Bayerischer Landtag
10. Wahlperiode

Drucksache **10/1664**

12. 08. 83

Fünfter Tätigkeitsbericht des Landesbeauftragten für den Datenschutz

Berichtszeitraum: 1. Januar bis 31. Dezember 1982

Der Landesbeauftragte für den Datenschutz
Nr. DSB/ 1 – 510 – 5

München, den 12. August 1983

An den
Herrn Präsidenten
des Bayerischen Landtags
München

Betreff: **Fünfter Tätigkeitsbericht des Landesbeauftragten für den Datenschutz**

Sehr geehrter Herr Landtagspräsident!

Anliegend übersende ich gemäß Art. 28 Abs. 4 des Bayerischen Gesetzes zum Schutz vor Mißbrauch personenbezogener Daten bei der Datenverarbeitung vom 28. April 1978 den fünften Tätigkeitsbericht für den Zeitraum vom 1. Januar bis 31. Dezember 1982.

Der Beirat hat den Entwurf in seiner Sitzung am 12. Juli 1983 vorberaten.

Mit vorzüglicher Hochachtung

Dr. Stollreither

Inhaltsübersicht:

1. Fünf Jahre Datenschutz in Bayern

Mit diesem 5. Tätigkeitsbericht, nach fünf Jahren Tätigkeit, kann die Aufbauphase des Datenschutzes in Bayern als abgeschlossen gelten.

Mit dem Ende der Aufbauphase ging eine bemerkenswerte Veränderung auf dem Arbeitsfeld des bayerischen Datenschutzes einher: Neben den Großrechenzentren, in denen die automatisierte Datenverarbeitung in der Verwaltung zunächst begann, führte die technische Entwicklung zum Einsatz von immer mehr mittleren und kleineren Rechnern - mit allen teils erleichternden, teils erschwerenden Folgen für technische und organisatorische Maßnahmen des Datenschutzes. Die neuen Medien beginnen in Bayern aus der Vorbereitungs- in die Testphase einzutreten; bei Bildschirmtext steht die Einführung sogar kurz bevor. Sie stellen, was freilich in der Öffentlichkeit noch wenig erkannt wird, für den Bürger eine noch wesentlich größere Gefährdung seiner Privatsphäre dar, als die „herkömmliche" automatisierte Datenverarbeitung der öffentlichen Verwaltung. Auf diese Entwicklungen der dezentralen Datenverarbeitung und des Einsatzes neuer Medien hat sich der Datenschutz einzustellen. Sie rufen aber auch den Gesetzgeber auf den Plan. Als Beispiele sei auf das Änderungsgesetz zum EDV-Gesetz in Bayern von 30.3.1982 und den Entwurf des Ausführungsgesetzes zum Bildschirmtext-Staatsvertrag hingewiesen.

Das Bayerische Datenschutzgesetz ist in den vergangenen fünf Jahren unverändert geblieben. Aufgrund der bisherigen Erfahrungen wäre die eine oder andere Änderung denkbar. Trotz äußerer Unabhängigkeit können für ein Änderungsgesetz aber die Bestrebungen nach einer Novellierung des Bundesdatenschutzgesetzes nicht außer Betracht bleiben. Das Bayerische Datenschutzgesetz hat sich gleichwohl im wesentlichen bewährt. Dies gilt vor allem auch für eine bayerische „Eigenheit": Den Beirat beim Landesbeauftragten für den Datenschutz.

Der Beirat (siehe dazu unten Nr. 2.1) stellt insbesondere eine sehr nützliche und erfreuliche Brücke zum Parlament dar. Von den 11 Mitgliedern des Beirats sind sechs Abgeordnete des Bayerischen Landtags, ein Mitglied vertritt den Bayerischen Senat. So war der Kontakt zu Landtag und Senat eng und

elastisch. Bei den den Datenschutz sehr stark berührenden Gesetzesvorhaben, zum Beispiel dem neuen Bayerischen Meldegesetz oder dem Gesetz über das Erziehungs- und Unterrichtswesen (EUG), trug eine enge Verbindung mit den Fraktionen erkennbare Früchte. Die Erörterung der Tätigkeitsberichte in den Landtags- und Senatsausschüssen gab wertvolle Hinweise für meine Arbeit.

Erfreulich gut war auch stets das Verhältnis zur Staatsregierung und Verwaltung. Sicher bringt der Datenschutz oft genug Komplikationen und Erschwerungen für die Ministerien und Verwaltungsbehörden, aber man weiß, das glaube ich wohl sagen zu dürfen, daß meine Mitarbeiter und ich, in oft zähem Ringen um größere oder kleinere Detailfragen, um die Wahrung der Rechte des Bürgers besorgt sind, ohne die Notwendigkeit einer funktionsfähigen Verwaltung außer acht zu lassen. Bei diesem unermüdlichen Bestreben beider Seiten - der Verwaltung wie des Datenschutzes - um sachgerechte Lösungen, tritt der Datenschutz in Bayern freilich in der Öffentlichkeit weniger häufig in Erscheinung. Stelle ich größere (was sehr selten ist) oder kleinere Verstöße gegen Datenschutzrecht fest, so werden diese beanstandet und, soweit noch möglich, behoben. Beanstandungen werden nach Art. 29 Abs. 5 BayDSG im Beirat erörtert, den ich auch sonst über bedeutsame Vorkommnisse und Entwicklungen unterrichte. Hier ist Gelegenheit zur Diskussion, die stets sachbezogen darauf abstellt, "wie man es besser machen kann".

In der Öffentlichkeit hat sich das Image des Datenschutzes, nach einer anfänglichen Datenschutzeuphorie, verschlechtert. Der Datenschutz erscheint einerseits nicht selten als Alibi, das mit Aufwand an Personal- und Sachmitteln zu wenig zum Schutze des Bürgers zustande bringe, andererseits wird er von manchem als „Tatenschutz" unzulässig vereinfachend abgetan, auch in sonst wohlmeinenden Medien. Gelegentlich wurden Datenschutzprobleme von außerhalb Bayerns auf Bayern übertragen, obwohl sie hier nicht auftraten, und aus dem Fehlen von Skandalberichten wurde auf Untätigkeit des Datenschutzbeauftragten geschlossen. Der vorliegende Tätigkeitsbericht zeugt, wie seine vier Vorgänger, von unserer Arbeit. Sie besteht in vielen Fällen aus Kleinarbeit, die viele verschiedene Gesichtspunkte berücksichtigen muß und sich daher aus ihrer Natur heraus kaum publikumswirksam darstellen läßt.

Was muß der Öffentlichkeit über Datenschutz noch klarer werden? Ich will aus meiner Sicht aufgrund der bisherigen Erfahrungen einige Fragen ansprechen:

- Datenschutz ist nicht „manipulierbar", er beruht auf den Artikeln 1 und 2 GG, seine Anforderungen können daher nicht beliebig korrigiert werden; sie sind damit weder in die Verfügung der verantwortlichen Dienstbehörden noch in das der Datenschutzbeauftragten gestellt.

- Die Formel „Datenschutz vor Sicherheit" ist so unrichtig wie ihr Gegenteil „Sicherheit vor Datenschutz"; in jedem Einzelfall muß daher die rechte Balance gefunden werden.

- Datenschutz muß im Zweifelsfall ein Bindeglied zwischen Bürger und Verwaltung darstellen. Gerade der gesetzestreue Bürger ist rascher, als er glaubt, auf Datenschutz angewiesen, z. B. wenn er in unbegründeten Verdacht gerät; die Meinung, „Wer nichts zu verbergen hat, hat auch nichts zu schützen", stimmt - leider - nicht.

- Eine nicht ohne weiteres erkennbare Gefährdung schutzwürdiger Belange kann in der Verknüpfung an sich nicht sensibler Daten liegen; gerade dieser Verknüpfungen hat sich der Datenschutz anzunehmen; ein Beispiel hierfür ist das Volkszählungsgesetz 1983; hierüber ist noch an späterer Stelle zu berichten;

- Die Einwilligung eines Bürgers in Datenerfassung oder Datenübermittlung löst nicht alle Probleme. Oft sind Einwilligungen aus den jeweiligen Lebensumständen erzwungen, so daß die Interessen der Betroffenen im Hinblick auf die Artikel 1 und 2 Grundgesetz trotz Einwilligung gewahrt werden müssen;

- Der Bürger kann, tritt er der Verwaltung gegenüber, davon ausgehen, daß diese pflichtbewußt und rechtmäßig handelt. Das Überhandnehmen von Datensammlungen in der Verwaltung unserer Tage beruht überwiegend auf dem Anwachsen der Leistungsverwaltung.

Rückblickend auf fünf Jahre Datenschutz-Arbeit lassen sich, neben den vorgenannten allgemeinen Erfahrungen, auch bestimmte Einflußfaktoren deutlicher erkennen, die sich auf den Stand des Datenschutzes oder seine Gefährdung auswirken. Ohne Anspruch auf Vollständigkeit sei dazu folgendes berichtet:

1.1 Die Anziehungskraft größerer Datensammlungen

Große Datensammlungen ermöglichen aufgrund der Menge der gespeicherten Datensätze in der Regel die Gewinnung neuer Informationen und zusätzlicher Nutzungen, die bei ihrer Errichtung nicht vorgesehen waren. So erlaubt das Durchsuchen großer Datenmengen in automatisierten Verfahren meist konkrete Aussagen über bestimmte Untermengen im Verhältnis zur übrigen oder zur gesamten Informationsmenge. Außerdem wird der Zugriff zu einzelnen Datensätzen einer großen zentralen Datensammlung gegenüber dem Zugriff zu mehreren verstreuten Datensammlungen schneller und billiger und die Treffer-Wahrscheinlichkeit im Vergleich zu Sammlungen kleineren Umfangs höher.

Dies gilt zunächst für die Gefahr des Mißbrauchs durch Unbefugte. Sie gewinnt bei zentralen Datensammlungen eine ganz andere Dimension als - beispielweise im Bereich medizinischer Daten - bei der Patientenkartei des einzelnen niedergelassenen Arztes. Andererseits sind aber auch die Möglichkeiten technischer und organisatorischer Sicherung einer zentralen automatisierten Datensammlung vielfältiger.

Neben der Gefahr unbefugter Inanspruchnahme großer Datensammlungen wächst bei diesen erfahrungsgemäß aber auch der Druck auf die Schaffung von Befugnissen für Zugriff und Auswertung für Stellen, die bisher keinen Zugang zu den Daten hatten. Es wird dann geltend gemacht, daß der Aufwand zur Erstellung der großen Datensammlung wirtschaftlich voll genutzt werden müsse. Indirekt wird unter Berufung auf den volkswirtschaftlichen Aufwand, der mit der Erstellung der Datensammlungen verbunden war, eine Art Sozialpflichtigkeit hinsichtlich ihrer Nutzung, vor allem im öffentlichen Bereich, postuliert. Gegen zusätzlich eröffnete Befugnisse zur Datenübermittlung sind aber Datenschutzargumente nur noch schwer geltend zu machen.

Ein Beispiel für diese Anziehungskraft von Datensammlungen, die ursprünglich für ganz andere und beschränktere Zwecke eingerichtet wurden, ist die bei den Kreisverwaltungsbehörden geführte Kaufpreissammlung nach dem Bundesbaugesetz. Während diese anfangs im wesentlichen dafür gedacht war, dem Gutachterausschuß als Material für die Erstellung von Gutachten über den Wert von Grundstücken zu dienen, hat sich in der Praxis daneben ein erheblicher Druck auf Auskünfte aus der Kaufpreissammlung entwickelt, die nicht zur Erstellung von Gutachten dienten. Die Staatsregierung mußte daher jüngst eine Verordnung zur Regulierung der Inanspruchnahme dieser Kaufpreissammlungen erlassen. Dabei wurde die Berechtigung einer ganzen Reihe von Stellen zur Kenntnisnahme anerkannt. Verwiesen sei als weiteres Beispiel auf die bei der Post gespeicherten Daten über Telefonbenutzer, die aufgrund von

Vorschriften der Strafprozeßordnung der Rasterfahndung dienten. Ein bedeutendes Beispiel ist weiter das allgemeine Interesse von öffentlichen und privaten Stellen an Einwohnermelderegistern. Während diese Register ursprünglich ausschließlich Behördenzwecken dienten und Datenübermittlungen an Personen oder nicht öffentliche Stellen durch Vollzugsbekanntmachungen geregelt wurden, wird aufgrund der massiven Nachfrage im neuen Melderecht (Melderechts-Rahmengesetz des Bundes, Landesmeldegesetze) ein Verfahren zur Auskunftserteilung an nichtöffentliche Stellen gesetzlich Teil des Meldewesens. Ein Beispiel für Schlüsse, die aus einer Datensammlung gezogen werden können, an die bei ihrer Einrichtung gewiß nicht gedacht wurde, ist die Schlußfolgerung aus einem niedrigen Wasserverbrauch, der sich aus der Wasserversorgungsdatei ergibt, auf die Abwesenheit des Hausbewohners - im Zusammenhang mit dem Vollzug anderer Verwaltungsaufgaben.

Diese Neben-Nutzungen von Dateien sind zwar nicht alle problematisch, sie zeigen aber die Tendenz, größere Datensammlungen wegen ihres umfassenden Informationsgehalts auch für andere Zwecke als die, für die sie angelegt wurden, zu nutzen. Solche Nutzungserweiterungen sind mit Sicherheit vor allem bei sensiblen Daten, wie medizinischen, problematisch.

1. Weitere Datensammlungen, die nach ihrer Einrichtung Gegenstand
   von Interessen wurden, die mit dem ursprünglich vorgesehenen **Nutzungszweck** nicht übereinstimmen:
   - Die Sammlung der Kraftfahrzeughalterdaten beim Kraftfahrt bundesamt, deren Nutzbarkeit zu Werbungszwekken schon seit längerem erkannt wurde. Die Tätigkeit der Datenschutzbeauf tragten hat immerhin dazu geführt, daß der Antragsteller im Zulassungsantrag nun gefragt wird, ob er mit einer Weitergabe von Daten für Werbungszwecke einverstanden ist.
   - Datensammlungen von Energieversorgungsunternehmen über Strombezugskunden haben das Interesse der Polizei für Zwecke von Rasterfahndungen erweckt.
   - Die physisch zentrale, wenn auch rechtlich nicht gemeinsame Speicherung von Daten von Gemeinden bei der AKDB hat für Stellen, die sich hierzu die Einwilligung von Gemeinden einholen, die erheblich vereinfachte Möglichkeit geschaffen, Datenbestände relativ einfach zentral abzugleichen (siehe 3. Tätigkeitsbericht Nr. 2.5, S. 8/9).
   - Die Sammlung der Daten aus der Volkszählung 1983 schließlich hätte auf Grund des Volkszählungsgesetzes 1983 über den engen Rahmen einer rein statistischen Verwendung hinaus die Teil habe von obersten Landesbehörden, Gemeinden und wissenschaft lichen Stellen an Einzeldaten ermöglicht. Dies ist durch die einstweilige Anordnung des Bundesverfassungsgerichts derzeit ausgesetzt.

