. Die Gründe der Mitteilung dürften dem Anzeigenerstatter keine unnötigen Einblicke in die Privatsphäre des Beschuldigten, Zeugen oder Dritter gewähren.

6.10.3 Einsicht in psychiatrische Gutachten

Im 11. und 12. Tätigkeitsbericht habe ich zwei Fälle geschildert, bei denen es in gerichtlichen Verfahren zu erheblichen Eingriffen in das Persönlichkeitsrecht der am Verfahren Beteiligten gekommen war, weil hochsensible Daten, die in psychiatrischen Gutachten enthalten waren, zur Kenntnis der anderen Verfahrenspartei gelangt sind und von diesen mißbräuchlich verwendet wurden.

Das Staatsministerium der Justiz hat mir mitgeteilt, daß der Persönlichkeitsschutz in gerichtlichen Verfahren – insbesondere im Zusammenhang mit psychiatrischen Gutachten – Gegenstand intensiver gesetzgeberischer Überlegungen des Staatsministeriums der Justiz sowie eines Meinungsaustausches mit der

Bundesministerin der Justiz und den übrigen Landesjustizverwaltungen sei.

Ich habe dem Staatsministerium der Justiz meine Überlegungen zur Verbesserung des Persönlichkeitsschutzes in gerichtlichen Verfahren mitgeteilt:

- Die **Leitungspflicht des Gerichtes** bezüglich der Tätigkeit des Sachverständigen sollte in den Verfahrensordnungen ergänzt werden: das Gericht hat einen Sachverständigen darauf hinzuweisen, daß das Gutachten personenbezogene Daten nur insoweit enthalten darf, als diese mit dem Gutachtensauftrag in unmittelbarem Zusammenhang stehen und das Ergebnis beeinflussen.

  Sollte das Gutachten dieser Anforderung nicht genügen, so sollte das Gericht die Möglichkeit haben, das Gutachten zurückzuweisen.

- Der **Betroffene** sollte über die Verwendung bzw. Verwendungsmöglichkeiten des Gutachtens (z.B. Übermittlung an Prozeßgegner) aufgeklärt werden.

- In die einzelnen Verfahrensordnungen sollte eine ausdrückliche Regelung aufgenommen werden, wonach die Einsicht **Dritter** in die Akten auch bei Vorliegen eines berechtigten Interesses zu versagen ist, soweit überwiegende schutzwürdige Interessen der Betroffenen entgegenstehen.

- **Umstände** aus dem persönlichen Lebensbereich der Betroffenen, die den Prozeßbeteiligten durch die gerichtliche Übersendung eines psychiatrischen Gutachtens bekannt werden, sollten der Verpflichtung zur Geheimhaltung unterliegen, soweit das Gericht ein entsprechendes Schweigegebot erläßt.

  Bisher kann das Gericht nach § 174 III Gerichtsverfassungsgesetz den Parteien lediglich **im Rahmen einer mündlichen Hauptverhandlung** die Geheimhaltung von Tatsachen zur Pflicht machen.

6.11 Übermittlung von Anschriften der Mitgliedsbetriebe der Handwerkskammer an Organe der Strafverfolgungsbehörden – keine Rasterfahndung

Eine Handwerkskammer teilte mir mit, daß sich Strafverfolgungsbehörden zunehmend an die Kammer wenden und zur Fahndung die Herausgabe von Anschriften bestimmter Gruppen von Mitgliedsbetrieben erbitten. In einem Fall (Unfallflucht mit tödlichem Ausgang) war nur ein Teil einer Fahrzeugaufschrift, die auf ein bestimmtes Handwerk schließen ließ, bekannt. Die Strafverfolgungsbehörde habe daraufhin um die Herausgabe der Anschriften aller in Betracht kommenden Handwerksbetriebe nachgesucht. Die Handwerkskammer war der Auffassung, daß Daten nur zur Erfüllung der ihr durch die Handwerksordnung zugewiesenen Aufgaben übermittelt werden dürfen und die Übermittlung von Daten über ihre Mitgliedsbetriebe zu Strafverfolgungszwecken unzulässig sei.

Nach meiner Auffassung, die auch vom Bayerischen Staatsministerium der Justiz geteilt wird, ist die Grundlage für das Auskunftsbegehren der Strafverfolgungsbehörde in §§ 160, 161 Strafprozeßordnung (StPO) zu sehen. Danach ist die Staatsanwaltschaft, wenn sie von dem Verdacht einer Straftat Kenntnis erhält, berechtigt, zur Sachverhaltserforschung von allen öffentlichen Behörden Auskunft zu erlangen. Diesem Auskunftsanspruch entspricht eine grundsätzliche Auskunftspflicht der ersuchten Behörden, die ihre Grenze in den Beschlagnahmeverboten nach § 97 StPO, einer Sperrerklärung durch die oberste Dienstbehörde nach § 96 StPO, dem Grundsatz der Verhältnismäßigkeit und besonderen Geheimhaltungspflichten der Behörde (z.B. Sozialgeheimnis) findet.

Dem Auskunftsanspruch der Staatsanwaltschaft stand auch die Sonderregelung über die Rasterfahndung (§ 98a StPO) nicht entgegen; denn im Gegensatz zur Rasterfahndung, bei der ein Datenabgleich von vermutlich auf den Täter zutreffenden Prüfungsmerkmalen mit anderen Daten erfolgt, waren im vorliegenden Fall konkrete Ermittlungsansätze vorhanden.

Die Handwerkskammer war deshalb berechtigt und verpflichtet dem Auskunftsbegehren der Staatsanwaltschaft zu entsprechen.

6.12 Beanstandungen

Aufgrund der Mitteilung eines Bürgers habe ich im Rahmen meiner anschließenden datenschutzrechtlichen Ermittlungen festgestellt, daß in einer Justizvollzugsanstalt im Jahre 1990 die Kopie einer Liste des Anstaltsarztes mit den Namen von 21 HIV-infizierten Gefangenen unberechtigt in die Hände von Mitgefangenen gelangt war und aus der Anstalt geschmuggelt wurde. Ob diese Liste wie von der Anstalt angegeben versehentlich vom Seelsorger einem Gefangenen zusammen mit dem Kirchenblatt ausgehändigt wurde, oder ob sie, wie in einem Zeitungsartikel zu lesen war, auf dem Gefängnisflur lag und weitergegeben wurde, konnte nicht mehr aufgeklärt werden.

Ich habe die im Ergebnis unzureichende Sicherung der Liste, die zu einem gravierenden rechtswidrigen Eingriff in das Recht auf informationelle Selbstbestimmung der in der Liste aufgeführten Gefangenen geführt hat, beanstandet und die Justizvollzugsanstalt aufgefordert, in Zukunft personenbezogene Unterlagen so zu verwahren, daß die unberechtigte Kenntnisnahme Dritter ausgeschlossen wird. Nach einer in-

ternen Anweisung wird in dieser Anstalt die HIV-Liste in Zukunft nur noch der Anstaltsleiter und dessen Vertreter erhalten.

Nach einer Behandlung dieses Falles im Datenschutzbeirat habe ich das Justizministerium um Mitteilung gebeten, wie in den übrigen Justizvollzugsanstalten mit HIV-Listen verfahren wird.

7. Landkreise, Städte und Gemeinden

7.1 Stärkerer Datenschutz im Gemeinderat

Am 1. September 1992 ist das Gesetz zur Änderung kommunalrechtlicher Vorschriften in Kraft getreten. Das Gesetz sieht in Art. 20 Abs. 4 der Gemeindeordnung und den entsprechenden Vorschriften der Landkreisordnung und Bezirksordnung höhere Sanktionen für Verstöße gegen den Datenschutz vor: Bei unbefugter Offenbarung personenbezogener Daten durch ehrenamtlich tätige Gemeindebürger beträgt das Ordnungsgeld bis zu 1000 DM. Bisher konnten Verstöße gegen die Sorgfalts- und Verschwiegenheitspflicht nur mit Ordnungsgeld bis zu maximal 500 DM belegt werden. Durch die Erhöhung der Obergrenze des Ordnungsgeldes bei unbefugter Offenbarung personenbezogener Daten wird der Bedeutung des allgemeinen Persönlichkeitsrechts und seinem Schutz im Gemeinderat angemessener als bisher Rechnung getragen.

Die Erhöhung der Obergrenze des Ordnungsgeldes auf 1000 DM geht auf meinen Vorschlag im Gesetzgebungsverfahren zurück. Mein weiterer Vorschlag, bei unbefugter Offenbarung personenbezogener Daten sollte dem Betroffenen das Ergebnis des Ordnungsgeldverfahrens mitgeteilt werden, wurde nicht berücksichtigt. Doch auch die Staatsregierung hält eine Unterrichtung des Betroffenen vom Ergebnis des Verfahrens für sinnvoll und hat mitgeteilt, das Staatsministerium des Innern werde nach Erlaß des Gesetzes die Kommunen besonders darauf hinweisen, daß ein Bürger, der die unbefugte Offenbarung seiner personenbezogenen Daten gerügt habe, davon zu unterrichten sei, welche Maßnahme die Kommune ergriffen habe.

Das Petitionsrecht (Art. 17 des Grundgesetzes und Art. 115 der Bayerischen Verfassung) gibt dem Bürger, der sich wegen unbefugter Offenbarung seiner personenbezogenen Daten im Gemeinderat an die Gemeinde wendet, einen verfassungsrechtlichen Anspruch auf Entgegennahme sowie auf sachliche Prüfung und Verbescheidung seiner Petition. Ich habe dem Staatsministerium des Innern empfohlen, in der Verwaltungsvorschrift zum Vollzug des Art. 20 Abs. 4 der Gemeindeordnung darauf hinzuweisen.

7.2 Prüfung eines Landratsamtes

1. **Beihilfe**

   Bei der Prüfung eines Landratsamtes mußte ich erneut feststellen, daß **Organisation und Verfahren der Beihilfeverwaltung** nicht den Anforderungen des Datenschutzes entsprechen.

   Nach der Organisation im Landratsamt ist für die Beihilfesachbearbeitung eine Mitarbeiterin des Personalsachgebiets zuständig. Die Sachbearbeiterin, die außerdem für Reisekosten zuständig ist, berechnet die Beihilfe, bereitet die Auszahlungsanordnung vor und leitet beides dem **Sachgebietsleiter der Personalverwaltung zur Unterschrift** zu.

   Die Beihilfeakten werden zusammen mit Personalakten in **einem** verschließbaren Schrank aufbewahrt. Einen Schlüssel zum Schrank besitzt die Beihilfesachbearbeiterin wie auch eine Personalsachbearbeiterin.

   Das Verfahren der Beihilfesachbearbeitung, die Aufbewahrung der Beihilfeakten und die Zuordnung der Beihilfeverwaltung zum Personalsachgebiet widersprechen dem **Gebot der sachlichen und organisatorischen Trennung von Personal- und Beihilfeverwaltung auf Sachgebietsebene**. Die Verstöße sind um so unverständlicher, als ich mich in meinen letzten Tätigkeitsberichten wiederholt unmißverständlich zu diesem Problem geäußert habe.

2. **Familienstand des Fahrlehrers**

   Auf den Antragsformularen auf Erteilung/Erweiterung einer Fahrlehrererlaubnis und auf Erteilung der Genehmigung für einen Gelegenheitsverkehr nach dem Personenbeförderungsgesetz wird jeweils nach dem Familienstand gefragt, ohne daß dieser für die Bearbeitung der Anträge erforderlich wäre.

   Ich habe das Landratsamt aufgefordert, von der Erhebung des Familienstandes künftig abzusehen.

3. **Unverschließbare Karteikästen mit Altakten**

   In einem Nebenraum der Registratur, der gleichzeitig Vorraum eines Putzraumes ist, habe ich unverschließbare Karteikästen mit Kfz-Scheinen, Führerscheinkarteikarten, Bodenverkehrsgenehmigungen und Sozialhilfeunterlagen (Rezepte, Krankenscheine, Suchkarten) vorgefunden. Eine Aussonderung hat seit Jahren nicht mehr stattgefunden.

   Ich habe das Landratsamt aufgefordert, die nicht mehr benötigten Karteikarten und Unterlagen ent-

sprechend den jeweiligen Richtlinien auszusondern (z.B. für erledigte Karteikarten und Akten der Zulassungs- und Führerscheinstelle nach der gemeinsamen Bekanntmachung der Staatsministerien des Innern und für Wirtschaft und Verkehr vom 11.10.1983, MABl. 1983, Seite 824).

Da der Raum, in dem sich diese Karteikarten und Unterlagen befinden, eine Tür zum Gang hat, die nicht immer verschlossen wird, mußte ich hier auch einen **Verstoß gegen die Datensicherheit** beanstanden.

4. **Verstöße gegen Datensicherheit**

Außerdem habe ich noch folgende Verstöße gegen die Datensicherheit festgestellt:

- Ausländerkarteien werden in verschließbaren **Karteikästen** aufbewahrt, die jedoch **nicht abgeschlossen** werden. Zum Zeitpunkt der Prüfung waren Schlüssel dazu nicht auffindbar.

- **Ungeschützter Zentralrechner**

  Das Sachgebiet Wasserrecht ist außerhalb des Hauptgebäudes untergebracht. Im Gang befindet sich der Zentralrechner. Da die Zugangstüre nicht abgeschlossen ist, kann nicht ausgeschlossen werden, daß Behördenfremde sich an den Geräten zu schaffen machen. Um den Zentralrechner zu sichern habe ich gefordert, die Zugangstüre mit einem Sicherheitsschloß (bündig mit Schließblech) zu versehen und für eine wirkungsvolle Zugangskontrolle zumindest eine Gegensprechanlage zu installieren. Behördenfremde dürfen sich nicht ohne Aufsicht im Flur aufhalten.

- **Gemeinsame Aufbewahrung von Originalunterlagen und Sicherungskopien**

  Im Sachgebiet Bauordnung werden die Schreibarbeiten mit Hilfe der EDV erledigt. Die Bauherrendaten sind auf Disketten gespeichert. Originaldisketten und Duplikate werden in demselben Blechschrank aufbewahrt. Aus Gründen der Datensicherheit habe ich gefordert, daß die **Sicherungskopien getrennt von den Originalunterlagen** sicher aufbewahrt werden.

- **Gemeinsame Aufbewahrung von Ausbildungs- mit Sachakten**

  Der Leiter des Umweltamtes ist gleichzeitig Ausbildungsleiter. Er bewahrt die Ausbildungsakten in einem abschließbaren Blechschrank neben den Aktenordnern mit den genehmigungspflichtigen Anlagen nach dem Bundesimmissionsschutzgesetz auf. Der Schlüssel zu dem Schrank wird in einem Schreibtisch im gleichen Zimmer in einem Fach aufbewahrt, das nicht abgeschlossen wird. Auf diese Weise können Unbefugte Zugang zu den Ausbildungsakten erhalten. Ich habe gefordert, daß die **Ausbildungsakten getrennt von den Sachakten** in einem Schrank aufbewahrt werden, zu dem nur der Ausbildungsleiter Zugang hat.

7.3 Weitergabe von Anträgen, Sitzungsunterlagen und Sitzungsniederschriften

Ein Bürger beschwerte sich darüber, daß eine Gemeinde seinen Antrag auf Erlaß eines Bauvorbescheids der örtlichen Presse übermittelt hat. Außerdem erhalte die Presse neben der Tagesordnung der öffentlichen Bauausschußsitzungen die diesbezüglichen Sitzungsvorlagen der Verwaltung, bestehend aus Sachvortrag und Beschlußvorschlag. Ihm seien die Vorlagen der Verwaltung zu seinem Vorbescheidsantrag hingegen nicht ausgehändigt worden. Schließlich gebe die Gemeinde auch die Sitzungsniederschriften an die örtliche Presse weiter, habe ihm gegenüber jedoch deren Herausgabe verweigert.

Mit dem Staatsministerium des Innern bewerte ich die Vorgänge aus datenschutzrechtlicher Sicht wie folgt:

- **Aushändigung der Tagesordnung an die Presse**

  Nach Art. 52 Abs. 1 Satz 1 und Art. 55 Abs. 2 der Gemeindeordnung sind Zeitpunkt und Ort der öffentlichen Sitzungen des Gemeinderats und der beschließenden Ausschüsse (hier: des Bauausschusses) unter Angabe der Tagesordnung ortsüblich bekanntzumachen. Bauanträge bzw. Anträge auf Erteilung eines Vorbescheids sind grundsätzlich in öffentlicher Sitzung zu behandeln.

  Die Art der ortsüblichen Bekanntmachung der Tagesordnung wird durch die Gemeinde selbst bestimmt, etwa durch Festlegung in der Geschäftsordnung des Gemeinderats oder durch die örtlichen Gepflogenheiten. So kann die Bekanntmachung z. B. durch Anschlag an den Gemeindetafeln, durch Mitteilung im Amtsblatt der Gemeinde und/oder auch in der Presse erfolgen.

  Die Aushändigung der Tagesordnung öffentlicher Sitzungen an die örtliche Presse kann daher je nach der örtlichen Praxis Voraussetzung einer ordnungsgemäßen Bekanntmachung der öffentlichen Sitzungen des Gemeinderats und seiner beschließenden Ausschüsse sein. Selbst wenn dies jedoch nicht der Fall sein sollte, ist die Weitergabe der Tagesordnung öffentlicher Sitzungen an die örtliche Presse aus datenschutzrechtlicher Sicht nicht zu beanstanden.

Die Tagesordnung nichtöffentlicher Sitzungen darf der Presse hingegen im Interesse der Geheimhaltung nicht bekanntgegeben werden.

- **Herausgabe des Antrags auf Erteilung eines Vorbescheids und der diesbezüglichen Sitzungsvorlage der Verwaltung an die Presse**

Da eine Einwilligung des betroffenen Bürgers zur **Weitergabe seines Antrags auf Erteilung eines Vorbescheids an die Presse** nicht vorlag, beurteilte sich die Herausgabe nach den Grundsätzen nach Art. 18 Abs. 1 BayDSG. Danach ist die Übermittlung an Dritte außerhalb des öffentlichen Bereichs zulässig, wenn der Empfänger ein berechtigtes Interesse an der Kenntnis der zu übermittelnden Daten glaubhaft macht und dadurch schutzwürdige Belange des Betroffenen nicht beeinträchtigt werden (Art. 18 Abs. 1 Satz 1 2. Alternative).

Die Presse konnte sich im vorliegenden Fall aus der Tagesordnung und in der öffentlichen Sitzung über das private Bauvorhaben informieren. Sie hatte jedoch kein berechtigtes Interesse an darüber hinausgehenden Informationen aus dem Antrag auf Erteilung eines Vorbescheids (z.B. Privatanschrift des Antragstellers sowie Einzelheiten des Vorhabens wie etwa Grundriß, genaue Maße, Ausstattung, Baumaterial etc).

Durch die Weitergabe des Antrags an die Presse wurden schutzwürdige Belange des Antragstellers beeinträchtigt. Dieser muß grundsätzlich darauf vertrauen können, daß mit seinem Antrag nur die zuständigen Stellen befaßt werden, der Antrag also im internen Bereich Bürger – Verwaltung – Entscheidungsgremium verbleibt.

Die Schutzwürdigkeit der Belange ist dabei vor allem auch anhand der berechtigten Interessen der – potentiellen – Empfänger an der Information zu messen. Fehlt ein derartiges berechtigtes Interesse, so sind schutzwürdige Belange durch die Übermittlung immer beeinträchtigt; ist das berechtigte Interesse an der Information gering, so genügt bereits eine geringe Beeinträchtigung schutzwürdiger Belange, um die Datenübermittlung unzulässig sein zu lassen. Da im vorliegenden Fall bereits kein berechtigtes Interesse der Presse an der Kenntnis der oben beschriebenen Informationen bestand, beeinträchtigte deren Weitergabe ohne Willen des Betroffenen dessen schutzwürdige Belange.

Auch bezüglich der **Sitzungsvorlage** konnte die Presse kein berechtigtes Interesse an der Herausgabe geltend machen. Sitzungsvorlagen der Verwaltung sind **interne** Ausarbeitungen für den Gemeinderat bzw. den Ausschuß. Die Vorlagen werden nur insoweit in die öffentliche Sitzung eingeführt, als sie der Bürgermeister mündlich vorträgt. An den Beschlußvorschlag ist der Gemeinderat bzw. der Ausschuß nicht gebunden. Für die Öffentlichkeit ist nur dessen Beschluß von Bedeutung, nicht jedoch die Empfehlung der Verwaltung und (interne) Bewertung des Antrags.

Auch der private Antragsteller hat keinen Anspruch auf die Herausgabe von (internen) Sitzungsunterlagen, die seinen Antrag betreffen.

- **Herausgabe und Veröffentlichung von Sitzungsniederschriften an die Presse**

Der Gemeinderat kann grundsätzlich beschließen, daß Niederschriften öffentlicher Sitzungen im gemeindlichen Amtsblatt zu veröffentlichen sind. Eine solche Veröffentlichung sieht die Gemeindeordnung zwar nicht vor; sie ist jedoch dann zulässig, wenn lediglich der in Art. 54 Abs. 1 der Gemeindeordnung vorgeschriebene Mindestinhalt veröffentlicht werden soll. Um mögliche Beeinträchtigungen von Interessen Dritter von vornherein zu vermeiden, sollte bei einer solchen Veröffentlichung im Amtsblatt darauf geachtet werden, daß sich die Bezeichnung der Behandlungsgegenstände nach denselben Grundsätzen richtet, die auch für die Bezeichnung der Tagesordnungspunkte bei der ortsüblichen Bekanntmachung nach Art. 52 Abs. 1 der Gemeindeordnung gelten. Im Hinblick darauf bestehen auch keine Bedenken, wenn Niederschriften über öffentliche Sitzungen, die lediglich die erforderlichen Mindestangaben enthalten, der örtlichen Presse zur Verfügung gestellt werden.

Niederschriften über nichtöffentliche Sitzungen dürfen nicht im Amtsblatt veröffentlicht werden. Selbstverständlich wäre in diesem Fall auch eine Weitergabe an die Presse unzulässig.

Die **Einsicht in die Niederschriften über öffentliche Sitzungen** steht nach Art. 54 Abs. 3 Satz 2 der Gemeindeordnung allen Gemeindebürgern frei. Daraus ergibt sich jedoch kein Recht des einzelnen auf Erteilung einer **Abschrift**. Die Erteilung von Abschriften ist aber auch nicht untersagt, so daß sie bei begründetem Anlaß nach Ermessen auch gewährt werden kann. Es ist nicht ermessensfehlerhaft, wenn die Gemeinde nur der Presse eine Abschrift der Niederschrift aushändigt und es im Hinblick auf den damit verbundenen möglichen Verwaltungsaufwand ablehnt, Gemeindebürgern Abschriften zu erteilen.

7.4 Mitnahme von Sitzungsunterlagen durch Gemeinderatsmitglieder

Eine Gemeinde fragte mich, ob Mitglieder des Gemeinderates Sitzungsunterlagen mit nach Hause nehmen dürfen.

Das Staatsministerium des Innern vertritt dazu die folgende Auffassung, die ich teile:

Zur Vorbereitung der Beratungsgegenstände für die Gemeinderatssitzung kann der erste Bürgermeister Sitzungsunterlagen bereits mit der Tagesordnung versenden. Enthalten die Unterlagen Angaben über besonders sensible, in nichtöffentlicher Sitzung zu behandelnde Beratungsgegenstände, so sollten sie lediglich als Tischvorlagen für die Dauer der Sitzung zur Verfügung gestellt werden.

In keinem Fall hat das einzelne Ratsmitglied einen Anspruch darauf, sämtliche Sitzungsunterlagen mit nach Hause zu nehmen und dort aufzubewahren. Die Art und Weise der Sachbehandlung und die getroffenen Entscheidungen werden durch die Aktenführung der Gemeindeverwaltung dokumentiert. Daneben ist die Anlegung „privater" Akten und Dateien durch Mandatsträger nicht erforderlich und im übrigen sogar in höchstem Maße bedenklich. Denn sie birgt stets die erhöhte Gefahr, daß in den Unterlagen enthaltene vertrauliche Informationen an unbefugte Dritte gelangen oder weitergegeben werden könnten. Dies ist mit der Zielsetzung des Art. 20 Abs. 2 GO nicht vereinbar.

Nach dieser Bestimmung haben die Gemeinderatsmitglieder (als ehrenamtlich tätige Gemeindebürger) über die ihnen bei ihrer ehrenamtlichen Tätigkeit bekanntgewordenen, geheimhaltungsbedürftigen Angelegenheiten grundsätzlich Verschwiegenheit zu bewahren. Bei den geheimhaltungsbedürftigen Angaben kann es sich auch um solche handeln, die in Unterlagen für eine öffentliche Sitzung enthalten, dort aber nicht zur Sprache gekommen sind. Denn die Nichtöffentlichkeit einer Sitzung ist zwar stets ein starkes Indiz für die Geheimhaltungsbedürftigkeit (Vertraulichkeit), sie ist jedoch nicht deren Voraussetzung. Somit bestehen auch gegen die private Sammlung und Aufbewahrung von Sitzungsunterlagen über öffentliche Sitzungen erhebliche Vorbehalte.

Nach Art. 20 Abs. 2 Satz 3 GO haben die Gemeinderatsmitglieder auf Verlangen des Gemeinderats einbehaltene Sitzungsunterlagen herauszugeben. Es ist auch denkbar, daß derartige Schriftstücke von vornherein nur unter der Auflage ausgehändigt werden, sie nach Behandlung der Angelegenheit in der Sitzung wieder an die Gemeindeverwaltung zurückzugeben. Im Hinblick auf Art. 20 Abs. 2 Satz 3 GO kann es jedoch auch zweckmäßig sein, einen Gemeinderatsbeschluß über die grundsätzliche Verpflichtung der Ratsmitglieder zur Rückgabe von Sitzungsunterlagen herbeizuführen.

7.5 Verteilung eines Anliegerschreibens an die Mitglieder des Stadtrates und Behandlung in öffentlicher Sitzung

Bürger einer Stadt, die sich als Nachbarn gegen die Sanierung und Erweiterung einer städtischen Sportanlage gewandt haben, haben mich um datenschutzrechtliche Überprüfung gebeten, ob die Stadt den Sitzungsunterlagen für die öffentliche Sitzung des Stadtrates, in der die Sanierung und Erweiterung der Sportanlage beraten worden war, als Anlage ein Schreiben der Anlieger der Sportanlage beifügen durfte, in dem diese ihre Zustimmung zu der vorgelegten Planung verweigert hatten. Das Schreiben habe die Adressen der Anlieger enthalten. Ich habe den Petenten folgende datenschutzrechtliche Bewertung der Angelegenheit mitgeteilt:

- **Verteilung des Anliegerschreibens an die Stadträte**

  Die Überlassung von Unterlagen mit personenbezogenen Daten an Stadtratsmitglieder zur Vorbereitung einer Stadtratssitzung war nicht nach dem Bayer. Datenschutzgesetz (BayDSG), sondern nach der Gemeindeordnung zu beurteilen, die nach Art. 2 Abs. 2 BayDSG dem allgemeinen Datenschutzgesetz vorgeht. Art. 14, 17 und 18 BayDSG schieden deshalb als Bewertungsmaßstab für diesen Vorgang aus.

  Die Verteilung des Anliegerschreibens an die Stadtratsmitglieder hielt sich im Rahmen des Art. 46 Abs. 2 der Gemeindeordnung. Nach Art. 46 Abs. 2 der Gemeindeordnung bereitet der erste Bürgermeister die Beratungsgegenstände für die Gemeinderatssitzungen vor. Das bedeutet, daß alle maßgeblichen tatsächlichen und rechtlichen Gesichtspunkte geklärt und mögliche Entscheidungsalternativen aufgezeigt werden müssen. Dabei sind die Gemeinderatsmitglieder in ausreichendem Umfang über die Angelegenheiten, die Gegenstand der Beratung und der Abstimmung sein sollen, zu informieren. Anderenfalls wäre eine sachdienliche Beratung und eine verantwortliche Teilnahme an der Beschlußfassung nicht möglich. Zur Vorbereitung der Beratungsgegenstände durch den ersten Bürgermeister gehört – neben dem mündlichen Vortrag – auch die Vorlage von Sitzungsunterlagen, die im Interesse eines ordnungsgemäßen Geschäftsganges insbesondere bei komplexen Angelegenheiten in Betracht kommen. Die Stadt hat in ihrer Stellungnahme die Auffassung vertreten, daß die Stadträte über die Einwendungen der Nachbarn unterrichtet sein sollten. Das schließt gerade in Bausachen, wo es um die Beteiligung der Nachbarn und die Entfernung zum Baugrundstück geht, die Kenntnis von Namen und Adresse ein. Die Verteilung des Anliegerschreibens an die Mitglieder des Stadtrates ist daher nicht zu beanstanden, zumal die Verteilung an Stadtratsmitglieder keiner Veröffentlichung gleichzusetzen ist, und die übermittelten Daten nicht von besonderer Sensibilität waren. Deshalb war auch die Einsammlung der Unterlagen nach der Sitzung nicht geboten.

– **Behandlung des Anliegerschreibens in öffentlicher Sitzung**

Nach Art. 52 Abs. 2 der Gemeindeordnung sind die Sitzungen öffentlich, soweit nicht Rücksichten auf das Wohl der Allgemeinheit oder auf berechtigte Ansprüche Einzelner entgegenstehen. Die Vorschriften des Bayerischen Datenschutzgesetzes stehen einer Behandlung des Bauantrages, des Bebauungsplanes und damit zusammenhängender Fragen in öffentlicher Sitzung des Gemeinderats oder eines Ausschusses grundsätzlich nicht entgegen, da, wie oben bereits dargelegt, das BayDSG hier nicht anwendbar ist. Nachbareinwendungen sind grundsätzlich in öffentlicher Gemeinderatssitzung zu behandeln. Ein generelles Geheimhaltungsinteresse der Nachbarn hinsichtlich ihrer Einwendungen gegen Bauvorhaben besteht im allgemeinen nicht. Lediglich wenn ausnahmsweise Rücksichten auf das Wohl der Allgemeinheit oder berechtigte Interessen Einzelner einer öffentlichen Behandlung entgegenstehen, wird in nichtöffentlicher Sitzung beraten und entschieden. Im Einzelfall kann aufgrund besonderer Umstände ein solches berechtigtes Interesse der Nachbarn an einer nichtöffentlichen Behandlung bestehen.

In dem zu entscheidenden Fall vermochte ich ein derartiges Interesse der Anlieger der Sportanlage nicht zu erkennen. Die Anlieger hatten sich mehrfach öffentlich mit Namen und Adresse gegen das Bauvorhaben gewandt, in Bürgerversammlungen geäußert und versucht, in öffentlicher Stadtratssitzung zu Wort zu kommen, um ihre Anliegen darzulegen. Das Bauvorhaben und die Nachbareinwendungen durften danach in öffentlicher Stadtratssitzung behandelt werden.

7.6 Weitergabe einer Unterschriftenliste einer Interessengemeinschaft an Mitglieder des Gemeinderates durch den ersten Bürgermeister

Eine Interessengemeinschaft hat um Überprüfung gebeten, ob der erste Bürgermeister einer Gemeinde berechtigt war, eine ihm übergebene Unterschriftenliste, in der Maßnahmen zur Sicherung der gemeindlichen Wasserversorgung gefordert wurden, an die Mitglieder des Gemeinderates weiterzugeben.

Mit dem Staatsministerium des Innern kam ich zu dem Ergebnis, daß die Weitergabe der Unterschriftenliste aus folgenden Gründen datenschutzrechtlich zulässig war:

Überprüfungsmaßstab für die Weitergabe der Unterschriftsliste war Art. 40 Abs. 1 des Gesetzes über kommunale Wahlbeamte, wobei bei der Beurteilung der Zulässigkeit der Weitergabe die Grundsätze des Bayerischen Datenschutzgesetzes entsprechend heranzuziehen waren. Die Weitergabe der Unterschriftsliste war danach zulässig, wenn sie **im Rahmen des dienstlichen Verkehrs zur rechtmäßigen Erfüllung der gesetzlichen Aufgaben** des ersten Bürgermeisters erforderlich war.

Durch die Vorlage der Unterschriftenliste an die Marktgemeindeverwaltung machte die Interessengemeinschaft von ihrem Petitionsrecht (Art. 56 Abs. 3 Gemeindeordnung, Art. 115 Bayerische Verfassung und Art. 17 Grundgesetz) Gebrauch. Da es sich bei der Forderung von Maßnahmen zur Sicherung des Fortbestandes der gemeindlichen Trinkwasserversorgung nicht um eine „laufende Angelegenheit" im Sinn des Art. 37 Gemeindeordnung handelte, sondern um eine Angelegenheit von grundsätzlicher Bedeutung, war zur Entscheidung darüber nicht der Bürgermeister, sondern der Gemeinderat zuständig (Art. 29 und 37 Gemeindeordnung). Aus diesem Grunde war der Bürgermeister nicht nur berechtigt, sondern sogar verpflichtet, den Gemeinderat über das Vorbringen der Interessengemeinschaft zu unterrichten. Dabei hatte er den Gemeinderatsmitgliedern auch Einsichtnahme in die vorgelegte Unterschriftsliste zu ermöglichen, damit sie sich aus der Zahl und den Namen der Unterschreibenden ihre Meinung über das Gewicht des beurkundeten Bürgerwillens bilden konnten. Besondere Maßnahmen zum Schutz der Daten in der Unterschriftsliste waren bei der Weitergabe an die Mitglieder des Gemeinderates nicht geboten, da es sich bei den Daten in der Unterschriftenliste nicht um besonders sensible Daten handelte und die Gemeinderatsmitglieder ihrerseits über die ihnen bei ihrer ehrenamtlichen Tätigkeit bekannt gewordenen geheimhaltungsbedürftigen Angelegenheiten zur Verschwiegenheit verpflichtet sind (Art. 20 Abs. 2 Gemeindeordnung). Für einen Verstoß gegen die Verschwiegenheitspflicht eines Gemeinderatsmitgliedes ergaben sich keine Anhaltspunkte.

Überdies lag nach meinen Ermittlungen die Unterschriftsliste mit bis zu 35 Eintragungen in örtlichen Geschäften frei zugänglich und völlig unbeaufsichtigt offen, so daß es jedem freistand, den Eintragungen beliebige Informationen zu entnehmen. Auch bei Unterschriftssammlungen von Haus zu Haus ist auf eine Abdeckung der vorangegangenen Einträge verzichtet worden. Jeder Bürger, der sich in die Liste eintrug, mußte daher damit rechnen, daß sein Name auch Dritten zur Kenntnis gelangen konnte und eine Geheimhaltung deshalb von vornherein nicht möglich war.

Aus diesen Gründen war es auch nicht zu beanstanden, daß der erste Bürgermeister die Unterschriftsliste den Gemeinderatsmitgliedern nicht schon von vornherein nur unter der Auflage aushändigte, diese nach Einsichtnahme wieder an die Gemeindeverwal-

tung zurückzugeben. Denn die Unterschriftenliste war keinesfalls von besonderer Sensibilität, die besondere Schutzmaßnahmen erfordert hätte.

7.7 Veröffentlichung von Angaben über Bauvorhaben

Im Berichtszeitraum habe ich mehrere Anfragen von Bürgern erhalten, die wissen wollten, ob personenbezogene Daten über Bauvorhaben, die im Gemeinderat bzw. Bauausschuß behandelt werden, veröffentlicht werden dürfen. Hierzu vertrete ich folgende Auffassung:

Die Bekanntgabe von Bauherrendaten über Bauanträge, die im Gemeinderat oder im Bauausschuß behandelt werden, beurteilt sich nicht nach dem Bayer. Datenschutzgesetz (BayDSG), sondern nach der Gemeindeordnung (GO), die nach Art. 2 Abs. 2 BayDSG dem allgemeinen Datenschutzgesetz vorgeht.