2. **An Projekten für größere Datensammlungen seien genannt**
   - die Planungen für Krebs- und andere Krankheitsregister (siehe 4. Tätigkeitsbericht Nr. 3.6.2 Seite 37 ff und dieser Bericht unter Nr. 4.2.4.),
   - die Einrichtung eines Mitgliederverzeichnisses nach § 319 a RVO (siehe diesen Bericht unter Nr. 4.2.4),
   - die Einrichtung von Steuerzentralen im Zusammenhang mit neuen Medien, in denen sich eine Vielzahl den persönlichen Bereich betreffender Informationen ansammeln dürfte (siehe Tätig keitsberichte Nr. 3/2.6 und Nr. 4/2.4), sowie
   - Vorhaben, alle irgendwie grundstücksbeziehbaren Verwaltungs daten in einer Datei zusammenzuführen, obwohl es keine Stelle der Verwaltung gibt, die zur Kenntnisnahme der gesamten Informationsmenge pro Grundstück bzw. je Eigentümer oder sonstiger beteiligter Personen zuständig wäre.

3. **Folgerungen aus dieser Anziehungskraft**

   Die Tatsache dieser Anziehungskraft größerer Datensammlungen auf weitere ursprünglich nicht vorgesehene Nutzungsinteressen muß meiner Ansicht nach bei jedem entsprechenden Projekt rechtzeitig berücksichtigt und durch entsprechende Maßnahmen aufgefangen werden. Dies setzt allerdings voraus, daß solche Maßnahmen auch möglich sind. In die Erwägung einzubeziehen wären daher meines Erachtens grundsätzlich auch Überlegungen, die durch Änderung in der Konzeption eine Herabsetzung dieser Anziehungskraft - unabhängig von allen rechtlichen oder technisch-organisatorischen Sicherungen - bewirken könnten. Ich meine damit auch die verantwortliche und bewußte Erwägung, von der Errichtung einer weiteren größeren oder einer zentralen Datei abzusehen.

   Insbesondere sind aber Bemühungen nötig, dieser Anziehungskraft eine dem jeweiligen Risiko für Betroffene oder die Allgemeinheit gerecht werdende Zweckbindung der Daten entgegenzustellen. Dabei dürfte es besonders schwierig sein, die Zulassung weiterer Nutzungen durch spätere Rechtsänderungen, etwa durch nachträgliches Einräumen von Befugnissen oder Pflichten zur Datenübermittlung, zuverlässig zu verhindern. Die Einräumung der Offenbarungserlaubnisse für Sozialdaten im X. Buch des Sozialgesetzbuches (Jahre nach der Festlegung des Sozialgeheimnisses in § 35 des I. Buches) ist ein Beispiel hierfür. Inzwischen zurückgezogene Bemühungen, die ärztliche Schweigepflicht im Interesse medizinischer Forschung generell aufzuheben, bieten ein weiteres Beispiel.

   Wichtig erscheint auch, Verknüpfungsmöglichkeiten zwischen Datenbeständen im Auge zu behalten, da nicht nur physisch in einer großen Datensammlung zusammengeführte Datenbestände entsprechende Nutzungen anziehen könnten, sondern auch einfach und preiswert verknüpfbare dezentrale Bestände. Die Schaffung technischer und organisatorischer Verknüpfungsmöglichkeiten muß daher besonderer Gegenstand der Aufmerksamkeit aus der Sicht des Datenschutzes sein. Als Beispiel für unsere Anstrengungen, dies in die Praxis umzusetzen, sei auf Regelungen im neuen Landesmeldegesetz zum Ordnungsmerkmal verwiesen. Sie sollen zu vermeiden helfen, daß sich das Ordnungsmerkmal der Meldeämter als allgemeines Verknüpfungsmerkmal im öffentlichen und gar im privaten Bereich etabliert. Verwiesen sei außerdem auf die Bemühungen, Bildschirmtextzentralen und andere Zentralen, die sich im Zuge der Einrichtung neuer Medien ergeben, vor einer zweckwidrigen Nutzung zu bewahren.

   Das Bundesverfassungsgericht hat in seinem Mikrozensusbeschluß das Phänomen der möglichen Betroffenheit des Einzelnen durch die Sammlung von Daten u.a. durch den treffenden Satz charakterisiert, daß eine Einsichtnahme in bestimmte Bereiche die freie Entfaltung der Persönlichkeit „durch den psychischen Druck öffentlicher Anteilnahme zu hemmen vermag". Dies halte ich für das zentrale Problem von Zweck- oder Nutzungserweiterungen insbesondere bei größeren Datensammlungen: Der Betroffene kann die zu erwartenden weiteren Nutzungen nicht mehr überblicken. Nutzungsänderungen können vielfältig sein; sie brauchen ihm nicht bekannt zu werden. Er wird daher, um schädliche Folgen der Datenspeicherung für seine berufliche oder persönliche Entwicklung abzuwehren, darum besorgt sein, daß nur solche Informationen über ihn gespeichert werden, die er vermeintlich für positiv hält, und schädigende erst gar

einer Einschränkung seiner natürlichen Lebensentfaltung führen. Dies gilt für Datensammlungen mit nicht überblickbarem variablem Zweck noch stärker als für Sammlungen, die nur einem klar überschaubaren sicher begrenzten Zweck dienen. Die Reaktion des Einzelnen kann so weit führen, daß er z.B. einen Arztbesuch - der möglicherweise nötig wäre - unterläßt, um zu vermeiden, daß über die Abrechnung der ärztlichen Leistung Informationen zu seiner Person in eine Datei gelangen, deren künftige Nutzung für ihn nicht vorhersehbar ist. Es kann aber auch zu anderen Verhaltensweisen - vor allem wohl Unterlassungen - führen, die bewirken sollen, daß in Dateien keine Spuren erzeugt werden. Diesem Phänomen könnte, soweit nicht überhaupt der Verzicht auf eine Datenspeicherung in Frage kommt, wohl nur durch strikte und unabänderbare Zweckbindung entsprechender Datensammlungen angemessen Rechnung getragen werden.

1.2 Weitere Einflußfaktoren

Als weitere Einflußfaktoren seien hervorgehoben:

- Umverteilungsmaßnahmen des Staates werden in der Regel durch Daten gesteuert, die die Betroffenen anzugeben haben. Mit der Zunahme solcher Maßnahmen steigt das staatliche Wissen über Einzelne und damit u.U. die Versuchung, die erhobenen Daten auch anderweitig zu nützen.
- In Zeiten wirtschaftlicher Engpässe verstärkt sich die Notwendigkeit zur Überprüfung staatlicher Leistungen, so daß zur Empfangsberechtigung weitere Differenzierungen eingeführt werden, die wiederum Datenerhebung, -speicherung und Übermittlung verursachen können. Als Beispiele seien die jüngste Datenerhebung zum Kindergeld erwähnt, sowie die erleichterte Möglichkeit zur Übermittlung von Sozialdaten für die Bekämpfung der Schwarzarbeit.
- Sicherheitsbehörden könnten künftig noch mehr Daten sammeln, da der neue maschinenlesbare Personalausweis nicht nur die tatsächliche Möglichkeit zu mehr Kontrollen eröffnet, sondern auch deren Festhalten in entsprechenden Dateien erleichtert. Auf der Basis der strikten Anwendung des Verhältnismäßigkeitsgrundsatzes werden hier Beschränkungen eingeführt werden müssen.

1.3 Technische und organisatorische Entwicklungen

Auch technische und organisatorische Entwicklungen haben Einfluß auf die Entwicklung des Datenschutzes:

- Die Vereinfachung der Datenerhebung, beispielsweise künftig durch den maschinenlesbaren Personalausweis, die Vielfalt der Übermittlungsmöglichkeiten durch die Einführung neuer Medien und die Verbilligung der Datenspeicher werden Datensammlungen und -bewegungen in neuen Bereichen entstehen lassen und die Vergrößerung bestehender Datensammlungen fördern. Damit ergeben sich auch neue Datenschutz-Aufgaben.
- Die zunehmende Verbreitung der Datenverarbeitung über die großen Rechenzentren hinaus zu weiteren kleineren dezentralen ADVLösungen „vor Ort" kann die Einhaltung von Verantwortlichkeiten fördern wie z.B. bei Einsatz von Kleincomputern im medizinischen Bereich. Sie könnte einen Schritt weg von der Tendenz zur Einrichtung großer Datensammlungen bedeuten, wenn und so lange nicht die Verknüpfung einer Vielzahl kleiner Einheiten letztlich den gleichen Effekt bewirkte - mit dem Ergebnis, daß die Datenverarbeitung insgesamt weniger transparent und kontrollierbar werden könnte.
- Auch die Dynamik der Datenverarbeitungs-Organisation und Programmierung ist nicht ohne Wirkung:

  Je mehr Arbeitsbereiche automationsunterstützt werden können, je mehr also automatisiert machbar wird, desto mehr könnte sich die Tendenz verbreiten, daß ADV-Spezialisten, insbesondere, soweit sie nicht aus der Tradition der jeweiligen Verwaltung kommen, Arbeitsabläufe umgestalten, ohne die rechtlichen Vorbedingungen und den Rahmen - gewissermaßen die Daten-Umwelt -, in die das Verfahren gesetzt wird, voll einzubeziehen. Die Anpassung von Rechtsvorschriften ist dann in vielen Fällen Aufgabe Anderer, die teilweise die ursprünglich vorhandene Flexibilität der möglichen ADV-Anwendungen nicht kennen und daher eine durch das automatisierte Verfahren festgelegte neue Struktur als weitgehend unveränderlich in die neue Rechtsnorm übernehmen.

  Es sei auch auf manche ADV-Bescheide verwiesen, die feststellenden Teil und Begründungen nicht mehr zu unterscheiden erlaubten. Erwähnt sei die Automation des Einwohnermeldewesens und der PK-Vergabe, die weit vorangetrieben war, als sich herausstellte, daß die dafür notwendigen Gesetze so nicht erlassen werden würden, die aber gleichwohl Festlegungen für das neue Melderecht brachten. Beispielsweise waren kirchliche Rechenzentren bereits an die Übermittlung von Meldedaten mit einem Ordnungsmerkmal zur leichteren Zuordnung gewöhnt, als über den Umfang der rechtlich zuzulassenden Übermittlung dieses Ordnungsmerkmals beim Erlaß der Landesmeldegesetze Erörterungen im Parlament stattfanden. Erwähnt sei auch das Beispiel der Vorbereitungen für die Einführung des maschinenlesbaren Personalausweises. Hier waren offenbar wesentliche Komponenten des Verfahrens schon so fixiert, daß der Gesetzgeber gezwungen war, die Speicherung von Antragsdaten in einer Zentrale für das Bundesgebiet zu erlauben - wenn auch nur für kurze Zeit, während des Herstellungsverfahrens.

  Ergebnis gesetzlicher Normierungen von ADV-Verfahren kann sein, daß ein begrenzender Effekt nur in Bereichen wirksam wird, in denen zu realisieren und durch entsprechende Investitionen in die Tat umzusetzen im Rahmen des ADV-Projektes bis dahin unterlassen wurde. Das entwickelte Verfahren wird dagegen in der Regel 1:1 im Gesetz abgebildet.

  Es wäre zu hoffen, daß die Regelung des Art. 26 Abs. 2 und 4 des Bayer. Datenschutzgesetzes, nach der verfahrensmäßig abzusichern ist, daß Anforderungen des Datenschutzes bereits vor der Erstellung des Detailkonzepts eines ADV-Projekts geprüft und berücksichtigt werden müssen, zur Durchsetzung von Datenschutzforderungen führt. Dabei muß nach den bisherigen Erfahrungen wohl noch mehr Gewicht auf eine zufriedenstellende Beantwortung folgender Fragestellung gelegt werden: Kann ein zunächst harmloses ADV-Vorhaben durch nicht zu verhindernde Zweckänderungen ganz andere Dimensionen erhalten, oder gelingt es, Zweckbindungen festzulegen und für ihre Beachtung auch in der Zukunft zu sorgen, damit unerwartete Auswirkungen verhindert werden können?

  Für die Vorlage von Gesetzentwürfen wäre zu fordern, daß im Vorblatt des Entwurfs nicht nur die Frage nach Kosten und Alternativen der vorgesehenen Regelungen, sondern auch Fragen nach Datenerhebung und Datennutzung, beantwortet werden und auch auf allgemeine Folgen des Vorhabens für die Situation des Datenschutzes, gewissermaßen zur Änderung der „Datenschutzbilanz" für die Betroffenen, eingegangen wird.

Der Rückblick sei mit dem Hinweis auf eine wesentliche Änderung abgeschlossen, nämlich der ab 1.1.1983 eingetretenen:

1.4 Bindung der Datenverarbeitung an eine Rechtsnorm

Das Bayer. Datenschutzgesetz verlangt für die Zulässigkeit der Datenverarbeitung personenbezogener Daten in einer Reihe von Bestimmungen das Vorliegen einer durch Rechtsnorm der datenverarbeitenden Stelle zugewiesenen Aufgabe. So sind insbesondere die Datenspeicherung (Art. 16 Abs. 1 BayDSG) und die Datenübermittlung (Art. 17 Abs. 1 und Art. 18 Abs. 11. Alternative BayDSG) nur zulässig, wenn sie zur rechtsmäßigen Erfüllung der durch Rechtsnorm einer Stelle zugewiesenen Aufgaben erforderlich sind. Weitere Vorschriften des Bayer. Datenschutzgesetzes, die das Vorliegen einer durch Rechtsnorm zugewiesenen Aufgabe verlangen, sind Art. 8 Abs. 3 Nr. 1 BayDSG (Beschränkung des Auskunftsanspruchs), Art. 11 Nr. 2 BayDSG (Löschungsanspruch) und Art. 20 Abs. 1 und 3 BayDSG (Sperrung und Löschung von Daten). Gemäß Art. 37 Abs. 3 Satz 1 BayDSG genügte es bis zum 1. Januar 1983, wenn die vorgenannten Aufgaben „öffentliche" Aufgaben waren. Diese Übergangsregelung ist, von einigen Sonderfällen in Art. 37 Abs. 3 Satz 2 BayDSG abgesehen, nun seit 1. Januar 1983 außer kraft getreten. Mit der nun geltenden Bindung der Datenverarbeitung an eine Rechtsnorm geht das Bayer. Datenschutzgesetz in einer vorbildlichen Weise über die vergleichbaren Regelungen des Bundesdatenschutzgesetzes und anderer Landesdatenschutzgesetze hinaus. Grundlegende Probleme haben sich auf Grund dieser nun notwendigen normativen Aufgabenzuweisung nicht ergeben. Der für die Datenverarbeitung uneingeschränkt geltende spezielle Gesetzesvorbehalt des Bayer. Datenschutzgesetzes ist in den meisten Bereichen der ohnehin weitgehend gesetzesakzessorischen Verwaltung erfüllt. Probleme könnten sich im Bereich der leistungsgewährenden Verwaltung dort ergeben, wo diese sich nicht auf eine spezialgesetzliche Grundlage stützt. Darüber hinaus sind im Einzelfall Schwierigkeiten dort nicht auszuschließen, wo von bayerischen Stellen Daten an Bundesbehörden oder öffentliche Stellen anderer Länder übermittelt werden, denen nicht ausdrücklich auf Grund eines Gesetzes Aufgaben zugewiesen sind. In diesem Zusammenhang habe ich festgestellt, daß - anders als in Art. 77 Bayer. Verfassung - im Grundgesetz und in einigen Landesverfassungen eine ausdrückliche Vorschrift fehlt, die eine Regelung des Verwaltungsaufbaus, der Behördenzuständigkeiten oder des Verwaltungsverfahrens durch Gesetz fordert.

Auf eine entsprechende Anfrage bei den bayerischen Staatsministerien nach einer eventuellen Datenverarbeitung, die nicht auf Grund einer durch Rechtsnorm zugewiesenen Aufgabenerfüllung vorgenommen wird, haben die Ministerien überwiegend mitgeteilt, daß eine derartige Datenverarbeitung nicht stattfindet, bzw. das Inkrafttreten der neuen Bestimmung die Datenverarbeitung nicht wesentlich erschwert oder gar in Frage stellt. Das Bayer. Staatsministerium für Wirtschaft und Verkehr hat für den Subventionsbereich darüber hinaus mitgeteilt, daß - soweit noch nicht geschehen - beabsichtigt sei, in den entsprechenden Antragsformularen die Einwilligung des Betroffenen gem. Art. 4 Abs. 1 Ziff. 2 BayDSG einzuholen.

2. Vorbemerkungen zum 5. Tätigkeitsbericht

2.1 Der Beirat

Der gemäß Art. 29 BayDSG beim Landesbeauftragten für den Datenschutz gebildete Beirat hat sich in den ersten 4 Jahren seines Bestehens zu einem gewichtigen Instrument entwickelt. Die trockene Aussage in Art. 29 Abs. 2 BayDSG „Der Beirat unterstützt den Landesbeauftragten für den Datenschutz in seiner Arbeit" wurde durch die Aktivität des Beirats-Vorsitzenden, Abgeordneter Hermann Regensburger, des stellvertretenden Beirats-Vorsitzenden, Abgeordneter Klaus Warnecke und der Mitglieder des Beirats in vielfältiger Weise mit Leben erfüllt. Die Beiratsmitglieder, vor allem die Abgeordneten, stellten immer wieder Datenschutzfragen zur Debatte, die ihnen aus ihrer täglichen Arbeit bekannt wurden und die den Landesbeauftragten für den Datenschutz sonst möglicherweise nicht erreicht hätten. Der Beirat erörterte außerdem schwerpunktmäßig Entwicklungen der EDV-Technik und des Rechts, die Auswirkungen auf den geschützten Persönlichkeitsbereich zeigen, wie z.B. die Einführung neuer Medien, die Neugestaltung des Melderechts, die Abwägung zwischen Erfordernissen von Sicherheitsbehörden und Notwendigkeiten des Schutzes der Privatsphäre, oder Gefahren einer Einschränkung des Arztgeheimnisses. Die Erörterung der Beanstandungen von Verletzungen von Vorschriften über den Datenschutz erhöht deren Gewicht. Schließlich gibt die Beratung des Entwurfs eines jeden Tätigkeitsberichtes dem Landesbeauftragten für den Datenschutz Hinweise für die Schlußredaktion des Berichts.

Die dem Landtag angehörenden Mitglieder des Beirats werden jeweils für die Wahldauer des Landtags bestellt, die übrigen Mitglieder jeweils für 4 Jahre. Nach der Landtagswahl im Herbst 1982 sind die Mitglieder des Beirats neu bestellt worden. Mitglieder des Beirats und ihre Stellvertreter sind danach gegenwärtig:

Die Landtagsabgeordneten:

Hermann Regensburger	Dr. Paul Wilhelm
Franz Josef Brosch	Manfred Humbs
Wolfgang Dandorfer	Johann Böhm
Franz Gruber	Konrad Kobler
Klaus Warnecke	Rolf Langenberger
Alfred Münch	Heinz Mehrlich

Die Senatoren:

Wolfgang Burnhauser	Otto Neukum

Für die Staatsregierung:

Dr. Friedrich Giehl Ministerialdirigent im Bayer. Staatsministerium des Innern	Dr. Werner Böhme Ministerialrat im Bayer. Staatsministerium der Finanzen

Für die Kommunalen Spitzenverbände:

Dr. Georg Wilhelm Geschäftsleitender Direktor der Anstalt für Kommunale Datenverarbeitung in Bayern	Klaus Eichhorn Ltd. Verwaltungsdirektor der Anstalt für Kommunale Datenverarbeitung in Bayern

Für die Sozialversicherungsträger:

Franz-Martin Fehn Erster Direktor der Landesversicherungs- anstalt Oberfranken und Mittelfranken	Herbert Schmaus Verwaltungsdirektor beim Landesverband der Orts- krankenkassen in Bayern

Für den Verband der Freien Berufe in Bayern e.V.:

Dr. med. H. Braun Präsident des Verbandes Freier Berufe in Bayern e.V.	Winfried Wachter Präsidiumsmitglied des Verbandes Freier Berufe in Bayern e.V.

Der Beirat tagte im Berichtsjahr 1982 dreimal, und zwar am 19. Januar, 20. April und, wegen des Endes der Legislaturperiode, zum letztenmal am 18. Mai 1982. Er befaßte sich in seinen Sitzungen mit folgenden Fragen:

- Unterrichtung über den Sachstand bei den „Neuen Medien",
- Besichtigung des Bildschirmtextsystems beim Landwirtschaftsministerium,

- Unterrichtung des Beirats über Beanstandungen von Verstößen gegen Datenschutzvorschriften gem. Art. 29 Abs. 5 Satz 2 BayDSG,
- Vorberatung des 4. Tätigkeitsberichtes des Landesbeauftragten für den Datenschutz gem. Art. 28 Abs. 4 und 6 BayDSG,
- Stand der Diskussion zu Gesetzesentwürfen für Krebsregister,
- Sicherung der Intimsphäre der Petenten bei der Beratung von Eingaben im Ausschuß für Eingaben und Beschwerden des Bayer. Landtags,
- Beratung des Entwurfs eines Bayer. Meldegesetzes,
- Erörterung des Entwurfs eines Gesetzes zur Änderung des Bundesdatenschutzgesetzes,
- personelle Veränderungen in der Geschäftsstelle des Landesbeauftragten für den Datenschutz und Umzug der Geschäftsstelle.

Zur Tätigkeit des Beirats siehe im übrigen in den Tätigkeitsberichten I unter 1.4, II unter 1.3, III unter 1.2.1 und IV unter 1.5.

2.2 **Behandlung des 4. Tätigkeitsberichts im Parlament**

Der Ausschuß für Verfassungs-, Rechts- und Kommunalfragen des Bayerischen Landtags beriet über den 4. Tätigkeitsbericht in der Sitzung am 15. Juli 1982. Dabei wurde das Bestreben des Landesbeauftragten für den Datenschutz anerkannt, gemeinsam mit der öffentlichen Verwaltung Lösungen zu finden, die die Belange des Datenschutzes nachhaltig berücksichtigen und gleichzeitig einen praktikablen Verwaltungsvollzug erlauben. Der Ausschuß erkannte auch das Bestreben an, öffentliche Auseinandersetzungen, die zu einer Verhärtung unterschiedlicher Auffassung führen und einen sinnvollen Kompromiß erschweren können, zu vermeiden, wobei der laufenden Erörterung schwieriger Datenschutzfragen im Datenschutz-Beirat besondere Bedeutung zukommt. Diese Beratung stellt ein Äquivalent für eine gewisse Zurückhaltung gegenüber öffentlichen Auseinandersetzungen dar.

Die beiden Berichterstatter, MdL Regensburger und MdL Warnecke stellten übereinstimmend fest, daß es im Berichtszeitraum nicht Datenschutzskandale gegeben habe, wohl aber vereinzelte Verstöße. Diese beruhten in der Regel auf mangelnder Erkenntnis der Datenschutzprobleme oder auf der Kompliziertheit oder Neuheit dieser Materie, sie belegten andererseits aber auch die Notwendigkeit des Datenschutzgesetzes und der Datenschutzkontrolle. Gegenstand der Erörterung im Ausschuß waren die Frage der Novellierung des Bundesdatenschutzgesetzes, die Tatsache, daß der Dateibegriff zwar in der theoretischen Auseinandersetzung, nicht aber in der Praxis eine Rolle gespielt hatte und der Datenschutzbeauftragte jederzeit Zugang zu den von ihm gewünschten Akten erhielt. Erörtert wurden auch die umfangreichen Datenschutzprobleme im Zusammenhang mit der Entwicklung der Neuen Medien, die Arbeit des Landesbeauftragten und des Beirats am Entwurf für ein neues Landesmeldegesetz, die Speicherung von Namen der Benutzer in Bibliotheken, die Speicherung von Daten über Telefongespräche und die Zustellung sensibler Informationen auf offenen Postkarten. Ein weiterer Schwerpunkt der Erörterungen betraf den Datenschutz im Bereich der Sicherheitsbehörden.

Berichterstatter und Mitberichterstatter hoben die umfängliche und gute Zusammenarbeit im Beirat und mit dem Landesbeauftragten für den Datenschutz hervor.

2.3 **Arbeitsbedingungen der Geschäftsstelle**

Der von mir angestrebte Personalstand ist fast erreicht Die Schwierigkeiten, geeignete Mitarbeiter zu finden, haben zwar die Besetzung der im Haushaltsplan ausgebrachten Stellen nicht unwesentlich verzögert, doch wird - nach der erkennbaren auf Dauer zu erwartenden Arbeitsbelastung bemessen - eine weitere Stellenvermehrung nicht angestrebt: Bei normalem Arbeitsablauf kann die Arbeit mit den zur Zeit vorhandenen bzw. noch zu erwartenden Mitarbeitern durchaus bewältigt werden. Sonderaktionen, etwa die jährliche Abfassung des Tätigkeitsberichts oder Stellungnahmen für das Bundesverfassungsgericht (Volkszählungsgesetz) erfordern jedoch oft von den Mitarbeitern einen Arbeitseinsatz weit über die normalen Dienststunden hinaus. Dies muß im Hinblick auf die angespannte Haushaltslage in Kauf genommen werden.

Der Umzug der Geschäftsstelle im Januar 1982 von der Königinstraße in die Wagmüllerstraße 18 hat den Bedürfnissen entsprechende Arbeitsräume gebracht. Sie vermeiden Reibungen, die sich bei zu gedrängter Unterbringung zwangsläufig ergeben. Die Dienststelle ist auch für Bürger, die Rat suchen oder in das Datenschutzregister Einblick nehmen wollen, gut erreichbar. Das Datenschutzregister konnte dabei auch in einem eigenen Raum, räumlich von der Registratur getrennt, untergebracht werden.

2.4 **Konferenz der Datenschutzbeauftragten**

Die Konferenz der Datenschutzbeauftragten der Länder und des Bundes tagte im Berichtsjahr in Stuttgart. In den Tagungen am 17.4., 21.6. und 28.9.1982 wurden wiederum eine Reihe gemeinsam interessierender Fragen erörtert. Beispielhaft zu nennen sind die gemeinsame Arbeit an einer Stellungnahme zu einem Referentenentwurf zur Novellierung des BDSG (der dann jedoch nicht als Regierungsentwurf eingebracht wurde), zur Novelle des Landesdatenschutzgesetzes Baden-Württemberg, zum Staatsvertrag Bildschirmtext, zum Musterentwurf eines Krebsregistergesetzes (das in dieser Form nunmehr nicht mehr weiter verfolgt wird), über Empfehlungen zur Sicherstellung des Datenschutzes im Archivwesen, zum Datenschutz im Sicherheitsbereich, zu Fragen des Datenschutzes im Bereich der Steuerverwaltung, über die gegenseitige Verständigung unter den Datenschutzbeauftragten über Schwachstellen bei Basissoft- und Hardware und überregional zum Einsatz kommende Anwendungsverfahren.

Die Empfehlungen zum Datenschutz im Archivwesen sind unter Punkt 4.12.1 abgedruckt.

Im Vorgriff auf den Tätigkeitsbericht für das Jahr 1983 ist wegen seiner Wichtigkeit der Beschluß der Konferenz zur Volkszählung 1983 in der Anlage wiedergegeben.

3. **Volkszählung: Überlegungen zum Erlaß einer einstweiligen Anordnung**

Zum Stichtag 27. April 1983 hätte die Volks- und Berufszählung 1983 durchgeführt werden sollen. Gegen das Volkszählungsgesetz 1983 vom 4. März 1982 wurden beim Bundesverfassungsgericht Verfassungsbeschwerden erhoben, mit denen die Verletzung von Grundrechten durch das Gesetz gerügt und beantragt wurde, den Vollzug des Volkszählungsgesetzes 1983 bis zur Entscheidung über die Verfassungsbeschwerden im Wege der einstweiligen Anordnung auszusetzen.