Bauanträge sind von den gemeindlichen Gremien grundsätzlich in öffentlicher Sitzung zu behandeln (Art. 52 Abs. 2 GO). Nach Art. 52 Abs. 1 GO sind Zeitpunkt und Ort der Sitzungen des Gemeinderats unter Angabe der Tagesordnung ortsüblich bekannt zu machen. Zur ordnungsgemäßen Bezeichnung des Tagesordnungspunktes ist bei Bauanträgen im Interesse der Transparenz des gemeindlichen Handelns für den Bürger im Regelfall erforderlich, daß die Angabe des Bauortes nach Straße und Hausnummer bzw. nach Flurnummer, ein Hinweis auf die Art des Bauvorhabens sowie der Name des Bauherrn genannt werden. Dies gilt auch dann, wenn ein Bauwerber der Veröffentlichung der Bauherrendaten gemäß Art. 84 der Bayer. Bauordnung (BayBO) widersprochen hat. Nach dieser Vorschrift dürfen die Bauaufsichtsbehörden (Landratsämter) und die Gemeinden Ort und Straße der Baustelle, Art und Größe des Bauvorhabens sowie Name und Anschrift des Bauherrn und des Entwurfsverfassers nur veröffentlichen oder an Dritte zum Zweck der Veröffentlichung übermitteln, wenn der Betroffene der Veröffentlichung nicht widersprochen hat. Diese Vorschrift will verhindern, daß kommerziellen Baustellen-Informationsdiensten die vollständigen Bauherrendaten gegen den Willen der Bauherren bekannt werden. Im Ergebnis ist somit festzustellen, daß die Veröffentlichung der zur ordnungsgemäßen Bezeichnung der Tagesordnung erforderlichen Bauherrendaten nach Art. 52 Abs. 1 GO und, wenn der Bauherr der Veröffentlichung nicht widersprochen hat, auch der weiteren in Art. 84 BayBO genannten Daten zulässig ist.

7.8 Herausgabe von Wahlbewerberdaten (NPD und Republikaner) für eine Dissertation

Im Rahmen seiner Dissertation im Fach Politikwissenschaft beabsichtigte ein Doktorand, einen Vergleich zwischen der NPD in den 60er und 80er Jahren und den Republikanern vorzunehmen. Hierzu beantragte er bei den bayerischen Wahlbehörden, ihm die Kandidatenlisten zu übersenden.

Das von mir eingeschaltete Staatsministerium des Innern teilte den nachgeordneten Behörden in Anlehnung an bereits früher in vergleichbaren Fällen mit mir getroffener Abstimmung mit, daß die Verwendung der für die Durchführung der Kommunalwahlen erforderlichen Daten auf den gesetzlich bestimmten (Wahl-)Zweck begrenzt sei und deshalb – insbesondere aus Datenschutzgründen – eine Herausgabe der Wahlvorschlagsdaten als Material für eine Dissertation nicht in Betracht komme. Für den angestrebten Vergleich erscheine die Kenntnis der Bewerbernamen nicht notwendig. Für die Dissertation würde die Zahl der Bewerber, deren Beruf und deren Alter genügen.

Das Staatsministerium des Innern empfahl den nachgeordneten Behörden, den Doktoranden an das Landesamt für Statistik und Datenverarbeitung zu verweisen, das über alle Wahlvorschläge zu den Kommunalwahlen verfügt. Diese restriktive Haltung gegenüber der Herausgabe von Wahlunterlagen, die in früheren Wahlverfahren bereits einmal veröffentlicht waren, zu einem späteren Zeitpunkt für Zwecke soziologischer Forschung entspricht der bereits bei anderer Gelegenheit vertretenen Auffassung, keine Kandidatennamen an Verlage zu liefern, welche Kandidatenlisten von früheren Kommunalwahlen veröffentlichen wollten. Sie entspricht ferner meiner Forderung, die Namen von gewählten Gemeinderäten nicht nach Partei, Beruf etc. geordnet der Handwerkskammer mitzuteilen.

7.9 Unzulässige Nutzung von Sozialdaten aus einem Wohngeldantrag durch den ersten Bürgermeister

Wohngeldanträge können bei den Gemeinden zur Vorprüfung der Angaben und Weiterleitung an das zuständige Landratsamt eingereicht werden. Die Gemeinde ist ebenfalls an das Sozialgeheimnis gebunden.

Der erste Bürgermeister einer Gemeinde, über dessen Schreibtisch der Wohngeldantrag eines Bürgers lief, schöpfte aufgrund der zur Begründung des Antrags gemachten Angaben den Verdacht auf Steuerhinterziehung, Urkundenfälschung und Betrug und sah sich veranlaßt, Strafantrag zu stellen und der Staatsanwaltschaft Daten aus dem Wohngeldantrag zu offenbaren.

Eine Offenbarung personenbezogener Sozialdaten zur Durchführung eines Strafverfahrens ist jedoch nach § 69 Abs. 1 Nr. 1 SGB X nur im Zusammenhang mit der Erfüllung einer gesetzlichen Aufgabe nach dem

Sozialgesetzbuch durch den Leistungsträger oder eine sonstige zur Berechnung oder Auszahlung von Sozialleistungen betraute Stelle zulässig. Der Gemeinde obliegt nach den wohngeldrechtlichen Vorschriften lediglich die Entgegennahme, Vorprüfung und Weiterleitung der Wohngeldanträge an die für die Bewilligung zuständige Stelle; über die Konsequenzen bei festgestellten Unstimmigkeiten hat die zuständige Wohngeldbewilligungsstelle zu entscheiden. Der Bürgermeister hätte seinen Verdacht durchaus äußern können, allerdings nicht gegenüber der Staatsanwaltschaft, sondern gegenüber dem Landratsamt.

Besonders pikant war dieser Verstoß gegen das Sozialgeheimnis, weil der durch den ersten Bürgermeister geäußerte Verdacht nach Feststellung der Staatsanwaltschaft jeglicher Grundlage entbehrte, der Betroffene also nicht nur von der unzuständigen Stelle, sondern dazu in der Sache völlig grundlos angeschwärzt wurde. Ich habe gegenüber dem ersten Bürgermeister die Unzulässigkeit der Offenbarung festgestellt.

7.10 Mieterinformation in förmlich festgelegten Sanierungsgebieten

In meinem letzten Tätigkeitsbericht habe ich über die Anfrage einer kreisfreien Stadt berichtet, die wissen wollte, ob es zulässig ist, daß das städtische Bauordnungsamt der „Familienhilfe" mitteilt, welche Gebäude in einem Sanierungsgebiet von einem Eigentümerwechsel betroffen sind. Die Stadt hatte mir mitgeteilt, die Familienhilfe, ebenfalls eine städtische Einrichtung, habe die Aufgabe, Mietern bei der Vermeidung von nachteiligen Auswirkungen durch städtebauliche Sanierungsmaßnahmen zu helfen. Die Bauordnungsbehörde erhalte die Mitteilung des bevorstehenden Eigentümerwechsels zur Prüfung ihres Vorkaufsrechts und zur Genehmigung der rechtsgeschäftlichen Veräußerung.

Mit dem Innenministerium bin ich der Auffassung, daß die Mitteilung von Wohngebäudeverkäufen in förmlich festgelegten Sanierungsgebieten an die Familienhilfe der Stadt und an die betroffenen Mieter unter folgenden Voraussetzungen zulässig ist:

Wird der Gemeinde zur Prüfung, ob ein gesetzliches Vorkaufsrecht besteht, ein Verkaufsfall angezeigt und besteht für das betreffende Grundstück ein Vorkaufsrecht der Gemeinde, so können die in diesem Rahmen mitgeteilten Daten über Verkäufer und Käufer des Grundstücks gemäß Art. 17 Abs. 1 und 3 BayDSG an andere Stellen innerhalb der Gemeinde weitergegeben werden, soweit dies zur Entscheidung über die Ausübung oder Nichtausübung des Vorkaufsrechts **erforderlich** ist oder soweit dies **erforderlich** ist, um baurechtliche Konsequenzen aus der Ausübung oder Nichtausübung des Vorkaufsrechts ziehen zu können. Art. 17 BayDSG gilt zwar bis zur Novellierung des Bayer. Datenschutzgesetzes nur für die Datenübermittlung aus Dateien, kann aber als allgemeiner Rechtsgedanke des Datenschutzrechts bei der Datenübermittlung aus Akten entsprechend angewendet werden.

In förmlich festgelegten Sanierungsgebieten und städtebaulichen Entwicklungsbereichen steht der Gemeinde stets ein Vorkaufsrecht zu.

In förmlich festgelegten Sanierungsgebieten hat die Gemeinde neben der Entscheidung über die Frage, ob sie das Vorkaufsrecht ausübt oder nicht, die Entscheidung über die Genehmigung einer rechtsgeschäftlichen Veräußerung eines Grundstücks nach § 144 Abs. 2 Nr. 1 BauGB zu treffen. Die im Rahmen dieses Verfahrens der Gemeinde zur Verfügung gestellten Daten können an **andere Stellen** innerhalb der Gemeinde (hier: Familienhilfe) weitergegeben werden, soweit dies für die Entscheidung über die Genehmigung oder Nichtgenehmigung der rechtsgeschäftlichen Veräußerung eines Grundstücks erforderlich ist, und soweit dies erforderlich ist, um aus der Genehmigung oder Nichtgenehmigung der rechtsgeschäftlichen Veräußerung eines Grundstücks baurechtliche Konsequenzen ziehen zu können. In diesem Rahmen ist eine Weitergabe der Daten an die Familienhilfe zulässig.

Eine **Information der Mieter** ist zulässig, wenn dies zur Erfüllung der oben beschriebenen Aufgaben der Gemeinde erforderlich ist. Hierbei ist zu berücksichtigen, daß die Gemeinde verpflichtet ist, sich bei der Entscheidung, ob ein Vorkaufsrecht ausgeübt oder einem Verkauf die Genehmigung erteilt oder versagt werden soll, die notwendigen Informationen hinsichtlich der Auswirkungen auf die betroffenen Mieter zu verschaffen. Wenn zur Entscheidungsfindung statistische Daten nicht ausreichen, sondern eine Erörterung zwischen der Gemeinde und den Mietern erforderlich ist, ist eine entsprechende Information der Mieter zulässig. Das Baugesetzbuch sieht selbst vor, daß die Gemeinde die Betroffenen zur Vermeidung negativer Auswirkungen über ihre Rechte zu informieren hat.

Diese Rechtslage ändert jedoch nichts an der Angemessenheit des sog. „zweistufigen Verfahrens" bei den Datenübermittlungen der Notare an die Gemeinde im Auftrag der Grundstücksverkäufer, mit denen die Verkäufer ihrer Mitteilungspflicht zur Prüfung, ob ein gemeindliches Vorkaufsrecht vorliegt, nachkommen. Daß zuerst der Gemeinde nur die Angaben über den Verkauf eines bestimmten Grundstücks mitgeteilt werden, die die Gemeinde in die Lage versetzen, festzustellen, ob überhaupt ein Vorkaufsrecht für dieses Grundstück gegeben ist, entspricht dem Erforderlichkeitsprinzip, d.h. dem datenschutzrechtlichen

Grundsatz, daß nur so viele Daten übermittelt werden dürfen, wie dies zur Aufgabenerfüllung erforderlich ist. Erst wenn die Gemeinde dem Notar mitteilt, daß überhaupt ein Vorkaufsrecht besteht, ist es gerechtfertigt, daß die Gemeinde den vollständigen Kaufvertrag erhält.

7.11 Bekanntgabe der Anschriften der Vereinsvorsitzenden im Mitteilungsblatt der Gemeinde

Ein Bürger bat mich um datenschutzrechtliche Überprüfung, ob Namen und Adressen der Vereinsvorsitzenden im Mitteilungsblatt der Gemeinde veröffentlicht werden dürfen.

Die Bekanntgabe von Adressen der Vereinsvorsitzenden im Mitteilungsblatt der Gemeinde dient dazu, den Bürgern die Kontaktaufnahme mit den örtlichen Vereinen zu erleichtern. In aller Regel haben die Vereine, die sich freiwillig bei der Gemeinde anmelden, selbst ein starkes eigenes Interesse daran, daß ihre Kontaktadressen den Bürgern bekannt sind und hierzu von der Gemeinde veröffentlicht werden. Von der Veröffentlichung muß die Gemeinde daher in diesen Fällen nur auf ausdrücklichen Wunsch eines Vereins absehen. Nur bei Zweifeln am Veröffentlichungsinteresse des Vereins sollte die vorherige Zustimmung eingeholt werden.

7.12 Regelmäßige Weitergabe aller Beihilfeunterlagen an das Rechnungsprüfungsamt

Anläßlich der Überprüfung einer Stadt stellte ich fest, daß sämtliche Beihilfeunterlagen, welche die Gesundheitsdaten nicht nur der Bediensteten, sondern auch von deren Familienangehörigen enthalten, ausnahmslos regelmäßig von der Beihilfestelle an das städtische Rechnungsprüfungsamt zu einer sog. Visaprüfung weitergeleitet werden.

Da ich diese regelmäßige Weitergabe **aller** Beihilfeunterlagen an den örtlichen Rechnungsprüfer für nicht unproblematisch hielt, stimmte ich mich mit dem für das Beihilferecht zuständigen Staatsministerium der Finanzen und dem Staatsministerium des Innern ab und habe auch den Bayerischen Kommunalen Prüfungsverband beteiligt. Übereinstimmend wurde festgestellt, daß die **regelmäßige** und ausnahmslose Weitergabe nicht erforderlich und damit unzulässig ist.

Selbstverständlich bestehen gegen eine stichprobenartige Überprüfung der Beihilfefestsetzungen durch das Rechnungsprüfungsamt keine Bedenken.

Die Stadt hat inzwischen durch Organisationsverfügung des Oberbürgermeisters für eine datenschutzgerechte Lösung gesorgt.

7.13 Veröffentlichung personenbezogener Daten von Bürgern in gemeindlichen Mitteilungsblättern

In früheren Tätigkeitsberichten habe ich wiederholt berichtet, daß die Bekanntgabe personenbezogener Daten wie Zuzüge, Wegzüge, Geburten und Sterbefälle, aber auch Gewerbeanmeldungen in gemeindlichen Mitteilungsblättern u.ä. **ohne (vorherige) Einwilligung** der Betroffenen unzulässig ist.

Auch im Berichtszeitraum mußte ich Verstöße beanstanden.

7.14 Datenschutz bei Aufgebotsbestellung nicht gewährleistet

Brautleute haben sich darüber beklagt, daß bei einem Standesamt **Aufgebotstermine für mehrere Paare gleichzeitig** durchgeführt würden. Dabei sei nicht ausgeschlossen, daß die übrigen Anwesenden Kenntnis von den anläßlich der Aufgebotsbestellung zu erhebenden und mitunter doch sehr sensiblen Daten (z.B. über voreheliche Kinder) des jeweiligen Brautpaares erhielten.

Der städtische Datenschutzbeauftragte trug vor, aufgrund der angespannten räumlichen Situation sei es nicht zu vermeiden, daß die Aufgebotsverhandlungen mehrerer Paare parallel geführt werden müßten. Da ein Ausbau weiterer Räume in nächster Zeit nicht zu erwarten sei, schlug er vor, im Warteraum ein Schild anzubringen, mit dem die Brautleute auf die Möglichkeit hingewiesen werden, auf Wunsch die Aufgebotsbestellung in einem Einzelzimmer (des stellvertretenden Standesamtsleiters) vornehmen lassen zu können.

Wegen der Sensibilität der Personenstandsdaten vermochte ich mich diesem Vorschlag übergangsweise anzuschließen und forderte wirksamere Abhilfe. Nach meinem Dafürhalten kommt generell nur eine individuelle Einzelberatung der Brautleute in Betracht. Meine Haltung hat dazu beigetragen, daß die Stadt derzeit intensive Überlegungen anstellt, wie die Situation doch durch bauliche Veränderungen entschärft werden könnte.

7.15 Auskunft aus der Kaufpreissammlung

Im 13. Tätigkeitsbericht habe ich mich zum Entwurf einer Gutachterausschußverordnung geäußert. Die Verordnung ist am 01. August 1992 in Kraft getreten. Sie regelt u.a., daß die Unterlagen zur Kaufpreissammlung geheimzuhalten sind und Auskünfte aus der Kaufpreissammlung nur erteilt werden dürfen, wenn sie zum Zweck der Wertermittlung des Grundstückes erforderlich sind und ein berechtigtes Interesse an der Auskunft nachgewiesen werden kann.

Gegenüber dem Staatsministerium des Innern hatte ich gefordert, in der Verordnung festzuschreiben, daß die Anfragen und das geltend gemachte berechtigte Interesse im Akt dokumentiert werden, da ohne ein Mindestmaß an Dokumentation der Geheimhaltungsschutz ins Leere gehe. Das Staatsministerium des Innern hat mir daraufhin mitgeteilt, daß es die Dokumentationspflicht in einer Vollzugsbekanntmachung zur Gutachterausschußverordnung regeln werde.

Die Vollzugsbekanntmachung wurde inzwischen erlassen. Die Gutachterausschüsse sind danach verpflichtet, das vom Antragsteller geltend gemachte berechtigte Interesse an der Auskunft aus der Kaufpreissammlung im Akt schriftlich festzuhalten. Dies gilt insbesondere für mündliche Anfragen.

7.16 Weitergabe von notariellen Urkunden durch den Gutachterausschuß an das Stadtsteueramt

Eine Stadt bat mich um Auskunft, ob eine Weitergabe von notariellen Urkunden durch den Gutachterausschuß an das Stadtsteueramt zulässig ist. Die Urkunden würden vom Stadtsteueramt zur Feststellung der Grundsteuerpflichtigen benötigt. Die Mitteilungen des Finanzamtes über erfolgte Eigentümerwechsel würden beim Stadtsteueramt erst nach ca. 1 Jahr eingehen.

Ich habe die Stadt darauf hingewiesen, daß die dem Gutachterausschuß zur Führung der Kaufpreissammlung übersandten notariellen Urkunden nach der Gutachterausschußverordnung geheimzuhalten sind. Sie dürfen nur von den Mitgliedern des Gutachterausschusses und den Bediensteten der Geschäftsstelle des Ausschusses **ausschließlich zur Erfüllung ihrer Aufgaben** – das sind insbesondere die Erstattung von Gutachten über den Verkehrswert von Grundstücken, das Führen einer Kaufpreissammlung und die Ermittlung der Bodenrichtwerte – eingesehen werden. Die Weitergabe der Urkunden an das Stadtsteueramt wäre danach unzulässig.

Auch eine Auskunft aus der Kaufpreissammlung an das Stadtsteueramt kommt nicht in Betracht. Nach § 195 Abs. 2 Baugesetzbuch darf die Kaufpreissammlung nur dem zuständigen Finanzamt für Zwecke der Besteuerung übermittelt werden. Unberührt bleiben nach dieser Bestimmung Vorschriften, nach denen Urkunden oder Akten den Gerichten oder Staatsanwaltschaften vorzulegen sind. Im übrigen sind nach § 11 Abs. 2 Satz 1 Gutachterausschußverordnung auf Antrag Auskünfte aus der Kaufpreissammlung zu erteilen, soweit ein berechtigtes Interesse nachgewiesen wird. Weitere Voraussetzung für eine Auskunftserteilung ist, daß sie zum **Zwecke der Wertermittlung** erforderlich ist (§ 11 Abs. 3 Satz 1 Gutachterausschußverordnung). Diese Voraussetzung ist hier nicht gegeben. Die Auskunft würde vom Stadtsteueramt zur Ermittlung von wechselnden Eigentümern im Rahmen des Besteuerungsverfahren verwendet. Sie wäre also nicht zum Zwecke der Wertermittlung einer damit befaßten Behörde erforderlich. Im übrigen dürfte eine Auskunft aus der Kaufpreissammlung nach § 11 Abs. 2 Satz 3 Gutachterausschußverordnung ohnehin keine Angaben über die Namen und Anschriften der jetzigen und früheren Eigentümer enthalten.

7.17 Vorlage von Einkommensteuer- und Rentenbescheiden im Verfahren zur Erhebung einer Fehlbelegungsabgabe

In einem Schreiben fragte mich eine Bürgerin, ob das Landratsamt berechtigt sei, im Verfahren zur Prüfung der Erhebung einer Fehlbelegungsabgabe die Vorlage von Einkommensteuer- und Rentenbescheiden zu verlangen und warum denn die hierzu erforderlichen Daten nicht direkt beim zuständigen Finanzamt erhoben worden seien.

Ich habe der Petentin mitgeteilt, daß das Landratsamt nach § 5 Abs. 1 des Gesetzes über den Abbau der Fehlsubventionierung im Wohnungswesen (AFWoG) berechtigt ist, im Verfahren zur Prüfung der Erhebung einer Fehlbelegungsabgabe von jedem Inhaber einer öffentlich geförderten Wohnung im Sinne des Wohnungsbindungsgesetzes Einkommensnachweise anzufordern. Die Wohnungsinhaber sind jedoch nicht zur Vorlage von Einkommensnachweisen gezwungen. Falls die Betroffenen auf die Beibringung von Einkommensnachweisen verzichten wollen und die geforderten Nachweise nicht innerhalb der gesetzten Frist beibringen, muß das Landratsamt davon ausgehen, daß die Einkommensgrenze um mehr als 140 v. H. überschritten wird und damit die Voraussetzungen für die Befreiung von der Abgabepflicht nicht mehr vorliegen. Die Ausgleichszahlung wird dann automatisch auf den Höchstbetrag von 6,- DM pro Quadratmeter Wohnfläche festgesetzt. Die Petentin wurde im vorliegenden Fall vom Landratsamt in einem Informationsblatt auf diese Tatsache hingewiesen.

Die **direkte Anforderung von Einkommensnachweisen** beim Finanzamt durch die Fehlbelegungsabgabestelle wäre aus datenschutzrechtlichen Gründen **unzulässig**. Zwar kann die Fehlbelegungsabgabestelle Auskünfte beim zuständigen Finanzamt einholen. Ein solches Auskunftsersuchen ist jedoch nur zulässig, soweit dies die Durchführung des AFWoG erfordert. Wie bereits ausgeführt, kann jeder Wohnungsinhaber selbst entscheiden, ob er der Fehlbelegungsabgabestelle sein Einkommen nachweisen will. Falls ein Wohnungseigentümer diese Nachweise nicht erbringt, greift die gesetzliche Vermutung ein, daß die Einkommensgrenze um mehr als 140 v.H. überschritten wird. Sofern ein Wohnungsinhaber von dieser

Möglichkeit Gebrauch macht, ist ein Auskunftsersuchen der Fehlbelegungsabgabestelle an das Finanzamt zum Einkommen des Wohnungsinhabers rechtlich unzulässig, da das Einkommen zur Durchführung des Gesetzes über den Abbau der Fehlsubventionierung im Wohnungswesen wegen der gesetzlichen Vermutung nicht benötigt wird.

7.18 Einsichtsrechte der Nachbarn in Baugenehmigungsverfahren

Ein Bürger vertrat in einer Eingabe die Meinung, die Einsichtsrechte des Nachbarn im Baugenehmigungsverfahren seien zu großzügig.

Ich habe dem Bürger geantwortet, daß der Nachbar im Baugenehmigungsverfahren nur diejenigen Unterlagen einsehen darf, die zur Wahrnehmung seiner nachbarlichen Rechte erforderlich sind. Anders sieht es jedoch aus, wenn ein Verwaltungsgerichtsverfahren anhängig wird. Dann hat der Nachbar gemäß § 100 Abs. 1 Verwaltungsgerichtsordnung ein umfassendes Akteneinsichtsrecht, das sämtliche Antrags- und Planungsunterlagen des Bauherrn umfaßt. Hier ist abzuwägen zwischen den datenschutzrechtlichen Belangen des Bauherrn und den prozessualen Rechten des Nachbarn. Eine absolut gerechte Lösung in diesem Konflikt zu finden, ist mitunter schwierig. Es muß darum gehen, die jeweils unterschiedlichen Interessen auszugleichen. Im Baugenehmigungsverfahren ist dieser Interessenkonflikt nach meiner Ansicht in vertretbarer Weise gelöst.

7.19 Weitergabe eines Antwortschreibens des Landratsamtes an ein Kreistagsmitglied

Die Vorsitzende einer Interessengemeinschaft der Betreiber von Ausweichunterkünften für Asylbewerber in einem Landkreis beschwerte sich bei mir darüber, daß das Landratsamt ein Antwortschreiben an eine Betreiberin einer Ausweichunterkunft in Ablichtung an ein Kreistagsmitglied gesandt hat. Das Kreistagsmitglied hatte sich zuvor mit Beschwerden über die Behandlung von Asylbewerbern in der betreffenden Ausweichunterkunft an das Landratsamt gewandt. Das in Ablichtung an das Kreistagsmitglied weitergeleitete Schreiben enthielt Angaben, die auf sachliche Verhältnisse der betroffenen Unterkunftsbetreiberin schließen ließen.

Die Befugnis des Landratsamts zur Weiterleitung des Antwortschreibens ergab sich nicht aus einem speziellen Gesetz. Insbesondere konnte sich das Landratsamt bei der Weiterleitung des Schreibens nicht auf das Informationsrecht des Kreistagsmitglieds nach der Landkreisordnung berufen, da der Vollzug des Asylbewerberunterbringungsgesetzes nicht in den Zuständigkeitsbereich des Kreistages fällt, sondern eine Aufgabe des Landratsamtes als Staatsbehörde ist. Bei der Weitergabe des Schreibens handelte es sich um eine Datenübermittlung außerhalb des öffentlichen Bereichs. Diese war in entsprechender Anwendung der Grundsätze des Art. 18 BayDSG nur zulässig, wenn das Kreistagsmitglied ein berechtigtes Interesse an der Kenntnis der zu übermittelnden Daten glaubhaft machen konnte und dadurch schutzwürdige Belange der betroffenen Betreiberin der Ausweichunterkunft nicht beeinträchtigt wurden.

Dem Kreistagsmitglied war ein berechtigtes Interesse an der Kenntnisnahme der Mitteilung des Landratsamtes, die an die Betreiberin der Ausweichunterkunft für Asylbewerber gegangen ist, nicht abzusprechen. Denn das Kreistagsmitglied hatte sich im Interesse der untergebrachten Asylbewerber für die Behebung von Mängeln bei der Unterbringung eingesetzt. Es hatte deshalb ein berechtigtes Interesse zu erfahren, ob und wie das Landratsamt für Abhilfe sorgt.

Durch die Übersendung einer Ablichtung des Schreibens an die Betreiberin der Ausweichunterkunft wurden letztlich deren schutzwürdige Interessen nicht beeinträchtigt. Zum einen wurden in dem Schreiben nur Punkte angesprochen, die von dem Kreistagsmitglied bereits in seinen Beschwerden vorgebracht worden waren. Zum anderen handelte es sich nicht um besonders sensible persönliche Daten, so daß an die Schutzwürdigkeit keine übertriebenen Anforderungen gestellt werden durften. Schließlich war zu berücksichtigen, daß es dem Landratsamt möglich sein mußte, sein Verhalten in dieser Angelegenheit gegenüber Beschwerdeführern zu rechtfertigen. Dies durfte im vorliegenden Fall auch durch Weitergabe des Antwortschreibens geschehen.

8. Einwohnermeldewesen

8.1 Prüfungen

Die Überprüfung der automatisierten Einwohnermeldeverfahren habe ich fortgesetzt. Insbesondere wurden **kommunale Eigenentwicklungen** sowie **Verfahren privater Softwarehäuser** auf Rechtmäßigkeit und Erforderlichkeit der Datenverarbeitung kontrolliert.

Erfreulicherweise war festzustellen, daß die Verfahrensmängel, auf die ich in früheren Jahren in großer Zahl gestoßen bin, stark zurückgegangen sind. Dies ist einerseits auf den Druck, den die von mir beanstandeten Anwender auf ihre Softwarehersteller ausüben, aber auch auf eine relativ gut funktionierende unmittelbare Kommunikation zwischen den Softwareherstellern und meiner Geschäftsstelle zurückzuführen. Zu beanstanden waren noch folgende Mängel:

- Fehlende datenschutzrechtliche **Verfahrensfreigabe** und Unterrichtung meiner Geschäftsstelle (Art. 26 Abs. 2 und 4 BayDSG)
- fehlende **Datenschutzregistermeldungen** (Art. 7 BayDSG i.V.m. § 7 Datenschutzregisterverordnung)
- mangelhafte **Zugriffssicherung** (Verwendung von Trivialpaßwörtern)
- Nichtbeachtung der zweijährigen Befreiung von der **Wehrerfassung** bei Aus- und Übersiedlern § 41 Wehrpflichtgesetz)
- unzulässige Hinweise auf **Kindesadoptionen** im Melderegister
- unzulässige Hinweise auf Wahlausschluß**gründe**, wie z.B. Entmündigung, vorläufige Vormundschaft, Strafhaft
- Nichtbeachtung von verschiedenen **Auskunfts- und Übermittlungssperren** bei den regelmäßigen Datenübermittlungen (§ 13 BayMeldeDÜV)
- Unterlassen von Berichtigungen gemäß Art. 10 MeldeG

8.2 Veröffentlichung von Gefängnisinsassen und Heimbewohnern im Adreßbuch

Im 13. Tätigkeitsbericht habe ich die Veröffentlichung von Gefängnisinsassen und Behinderten in einem Adreßbuch angeprangert. Auf diesen Mißstand war ich bei einer Routinekontrolle gestoßen.

Im Berichtsjahr überprüfte ich nun systematisch **sämtliche** bayerischen Städte und Gemeinden, auf deren Gebiet sich eine Justizvollzugsanstalt befindet und die gleichzeitig Auskünfte an Adreßbuchverlage geben. Die Trefferquote lag bei 20 %. Ich habe die Städte beanstandet.

Da nun Personen, die in einem Krankenhaus, Pflegeheim oder in sonstigen Einrichtungen, die der Betreuung pflegebedürftiger oder behinderter Menschen, der Rehabilitation oder der Heimerziehung dienen, gemeldet sind, ebenfalls einer Beeinträchtigung ihrer schutzwürdigen Belange durch Erscheinen im Adreßbuch ausgesetzt wären, trug ich die Problematik den Staatsministerien des Innern und für Arbeit, Familie und Sozialordnung vor. Eine systematische Kontrolle sämtlicher Gemeinden, in denen solche Einrichtungen vorhanden sind, schied wegen des wohl unverhältnismäßigen Aufwandes aus.

Das Staatsministerium des Innern hat wunschgemäß in zwei Rundschreiben – die ich auszugsweise wiedergebe – **alle** bayerischen Meldebehörden aufgefordert, den schutzwürdigen Belangen des betroffenen Personenkreises besondere Bedeutung beizumessen:

„Nach Art. 35 Abs. 3 MeldeG dürfen die Meldebehörden den Adreßbuchverlagen Auskünfte über Vor- und Familiennamen, akademische Grade und Anschriften (Art. 34 Abs. 1 Satz 1 MeldeG) sämtlicher Einwohner, die das 18. Lebensjahr vollendet haben, erteilen. Die Auskünfte dürfen **nicht** erteilt werden, wenn der Betroffene der Weitergabe seiner Daten widersprochen hat oder wenn im Melderegister eine Auskunftssperre nach Art. 34 Abs. 5–7 MeldeG vermerkt ist.

Bei meldepflichtigen JVA-Insassen sowie bei Personen, die in einem Krankenhaus, Pflegeheim oder in sonstigen Einrichtungen, die der Betreuung pflegebedürftiger oder behinderter Menschen, der Rehabilitation oder der Heimerziehung dienen, gemeldet sind, ist bei Datenübermittlungen und bei Auskunftserteilungen Art. 25 Abs. 4 MeldeG zu beachten. Danach dürfen Daten dieses Personenkreises nur übermittelt werden, wenn die Meldebehörden durch Prüfung **im Einzelfall** – ausgenommen im Rückmeldeverfahren – festgestellt haben, daß durch die Übermittlung keine schutzwürdigen Belange des Betroffenen beeinträchtigt werden. Vor Melderegisterauskünften – dies gilt auch bei Auskünften an Adreßbuchverlage nach Art. 35 Abs. 3 MeldeG – ist der Betroffene **zu hören**. Erklärt sich dabei der Betroffene nicht ausdrücklich mit der Auskunftserteilung an den Adreßbuchverlag einverstanden, ist die Auskunft zu verweigern, weil davon auszugehen ist, daß durch die Veröffentlichung seines Namens unter der Anschrift der Einrichtung schutzwürdige Belange beeinträchtigt werden."

Da die Erteilung einer Auskunft – ohne vorherige Anhörung – über Namen in Verbindung mit der Anschrift der Justizvollzugsanstalt oder eines Krankenhauses, Pflegeheimes, einer Einrichtung, die der Betreuung pflegebedürftiger oder behinderter Menschen, der Rehabilitation oder der Heimerziehung dient, die schutzwürdigen Belange des betroffenen Personenkreises erheblich beeinträchtigen kann, habe ich außerdem die Eintragung einer entsprechenden Auskunftssperre von Amts wegen angeregt.

Das Staatsministerium für Arbeit, Familie und Sozialordnung hat die Problematik den Regierungen, dem Bayer. Landesamt für Versorgung und Familienförderung für den Bereich der Kurkliniken, dem Deutschen Herzzentrum München, dem Krankenhaus mit Rehabilitationsklinik für Rückenmarkverletzte Hohe Warte, dem Verband der Bayer. Bezirke, dem Bayer. Landkreistag und dem Bayer. Städtetag mit der Bitte um Kenntnisnahme, Beachtung und Bekanntmachung im Kreise der Mitglieder nahegebracht.

Auskünfte aus dem Melderegister an Adreßbuchverlage werden **auch künftig** von mir in die Überprüfungen von Gemeinden einbezogen.

8.3 „Erweiterte" Melderegisterauskünfte an Kreditauskunfteien, Inkassobüros usw.

Nach Art. 34 Abs. 2 MeldeG darf die Meldebehörde eine „erweiterte" Melderegisterauskunft bei Vorliegen eines „berechtigten Interesses" erteilen. Die Einzelheiten – insbesondere bei Kreditauskunfteien, Inkassobüros, Rechtsanwälten – sind in Nr. 34 der Vollzugsbekanntmachung zum Bayerischen Meldegesetz vom 28.04.1984 (MABl S. 177) geregelt. Als „berechtigtes Interesse" ist jedes von der Rechtsordnung erlaubte, insbesondere auch ein wirtschaftliches Interesse anzusehen (vgl. Nr. 34.2 VollzBekMeldeG).

Die Meldebehörden sind nach Art. 34 Abs. 2 Satz 2 MeldeG verpflichtet, den Betroffenen über die Erteilung einer erweiterten Melderegisterauskunft unter Angabe des Datenempfängers unverzüglich zu unterrichten. Ich halte es für geboten, daß bei der Meldebehörde ein Durchschlag verbleibt. Dadurch wird das gemeindliche Handeln – insbesondere auch für Überprüfungszwecke durch die Kommunalaufsichtsbehörde, die Rechnungsprüfung und den Landesbeauftragten für den Datenschutz – transparent. Diese Verfahrensweise würde auch dem Beschluß des Bundesverwaltungsgerichts vom 16.03.1988, 1 B 153/87 (Koblenz) entsprechen, wonach die Meldebehörde u.a. verpflichtet ist, die Behandlung und die Bescheidung von Anträgen auf Erteilung von erweiterten Melderegisterauskünften wahrheitsgetreu und vollständig in Akten nachzuweisen. Der Betroffene kann durch gesonderte Mitteilung oder mit Hilfe einer Ablichtung der Auskunft benachrichtigt werden.