Die Landesbeauftragten und der Bundesbeauftragte für den Datenschutz waren vom Bundesverfassungsgericht aufgefordert worden, sich zu den Beschwerden und zum Antrag auf einstweilige Anordnung zu äußern. Für die Entscheidung über den Antrag auf einstweilige Anordnung war zu prüfen, ob es „zur Abwehr schwerer Nachteile oder aus einem anderen wichtigen Grund zum gemeinen Wohl dringend geboten" war, „einen Zustand vorläufig zu regeln". Die Untersuchung erstreckte sich also darauf, ob Maßnahmen im Rahmen der Volkszählung vor der Entscheidung in der Hauptsache in Form von schweren

Nachteilen für Betroffene oder im Hinblick auf die Gründe des allgemeinen Wohls vollendete Tatsachen schaffen würden.

In meiner Äußerung gegenüber dem Gericht konnte ich davon ausgehen, daß eine Auswertung der Statistikdaten erst nach Ende der Aufbereitungs- und Bereinigungsphase Ende des Jahres 1984 frühestens möglich gewesen wäre. Die nach § 9 Abs. 2 - 4 VZG 1983 mögliche Nutzung von Volkszählungsdaten hätte daher nicht begonnen, bevor eine Entscheidung des Bundesverfassungsgerichts in der Hauptsache zu erwarten war. Die Entscheidung ist mittlerweile für Herbst 1983 in Aussicht gestellt worden.

Wegen der Bedeutung der Angelegenheit sei im Vorgriff auf den Tätigkeitsbericht für 1983 nachfolgend kurz über von mir vorgetragene Punkte berichtet:

Zu dem in § 9 Abs. 1 VZG 1983 vorgesehenen Melderegisterabgleich habe ich in meiner schriftlichen Stellungnahme zum Antrag auf einstweilige Anordnung die Ansicht vertreten, daß belastende Maßnahmen öffentlicher Stellen, die aufgrund der Berichtigung des Melderegisters erlassen werden könnten, jedenfalls in Rechtsbehelfsverfahren anfechtbar wären, so daß endgültige, erhebliche Nachteile bis zum Erlaß der Hauptsache-Entscheidung des Bundesverfassungsgerichts wohl nicht eintreten würden.

In meinem mündlichen Vortrag habe ich noch auf die beiden folgenden Punkte hingewiesen:

- Wäre es dem Gesetzgeber aus verfassungsrechtlichen Gründen verwehrt, gesetzlich eine Befragung anzuordnen, allein zu dem Zweck, die Melderegister auf den neuesten Stand zu bringen? Und würde - wenn dies für zulässig gehalten würde - die Verbindung einer solchen Befragung zur Korrektur der Melderegister mit einer allgemeinen statistischen Erhebung den gesamten Vorgang der gemeinsamen Datenerhebung für Statistik und Meldeamt verfassungswidrig machen? Die Verbindung von Statistik und Verwaltungsvollzug ist unserer Rechtspraxis nicht völlig fremd. So bestehen eine ganze Reihe von Verwaltungsverfahren, aus deren Daten statistische Erhebungen gespeist werden. Die Tendenz, statistische und planerische Daten als Nebenprodukt aus dem Verwaltungsvollzug zu gewinnen, hat im übrigen in den vergangenen Jahren stetig zugenommen.
- Im Zusammenhang mit dem Melderegisterabgleich ist weiter zu prüfen, inwieweit sich die nicht eben sehr klare Formulierung in § 9 Abs. 1 Satz 2 VZG auf die verfassungsrechtliche Bewertung des § 9 Abs. 1 Satz 1 VZG auswirkt. Dabei stellt sich auch die Frage, ob gegen die gesetzliche Anordnung des Melderegisterabgleichs auch dann keine verfassungsrechtlichen Bedenken beständen, wenn der Gesetzgeber von dem in § 9 Abs. 1 Satz 2 VZG formulierten Versprechen abgesehen hätte, daß die Bürger keine nachteiligen Maßnahmen zu erwarten hätten.

Besonders hingewiesen habe ich auf die meiner Ansicht nach möglicherweise besonders problematische Frage der Alternativen zur Datenerhebung durch eine Volkszählung:

Sollte die Volkszählung aufgeschoben oder aufgehoben werden, bin ich überzeugt, daß die öffentliche Verwaltung sowohl zur Gewinnung aktueller Adreßdaten als auch für statistische und planerische Zwecke nach anderen Wegen suchen wird, um an die Daten zu gelangen, die im Rahmen der Volkszählung erhoben werden sollten. Ich meinte, daß auch im Rahmen der Entscheidung über die einstweilige Anordnung, und zwar bei der Auseinandersetzung mit dem Verhältnismäßigkeitsgrundsatz, diese Befürchtungen berücksichtigt werden müßten:

- So könnte ein Druck auf den Gesetzgeber entstehen, zur Gewinnung aktuellerer Daten als der teilweise unrichtigen Angaben des Melderegisters, die Datensammlungen anderer Behörden für Zwecke zur Verfügung zu stellen, die eigentlich nur das Melderegister zu erfüllen hat. Im Bereich der sensiblen Sozialdaten hat der Gesetzgeber einem solchen Druck bereits nachgegeben, wie §§ 68 ff SGB X beweisen. Auch die Verwaltungspraxis würde sich dem anpassen. Je unzutreffender die Melderegisterangaben werden, desto mehr Anfragen beispielsweise der Polizei und anderer Behörden sind bei den Allgemeinen Ortskrankenkassen zu erwarten. Der Gesetzgeber ging zwar in § 68 Abs. 1 Satz 2 SGB X davon aus, daß zunächst das Melderegister zu befragen sei und Sozialleistungsträger nur subsidiär zur Hilfe verpflichtet seien. Dieses Regel-Ausnahme-Verhältnis dürfte sich in einer aus der Sicht des Datenschutzes bedenklichen Weise immer mehr umkehren, je inaktueller die Melderegister werden.
- Hinsichtlich der eigentlichen Volkszählungsdaten wäre auch zu befürchten, daß Anstrengungen unternommen würden, alle diese Angaben aus bereits vorhandenen Unterlagen, Karteien und Dateien der verschiedenen Verwaltungszweige zusammenzuführen. Dies setzte zwar voraus, daß technische, organisatorische und rechtliche Maßnahmen getroffen würden, die es erst erlauben würden, diese Daten, bezogen auf eindeutig bestimmte Personen, zusammenzuführen. Vorüberlegungen in dieser Richtung wurden aber Anfang der 70-er Jahre bereits im Zusammenhang mit verschiedenen Landes- oder Bundesinformationssystemen angestellt. Diese Überlegungen waren damals nicht mehr weiter verfolgt worden, als der Bundestag - wohl aus verfassungsrechtlichen Gründen - von der Einführung eines allgemeinen Personenkennzeichens durch ein Bundesmeldegesetz absah. Wären die für Statistik und Planung benötigten Daten aber nur noch über die Zusammenführung entsprechender Daten aus verschiedenen Verwaltungszweigen zu erlangen, so würden solche Überlegungen wohl wieder aufleben. Dabei wäre noch ungewiß, ob ein entsprechendes Verknüpfungsmerkmal überhaupt durch Gesetz eingeführt würde.

  Ein einmal eingeführtes Verknüpfungskennzeichen oder eine andere Möglichkeit, die Daten zusammenzuführen, würde es erlauben, nicht nur die für die Volkszählung benötigten Angaben zusammenzuführen, sondern auch alle anderen Daten, die in den mit dem Kennzeichen ausgestatteten Dateien enthalten sind. Damit wäre aber endgültig die Erstellung verfassungsrechtlich bedenklicher Persönlichkeitsprofile möglich.

  Wenn die Erhebung bestimmter, alle Bürger betreffender personenbezogener Daten im Einzelfall erforderlich und verhältnismäßig ist, gebe ich daher einer Datenerhebung im Wege der Volkszählung den Vorzug gegenüber einer problematischen Auswertung und Aufbereitung vorhandener Dateien der Verwaltung.

Zu den Nutzungen von statistischen Daten entsprechend § 9 Abs. 2 - 4 VZG habe ich in der mündlichen Verhandlung die Ansicht vertreten, daß diese wesentlich problematischer sein könnten, als der im Datenumfang beschränkte Melderegisterabgleich. Die Gefahr, daß Volkszählungsdaten mit Datenbeständen der Verwaltung zusammengeführt werden könnten, muß daher zuverlässig ausgeschlossen werden. Ich meine zwar, daß das Volkszählungsgesetz 1983 in Verbindung mit dem Bundesstatistikgesetz so auszulegen ist, daß Nutzungen nach § 9 Absätzen 2 - 4 VZG entsprechend dem Grundsatz des § 11 des Bundesstatistikgesetzes auf rein statistisch-planerische Nutzungen zu reduzieren sind, und daß das VZG 83, abgesehen von § 9 Abs. 1, hiervon keine Ausnahme vorsieht. Trotzdem würde ich jedoch eine entsprechende Absicherung dieser Ansicht durch einen Beschluß des Bundesverfassungsgerichts im Interesse aller Beteiligten begrüßen. Damit könnte der Datenschutz bei Unklarheiten im Zusammenhang

mit Datennutzungen im Grenzbereich zwischen Verwaltungsvollzug und Statistik wirkungsvoller durchgesetzt werden.

In meiner Beurteilung der Volkszählung bin ich - übrigens auch mit dem Bundesbeauftragten für den Datenschutz - davon ausgegangen, daß die Datenschutzbeauftragten keine Befugnis haben, Gesetze vor dem Bundesverfassungsgericht anzufechten, so daß sie vor der Entscheidung des Gerichts nur auf eine verfassungskonforme und datenschutzgerechte Durchführung des vom Bundestag beschlossenen Gesetzes hinwirken konnten. Dies war in intensiven Verhandlungen mit dem Bayer. Staatsministerium des Innern, dem Bayer. Landesamt für Statistik und Datenverarbeitung und einzelnen Kommunen geschehen. Die von der Konferenz der Datenschutzbeauftragten der Länder und des Bundes in ihrer Sitzung am 22. März 1983 in Bremerhaven verabschiedeten 15 Forderungen zur Durchführung der Volkszählung (siehe Teil II des diesem Tätigkeitsbericht anliegenden Konferenzbeschlusses) wären aufgrund der mit den zuständigen Stellen getroffenen Vereinbarungen nach meiner Erkenntnis in Bayern im Wesentlichen eingehalten worden. Dieser Konferenzbeschluß endet mit der Aussage, daß nach Überzeugung der Datenschutzbeauftragten die Sorgen der Bürger im wesentlichen unbegründet gewesen wären, wenn diesen Forderungen der Datenschutzbeauftragten Rechnung getragen wurde. Ich teile die Ansicht des Bundesbeauftragten für den Datenschutz, der festgestellt hat, daß die Risiken für den einzelnen Bürger bei einer Volkszählung, die entsprechend den Forderungen der Datenschutzbeauftragten durchgeführt wird, sehr viel geringer sind als bei vielen anderen Formen personenbezogener Datensammlungen und -auswertungen. Ich sehe darüber hinaus die dringende Notwendigkeit, in die Prüfung der Verhältnismäßigkeit der mit der Volkszählung verbundenen Eingriffe die alternativen Formen staatlicher Datenerhebung, die als Ersatz für eine Volkszählung in Frage kommen könnten, mit einzubeziehen.

Nachdem das Bundesverfassungsgericht durch sein Urteil die Durchführung der Volkszählung einstweilen ausgesetzt hat, steht mit Sicherheit eine für die Weiterentwicklung der Datenverarbeitung und des Datenschutzes bedeutsame Entscheidung heran. Die Entscheidung über die einstweilige Anordnung ist zunächst eine Bestätigung für unseren Rechtsstaat. Ich begrüße es, daß das Bundesverfassungsgericht nach der Aussetzung in Ruhe alle aufgeworfenen Datenschutzfragen erörtern und klären kann.

Zu klären sind aus meiner Sicht vor allem Fragen der Nutzung der erhobenen Daten durch andere Stellen als das Statistische Landesamt selbst, also Fragen der richtigen Auslegung des § 9 des Volkszählungsgesetzes 1983 und darin eingeschlossen die wichtige Frage, wie weit Statistik und Verwaltungsvollzug in der Praxis zu trennen sind.

Auch geklärt werden muß die Bedeutung des Verbots nachteiliger Maßnahmen aus § 9 Abs. 1 Satz 2 VZG 1983, die bisher unklar blieb. Schließlich ist von der Hauptsache-Entscheidung des Bundesverfassungsgerichts auch eine Äußerung darüber zu erwarten, ob die vorgesehene Erhebung der 37 Angaben pro Person sowohl hinsichtlich der Einzeldaten, als auch hinsichtlich der Summe der Informationen pro Person die Grenze des hinzunehmenden Eingriffs berührt. Von Bedeutung ist in diesem Zusammenhang der Umfang der Weitergabe von Daten an andere Stellen und die Bindung dieser Datenempfänger an eine ausschließlich statistisch-planerische Nutzung sowie an das Verbot einer personenbezogenen Nutzung.

4. Bericht zur Datenschutzkontrolle im rechtlichen Bereich

4.1 Neue Medien

Zu den Datenschutzfragen bei Neuen Medien habe ich grundsätzliche Ausführungen bereits in meinen letzten beiden Tätigkeitsberichten gemacht. Dabei habe ich auf die verschiedenen Ausprägungen der Neuen Medien hingewiesen:

- Videotext
- Bildschirmtext
- Satellitenfernsehen
- Kabelfernsehen
- Kabeltext

Von aktueller Datenschutzbedeutung ist zum einen die für Herbst 1983 geplante bundesweite Einführung des Mediums „Bildschirmtext" und der für Herbst 1983 geplante Start des Kabelpilotprojekts München.

4.1.1 Bildschirmtext

4.1.1.1 Umfangreiche Nutzungsformen

Bildschirmtext erlaubt umfangreiche Nutzungsformen. Beispielhaft seien genannt:

Warenbestellungen in Kaufhäusern,
Informationsabrufe,
Überweisungsverkehr mit Banken und Sparkassen,
Buchungen von Reisen,
Tests bei psychologischen Instituten,
mathematische Berechnung von Renten und Steuern,
Finanzierungsberatung.

Damit fallen bei Benutzung des Bildschirmtextes viele personenbezogene Daten an.