Im übrigen habe ich mich zum Thema „Melderegisterauskünfte an Kreditauskunfteien u.ä." ausführlich in meinem 12. Tätigkeitsbericht (siehe dort unter Nr. 8.4.5) geäußert.

9. Ausländerwesen

9.1 Gesetz zur Neuregelung des Asylverfahrens

Am 1. Juli 1992 ist das Gesetz zur Neuregelung des Asylverfahrens in Kraft getreten.

1. **Erkennungsdienstliche Behandlung aller Asylbewerber**

   Das Gesetz sieht vor, daß nunmehr alle Asylbewerber zur Feststellung und Sicherstellung ihrer Identität erkennungsdienstlich behandelt werden.

   Bereits am 3. Mai 1991 hatte die Mehrheit der Datenschutzbeauftragten sich gegen die Erfassung aller Asylbewerber ausgesprochen, weil dies gegen den Grundsatz der Verhältnismäßigkeit verstoße; nur bei Zweifeln an der Identität sei eine erkennungsdienstliche Behandlung zulässig.

   Bundestag und Bundesrat haben diesen Einwänden zu Recht keine Beachtung geschenkt. Der Mißbrauch des Asyl- und Sozialhilfegesetzes durch gleichzeitige oder nacheinander geschaltete mehrfache Anträge läßt sich nur dadurch wirksam einschränken, daß bei grundsätzlich allen Asylbewerbern eine Identitätssicherung durchgeführt wird. Da nur 5–6 % der Asylbewerber vom Bundesamt für die Anerkennung ausländischer Flüchtlinge anerkannt werden und für abgelehnte Asylbewerber starke materielle Anreize für einen weiteren Aufenthalt in der Bundesrepublik bestehen, ist mit einer hohen Zahl von Zweitanträgen unter anderem Namen zu rechnen. Dabei kann kein (Erst-)Antragsteller von vornherein ausgeschlossen werden.

2. **Fertigung eines 10-Finger-Abdruckes**

   Das Gesetz läßt die Aufnahme der Abdrucke aller zehn Finger zu.

   Nach Auffassung der Mehrheit der Datenschutzbeauftragten sollte jedoch nur ein einziger Fingerabdruck genommen und verformelt werden, weil dies zur eindeutigen Feststellung der Identität genüge.

   Die Mehrheit legt hier den Grundsatz der Verhältnismäßigkeit viel zu eng aus. Es ist zwar richtig, daß die Identität einer Person auch schon durch die Langsatzverformelung eines einzigen Fingers bestimmbar ist. Wegen bestehender Umgehungsmöglichkeiten (z.B. durch Vernarbung des Fingers) ist der Gesetzgeber jedoch nicht gehalten, die Identitätssicherung auf den Abdruck eines einzigen Fingers zu beschränken, zumal es sich bei Fingerabdrücken nur um einen geringfügigen Eingriff handelt.

3. **Mitverwendung der ED-Unterlagen zur Strafverfolgung und Gefahrenabwehr**

   Informationen über Asylbewerber, die im Asylverfahren gewonnen worden sind, sollen nach dem Willen des Gesetzgebers auch zur Verfolgung von Straftaten und zur Abwehr einer erheblichen Gefahr für die öffentliche Sicherheit, z.B. zur vorbeugenden Bekämpfung von Straftaten, verwendet werden dürfen.

   Die Mehrheit der Datenschutzbeauftragten will die Asylbewerberdaten nur zur Aufklärung bestimmter, in einem Straftatenkatalog aufgezählter Straftaten zulassen. Zur Gefahrenabwehr sollten die Daten nur zur Abwehr einer gegenwärtigen er-

heblichen Gefahr für die öffentliche Sicherheit zugelassen werden.

Auch in diesem Punkt werden aus dem Verhältnismäßigkeitsgrundsatz zu weit gehende Forderungen abgeleitet. Es gibt keinen Grund, Asylbewerber gegenüber deutschen Staatsangehörigen zu privilegieren, deren Lichtbild nach den näheren Bestimmungen des Paß- und Personalausweisgesetzes für die Erledigung polizeilicher Aufgaben zur Verfügung steht.

10. Steuerverwaltung

10.1 Prüfung bei einem Finanzamt

Gegenstand der diesjährigen datenschutzrechtlichen Kontrolle eines Finanzamts waren Dateien, Karteien, Erhebungsvordrucke und nach bestimmten Gesichtspunkten ausgewählte Aktenunterlagen. In Dateien und Karteien wurde die Erforderlichkeit der erfaßten Informationen überprüft. Die Angabe der Rechtsgrundlage zur Datenerhebung war der Prüfzweck bei Erhebungsvordrucken, insbesondere bei solchen, die von der Dienststelle selbst abgefaßt waren. Die Steuerakten habe ich darauf überprüft, ob Datenübermittlungen von Dritten und an Dritte zulässig waren.

Die datenschutzrechtliche Überprüfung hat nur geringe Mängel ergeben:

1. **Datenspeicherung in Freitextfeldern**

Nach Abgabe z.B. der Einkommensteuererklärungen werden die zur Berechnung und Festsetzung erforderlichen Steuerdaten beim Finanzamt über Bildschirmmasken erfaßt und an den Zentralrechner beim zuständigen Zentralfinanzamt (München oder Nürnberg) übermittelt und dort gespeichert. Anhand der gespeicherten Informationen wird die Einkommensteuer berechnet und der Steuerbescheid ausgedruckt. Bestimmte Bildschirmmasken bieten dem Sachbearbeiter die Möglichkeit, Vermerke und Bearbeitungshinweise in Kurzform in sogenannte Freitextfelder einzugeben, auf die er bei den nächsten Steuerveranlagungen zurückgreifen kann.

Bei der Prüfung wurden beispielsweise folgende Eintragungen festgestellt:
- Bei den Kfz-Kosten ist einschließlich der AfA noch der Privatanteil abzuziehen. 1991 betrug er 25 %.
- Genaue Ermittlung der Werbungskosten für das Arbeitszimmer.
- Computer lt. Rechnung vom 11.12.90 DM 1498.-, AfA auf 3 Jahre = DM 500.-, davon 1/2 = 250 für 1990.
- Überwachungsfall (Abgabe der ESt-Erklärung) ab 1.1.1985!
- Verheiratet seit 4.8.77.
- § Kirchenaustritt zum 5.4.90.
- Geschieden seit 1986, verheiratet seit 20.11.87.

Die Beispiele zeigen, daß nicht mehr aktuelle Vermerke neben aktuellen, d.h. für die Sachbearbeitung erforderlichen, stehen. Die Löschung dieser Freitextangaben bei Wegfall der Erforderlichkeit ist bisher nicht geregelt. Ich habe deshalb die Entwicklung eines für die Sachbearbeitung wenig aufwendigen Löschverfahrens zumindest für Eintragungen sensibler Natur angeregt.

2. **Datenübermittlungen des Finanzamts an Dritte**

Datenübermittlungen des Finanzamts an Dritte wurden bei der stichprobenweisen Durchsicht der Steuerakten nicht festgestellt.

3. **Kontrollmitteilungen an das Finanzamt**

Bei der stichprobenweisen Aktendurchsicht fand sich die Kontrollmitteilung einer anderen staatlichen Dienststelle über eine unversteuerte Zahlung an den Steuerbürger. Für die Übersendung einer derartigen Kontrollmitteilung besteht jedoch derzeit keine Rechtsgrundlage. Von der in § 93 a Abgabenordnung enthaltenen Ermächtigung durch Rechtsverordnung Behörden zur Abgabe solcher Kontrollmitteilungen zu verpflichten, hat die Bundesregierung bislang noch keinen Gebrauch gemacht. Das Finanzministerium hat mit Rundschreiben vom 21. Juni 1990 alle Ministerien gebeten, „von der bisherigen Praxis allgemeiner Kontrollmitteilungen Abstand zu nehmen und die jeweils nachgeordneten Dienstbehörden entsprechend zu unterrichten." Auf die Ausführungen in meinem 12. Tätigkeitsbericht (Seite 39, Nr. 9.2) nehme ich Bezug.

Den Fund beim Finanzamt habe ich zum Anlaß genommen, das Ministerium, das für die noch immer Kontrollmitteilungen versendende Behörde zuständig ist, zu bitten, die Dienststelle nochmals auf die Rechtslage hinzuweisen, damit derartige Mitteilungen an die Finanzämter unterbleiben.

Bereits im 12. Tätigkeitsbericht, Seite 40, habe ich ausgeführt, daß ohne Rechtsgrundlage ausgefertigte Kontrollmitteilungen nach meiner Überzeugung einem Verwertungsverbot unterliegen. Solche Kontrollmitteilungen sind unzulässig, dürfen nicht ausgewertet werden und sind deshalb zu vernichten. Das Finanzministerium ist jedoch der Auffassung, daß zwar wegen der noch ausstehenden Kontrollmitteilungsverordnung des Bundes keine Verpflichtung zur Übermittlung von Kontrollmitteilungen bestehe; unberührt bleibe davon

jedoch die Zulässigkeit einzelner Mitteilungen und ihre Verwertbarkeit.

4. **Angabe der Rechtsgrundlage auf Datenerhebungsvordrucken**

   Das Finanzamt verwendet neben amtlich vorgeschriebenen auch selbstentworfene Vordrucke zur Datenerhebung. Auf einer Vielzahl der selbstverfaßten Vordrucke fehlte der in Art. 16 Abs. 2 BayDSG vorgeschriebene Hinweis auf die Rechtsgrundlage der Datenerhebung bzw. der Hinweis auf die Freiwilligkeit von Angaben.

   Ich habe die gründliche Überarbeitung dieser Formulare gefordert.

5. **Namenskartei und Bußgeldliste der Bußgeld-/Strafsachenstelle**

   In der Bußgeld- und Strafsachenstelle wird eine Namenskartei und eine Bußgeldliste über die Einleitung und Abwicklung von Straf- und Bußgeldverfahren geführt. Die Vernichtung dieser Unterlagen erfolgte bisher 30 Jahre nach Verfahrensende. Gemäß Nr. 4.5.3 der vorläufigen Bestimmungen zur Aufbewahrung und Aussonderung von Schriftgut bei den Finanzämtern sind diese Unterlagen jedoch schon nach 10 Jahren zu vernichten.

   Ich habe die nicht zeitgerechte Vernichtung beanstandet, die Einhaltung der Aussonderungsvorschrift gefordert und darauf hingewiesen, daß eine datenschutzgerechte Entsorgung dieser unter das Steuergeheimnis fallenden Unterlagen sicherzustellen ist.

6. **Rechtswidrige Verwendung steuerlicher Kenntnisse aus dem Besteuerungs- im Vollstreckungsverfahren**

   Die Finanzbehörden in Bayern vollstrecken aufgrund gesetzlicher Vorschriften auch Geldforderungen anderer Verwaltungen. In diesen Vollstreckungsverfahren für Dritte dürfen im Besteuerungsverfahren erlangte Kenntnisse gemäß § 249 Abgabenordnung nicht verwendet werden. Eine Änderung dieser Vorschrift ist im Entwurf eines Gesetzes zur Änderung der Abgabenordnung (AOÄG 1992) jedoch vorgesehen.

   Bei Durchsicht mehrerer Vollstreckungsakten wurde nur in wenigen Einzelfällen festgestellt, daß im Besteuerungsverfahren bekannt gewordene Bankkonten zur Begleichung von Geldforderungen anderer Verwaltungen durch das Finanzamt gepfändet worden sind. In der Mehrzahl der Fälle erfolgte die Beitreibung der Forderung nicht über eine Pfändung sondern durch einen Vollstreckungsbeamten des Finanzamts, der beim Schuldner die Begleichung der Geldforderung erwirkte. Bei dieser Vorgehensweise werden keine steuerlichen Erkenntnisse genutzt.

   Ich habe das Amt aufgefordert, bis zum Inkrafttreten der Gesetzesänderung zu § 249 Abgabenordnung auf die zweckfremde Nutzung steuerlicher Erkenntnisse bei der Beitreibung von Geldforderungen anderer Behörden zu verzichten.

7. **Verfahrensfreigabe und Meldung zum Datenschutzregister**

   Aufgrund einer Dienstvereinbarung mit dem Personalrat wird beim Finanzamt die Arbeitszeit automatisiert erfaßt. Dieses automatisierte Verfahren war bei seinem erstmaligen Einsatz nicht freigegeben (Art. 26 Abs. 2 BayDSG) und auch nicht zum Datenschutzregister gemeldet worden (Art. 7 BayDSG).

   Ich habe das Finanzamt aufgefordert, die Freigabe nachzureichen und die Meldung zum Datenschutzregister abzugeben.

10.2 Kontopfändung zur Beitreibung von Vermessungsgebühren

Zur Beitreibung von Vermessungsgebühren hat die Vollstreckungsstelle eines Finanzamts das Bankkonto des Vollstreckungsschuldners gepfändet. Die Vollstreckungsstelle nutzte hierzu die Angabe der Bankverbindung in der Einkommensteuererklärung des Vollstreckungsschuldners.

Zur Zweckbindung der für Steuerzwecke erhobenen Daten und zum Umfang der Befugnisse des Finanzamts bei Vollstreckung der Forderung einer anderen Behörde habe ich das Finanzministerium um Stellungnahme gebeten.

Das Finanzministerium teilte meine aus dem Steuergeheimnis (§ 30 AO) herrührenden Bedenken gegen die Verwendung der zu steuerlichen Zwecken erhobenen Daten für die Vollstreckung nichtsteuerlicher Geldforderungen. Um diese Vollstreckungen auf eine eindeutige Rechtsgrundlage zu stellen, hat das Finanzministerium dem Bundesfinanzminister eine Änderung des § 249 AO vorgeschlagen. Die Novellierung dieser Vorschrift ist nun im AO-Änderungsgesetzentwurf 1992 vorgesehen.

10.3 Mitteilung von Dozentenvergütungen

Ein Finanzamt forderte von einer Volkshochschule generell die Übermittlung von Angaben über Dozentenvergütungen. Es bezog sich dabei auf eine frühere von Finanzministerium und Landesbeauftragtem für den Datenschutz gemeinsam vertretene Auffassung,

nach der diese Datenübermittlung – abgesehen von der Höhe des Betrags – zulässig sei (§§ 93, 93 a AO).

Diese Beurteilung kam 1987 im Hinblick auf den Übergangsbonus und die damals unmittelbar zu erwartende Kontrollmitteilungsverordnung zustande. Sie ist seit Mitte 1990 gegenstandslos, weil der Erlaß der Kontrollmitteilungsverordnung immer noch aussteht. Das Finanzministerium hat verfügt, daß „allgemeine Kontrollmitteilungen an die Finanzämter gegenstandslos geworden" sind, weil dazu die Rechtsgrundlage fehlt. Eine Einzelauskunft nach § 93 AO ist davon nicht betroffen.

Das Finanzamt verlangte die Auskunft in der Form der allgemeinen Kontrollmitteilung, für die es nach wie vor an einer Rechtsgrundlage fehlt. Die Weigerung der Volkshochschule, die geforderten Dozentendaten zu übermitteln, war somit rechtens.

10.4 Zeichnungsvorbehalt des Finanzamtsvorstehers

Mehrere Eingaben von Mitarbeitern der Steuerbehörden befaßten sich mit dem Zeichnungsvorbehalt des Finanzamtsvorstehers in Steuerangelegenheiten von Amtsangehörigen. Dem Finanzamtsvorsteher ist es vorbehalten, Steuerveranlagungen der Amtsangehörigen abschließend zu unterzeichnen. Hierdurch soll die Korrektheit der Steuerveranlagung von Amtsangehörigen zusätzlich gewährleistet werden. Auf diesem Weg erhält er Einsicht in die persönlichen und finanziellen Verhältnisse der Bediensteten und ihrer Angehörigen. Die Petenten waren in Sorge, daß die Kenntnisse aus den Steuerakten Personalentscheidungen bewußt oder unbewußt beeinflussen könnten.

Auf meine Vorstellungen hin beabsichtigt das Finanzministerium nunmehr, die Finanzamtsvorsteher vom Zeichnungsvorbehalt in Steuerangelegenheiten von Amtsangehörigen zu entbinden. In diesen Fällen soll der Zeichnungsvorbehalt künftig dem für die Veranlagung fachlich zuständigen Sachgebietsleiter übertragen werden. Die Steuerangelegenheiten von Amtsangehörigen des eigenen Sachgebiets soll der Vertreter dieses Sachgebietsleiters unterschreiben. Die Möglichkeit, im Wege einer Zuständigkeitsvereinbarung nach § 27 AO die Bearbeitung durch ein anderes Finanzamt vorzusehen, bleibt weiterhin bestehen.

Mit der beabsichtigten Regelung bin ich einverstanden. Ich habe das Finanzministerium jedoch gebeten, im Vertretungsfall den Vertreter des fachlich zuständigen Sachgebietsleiters nicht in Personalangelegenheiten des vertretenen Sachgebiets tätig werden zu lassen. Den Antrag auf Vereinbarung einer anderen Zuständigkeit nach § 27 AO sollte der Mitarbeiter nach meiner Auffassung nicht begründen müssen. Eine Begründung hält ihn möglicherweise von einer Antragstellung ab.

11. Personalwesen

11.1 Datenschutz bei der behördeninternen Telekommunikation

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat zur Telekommunikation eine Stellungnahme beschlossen, die auch die behördeninterne Telekommunikation betrifft. Einzelheiten, u. a. auch zur Frage der Telefongesprächsdatenerfassung, die im 13. Tätigkeitsbericht unter Nr. 12.3 behandelt wurde, sind unter Nr. 19.4 sowie im Anhang I dieses Tätigkeitsberichts wiedergegeben.

11.2 Personaldaten im städtischen Telefonbuch

Eine Stadt ließ ein städtisches Telefonbuch drucken, in dem sämtliche städtische Bedienstete mit Familienname, Dienststelle, Funktion und Aufgabe, Dienstanschrift, Zimmernummer und Telefondurchwahl aufgeführt sind. Um die Herstellungskosten niedrig zu halten, war beabsichtigt, das Telefonbuch neben der dienstlichen Verwendung auch an jedermann zu verkaufen. Ein Teil der Unkosten sollte durch Anzeigengebühren abgedeckt werden.

Der Stadt kamen jedoch Bedenken, ob die Veröffentlichung ihres Telefonbuches mit Angaben zu **sämtlichen Bediensteten** mit dem Datenschutzrecht vereinbar sei.

Mit dem Innenministerium war ich mir einig, daß die gesetzlichen Voraussetzungen für eine Veröffentlichung des städtischen Telefonbuches nicht vorlagen (Art. 18 BayDSG). Eine der Voraussetzung lautet, daß ein allgemeines berechtigtes Interesse besteht, von allen im Telefonbuch aufgeführten städtischen Bediensteten, Name, Dienststelle, Funktion, Zimmernummer und Telefondurchwahl in Erfahrung bringen zu können.

Ein solches anerkennenswertes Interesse kann allenfalls bezüglich solcher Bediensteter bestehen, mit denen das Publikum erfahrungsgemäß telefonisch in Verbindung treten will. Dies trifft aber nur für Sachbearbeiter und in der Behördenhierarchie höher gestellte Bedienstete zu, nicht hingegen z.B. für den Schreibdienst und den übrigen „inneren" Dienst. Dies habe ich der Stadt mitgeteilt.

11.3 Gestaltung des Personalbogens

Ein Staatsministerium hat mir den Entwurf eines überarbeiteten Personalbogens für Beamtinnen/Beam-

te des Ministeriums zur datenschutzrechtlichen Stellungnahme übermittelt.

Ich habe darauf hingewiesen, daß für den Betroffenen die **Rechtsvorschrift** für die jeweilige Datenerhebung ersichtlich sein muß. Außerdem habe ich angeregt, die Frage nach geleistetem **Wehrdienst bzw. Ersatzdienst** zusammenzufassen, da aus nachgewiesenen Dienstzeiten keine unterschiedlichen beamtenrechtlichen Konsequenzen zu ziehen sind. Die zusätzliche Dokumentation, ob es sich um Wehr- oder Zivildienst handelt, ist nicht erforderlich.

Gegen die Frage nach einer **Schwerbehinderung** bei der Einstellung eines Bewerbers habe ich keinen Einwand erhoben. Eine Mitteilung an den Dienstherrn über eine später eingetretene Schwerbehinderung ist allerdings freiwillig. Hierauf sind die Bediensteten durch die Personalabteilung hinzuweisen. Voraussetzung dafür ist allerdings, daß keine Vergünstigungen in Anspruch genommen werden und die Behinderung nicht von ausschlaggebender Bedeutung für die Beschäftigung ist.

Der Entwurf des Personalbogens enthält im Zusammenhang mit der Frage nach Kindern **Bemerkungsfelder.** Ich habe darauf hingewiesen, daß ich Vorgaben an den Personalsachbearbeiter, welche die möglichen Eintragungen in diesen Feldern einschränken, für wünschenswert halte. Bei „Freitextfeldern" besteht sonst die Gefahr, daß zur Aufgabenerfüllung nicht erforderliche oder gar problematische Eintragungen vorgenommen werden.

Mit dem Personalbogen wird auch die **Religionszugehörigkeit** des Bediensteten erhoben. Rückfragen bei anderen Ministerien haben ergeben, daß auf die Angabe dieses Datums teilweise verzichtet wird. Dies legt den Schluß nahe, daß dieses Datum zur Personalverwaltung nicht benötigt wird und die Frage nach der Religion deshalb unzulässig ist.

11.4 Erhebung von Krankheitsdaten in der Probezeitbeurteilung von Lehrkräften

Ein Lehrer bat mich um Überprüfung eines von der Schule verwendeten Formblattes, in das die Lehrkräfte auf Probezeit die Erkrankungen und Beurlaubungen während der Probezeit einzutragen hatten. Die Daten werden für die Probezeit-Beurteilung benötigt. Bedenken ergäben sich insbesondere daraus, daß nach dem Formular die **Art der Krankheiten** seit der Berufung in das Beamtenverhältnis auf Probe anzugeben sei.

Mit dem Staatsministerium der Finanzen habe ich die Auffassung vertreten, daß in diesem Zusammenhang **keine Rechtsgrundlage** für die generelle Erhebung der **Art** der Erkrankung besteht. Vielmehr sind nach den Richtlinien für die dienstliche Beurteilung der Lehrer Erkrankungen des Lehrers in der Beurteilung nur dann anzuführen, wenn sie zu häufigen Abwesenheiten führten oder das körperliche Leistungsvermögen mehr als nur kurzzeitig beschränkt war. Dem kann jedoch auch durch eine Erhebung, beschränkt auf die Tatsache solcher Erkrankungen, Rechnung getragen werden.

Es muß daher ausreichen, im betreffenden Formblatt nur die **Tatsache** und die **Dauer** der Erkrankung anzugeben. Wenn diese Angaben auf häufige Abwesenheiten oder eine längere Erkrankung schließen lassen, und infolgedessen Zweifel an der Dienstfähigkeit bestehen, kann die Dienststelle eine amtsärztliche Untersuchung veranlassen.

Das Staatsministerium für Unterricht, Kultus, Wissenschaft und Kunst hat meinen Bedenken durch Änderung des Formblattes Rechnung getragen. Es ist nunmehr klargestellt, daß die Lehrer auf Probezeit nicht verpflichtet sind, gegenüber der Schule Angaben zur Art der Erkrankung zu machen. Wenn allerdings Zweifel an der gesundheitlichen Eignung bestehen, muß eine amtsärztliche Untersuchung angeordnet werden.

11.5 DV-Einsatz beim Personalrat

Auf Anfragen von Personalräten war zu klären, in welchem Umfang der Personalrat Daten über Behördenangehörige automatisiert speichern darf. Nach Einholung einer Stellungnahme des Staatsministeriums der Finanzen vertrete ich die Auffassung, daß ein Personalrat die folgenden **Grunddaten** der Beschäftigten ohne datenschutz- bzw. personalvertretungsrechtliche Bedenken selbst speichern darf: Name und Vorname, Sachgebiet, Besoldungs- und Vergütungsgruppe des Bediensteten.

Hierfür sind folgende Gründe maßgebend: Aus Art. 69 des Bayerischen Personalvertretungsgesetzes folgt, daß dem Personalrat kein uneingeschränktes Informationsrecht zusteht. Sein Informationsrecht beschränkt sich auf die zur Behandlung des konkreten Falles erforderlichen Informationen. Auch ein **Einsichtsrecht in Personalakten** besteht nur für bestimmte Mitglieder des Personalrats und nur dann, wenn der betreffende Beschäftigte seine Zustimmung dazu erklärt hat. Daraus ist abzuleiten, daß dem Personalrat ein dateimäßiges Vorhalten von Daten untersagt ist, wenn ihm Unterlagen **nur zur Beurteilung des Einzelfalles** überlassen werden oder, wenn sie **lediglich zur Einsichtnahme** zur Verfügung stehen. Grundsätzlich für unzulässig hielte ich demnach, wenn über den oben genannten Rahmen hinaus aus einzelnen Beteiligungsfällen personenbezogene Daten von Beschäftigten **auf Vorrat automatisiert gespeichert** würden, um ggf. später darauf zurückgreifen zu können. Ins-

besondere darf der Personalrat nicht auf diese Weise eine zweite (automatisierte) Personalakte aufbauen.

Für die Speicherung von Daten im Rahmen der Erfüllung der öffentlich-rechtlichen Aufgaben der Personalvertretung, die durch das BayPVG zugewiesen sind, ist der Personalrat datenschutzrechtlich verantwortlich. Verstöße gegen den Datenschutz, die in diesen Verantwortungsbereich fallen, hat der Personalrat zu beheben. Er unterliegt der Kontrolle des Landesbeauftragten für den Datenschutz.

11.6 Übergabe von Stellenbesetzungslisten an die Personalvertretung

Jede Personalverwaltung führt eigene Stellenbesetzungslisten in denen festgehalten ist, welche Bediensteten welche Planstellen des Haushaltsplanes besetzen. Personalvertretungen wünschen gelegentlich Einblick in diese Listen um zu erfahren, wie die Personalverwaltung die vorhandenen Planstellen nutzt.

Nach der von mir geteilten Auffassung der für das Personalrecht federführenden Staatsministerien der Finanzen (staatlicher Bereich) und des Innern (Kommunalbereich) richtet sich die Übergabe von Stellenbesetzungslisten nach Art. 69 Abs. 2 des Bayerischen Personalvertretungsgesetzes. Danach hat der Personalrat nicht das Recht, Informationen für eine allgemeine Kontrolle der Tätigkeit der Dienststelle zu verlangen. Die Stellenbesetzungslisten dienen der Überwachung des ordnungsgemäßen Vollzugs der haushaltsrechtlichen Bestimmungen. Diese Überwachung gehört nicht zu den Aufgaben des Personalrats.

Die Rechtslage wäre anders zu beurteilen, wenn Aufzeichnungen über die Stellenbesetzung im Einzelfall für eine konkrete im Personalvertretungsgesetz normierte Aufgabe des Personalrats erforderlich wären. Eine Übermittlung von Stellenbesetzungslisten „auf Vorrat", für den Fall, daß die Daten künftig einmal erforderlich würden, gestattet das Personalvertretungsrecht jedoch nicht.

12. Gewerbe und Handwerk

12.1 Rechtliche Entwicklung im Gewerberecht

Neun Jahre nach dem Volkszählungsurteil des Bundesverfassungsgerichts vom 15.12.1983 sind bereichsspezifische Datenschutzregelungen in der Gewerbeordnung (GewO) überfällig. Zur Zeit liegt ein Referentenentwurf vor, der u.a. die Ergänzung des § 14 GewO um Übermittlungs- und Auskunftsbestimmungen vorsieht. Danach soll die Übermittlung von Name, betrieblicher Anschrift und angezeigter Tätigkeit aus der Gewerbeanzeige an nichtöffentliche Stellen und an öffentlich-rechtliche Unternehmen, die am Wettbewerb teilnehmen, nur dann zulässig sein, wenn der Auskunftsbegehrende ein berechtigtes Interesse an der Kenntnis der zu übermittelnden Daten glaubhaft macht. Die Übermittlung weiterer Daten aus der Gewerbeanzeige soll zulässig sein, wenn der Auskunftsbegehrende ein rechtliches Interesse, insbesondere zur Geltendmachung von Rechtsansprüchen an der Kenntnis der zu übermittelnden Daten glaubhaft macht und kein Grund zu der Annahme besteht, daß das schutzwürdige Interesse des Gewerbetreibenden überwiegt.

Nach meinem Dafürhalten geht es doch etwas zu weit, wenn man, um eine ganz einfache Gewerbeauskunft zu erhalten, ein berechtigtes Interesse glaubhaft machen muß. Dadurch wird die Beschaffung einfachster Informationen zu sehr erschwert. Ich halte es für vertretbar und angemessen, wenn eine einfache Gewerbeauskunft, ähnlich wie im Melderecht, vom Gewerbeamt ohne Bedingungen zu erhalten ist.

Für **erweiterte** Gewerbeauskünfte müßte es genügen, wenn der Auskunftssuchende anstelle eines **rechtlichen** nur ein **berechtigtes** Interesse glaubhaft macht, wobei unter **berechtigtem** Interesse jedes von der Rechtsordnung geschützte, insbesondere auch ein wirtschaftliches Interesse, zu verstehen ist. Auch die Verpflichtung, den Gewerbetreibenden über eine erteilte **erweiterte** Auskunft zu benachrichtigen, sollte erwogen werden.

12.2 Regelmäßige Weitergabe der Daten von Gewerbetreibenden an den Jugendschutzbeauftragten einer Stadt

Eine Stadt beabsichtigte, von nachfolgenden Gewerbezweigen Namen und Anschrift der Hauptniederlassung, Datum der Betriebsbeendigung, Filial-Hinweis und Betriebsart aus der Gewerbedatei an den städtischen Jugendschutzbeauftragten zu übermitteln: Discotheken, Gaststätten, Videotheken, Spielotheken, Sex-Shops, Nachtclubs, Einzelhandel mit Alkohol, Tabak und Zeitschriften, Buch- und Zeitschriftenhandel, Tankstellen mit Videoverkauf oder -verleih und/oder Buch- und Zeitschriftenhandel, Alkohol- und Tabakverkauf.

Als Begründung wurde angegeben, der Jugendschutzbeauftragte benötige diese Angaben, um diese Gewerbezweige auf Gefahren für die Jugend hinweisen zu können. Es sei beabsichtigt, dem Jugendschutzbeauftragten einen einmaligen EDV-Listenausdruck mit den bereits bestehenden Gewerbebetrieben zu überlassen und diesen durch eine monatliche Auflistung über die genannten Daten fortzuschreiben.

Die Zulässigkeit der Datenübermittlung aus der Gewerbedatei beurteilt sich wegen der noch fehlenden

spezialgesetzlichen Regelung in der Gewerbeordnung nach Art. 17 Abs. 1 BayDSG. Demnach ist die Übermittlung der Daten aus der Gewerbedatei zulässig, da sie zur rechtmäßigen Erfüllung der dem Jugendschutzbeauftragten zugewiesenen Aufgaben erforderlich ist (§ 1 Abs. 3 Nr. 3 KJHG i.V.m. Art. 8 a Abs. 1 AGKJHG). Gegen die beabsichtigte Datenübermittlung bestehen, sofern sie sich auf die genannten Gewerbezweige und die genannten Datenarten beschränkt, keine Bedenken.

13. Statistik

13.1 Fernmündliche Datenerhebung bei der Durchführung von Statistiken

Das Statistische Amt einer bayerischen Großstadt erkundigte sich nach der Zulässigkeit von telefonischen Befragungen bei der Durchführung von statistischen Erhebungen.

Ich habe darauf hingewiesen, daß bei diesem Verfahren **Mißbräuche** nicht ausgeschlossen werden können. Nach Bekanntwerden dieser Erhebungsmethode in der Öffentlichkeit könnten sich Unbefugte dieser Methode bedienen und damit Informationen von schlecht unterrichteten Bürgern erschleichen. Ich habe deshalb empfohlen, die Interviews grundsätzlich nicht auf Anruf, sondern auf Rückruf bei der erhebenden Stelle zu führen.

Außerdem ist der Bürger im Vorfeld der Befragung **schriftlich** ausdrücklich darauf **hinzuweisen**, daß er sich auf die Erhebungsmethode nicht einzulassen braucht. Die daneben bestehenden Möglichkeiten der mündlichen (persönlich gegenüber dem Interviewer) oder schriftlichen Beantwortung der Fragen (gegenüber dem Statistischen Amt) müssen dabei deutlich mitgeteilt werden. Außerdem sollte in die Benachrichtigung der Namen des Interviewers aufgenommen werden.

13.2 Einsatz von Laptops bei statistischen Befragungen

Im Frühjahr 1991 wurde erstmals eine Befragung unter Verwendung von Laptops als Probeerhebung nach dem Bundesstatistikgesetz bei rund 450 Haushalten in München und den Umlandgemeinden auf freiwilliger Basis durchgeführt. Das Bayer. Landesamt für Statistik und Datenverarbeitung hatte sich an einer vom Statistischen Bundesamt im Auftrag des Statistischen Amtes der Europäischen Gemeinschaft durchgeführten Studie zum Einsatz von Laptops bei Haushaltsbefragungen beteiligt.

Dabei wurden die zur Teilnahme bereiten Bürgerinnen und Bürger durch einen Interviewer zu bestimmten Themenkomplexen um Auskunft gebeten. Die Befragung erfolgte anhand eines vorgegebenen Fragenkataloges. Die Antworten wurden jedoch nicht auf dem Fragebogen vermerkt und anschließend im Landesamt auf Datenträger erfaßt, sondern vom Interviewer direkt in einen tragbaren Computer (Laptop) eingegeben. Am Folgetag wurden die Daten direkt an den Großrechner übergeben.

Gegen den Einsatz von Laptops als **zusätzliches** Erhebungsinstrument bei Befragungen bestehen grundsätzlich keine Bedenken. Im Hinblick auf das informationelle Selbstbestimmungsrecht des auskunftspflichtigen Bürgers muß dabei allerdings auch für die Zukunft das Wahlrecht des Befragten, die Angaben entweder mündlich gegenüber dem Interviewer oder schriftlich bzw. auf postalischem Weg zu machen, sichergestellt bleiben und für den Bürger deutlich erkennbar gemacht werden.

Die bei den bisherigen Erhebungen praktizierte getrennte Erfassung von Hilfs- und Erhebungsmerkmalen sollte auch bei Erhebung per Laptop beibehalten werden. Die Datensicherheit beim Laptopeinsatz muß durch erhöhte Sicherungsmaßnahmen gewährleistet werden. Insbesondere müssen gespeicherte Daten gegen unberechtigten Zugriff gesichert sein (Verschlüsselung, Paßwort). Ich verweise in diesem Zusammenhang auf meine Ausführungen im 13. Tätigkeitsbericht auf Seite 79 unter der Nummer 22.2.2.

14. Schulwesen

14.1 Prüfung von Staatlichen Schulämtern

Bei Volksschulen obliegt die unmittelbare staatliche Schulaufsicht den Staatlichen Schulämtern, die organisatorisch den Kreisverwaltungsbehörden angegliedert sind. Im Berichtszeitraum habe ich zwei Staatliche Schulämter auf die Einhaltung datenschutzrechtlicher Bestimmungen hin überprüft. Dabei konnte ich feststellen, daß dem Umgang mit personenbezogenen Daten, meist solchen von Lehrern, insgesamt Rechnung getragen wurde. Nachfolgende Mängel bat ich zu beheben:

- **Karteikarten** mit zum Teil sensiblen Lehrerdaten, wie Noten der Lehramtsprüfung und Prädikat der Beurteilung, lagen trotz Abwesenheit des Sachbearbeiters **unverschlossen** auf dem Schreibtisch.

- In der sog. **Stammkartei**, die über die Lehrer im Schulamtsbezirk angelegt wird, fanden sich folgende Daten, die für die Aufgabenerfüllung nicht erforderlich sind: Datum der Eheschließung, Name und Geburtstag des Ehemannes und – soweit nicht für die Prüfung von Teilzeit- und Urlaubsanträgen nach Art. 86 a BayBG erforderlich – Name und

Geburtsdaten der Kinder. In diese Stammdatei, die einen schnellen Zugriff des Schulamts auf die für die Aufgabenstellung notwendigen Lehrerdaten ermöglichen soll, dürfen nur Stammdaten aufgenommen werden. In die Stammdatei dürfen nicht alle Daten aufgenommen werden, die dem Schulamt bekannt werden. Im Hinblick darauf, daß nach der bevorstehenden Einführung des automatisierten Schulverwaltungsprogrammes SVS die manuellen Karteien nach Ablauf einer Übergangsfrist überflüssig werden, habe ich von der Forderung abgesehen, daß die nicht mehr benötigten Daten geschwärzt werden. Sollte sich jedoch herausstellen, daß eine Weiterführung der Karteikarten für einen längeren Zeitraum trotz der Einführung des automatisierten Programms unumgänglich ist, müßten die nicht benötigten Daten gelöscht werden.

- **Handakten mit Personalunterlagen** wurden zum Teil in übereinandergestellten Metallcontainern, die nur mit leicht aufbrechbaren Schlössern versehen waren, in einer Nische des Ganges aufbewahrt. Außerdem war an ihnen eine Beschriftung nach den jeweiligen Anfangsbuchstaben der Lehrer angebracht, die einen gezielten Zugriff ermöglichten. Wegen der Sensibilität der in Personalakten enthaltenen Unterlagen habe ich die Aufbewahrung in geeigneten verschließbaren Schränken gefordert, die einen Zugriff Unberechtigter weitgehend ausschließen.

- Scheidet ein Lehrer aus dem Schuldienst aus oder wird er versetzt, so bewahrt das Schulamt die für ihn angelegte Karteikarte in sog. **Ausgeschiedenen-Karteien** zeitlich unbegrenzt auf. Das sei nach Angaben der Schulamtsleiter unabdingbar, weil von Angehörigen und anderen staatlichen Stellen immer wieder Rückfragen zu einzelnen Daten gestellt würden, die mangels Akten nicht mehr beantwortet werden könnten. Damit erfolgt zumindest bei mehreren Versetzungen eine Doppelspeicherung von Daten desselben Lehrers an verschiedenen Stellen. Ich habe das Kultusministerium um Mitteilung gebeten, ob und inwieweit hier Abhilfe geschaffen werden kann.

14.2 Weitergabe der Daten von Berufsschulschwänzern an eine Beratungsstelle

Immer häufiger kommt es vor, daß in der Ausbildung befindliche Jugendliche oder bereits volljährige Berufsschulpflichtige ihrer Pflicht zum Besuch beruflicher Schulen nicht nachkommen. Solchen „Schulschwänzern" droht für ihr unentschuldigtes Fernbleiben vom Unterricht oder den anderen als verbindlich erklärten schulischen Veranstaltungen eine Geldbuße, eine Arbeitsauflage und schließlich Erzwingungshaft oder Jugendarrest. Die Verfahren werden nach dem Ordnungswidrigkeitengesetz abgewickelt, mit jährlich steigender Tendenz.

Um diese Entwicklung zu stoppen, schuf eine Stadt vor kurzem eine Anlaufstelle für Schulverweigerer, in der dem Schuleschwänzen mit pädagogischen Mitteln begegnet werden soll. In Beratungsgesprächen wollen Sozialpädagogen und Psychologen Hilfestellung bei Bußgeld- und sonstigen Problemen leisten. Um die Betroffenen auf diese Beratungsmöglichkeit hinweisen zu können, war geplant, ihre Personalien aus dem automatisierten Verfahren „Berufsschulpflicht" des Schulreferates per Abdruck des Bußgeldbescheides an die Beratungsstelle, die bei einem Erwachsenenbildungsträger angesiedelt ist, zu übermitteln.

In Übereinstimmung mit dem Staatsministerium für Unterricht, Kultus, Wissenschaft und Kunst habe ich die Datenübermittlung aus folgenden Gründen für datenschutzrechtlich unzulässig gehalten:

Nach Art. 62 Abs. 2 Bayerisches Erziehungs- und Unterrichtsgesetz ist die Weitergabe personenbezogener Schülerdaten an außerschulische Stellen wie die Beratungsstelle untersagt, soweit nicht ein rechtlicher Anspruch auf die Herausgabe der Daten nachgewiesen wird. An einem solchen rechtlichen Anspruch fehlt es nach der derzeit geltenden Rechtslage.

Die Weitergabe der Daten kann auch nicht mit der „Erfüllung der den Schulen durch Rechtsvorschriften jeweils zugewiesenen Aufgaben" begründet werden (Art. 62 Abs. 1 Satz 1 BayEUG). Die Maßnahmen zur Durchsetzung der Schulpflicht, die sowohl Schulleiter als auch Lehrer zu überwachen haben, sind nämlich im Schulpflichtgesetz abschließend aufgezählt. Eine außerschulische Schülerberatung ist darin nicht enthalten. Sie bedürfte als weitere (flankierende) Maßnahme zur Durchsetzung der Schulpflicht einer entsprechenden Rechtsgrundlage.

Es besteht allerdings die Möglichkeit, daß die „Schulschwänzer"-Daten an die Beratungsstelle **mit Einwilligung** der Erziehungsberechtigten bzw. der volljährigen Schüler weitergeleitet werden.

14.3 Speicherung der Daten von Eltern volljähriger Schüler in der Schülerdatei

Da der Datensatz der bayerischen Schülerdatei die Speicherung von Name, Vorname, Ort und Anschrift der/des Erziehungsberechtigten (bzw. des volljährigen Schülers) vorsieht, wurde ich um Auskunft gebeten, wann die Daten der Eltern von volljährig gewordenen Schülern zu löschen sind bzw. wie lange und zu welchem Zweck sie noch vorgehalten werden dürfen

Das Staatsministerium für Unterricht, Kultus, Wissenschaft und Kunst hat zu dieser Frage wie folgt Stellung genommen:

Mit Eintritt der Volljährigkeit der Schüler endet zwar das Erziehungsrecht der Eltern oder sonstiger Sorgeberechtigter. Keineswegs enden damit jedoch die Rechtsbeziehungen zwischen dem Schüler und seinen bisherigen Erziehungsberechtigten. Letztere sind beispielsweise in der Regel weiterhin unterhaltspflichtig. Bei einem Schulunfall werden – sofern der Schüler nicht ausdrücklich anderes wünscht – zunächst sie zu verständigen sein. Die Mitgliedschaft im Elternbeirat endet erst mit dem Ablauf der Amtszeit des Elternbeirats. Aus diesen Beispielen ergibt sich, daß das Speichern und ggf. Verändern der personenbezogenen Daten ehemaliger Erziehungsberechtigter auch nach der Volljährigkeit ihrer Kinder noch zur rechtmäßigen Erfüllung der schulischen Aufgaben erforderlich und zumindest bis zur Beendigung des Schulbesuchs des Schülers zulässig ist.

Diese Rechtsauffassung des Ministeriums erscheint plausibel. Wie alle Daten, die in der bayerischen Schülerdatei gespeichert werden, müssen auch die Daten ehemaliger Erziehungsberechtigter spätestens ein Jahr nach Ablauf des Schuljahres, in dem der Schüler die Schule verlassen hat, gelöscht werden.

14.4 Herausgabe von Schuljahresberichten an eine Krankenversicherung

Immer wieder versuchen Krankenversicherungen auf unterschiedlichste Weise an Name und Adresse möglicher Neukunden heranzukommen. So legte eine Krankenkasse der Meldebehörde eine Liste mit Namen und Geburtsdaten von Schulabgängern mit der Bitte um Ergänzung der Wohnadressen vor. Die Krankenkasse hatte die Schuljahresberichte von den Schulen gekauft. Die Meldebehörde lehnte den Antrag auf Sammelauskunft jedoch ab, da ein Mißbrauch des Auskunftsverfahrens vorliegt, wenn Namenslisten ohne weitere Adressenangabe von der Meldebehörde durch die Anschrift ergänzt werden sollen.

Mit Blick auf Art. 62 Abs. 2 und 3 Bayer. Gesetz über das Erziehungs- und Unterrichtswesen (BayEUG) habe ich das Kultusministerium um Stellungnahme zur Zulässigkeit der Weitergabe von Schuljahresberichten an Dritte gebeten.

Das Ministerium wies darauf hin, daß die Weitergabe von Jahresberichten an Dritte zwar vom BayEUG nicht vorgesehen sei. Vielmehr sei darin die Rede, daß der Jahresbericht für die Schüler und Erziehungsberechtigten „herausgegeben wird". Andererseits lasse sich aus dieser Formulierung aber auch ein Verkaufs- oder Weitergabeverbot an Dritte nicht herauslesen. Da der Jahresbericht eines der wenigen Instrumente für die Selbstdarstellung einer Schule sei und andererseits durch ein Verbot der Weitergabe nicht ausgeschlossen werden könne, daß sich Dritte Jahresberichte doch auf Umwegen beschaffen, hält das Ministerium ein generelles Weitergabeverbot an Dritte auch für wenig wirksam. Zudem enthalte der Jahresbericht selbst nicht die Adresse eines Schülers. Eine Versicherung, die den Jahresbericht erwirbt, kann die Adressen der Schüler jedoch dann z.B. unter Umständen aus dem Telefonbuch ergänzen.

Um zumindest den Mißbrauch von Schuljahresberichten zur Mitgliederwerbung durch Krankenkassen einzudämmen, sollten die Schulen künftig Bitten um Übersendung von Jahresberichten ablehnen, wenn erkennbar ist, daß diese auf die Gewinnung von schülerbezogenen Daten abzielen.

14.5 Anforderung von Zeugnissen durch die Sozialhilfeverwaltung nach Übernahme von Heimkosten im Rahmen der Eingliederungshilfe

Eine private Schule für Behinderte wies mich auf die unterschiedliche Sachbearbeitung der überörtlichen Sozialhilfeträger bei Gewährung von Eingliederungshilfe hin. So fordere ein Bezirk zur Prüfung der Übernahme von Heim- und Schulbesuchskosten Erziehungsberichte **und** Zeugnisse an, ein anderer Bezirk beschränke sich auf die Anforderung nur von Erziehungsberichten.

Nach § 39 Abs. 4 des Bundessozialhilfegesetzes (BSHG) wird Personen, die nicht nur vorübergehend körperlich, geistig oder seelisch wesentlich behindert sind, Eingliederungshilfe gewährt, wenn und solange nach der Besonderheit des Einzelfalles, vor allem nach Art und Schwere der Behinderung, Aussicht besteht, daß die Aufgabe der Eingliederungshilfe erfüllt werden kann. Diese besteht darin, dem Behinderten die Teilnahme am Leben in der Gemeinschaft und die Ausübung eines angemessenen Berufs zu ermöglichen und ihn soweit wie möglich unabhängig von Pflege zu machen.

Zur Vorbereitung dieser Prognoseentscheidung ist eine Herausgabe von geeigneten Unterlagen über den Schüler und seine Erziehungsberechtigten nach Art. 62 Abs. 2 BayEUG grundsätzlich zulässig. Jedoch bestanden über die Frage, in welchem Umfang Einzelangaben zur Prüfung des § 39 Abs. 4 BSHG erforderlich sind, zunächst unterschiedliche Auffassungen. Das Staatsministerium für Arbeit, Familie und Sozialordnung hielt die Anforderung von Erziehungsberichten **und** Zeugnissen zur Prüfung der Kostenübernahme für erforderlich. Nur dann könne nach § 12 Eingliederungshilfe-Verordnung beurteilt werden, ob die Maßnahme erforderlich und geeignet sei.

Demgegenüber verwies einer der überörtlichen Sozialhilfeträger darauf, daß die Schulzeugnisse wegen ihrer geringen Aussagekraft über die Entwicklung von körperlich, seelisch oder geistig wesentlich Behinderten nur in Ausnahmefällen zur Beurteilung der Erfolgsaussichten der Eingliederungshilfe hilfreich seien. Ein solcher Ausnahmefall liege beispielsweise vor bei der Entscheidung über die Kostenübernahme zum Besuch weiterführender Schulen, wenn Zweifel daran bestünden, ob das Klassenziel erreicht werde. Im Regelfall sei jedoch der Erziehungs- bzw. Entwicklungsbericht, der sich mit der Wirksamkeit der gewährten Eingliederungshilfe befasse, ausreichend. Diese Berichte werden jährlich individuell erstellt und enthalten, ausgehend von Art und Schwere der Behinderung, eine Beschreibung der Erfolge und Mißerfolge der jeweils durchgeführten Maßnahmen sowie Empfehlungen für weitere Maßnahmen.

Aufgrund der Ausführungen dieses Bezirkes habe ich dem Ministerium mitgeteilt, daß ich zwar die Anforderungen von Zeugnissen im Einzelfall, nicht jedoch generell für zulässig halte. Das Ministerium hat sich mittlerweile meiner Auffassung angeschlossen.

15. Hochschule

15.1 Prüfung einer Universität

Bei der Kontrolle einer Universität waren nur wenige Mängel festzustellen:

- Der Vizekanzler, der zumindest im Vertretungsfall mit Personalangelegenheiten befaßt ist, nimmt zugleich die Aufgaben des Datenschutzbeauftragten wahr. Ich habe empfohlen, eine andere Person zum Datenschutzbeauftragten zu berufen, da die Datenschutzkontrolle grundsätzlich von der Personalverwaltung getrennt sein sollte. Außerdem wäre auch eine Interessenkollision mit den Bereichen Studenten- und Prüfungsamt, die in seiner Zuständigkeit liegen, nicht auszuschließen.

- Das Sachgebiet **Beihilfe** war zwar räumlich, nicht jedoch organisatorisch von der Personalabteilung getrennt, sondern in die Abteilung „Personal" eingegliedert. Um die Verwendung von Kenntnissen aus dem Beihilfevollzug bei der Personalsachbearbeitung auszuschließen, habe ich gefordert, die Bearbeitung der Beihilfeangelegenheiten einer anderen Abteilung zu unterstellen.

- In der Studentenverwaltung wurde neben einer Archivdatei exmatrikulierter Studenten eine **manuelle Studentenkartei früherer Studienjahrgänge** vorgefunden, die teilweise dieselben Daten enthielt. Da eine Doppelspeicherung unzulässig ist, soll nun ein Gesamtkonzept für Archivdaten entworfen werden, in das auch die bisherigen Archivdaten einbezogen werden.

- Im Hochparterre des provisorischen Verwaltungsgebäudes wurden Briefe und Päckchen der Universität am geöffneten Fenster der Poststelle zur Abholung durch das Postauto bereitgelegt. Unbefugten wäre es ohne Schwierigkeiten möglich gewesen, beim Vorbeigehen einzelne Briefe zu entwenden, zumal sie nicht immer im Blickfeld des Postsachbearbeiters lagen.

16. Archiv und Forschung

16.1 Veröffentlichung von Zuschüssen aus Mitteln des Entschädigungsfonds nach dem Denkmalschutzgesetz

Bereits in meinem letzten Tätigkeitsbericht bin ich ausführlich auf die Problematik eingegangen, die sich für Eigentümer denkmalgeschützter Objekte dadurch ergeben kann, daß die genaue Höhe der aus dem vom Staatsministerium für Unterricht, Kultus, Wissenschaft und Kunst verwalteten Entschädigungsfonds nach dem Denkmalschutzgesetz bewilligten Zuwendungen in Verbindung mit der Bezeichnung des geförderten Objekts von der Bewilligungsbehörde, dem Ministerium, veröffentlicht wird. Dem Interesse der Öffentlichkeit an der Transparenz des Verwaltungshandelns bei der Vergabe von Zuschüssen steht das Recht auf Wahrung der Privatsphäre des Denkmaleigentümers gegenüber, das gestört werden kann, wenn Dritte aus der Höhe des gewährten Zuschusses Rückschlüsse auf die vermutete Vermögenslage des Zuschußempfängers ziehen.

Zwischenzeitlich hat das Staatsministerium für Unterricht, Kultus, Wissenschaft und Kunst eine Regelung gefunden, die auch den Datenschutz berücksichtigt.

In Zukunft wird in den Bewilligungsbescheid eine Klausel aufgenommen, daß innerhalb einer Frist von zwei Wochen nach Zugang des Bescheides schriftlich Einwendungen gegen die beabsichtigte Veröffentlichung geltend gemacht werden können. Werden solche Einwendungen erhoben, gehen die schutzwürdigen Belange des Zuwendungsempfängers den berechtigten Interessen der Öffentlichkeit an der Kenntnis der Daten vor. Eine Veröffentlichung von Objekt und Höhe des Zuschusses unterbleibt. Andernfalls erfolgt die Veröffentlichung wie bisher in einer Presseerklärung des Ministeriums.

16.2 Auskünfte über sonstige Zuschüsse nach dem Denkmalschutzgesetz durch das Landesamt für Denkmalpflege

Die genaue Höhe der Zuschüsse, die das Landesamt für Denkmalpflege aus den ihm zur Bewirtschaftung

zugewiesenen Haushaltsmitteln für einzelne Restaurierungsmaßnahmen bewilligt, ist häufig auch für Abgeordnete, Kommunalpolitiker und Journalisten ein begehrtes Nachfrageobjekt. Da durch solche Auskünfte schutzwürdige Interessen der Antragsteller beeinträchtigt werden können, besteht beim Bayerischen Landesamt für Denkmalpflege eine amtsinterne Regelung, wonach Dritten gegenüber Auskünfte über Förderdaten nur von der Amtsleitung oder dem Zuschußreferenten, nicht aber unmittelbar durch die Sachbearbeiter des Zuschußreferates oder die Mitarbeiter der Pressestelle erteilt werden dürfen. Diese amtsinterne Festlegung dient der Sicherstellung im Einzelfall, daß Daten nur nach rechtlicher Überprüfung, ob schutzwürdige Belange der Antragsteller betroffen sind, weitergegeben werden. Um die Erfordernisse des Datenschutzes zu wahren, werden bei Anfragen, welche die während eines bestimmten Zeitraums in ein bestimmtes Gebiet geflossenen staatlichen Leistungen betreffen, entsprechende Daten regelmäßig nur in aggregierter Form zur Verfügung gestellt. Rückschlüsse auf Einzelvorhaben oder im Einzelfall gewährte Förderungen sind dadurch nicht möglich.

Bei Anfragen, die Einzelobjekte betreffen, werden Auskünfte nur erteilt, wenn feststeht, daß die jeweilige Anfrage in Kenntnis und mit Einwilligung des Betroffenen erfolgt.

Die restriktive Handhabung dieser Auskunftspraxis ist zu begrüßen. Schutzwürdige Belange Betroffener werden dadurch angemessen berücksichtigt.

17. Umweltfragen

17.1 Umweltinformationsgesetz

Der Rat der Europäischen Gemeinschaften hat am 07.06.1990 eine Richtlinie über den freien Zugang zu Informationen über die Umwelt erlassen.

Die Richtlinie sieht einen Auskunftsanspruch des Bürgers über Umweltdaten vor. Nach Art. 3 gewährleisten die Mitgliedstaaten, daß die Behörden verpflichtet werden, allen natürlichen oder juristischen Personen auf Antrag **ohne Nachweis eines Interesses** Informationen über die Umwelt zur Verfügung zu stellen. Bisher gibt es in unserer Rechtsordnung kein durch allgemeines Gesetz gewährtes umfassendes subjektives öffentliches Recht auf Zugang zu Informationsbeständen der öffentlichen Verwaltung. Hingegen ist die Beteiligung der Öffentlichkeit in zahlreichen Zulassungs- und Planungsverfahren, beispielsweise in der Bauleitplanung oder im Immissionsschutzrecht, in beträchtlichem Umfang gewährleistet.

Die Richtlinie muß bis zum 31.12.1992 in jeweiliges nationales Recht umgesetzt werden. In der Bundesrepublik Deutschland soll dies durch das Umweltinformationsgesetz (UIG), das im Entwurf vorliegt, geschehen. Dabei werden dem Informationsanspruch des Bürgers die Belange des Datenschutzes in angemessener Weise gegenübergestellt. Da das Gesetz nicht rechtzeitig erlassen wurde, gilt die EG-Richtlinie ab 1.1.1993 unmittelbar.

Der Entwurf des UIG sieht vor, daß der Bürger grundsätzlich wählen kann, ob er Auskunft über Umweltinformationen oder die Bereitstellung von Informationsträgern verlangen will. Informationsträger können allerdings nicht schrankenlos zugänglich gemacht werden. Nach § 4 Abs. 1 Satz 3 des Entwurfs ist der Anspruch auf Auskunftserteilung beschränkt, wenn zum Schutz öffentlicher oder privater Belange eine unvertretbar aufwendige Aussonderung von Daten erforderlich wäre und die Auskunft auch ohne das zur Verfügungstellen des Informationsträgers verständlich wäre. Damit soll sichergestellt werden, daß die eigentliche Aufgabe der Behörde, nämlich effektiven Umweltschutz zu betreiben, nicht durch eine zeitaufwendige Datenaussonderung gefährdet wird. Auch spezialgesetzlich geregelte Informationsansprüche werden durch den Entwurf nicht verdrängt. Vielmehr können sie parallel zu den Ansprüchen aus dem UIG geltend gemacht werden. Schließlich regelt § 4 Abs. 3 des Entwurfs, daß die Behörde den Auskunftsantrag innerhalb von zwei Monaten zu verbescheiden hat.

Neben Tatbeständen, die den Anspruch auf Informationen über die Umwelt zum Schutz **öffentlicher** Belange beschränken oder ausschließen, regelt § 6 des Entwurfs auch den Ausschluß und die Beschränkung des Anspruchs zum Schutz **privater** Belange. Diese Vorschrift dient dem Schutz der informationellen Selbstbestimmung dadurch, daß nach Abs. 1 ein Auskunftsanspruch nicht besteht, soweit durch das Bekanntwerden der Informationen personenbezogene Daten offenbart und dadurch schutzwürdige Interessen der Betroffenen beeinträchtigt werden. Hierbei ist eine **Abwägung** im Einzelfall erforderlich. Zusätzlich nennt der Entwurf in § 6 Abs. 2 ausdrücklich „Betriebs- und Geschäftsgeheimnisse sowie geistiges Eigentum", welche „nicht unbefugt zugänglich gemacht werden dürfen". Der Anspruch ist nach Abs. 3 dieser Bestimmung allerdings nicht ausgeschlossen, wenn der Zugang zu Informationen über die Umwelt unvermeidbar mit der Offenbarung des Namens, des Berufes, der Branchen- oder Geschäftsbezeichnung des Verursachers einer Umweltbeeinträchtigung verbunden ist, es sei denn, daß schutzwürdige Interessen des Verursachers überwiegen.

17.2 Umweltinformationssystem UMSYS bzw. KUNIS

In meinem 10. Tätigkeitsbericht habe ich über das Umweltüberwachungssystem UMSYS berichtet, das 1988 als Pilotprojekt bei einem Landratsamt erprobt wurde. In enger Abstimmung mit dem Staatsministerium für Landesentwicklung und Umweltfragen wurde zwischenzeitlich ein landeseinheitliches Informationssystem für umweltrelevante Aufgabenstellungen bei den Vollzugs- und Überwachungsbehörden erarbeitet, das die Tätigkeit der Umweltbehörden erleichtern soll. Gegenüber dem ursprünglichen UMSYS-Projekt sind nun auch zahlreiche Datenübermittlungen zwischen Verwaltungs- und Fachbehörden vorgesehen. Ferner soll es auch der Information von politischen Entscheidungsträgern, Parlament und Öffentlichkeit dienen. Die Anstalt für Kommunale Datenverarbeitung bietet das Verfahren den Kreisverwaltungsbehörden unter dem Namen KUNIS (Kommunales Umwelt- und Naturschutzinformationssystem) an.

Der Beirat beim Landesbeauftragten für den Datenschutz nutzte die Möglichkeit, das Projekt bei einer kommunalen Umweltbehörde zu besichtigen. Im Mittelpunkt des Interesses stand dabei die Frage, ob und inwieweit dem Schutz von Betriebs- und Geschäftsgeheimnissen im Rahmen des automatisierten Verfahrens Rechnung getragen wird. So wurde der Verdacht geäußert, einzelne kommunale Mandatsträger oder auch die übergeordneten Behörden wie das Staatsministerium für Landesentwicklung und Umweltfragen könnten nun „auf Knopfdruck" abfragen, mit welchen Stoffen eine bestimmte Firma umgehe und so Rückschlüsse auf die genaue Zusammensetzung ihres Produkts ziehen. Diese Vermutungen bestätigten sich jedoch nicht. Vielmehr gaben weder die Art der gespeicherten Informationen noch die möglichen Abrufverfahren zu datenschutzrechtlichen Bedenken Anlaß.

Das Verfahren KUNIS dient in erster Linie als Hilfsmittel zur Beschleunigung und Verbesserung der Aufgabenerfüllung durch die Umweltbehörden, was nachfolgend für den Bereich „technischer Umweltschutz" dargestellt werden soll. Teilverfahren wie „Natur- und Landschaftsschutz" und „Abfallwirtschaft" sollen folgen.

Zahlreiche neue Rechtsvorschriften auf der einen, eine Vielzahl von überwachungspflichtigen Anlagen auf der anderen Seite belasten die Umweltverwaltungen quantitativ und qualitativ stark. KUNIS sieht zur Unterstützung dieser Tätigkeit verschiedene Dateien vor.

Die **Sachdatei** enthält als **Stammdaten** den Betreiber, die Anlage, den Standort sowie einen Raumbezug.

In der Vorgangsverwaltung finden sich Genehmigungs- und Überwachungsdaten sowie Angaben zum Einzelvorgang, die Wiedervorlage- oder Prüfungsfristen festlegen können.

An technischen Daten enthält das Verfahren die Dateien Luftreinhaltung (Stoffe, Stoffströme, Emissionsquellen usw.), Lärm (Emissionszeiten, Pegelwerte, Immissionsort usw.), Anlagensicherheit, Störfallverordnung und Lagerbehälter/Anlagen-Verordnung (Daten zum Baujahr, Fassungsvermögen, Bauart von Tanks).

Neben den Sachdaten existiert eine Datei „Wissens- und Gliederungsbasis", die neben allgemein verbindlichen umweltrelevanten Vorschriften (Gesetze, Verordnungen usw.) auch chemische Stoffinformationen und allgemeine Hintergrundinformationen zur Vorgangsbearbeitung enthält.

Betriebsgeheimnisse sind (derzeit) in dem automatisierten Verfahren noch nicht enthalten. Sie befinden sich weiterhin in den Genehmigungsakten. Nach § 27 Abs. 3 BImSchG muß der Antragsteller bereits bei der Einreichung seiner Planungsunterlagen Betriebsgeheimnisse als solche kennzeichnen und der Verwaltung eine brauchbare Version liefern, wie sie in verklausulierter Form in einen Genehmigungstext eingebaut werden dürfen. In Zweifelsfällen kann sich die Umweltverwaltung durch Rückfragen nochmal versichern, ob der Betrieb tatsächlich alle Betriebsgeheimnisse genannt und als solche gekennzeichnet hat.

KUNIS sieht zudem die Möglichkeit vor, Sperrvermerke anzubringen, so daß sensible Informationen nur autorisierten Benutzern zugänglich sind. So können die Zugriffskompetenzen individuell nach der Geschäftsverteilung und den fachlichen Erfordernissen vergeben werden. Der Zugriffsschutz selbst besteht zum einen im Login (Benutzerkennung und Passwort), zum anderen in einem zweistufigen lokalen Schutz, der die jeweiligen Zugriffe protokolliert und bestimmte Anlagen nur für bestimmte Sachbearbeiter einsehbar macht. Die Vermutung, „auf Knopfdruck" könne das Umweltministerium im Online-Verfahren genaue Produktzusammensetzungen des Betriebes A im Landkreis B erfahren, bestätigte sich somit nicht.

Auch wenn das Umweltministerium im Rahmen seiner Aufsichtspflicht beispielsweise für eine Landtagsanfrage bayernweit Daten (z.B. über die Anzahl chemischer Reinigungen) benötigt, müssen diese Daten erst durch den zuständigen Umweltschutzingenieur der speichernden Stelle freigegeben werden. Daneben sind auch die Regierungen im Rahmen ihrer bisherigen Zuständigkeiten als Genehmigungs- oder Aufsichtsbehörden in das automatisierte Verfahren einbezogen.

Inwieweit das neue **Umweltinformationsgesetz** eine Änderung der bisherigen Informationsmöglichkeiten der Bürger mit sich bringt, bleibt abzuwarten. Zumindest Betriebs- und Geschäftsgeheimnisse müssen aber auch dann gewahrt bleiben.

Da das Verfahren laufend weiterentwickelt und auf zusätzliche Bereiche der Umweltverwaltung ausgedehnt werden soll, werde ich dem Verfahren weiterhin meine Aufmerksamkeit widmen.

17.3 Adreßfeststellung bei Einsicht in immissionsschutzrechtliche Genehmigungsunterlagen

Daß es auch bei der Durchführung von detailliert geregelten Genehmigungsverfahren immer wieder zu Verfahrensfehlern kommen kann, zeigt folgender Fall:

Eine Petentin wollte Einsicht in öffentlich ausgelegte immissionsschutzrechtliche Genehmigungsunterlagen nehmen, die Angaben über die Auswirkungen einer Fabrikanlage auf die Nachbarschaft und die Allgemeinheit enthalten. Im Bauamt eines Landratsamtes, in dem die Unterlagen ausgelegt waren, forderte sie ein Mitarbeiter auf, eine Erklärung mit Angabe ihrer Adresse zu unterschreiben, wonach ihr Einsicht in die Unterlagen gewährt worden sei. Auf ihre Nachfrage erklärte der Mitarbeiter, ihre Unterschrift werde als Nachweis der Einsichtnahme zu den Verfahrensunterlagen genommen. Darüber hinaus – so die Petentin – wollte der Beamte ihre Adresse auch an den Betreiber weiterleiten, ein Vorwurf, der allerdings im Rahmen meiner Ermittlungen vom Landratsamt entschieden dementiert wurde.

Die 9. Verordnung zur Durchführung des Bundes-Immissionsschutzgesetzes, die Grundsätze des Genehmigungsverfahrens enthält, regelt in § 10 die Auslegung von Antrag und Unterlagen des beantragten Vorhabens bei der Genehmigungsbehörde oder an anderer geeigneter Stelle in der Nähe des Standorts. Nach § 10 Abs. 1 Satz 2 ist während der Dienststunden Einsicht in den Antrag und die Unterlagen zu gewähren. Weder die 9. BImSchV noch ähnliche Vorschriften über die Durchführung von förmlichen Verwaltungsverfahren bzw. Planfeststellungsverfahren enthalten eine Regelung dahingehend, daß bei der Einsichtnahme in ausgelegte Unterlagen Name und Adresse festzuhalten sind. Dies würde im Gegenteil der gesetzlich vorgeschriebenen Bürgerbeteiligung am Verfahren zuwiderlaufen und möglicherweise dazu führen, daß sich Bürger durch die Adreßfeststellung von einer Einsichtnahme abschrecken ließen. Erst in einem späteren Verfahrensstadium, nämlich, wenn schriftliche Einwendungen gegen das Verfahren vorliegen, ist deren Weiterleitung mit Name und Adresse an den Antragsteller zur Überprüfung der Vorwürfe ggf. erforderlich und auch rechtlich zulässig (§ 12 Abs. 2 9. BImSchV).

In seiner Stellungnahme hat das Landratsamt meine Rechtsauffassung ebenfalls bestätigt.

Zwischenzeitlich wurde mir bereits ein weiterer ähnlicher Fall bekannt. Auch hier wurde eine Bürgerin, die Einsicht in einen öffentlich ausgelegten Bebauungsplanentwurf nahm, aufgefordert, sich mit Name und Anschrift in eine Liste, die beim örtlichen Stadtbauamt als Auslegungsort geführt wurde, einzutragen. Zwar brachte die Stadt auf meine Anfrage vor, der Eintrag in die Unterschriftenliste sei auf freiwilliger Basis erfolgt und werde lediglich als Nachweis für die ordnungsgemäße Durchführung der Bürgerbeteiligung zu den Akten genommen. Da jedoch das Baugesetzbuch, das das Bauleitplanverfahren detailliert regelt, keine Vorschrift über Aufzeichnungen anläßlich der vorgezogenen Bürgerbeteiligung enthält, war das Führen einer Unterschriftsliste datenschutzrechtlich unzulässig. Ich habe die Stadt aufgefordert, die Unterschriftsliste zu vernichten und ihre Bediensteten entsprechend zu belehren. Zum Nachweis der ordnungsgemäßen Bürgerbeteiligung ist die öffentliche Bekanntmachung nach § 3 Abs. 2 Satz 1 und 2 BauGB ausreichend.

18. Verkehrswesen

18.1 Speicherung von Unschuldigen in „Schwarzfahrerdateien"

Im 12. und 13. Tätigkeitsbericht habe ich darüber berichtet, daß die Stadtwerke München Unschuldige, deren Namen von unbekannten Schwarzfahrern mißbraucht werden, speichern. Ich hatte gefordert, daß Personen, deren Name mißbraucht worden ist, nur mit ihrem ausdrücklichen Einverständnis gespeichert werden dürfen. Hierzu habe ich folgendes Verfahren vorgeschlagen:

Wird nach einer Fahrgastbeanstandung ein Namensmißbrauch festgestellt, so werden die Daten des Betroffenen in der Datei für erhöhtes Beförderungsentgelt sofort gelöscht, es sei denn, der Betroffene willigt ausdrücklich schriftlich in die weitere Speicherung seiner Daten für weitere drei Monate zur Täterermittlung ein. Hierzu übersenden die Stadtwerke dem Betroffenen sofort nach Feststellung des Namensmißbrauchs einen Datensatz mit den von ihm gespeicherten Personalien. Der Datensatz muß in der Datei als Namensmißbrauchsfall gekennzeichnet werden. Willigt der Betroffene nicht innerhalb von 8 Tagen schriftlich in die Speicherung seiner Daten ein, werden diese gelöscht. Der Betroffene ist darauf hinzuweisen.

In den Fällen, in denen der Betroffene bestreitet, daß es sich bei ihm um den beanstandeten Fahrgast handelt, und sich weder die Richtigkeit noch die Unrichtigkeit seiner Angaben feststellen läßt, werden die Daten gem. § 35 Abs. 4 Bundesdatenschutzgesetz zunächst gesperrt und spätestens nach drei Monaten gelöscht, es sei denn, in der Zwischenzeit stellt sich zweifelsfrei heraus, daß es sich bei dem Betroffenen doch um den beanstandeten Fahrgast handelt und die Stadt beabsichtigt, gegen ihn Ansprüche geltend zu machen.