4.1.1.2 Neue Gefahren

Aus der Sicht des Datenschutzes zu beobachtende neue Gefahren für die durch Art. 1 Abs. 1, Art. 2 Abs. 1 GG geschützte Privatsphäre liegen bei der Benutzung von Bildschirmtext in erster Linie in der technisch grundsätzlich möglichen umfassenden Sammlung personenbezogener Daten in den technischen Einrichtungen, die zur Nutzung von Bildschirmtext bereitgestellt werden. Über diese technischen Einrichtungen wird die vollständige Kommunikation zwischen den Anbietern und den Teilnehmern abgewickelt. Über diese Einrichtungen gehen alle Angebotsanforderungen, fließen alle ausgetauschten Daten und wird die Gebührenrechnung abgewickelt. Aus diesen dabei angefallenen Daten können Rückschlüsse auf das Lebensverhalten des Einzelnen gezogen werden. Darüber hinaus könnte festgestellt werden, wann der einzelne Teilnehmer zuhause gewesen ist und mit welcher Geschicklichkeit er sich beispielsweise im BildschirmtextSuchbaum zurechtgefunden hat.

Aus datenschutzrechtlicher Sicht ist zusätzlich folgendes zu berücksichtigen:

Bei Benutzung von Bildschirmtext werden Lebenssachverhalte individualisiert, die bisher zum großen Teil anonym, nämlich ohne Kenntnis des Vertragspartners abgewickelt worden sind. Gleichzeitig werden diese individualisierten Lebenssachverhalte zentral erfaßt. Dies gilt beispielsweise, wenn statt des Kaufs einer Zeitschrift am Kiosk der Inhalt der Zeitschrift über Bildschirmtext abgerufen wird oder wenn Waren, statt im Kaufhaus erworben, nun über Bildschirmtext bestellt werden. Die Unmittelbarkeit des Dialogs mit dem Bildschirmtextrechner erlaubt eine einfache Datenerhebung beim einzelnen Teilnehmer. Die Tatsache, daß Bildschirmtext über den häuslichen Fernsehapparat genutzt wird, kann zu einer leichteren Überwindung natürlicher Hemmschwellen bei der Übermittlung von Daten an Dritte führen. Dies gilt neben einer Datenerhebung bei Bestellungen gerade auch für Meinungsumfragen über Bildschirmtext.

Da jedermann bei Bildschirmtext Anbieter von Informationsangeboten werden kann, wäre es relativ leicht möglich, ehrverletzende Äußerungen über eine bestimmte Person an einen gro-

ßen Empfängerkreis zu richten („Dorfklatsch per Bildschirmtext").

Die Bildschirmtextversuche in Berlin und Nordrhein-Westfalen haben gezeigt, daß Bildschirmtext mißbräuchlich dazu benützt worden ist, um an Daten der Teilnehmer zu gelangen, um auf Rechnung anderer kostenpflichtige Angebotsseiten abzurufen und durch Manipulation an technischen Geräten unter falschem Namen Informationen einzustellen.

Weil diese umfassenden Datenmengen auf elektronischen Medien anfallen, ist es mit vergleichsweise geringem technischen Aufwand möglich, umfassende Verhaltenskontrollen durch Nutzungsprotokolle zu erstellen und durch entsprechende Auswertungen Teilnehmerprofile zu erstellen. Dies gilt nicht zuletzt für die dem System angeschlossenen externen Computer. Neben dieser Auswertung erlauben die elektronischen Medien eine wesentlich leichtere Übermittlung dieser Daten an Dritte.

4.1.1.3 Schranken durch die Verfassung

Einer allzu umfassenden Verarbeitung der Daten des Einzelnen sind jedoch vom Grundgesetz und den Länderverfassungen Grenzen gesetzt. So hat beispielsweise das Bundesverfassungsgericht in seinem Mikrozensus-Beschluß (E 27, 1/6) erklärt, daß es mit der Menschenwürde nicht vereinbar wäre, wenn der Staat das Recht für sich in Anspruch nehmen könnte, den Menschen zwangsweise in seiner ganzen Persönlichkeit zu registrieren und zu katalogisieren, sei es auch in der Anonymität einer statistischen Erhebung. Ein solches Eindringen in den Persönlichkeitsbereich durch eine umfassende Einsichtnahme in die persönlichen Verhältnisse seiner Bürger sei dem Staat auch deshalb versagt, weil dem Einzelnen um der freien und selbstverantwortlichen Entfaltung seiner Persönlichkeit willen ein Innenraum verbleiben müsse, in dem er sich selbst besitze und in den er sich zurückziehen könne, zu dem die Umwelt keinen Zutritt habe, in dem er in Ruhe gelassen werde und ein Recht auf Einsamkeit genieße. In diesen Bereich könne bereits dann durch eine Einsichtnahme eingegriffen werden, wenn dadurch die freie Entfaltung der Persönlichkeit durch den psychischen Druck öffentlicher Anteilnahme gehemmt werden könnte. Auch das Bundesverwaltungsgericht hat in einer früheren Entscheidung bereits im Jahre 1956 deutlich gemacht, daß auch persönliche Verhältnisse nicht schrankenlos durchleuchtet werden dürfen.

Diese Verfassungsgrundsätze gelten auch für die Benutzung von Bildschirmtext.

4.1.1.4 Notwendigkeit einer bereichsspezifischen Regelung

Um den aufgezeigten speziellen Risiken zu begegnen und die verfassungsrechtlich geschützte Privatsphäre zu bewahren, hat auch der Bayer. Landesbeauftragte für den Datenschutz eine bereichsspezifische Datenschutzregelung für Bildschirmtext als notwendig erachtet. Wie bereits oben bemerkt, haben mich zu dieser Forderung nicht nur die theoretisch denkbaren Gefahren einer Benutzung von Bildschirmtext bewogen, vielmehr hat die Praxis der Bildschirmtextversuche gezeigt, daß Gefahren wirklich vorhanden sind: So wurden in Einzelfällen Bürger zur Abgabe von Daten überlistet, haben Unbefugte durch technische Manipulation unter fremden Namen an andere Teilnehmer Mitteilungen versandt und unter fremden Namen zu Lasten Dritter kostenpflichtige Seiten abgerufen und wurden Angebote bedenklichen Inhalts eingestellt.

Meine Forderung lautete daher immer, daß sich durch die Verwendung des Mediums „Bildschirmtext" die Position der Bürger nicht verschlechtern dürfe. Die grundsätzlich leichtere Verfügbarkeit der Daten darf auch aus dem Gesichtspunkt des Verbraucherschutzes nicht zur leichteren Verführbarkeit der Bürger führen. Daraus ergeben sich folgende Mindestforderungen:

- Das Erheben und das Speichern personenbezogener Daten durch Betreiber und Anbieter darf nur im unbedingt notwendigen Umfang erfolgen.
- Der Betreiber darf an den Anbieter nur möglichst wenig Daten, die den Teilnehmer betreffen, übermitteln.
- Die Teilnehmerdaten und die bei der Benutzung des Systems anfallenden Informationen sind weitgehend zu anonymisieren.
- Nicht mehr benötigte personenbezogene Daten sind umgehend zu löschen.
- Meinungsäußerungen sollen möglichst überhaupt nicht über Bildschirmtext gespeichert werden.
- Für die Bürger ist ein ausreichender Ehrenschutz sicherzustellen.

4.1.1.5 Ziele einer Datenschutzregelung

Aus diesen Forderungen ergaben sich für eine bereichspezifische Datenschutzvorschrift für Bildschirmtext folgende Ziele:

- Den erkannten Datenschutzgefahren muß begegnet werden.
- Soweit möglich, soll die neue Regelung auf bereits geltendes Recht Bezug nehmen, um die Anwendbarkeit der Vorschrift zu erleichtern und ihre Akzeptanz zu erhöhen.
- Soweit besondere bereichsspezifische Regelungen notwendig sind, sollten diese in Aufbau, Struktur und Terminologie bereits bestehenden Vorschriften möglichst angeglichen werden.
- Datenschutzbestimmungen sollen eine sinnvolle Anwendung von Bildschirmtext nicht verhindern.

4.1.1.6 Staatsvertrag „Bildschirmtext"

Die Datenschutzbeauftragten der Länder haben für den Staatsvertrag „Bildschirmtext" eine bereichsspezifische Datenschutzvorschrift erarbeitet. Wesentliche Vorstellungen der Datenschutzbeauftragten sind nun in dem von den Ministerpräsidenten beschlossenen Bildschirmtext-Staatsvertrag in dessen Art. 9 übernommen worden. Damit sind viele meiner wesentlichen Forderungen erfüllt. Abweichungen gibt es insbesondere in der Form der Abrechnung der bei Benutzung des Bildschirmtextes angefallenen Gebühren. Hier hatte ich für eine Lösung plädiert, die eine völlig anonyme Abrechnung erlaubt und dem Anbieter keinerlei Hinweise über die Personen gegeben hätte, die sein Angebot abgerufen haben. Auf diese Weise wollte ich verhindern, daß überhaupt die Daten vorliegen, aus denen ein meines Erachtens unzulässiges Persönlichkeitsprofil erstellt werden kann.

Auch im unmittelbaren Verhältnis zwischen Teilnehmer und Anbieter bei Abschluß von Verträgen oder Inanspruchnahme von sonstigen Leistungen beispielsweise hatte ich strengere Anforderungen an die Erhebung und Verarbeitung von Daten gestellt.

Soweit meine Vorschläge in der endgültigen Fassung des Staatsvertrages nicht berücksichtigt worden sind, werde ich die künftige Praxis besonders aufmerksam verfolgen. Sollten sich besondere Gefährdungen zeigen, mache ich schon jetzt einen datenschutzrechtlichen Nachbesserungsvorbehalt geltend.

4.1.1.7 Umsetzung des Staatsvertrages in die Praxis

Derzeit sind die Programme, mit denen Bildschirmtext in den Bildschirmtextzentralen abgewickelt werden soll, noch nicht vollständig bekannt. Sobald die Programme vorliegen, werde ich sie daraufhin überprüfen, ob die Regelungen im Staatsvertrag eingehalten werden. Insbesondere werde ich dabei auf die für den Betreiber geltenden Vorschriften achten.

Im folgenden zeige ich noch einige Gesichtspunkte auf, die mir im Zusammenhang mit den Datenschutzzielen wichtig sind, nämlich zu verhindern, daß der Bürger durch Bildschirmtext gefährdet werde und er möglichst weitgehend über die Verwendung seiner Daten bei Bildschirmtext unterrichtet wird:

- Die Funktionen eines Betreibers und eines Anbieters sollten möglichst getrennt sein. Jedenfalls muß für den Teilnehmer deutlich sein, ob eine Behörde oder ein Unternehmen ihm als Anbieter oder als Betreiber gegenübertritt. Soweit bei Benutzung des Bildschirmtextes von der Bildschirmtextzentrale auf einen externen Rechner umgeschaltet wird, muß der Bürger diesen Umschaltvorgang eindeutig erkennen können. Eventuell wird hier ein eindeutiger und standardisierter Hinweis zu fordern sein (z.B vergleichbar dem Eurovision-Zeichen).

  Die nach Abs. 6 des Art. 9 Bildschirmtext-Staatsvertrag mögliche Einwilligung zu einer weiteren Datenverarbeitung darf nicht mißbraucht werden. Hier werde ich die Praxis ebenfalls aufmerksam verfolgen.

  Damit die Datenschutzbestimmungen des Bildschirmtext-Staatsvertrages von allen Beteiligten eingehalten werden, ist eine ausreichende Datenschutzkontrolle erforderlich. Die das übrige Datenschutzrecht prägende Zersplitterung der Datenschutzkontrolle würde, insbesondere wegen der Schwierigkeit der Materie, eine ausreichende Überwachung des Datenschutzes wohl nicht gewährleisten. Außerdem muß sichergestellt werden, daß wegen der Datenschutzrisiken, die die Benutzung von Bildschirmtext in sich birgt, eine Kontrollmöglichkeit vorgesehen wird, die nicht nur auf Beschwerden von Bürgern hin reagieren kann. Zumal der Einzelne häufig gar nicht erkennen kann, ob im Rahmen von Bildschirmtext seine Daten mißbräuchlich verwendet worden sind.

  Daher fordere ich eine eindeutige Regelung zur Fremdkontrolle des Datenschutzes, die einer Stelle die Datenschutzkontrolle zuweist. Wenn der Landesgesetzgeber die Regelungskompetenz für den Bildschirmtext in Anspruch nimmt, dann ist er auch berufen, die Datenschutzkontrolle zu regeln.

  Die Datenschutzbestimmung im Staatsvertrag Bildschirmtext/ darf nicht dadurch faktisch nutzlos werden, daß das Medienprivileg, das in § 1 Abs. 3 Bundesdatenschutzgesetz festgelegt ist, so extensiv ausgelegt wird, daß die Mehrzahl der Bildschirmtextangebote unter diese Ausnahmevorschrift fallen. Ggf. muß für das Medium Bildschirmtext/das Medienprivileg dahingehend fortgeschrieben werden, daß bei Beachtung der verfassungsrechtlich garantierten Freiheit von Presse, Rundfunk und Film dennoch die Schutzbedürfnisse der Bildschirmtext-Teilnehmer in ausreichendem Maße berücksichtigt werden.

  Die Bundespost hat eine Erklärung abgegeben, daß sie die Datenschutzbestimmung des BTX-Staatsvertrags beachten werde; dies begrüße ich. Damit kann die Streitfrage dahinstehen, inwieweit die Länder die Gesetzgebungskompetenz für die Regelungen betreffend Betriebszentralen besitzen, wenn diese von der Deutschen Bundespost betrieben werden. Über diese Erklärung hinaus fordere ich, daß in der für BTX zu erlassenden Rechtsverordnung die Geltung der Datenschutzbestimmung für die Deutsche Bundespost ausdrücklich festgelegt wird.

4.1.2 Kabelkommunikation

4.1.2.1 Neue Risiken

Der für die nähere Zukunft bereits geplante zunehmende Einsatz von Breitbandkabeln, insbesondere von Glasfaserkabeln, wird im Bereich der Kommunikation eine Reihe neuer Möglichkeiten eröffnen. Die Kabelpilotprojekte sollen die technischen Möglichkeiten und deren Bewältigungschancen aufzeigen.

Durch die große Kapazität der Breitbandkabel können weit über die technischen Übermittlungsmöglichkeiten, die Bildschirmtext eröffnen soll,

neue Breitbanddienste,
Rückkanal im Breitband,
bewegte Bilder,
Fernmessen,
Fernwirken,
ein umfassender Informationsabruf mit Echtzeitverarbeitung,
ein erweitertes Fernsehangebot und
der Filmabruf

dem einzelnen Teilnehmer eröffnet worden.

Dieses umfassende Informationsangebot kann neben anderen, aus gesellschaftspolitischer Sicht zu diskutierenden Risiken auch datenschutzrechtliche Gefahren enthalten. Neben den Gefahren, die bereits im Zusammenhang mit Bildschirmtext zu beobachten sind und die bei Breitbandkommunikation, welche noch weitere Lebensbereiche betreffen kann, entsprechend breiter gefächert sein werden, sind neu die Möglichkeiten, in die Wohnung der Bürger einzuwirken und damitdie Bürger mehr als bisher durch Auswertung der bei Benutzung der Breitbanddienste anfallenden Daten und durch Maßnahmen des Fernmessens zu überwachen. Zu beobachten wird auch sein, wieweit der Verhaltensdruck wächst, Dienste in einer bestimmten Weise zu benutzen oder nicht zu benutzen, weil aus der Tatsache der Nutzung oder Nichtnutzung wieder Daten anfallen, die entsprechenden Auswertungen zugeführt werden können. Bei alledem ist wohl festzustellen, daß das Fernmeldegeheimnis ebensowenig wie bereits bei Bildschirmtext ausreichenden Schutz garantiert, denn die Kabelzentralen, bei denen die großen Datenmengen anfallen, werden wohl vom Fernmeldegeheimnis nicht erfaßt sein.

Daraus ergeben sich auch

4.1.2.2 weitere Datenschutzforderungen:

Die freie Entfaltung der Persönlichkeit, die Unverletzlichkeit der Wohnung, die negative Meinungsfreiheit müssen gewahrt bleiben. Diese Rechtsgüter sind zunehmend gefährdet. Datenschutz heutiger Konzeption reicht hier nicht mehr aus. Die Forderung mag banal klingen, jedoch muß Datenschutz zum Informationsschutz ausgeweitet werden. In welcher Form eine Information vorliegt, in welcher Weise sie gespeichert ist und auf welchem Wege sie übermittelt wird, darf nicht mehr Kriterium dafür sein, ob ein Schutzgesetz anwendbar ist. Deswegen müssen über die generellen dem Datenschutz zugrundeliegenden Forderungen hinaus wohl eine Reihe von neuen Maßnahmen getroffen werden. Zwar wird in erster Linie auf die Einwilligung des mündigen Bürgers abzustellen sein, doch kann dies nur als erster Schritt gelten, weil die möglicherweise schwierigen technischen Zusammenhänge für viele Bürger nicht mehr durchschaubar sind. Inwieweit die Lizensierung der Teilnehmer bei Kabelkommunikationsprojekten ein Weg zur Lösung dieses Problems sein kann, wäre zu prüfen.

Unabhängig davon müssen die bereits im Bildschirmtext-Staatsvertrag für Angebote geltenden Schutzbestimmungen auf alle angebotenen Informationen ausgedehnt werden.

Privilegien für besondere Anbieter - vergleichbar mit dem heutigen Medienprivileg - sollten weitgehend ausgeschlossen sein.

Soweit Informationen beim Teilnehmer erhoben werden, sei dies durch Anbieter oder andere Teilnehmer, muß dem betroffenen Teilnehmer die Tatsache des Abrufs offenkundig sein.

Der Teilnehmer muß die Möglichkeit haben, sich aus einem Abruf auszuschalten und gegebenenfalls innerhalb einer bestimmten Frist die unüberlegt abgegebenen Informationen zurückzuholen.

Gerade wenn die Datenkommunikation alle Lebensbereiche betreffen kann, muß gesetzlich verboten werden, daß besonders sensible Daten, z.B. medizinische Angaben, Sozialdaten und ähnliche, vom Teilnehmer abgefragt werden.

Einer besonderen Regelung bedürfen Dienste wie Fernwirken und Fernmessen, weil hier in besonders starkem Maße in die Wohnung der Betroffenen eingewirkt werden kann; vergleiche hierzu die Überlegungen im nachfolgenden Punkt 4.

Selbstverständlich müssen die Daten, die anläßlich der Benutzung anfallen, besonders geschützt werden. Würden diese Daten für eine Auswertung freigegeben, wäre der Bürger endgültig „gläsern".

4.1.2.3 Anforderungen an die Gesetzgebung

Gerade wegen der besonderen Risiken, die eine umfassende Kabelkommunikation für die Privatsphäre der Bürger mit sich bringen kann, halte ich klare und eindeutige gesetzliche Regelungen für erforderlich. Hinsichtlich der zugelassenen Dienste bedarf es konkreter Definitionen. Die Ausgestaltung darf nicht zu weitgehend dem Verordnungsgeber überlassen bleiben.

Dabei muß der Gesetzgeber auch ausreichende technisch-organisatorische Maßnahmen fordern. Wegen der umfassenden technischen Möglichkeiten müssen gesteigerte Sicherheitsanforderungen erhoben werden, die sich am jeweiligen Stand der Technik auszurichten haben.

Eine ausreichende Kontrolle der Einhaltung der Informationsbestimmungen und strenge Sanktionsmöglichkeiten müssen die Beachtung der Gesetze sicherstellen. Damit Datenschutzkontrolle von unabhängigen Datenschutzbeauftragten durchgeführt werden kann, würde ich es begrüßen, wenn Kabelkommunikationsdienste unter öffentlichrechtlicher Trägerschaft abgewickelt würden.

Damit die Weichenstellungen, die mit dem Kabelpilotprojekt vorgenommen werden sollen, auch die Privatsphäre der Bürger hinreichend berücksichtigen, wäre ich für eine rechtzeitige Beteiligung bei Entscheidungen über deren technische Realisierung dankbar.

4.1.2.4 Neue Dienste des Fernwirkens und Fernmessens

Nicht bereits zu Beginn des Kabelpilotprojektes, jedoch im Endzustand der Projektphase, werden auch sog. „Fernwirkdienste" zur Verfügung stehen. Hierunter sind die Möglichkeiten des sog. „Fernwirkens" und „Fernmessens" zu verstehen. Das bedeutet, daß von außen in der Wohnung eines Teilnehmers Wirkungen ausgelöst, Messungen vorgenommen und Beobachtungen angestellt werden können. Beispielsweise könnten die Gas-, Wasser- und Stromablesungen im Wege des „Fernwirkens" direkt von den Stadtwerken abgelesen werden, ohne daß ein Ableser in das einzelne Haus oder die einzelne Wohnung kommen müßte. Für wichtige Meldungen beispielsweise könnte von außen das Fernsehprogramm unterbrochen oder der Fernsehapparat überhaupt erst eingeschaltet werden. Damit könnten dem Einzelnen direkt von außen Informationen zuteil werden. Ältere und pflegebedürftige Personen könnten in der ihnen vertrauten Wohnung bleiben, weil über „Fernmessen" beispielsweise ihr Gesundheitszustand von außen ständig überwacht werden und rechtzeitig ärztliche Hilfe eintreffen könnte. Auch Mütter könnten zwischen verschiedenen Einkäufen im Wege des „Fernmessens" prüfen, ob ihre Kleinkinder noch schlafen. Die Beispiele ließen sich noch fortsetzen. Damit spricht zweifelsohne einiges für den Einsatz dieser neuen technischen Möglichkeiten.

Andererseits dürfen diese „Fernwirkdienste" nicht das Grundrecht der Unverletzlichkeit der Wohnung (Art. 13 GG) verletzen oder in die durch Art. 1 und Art. 2 Grundgesetz geschützte Privatsphäre eindringen. Um nachteilige Folgen derartiger Dienste für den Bürger zu vermeiden, müssen meines Erachtens folgende Bedingungen erfüllt sein:

- „Fernwirkdienste" dürfen nicht zur Kontrolle der Betroffenen führen. So darf beispielsweise nicht über „Fernmessen" des aktuellen Wasser- oder Stromverbrauchs festgestellt werden, ob sich gerade jemand in einer Wohnung aufhält oder nicht und ob er gerade große Stromverbraucher eingeschaltet hat.
- Der vom „Fernwirkdienst" Betroffene muß über Art, Umfang, Häufigkeit und möglichst auch Termin der jeweiligen „Fernwirkung" unterrichtet sein. Der Bürger muß rechtzeitig erfahren, wenn „Fernwirkungen" oder „Fernmessungen" in seiner Wohnung vorgenommen werden.
- Auch hier muß der sog. „informed consent" gelten.
- Gegen seinen Willen darf der Bürger „Fernmessen" und „Fernwirken" überhaupt nicht ausgesetzt sein.
- Verweigert ein Bürger den Anschluß an „Fernwirk-" oder „Fernmeßdienste", so dürfen ihm keine über die der Verweigerung unmittelbar zuzurechnenden Kosten hinausgehenden Nachteile entstehen. Es darf somit weder finanzieller noch sozialer Druck auf ihn ausgeübt werden, wenn er derartige Einwirkungen in seine Privatsphäre und in seine Wohnung nicht wünscht.
- Durch „Fernwirken" und „Fernmessen" darf der Einzelne nicht einem psychischen Druck dergestalt ausgesetzt sein, daß er seine Lebensführung in der Wohnung danach ausrichtet.

Wegen der möglichen Auswirkungen derartiger „Fernwirkdienste" auf Grundrechtspositionen der Bürger fordere ich daher rechtzeitig vor deren Einführung eine gesetzliche Regelung, die die vorgenannten Forderungen berücksichtigt.

4.2 **Datenschutz im Gesundheitsbereich**

Der Grundsatz der ärztlichen Schweigepflicht ist Voraussetzung dafür, daß sich der Patient dem Arzt rückhaltslos offenbart. Dies ist wiederum in vielen Fällen Voraussetzung einer erfolgreichen Behandlung. Eine solche liegt aber nicht nur im Interesse des einzelnen Patienten, sondern auch der Allgemeinheit am möglichst optimalen Funktionieren des Gesundheitssystems. Die ärztliche Schweigepflicht hat die Aufgabe, den Schutz der Intim- bzw. Privatsphäre zu sichern, der viele Angaben zuzurechnen sind, die der Patient dem Arzt macht.

Der Schutz dieses privaten Bereichs wird durch eine Reihe von Vorschriften ergänzt, die Behörden und anderen öffentlichen Stellen Zurückhaltung beim Eindringen in diesen Bereich auferlegen. Patientendaten sind beim Arzt durch die Bestimmungen der Strafprozeßordnung durch Zeugnisverweigerungsrecht (§ 53 Abs. 1 Nr. 3 StPO), durch Ausnahme von der Pflicht zur Herausgabe von Beweismitteln (§ 95 StPO) und durch Beschlagnahmeverbot (§ 97 StPO) geschützt. Die ärztliche Schweigepflicht wird außerdem durch die Vorschriften der Art. 17 Abs. 2 und 18 Abs. 2 des Bayerischen Datenschutzgesetzes und der §§ 10, Abs. 1 Satz 2 und 11 Abs. 1 Satz 2 des Bundesdatenschutzgesetzes verlängert: Soweit nämlich personenbezogene Daten einem Berufs- oder besonderen Amtsgeheimnis unterliegen und der übermittelnden Stelle von der zur Verschwiegenheit verpflichteten Person in Ausübung ihrer Berufs- oder Amtspflicht übermittelt wurden, ist für die Zulässigkeit der Weiterübermittlung erforderlich, daß entweder der Empfänger die Daten für die Erfüllung des gleichen Zwecks benötigt, zu dem sie die übermittelnde Stelle erhalten hat (so für Übermittlung

innerhalb des öffentlichen Bereichs), bzw. daß die gleichen Voraussetzungen gegeben sind, unter denen die Angaben durch die zur Verschwiegenheit verpflichtete Person selbst übermittelt werden durften. § 76 des X. Buches des Sozialgesetzbuches will auf ähnliche Weise die Verlängerung der ärztlichen Schweigepflicht erreichen, indem er eine Weiterübermittlung von Daten, die ein Sozialleistungsträger von einem Arzt erhalten hat, nur erlaubt, wenn sie auch dem Arzt gestattet wäre. Diese Regelung wird allerdings durch Absatz 2 des § 76 stark relativiert. Das Bayerische Krankenhausgesetz (BayKrG) konkretisiert in seinem Artikel 13 die sich aus der ärztlichen Schweigepflicht für Krankenhäuser ergebenden Folgen. Die Speicherung von Patientendaten, Auskunft über dieselben, Zugriff auf Patientendaten und deren Übermittlung sowie die notwendigen Datensicherungsmaßnahmen werden in dieser Vorschrift geregelt. Andere Gesetze sollen für besondere Fälle die notwendige Rücksichtnahme bei Angaben über gesundheitliche Verhältnisse bewirken. So sind bei der statistischen Mikrozensusbefragung die Angaben zur Gesundheit ausdrücklich freiwillig. Nach § 27 Abs. 3 und § 35 Abs. 2 des Bundesdatenschutzgesetzes sind Daten über gesundheitliche Verhältnisse zu löschen, wenn ihre Richtigkeit von der speichernden Stelle nicht bewiesen werden kann.

Die Rechtsprechung hat sich im Hinblick auf Art. 1 Abs. 1 und 2 Abs. 1 des Grundgesetzes des Schutzes des Persönlichkeitsbereichs und von Gesundheits- bzw. Krankheits-Daten angenommen. An erster Stelle ist auf das schon oben, im Zusammenhang mit Neuen Medien erwähnte Grundsatzurteil hinzuweisen, das zur Verfassungsmäßigkeit der Mikrozensusstatistik erging (BVerfGE 27, 5 ff). Danach widerspricht es der menschlichen Würde, den Menschen zum bloßen Objekt im Staat zu machen. Mit der Menschenwürde wäre es danach nicht zu vereinbaren, wenn der Staat das Recht für sich in Anspruch nehmen könnte, den Menschen zwangsweise in seiner ganzen Persönlichkeit zu registrieren, zu katalogisieren, sei es auch in der Anonymität einer statistischen Erhebung, und ihn damit wie eine Sache zu behandeln, die einer Bestandsaufnahme in jeder Beziehung zugänglich ist. Nach dieser Entscheidung gewährt das Grundgesetz dem einzelnen Bürger aber auch einen unantastbaren Bereich privater Lebensgestaltung, der der Einwirkung der öffentlichen Gewalt entzogen ist. Nach Ansicht des Gerichts kann ein Eingriff in diesen Bereich u. U. bereits bei einer - wenn auch bewertungsneutralen - Einsichtnahme gegeben sein, „die die freie Entfaltung der Persönlichkeit durch den psychischen Druck öffentlicher Anteilnahme zu hemmen vermag".