Die Stadtwerke haben erklärt, daß sie meinem Vorschlag entsprechend verfahren werden.

18.2 Weitergabe einer Führerscheinakte durch die Kfz-Zulassungsstelle an den TÜV

Ein Bürger beschwerte sich bei mir darüber, daß die Führerscheinstelle einer kreisfreien Stadt seine Führerscheinakten an den Technischen Überwachungsverein weitergegeben hat. Zwar habe er sein Einverständnis dazu erteilt, die Akten hätten jedoch um die darin enthaltenen Auskünfte aus dem Verkehrszentralregister bereinigt werden müssen.

Eine Überprüfung ergab, daß die Weitergabe der Akten an den Technischen Überwachungsverein datenschutzrechtlich zulässig war.

Nach der Staßenverkehrszulassungsordnung kann die Straßenverkehrsbehörde unter bestimmten Voraussetzungen anordnen, daß der Bewerber um eine Fahrerlaubnis das Gutachten eines Amts- oder eines Facharztes, einer amtlich anerkannten medizinisch-psychologischen Untersuchungsstelle oder eines amtlich anerkannten Sachverständigen oder Prüfers für den Kraftfahrzeugverkehr über die körperliche oder geistige Eignung zum Führen von Kraftfahrzeugen beizubringen hat. Da dem Petenten bereits 1988 und 1991 die Fahrerlaubnis entzogen wurde, bestanden bei der Straßenverkehrsbehörde begründete Zweifel an seiner Fahreignung. Die Führerscheinakte des Petenten wurde deshalb anläßlich seines Antrags auf Neuerteilung einer Fahrerlaubnis an die Begutachtungsstelle für Fahreignung beim Technischen Überwachungsverein weitergegeben. Zu diesem Verfahren erteilte der Petent seine Zustimmung. Bei dem Technischen Überwachungsverein handelt es sich um eine amtlich anerkannte Untersuchungsstelle für die Feststellung der Eignung zum Führen von Kraftfahrzeugen. Die in den Führerscheinakten des Petenten enthaltenen Auskünfte aus dem Verkehrszentralregister waren verwertbar, da die Tilgungsfrist noch nicht verstrichen war.

18.3 Überlassung von Daten durch die Kfz-Zulassungsstelle an die Polizei

Ein Bürger bat mich um Überprüfung, ob die Polizei in seine Akte bei der Kfz-Zulassungsstelle Einsicht nehmen durfte. Er teilte mir dazu mit, die Polizei habe ihn verdächtigt, Kraftfahrzeuge ohne Gewerbeanmeldung zu veräußern. Tatsächlich sei er jedoch nur auf der Suche nach einem „Oldtimer" gewesen und habe deshalb für mehrere Probefahrten „rote Kraftfahrzeugkennzeichen" benötigt.

Meine datenschutzrechtlichen Ermittlungen haben ergeben, daß die Polizei gegen den Petenten den Verdacht hatte, ohne Gewerbeanmeldung einen Kfz-Handel zu betreiben. Der Polizei waren mehrere Male vor der Wohnung des Petenten immer wieder andere Fahrzeuge mit roten Überführungskennzeichen aufgefallen. Zur Überprüfung dieses Verdachts suchte der zuständige Polizeisachbearbeiter die Kfz-Zulassungsstelle auf und nahm dort Einsicht in die Unterlagen des Petenten.

Die Akteneinsichtnahme war datenschutzrechtlich nicht zu beanstanden. Gemäß § 35 Abs. 1 Nr. 3 des Straßenverkehrsgesetzes dürfen Fahrzeug- und Halterdaten an Polizeidienststellen zur Verfolgung von Ordnungswidrigkeiten übermittelt werden. Der Betrieb eines Kfz-Handels ohne die Anmeldung beim Gewerbeamt ist eine Ordnungswidrigkeit. Die Einsichtnahme durch den Polizeibeamten in die Unterlagen des Petenten bei der Zulassungsstelle stellte eine Datenübermittlung im Sinne von § 35 Abs. 1 Nr. 3 Straßenverkehrsgesetz dar. Zum Zeitpunkt der Einsichtnahme in die Unterlagen des Petenten war für die Polizei nicht erkennbar, daß der Petent die roten Kennzeichen lediglich für den Erwerb des „Oldtimers" verwenden wollte.

Die Polizei war danach berechtigt, im Rahmen des gegen den Petenten bestehenden Anfangsverdachts seine Halterdaten bei der Zulassungsstelle einzusehen. Nur mit Hilfe solcher Einsichtnahmen kann die Polizei ihre gesetzlichen Aufgaben – zu denen auch die Verfolgung von Ordnungswidrigkeiten gehört – erfüllen.

18.4 Direktzugriff kommunaler Verkehrsüberwachungsdienste im automatisierten Verfahren auf die Halterdaten der Kfz-Zulassungsstellen

Im Berichtszeitraum war ich mit der Frage befaßt, ob kommunale Verkehrsüberwachungsdienste (städtische Behörde) von der städtischen Kfz-Zulassungsstelle im Online-Verfahren Halterdaten zum Zwecke der Verfolgung von Verkehrsordnungswidrigkeiten gem. § 35 Abs. 1 Nr. 3 in Verbindung mit § 32 Abs. 2 Straßenverkehrsgesetz abrufen dürfen. Nach § 2 Abs. 3 der Verordnung über Zuständigkeiten im Ordnungswidrigkeitenrecht sind die in der Anlage zu dieser Verordnung aufgeführten Kommunen für die Verfolgung geringfügiger Ordnungswidrigkeiten nach § 24 des Straßenverkehrsgesetzes, die im ruhenden Ver-

kehr festgestellt werden, in gleicher Weise wie die Polizei zuständig.

Zum Direktzugriff kommunaler Verkehrsüberwachungsdienste im automatisierten Verfahren auf die Halterdaten der Kfz-Zulassungsstelle vertrete ich die Auffassung, daß der Online-Zugriff von Überwachungsdiensten von kreisangehörigen Gemeinden unzulässig, von kreisfreien Gemeinden hingegen zulässig ist:

1. **Überwachungsdienst von kreisangehörigen Gemeinden**

   Die Übermittlung von Daten durch Abruf im automatisierten Verfahren aus dem Zentralen Fahrzeugregister und aus den örtlichen Fahrzeugregistern ist in § 36 des Straßenverkehrsgesetzes geregelt. Nach § 36 Abs. 2 Satz 2 des Straßenverkehrsgesetzes und § 12 Abs. 2 der Fahrzeugregisterverordnung steht den örtlich zuständigen Polizeidienststellen der Länder der Direktzugriff auf die Halterdaten der Kfz-Zulassungsstellen zu. Unter Polizeidienststellen im Sinne von § 36 Abs. 2 Satz 2 des Straßenverkehrsgesetzes sind die **Polizeivollzugs**dienststellen zu verstehen. Die kommunalen Verkehrsüberwachungsdienste sind keine Polizeivollzugsdienststellen. In § 36 des Straßenverkehrsgesetzes sind sie als abrufberechtigte Stellen nicht aufgeführt. Nach dieser Vorschrift sind die kommunalen Verkehrsüberwachungsdienste somit nicht berechtigt, Halterdaten im Online-Verfahren von den Kfz-Zulassungsstellen abzufragen.

2. **Überwachungsdienst von kreisfreien Gemeinden**

   § 36 des Straßenverkehrsgesetzes enthält eine bereichsspezifische Regelung allerdings nur für die **Übermittlung** von Daten aus dem Zentralen Fahrzeugregister und den örtlichen Fahrzeugregistern. Nach § 3 Abs. 5 Ziffer 3 des Bundesdatenschutzgesetzes, das im Interesse einer bundesweit einheitlichen Anwendung der Vorschriften zur Datenverarbeitung im Straßenverkehrsgesetz und in der Fahrzeugregisterverordnung zur Begriffsbestimmung heranzuziehen ist, ist Übermitteln die Bekanntgabe personenbezogener Daten an einen **Dritten**. Keine Übermittlung liegt danach bei einer Abfrage von Daten **innerhalb der speichernden Stelle** vor.

   Eine Abfrage von Halterdaten der Kfz-Zulassungsstellen im Online-Verfahren innerhalb der speichernden Stelle kommt bei kreisfreien Städten, die kommunale Verkehrsüberwachungsdienste haben, in Betracht. Der Direktzugriff kommunaler Verkehrsüberwachungsdienste im automatisierten Verfahren auf die Halterdaten der Kfz-Zulassungsstellen ist somit bei kreisfreien Städten im Straßenverkehrsgesetz und in der Fahrzeugregisterverordnung nicht geregelt. Da es sich bei diesen Abfragen nicht um eine Übermittlung von Daten im Online-Verfahren handelt, für die § 36 des Straßenverkehrsgesetzes i.V.m. § 12 der Fahrzeugregisterverordnung eine abschließende Regelung darstellen, richtet sich die Zulässigkeit derartiger Abfragen gem. § 46 des Straßenverkehrsgesetzes nach den Landesdatenschutzgesetzen.

   Nach Art. 17 Abs. 3 Satz 2 i.V.m. Art. 17 Abs. 1 des Bayer. Datenschutzgesetzes ist die Abfrage der Halterdaten der Kfz-Zulassungsstellen durch die kommunalen Verkehrsüberwachungsdienste zulässig, wenn sie zur rechtmäßigen Aufgabenerfüllung einer dieser Stellen erforderlich ist. Kommunale Verkehrsüberwachungsdienste sind, wie ich oben bereits ausgeführt habe, nach § 2 Abs. 3 der Verordnung über Zuständigkeiten im Ordnungswidrigkeitenrecht zur Verfolgung geringfügiger Ordnungswidrigkeiten nach § 24 des Straßenverkehrsgesetzes, die im ruhenden Verkehr festgestellt werden, in gleicher Weise wie die Dienststellen der Polizei zuständig. Zur Erfüllung dieser Aufgabe ist die Kenntnis der Halterdaten der Personen, mit deren Kfz eine Ordnungswidrigkeit im ruhenden Verkehr begangen wurde, erforderlich.

Im Ergebnis besitzen danach die kommunalen Verkehrsüberwachungsdienste der kreisfreien Städte einen Direktzugriff im automatisierten Verfahren auf die Halterdaten der kommunalen Kfz-Zulassungsstellen, während den Verkehrsüberwachungsdiensten der kreisangehörigen Gemeinden, die sich die Halterdaten durch Abfrage bei den Kfz-Zulassungsstellen der Kreisverwaltungsbehörden übermitteln lassen müssen, dieser nicht zusteht.

18.5 Aufbewahrungsfristen bei Führerscheinakten

Ein Bürger bat mich um Auskunft, ob ein verkehrsstrafrechtlicher Vorgang, der nach fünf Jahren aus dem Verkehrszentralregister beim Kraftfahrtbundesamt gelöscht wird, weiter in den Akten der Führerscheinstelle des Landratsamtes geführt werden darf.

Für Eintragungen im Bundeszentralregister und im Verkehrszentralregister über Vorstrafen und den Entzug der Fahrerlaubnis gelten Wirkungsfristen und Verwertungsverbote. Nach § 51 Abs. 1 Bundeszentralregistergesetz darf die Tat und die Verurteilung dem Betroffenen im Rechtsverkehr grundsätzlich nicht mehr vorgehalten und nicht zu seinem Nachteil verwertet werden, wenn die Eintragung über die Verurteilung im Register getilgt worden oder sie zu tilgen ist. Abweichend von § 51 Abs. 1 Bundeszentralregistergesetz darf jedoch eine frühere Tat weiterhin in einem Verfahren berücksichtigt werden, das die Erteilung oder Entziehung einer Fahrerlaubnis

zum Gegenstand hat, wenn die Verurteilung wegen dieser Tat in das Verkehrszentralregister einzutragen war (§ 52 Abs. 2 Bundeszentralregistergesetz). Diese Vorschrift will den Belangen der Verkehrssicherheit Rechnung tragen und erlaubt bei gerichtlichen oder verwaltungsbehördlichen Verfahren, in denen es um die Wiedererteilung der Fahrerlaubnis geht, die Berücksichtigung lange zurückliegender Straftaten. Die Führerscheinstelle ist in diesen Fällen berechtigt, die diesbezüglichen Akten weiterzuführen und die Unterlagen bei einem eventuellen Verfahren auf Erteilung oder Entziehung einer Fahrerlaubnis zu verwerten.

Die Führerscheinstelle ist verpflichtet, Führerscheinakten mit Vorgängen, die mit der Versagung, Beschränkung oder Entziehung einer Fahrerlaubnis in Zusammenhang stehen oder Unterlagen enthalten, die über die körperliche und geistige Eignung von Fahrerlaubnisbewerbern oder Inhabern etwas aussagen, mindestens 10 Jahre aufzubewahren. Auch nach Ablauf dieser Mindestaufbewahrungsfrist hat die Tilgung von Vorgängen zu unterbleiben, solange die Erteilung einer neuen Fahrerlaubnis untersagt ist.

18.6 Zentrales Verkehrsinformationssystem (ZEVIS)

Das Kraftfahrtbundesamt (KBA) in Flensburg hält im Zentralen Verkehrsinformationssystem (ZEVIS) einen Teil der Daten des Zentralen Fahrzeugregisters und des Verkehrszentralregisters für den Direktabruf durch die Polizei bereit. Die Polizei kann auf diesem Weg rund um die Uhr in Sekundenschnelle die Halter von Kraftfahrzeugen ermitteln und feststellen, ob einem kontrollierten Fahrzeuglenker der Führerschein entzogen ist.

Dem Schutz der Daten im ZEVIS vor mißbräuchlicher Verwendung hat der Gesetzgeber 1986 ganz besondere Bedeutung beigemessen.

Neben anderen Sicherungsverfahren ist ein besonderes **Anmeldeverfahren** vorgesehen.

Bei der Prüfung des Anmeldeverfahrens für ZEVIS-Abfragen habe ich folgende Feststellungen getroffen:

Jeder Polizeibeamte der Bayerischen Polizei, der von einem der über 2000 zugelassenen Datenendgeräte aus ZEVIS abfragen möchte, muß sich zunächst durch Eingabe **seiner Stammnummer** oder einer **entsprechenden Benutzerkennung** und einem 6- bis 8stelligen Paßwort über den jeweiligen örtlichen Rechner beim Informationssystem der Bayerischen Polizei (IBP) anmelden. Wird diese Anmeldung akzeptiert **und** ist das benutzte Datenendgerät **sowohl** beim Bayer. Landeskriminalamt als Zentralstelle der Bayerischen Polizei **als auch** beim KBA als für ZEVIS berechtigt gemeldet, so kann der Beamte die Abfrage im ZEVIS durchführen. Gibt der Beamte die **Benutzerkennung** oder das **Paßwort mehrmals** falsch ein, wird das entsprechende Datenendgerät vom Rechner der örtlichen Dienststelle gesperrt, mit der Folge, daß weitere Anmeldeversuche unmöglich sind. Diese Vorkehrung dient dem Schutz des Datenbestandes im ZEVIS vor Abfragen durch Unberechtigte.

Die **Anzahl der gestatteten Fehlversuche** kann jedoch bei den einzelnen örtlichen Polizeirechnern – je nach Einstellung des Rechners – unterschiedlich sein. Während beispielsweise bei einem Großstadtpräsidium lediglich zwei Fehlversuche toleriert werden, werden die Datenendgeräte des Bayer. Landeskriminalamts erst bei der sechsten Fehlanmeldung gesperrt. Unter Berücksichtigung der Regelungen in der Fahrzeugregisterverordnung dürfen jedoch nur zwei Fehlanmeldungen gestattet werden.

Ich habe das Innenministerium gebeten, landesweit einheitlich nur zwei folgenlose Fehlversuche zuzulassen. Das Innenminisiterium hat meine Forderung aufgegriffen und das Bayer. Landeskriminalamt mit der technischen Umsetzung beauftragt.

19. Medien

19.1 Entwurf des Bayerischen Mediengesetzes

In meinem letzten Tätigkeitsbericht habe ich über die datenschutzrechtlichen Regelungen im Entwurf des Bayerischen Mediengesetzes berichtet. Zur weiteren Verbesserung des Datenschutzes hatte ich vorgeschlagen, über den vorgesehenen Auskunfts- und Berichtigungsanspruch hinaus auch einen **Anspruch auf Sperrung** unrichtiger Daten vorzusehen, wenn die richtigen Daten nicht festgestellt werden können und deshalb eine Berichtigung nicht möglich ist. Dieser Vorschlag wurde vom Bayerischen Senat aufgegriffen und im neuen Mediengesetz berücksichtigt, das am 1. Dezember 1992 in Kraft getreten ist.

19.2 Gesetzentwurf zur Änderung des Bayerischen Rundfunkgesetzes

Am 1. Januar 1992 ist der Staatsvertrag über den Rundfunk im vereinten Deutschland in Kraft getreten. Dieser Staatsvertrag enthält in Art. 1 den neuen Rundfunkstaatsvertrag, der den Rundfunkstaatsvertrag vom 3. April 1987 ersetzt.

Die Bayerische Staatsregierung hat im Berichtszeitraum den Entwurf eines Gesetzes zur Änderung des Bayerischen Rundfunkgesetzes vorgelegt. Mit dem Gesetzentwurf soll das Bayerische Rundfunkgesetz an den neuen Rundfunkstaatsvertrag und an neuere

Rechtsentwicklungen innerhalb des öffentlich-rechtlichen Rundfunks angepaßt werden.

Der Entwurf enthält auch **bereichsspezifische Datenschutzregelungen für den Bayerischen Rundfunk**. Im 13. Tätigkeitsbericht habe ich gefordert, zugunsten des von der Datenverarbeitung des Bayerischen Rundfunks Betroffenen weitere Ansprüche zu schaffen, um eine Beeinträchtigung seines Persönlichkeitsrechts durch die Datenverarbeitung zu verhindern. Der vorliegende Gesetzentwurf enthält nunmehr ein **Auskunftsrecht** der Betroffenen. Er sieht vor, daß der von einer Berichterstattung in seinem Persönlichkeitsrecht **Betroffene** Auskunft über die der Sendung zugrundeliegenden, zu seiner Person gespeicherten Daten verlangen kann. Der Gesetzentwurf sieht außerdem vor, daß der Datenschutz beim Bayerischen Rundfunk wie bisher durch einen rundfunkeigenen, weisungsunabhängigen **Datenschutzbeauftragten** überwacht wird. Der Gesetzentwurf berücksichtigt auch die folgenden von mir zu einem früheren Referentenentwurf vorgeschlagenen datenschutzrechtlichen Verbesserungen:

- Der Bayerische Rundfunk hat die Rundfunksendungen vollständig aufzuzeichnen und auf die Dauer von 2 Monaten aufzubewahren. Geht innerhalb dieser Frist eine Beanstandung oder Beschwerde ein, so ist die Aufzeichnung aufzubewahren, bis die Beanstandung oder Beschwerde durch rechtskräftige gerichtliche Entscheidung, durch gerichtlichen Vergleich oder auf andere Weise erledigt ist.

- Der von einer Berichterstattung Betroffene hat einen Anspruch auf Sperrung unrichtiger Daten für den Fall, daß richtige Daten nicht festgestellt werden können und deshalb eine Berichtigung nicht möglich ist.

In meinen früheren Tätigkeitsberichten hatte ich für jeden Bürger – unabhängig davon, ob er von einer vorausgehenden Sendung in seinem Persönlichkeitsrecht bereits verletzt wurde – ein Auskunftsrecht über die zu seiner Person von Rundfunk und Presse gespeicherten Daten gefordert, weil nur ein schon vor einer Rechtsverletzung gewährter Auskunftsanspruch eine Verletzung des Persönlichkeitsrechts wirksam verhindern kann. Diese Forderung ist angesichts des im Rundfunkstaatsvertrags erst vor kurzem festgelegten Datenschutzstandards derzeit nicht durchsetzbar. Ich werde sie aber umgehend wieder aufgreifen, sobald Mißbrauchsfälle belegen, daß die Regelung des Rundfunkstaatsvertrags unzureichend ist.

19.3 Presseerklärungen der Verwaltung

Im Berichtszeitraum war ich wiederholt mit der Frage befaßt, auf welcher Rechtsgrundlage und unter welchen Voraussetzungen die Verwaltung die Presse von Verwaltungsvorgängen unterrichten darf.

Das Innenministerium vertritt folgende Auffassung:

Das in § 4 Abs. 1 Satz 1 des Bayerischen Pressegesetzes geregelte **Auskunftsrecht der Presse gegenüber Behörden** findet seine Grundlage unmittelbar im Grundrecht auf Pressefreiheit nach Art. 5 Abs. 1 Satz 2 Grundgesetz (GG). Nach allgemein herrschender Auffassung verpflichtet die Garantie der Pressefreiheit den Staat, die ungehinderte Betätigung der Presseangehörigen von der Beschaffung der Information bis zur Verbreitung der Nachrichten zu ermöglichen, zum Teil auch durch die Gewährung positiver Rechte. Eines dieser für die Pressetätigkeit essentiellen Forderungsrechte ist der Anspruch der Presse, von Behörden über Vorgänge der innerstaatlichen Verwaltung unterrichtet zu werden. Das Bundesverfassungsgericht hat bereits in seinem Urteil vom 5.8.1966 dargelegt, daß die Auskunftspflicht der öffentlichen Behörden eine prinzipielle Folge der Pressefreiheit ist.

Entsprechend den Grundsätzen des Bundesverfassungsgerichts, wonach die Verfassung und insbesondere ihr Grundrechtsteil als Einheit anzusehen ist, ist für die Bestimmung der Schranken der Pressefreiheit auch das aus dem Grundrecht des Art. 2 Abs. 1 GG abgeleitete Recht auf informationelle Selbstbestimmung zu beachten. **Umgekehrt** sind die Schranken des Rechts auf informationelle Selbstbestimmung, was den Pressebereich anbelangt, im Lichte der besonderen Bedeutung der Pressefreiheit zu bestimmen. Die Beschränkung des Auskunftsanspruchs in § 4 Abs. 2 Bayerisches Pressegesetz und der darin liegende generalisierende Ausgleich zwischen allgemeinem Persönlichkeitsrecht und Pressefreiheit entspricht dem verfassungsrechtlichen Gebot, nach dem Grundsatz der praktischen Konkordanz beide Grundrechte bestmöglich zur Geltung zu bringen.

Anders stellt sich die Rechtslage dar, wenn eine Behörde Auskünfte an die Presse erteilt, **ohne dazu durch ein Auskunftsersuchen verpflichtet** zu sein. Ein Rechtsanspruch der Presse auf Versorgung mit Informationen von seiten der öffentlichen Hand über alle die Öffentlichkeit interessierenden amtlichen Vorgänge läßt sich aus der grundrechtlich gewährten Pressefreiheit nicht ableiten. Insoweit kann sich die Behörde nicht darauf berufen, aus Art. 5 GG zur Auskunft verpflichtet zu sein, wenn sie von sich aus Informationen mit persönlichen Daten über Bürger an die Presse gibt. Damit kommen in diesem Fall die Grundsätze des Art. 18 BayDSG zur Anwendung. Eine Übermittlung an Dritte außerhalb des öffentlichen Bereichs ist danach zulässig, wenn der Empfänger ein berechtigtes Interesse an der Kenntnis der zu übermittelnden Daten glaubhaft macht und dadurch

schutzwürdige Belange der Betroffenen nicht beeinträchtigt werden.

Im Prinzip teile ich die Rechtsauffassung des Innenministeriums. Sowohl bei der Unterrichtung der Presse aufgrund eines Auskunftsersuchens eines Journalisten als auch bei einer Presseinformation ohne ein solches Ersuchen halte ich es wegen der Konkordanz der Grundrechte für geboten, daß die Würde des Menschen, sein Persönlichkeitsrecht und sein daraus abgeleitetes Recht auf informationelle Selbstbestimmung angemessen bei der Unterrichtung der Öffentlichkeit berücksichtigt werden. In jedem Fall ist daher eine Abwägung zwischen der Pressefreiheit und den schutzwürdigen Interessen des Einzelnen erforderlich. Diese **Abwägungspflicht** sollte im Bayer. Pressegesetz zum Ausdruck gebracht werden.

Zur Frage, in welcher Form Auskunftsersuchen der Presse beantwortet werden, bin ich der Meinung, daß es in der Regel nicht erforderlich ist, Schreiben von Bürgern oder andere Verwaltungsvorgänge mit personenbezogenen Daten an die Presse weiterzuleiten. Wenn die Bürger damit rechnen müßten, daß ihre Petitionen in vollem Inhalt und Wortlaut an die Presse weitergegeben werden, dann werden sie häufig davon absehen, von ihren Rechten Gebrauch zu machen. Dies gilt erst recht für die Fälle, in denen eine Behörde Auskünfte an die Presse erteilt, ohne dazu durch ein konkretes Ersuchen verpflichtet zu sein. Eine Weiterleitung von Petitionen, sonstigen Schreiben und Unterlagen mit personenbezogenen Daten von Bürgern an die Presse kommt in der Regel nur mit Einwilligung der Betroffenen in Betracht. Für zu weitgehend halte ich auch die verschiedentlich festgestellte Praxis in Gemeinden, bei der Behandlung von Bauanträgen die behördeninternen Vermerke zu dem Vorhaben, die im Gemeinderat nicht vorgetragen werden, der Presse zur Verfügung zu stellen, so daß der Journalist auf der Pressebank über die behördliche Bewertung eines Baugesuchs besser informiert ist als der bauantragstellende Bürger.

19.4 Datenschutz bei internen Telekommunikationsanlagen

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat sich in ihrer Sitzung am 1./2. Oktober 1992 mit dem Thema „Datenschutz bei internen Telekommunikationsanlagen" befaßt. Der Schutz des Fernmeldegeheimnisses und des nichtöffentlich gesprochenen Wortes ist gerade bei Arbeitnehmern bedeutsam, da diese sich in einem besonderen Abhängigkeitsverhältnis befinden. Geschützt werden müssen aber auch Dritte, die anrufen oder angerufen werden. Zum Schutz dieser Personen und der Arbeitnehmer haben die Datenschutzbeauftragten in einer Entschließung bundesrechtliche Regelungen gefordert, die verbindliche Vorgaben für die technische Ausgestaltung von Telekommunikationsanlagen geben und den Umfang der zulässigen Datenverarbeitung festlegen. Die Entschließung ist in der Anlage zu diesem Tätigkeitsbericht abgedruckt.

19.5 Regelmäßige Übermittlung von Einwohnermeldedaten an die GEZ für den Rundfunkgebühreneinzug

Dem Bayer. Rundfunk (BR) entstehen nach Darstellung des Bayer. Obersten Rechnungshofes (ORH), der sich in einem Sonderbericht mit der finanziellen Situation des BR befaßt hat, durch die Rundfunkteilnehmer, die ihre Radio- und Fernsehgeräte nicht angemeldet haben, erhebliche Einnahmeausfälle.

Nach Auffassung des ORH könnte die offensichtliche Divergenz zwischen den vorhandenen und den angemeldeten Geräten durch eine regelmäßige Übermittlung von Einwohnermeldedaten an die Gebühreneinzugszentrale (GEZ) vermindert werden. Der ORH empfiehlt dazu den Erlaß einer Verordnung nach Art. 31 Abs. 5 des Bayer. Meldegesetzes, welche die regelmäßige Übermittlung der Daten über An- und Abmeldungen sowie Sterbefälle aller volljährigen Einwohner von den Meldeämtern an den Bayer. Rundfunk bzw. die GEZ zuläßt.

Aus datenschutzrechtlicher Sicht ist die regelmäßige Übermittlung von Meldedaten an die GEZ zulässig, wenn sie zur rechtmäßigen Erfüllung der Aufgaben der GEZ erforderlich ist und schutzwürdige Belange der Betroffenen nicht beeinträchtigt werden (Art. 31 Abs. 1 Satz 1 und Art. 7 MeldeG).

Nach dem Rundfunkgebühren-Staatsvertrag ist der Einzug der Rundfunkgebühren Aufgabe des Bayer. Rundfunks. Erforderlich ist die Datenübermittlung, wenn **der Bayer. Rundfunk bzw. die GEZ den Nachweis führen, daß ohne diese Angaben ein erheblicher Einnahmeausfall entsteht.**

In Nordrhein-Westfalen, das ebenso wie Hessen in seiner Meldedatenübermittlungsverordnung die regelmäßige Datenübermittlung durch die Einwohnermeldeämter an die Landesrundfunkanstalt bzw. die GEZ zur Erfüllung der Aufgaben des Rundfunkgebühreneinzugs geregelt hat, haben Werbemaßnahmen, die mit Hilfe der übermittelten Daten durchgeführt werden konnten, zu Gebührenmehreinnahmen in zweistelliger Millionenhöhe geführt.

Auch der Bayer. Rundfunk rechnet bei einer entsprechenden Änderung der Bayer. Meldedatenübermittlungsverordnung mit einer wesentlichen Erhöhung des Rundfunkgebührenaufkommens. Dies soll vor allem durch Direktwerbemaßnahmen wie in Nordrhein-Westfalen und einen Datenabgleich, den die GEZ bei einer regelmäßigen Übermittlung von Meldeänderungsdaten mit den bei ihr gespeicherten Teil-

nehmerdaten vornehmen könnte, erreicht werden. Durch den Datenabgleich wäre es möglich, den Datenbestand der GEZ laufend zu aktualisieren. Damit würde vermieden, daß aufgrund veralteter Daten Gebühren entweder zu Unrecht nicht eingezogen oder umgekehrt zu Unrecht eingezogen würden. Durch einen zutreffenden Gebühreneinzug würde auch vermieden, daß die Gebühren der falschen Rundfunkanstalt gutgeschrieben werden. Da nämlich das Gebührenaufkommen der Landesrundfunkanstalt zusteht, in deren Anstaltsbereich der Rundfunkteilnehmer wohnt, sich ständig aufhält oder ständig ein Rundfunkgerät zum Empfang bereit hält, dürfte der Bayer. Rundfunk infolge der hohen Zuzugsquote nach Bayern hier besonders betroffen sein.

Zu berücksichtigen ist allerdings, daß von einer regelmäßigen Übermittlung von Meldedaten an die GEZ auch Personen erfaßt werden, die nicht gebührenpflichtig sind und auf deren Daten der Bayer. Rundfunk somit keinen Anspruch hat. Diese Personen wären in ihrem Recht auf informationelle Selbstbestimmung betroffen. Es kann sich hier aber zahlenmäßig nur um eine sehr kleine Gruppe handeln, denn nach den Angaben des Statistischen Bundesamtes sind 99 v. H. aller privaten Haushalte mit Hörfunk und 96 v. H. mit Fernsehgeräten ausgestattet. Hinzu kommt, daß die zu übermittelnden Daten nicht von besonderer Sensibilität sind. Im Hinblick auf den Nutzen des Verfahrens – Verminderung von Einnahmeausfällen durch Schwarzhörer und Schwarzseher im Interesse der Gebührengerechtigkeit und Lastengleichheit – halte ich die Übermittlung von Meldedaten auch dieser Personen für zumutbar, wenn durch eine Regelung in der Meldedatenübermittlungsverordnung sichergestellt wird, daß die übermittelten Daten ausschließlich zum Zwecke des Gebühreneinzugs verwendet und nicht mehr benötigte Daten unverzüglich gelöscht werden. Unter dieser Voraussetzung sehe ich auch nicht die Gefahr, daß durch die regelmäßige Meldedatenübermittlung beim Bayer. Rundfunk ein verkürztes Einwohnerregister entsteht.

20. Technischer und organisatorischer Bereich

20.1 Fortentwicklung der Datensicherheit

20.1.1 Sicherheit beim Einsatz von UNIX-Systemen

20.1.1.1 Allgemeines

Die Zahl der UNIX-Systeme innerhalb der öffentlichen Verwaltung Bayerns nimmt ständig zu. Viele öffentliche Stellen betreiben UNIX-Rechner als Abteilungsrechner sowohl für **klassische Datenverarbeitungsaufgaben** als auch für die innerbehördliche **Bürokommunikation**.

Das Betriebssystem UNIX bietet standardmäßig folgende Einrichtungen der Zugriffssicherung:

- Die **hierarchisch gestuften Benutzerkennungen** „owner" (Ersteller einer Datei), „group" (Gruppe, zu der ein Benutzer gehört) und „other" (alle Benutzer, die auf einem Rechner arbeiten können) steuern den Zugriff auf eine Datei. Über die drei Datei-Zugriffsklassen „r" (Lesen), „w" (Schreiben) und „x" (Ausführen) wird die Zugriffsart für die Benutzerkreise gesteuert. Schließlich ist jede Benutzerkennung mit einem Paßwort zu schützen.
- Die **Paßworte** werden in einwegverschlüsselter Form auf dem Rechner abgespeichert und können auch vom Systemverwalter (Super User) nicht entschlüsselt werden.
- Hat ein Benutzer sein Paßwort vergessen, geht der Zugang zu den geschützten Dateien nicht verloren, sondern der Systemverwalter kann das Paßwort, ohne es kennen zu müssen, entfernen und durch ein anderes ersetzen.
- Festlegungen über **Mindestlänge** und **Gültigkeitsdauer** gehören hingegen erst ab den neuesten UNIX-Versionen zum sogenannten UNIX-Standard.

Als ein großer Mangel gilt allerdings, daß ein potentieller Eindringling **beliebig viele Versuche** hat, um ein Paßwort durch Probieren herauszubekommen. Das Sperren der Benutzerkennung oder des Endgerätes, von dem aus der Penetrationsversuch gestartet wird, unterstützt UNIX derzeit nicht. Zur Selbstkontrolle zeigt das Betriebssystem dem Benutzer nach der erfolgreichen Anmeldung allerdings das Datum und die Uhrzeit der letzten Sitzung an. Sollte ein anderer Benutzer beim Ausspähen des Paßworts Erfolg gehabt haben, würde die mißbräuchliche Verwendung auf diese Weise im Nachhinein bekannt.

Diese Zugriffsschutzmechanismen genügen den heutigen differenzierten Sicherheitsanforderungen mancher Anwender nicht mehr, insbesondere dann, wenn sich die Benutzer nicht in eine klassische hierarchische Struktur einordnen lassen. Die feste Verknüpfung der Zugriffsrechte eines Benutzers und seiner Gruppe kann überall dort zu Schwierigkeiten führen, wo ein Benutzer mehreren Gruppen angehören muß. Dies ist in der Praxis beispielsweise dann der Fall, wenn jemand vorübergehend eine Kranken- oder Urlaubsvertretung übernehmen soll oder ständig gruppenübergreifend tätig werden muß.

Das Standard-UNIX, ohne Verwendung von Zusatzsicherheitsprodukten, ist vom Departement of Defense (DoD) nach den amerikanischen Sicherheitskriterien in die Sicherheitsklasse „D" eingestuft worden. „D" bedeutet „minimale Sicherheit". In den deutschen IT-Sicherheitskriterien ist dafür überhaupt keine Funktionalitätsklasse vorgesehen. Für sicherheitsrelevante Anwendungen ist jedoch die Funktionalitätsklasse F2

(entsprechend der Funktionalität der Klasse C2 nach DoD = „ausreichende" Sicherheit) zu empfehlen, in der Funktionen der Identifikation und Authentisierung, der Rechteverwaltung, der Rechteprüfung, der Beweissicherung und der Wiederaufbereitung unterstützt sind (siehe IT-Sicherheitskriterien vom 11.1.1989, Bundesanzeigerverlagsgesellschaft).

20.1.1.2 Schwachpunkte

a) Systemverwaltung

Der Systemverwalter in UNIX-Systemen
- hat standardmäßig die Zugriffsrechte auf sämtliche Ressourcen und Objekte,
- kann alle Dateien lesen (sofern nicht verschlüsselt) und verändern,
- kann Eigentums- und Zugriffsrechte verändern,
- kann Systeminformationen manipulieren,
- kann auf Paßworttabellen zugreifen und
- kann Benutzer einrichten, sperren und deren Berechtigungen verändern.

Diese **umfassenden Rechte sind nicht kontrollierbar**, da der Systemverwalter die systemseitig geführten Systemprotokolle problemlos verändern oder ganz löschen kann. Im übrigen sagen diese Standardprotokolle wenig über die durchgeführten Aktivitäten aus. Aus der Sicht der Datensicherheitskontrolle ist das unbefriedigend, weil eine ordnungsgemäße Datenverarbeitung nicht in allen Phasen der Verarbeitung revisionsfähig dokumentiert ist.

b) Technische Sicherheit

Die Betriebssicherheit in UNIX-Systemen gilt als gut. Probleme können allerdings **Spannungsausfälle** verursachen. Das Dienstprogramm fsck (fsck = filesystem check) beseitigt zwar nach einem Spannungsausfall entstandene Fehlerzustände. Dabei versucht das Dienstprogramm defekte Dateisysteme zu reparieren. Trotzdem können Dateien und Dateiverzeichnisse (DVZ) verloren gehen.

Es ist deshalb sicherer, wenn man Spannungsausfälle durch Verwendung von **Spannungsstabilisatoren** innerhalb einer unterbrechungsfreien Stromversorgung ganz vermeiden kann. Auch eine doppelte (gespiegelte) Festplatte und der Einsatz von Datenbanksystemen, wie Informix und Oracle, bringen wegen der Transaktionssicherungstechnik (Speicherung der after- und before-images) zusätzliche Sicherheiten.

UNIX-Viren sind bisher noch nicht bekannt geworden. Experten rechnen allerdings damit, daß mit zunehmender Verbreitung von UNIX und mit steigendem Programmaustausch durch Raubkopien und Public Domain Software auch UNIX-Viren auftauchen werden.

20.1.1.3 Maßnahmen zur Verbesserung der Sicherheit

a) Systemverwalter

Die sorgfältige Auswahl eines befähigten und zuverlässigen Systemverwalters und mindestens eines Vertreters mit gleicher Qualifikation ist die Grundvoraussetzung für einen sicheren UNIX-Betrieb. (Jedes Betriebssystem läßt sich so verwalten, daß es Sicherheitslücken gibt.) Zur Verbesserung der Datensicherheit empfiehlt es sich, so weit wie möglich Funktionen zu trennen. Der Systemverwalter ist der DV-Abteilung oder dem Benutzerservice zuzuordnen und sollte nicht, sofern es die Personalsituation erlaubt, selbst Anwenderaufgaben wahrnehmen müssen. Schließlich bietet sich an, bei der Verarbeitung von besonders sensiblen Daten für diese Aufgaben ein geteiltes Paßwort zu verwenden, so daß bei der Anmeldung das Vier-Augen-Prinzip gilt. Vor der Installation und Einrichtung eines UNIX-Systems ist ferner auf eine ausreichende Schulung des Systemverwalters zu achten, da mangelhafte Sachkenntnis zu peinlichen Fehlern und letztlich zu Datenverlusten führen kann.

b) Systemverwaltung

Die Vergabe der „root"- und „admin"-Berechtigungen ist restriktiv zu handhaben. Der Vertreter des Systemverwalters muß allerdings in Ausnahmefällen, in denen der Systemverwalter nicht erreichbar ist, Zugang zum Systempaßwort erhalten. Durch organisatorische Festlegungen, etwa durch eine Neuvergabe des Paßworts, ist die Sicherheit des Systempaßwortes nach einer notwendig gewordenen Bekanntgabe an Dritte wieder herzustellen.

Im allgemeinen kann man davon ausgehen, daß, nachdem das System generiert ist und die Verfahren eingerichtet sind, ein Zugriff unter der root-Kennung nur in Ausnahmefällen nötig sein wird. Deshalb sollte man dem Vertreter lediglich durch Zurverfügungstellung einer eingeschränkten Shell-Berechtigung (etwa mit dem „rsh"- oder „sh-r"-Kommando) den Zugriff auf solche Befehle eröffnen, die für eine eingeschränkte Systemverwaltung und für die Fehlerbehebung notwendig sind.

Da eine eingeschränkte Shell-Berechtigung nicht für die Systemverwaltung geeignet ist, empfiehlt es sich, die „sh-r"-Berechtigung lediglich für den Anwendungsadministrator einzurichten, der nur bestimmte Funktionen im Fehlerfall innerhalb einer bestimmten Anwendung ausführen muß. Als Beispiele wären hier denkbar:
- Aktivierung eines blockierten Bildschirmes durch die Anwendung des kill-Kommandos, wobei zuerst durch „ps -txxx" die entsprechenden Prozessnummern (PID, Prozess ID) zu ermitteln sind und danach die Prozesse durch „kill -9 PID" abgebrochen werden.

- Löschung von core-Dateien, in denen dumps nach Systemabstürzen gespeichert sind, mit dem rm-Kommando (remove), um Speicherplatzengpässe zu beheben.

Da die Datei „/etc/passwd" normalerweise für alle Benutzer lesbar ist, können auch die verschlüsselten Paßworte von jedem Benutzer gelesen werden. Da der Verschlüsselungsalgorithmus bekannt ist, kann ein Eindringling ein Programm zum Ausforschen der Paßworte schreiben, obwohl der Verschlüsselungsmechanismus selbst nicht umkehrbar ist. Derartige Programme verschlüsseln eine vorgegebene Wortmenge und vergleichen die Chiffrate mit den Einträgen in /etc/passwd. Bei einer Übereinstimmung kennt der Eindringling das Paßwort des entsprechenden Benutzers und verfügt somit auch über dessen Rechte. Um dieses systematische Ausforschen zu verhindern, kann der Systemverwalter die Paßworte in der nur von ihm lesbaren Datei „/etc/shadow" ablegen. Das Auslagern der Paßworte in diese Datei geschieht mit dem Kommando „pwconv", sofern das jeweilige Unix-Derivat diese Möglichkeit vorsieht.

Der Systemverwalter hat beim Einrichten der PATH-Variablen der Benutzer darauf zu achten, daß die Systemverzeichnisse stets vor den Benutzer-Dateiverzeichnissen durchlaufen werden. Auf diese Weise wird sichergestellt, daß keine benutzereigenen Systemprogramme aktiviert werden können. Schließlich empfiehlt es sich, die HOME- und PATH-Festlegungen nach deren Definition auf „read only" zu setzen, damit sie von unprivilegierten Benutzern nicht verändert werden können.

Dateiverzeichnisse, auf die jeder Benutzer das Schreibrecht hat, etwa /tmp oder /usr/tmp, sollten in der PATH-Festlegung nicht vorkommen. Andernfalls könnte ein Eindringling in ein solches Verzeichnis ein Programm mit gleichem Namen wie das, das der Benutzer ausführen will, einstellen. Dieses Programm könnte dann unter dessen Benutzerkennung mit dessen individuell festgelegten Zugriffsrechten ablaufen und Aktionen ausführen, die einem Dritten ungewollt Zugang zu vertraulichen Informationen verschaffen.

Systemverwalterkommandos sollten darüber hinaus nur von wenigen ausgewählten und zudem besonders sicheren Arbeitsplätzen aktiviert werden können. In einigen UNIX-Derivaten besteht die Möglichkeit, eine Datei „/etc/secure/tty" einzurichten, in der die Bildschirmarbeitsplätze mit root-Berechtigung eingetragen sind.

Bei einigen UNIX-Systemen steht das Kommando „lock" zur Verfügung, mit dem ein **Bildschirm gesperrt** werden kann, ohne die Sitzung beenden zu müssen. Das „lock"-Kommando verlangt bei seiner Benutzung ein Key-Wort, das zweimal hintereinander eingegeben werden muß, danach ist die Tastatur gesperrt. Entsperrt wird der Bildschirm durch Eingabe dieses Key-Wortes.

Standardmäßig ist über das „su"-Kommando ein Einloggen mit der Systemverwalterkennung von jedem Bildschirm aus möglich. Über das „chmod"-Kommando läßt sich die Ausführungsberechtigung für das „su"-Kommando jedoch einschränken.

Schließlich ist bei der Installation eines UNIX-Systems noch zu beachten, daß bei allen Benutzerkennungen und auch bei den für Wartungszwecke vorgesehenen Kennungen die Installationspaßworte, die von der Hersteller- oder Lieferfirma vergeben wurden, durch **neue Paßworte** ersetzt werden. Nicht selten kommt es vor, daß die Kennungen root, admin, mgast und gast noch mit den sogenannten Installationspaßworten geschützt sind.

c) Erhöhung der Betriebssicherheit

Zur Erhöhung der Betriebssicherheit von UNIX-Systemen ist es erforderlich, die **Benutzerkompetenzen** auf das für die Anwendung notwendige Maß zu begrenzen und folgende Grundsätze zu beachten:

- Eine Shell-Berechtigung ist für normale Benutzer nicht erforderlich.
- Der Zugang zur Shell-Ebene ist für den Anwendungsbenutzer dadurch zu verhindern, daß in der Benutzertabelle „/etc/passwd" bereits der Aufruf der Anwendung eingetragen wird, so daß das System nach dem Login sofort in die Anwendungsprogramme verzweigen kann und der Benutzer von da an menuegesteuert geführt wird.
- Das Kommando „chown" (change owner), mit dem der Eigentümer selbst seine Datei auf einen anderen Eigentümer umsetzen kann, ist für den Anwendungsbenutzer zu sperren, da eine solche Umsetzung nur in den seltensten Fällen sinnvoll ist.
- Das Kommando „su" (become superuser) ist zwar nur unter der root-Kennung ausführbar. Durch „su" kann aber ein beliebiger Benutzer Superuser werden. Wegen der weitreichenden Kompetenzen, die ein zusätzlicher Benutzer unter dieser Kennung erreichen kann, ist dieses Kommando für den laufenden Betrieb zu sperren.

Zusätzliche Sicherheit bringt auch die Einschränkung, bestimmte Prozesse oder Benutzer, beispielsweise durch Zwischenschalten von Prüfprozeduren, nur von **bestimmten Terminals** aktiv werden zu lassen. Die Einschränkung, nur von bestimmten Bildschirmarbeitsplätzen arbeiten zu können, wird in „/etc/secure/tty" definiert.

Im UNIX gibt es außerdem eine Verschlüsselungsroutine, die mit „crypt" aufgerufen werden kann. Mit „crypt" verschlüsselte Dateien sind nur demjenigen

im Klartext zugänglich, der das Verschlüsselungspaßwort des Eigentümers kennt, der die Verschlüsselung angestoßen hat. Mit „decrypt" kann ein kryptierter Text wieder entschlüsselt werden. Auf diese Weise können Anwender auch dem Systemverwalter die Kenntnisnahme von Dateiinhalten verschließen.

Vor der Inbetriebnahme eines UNIX-Systems empfiehlt es sich, daß der Systemverwalter mit dem find-Kommando alle SUID- und SGID-Programme (Set User- bzw. Set Group-ID) ausfindig macht und die Gültigkeit von s-Bits überprüft, mit denen zusätzliche Zugriffsberechtigungen erreicht werden können. Im Zweifelsfalle ist das s-Bit zu löschen.

Bei Dateien, die mit dem „rm"-Befehl (remove) gelöscht werden, ist zu beachten, daß lediglich der sogenannte „I-node" der Datei (Identifikator der Datei, Eintrag in der Directory) gelöscht wird. Auf dem Speichermedium bleiben die Daten hingegen bis zur Wiederverwendung des Speicherplatzes gespeichert. Mit geeigneten Programmen können solche Dateien wieder lesbar und damit weiterverwendbar gemacht werden. Für die Löschung von Dateien sensiblen Inhalts sind deshalb Löschprogramme zu verwenden, die die zu löschenden Dateien physikalisch und nicht nur logisch überschreiben.

Sicherheitslücken im UNIX versucht man auch durch sog. elektronische „Wachhunde" aufzuspüren, die in die Datei „crontab" eingestellt werden, um entdeckte Sicherheitslücken sofort an den Systemverwalter zu melden, damit dieser Gegenmaßnahmen einleiten kann. Die „crontab" enthält Einträge über Prozesse, die unter einem bestimmten Benutzernamen regelmäßig ausgeführt werden.

Auch die tägliche, wöchentliche oder monatliche Sicherung kann über automatisch ablaufende Prozesse, die in die „crontab" eingestellt werden, organisiert werden.

Zur Erhöhung der Zugriffssicherheit werden nunmehr auch für UNIX-Systeme Chipkarten-Systeme angeboten, die ohne eigene Lesegeräte auskommen und somit recht wirtschaftlich arbeiten. Die Arbeitsweise eines derartigen Systems basiert auf einem Programm im Rechner, das jede ihm bekannt gemachte Chipkarte verwaltet und bei deren Benutzung einen entsprechenden Passcode generiert. Jeder Passcode hat für eine bestimmte Chipkarte nur eine begrenzte Gültigkeitsdauer. Will ein Benutzer mit dem DV-System in Verbindung treten, aktiviert er die Chipkarte mit seiner Geheimnummer und erhält dann im Display der Chipkarte den zu dieser Zeit für diese Chipkarte gültigen Passcode. Dieser Passcode wird dem DV-System mitgeteilt und dort auf Gültigkeit geprüft. Chipkarte und DV-System müssen deshalb gleich getaktet sein. Die Sicherheit dieses Verfahren wird schließlich noch dadurch erhöht, daß die Gültigkeit des Passcodes begrenzt ist, keine Passworte auf Leitungen übertragen werden und die Chipkarte auf ungültige Geheimnummerneingabe durch entsprechende Maßnahmen, etwa mit einer Sperrung, reagiert. Schließlich bieten manche Hersteller sog. Security-Versionen an.

d) Protokollierung

Auch UNIX schreibt über Systemaktivitäten Protokolldaten. Diese Daten werden in den Dateien „utmp" und „wtmp" in binärer Form gespeichert.

Der Zugriff auf diese Dateien sollte nur solchen Personen gestattet sein, die die Ordnungsmäßigkeit der Datenverarbeitung kontrollieren. In die Kontrolle sollte auch derjenige, der die root-Privilegien innehat, einbezogen werden. Leider enthalten die Protokolle keine Hinweise auf den Dateizugriff, ein Mangel, der besonders für die Kontrolle des root-Benutzers, der über einen universellen Zugriff verfügt, von Nachteil ist.

Standardmäßig werden protokolliert:
- der Benutzername (Login-Name)
- der Gerätename (z.B. Console, ttyxxx)
- die Prozeßnummer
- die Art des Eintrages
- Angaben über die Beendigung eines Prozesses
- den Ende-Status
- Angaben über die Zeit des Login und des Logoff

Aus den aufgezeichneten Informationen ist deshalb nicht ersichtlich, welche Aktivitäten ein Benutzer ablaufen ließ, das heißt mit welchen Prozessen auf welche Dateien zugegriffen wurde. Eine Ausnahme stellen lediglich die Verwendungen des su-Kommandos dar, die in der Datei „sulog" vollständig aufgezeichnet werden.

Sollten bei besonders vertraulichen Anwendungen zusätzliche Daten protokolliert werden müssen, ist das über einen User-Exit innerhalb der Anwendung selbst vorzunehmen. Die dabei entstehende Protokolldatei ist wie jede andere Datei durch die bekannten Zugriffsschutzmechanismen zu schützen, wobei besonders darauf zu achten ist, daß nur die mit der Auswertung und Kontrolle der Datei befaßten Personen zugriffsberechtigt sind.

Nach 5 erfolglosen Login-Versuchen werden solche Versuche in einer Datei protokolliert. Jeder Eintrag enthält neben dem Benutzernamen (Login-Name), die Terminal-Bezeichnung und den Zeitpunkt. Standardmäßig ist die Datei „loginlog" allerdings nicht vorhanden, sie muß vom Systemverwalter (root) eingerichtet werden. Außerdem werden alle Aktivitäten von „cron" (Steuerung der regelmäßig automatisch ablaufenden Prozesse) in einer cron-eigenen Log-Datei protokolliert.

Protokolldateien sind regelmäßig nach bestimmten vorgegebenen Kriterien (z.B. Sicherheitsverletzungen) durch eine dafür bestimmte Person zu kontrollieren. Da Protokolldateien personenbezogen sind, sollten sie nur für Zwecke der Datensicherheit verwendet und nach einem genau festgelegten Zeitraum gelöscht werden.

Trotz dieser Möglichkeiten ist der Informationsgehalt der Standard-Protokollierung eher bescheiden. Es fehlen Hinweise über Aktionen (Zugriffe, Änderungen) von bestimmten Subjekten auf bestimmte Objekte sowie über sonstige relevanten Fehlerzustände. Ansätze für eine um diese Informationen erweiterte Protokollierung gibt es in den Accounting-Mechanismen bei einigen UNIX-Derivaten (etwa SINIX-S von SNI) und im SCO UNIX (UNIX System V/386 der Santa Cruz Operations), das vom amerikanischen Department of Defense (DoD) nach den amerikanischen Sicherheitskriterien des sog. Orange Books nach C2 eingestuft wurde.

20.1.1.4 Sicherheits-UNIX

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) hat 1991 das **SINIX-S** (ein UNIX-Derivat) der Siemens-Nixdorf Informationssysteme AG zertifiziert. Dieses Betriebssystem wurde nach den nationalen IT-Sicherheitskriterien nach F1/Q2 (= „ausreichende" Sicherheit) eingestuft, wobei die Identifikation und Authentisierung, die Rechteprüfung, die Beweissicherung und Wiederaufbereitung die Funktionalitätsklasse F2 erfüllen. Für sicherheitsrelevante Anwendungen empfehle ich deshalb den Einsatz dieses Betriebssystems.

Zusätzliche Hinweise zur UNIX-Sicherheit können bei meiner Geschäftsstelle angefordert werden.

20.1.2 Integrierte Chipkartensysteme

Im 13. Tätigkeitsbericht wurde über die Chipkarte als Hilfsmittel zur sicheren Authentisierung berichtet. Die Chipkarte wird mittlerweile sogar für die Abteilungsrechner, also für Mehrplatzsysteme, angeboten. Trotz der vielfachen Verwendungsmöglichkeiten ist ihr Einsatz bislang spärlich anzutreffen.

Es gibt heute integrierte Sicherheitssysteme, die auf Chipkartenbasis arbeiten, die neben der Steuerung des Zugangs zur DV-Anlage zusätzlich den Zugang zu Gebäuden und Gebäudeteilen regeln und sich obendrein für Abrechnungszwecke aller Art (Gleitzeit, Kantine etc.) verwenden lassen.

Schließlich lassen sich über die Chipkarte im Netzbetrieb nach dem Client-Server-Prinzip die Workstations, das sind Arbeitsstationen ohne eigenen Speicher, absichern und komplizierte Kompentenzregelungen abbilden.

Neben der Datenschutzkomponente tritt die Datensicherheitskomponente immer mehr in den Vordergrund. Untersuchungen haben gezeigt, daß die meisten Informationsverluste durch Bedienungsfehler hervorgerufen werden. Gelingt es, die Chipkartentechnik auch für die Erhöhung der Datenintegrität zu nutzen, dürften ihr hohe Zuwachsraten beschieden sein.

20.1.3 Steuerung der Zugriffsberechtigung bei neuen AKDB-Verfahren

Die Anstalt für Kommunale Datenverarbeitung in Bayern (AKDB) arbeitet an einem neuen Zugriffschutzsteuerungssystem, das zukünftig in allen neuen Anwendungen integriert werden soll. Bereits in der Planungsphase wurde ich über die Eigenschaften dieses Systems unterrichtet, um eventuell notwendig werdende Änderungswünsche rechtzeitig einbringen zu können.

Das neue Zugriffschutzsteuerungsverfahren soll den bisherigen Zugriffsschutz in den AKDB-Verfahren ersetzen. Der Zugang zu allen schützenswerten Anwendungen soll künftig über diesen Modul laufen. Das neue Verfahren soll zuerst auf der HP3000 realisiert werden, später auch auf UNIX (MX-Bereich, Digital-Kienzle und HP-Vectra). Der Logon-Schutz bleibt davon unberührt.

In diesem neuen Zugriffschutzsteuerungssystem existiert eine Benutzertabelle, in der je Benutzer dessen aktuelle Zugriffsberechtigungen abgespeichert werden. Die Benutzertabelle ist verfahrensbezogen. Nach jeder Änderung wird ein Protokoll ausgedruckt, in dem der aktuelle Stand für alle Benutzer enthalten ist. Das Protokoll enthält Datum, Uhrzeit sowie eine fortlaufende Nummer und ist damit revisionsfähig. Die Ausdrucke gestatten eine lückenlose Kontrolle der Zugriffsberechtigungen. Zur leichteren Kontrolle habe ich empfohlen, je Benutzer einen Versionszähler mitzuführen.

Protokolliert werden ferner Angaben über den Verfahrensaufruf und über Veränderungen am Datenbestand. Beim Aufruf eines Verfahrens (z.B. EWO = Einwohnerwesen) erfolgt ein Eintrag in die Protokolldatei, aus dem ersichtlich ist, wer wann das Verfahren aufgerufen hat. Bei Änderungen werden der Satzschlüssel, der Veranlasser, die Funktionsart (TAC = Transaktionscode) sowie Datum und Uhrzeit festgehalten. Die Protokollierung kann wahlweise sein.

Die AKDB generiert bei der Installation die Benutzertabelle. Der Verfahrensadministrator beim Kunden legt später die Berechtigungen fest und jeder Benutzer kann sein persönliches Paßwort selbst vergeben. Wird die Benutzertabelle gelöscht, ist kein Zugriff auf das Anwenderverfahren mehr möglich. Zugriffs-

verfehlungen, etwa Eingabe eines falschen Paßworts, werden allerdings auf dieser Ebene nicht protokolliert.

Die Kontrolle der Systemverwaltertätigkeiten läuft außerhalb dieses Zugriffschutzsteuerungssystems, d.h. auf Betriebssystemebene ab.

20.1.4 Wartung und Fernwartung von DV-Systemen

Die Wartung und Fernwartung von DV-Systemen wurden bereits in früheren Tätigkeitsberichten (6. Tätigkeitsbericht Seite 82 und 7. Tätigkeitsbericht Seiten 74 und 88) aufgegriffen. Die gebotenen Sicherheitsmaßnahmen haben sich gegenüber den damaligen Aussagen nicht geändert. Durch die Dezentralisierung der Datenverarbeitung und die Verlagerung der DV-Geräte an den Arbeitsplatz hat die Fernwartung allerdings eine größere Bedeutung erhalten. Während sich die Wartung im Host-Bereich früher hauptsächlich auf die Hardware beschränkte, kommt es heute viel öfters vor, daß von außen auch auf Anwendungssoftware, die bei Externen gekauft, gemietet oder erstellt wurde, zum Zwecke der Fehlersuche und Programmpflege zugegriffen werden muß. Im Gegensatz zur reinen Hardware-Wartung kann der externe Betreuer **bei der Software-Wartung auch auf die Daten** des Kunden zugreifen, sofern die Datenbestände vorher nicht aus dem direkten Zugriff genommen wurden.

Bei der Wartung, insbesondere aber bei der Fernwartung von DV-Systemen, mit denen sensible oder einer besonderen Verschwiegenheitspflicht unterliegende personenbezogene Daten verarbeitet werden, ist deshalb stets zu prüfen, ob dadurch geschützte personenbezogene Daten **offenbart** werden. Eine Offenbarung kommt – abgesehen von der Zustimmung des Betroffenen – nur in solchen Fällen in Betracht, in denen eine Fehlerbehebung durch eigenes Personal nicht möglich ist und ein Ausfall des DV-Systems die Aufgabenerfüllung nicht nur unerheblich beeinträchtigen würde. Für eine Offenbarung muß eine ausreichende Befugnis vorliegen (siehe dazu auch die Ausführungen im Abschnitt 2.2 dieses Berichts). Die Personen, die die Programmpflege (Fernbetreuung) ausführen, sind auf die Einhaltung der Verschwiegenheitspflicht zu verpflichten. Will man eine Offenbarung trotzdem vermeiden, sind die entsprechenden Datenbestände vor der Wartung aus dem direkten Zugriff zu entfernen, was manchmal zur Folge haben kann, daß bestimmte Fehler nicht mehr lokalisiert werden können.

Bei der Wartung und Fernwartung durch Externe sind eine Reihe von Sicherheitsmaßnahmen zu beachten, die letztendlich darauf abzielen, daß alle Aktivitäten unter ständiger Kontrolle eines sachkundigen Mitarbeiters der speichernden Stelle stehen und manipulationssicher protokolliert wird, auf welche Daten zugegriffen wurde. Dabei ist es im allgemeinen technisch unerheblich, ob die Wartung lokal oder über Leitung durchgeführt wird.

Bei der Wartung und Fernbetreuung ist schließlich auf die Einhaltung folgender Sicherheitsmaßnahmen zu achten:

- Beim Verbindungsaufbau muß sichergestellt sein, daß die DV-Anlage auch mit der Fernwartungszentrale verbunden wird. Die Verbindung wird **ausschließlich vom Anwender** aufgebaut.
- Die Wartungstechniker müssen sich strengen **Zugangskontrollprüfungen** unterziehen und dürfen nur im Rahmen ihrer Wartungsprivilegien tätig werden.
- Ein sachkundiger Mitarbeiter der datenverarbeitenden Stelle muß alle Wartungsaktivitäten erkennen und überwachen sowie den Wartungsvorgang jederzeit unterbrechen können.
- Eine Datenübertragung aus dem DV-System des Anwenders an die Fernwartungszentrale ist nur bei gleichzeitiger Protokollierung aller übertragenen Daten zuzulassen. Ein sachkundiger Mitarbeiter der datenverarbeitenden Stelle muß am Bildschirm mitverfolgen können, welche Daten der Wartungstechniker auf seinem Bildschirm angezeigt bekommt. Der Hersteller hat dafür Sorge zu tragen, daß dem Anwender DV-gestützte Hilfsmittel zur Verfügung gestellt werden, mit denen auch eine nachträgliche Kontrolle der protokollierten Daten möglich ist.
- Die Fernwartungszentrale darf sich nur eines Endgerätes mit Terminaleigenschaft bedienen, damit **keine maschinelle Speicherung** der übertragenen Bildschirminhalte in der Wartungszentrale möglich ist. Die Benutzung der Hardcopy-Funktion ist zu untersagen.
- Bevor ein Datenträger mit Anwenderdaten zu Wartungszwecken oder zur Fehleranalyse den DV-Bereich verläßt, ist die Genehmigung einer von der datenverarbeitenden Stelle dafür autorisierten Person einzuholen. Auf einem Begleitschein sind die Art der Daten und des Datenträgers sowie Vorgaben über die Weiterbehandlung dieser Daten zu vermerken.
- Bei der lokalen Wartung ist sicherzustellen, daß keine Datenträger den DV-Bereich des Anwenders unkontrolliert verlassen.
- Werden Test- und Service-Programme des Herstellers auf der DV-Anlage gespeichert, sind diese unter der Wartungskennung abzuspeichern.
- Der Betreiber der DV-Anlage muß alle ablauffähigen Programme durch geeignete Zugriffsschutzmechanismen schützen, damit nicht unkontrolliert auf Dateien zugegriffen werden kann.
- Ist für Wartungszwecke ein Zugriff auf Anwenderdaten erforderlich, ist zu prüfen, ob sensible personenbezogene Daten vorher aus dem direkten Zugriff zu entfernen sind.

- Die Fernwartung von Anwendungsprogrammen ist unter einer Kennung vorzunehmen, die keine Systemverwalterprivilegien einschließt, so daß beispielsweise eine systematische Abfrage und Durchsuche von Anwenderdaten über Systemdienstprogramme ausgeschlossen ist.
- Solange Anwenderdaten auf der Anlage im direkten Zugriff stehen, ist die Systemebene für die Wartung der Anwendungssoftware generell zu sperren.
- Im Rahmen der Fernwartung ist das Einspielen von Änderungen in die Software (Betriebssystem, systemnahe Software und Anwendungssoftware) nicht zuzulassen. Die Änderungen sind ausschließlich vor Ort entweder durch einen Mitarbeiter der datenverarbeitenden Stelle selbst oder mit dessen Einwilligung und unter dessen Kontrolle durch den Software-Hersteller in die entsprechende Software zu übernehmen.
- Für den Fall, daß in einem Wartungsvorgang ein paßwortgeschützter Zugriff auf Dateien mit sensiblen Anwenderdaten oder direkt auf die Paßwortdatei notwendig ist, sind nach Abschluß der Wartungsarbeiten alle der Wartung offenbarten Paßworte unverzüglich zu ändern.
- Alle Aktivitäten eines Wartungsvorgangs, die in einer Protokolldatei festgehalten werden, sind zu überprüfen und mindestens ein Jahr aufzubewahren. Die Verpflichtung des bei der datenverarbeitenden Stelle für das DV-System Verantwortlichen, den Wartungsvorgang am Bildschirm zu verfolgen und gegebenenfalls zu unterbrechen, bleibt davon unberührt.
- Im Wartungsvertrag sind klare Regelungen hinsichtlich der Abgrenzung der Kompetenzen und Pflichten zwischen Wartungspersonal und datenverarbeitender Stelle zu treffen. Art und Umfang der Wartung (Hard- und Software) sind schriftlich festzulegen.
- Das Wartungspersonal ist auf das Datengeheimnis zu verpflichten (gegebenenfalls auch auf die entsprechenden Verschwiegenheitsvorschriften, denen die Anwenderdaten unterliegen).
- Eine Weitergabe von Anwenderdaten, die dem Wartungspersonal übergeben oder bei der Fernwartung übertragen wurden, an Dritte ist vertraglich auszuschließen. Diese Daten sind ausschließlich für Zwecke der Programmpflege zu verwenden und nach Abschluß der Arbeiten bzw. nach der Fehlerbehebung unverzüglich zu löschen oder dem Anwender zurückzugeben.
- Beim Transport von Datenträgern sind der Transportweg und die am Transport beteiligten Personen festzulegen. Die Vollständigkeit der Datenträger ist zu prüfen. Beim Transport sind Begleitpapiere zu verwenden.
- Die Systemverantwortlichen bei der datenverarbeitenden Stelle sind bezüglich der Möglichkeiten der Fernwartung ausreichend zu schulen. Die Einhaltung der getroffenen Sicherheitsmaßnahmen ist regelmäßig zu überprüfen.

20.2 Prüfungstätigkeit

20.2.1 Kontrolle und Beratung

Die Kontrolle der von den öffentlichen Stellen getroffenen technisch-organisatorischen Datensicherheitsmaßnahmen war wieder ein Schwerpunkt meiner Tätigkeit.

Folgende Dienststellen habe ich gemäß Art. 15 BayDSG (teilweise in Verbindung mit § 9 BDSG und Anlage) kontrolliert:

- Amtsgericht Garmisch-Partenkirchen
- Betriebskrankenkasse AUDI, Ingolstadt
- Büro eines Gerichtsvollziehers in München
- Finanzamt Fürstenfeldbruck
- Finanzamt Hof
- Gemeindeverwaltung Gauting
- Innungskrankenkasse Hof
- Landratsamt Coburg
- Landratsamt Kitzingen
- Staatliche Lotterieverwaltung, München
- Staatliches Gesundheitsamt, Erlangen
- Staatliches Schulamt, Rosenheim
- Stadt und Verwaltungsgemeinschaft Schrobenhausen
- Stadtverwaltung Ansbach
- Stadtverwaltung Würzburg
- Stadtverwaltung Wunsiedel
- Zweckverbandskrankenhaus Ansbach.

Außerdem habe ich in den Rechenzentren der Stadtverwaltungen München und Nürnberg spezielle Prüfungen der **Benutzerverwaltung** und der **Abschottung** der einzelnen Benutzer und Benutzergruppen gegeneinander durchgeführt.

Wie in den Vorjahren habe ich großen Wert auf die datenschutzgerechte **Entsorgung** von Datenträgern mit personenbezogenen Daten gelegt. Hier galt mein besonderes Interesse der datenschutzgerechten Entsorgung von Papierunterlagen, weil deren Inhalt ohne Einsatz sonstiger technischer Mittel sofort auswertbar ist. Ich habe die Entsorgung bei 16 Dienststellen geprüft. Im Ergebnis kann ich festhalten, daß sich die Sensibilität der Dienststellen bei der datenschutzgerechten Entsorgung von Datenträgern im Vergleich zu den Vorjahren erheblich erhöht hat. So werden die Bediensteten meist durch **Dienstanweisung** verpflichtet, die gebotenen Entsorgungsmöglichkeiten einzuhalten, und auf die Folgen bei einem sorglosen Umgang bei der Entsorgung von Datenträgern hingewiesen. Viele Behörden haben mittlerweile Aktenvernichter nach DIN 32757 (Entsorgungsstufe 3) beschafft. Hervorzuheben ist in diesem Zusammenhang

der Bayer. Bauernverband, der für seine Bezirks- und Kreisverbände in einer Einmal-Aktion etwa 150 Aktenvernichter beschaffte. Alles in allem hat meine intensive Prüftätigkeit auf diesem Gebiet dazu beigetragen, daß mir im Berichtszeitraum keine gravierenden Fälle von Datenschutzverletzungen bekannt geworden sind.

Zahlreiche Dienststellen habe ich in Fragen des Datenschutzes und der Datensicherheit **beraten**. Etwa 30 Dienststellen haben im Vorfeld von Um- und Neubauten ihrer Behördengebäude oder ihrer DV-Bereiche verbindliche Aussagen über notwendige Sicherheitsmaßnahmen erbeten. Sie betrafen in erster Linie Maßnahmen zum Zutrittsschutz, zur Außenhaut- und Innenraumsicherung von DV-Bereichen, zur Entsorgung von Datenträgern sowie Maßnahmen zur Datensicherheit beim Einsatz von PC und beim Aufbau von hausinternen Netzen (LAN).

In einigen Fällen habe ich **Nachkontrollen** durchgeführt. Sie haben gezeigt, daß meine Prüfungsbemerkungen im großen und ganzen befolgt, und die bei der Beratung geforderten Maßnahmen zur Datensicherheit umgesetzt worden sind. Allerdings werden mir immer häufiger **fehlende Haushaltsmittel** als Grund genannt, wenn als notwendig angesehene Datenschutz- und Datensicherheitsmaßnahmen zumindest zeitlich verzögert werden. Finanzielle Engpässe dürfen aber nicht dazu führen, daß gar keine Sicherheitsmaßnahmen ergriffen werden.

20.2.2 Ergebnisse der Kontrolltätigkeit

In der gesamten öffentlichen Verwaltung war das Bemühen festzustellen, Maßnahmen zum Datenschutz und zur Datensicherheit zu ergreifen. Trotzdem gab es eine Reihe von Mängeln, die entweder nicht gesehen oder deren Behebung aus finanziellen Gründen zurückgestellt wurden. Anhand von allgemein interessierenden Beispielen werden einige Mängel näher erläutert.