In seinem Beschluß vom 8.3.1972 bezeichnete das Bundesverfassungsgericht die Beschlagnahme der Karteikarte eines Arztes gegen den Willen des Betroffenen als Verletzung des dem Patienten zustehenden Grundrechts auf Achtung seines privaten Bereichs (E 32, 373/379 ff.). Das Gericht ordnete in dieser Entscheidung die Notizen auf einer ärztlichen Karteikarte näher ein: Es prüfte, ob die Angaben der unantastbaren „Intimsphäre des einzelnen" angehören und stellte fest, daß nicht der gesamte Bereich des privaten Lebens unter dem absoluten Schutz des Grundrechts aus Art. 2 Abs. 1 i. V. mit Art. 1 Abs. 1 GG stehe. Als gemeinschaftsbezogener und gemeinschaftsgebundener Bürger müsse vielmehr jedermann staatliche Maßnahmen hinnehmen, die im überwiegenden Interesse der Allgemeinheit unter strikter Wahrung des Verhältnismäßigkeitsgebots getroffen werden, soweit sie nicht den unantastbaren Bereich privater Lebensgestaltung beeinträchtigen. Ärztliche Karteikarten betreffen mit ihren Angaben über Anamnese, Diagnose und therapeutische Maßnahmen nach Ansicht des Gerichts zwar nicht die unantastbare Intimsphäre, wohl aber den privaten Bereich des Patienten. Damit nehmen sie am Schutz aus Art. 2 Abs. 1 und 1 Abs. 1 GG teil, der dem Einzelnen vor dem Zugriff der öffentlichen Gewalt gewährt ist. Dies gelte insbesondere für Erkenntnisse, die der Arzt durch seine berufliche Tätigkeit über den Gesundheitszustand des Patienten gewinne und schriftlich niederlege. Dabei komme es nicht darauf an, ob derartige Aufzeichnungen Krankheiten, Leiden oder Beschwerden verraten, deren Offenbarung den Betroffenen mit dem Verdacht einer Straftat belastet, ihm in anderer Hinsicht peinlich oder seiner sozialen Geltung abträglich sei. Vielmehr verdiene ganz allgemein der Wille des Einzelnen Achtung, so höchstpersönliche Dinge, wie die Beurteilung seines Gesundheitszustandes durch einen Arzt, vor fremdem Einblick zu bewahren. Wer sich in ärztliche Behandlung begibt, müsse und dürfe erwarten, daß alles, was der Arzt im Rahmen seiner Berufsausübung über seine gesundheitliche Verfassung erfährt, geheim bleibe und nicht zur Kenntnis Unberufener gelange. Nur so könne zwischen Patient und Arzt jenes Vertrauen entstehen, das zu den Grundvoraussetzungen ärztlichen Wirkens zähle, weil es die Chancen der Heilung vergrößere und damit - im ganzen gesehen - der Aufrechterhaltung einer leistungsfähigen Gesundheitsfürsorge diene. Das Gericht zieht daraus den Schluß, daß sich der verfassungsrechtliche Schutz der Privatsphäre des Einzelnen auch auf die Karteikarte des Arztes mit Eintragungen über den Gesundheitszustand des Patienten beziehe und daß eine solche Karteikarte dem Zugriff der öffentlichen Gewalt grundsätzlich entzogen sei. Schutzwürdige Geheimhaltungsinteressen des Einzelnen hätten allerdings dann zurückzutreten, wenn überwiegende Belange des Gemeinwohls dies zwingend gebieten. So begegne es keinen Bedenken, wenn der Staat den Gefahren, die der Volksgesundheit durch bösartige Ansteckungskrankheiten oder epidemisch auftretende Leiden drohen, dadurch zu steuern suche, daß er dem Arzt unter weitestmöglicher Schonung der Interessen des Patienten die Meldung an öffentliche Gesundheitsämter zur Pflicht mache. Für alle Regelungen auf diesem Gebiet komme es allerdings entscheidend darauf an, ob der Eingriff in die Privatsphäre des Bürgers bei einer Abwägung, die alle Umstände des Einzelfalles in Betracht zieht, dem Verhältnismäßigkeitsgrundsatz entspreche. Die Beschlagnahme einer ärztlichen Karteikarte verletze jedoch in aller Regel das dem Einzelnen zustehende Grundrecht auf Achtung seines privaten Bereichs (das Bundesverfassungsgericht hat dies hinsichtlich einer Karteikarte im Gewahrsam des Praxisnachfolgers festgestellt).

In einem Beschluß vom 24.5.1977 bezeichnete das Bundesverfassungsgericht die Beschlagnahme von Klientenakten einer öffentlichrechtlich anerkannten Suchtberatungsstelle als Verletzung des Grundrechts des Trägers dieser Stelle aus Art. 2 Abs. 1 GG und der Grundrechte der Klienten aus Art. 2 Abs. 1 i. V. mit Art. 1 Abs. 1 GG, wenn durch die Beschlagnahme die Belange der Gesundheitsfürsorge in einem solchen Maße beeinträchtigt werden, daß der durch den Eingriff verursachte Schaden außer Verhältnis zu dem mit der Beschlagnahme angestrebten erreichbaren Erfolg stehe. Die Beschlagnahme solcher Akten verletze den Grundsatz der Verhältnismäßigkeit, wenn sie sich lediglich auf den allgemeinen Verdacht stütze, daß sich Klienten der Beratungsstelle durch Erwerb und Besitz von Betäubungsmitteln strafbar gemacht und solche Mittel illegal bezogen hätten (E 44, 353/372 ff).

Vor allem Fragen der Befugnis zur Weitergabe von Patientendaten oder zur Einsichtnahme in diese haben sich im Bereich des Datenschutzes im Gesundheitswesen als problematisch erwiesen. Daneben sind auch Vorschriften über die Speicherung, Veränderung und Löschung von Daten und über Rechte der Betroffenen zu beachten. Aufgetretene Fragen werden im folgenden für die Bereiche Krankenhäuser, Gesundheitsämter und Sozialleistungsträger dargestellt. Ein Ausblick auf Planungen für größere Krankheitsregister schließt sich an.

4.2.1 Öffentliche Krankenhäuser der Gemeinden, Kreise, Bezirke oder des Staates
006
4.2.1.1 Speicherung von Patientendaten
006
Nach Art. 13 Abs. 2 BayKrG dürfen Patientendaten vom Krankenhaus nur gespeichert werden, soweit dies zur Erfüllung der Aufgaben des Krankenhauses oder im Rahmen des krankenhausärztlichen Behandlungsverhältnisses erforderlich ist. Dem Patienten ist auf Verlangen vom Krankenhaus Auskunft darüber zu erteilen, welche Daten über ihn gespeichert werden und an wen welche Daten weitergegeben wurden. Die Auskunft kann von einem Arzt beschränkt werden, soweit dies mit Rücksicht auf den Gesundheitszustand des Patienten dringend geboten ist. Der Patient hat Anspruch auf Berichtigung falscher Daten. Abs. 4 der Vorschrift bestimmt, daß der Krankenhausarzt auf die von ihm gespeicherten Patientendaten zugreifen darf, während die Krankenhausverwaltung nur insoweit auf gespeicherte Patientendaten zugreifen darf, als dies zur verwaltungsmäßigen Abwicklung der Behandlung des Patienten erforderlich ist. Hieraus ergibt sich die Notwendigkeit, die Speicherung von Patientendaten so zu organisieren, daß eine Trennung von Daten für die verwaltungsmäßige Abwicklung der Behandlung von sonstigen Patientendaten durchführbar ist. Abs. 6 der Vorschrift fordert besondere Schutzvorkehrungen technischer und organisatorischer Art, die verhindern, daß auf Patientendaten unberechtigt zugegriffen wird.

Die Vorschrift des Art. 13 BayKrG geht gem. Art. 2 Abs. 2 des Bayerischen Datenschutzgesetzes (BayDSG) den Vorschriften des BayDSG vor. Soweit im Datenschutzgesetz weitere Konfliktlagen angesprochen werden, ist dieses grundsätzlich ergänzend heranzuziehen, wobei zu beachten ist, daß die Vorschriften des BayKrG nicht die Speicherung von Patientendaten in Form einer manuellen oder automatisierten Datei voraussetzen, sondern alle Arten von Patientenunterlagen betreffen, während die Vorschriften des Datenschutzgesetzes grundsätzlich nur eingreifen, wenn Patientendaten in Dateiform gespeichert sind. Soweit danach eine Anwendung von Vorschriften des Datenschutzgesetzes in Frage käme, ist außerdem Art. 22 BayDSG zu berücksichtigen, wonach auf öffentliche Stellen, soweit sie am Wettbewerb teilnehmen, nicht die Vorschriften des BayDSG - ausgenommen diejenigen über die Kontrolle des Datenschutzes - sondern die Vorschriften des Bundesdatenschutzgesetzes in dessen ersten, dritten und ggfs. vierten Abschnitt anzuwenden sind. Nach h. M. sind Krankenhäuser überwiegend als solche Wettbewerbseinrichtungen anzusehen, da sie hinsichtlich des Bettenangebots untereinander konkurrieren. Kein Wettbewerb ist dagegen wohl bei einigen wenigen Spezialkliniken ohne Konkurrenz anzunehmen. Außerdem fehlt der Wettbewerbscharakter auch in Fällen unfreiwilligen Krankenhausaufenthalts (z. B. bei Bezirkskrankenhäusern). Von den danach ergänzend heranzuziehenden Vorschriften des Bundesdatenschutzgesetzes sei insbesondere auf § 27 hingewiesen, der über das Krankenhausgesetz hinaus in Abs. 3 noch eine Regelung für Sperrung und Löschung enthält: Danach sind Daten über gesundheitliche Verhältnisse zu löschen, wenn ihre Richtigkeit von der speichernden Stelle nicht bewiesen werden kann. Die Vorschriften des BDSG über Speicherung und Übermittlung von Daten (§§ 23 und 24 BDSG) sind im Bereich der Krankenhäuser außerdem für die Speicherung der Daten von ambulanten Patienten anzuwenden, weil sich auf diesen Bereich das BayKrG nicht bezieht. Im Vergleich zu dieser komplizierten Rechtslage einfach geregelt ist die Kontrolle des Datenschutzes, die nach Art. 28 BayDSG dem Landesbeauftragten für den Datenschutz obliegt, was nach Art. 22 Abs. 1 BayDSG auch für öffentliche Stellen gilt, soweit sie am Wettbewerb teilnehmen.

4.2.1.2 Datenübermittlung bzw. Offenbarung

Die eingangs angesprochenen Fragen der ärztlichen Schweigepflicht betreffen das Offenbaren von Patientendaten gegenüber anderen Personen oder Stellen. Die Datenschutzgesetze sprechen dagegen hinsichtlich der Weitergabe von Daten von „übermitteln". Das Übermitteln ist als Weitergabe an einen „Dritten"/definiert. Eine Übermittlung an Dritte liegt beispielsweise nicht vor, wenn bayerische Behörden Daten im Auftrag bei einer anderen Stelle verarbeiten lassen, die völlig den Weisungen des Auftraggebers über den Umgang mit den Daten unterworfen ist (s. Art. 17 Abs. 4 BayDSG). Eine solche Weitergabe zur Auftrags-Datenverarbeitung ist jedoch, ohne eine Übermittlung im Sinne der Datenschutzgesetze zu sein, im Regelfall durchaus eine Offenbarung im Sinne der ärztlichen Schweigepflicht, so daß die Übergabe von Patientendaten zur Verarbeitung im Auftrag einer entsprechenden Befugnis bedarf.

Zwecke, für die Patientendaten weitergegeben werden, lassen sich in vier Gruppen einteilen:

- Behandlungszwecke,
- Abrechnung der Behandlung,
- Aufgaben der öffentlichen Verwaltung bzw. der Gerichte, insbesondere im Bereich Sicherheit und Ordnung (z. B. Seuchenrecht), und
- Forschung und Statistik.

1. Weitergabe von Patientendaten für Behandlungszwecke:

   Bei Weitergabe von Patientendaten zu Behandlungszwekken zwischen Ärzten ist immer wieder festzustellen, daß das Bewußtsein darüber fehlt, daß das Gebot der ärztlichen Schweigepflicht auch zwischen behandelndem und nichtbehandelndem Arzt gilt. Eine Entbindung von ihr setzt eine Erklärung des Patienten voraus. Nach Literatur und Rechtsprechung zu § 203 StGB kann auch eine konkludente Einwilligung ausreichen. Eine solche kann in Frage kommen, wenn der Patient, wie öfters im Krankenhaus, von verschiedenen Ärzten behandelt wird. In der Einwilligung in diese Behandlung liegt auch die konkludente Einwilligung in die Weitergabe der erforderlichen Daten an den weiter- oder mitbehandelnden Arzt. Die Frage nach dem Vorliegen wenigstens einer konkludenten Einwilligung stellt sich auch im Fall der Übermittlung von Krankenhausberichten an den einweisenden Arzt, sowie an nachbetreuende nichtärztliche Einrichtungen (z.B. Sozialdienst, Pflegeeinrichtungen) einschließlich der Einrichtungen zur Rehabilitation.

   Aufgrund einer Eingabe und der Anfrage eines Krankenhauses hatte ich zu der Frage Stellung zu nehmen, in welchen Fällen Bedenken gegen die Übermittlung eines Patientenberichts vom Krankenhaus an einen niedergelassenen Arzt bestehen könnten. Solche Bedenken können sich aus der ärztlichen Schweigepflicht (§ 203 StGB) und Art. 13 Bayer. Krankenhausgesetzes ergeben, der die Fragen der Schweigepflicht für den Bereich der dem Gesetz unterliegenden Krankenhäuser konkretisiert, materiell jedoch nicht erweitert. Nach den Regeln der ärztlichen Schweigepflicht und nach Art. 13 Abs. 5 BayKrG ist die Weitergabe von Patientendaten nur erlaubt, wenn eine, sei es auch konkludente, Einwilligung des Patienten vorliegt. Nach einhelliger Meinung gilt die Schweigepflicht auch für die Weitergabe an einen Arzt (vgl. BGHSt 4, 356; Dreher/Tröndle, StGB § 203, Anm. 28, und Laufs, Die Entwicklung des Arztrechts 1979/80, NJW 80 1219). § 2 Abs. 7 der Ärztlichen Berufsordnung, der die Ärzte untereinander von der Schweigepflicht befreit sieht, solange der Patient nichts anderes bestimmt, ist entsprechend auszulegen. Durch die Regelung der Berufsordnung könnte die Verfügungsbefugnis des Patienten über seine Krankheitsdaten nicht eingeschränkt werden (vgl. Schönke/

Schröder, StGB § 203, Anm. 27). Zu der angesprochenen Frage sind verschiedene Varianten denkbar:

a) Das Krankenhaus gibt die Behandlung an einen niedergelassenen Arzt erstmals ab,

b) das Krankenhaus ist aufgrund einer Einweisung tätig geworden, und der Patient begibt sich nach Behandlung im Krankenhaus in die Behandlung des einweisenden Arztes zurück,

c) wie b, der Patient kehrt nach der Krankenhausbehandlung nicht mehr zum einweisenden Arzt zurück oder wechselt den Arzt.