Aufbewahrung von Sicherungdatenträgern

Manche Dienststellen verfahren recht großzügig bei der Aufbewahrung der Sicherungsdatenträger, obwohl bei einer Zerstörung der DV-Anlage, etwa durch Brand, nur diese Datenträger den Datenbestand bereitstellen und die Fortführung der Datenverarbeitung gewährleisten können. So werden die Sicherungsdatenträger teilweise in Behältnissen aufbewahrt, die nicht der Güteklasse nach VDMA 24991 entsprechen, also keinen ausreichenden Schutz bieten. Solche „Tresore" gewährleisten lediglich einen Zugriffs-, aber keinen ausreichenden Feuerschutz. Es wird auch häufig übersehen, daß die Behältnisse für die Sicherungsdatenträger nicht im Rechnerraum aufgestellt sein sollten, damit im Schadensfall nicht Daten **und** Rechner verloren gehen.

Ich habe die Dienststellen und die Aufsichtsbehörden in den Prüfungsberichten aufgefordert, für Sicherungsdatenträger Data-Safes der Güteklasse **S 120 DIS** zu beschaffen, die einer Beflammungszeit von 120 Minuten standhalten und auch für die Aufbewahrung von Disketten, die empfindlicher als Magnetbänder sind, geeignet sind.

Problematisch ist in vielen Fällen die Aufbewahrung der Sicherungsdatenträger dort, wo Personal Computer (PC) als stand-alone-Geräte eingesetzt werden. Häufig haben die Dienststellen keine oder allenfalls solche Sicherungsschränke beschafft, die für die Aufbewahrung von Disketten nicht geeignet sind. Nicht selten werden Datensicherungen von den Sachbearbeitern nach eigenem Gutdünken durchgeführt, die Sicherungsdisketten offen oder im Schreibtisch verwahrt, weil die Mitarbeiter zu wenig auf mögliche Gefahren aufmerksam gemacht wurden und entsprechende Dienstanweisungen fehlen. Abgesehen davon, daß im Schadensfall zumindest eine umfangreiche Datenneuerfassung notwendig wäre, können mangelhaft geschützte Sicherungsdisketten auch von Unbefugten unzulässigerweise und vor allem unbemerkt genutzt werden.

Besonders bei der Datenverarbeitung mit Einplatz-PC habe ich den Erlaß einer entsprechenden **Dienstanweisung** gefordert, in der die Datensicherung und die Aufbewahrung der Sicherungsdatenträger sowie der Standort eines geeigneten Data-Safes geregelt sind.

Benutzerverwaltung, Paßwortvergabe und -änderung

Die Prüfungen der Benutzerverwaltung in Mehrzweckrechenzentren zeigten unterschiedliche Ergebnisse. Für manche Betreiber eines solchen Rechenzentrums ist wegen der unterschiedlichen Zuständigkeit für die Betreuung der Dialogverfahren oft nicht nachzuvollziehen, welche Benutzer wann welche Zugriffsberechtigungen hatten. Die Benutzerverwaltung ist entweder zentral oder bei den Fachdienststellen durchzuführen, wobei darauf zu achten ist, daß eine einheitliche Benutzeroberfläche hergestellt wird. Es gibt aber auch Betreiber, die ein System entwickelt haben, das einem Außenstehenden einen genauen Überblick verschafft, wer seit wann über welche Zugriffsberechtigungen verfügt. Die Historie wird allerdings meist nur auf Papier vorgehalten; hier ist die Revisionsfähigkeit (Nachweis der lückenlosen Zugriffsberechtigungen) zu verbessern.

Bei der Überprüfung des **Zugriffsschutzes** auf Dateien, in denen personenbezogene Daten gespeichert werden, habe ich festgestellt, daß das **persönliche Paßwort** oftmals immer noch von einem Systemverwalter oder einem Anwendungskoordinator vergeben und geändert wird, weil entweder Benutzergruppen eingerichtet wurden oder das Programmsystem eine

Paßwortänderung durch den Benutzer überhaupt nicht vorsieht. Es gibt allerdings auch Fälle, wo es die eingesetzte Software dem Benutzer gestatten würde, sein Paßwort selbst zu vergeben und zu ändern, wovon aber nicht Gebrauch gemacht wird. Eine derartige Praxis hat zur Folge, daß die Paßworte – wenn überhaupt – nur in großen Zeitabständen geändert werden, weil die Systemverwaltung durch andere Aufgaben ausgelastet und die Paßwortänderung meist mit einem nicht unerheblichen Arbeitsaufwand verbunden ist. Auch Regelungen darüber, was bei einer Paßwortwahl zu beachten ist, sind nicht überall getroffen und festgeschrieben worden.

Diese Feststellungen haben mich veranlaßt, meine bereits im 12. Tätigkeitsbericht aufgestellten Grundsätze zur Paßwortvergabe und -änderung zu präzisieren.

Bei der Vergabe von Paßworten sind folgende Sicherheitsgrundsätze zu beachten:

- Alle Benutzerkennungen sind mit einem Paßwort zu schützen.
- Für besonders wichtige Funktionen (evtl. Systemverwalter) sollte ein Zusatzpaßwort („Vier-Augen-Prinzip") verwendet werden.
- Paßworte dürfen nur dem Benutzer bekannt sein und müssen es auch bleiben. Er muß sich sein Paßwort selbst geben und jederzeit selbst ändern können.
- Als Mindestlänge von Paßwörten sind 6 Stellen vorzusehen.
- Es ist der gesamte verfügbare Zeichenvorrat, auch numerische und Sonderzeichen, auszuschöpfen.
- Es dürfen keine Zeichen mehrmals hintereinander verwendet werden. Dasselbe gilt auch für nebeneinander liegende Tasten, wie „1 2 3 4 5".
- Das Paßwort darf keinen Bezug auf den Paßwortinhaber oder seine Umgebung haben (Name, Vorname, Freund(in), Name der Kinder, Tel.-Nr.).
- Trivialpaßworte sind zu vermeiden (Asterix, Obelix usw.). Sie sollten möglichst vom DV-System über eine sogenannte Stopliste automatisch abgewiesen werden.
- Das Paßwort muß einwegverschlüsselt abgespeichert werden.
- Paßworte dürfen nicht auf Funktionstasten gelegt werden.

Bei der Verwendung von Paßworten ist zu beachten:
- Paßwortwechsel
  - häufig und in (un)regelmäßigen Abständen (etwa alle 3 Monate) möglichst maschinell erzwungen,
  - nach Bekanntwerden,
  - im Anschluß an Wartungsarbeiten,
  - nach Vorführungen.
- Der Benutzer hat sein Paßwort selbst zu ändern.
- Beim Paßwortwechsel sollte eine Paßworthistorie durchlaufen werden, damit bereits früher verwendete Paßworte abgewiesen werden.
- Zettelpaßworte sind ebenso zu verbieten wie das Anbringen des Paßwortes an Bildschirmen, unter Schreibunterlagen u.ä..
- Es muß festgelegt werden, was zu tun ist, wenn ein Benutzer sein Paßwort vergessen hat.
- Ein vom Systemverwalter vergebenes Paßwort (Transportpaßwort) sollte sich nur zur Erstanmeldung verwenden lassen und der erste Dialogschritt bei dieser Anmeldung muß zur „Paßwortänderung" führen.
- Bei Ausscheiden eines Mitarbeiters darf dessen Paßwort nicht an den neuen Benutzer weitergegeben werden.
- Das Installationspaßwort (z.B. IBM, Siemens) darf nicht als persönliches Paßwort weiterverwendet werden.

Soweit das eingesetzte DV-System einen Paßwortwechsel des Benutzers nicht zuläßt, rate ich dringend dazu, eine Zusatzsoftware zu implementieren, die diese Sicherheitsvorgaben erfüllt.

Pilotprojekt „Gesundheitsamt"

Ende November 1991 wurde das Pilotprojekt „Datenbankanwendungen für die Staatlichen Gesundheitsämter in Bayern" beim Staatl. Gesundheitsamt Erlangen gestartet. Dieses Verfahren soll in den nächsten Jahren auch bei anderen Gesundheitsämtern in Bayern zum Einsatz kommen.

Da meine Geschäftsstelle seit Beginn der Planungsphase dieses Projekt technisch begleitete, konnten bereits vor dem Echteinsatz die technisch-organisatorischen Belange des Datenschutzes bei diesem Verfahren berücksichtigt werden, so daß bei der durchgeführten Prüfung im wesentlichen nur noch kleinere organisatorische Mängel (Revisionsfähigkeit der Datenverarbeitung, Vorgaben für die Paßwortgestaltung, Erstellung eines Notfall-Konzeptes) festzustellen waren.

20.2.3 Kontrolle von Personal Computern

Bei meinen Kontrollen habe ich folgende Mängel festgestellt:

- Neben technischen Störungen sind **Fehlbedienungen** infolge unzureichender Ausbildung sowie mangelndes Sicherheitsbewußtsein der Anwender häufige Ursache für Datenverluste
- Die in der Groß-EDV gebräuchliche **Sicherung der Anwenderdaten** wird selten regelmäßig durchgeführt, was bei Störungen dann zwangsläufig zu Datenverlusten führen kann.
- Die Führung brauchbarer Programmdokumentationen (z. B. Benutzerhandbuch) wird vernachlässigt.

Ich habe folgende Sicherheitsmaßnahmen gefordert:

- Zur Überwachung der ordnungsgemäßen Anwendung der Datenverarbeitungsprogramme auf den Personal Computern ist eine **Verpflichtung der Anwender** auf die Einhaltung von Sicherheitsmaßnahmen und die Durchführung von internen Kontrollen unerläßlich.
- Vor einer Kontrolle muß sich die damit beauftragte Person mit den vorhandenen **Betriebssystemen** und den **Utilities**, den Sicherheitseinrichtungen (Zugriffsschutzsoft- und -hardware, Protokollaufzeichnungen, Prüfsummenprogramm, Verschlüsselungssoftware) und entsprechenden Prüfungswerkzeugen, wie Virensuchprogrammen und Software-Tools für den DOS-Bereich, vertraut machen.
- Die Kontrolle sollte unangemeldet und in unregelmäßigen Abständen stattfinden, um zu verhindern, daß eventuell unerlaubt eingesetzte Software (z.B. Raubkopien, Spiele) vor der Prüfung entfernt und nachher wieder eingespielt wird.
- Die bei der Kontrolle vorgefundenen personenbezogenen Dateien sind mit den vorliegenden Dateimeldungen zu vergleichen.

Für die Durchführung der Prüfung von PC wurde ein **Fragenkatalog** „Prüfansätze des PC-Einsatzes" entwickelt, der bei meiner Geschäftsstelle angefordert werden kann.

20.2.4 Gefährdung durch Computerviren

Großes Aufsehen erregte Anfang des Jahres 1992 die Meldung, der sogenannte Michelangelo-Virus werde die DOS-Computersysteme lahmlegen. Durch gezielte Vorsorgemaßnahmen hielt sich der Schaden aber in Grenzen. Ähnliche Gefahren können allerdings jederzeit wieder auftreten, so daß es sich empfiehlt, rechtzeitig ein wirksames Kontrollsystem zu entwickeln und einzusetzen. Nach wie vor ist die **nichtlizenzierte** Privatsoftware eine der Hauptquellen für Computerviren.

Beim Einsatz von Hard- und Software, die nicht der unbeschränkten rechtlichen und tatsächlichen Verfügungsgewalt des Dienstherrn unterliegen, ist das Risiko einer Gefährdung der ordnungsgemäßen Datenverarbeitung durch Computerviren besonders groß. Aus diesem Grund müssen die Verwendung nicht dienstlich beschaffter (privater) Software zur Erledigung dienstlicher Aufgaben und der Einsatz privater Hardware im öffentlichen Bereich auf Ausnahmen beschränkt bleiben. Private Rechner dürfen nicht an behördliche Netze angeschlossen werden, will man Sicherheitsrisiken vermeiden. Eine Umfrage bei den Ressorts brachte u.a. folgende Ergebnisse:

- **Richter** bedienen sich zunehmend privater Hard- und Software. Im Blick auf die richterliche Unabhängigkeit sind sie zur Vermeidung von Datenverfälschungen und -verlusten für die Einhaltung der gebotenenen Sicherheitsmaßnahmen eigenverantwortlich.
- Im Bereich der **Staatsforstverwaltung** wird bei den Revierleitern zur Betreuung des Privatwaldes die Verwendung privater Hardware derzeit noch geduldet, solange dienstliche Geräte noch nicht beschafft worden sind.
- In der **Steuerverwaltung** ist der Einsatz privater Hard- und Software in den Bereichen Geschäftsstelle, Betriebsprüfung, Steuerfahndung und Rechtsbehelfsstelle nur solange gestattet, bis dienstliche Hard- oder Software zur Verfügung steht. In anderen Bereichen ist ihre Nutzung nicht erlaubt. Außerdem sind für diese Ausnahmefälle Datensicherheitsmaßnahmen angeordnet, deren Nichteinhaltung neben dienstrechtlichen Folgen auch ein Verbot der Nutzung privater Hard- und Software nach sich zieht.
- Im **Schulbereich** dürfen Lehrer personenbezogene Daten ihrer Schüler auf privaten Rechnern speichern (z.B. Notenbuch).

Für die Beachtung der technischen und organisatorischen Datenschutz- und Datensicherheitsmaßnahmen insbesondere im häuslichen Bereich, die Sicherung der Datenbestände und die Löschung der dienstlichen Informationen nach Aufgabenerledigung ist der Benutzer selbst verantwortlich. Er muß für Verfehlungen selbst gerade stehen. Der Dienstherr ist gehalten, den Einsatz privater Hard- und Software durch **Dienstanweisung** eindeutig zu regeln. Jeder Dienststellenleiter muß von einer beabsichtigten Verwendung privater Hard- und Software vom Mitarbeiter rechtzeitig unterrichtet werden.

20.3 Technische Einzelprobleme

20.3.1 Maßnahmen zur Netzsicherheit

Die Anstalt für Kommunale Datenverarbeitung in Bayern (AKDB) bietet den angeschlossenen Landratsämtern und kreisfreien Städten einen Direktanschluß an das Ausländerzentralregister in Köln an. Das Rechenzentrum der AKDB ist mit einer Datex-P-Festverbindung mit dem sog. AZR-Dialogverfahren verbunden. Die Ausländerbehörden der Landratsämter und kreisfreien Städte benutzen für ihre Anfragen aus Kostengründen jedoch von ihrem Rechner zum AKDB-Rechner eine Wählverbindung. Damit sichergestellt wird, daß ausschließlich Berechtigte an das AZR-Dialogverfahren weitergereicht werden, hat die AKDB die Wählleitungsanschlüsse durch das Netzsicherheitssystem NC-PASS abgesichert.

NC-PASS, das mit Chipkarte und Paßwort (sog. „Zwei-Faktor-Authentisierung") und wegen des Ab-

hörrisikos mit sog. Einmal-Paßworten arbeitet, stellt sicher, daß nur Berechtigte Zugang zum AZR-Dialogverfahren erhalten. Es erfüllt die Anforderungen zum Schutz gegen unberechtigte Benutzung von Wählverbindungen in vollem Umfang.

NC-PASS bietet auch die Möglichkeit, den Zugang zum Netzwerk durch Prüfung der Terminal-ID zu kontrollieren und Sicherheitsverstöße aufzuzeichnen. Für die Auswertung der Protokolldateien gibt es Auswertehilfen, die im Online-Betrieb einsetzbar sind und die Selektion nach beliebig vorzugebenden Kriterien gestatten.

20.3.2 Benutzerservice

Angesichts der Zunahme eingesetzter Personal Computer (PC) in den Behörden und der dadurch wachsenden Zahl von Anwendern empfiehlt sich die Schaffung eines zentralen Benutzerservices zur Gewährleistung des reibungslosen Einsatzes und der ordnungsgemäßen Nutzung dieser PC bei den einzelnen Verwaltungseinheiten. Die wesentliche Aufgabe des Benutzerservices liegt in der Förderung, Unterstützung und zentralen Steuerung der individuellen Datenverarbeitung (IDV). Der Benutzerservice sollte sowohl die zentrale Beschaffungsstelle für die eingesetzte Hard- und Software als auch die Koordinierungsstelle für den Einsatz der Personal Computer mit Kommunikationschnittstellen zu allen anderen Bereichen der Behörde (z.B. Rechenzentrum) sein.

Ein Benutzerservice hat u.a. folgende **Aufgaben**:
- Erstellen eines Gesamtkonzepts für den Einsatz von Personal Computern mit Konfigurationsplan und Festlegung der einzusetzenden Hard- und Software (nach den Vorgaben der Behördenleitung)
- Planung von Netzwerken
- Durchführung und Auswertung von Sicherheitsanalysen
- Ausarbeitung von Datenschutzrichtlinien, Benutzeranweisungen und Datensicherheitskonzepten (in Zusammenarbeit mit dem Datenschutzbeauftragten)
- Regelungen für die Verwendung privater PC und privater Software (i.d.R. sollte der Einsatz privater Hard- und Software verboten sein)
- Regelungen zur Datensicherung
- Festlegung der Sanktionen bei Verletzung der Datensicherheitsmaßnahmen (in Benehmen mit der Behördenleitung)
- Erfassung der bereits vorhandenen Personal Computer, ihrer Standorte, Hard- und Softwareausstattung, Benutzer, vorhandenen Datenbestände und ihrer Nutzungszwecke (eingesetzte Verfahren)
- Zentrale Neubeschaffung der benötigten Hard- (Rechner, Speichermedien, Peripheriegeräte) und Software (Betriebssysteme, Anwendungsprogramme, Zusatzsoftware) unter Berücksichtigung der gebotenen Sicherheitsaspekte
- Installation des Betriebssystems und Anpassung der Software
- Zentrale Systempflege und Systemkontrolle
- Auswahl, Installation und Betreuung benötigter Zusatzhard- und -software für die Zugriffssicherung und Protokollierung
- Einrichten und Ändern der Benutzerprofile (unter besonderer Beachtung der Revisionsfähigkeit) einschließlich der jeweiligen Zugriffsberechtigungen
- Zuordnung der benötigten Ressourcen
- Schulung und Sensibilisierung der Benutzer (verfahrensbezogen und datenschutzrechlich)
- Verfahrens- und Benutzerbetreuung
- Einrichtung einer „Hotline" für die Annahme anfallender Probleme
- Durchführung der Hard- und Softwarewartung bzw. Abschließen entsprechender Wartungsverträge
- Evtl. Durchführung der regelmäßigen Datensicherung, falls von der Server-Technik Gebrauch gemacht wird
- Kontrolle der Datenverarbeitung auf den Personal Computern
- Auswertung der Log-Protokolle (z.B. hinsichtlich Zugriffsverletzungen)
- Evtl. Anwendungsprogrammentwicklung und -pflege
- Mitwirkung beim Verfahrenstest und -freigabe für neuentwickelte bzw. geänderte Programme und Anwendungen
- Gewährleistung entsprechender Verfahrensdokumentationen
- Führen der Hardware-, Software- und User-Kataster.

Die aufgrund dieser Tätigkeiten erstellten Unterlagen müssen immer auf dem neuesten Stand gehalten und zu Kontrollzwecken dem internen Datenschutzbeauftragten bzw. der Aufsichtsbehörde vorgelegt werden.

20.3.3 Datenverarbeitung mit einem Laptop

Die Nutzungsmöglichkeiten von tragbaren Rechnern, sog. Laptops, nehmen ständig zu. Die gebotenen Sicherheitsmaßnahmen sind dieselben, wie sie bei ortsgebundenen Rechnern gefordert werden. Allerdings ist für die Überprüfung der Einhaltung der Sicherheitsmaßnahmen ein anderes Konzept erforderlich.

Sicherungsmaßnahmen:
- Bei der Verarbeitung personenbezogener Daten ist darauf zu achten, daß Unbefugte keinen Zugriff auf gespeicherte Daten und Programme erhalten können. Das ist im DOS-Betriebssystem nur mit dem Einsatz einer **Sicherheitssoftware** garantiert.
- Bei Verwendung eines Laptops muß diese Sicherheitssoftware zusätzlich über eine **Verschlüsselungskomponente** verfügen, damit bei einer möglichen Entwendung des Gerätes personenbezogene Daten nicht im Klartext in unbefugte Hände fallen

können. Sind die Daten verschlüsselt, gibt es für den nicht autorisierten Benutzer keine Möglichkeit, die verschlüsselten Daten in ihre Ursprungsform zurückzuverwandeln.

Es gibt eine Reihe von Sicherheitsprodukten, die diese Forderungen erfüllen. Auf diese Weise ist schließlich sichergestellt, daß auch im häuslichen Bereich kein Unbefugter Zugriff zu den gespeicherten Daten erhält.

Darüber hinaus ist noch folgendes zu beachten:
- Gegen Datenverluste durch Bedienungs- oder Hardwarefehler sind **regelmäßige Sicherungen** durchzuführen.
- Auf dem Laptop dürfen genauso wie auf einem anderen dienstlichen Computer **keine privaten Daten und Programme** gespeichert werden.
- Zum Schutz gegen **Computerviren** sollte jede Diskette, von der Programme und Daten in den Computer übernommen werden, zuvor mit einer geeigneten Software auf das Vorhandensein von Computerviren untersucht werden.

20.3.4 Abhören des Sprechfunkverkehrs

Während es bisher nur Bastlern möglich war, das Frequenzband ihres Rundfunkgerätes so zu strecken, daß sie verbotenerweise den Funkverkehr von Polizei, Feuerwehr, Rettungsdiensten und ähnlichen Einrichtungen abhören konnten, ist es nach der Aufhebung der Beschränkung der zulässigen Empfangsbereiche für Rundfunkempfänger durch den Bundespostminister nunmehr allgemein zulässig, Rundfunkempfänger zu betreiben, die **technisch** das Abhören des Funkverkehrs ermöglichen, auch wenn dies gesetzlich nach wie vor **verboten und unter Strafe** gestellt ist. Entsprechende Geräte, die den Empfang des Behördenfunkverkehrs gestatten, sind im Handel erhältlich. Dies stellt eine erhebliche **Bedrohung des Fernmeldegeheimnisses** und des Persönlichkeitsschutzes dar. Durch Abhören des Polizeifunkes können die Personalien von Unfallbeteiligten oder von kontrollierten Personen interessierten Dritten bekannt werden. Erteilt die Einsatzzentrale per Funk einer Polizeistreife den Auftrag, zu einer Familienstreitigkeit, zu einem „Tatort" oder einem sonstigen interessanten Einsatzort zu fahren, so werden künftig die betroffenen Bürger noch öfter als bisher damit rechnen müssen, daß der „Fall" in der Zeitung steht. Abschleppunternehmen, Käufer von Unfallfahrzeugen und Neuwagenhändler können dem Polizeifunk die Namen und Anschriften von Unfallbeteiligten entnehmen. Durch Mithören der Funkgespräche des Rettungsdienstes können Gesundheitsdaten von Verunglückten und Kranken bekannt werden.

Nachdem eine Wiedereinführung der früher geltenden Beschränkungen der zulässigen Empfangsbereiche nach EG-Recht nicht zulässig ist, müssen aus der zusätzlichen Gefährdung der Persönlichkeitsrechte **Konsequenzen** gezogen werden: Ich habe die zuständigen Fachressorts auf diese Gefährdung aufmerksam gemacht und gebeten, ein Konzept zu entwickeln, das die Einhaltung des Fernmeldegeheimnisses so weit wie möglich sicherstellt. Ob dabei der gesamte Funkverkehr zu **verschlüsseln** oder durch andere Maßnahmen die Geheimhaltung von personenbezogenen Daten zu gewährleisten ist, wird nicht zuletzt auch von den hierfür aufzuwendenden Kosten abhängen.

Die Polizei verwendet heute in besonderen speziell damit ausgestatteten Fahrzeugen sog. **Sprachverschleierungsgeräte**, bei deren Benutzung Außenstehende den Funkverkehr nicht interpretieren können. Dieses Verfahren bietet gegen den Abhörer eine ausreichend hohe Sicherheit. Da mittelfristig jedoch geplant ist, den Funkverkehr in Digital-Netzen abzuwickeln, ist eine Ausstattung aller Fahrzeuge mit diesen **Analog-Verschlüsselungsgeräten** aus Kostengründen derzeit nicht vertretbar. Der Einsatz sicherer, heute verfügbarer Digital-Verschlüsselungsgeräte ist wegen der notwendigen Digital-Analog-Um- und Rückwandlung ebenfalls nicht vertretbar, weil das Analognetz spätestens bis 1998 durch Digitalnetze ersetzt wird. Auch das Ausweichen auf andere Kanäle ist angesichts moderner Rundfunkgeräte und des Defizits an freien Kanälen keine Lösung.

Als Sofortmaßnahme sollten Funkgespräche mit sensiblem Inhalt noch konsequenter als bisher **auf das Notwendigste beschränkt** werden. So sollten beispielsweise bei einer Polizeikontrolle Computerabfragen zwischen der Streifenwagenbesatzung und der Einsatzzentrale in besonders sensiblen Fällen – soweit möglich – über das herkömmliche Telefon abgewickelt werden. Die von einigen Datenschutzbeauftragten erhobene Forderung, innerhalb des Sprechfunkverkehrs vorerst gar keine personenbezogenen Daten mehr auszutauschen, halte ich jedoch für unrealistisch, da durch ein derartiges Funkverbot die polizeiliche Arbeit in unvertretbarer Weise behindert würde. Bei Fahrzeugkontrollen im fließenden Verkehr, bei der Überprüfung von Personen auf Autobahnrastplätzen und bei Personenkontrollen an Kontrollstellen wäre die schnelle Computerabfrage an Ort und Stelle nicht möglich, so daß auf die Bürger beträchtliche Unannehmlichkeiten zukämen.

20.3.5 Persönlichkeitsschutz beim Einsatz digitaler Telekommunikationsanlagen

Im 13. Tätigkeitsbericht habe ich bereits darauf hingewiesen, daß Interessenten eine **Orientierungshilfe** für Sicherheitsmaßnahmen beim Betrieb von digitalen Telekommunikationsanlagen bei meiner Geschäftsstelle anfordern können.

Probleme bereiten manchen Anwendern die Leistungsmerkmale „Aufschalten" und „Direktansprechen".

Hat eine Nebenstelle die Berechtigung zum Aufschalten auf bestehende Gespräche, so ertönt beim Aufschalten zu Beginn **dreimal** der nicht zu überhörende **Aufmerksamkeitston**, den sowohl der Rufende als auch der Angerufene hören können. Außerdem leuchtet bei beiden Teilnehmern eine **optische Anzeige** auf, sofern die Endgeräte mit einem Display ausgestattet sind. Darüber hinaus wird in diesem Display die **Rufnummer** des Aufschaltenden angezeigt. Diese Maßnahmen reichen aus. Weitere Maßnahmen, etwa ein immer wiederkehrender Signalton, werden nach Meinung der Entwickler als zu störend empfunden.

Für das Leistungsmerkmal „Direktansprechen" gilt folgendes: Teilnehmer mit gleichartigen Endgeräten können sich unmittelbar über einen intergrierten Lautsprecher ansprechen. Über das eingebaute Mikrofon kann der Teilnehmer, ohne den Hörer zu benutzen, antworten. Dieses Leistungsmerkmal kann aber zum Mithören beim Angerufenen mißbraucht werden. Um ein unbemerktes Mithören zu vermeiden, läßt sich die Funktion „Direktansprechen" mit dem Leistungsmerkmal „Ansprechschutz" gezielt verhindern. Ein „Direktansprechen" wird dann als normaler Anruf signalisiert, wie es bei Teilnehmern mit analogen Telefonen geschieht. Ist das Leistungsmerkmal „Ansprechen" nicht generiert, so wird das „Direktansprechen" durch einen sogenannten Ein-Sekunden-Ton und das Aufleuchten einer Lampe angezeigt. Zur Verbesserung des Persönlichkeitsschutzes werden die Hersteller im Rahmen der Fortentwicklung der Systeme einen permanenten Aufmerksamkeitston realisieren, der dann zu hören ist, wenn dieses Leistungsmerkmal in Anspruch genommen wird. Ein unbemerktes Mithören ist dann ausgeschlossen. Da diese Sicherheitseinrichtung softwaretechnisch realisiert wird, ist ein Nachrüsten bestehender Anlagen problemlos möglich.

Zur Erhöhung des Persönlichkeitsschutzes dienen schließlich noch weitere Sicherheitseinrichtungen:
- Es gibt bereits Endgeräte, die die ausgetauschten Informationen verschlüsseln. Allerdings müssen diese Endgeräte mit einem Verschlüsselungsgerät ausgestattet sein, das durch eine Chipkarte aktiviert wird. Nach dem Verbindungsaufbau findet in der Regel ein Schlüsselaustausch statt, wobei der Schlüssel in der Chipkarte gespeichert ist. Die Aktivierung der Chipkarte erfolgt über eine PIN (persönliche Identifikationsnummer). Bei mehrfachen Fehlaktivierungen in Folge sperrt sich die Chipkarte von selbst.
- In vielen Nebenstellenanlagen ist heute bereits ein Computer integriert, so daß bei der Gesprächsdatenaufzeichnung beliebige behördenspezifische Vorgaben für die Aufzeichnung von Gesprächsdaten programmiert werden können, etwa die Unterdrückung beliebig vieler Ziffern der Zielnummer von Privatgesprächen bei deren Speicherung oder die generelle Unterdrückung der angerufenen Nummer für ganz bestimmte Nebenstellen. Ein besonderer Aufwand ist damit nicht verbunden.

20.3.6 Aufgaben eines behördlichen Datenschutzbeauftragten

Im Berichtszeitraum haben des öfteren Behörden angefragt, wann ein behördlicher Datenschutzbeauftragter zu bestellen sei, welche Aufgaben dieser habe und wieviel Zeitaufwand für eine solche Tätigkeit zu veranschlagen sei. Dazu habe ich mich wie folgt geäußert:

Gemäß der derzeit geltenden Vollzugsbekanntmachung (VollzBekBayDSG) zu Art. 26 des Bayer. Datenschutzgesetzes haben Gerichte, Behörden und sonstige öffentliche Stellen des Freistaates Bayern, die Datenverarbeitung im Sinne des Bayerischen Datenschutzgesetzes betreiben, unter folgenden Voraussetzungen einen Beauftragten für den Datenschutz zu bestellen:
- bei automatisierter Datenverarbeitung, wenn in der Regel mindestens 5 Bedienstete ständig beschäftigt werden;
- bei herkömmlicher Verarbeitung personenbezogener Daten, wenn hierbei in der Regel mindestens 20 Bedienstete ständig beschäftigt sind;
- wenn keine Auskunftspflicht nach Art. 8 Abs. 2 BayDSG besteht oder Daten im Auftrag anderer Stellen verarbeitet werden.

Gemeinden, Gemeindeverbänden und den sonstigen der Aufsicht des Freistaates unterstehenden juristischen Personen des öffentlichen Rechts und deren Vereinigungen wird empfohlen, ebenfalls einen Beauftragten für den Datenschutz zu bestellen. Darüber hinaus haben öffentliche Stellen, die als Leistungsträger nach dem Sozialgesetzbuch Sozialdaten verarbeiten, nach § 79 Abs. 1 SGB einen behördlichen Datenschutzbeauftragten zu benennen.

Die Aufgaben des behördlichen Datenschutzbeauftragten sind in Ziff. 26.3 der VollzBekBayDSG wie folgt beschrieben: „Der Beauftragte für den Datenschutz hat den Behördenleiter bei der Ausführung der Aufgaben nach dem BayDSG zu unterstützen und zu beraten. Unberührt davon bleibt die Verantwortung des Behördenleiters und jedes Bediensteten, die Vorschriften des Datenschutzes in der Behörde gewissenhaft zu beachten."

Nähere Angaben über die Aufgaben und Eingliederung des Datenschutzbeauftragten in die Behörde enthält die Vollzugsbekanntmachung nicht. Meines Erachtens sollte der behördliche Datenschutzbeauftragte folgende Aufgaben erfüllen:

- Kontrolle der Einhaltung der Datenschutzvorschriften und innerbehördlicher Dienstanweisungen zu Datenschutz und Datensicherheit
- Überwachung der ordnungsgemäßen Anwendung der Datenverarbeitungsprogramme, mit denen personenbezogene Daten verarbeitet werden sollen (Einbindung bei Programmfreigabeverfahren, Durchführung von Kontrollen)
- Führung einer Übersicht aller Dateien mit personenbezogenem Inhalt (Dateiinhalt, regelmäßige Datenübermittlung)
- Mitwirkung bei der Schulung der bei der Verarbeitung personenbezogener Daten tätigen Personen hinsichtlich des Datenschutzes und Verpflichtung auf das Datengeheimnis (Art. 14 BayDSG), soweit dies nicht von der Personalabteilung vorgenommen wird
- Beteiligung bei der Erstellung von Arbeits- und Benutzeranweisungen
- Prüfung der Zugriffsberechtigungen der Benutzer
- Mitwirkung bei der Freigabe automatisierter Verfahren der Behörde nach Art. 26 Abs. 2 BayDSG
- Führung einer Übersicht aller Dateien mit personenbezogenem Inhalt
- Mitwirkung bei der Meldung personenbezogener Dateien zum Datenschutzregister beim Landesbeauftragten für den Datenschutz, soweit diese nicht nur vorübergehend vorgehalten und innerhalb von drei Monaten nach ihrer Erstellung wieder gelöscht werden
- Beratung bei der Erstellung einer Risikoanalyse und eines daraus resultierenden Sicherheitskonzepts für die Datenverarbeitung
- Überprüfung der Auftragsdatenverarbeitung (Art. 3 BayDSG) hinsichtlich Vertragsgestaltung (Nr. 3.1 ff. VollzBekBayDSG) und Einhaltung der vorgegebenen Maßnahmen zum Datenschutz und zur Datensicherheit
- Anlaufstelle des Bürgers in Datenschutzfragen
- Koordination der Auskünfte an Bürger nach Art. 8 BayDSG.

Der Datenschutz in einer Behörde kann nur von einem Datenschutzbeauftragten gewährleistet werden, der in der Lage ist, die jeweiligen konkreten **Risiken der Informationstechnik** für den Datenschutz zu erkennen. Unabdingbare Voraussetzungen sind dafür fundierte organisatorische, DV-technische und rechtliche Kenntnisse. Der behördliche Datenschutzbeauftragte kann innerhalb der Behörde auch mit anderen Aufgaben (z.B. bei der Revision) beauftragt werden, da er nur bei großen Behörden mit den Datenschutzaufgaben voll ausgelastet sein wird. Er sollte jedoch nicht mit solchen Aufgaben beschäftigt sein, die mit seiner Schutzaufgabe kollidieren. Insbesondere sollte er nicht Leiter der DV-Abteilung sein, auch wenn dies gesetzlich nicht verboten ist.

20.3.7 Hinweise auf neue Orientierungshilfen

Zur Verbesserung der Datensicherheit bei der automatisierten Datenverarbeitung habe ich weitere Orientierungshilfen zusammengestellt, die von Interessenten bei meiner Geschäftsstelle angefordert werden können.

- **Checkliste zum Sicherheitsstatus einer ISDN-Nebenstellenanlage**
  Eine ISDN-Nebenstellenanlage unterstützt heute eine Vielzahl von Kommunikationsdiensten, so daß vor ihrer Installation und der Generierung der Leistungsmerkmale genau zu überlegen ist, wer welche Berechtigungen erhalten soll und wie ein ordnungsgemäßer Betrieb dieser Anlage sicherzustellen ist. Dazu wurde eine Checkliste entwickelt, die als Hilfsmittel zur Dokumentation und als Prüfungsunterlage für die Revision zu verwenden ist.
- **Orientierungshilfe für Sicherheitsmaßnahmen beim Einsatz von UNIX-Rechnern der Digital-Kienzle Computersysteme GmbH**
  Wegen der zunehmenden Verbreitung von UNIX-Systemen wurde zusammen mit dem Hersteller diese Orientierungshilfe erarbeitet. Unter Einbeziehung von KIOFFICE bietet dieses UNIX-Derivat höherwertige Sicherheitskomponenten als das reine UNIX.
- **Kontrollansätze der Benutzerverwaltung in einem Mehrzweckrechenzentrum**
  Die Abschottung der Benutzer unterschiedlicher Aufgabenbereiche in einem Rechenzentrum ist ein wichtiges Anliegen aller Beteiligten. Aus diesem Grunde habe ich eine Orientierungshilfe für Kontrollansätze der Benutzerverwaltung in einem Mehrzweckrechenzentrum zusammengestellt, die sich auch für Betreiber mittlerer DV-Systeme verwenden läßt, sofern dort Benutzer mit unterschiedlichen Aufgaben arbeiten.
- **Prüfansätze für den PC-Einsatz**
  (siehe 20.2.3)

21. Datenschutzregister

Nach § 8 der Verordnung über das Datenschutzregister (DSRegV) vom 23.11.1978 veröffentlicht der Landesbeauftragte für den Datenschutz im Bayer. Staatsanzeiger jährlich eine **Übersicht über den Inhalt des Datenschutzregisters**. Diese Übersicht kann sich auch auf Nachträge zu bereits veröffentlichten Übersichten beschränken.

Wegen der Vielzahl der inzwischen angemeldeten Dateien und des sehr begrenzten Nutzens der Übersicht für den Bürger wurde 1984 letztmalig eine Übersicht des Gesamtinhalts des Datenschutzregisters veröffentlicht. Auch der Umfang der Nachträge ist wegen der starken Ausweitung der automatisierten Datenverarbeitung von Jahr zu Jahr angewachsen. Ein Nachtrag füllt inzwischen ebenfalls weit über 100 DIN-A4-Druckseiten pro Jahr.

Der 8. Nachtrag vom 27. November bzw. 4. Dezember 1992 (Beilagen zum Bayer. Staatsanzeiger Nr. 49, 50) enthält die Meldungen, die vom 11. Oktober 1991 bis 23. Oktober 1992 in meiner Geschäftsstelle eingegangen sind.

Am 11. Oktober 1991 umfaßte das gesamte Datenschutzregister 22.391 Dateien von insgesamt 6.927 speichernden Stellen. Zum Stichtag des 8. Nachtrags waren 23.708 Dateien (+ 1.317) von 7.410 speichernden Stellen (+ 483) gemeldet. Die Anzahl der unterschiedlichen Dateien hat sich zum Stichtag auf 3.284 erhöht.

Die Zahl der Bürger, die jährlich nachfragen, in welchen Dateien Daten über sie gespeichert sein können, ist auch in diesem Berichtszeitraum weiter **zurückgegangen**. Bei einer Anfrage erhält der Auskunftsuchende, bezogen auf seinen Wohnsitz, einen Auszug aus der Übersicht zum Datenschutzregister über alle Stellen, deren Zuständigkeitsbereich sich auf seinen Wohnsitz erstreckt. Der Auszug enthält neben dem Namen und der Anschrift der Behörde die Art der Datei in einer Form, die ihm die Feststellung ermöglicht, ob er in dieser Datei gespeichert sein kann.

22. Datenschutz beim Bayerischen Rundfunk

Bericht des Rundfunkbeauftragten

Nach Art. 21 Abs. 3 BayDSG wird die Einhaltung des Datenschutzes im Bayerischen Rundfunk vom dortigen Datenschutzbeauftragten überwacht, der jährlich über seine Tätigkeit einen Bericht erstattet. Diesen Bericht hat er auch dem Landesbeauftragten für den Datenschutz zu übermitteln (Art. 21 Abs. 3 Satz 6 BayDSG). Hieraus leite ich, wie schon in den Jahren zuvor, für mich die Aufgabe ab, kurz über den Datenschutz beim Bayerischen Rundfunk zu berichten.

Bei der Überwachung der Datenverarbeitung des Bayerischen Rundfunks im Zeitraum vom 01.01. bis 31.12.1991 hat der Datenschutzbeauftragte – wie auch in den Vorjahren – keine datenschutzrechtliche Beanstandung ausgesprochen.

Der Datenschutzbeauftragte schildert die Entwicklung des Datenschutzrechts im Bereich der Medien anhand der Neufassungen des Rundfunkgebührenstaatsvertrages und des ZDF-Staatsvertrages, des Referentenentwurfs für die Änderung des Bayerischen Rundfunkgesetzes und des Entwurfs des Bayerischen Mediengesetzes. Zur Novellierung des Bayerischen Datenschutzgesetzes weist er darauf hin, daß entgegen der bisherigen Sonderregelung in Art. 21 BayDSG der Datenschutz im Bayerischen Rundfunk künftig bereichsspezifisch im Bayerischen Rundfunkgesetz geregelt werden soll.

Zum Datenschutz im Bayerischen Rundfunk berichtet der Datenschutzbeauftragte, daß die elektronische Datenverarbeitung beim Bayerischen Rundfunk weiter voranschreite. Derzeit müßten ca. 550 EDV-Einrichtungen datenschutzrechtlich kontrolliert und überwacht werden. Der Schwerpunkt seiner Tätigkeit liege dabei bei der Neuinstallierung von Anlagen und Dateien mit personenbezogenen Daten.

Der Datenschutzbeauftragte verweist auf seinen letzten Bericht, in dem er die Zusammenfassung der geplanten Datenschutz-Richtlinie für dezentrale DV-Anlagen und der Dienstanweisung für dezentrale elektronische Personaldatenverarbeitung in einer Dienstanweisung angeregt habe. Daraufhin habe der Bayerische Rundfunk den Entwurf einer neuen Dienstanweisung erstellt und dem Personalrat zur Stellungnahme zugeleitet. Der Personalrat habe den Vorschlag begrüßt und sich mit dem Bayerischen Rundfunk über den Inhalt der Dienstanweisung im wesentlichen abgestimmt. Allerdings wünsche der Personalrat nach wie vor die Regelung in einer Dienstvereinbarung. Aus der Sicht des Datenschutzbeauftragten sei die Form der Regelung nebensächlich, entscheidend sei, daß der bereits seit langem als notwendig erkannte Regelungsbedarf nun endlich durch die bereits abgestimmten Regelungen ausgefüllt werde.

Der Datenschutzbeauftragte berichtet über ein Gespräch, das zwischen der Generaldirektion der Deutschen Bundespost Telekom und einigen Mitgliedern des Arbeitskreises der Rundfunkdatenschutzbeauftragten stattgefunden habe. Die Datenschutzbeauftragten hätten insbesondere mit Blick auf den **Informantenschutz** bei den Rundfunkanstalten eine Regelung gefordert, wie sie in der TDSV für bestimmte Sozialdienste, wie Telefonseelsorge und Gesundheitsberatung vorgesehen sei. Der Anruf bei Sozialdiensten, Personen und Behörden, die selbst oder deren Mitarbeiter besonderen Verschwiegenheitspflichten unterliegen und die Beratungsaufgaben in sozialen oder kirchlichen Bereichen ganz oder überwiegend über Telefon abwickeln, darf nach der TDSV aus dem Einzelentgeltnachweis für den Kunden nicht ersichtlich sein. Das Gespräch mit der Telekom habe zu keinem Ergebnis geführt. ARD und ZDF hätten deshalb auf Anregung des Arbeitskreises der Datenschutzbeauftragten im November 1991 einen förmlichen Antrag an Telekom mit dem Ziel der Gleichbehandlung mit den Sozialdiensten gerichtet. Zum Zeitpunkt der Vorlage des Datenschutzberichtes habe eine Antwort noch nicht vorgelegen.

Zum Datenschutz im Personalbereich berichtet der Datenschutzbeauftragte, er habe sich nunmehr der

Auffassung des Landesbeauftragten für den Datenschutz und der Finanzminister von Bund und Ländern angeschlossen, wonach für die Kontrollmitteilungen an die Finanzämter über die Empfänger von Honoraren des Bayerischen Rundfunks die nach § 93 a Abgabenordnung erforderliche Rechtsgrundlage fehle und diese Kontrollmitteilungen damit unzulässig seien. Die Kontrollmitteilungen des Bayerischen Rundfunks an die Finanzämter seien eingestellt worden.

Die Bearbeitung von **Beihilfeanträgen**, die sensible Daten enthielten, habe er nach mehreren Jahren nochmals überprüft. Er habe angeregt, daß unbearbeitete Anträge wegen der beigefügten Belege während der Abwesenheit der Sachbearbeiter verschlossen aufbewahrt werden. Ebenso habe er sich dafür ausgesprochen, daß die Ablage der Beihilfeakten im Zentralarchiv von den übrigen Akten getrennt werde.

Zum Datenschutz beim **Rundfunkgebühreneinzug** weist der Datenschutzbeauftragte darauf hin, daß der Rundfunkgebührenstaatsvertrag nunmehr detailliert vorschreibe, welche Daten der Rundfunkteilnehmer für den Rundfunkgebühreneinzug erhoben und gespeichert werden dürften. Die bei der GEZ gespeicherten Daten über Ordnungswidrigkeitenverfahren seien ein Jahr nach Abschluß des jeweiligen Verfahrens zu löschen. Die Tätigkeit der GEZ und der Gebührenbeauftragten sei datenschutzrechtlich als sog. Auftragsdatenverarbeitung eingeordnet. Ungeachtet der damit bei den einzelnen Landesrundfunkanstalten verbliebenen Verantwortlichkeit für die Einhaltung des Datenschutzes bei der GEZ und der Zuständigkeit ihrer Datenschutzbeauftragten für die Überwachung des Datenschutzes hinsichtlich der Rundfunkteilnehmerdaten sei nunmehr bei der GEZ ein betrieblicher Datenschutzbeauftragter zu bestellen. Für diesen würden die Vorschriften des Bundesdatenschutzgesetzes für den betrieblichen Datenschutzbeauftragten entsprechend gelten.

Der Datenschutzbeauftragte berichtet, daß im Berichtszeitraum bei der GEZ **nur wenige Anfragen** zu verzeichnen gewesen sein, die sich auf die Datenverarbeitung bezogen hätten. Nach wie vor kämen die meisten Anfragen von den Finanzämtern, welche die bei der GEZ gespeicherten Kontoverbindungen der Lastschriftzahler erfahren möchten, um wegen rückständiger Steuerforderungen in etwaige Kontoguthaben vollstrecken zu können. Derartige Auskunftsersuchen seien sowohl vom Datenschutzbeauftragten der GEZ als auch von ihm unter Hinweis auf datenschutzrechtliche Bedenken zurückgewiesen worden. Auch wenn der Landesbeauftragte für den Datenschutz der Auffassung sei, daß den Finanzämtern dieser Auskunftsanspruch zustehe, würden die Rundfunkanstalten aus grundsätzlichen, auch unternehmenspolitischen Überlegungen diese Auskunftsersuchen nicht beantworten, da hierdurch ihre Finanzautonomie gefährdet werden könne.

Auskunftsersuchen von Rundfunkteilnehmern nach den über sie beim Bayerischen Rundfunk gespeicherten Daten habe es im Berichtszeitraum nicht gegeben. Infolge der von der GEZ im Auftrag des Bayerischen Rundfunks durchgeführten Direktwerbemaßnahmen sei aber mehrfach Auskunft nach der Herkunft der verwendeten Daten erbeten worden. In diesen Fällen habe der Datenschutzbeauftragte die Teilnehmer darauf hingewiesen, daß die Daten aus dem Adreßhandel stammten und nach Abschluß der Werbeaktion gelöscht würden. Diese Teilnehmer seien von ihm gleichzeitig über Sinn und Zweck dieser Aktionen und deren datenschutzrechtliche Unbedenklichkeit aufgeklärt worden.

Ferner berichtet er über eine **Werbemaßnahme „abgemeldete Teilnehmer"**. Die GEZ habe im Auftrag des Bayerischen Rundfunks im Oktober 1991 ehemalige Rundfunkteilnehmer angeschrieben und sie gebeten, ggf. wieder zum Empfang bereitgehaltene Rundfunkgeräte anzumelden. Auf die Beschwerde eines Teilnehmers habe er diese Aktion datenschutzrechtlich überprüft. Die GEZ verwende für diese Werbeaktion Daten von Teilnehmern, die sich knapp ein Jahr vorher abgemeldet hätten. Insofern könnte die Auffassung vertreten werden, daß sämtliche Daten des Teilnehmerverhältnisses mit der Abmeldung zu löschen seien, so daß eine Verwendung der Adressen für den Werbebrief ausgeschlossen wäre. Gemäß Art. 20 Abs. 4 BayDSG seien Daten zu löschen, wenn es der Betroffene verlange oder wenn ihre Speicherung unzulässig sei. Mit der Abmeldung zeige der Betroffene an, daß er keine gebührenpflichtigen Geräte mehr zum Empfang bereithalte. Dies habe zur Folge, daß im Teilnehmerverhältnis die entsprechende Abmeldung vermerkt und künftig keine Rundfunkgebühren mehr in Rechnung gestellt würden. Die Löschung der Daten – insbesondere der Adreßdaten – werde vom Betroffenen nicht verlangt. Da die Daten von der GEZ auch nach der Abmeldung noch benötigt würden, um etwaige Ansprüche auf Rundfunkgebühren bzw. auf deren Erstattung bearbeiten zu können, bleibe deren Speicherung zulässig. Im Anschluß an diese Feststellungen erhebe sich die weitere Frage, ob diese Adressen für Werbezwecke der GEZ verwendet werden dürften. Da die Werbung im Rahmen der Zweckbindung des § 3 Abs. 3 Satz 1 Rundfunkgebührenstaatsvertrag für den Rundfunkgebühreneinzug erfolge, stünden auch insoweit datenschutzrechtliche Bedenken der Werbemaßnahme nicht entgegen. Im übrigen lehre die Erfahrung, daß zahlreiche Abmeldungen von den Teilnehmern von vornherein nur für kurze Zeit beabsichtigt seien. Insbesondere diesem Teilnehmerkreis erleichtere die Werbemaßnahme die Wiederanmeldung.

Der Datenschutzbeauftragte berichtet weiter, das Staatsministerium für Arbeit, Familie und Sozialordnung habe ihn gebeten, zur **Speicherung von Sozialdaten** durch eine Stadt bei der Bearbeitung von Anträgen auf Befreiung von der Rundfunkgebührenpflicht Stellung zu nehmen. Gegen die Speicherung seien Bedenken aufgekommen, weil nicht nur zu den gebührenbefreiten Personen, sondern auch zu den Haushaltsangehörigen Angaben erhoben und gespeichert worden seien.

Befreiung von der Rundfunkgebührenpflicht werde in den Fällen geringen Einkommens gemäß § 1 Abs. 1 Nr. 7 Befreiungsverordnung Personen gewährt, deren monatliches Einkommen zusammen mit dem Einkommen der Haushaltsangehörigen eine Einkommensgrenze nicht übersteige, die sich ergebe aus
- dem 1fachen des Regelsatzes der Sozialhilfe für den Haushaltsvorstand,
- dem Regelsatz der Sozialhilfe für sonstige Haushaltsangehörige und
- einem Zuschlag von 30 v.H. des Regelsatzes der Sozialhilfe für jeden Haushaltsangehörigen, der das 65. Lebensjahr vollendet habe oder erwerbsunfähig im Sinne der gesetzlichen Rentenversicherung sei.

Aus dieser Regelung ergebe sich, daß eine Befreiung von den Rundfunkgebühren wegen geringen Einkommens nur gewährt werde, wenn der gesamte Haushalt im Bezug auf Bedarf und Einkommen einander gegenübergestellt werde. Seien also Haushaltsangehörige vorhanden, so sei es erforderlich, auch für diese den vom jeweiligen Alter abhängigen Regelsatz und ein ggf. erzieltes Einkommen festzustellen. Dies gelte auch für die Frage der Erwerbsunfähigkeit.

Da die Gemeinden gemäß § 5 Abs. 2 Befreiungsverordnung für die Entgegennahme der Befreiungsanträge und die Aushändigung der Befreiungsbescheide zuständig seien und ihre Entscheidung über die Befreiung im Auftrag des Bayerischen Rundfunks treffen würden, benötigten sie zur Wahrnehmung der ihnen übertragenen Aufgaben auch die aufgeführten Daten von Haushaltsangehörigen. Er habe daher dem Sozialministerium mitgeteilt, daß gegen die Speicherung der Daten durch die Stadt in den Fällen der Befreiung wegen geringen Einkommens keine datenschutzrechtlichen Bedenken bestünden.

23. Der Beirat

Die Mitglieder des Beirats werden nach Art. 29 Abs. 2 BayDSG für vier Jahre, die Beiratsmitglieder des Landtags für die Wahldauer des Landtags bestellt. Im Berichtszeitraum gehörten dem Beirat an:

Ordentliche Mitglieder	**Vertreter**
die Landtagsabgeordneten	
Franz Brosch	Dr. Hans Gerhard Stockinger
Alois Braun	Dr. Helmut Müller
Franz Meyer	Wilhelm Wenning
Markus Sackmann	Georg Grabner
Dr. Klaus Hahnzog	Armin Nentwig
Carmen König	Joachim Wahnschaffe
die Senatoren	
Wolfgang Burnhauser	Hartwig Reimann
für die Staatsregierung	
Christian P. Wilde Ministerialrat im Bayer. Staatsministerium des Innern	Hubert Kranz Ministerialrat im Bayer. Staatsministerium der Finanzen
für die Sozialversicherungsträger	
Ludwig Bergner Erster Direktor der Landesversicherungsanstalt Oberbayern	Herbert Schmaus Verwaltungsdirektor beim AOK-Landesverband Bayern
für die Kommunalen Spitzenverbände	
Klaus Eichhorn Geschäftsführender Direktor der Anstalt für Kommunale Datenverarbeitung in Bayern	Hans Herlitz Direktor bei der Anstalt für Kommunale Datenverarbeitung in Bayern
für den Verband der Freien Berufe in Bayern e.V.	
Erwin Stein, MdL Präsident der Steuerberaterkammer München	Winfried Wachter Präsidiumsmitglied des Verbandes der Freien Berufe in Bayern e.V.

Den Vorsitz im Beirat führt Franz Brosch, MdL. Stellvertreterin ist Carmen König, MdL.

Der Beirat befaßte sich in seinen 5 Sitzungen am 07.04.1992, 19.05.1992, 14.07.1992, 03.11.1992 und 08.12.1992 insbesondere mit folgenden Themen:

- Beratung des 14. Tätigkeitsberichts
- Berichte über Prüfungen und Beanstandungen
- Berichte von Arbeitskreisen und Datenschutzkonferenzen
- Verfahrenseinstellungen nach § 170 Abs. 2 Strafprozeßordnung
- Auskunft durch das Landesamt für Verfassungsschutz (Ausweiskopie)
- Mißbrauch von ZEVIS-Daten
- Identitätssichernde Behandlung aller Asylbewerber mit Lichtbildern und 10-Fingerabdrucken
- Auswertung der Protokolldatei beim LKA
- Gesetz zur Bekämpfung der Organisierten Kriminalität (OrgKG)

- Einsatz von Abhörgeräten in Wohnungen
- Behandlung des Schriftwechsels von Strafgefangenen in bayerischen Justizvollzugsanstalten
- Krankenhaus-Betten-Vermittlungszentrale bei einer Städtischen Feuerwehr
- Mieterinformationen in Stadterneuerungsgebieten durch Bauordnungsbehörde und Familienhilfe
- Einsicht in Notenbogen eines Schülers durch alle Lehrer einer Schule
- Aufnahme des Datenschutzes in die Verfassung
- „Konferenzbeschlüsse" der Konferenz der Datenschutzbeauftragten

Auf Einladung des Polizeipräsidiums München besichtigte der Beirat die dort betriebene Datei „Polizeiliche Sachbearbeitung/Vorgangsverwaltung-Verbrechensbekämpfung. Beim Umweltreferat der Landeshauptstadt München unterrichtete er sich über das Umwelt-Informationssystem KUNIS (bisher UMSYS).

24. Konferenz der Datenschutzbeauftragten des Bundes und der Länder

Die Datenschutzbeauftragten des Bundes und der Länder trafen sich 1992 zu zwei regulären Konferenzen und zu einer Sonderkonferenz.

24.1 Schwerpunkte der Erörterungen waren

- Vereinbarung einer Geschäftsordnung für die Konferenz
- Beachtung des Einstimmigkeitsprinzips
- Vorsitz in der Konferenz
- Zusätzliche Verankerung des Grundrechts auf Datenschutz im Grundgesetz und Schaffung eines Grundrechts auf Informationsfreiheit
- Einsatz von Abhörgeräten als Fahndungsmittel gegen Organisierte Kriminalität
- Erkennungsdienstliche Behandlung von Asylbewerbern
- Arbeitnehmerdatenschutz
- Epidemiologisches Krebsregister
- Datenschutz bei innerbetrieblichen Telekommunikationsanlagen
- Gesundheitsstrukturgesetz
- Chipkarte als elektronische Krankenversichertenkarte

24.2 Vereinbarung einer Geschäftsordnung für die Konferenz, Beachtung des Einstimmigkeitsprinzips und Vorsitz in der Konferenz

Die Datenschutzbeauftragten des Bundes und der Länder sind 1978 in Bonn zu ihrer ersten Konferenz zusammengekommen. In den ersten Jahren seit ihrem Bestehen wurden in der Konferenz lediglich Erfahrungen ausgetauscht. Erst später wurden auch Beschlüsse gefaßt, die stets einstimmig ergingen. Spätestens seit 1987, als ich einem Vorschlag zur Speicherung eines HIV-Hinweises im Kriminalaktennachweis nicht zustimmte, gibt es in der Konferenz jedoch Differenzen in der Frage, unter welchen Voraussetzungen die Konferenz Beschlüsse fassen kann. Ich habe, seit ich an der Konferenz teilnehme, die Auffassung vertreten, daß Beschlüsse grundsätzlich **nur einstimmig** ergehen können. Die Datenschutzkonferenz ist eine Einrichtung des kooperativen Föderalismus, in der das Einstimmigkeitsprinzip maßgebend ist. Das Mehrstimmigkeitsprinzip könnte nur gelten, wenn in einer Geschäftsordnung eine entsprechende Regelung getroffen wäre. **Eine Geschäftsordnung der Konferenz gibt es jedoch bis heute nicht.** Die Mehrheit hat überdies auf der letzten Konferenz die Vereinbarung einer Geschäftsordnung, in der die Grundlagen der Zusammenarbeit geregelt werden, abgelehnt, so daß die Konferenz auch weiterhin ohne Geschäftsordnung, d.h. ohne Ordnung nach Gutdünken einer Mehrheit „arbeitet".

Obwohl das Einstimmigkeitsprinzip gilt, hat die Mehrheit zum Einsatz von Observationsmitteln in Wohnungen einen „Konferenzbeschluß" verkündet, den es wegen fehlender Einstimmigkeit gar nicht gibt. Wegen Differenzen über die Grundsätze der Zusammenarbeit in der Konferenz habe ich es deshalb abgelehnt, für 1993 den Vorsitz zu übernehmen.

24.3 Pervertierung der Grundrechte durch „rechtsfreien Raum Wohnung" für Schwerstverbrecher

Zum Einsatz von Observierungsmitteln in Wohnungen konnte unter den Konferenzteilnehmern keine einheitliche Auffassung erzielt werden.

Der Bundestag hatte schon bei der Verabschiedung des Gesetzes zur Bekämpfung des illegalen Rauschgifthandels und anderer Erscheinungsformen der Organisierten Kriminalität (OrgKG) in einer Entschließung vom Juni 1992 ausdrücklich festgestellt, daß zur Frage des Einsatzes von Abhörgeräten in Wohnungen zur Bekämpfung der organisierten Schwerstkriminalität nach der parlamentarischen Sommerpause die Beratungen wieder aufgenommen werden sollten. Der Bundestag war also eindeutig **nicht** der Auffassung, daß mit dem OrgKG bereits alle derzeit für erforderlich gehaltenen gesetzlichen Eingriffsbefugnisse geschaffen seien und die Erfahrungen mit dem OrgKG abgewartet werden müßten, ehe zusätzliche Maßnahmen diskutiert werden sollten.

Trotzdem kritisierte die Mehrheit der Datenschutzbeauftragten, daß die Erfahrungen mit dem OrgKG nicht abgewartet und Überlegungen über den Einsatz von Abhörgeräten in Wohnungen angestellt würden.

In der Datenschutzkonferenz am 01./02. Oktober 1992 in Stuttgart lehnte die Mehrheit den Einsatz von Abhörgeräten in Wohnungen ab mit der Begründung, ein solcher Einsatz verstoße gegen die Menschenwürde; auch ein Schwerstverbrecher habe in seiner Wohnung ein unantastbares Recht auf Privatheit. Lediglich in „Wohnungen minderen Ranges" könne der Verfassungsgeber im Grundgesetz den Einsatz von Abhörgeräten zulassen.

Ich habe dieser Interpretation des Grundgesetzes entschieden widersprochen. Um nicht mißverstanden zu werden: Ich sehe es nicht als meine Aufgabe an, den Einsatz von Observierungsmitteln zu fordern. Diese Forderung ist von den für die innere Sicherheit Verantwortlichen erhoben und schlüssig und überzeugend begründet worden. Ich kann aber nicht tatenlos zusehen, wie in der politischen Auseinandersetzung mit der Menschenwürde Schindluder getrieben und der Datenschutz, wenn er zum Täterschutz ausartet, weiter in Verruf gebracht wird.

Die Mehrheit der Datenschutzbeauftragten geht von der völlig irrigen Rechtsmeinung aus, daß das Grundgesetz dem Schwerstverbrecher einen unantastbaren Raum gewährleiste, in dem er ungestört seine Verbrechen an der Gemeinschaft planen, vorbereiten und durchführen könne, ohne daß ihn die Justiz daran hindern könne. Eine solche maßlose Übersteigerung eines Grundrechts ist der bisherige Gipfelpunkt der Pervertierung der Grundrechte.

Wenn nach geltendem Verfassungsrecht ungleich tiefere Eingriffe in die menschliche Freiheit, wie Verhaftungen in und Durchsuchungen von Wohnungen nach dem Grundgesetz erlaubt sind, dann muß um so mehr der Grundgesetzgeber imstande sein, das Abhören der Gespräche von Personen zu gestatten, die schwerster Verbrechen gegen die Gemeinschaft (Terrorakte, Mordanschläge, Rauschgiftgeschäfte) verdächtig sind. Die Gestattung des Einsatzes von Observationsmitteln in Wohnungen ist die durch die Not erzwungene Fortentwicklung des Verfassungsrechts. Es ist vorrangige Aufgabe des Rechtsstaats, das weitere Eindringen der Organisierten Kriminalität in die Gesellschaft zu verhindern. Eine Gesellschaft, die unfähig ist, ihre Bürger vor diesem Übel zu schützen, verliert ihre Existenzberechtigung.

Ein Blick über die deutschen Grenzen könnte auch hier sehr hilfreich sein. Wenn in fast allen westlichen Staaten mit ungebrochener rechtsstaatlicher Tradition der Einsatz von Observierungsmitteln in Wohnungen gegen Schwerstverbrecher der Organisierten Kriminalität nicht gegen die Menschenwürde verstößt und erfolgreich praktiziert wird, dann kann auch in Deutschland die Menschenwürde nicht verletzt sein.

24.4 Zusätzliche Verankerung des Grundrechts auf Datenschutz im Grundgesetz und Schaffung eines Grundrechts auf Informationsfreiheit

Während in der aktuellen Diskussion um die Änderung des Grundgesetzes die Mehrheit der Datenschutzbeauftragten sich für die zusätzliche Verankerung des Datenschutzes in der Verfassung ausspricht, sehe ich für eine **Verdoppelung des Datenschutzes** im Grundgesetz keinerlei Notwendigkeit. Der Datenschutz ist nach der ständigen Rechtssprechung des Bundesverfassungsgerichts bereits eindeutig, klar und an hervorragender Stelle, nämlich durch die Verpflichtung des Staates zur Beachtung der Menschenwürde und der persönlichen Entfaltungsfreiheit (Art. 1 und 2 GG) im Grundgesetz verankert.

Ein **Grundrecht auf Informationsfreiheit**, das von der Mehrheit der Datenschutzbeauftragten gefordert wird, findet seine Begründung weniger in der Menschenwürde und im Persönlichkeitsrecht als im Recht auf demokratische Mitgestaltung. Der Informationsanspruch gegenüber dem Staat steht indessen in vielfacher Hinsicht mit dem Grundrecht auf Datenschutz im Widerspruch. Die Verankerung eines solchen Grundrechts kann deshalb nicht erklärtes Ziel von Datenschutzbeauftragten sein.

Anlage 1: Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 1./2. Oktober 1992 zum Datenschutz bei internen Telekommunikationsanlagen

Der zunehmende Einsatz von digitalen Telekommunikationsanlagen (TK-Anlagen) in Wirtschaft und Verwaltung birgt Datenschutzrisiken in sich, denen durch eine datenschutzfreundliche **Ausgestaltung der Technik** und durch geeignete bereichsspezifische **Regelungen** entgegengewirkt werden muß. Telefongespräche stehen – auch wenn sie von einem Dienstapparat aus geführt werden – unter dem Schutz des Grundgesetzes. Dies hat das Bundesverfassungsgericht in seiner neueren Rechtsprechung hervorgehoben.

Der Schutz des Fernmeldegeheimnisses und des nichtöffentlich gesprochenen Wortes ist gerade bei Arbeitnehmern bedeutsam, da diese sich in einem besonderen Abhängigkeitsverhältnis befinden; aber auch das informationelle Selbstbestimmungsrecht Dritter, die anrufen oder angerufen werden, muß gewahrt werden.

Entsprechende bundesrechtliche Regelungen für interne TK-Anlagen sind überfällig, da in diesen Anlagen – insbesondere wenn sie digital an das öffentliche ISDN angeschlossen sind – umfangreiche Sammlungen sensibler personenbezogener Daten entstehen können, die sich auch zur **Verhaltens- und Lei-**

stungskontrolle eignen und zudem Hinweise auf das **Kommunikationsverhalten** aller Gesprächsteilnehmer geben.

Die Regelungen sollten verbindliche Vorgaben für die technische Ausgestaltung von TK-Anlagen geben und den Umfang der zulässigen Datenverarbeitung festlegen:

- Es müssen die technischen Voraussetzungen gewährleistet sein, daß Anrufer und Angerufene die **Rufnummernanzeige** fallweise abschalten können.
- Die **automatische Speicherung der Rufnummern von externen Anrufern** nach Beendigung des Telefongesprächs ist auszuschließen, es sei denn, eine sachliche Notwendigkeit besteht hierfür (z.B. bei Feuerwehr und Rettungsdiensten)
- Die **Weiterleitung eines Anrufs** an einen anderen als den gewählten Anschluß sollte dem Anrufer so rechtzeitig signalisiert werden, daß dieser den Verbindungsaufbau abbrechen kann.
- Das **Mithören und Mitsprechen** weiterer Personen bei bestehenden Verbindungen sollte nur nach eindeutiger und rechtzeitiger Ankündigung möglich sein.
- **Verbindungsdaten** einschließlich der angerufenen Telefonnummern sollten nach Beendigung der Gespräche nur insoweit **gespeichert** werden, als dies für Abrechnungszwecke und zulässige Kontrollzwecke erforderlich ist. Die Nummern der Gesprächspartner von Arbeitnehmervertretungen, internen Beratungseinrichtungen und sonstigen auf Vertraulichkeit angewiesenen Stellen dürfen nicht registriert werden.
- Die TK-Anlagen müssen durch geeignete technische Maßnahmen gegen unberechtigte **Veränderungen der Systemkonfiguration** und unberechtigte Zugriffe auf Verbindungs- und Inhaltsdaten geschützt werden.

Da TK-Anlagen geeignet sind, das Verhalten und die Leistung der Arbeitnehmer zu kontrollieren, und sie überdies häufig die Arbeitsplatzgestaltung beeinflussen, löst ihre Einführung in Betrieben und Behörden **Mitbestimmungsrechte** der Betriebsräte und überwiegend auch der Personalräte aus. Sie dürfen daher nur betrieben werden, wenn unter Beteiligung der Arbeitnehmervertretungen verbindlich festgelegt wurde, welche Leistungsmerkmale aktiviert und unter welchen Bedingungen sie genutzt werden, welche Daten gespeichert, wie und von wem sie ausgewertet werden. Die Nutzer der TK-Anlage sind über den Umfang der Datenverarbeitung umfassend zu unterrichten.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder fordert, daß umgehend datenschutzrechtliche Regelungen für den Einsatz und die Nutzung von internen TK-Anlagen mit einer bereichsspezifischen Rechtsgrundlage für die Verarbeitung von Arbeitnehmerdaten geschaffen werden.

Anlage 2: Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 1./2. Oktober 1992 zum Entwurf eines Gesundheits-Strukturgesetzes 1993

„Die Bundesregierung will mit dem Gesundheitsstrukturgesetz dem Kostenanstieg in der gesetzlichen Krankenversicherung entgegenwirken. Dieses begrüßenswerte Ziel soll nach dem vorgelegten Gesetzentwurf u.a. auch durch eine verstärkte automatisierte Datenverarbeitung erreicht werden. Die damit verbundenen Eingriffe in die Persönlichkeitsrechte der Versicherten und in die sie schützende ärztliche Schweigepflicht müssen auf das unbedingt Notwendige beschränkt werden. Die Datenschutzkonferenz hält vor allem folgende Verbesserungen des Gesetzentwurfs für notwendig:

- Der Gesetzentwurf sieht vor, daß die Krankenhäuser den Krankenkassen mehr Versichertendaten zur Verfügung stellen müssen als bisher. Es sollte deshalb eingehend geprüft werden, ob die Krankenkassen tatsächlich alle geforderten Angaben benötigen; die Aufgabenteilung zwischen Krankenkassen und Medizinischem Dienst muß aufrechterhalten bleiben.
- Für das Modellvorhaben zur Überprüfung des Krankenhausaufenthalts müssen die Erhebung, Verwendung und Löschung von Versichertendaten durch den Medizinischen Dienst präziser als bisher vorgesehen geregelt werden.
- Beim Einzug der Vergütung der Krankenhausärzte für Wahlleistungen durch Krankenhäuser sollte die **Einschaltung privater Abrechnungsstellen** ohne Einwilligung der Patienten nicht zugelassen werden, da dabei Abrechnungsdaten an Dritte offenbart werden. Die Daten sind gegen unbefugte Offenbarung und Beschlagnahme rechtlich besser geschützt, wenn sie – auch zur Abrechnung – im Krankenhaus verbleiben. Die Krankenhäuser sind zudem selbst in der Lage, die Vergütung einzuziehen.
- Für die neu vorgesehenen **Patienten-Erhebungsbogen** zur Ermittlung des Bedarfs an Pflegepersonal im Krankenhaus sollte eine strikte Zweckbindung sowie eine frühestmögliche Löschungs- oder Anonymisierungspflicht festgelegt werden. Eine Überlassung der Patienten-Erhebungsbogen in der im Gesetzentwurf vorgesehenen Fassung an die Krankenkassen ist abzulehnen".