Für alle Varianten ist die Einwilligung des Patienten Voraussetzung der Weitergabe von Untersuchungdaten des Krankenhauses an den niedergelassenen Arzt. In Übereinstimmung mit der bisherigen Rechtsprechung zu § 203 StGB vertrete ich die Ansicht, daß auch hier in bestimmten Fällen das Vorliegen einer konkludenten Einwilligung angenommen werden kann. Mit der Rechtsprechung ist jedoch zu fordern, daß die Grenzen für die Annahme einer mutmaßlichen Einwilligung nicht zu weit zu ziehen sind und in Zweifelsfällen stets von der Notwendigkeit einer positiven Einwilligung ausgegangen werden muß. Für die genannten Varianten ergibt sich folgende Beurteilung:

a) Die Übermittlung der Patientendaten an einen bisher noch nicht tätig gewordenen, niedergelassenen Arzt kann sich auf die Annahme einer konkludenten Einwilligung stützen, wenn sich der Patient gegenüber dem Krankenhaus mit der Weiterbehandlung oder Nachsorge durch diesen Arzt einverstanden erklärt hatte.

b) Wurde das Krankenhaus aufgrund Einweisung eines niedergelassenen Arztes tätig, so ist die Weitergabe der Daten an den einweisenden Arzt als von der Einwilligung des Patienten gedeckt anzusehen, wenn dieser in die Behandlung des einweisenden Arztes zurückkehrt.

c) Will der Patient nach der Krankenhausbehandlung nicht mehr zum einweisenden Arzt zurückkehren, z.B. bei Weiterbehandlung durch einen anderen Arzt und tut er dies auch gegenüber dem Krankenhaus kund, so kann nicht mehr ohne weiteres von einer Einwilligung in die Datenübermittlung an den einweisenden Arzt ausgegangen werden. Will das Krankenhaus dem einweisenden Arzt trotzdem den Krankenhausbericht zukommen lassen, z.B. um diesem die Kontrolle über die Richtigkeit seiner vorausgegangenen Diagnose zu ermöglichen, so muß es hierzu die Einwilligung des Patienten einholen (vgl. auch Laufs, Entwicklung des Arztrechts 1979/80, NJW 80, 1219).

Hält es ein Krankenhaus im Interesse der Ärzteschaft für erforderlich, den Krankenhausbericht an den einweisenden Arzt in jedem Falle weiterzugeben, so empfiehlt es sich, hierzu grundsätzlich die Einwilligung des Patienten einzuholen. Aus der Verweigerung der Einwilligung darf ihm jedoch kein Nachteil entstehen.

2. Weitergabe von Patientendaten zur Abrechnung der Behandlung:

Patientendaten werden in größerem Umfang zur Abrechnung der Behandlung an Sozialleistungsträger weitergegeben. In vielen Fällen erledigt dies für die Krankenhäuser ein Auftragnehmer im automatisierten Verfahren. Die Leistungsträger benötigen zur Prüfung sowohl des Ausmaßes als auch der Voraussetzungen ihrer Kostenerstattungspflicht Patientendaten, die nicht nur reine Verwaltungsdaten sind, sondern auch in gewissem Umfang Diagnosen und Befunde enthalten. Die Befugnis zur Weitergabe solcher Daten an Sozialleistungsträger leitet sich aus den vom Patienten gegenüber dem Krankenhaus bekanntgegebenen Wunsch ab, die Leistungen mit dem Leistungsträger abzurechnen. Der Patient ist nach dem Sozialversicherungsrecht als Folge seines Kostenübernahmeantrags - in erforderlichem Umfang - zur Mitwirkung verpflichtet. Eine darüber hinausgehende Übermittlung weiterer Daten an den Leistungsträger würde allerdings die gesonderte Einwilligung des Patienten voraussetzen. Art. 13 BayKrG sieht dementsprechend die für Abrechnungszwecke erforderliche Übermittlung als zulässig an. Diese Befugnis umfaßt auch die Offenbarung der Verwaltungs- und Abrechnungsdaten einschließlich der Abrechnungsdiagnosen oder -Befunde an den sorgfältig ausgewählten Auftragnehmer zur Abwicklung der automatisierten Verarbeitung. Diese unterliegt ihrerseits gesetzlichen Bindungen aus Art. 3 BayDSG sowie vertraglichen Bindungen mit Krankenhäusern. Der Auftragnehmer hat die erforderlichen Sicherungsmaßnahmen zu treffen.

Wie schon im Berichtsjahr 1981 (siehe 4. Tätigkeitsbericht Nr. 3.4.5 Seite 31) wurde auch im Berichtsjahr 1982 wieder festgestellt, daß Daten von Krankenhauspatienten dem Sozialamt gemeldet werden, obwohl dies zur Klärung der Kostenübernahme nicht erforderlich ist. Die vorsorgliche Meldung einer Vielzahl von Patienten an das Sozialamt - ohne konkrete Anhaltspunkte für dessen Zuständigkeit - ist nach Art. 13 Abs. 4 des Bayer. Krankenhausgesetzes unzulässig und verstößt gegen die ärztliche Schweigepflicht. Zur Vermeidung einer Versäumung der Frist nach § 121 BSHG wurde empfohlen, auf örtlicher Ebene eine Absprache zwischen Krankenhaus und Sozialhilfeträger zu treffen. Ich habe mit dieser Empfehlung den Hinweis verbunden, daß ich die Angabe der Krankheit, wegen der sich der Betroffene in Krankenhauspflege befindet, auf den Anzeigen über Krankenhauspflege nach § 121 BSHG nicht für notwendig und damit für unzulässig erachte, nachdem die einschlägigen Fragen in einem eigenen „ärztlichen Fragebogen zur Feststellung des sachlich zuständigen Sozialhilfeträgers" festgehalten werden.

3. Übermittlung von Patientendaten für Aufgaben der öffentlichen Verwaltung bzw. der Gerichte:

Die Übermittlung von Patientendaten an Behörden der Hoheitsverwaltung sehen beispielsweise das Bundesseuchengesetz oder das Gesetz zur Bekämpfung von Geschlechtskrankheiten vor. Außer in gesetzlich normierten Fällen ist zwar keine Befugnis, aber eine Rechtfertigung für den einzelnen Arzt bei Weitergabe medizinischer Daten von der Rechtsprechung für besondere Fälle anerkannt worden, in denen eine erhebliche gegenwärtige Gefahr für ein höherwertiges Rechtsgut nur durch die Übermittlung von Angaben über einen Patienten abgewendet werden kann (rechtfertigender Notstand, § 34 StGB). Ein darüber hinausgehendes allgemeines Recht des Arztes zur Güterabwägung und Offenbarung medizinischer Daten besteht dagegen nicht. Eine Befugnis von Krankenhäusern oder anderen öffentlichen Stellen, denen die in § 203 StGB genannten Personen angehören, läßt sich hieraus angesichts der klaren Regelung in § 13 BayKrG nicht ableiten. § 2 der Berufsordnung für die Ärzte Bayerns ist in diesem Sinne auszulegen.

Übermittlung von Patientendaten bei der Erstattung ärztlicher Gutachten:

Basis der ärztlichen Schweigepflicht ist der Vertrauensschutz, den der Patient genießt. Deswegen kann die Schweigepflicht dort eingeschränkt sein, wo ein Vertrauensverhält-

nis nicht notwendig und nicht in allen Fällen bestehen muß. Dies ist z.B. der Fall bei der Erstattung medizinischer Gutachten vor Gericht und teilweise bei amtsärztlichen Untersuchungen. Grundlage der ärztlichen Tätigkeit ist in diesen Fällen nicht das Einverständnis des Patienten, sondern eine gesetzliche Pflicht (z.B. aufgrund von § 81 a StPO), die ärztliche Tätigkeit zu dulden. Im Rahmen dieser Duldungspflicht können Informationen auch ohne Einwilligung des Betroffenen an Stellen weitergegeben werden, die die ärztliche Gutachtentätigkeit befugterweise angeordnet haben. Dies gilt aber nur für Angaben, die für die Durchführung des Gutachtensauftrages erforderlich sind.

4. Weitergabe von Patientendaten für Forschung und Statistik:

   Für die medizinische Forschung stellt sich, wie für andere Forschungsvorhaben, die Frage nach dem Verhältnis von Wissenschaftsfreiheit zu Datenschutz. Ich verweise hierzu auch auf Ausführungen im 4. Tätigkeitsbericht Nr. 3.6.1 (S. 37). Daß die Wissenschaftsfreiheit nach Art. 5 Abs. 3 Satz 1 GG nicht durch Gesetz beschränkt werden kann, steht der Notwendigkeit, einen Ausgleich zu finden, nicht entgegen. Auch die Wissenschaftsfreiheit ist nicht gänzlich schrankenlos gewährt. In einem Spannungsverhältnis mit anderen Grund- und Verfassungsrechten kommt ihr gegenüber kollidierenden, gleichfalls verfassungsrechtlich geschützten Prinzipien nicht schlechthin der Vorang zu (BVerfG E 57,70/99).

   Schweigepflichtprobleme ergeben sich im Forschungsbereich in verschiedenen Fallkonstellationen. Unproblematisch ist in der Regel der Fall, daß der behandelnde Arzt selbst mit den von ihm erhobenen Daten forscht. Schwierigkeiten ergeben sich dagegen oft, wenn andere Forscher der gleichen Klinik oder von anderen Kliniken oder andere Institute, die selbst keinerlei Patientenbetreuung betreiben, die vom behandelnden Arzt erhobenen Daten zu Forschungszwecken erbitten.

   4.1 An erster Stelle ist regelmäßig zu prüfen, ob Patientendaten vor ihrer Weitergabe **anonymisiert** werden könnten. Nach h. A. ist die Zuverlässigkeit der Anonymisierung von dem Aufwand abhängig, der für die Reidentifizierung von Personen erforderlich wäre. Der Aufwand wird für verschiedene Empfänger derselben Daten unterschiedlich sein. Daher wird die Anonymisierungsfrage auch von Empfänger zu Empfänger verschieden zu beantworten sein. Schließlich ist in die Prüfung des Aufwands auch einzubeziehen, ob dritte Stellen - beispielsweise über ein Beschlagnahmerecht - die Daten beim Empfänger in Anspruch nehmen könnten, was ihnen beim Arzt verwehrt wäre. Auch die Reidentifizierungsmöglichkeiten einer solchen beschlagnahmenden Stelle wären deshalb unter Umständen in die Überlegungen mit einzubeziehen.

   Für bestimmte Forschungsvorhaben wird jedoch geltend gemacht, daß anonymisierte Daten nicht ausreichen. Soll z.B. ein Krankheitsverlauf über längere Zeit verfolgt werden, so bedarf es einer Möglichkeit, immer wieder neue Nachrichten zur vorhandenen Information hinzuzufügen. Hierfür ist eine eindeutige und gleiche Kennzeichnung der vorhandenen, wie der hinzuzufügenden Daten des Falls bzw. der Person des Patienten erforderlich. Damit kann eine Reidentifizierungsmöglichkeit der Person verbunden sein, sodaß eine Anonymisierung nicht gegeben ist. Voraussetzung einer Weitergabe nicht anonymisierter Daten ist aber eine hinreichende Befugnis.

   Für die Durchführung einer bayerischen Perinatalerhebung durch die Kassenärztliche Vereinigung Bayerns (KV) wurde durch einen entsprechenden Erhebungsbogen und durch vertragliche Absicherung zwischen Kassenärztlicher Vereinigung und den beteiligten Kliniken sichergestellt, daß eine tatsächliche Anonymisierung der erhobenen Daten gegenüber der KV erreicht und die Verfügungsgewalt über die Daten eindeutig geregelt wird. Besonderes Gewicht habe ich darauf gelegt, daß die Daten aus dem perinatologischen Basis-Erhebungsbogen nicht an andere Stellen weitergegeben werden, denn die Frage der Verläßlichkeit der Anonymisierung, also der weitgehenden Unmöglichkeit der Reidentifizierung einzelner Personen, hängt wesentlich von dem Zusatzwissen der Stelle ab, die die Daten besitzt. Diese Frage müßte für jeden eventuellen Empfänger der Daten neu überprüft werden.

   4.2 Fehlt eine gesetzliche Befugnis zur Offenbarung, wie sie z.B. im Seuchenrecht gegeben ist, ist die **Einwilligung** des Patienten erforderlich. Auf die Schaffung gesetzlicher Befugnisse zur Offenbarung von Patientendaten für Forschungszwecke wird von Forschern derzeit gedrängt. Zur Begründung wird darauf verwiesen, daß den Patienten in Fällen von gravierenden Krankenheiten die vorherige Einwilligung oft nicht zumutbar sei, da sie teilweise über die Art ihrer Krankheit nicht aufgeklärt seien.

   Soweit dieser Hinderungsgrund nicht besteht, ist die Einholung der Einwilligung aber mit anderen Problemen belastet: Im Zeitpunkt, in dem die Einwilligung eingeholt werden müßte, ist u. U. nicht hinreichend konkret bekannt, was mit den Daten geschehen soll, so daß auch etwaige Gefährdungen kaum kalkulierbar sind. Hieraus können sich Zweifel an der rechtlichen Wirksamkeit der Einwilligung ergeben. Denkbar ist auch, daß der Patient bei Verweigerung der Einwilligung Nachteile befürchtet. Ihm muß deshalb zugesichert werden, daß die Verweigerung keine Nachteile bei der medizinischen Versorgung zur Folge hat. Schließlich wird der Patient auch keine hinreichende Klarheit darüber gewinnen können, inwieweit seine personenbezogenen Daten noch durch die o.g. Vorschriften der StPO geschützt sind. Die Einwilligung stellt mithin kaum einen Schutz gegen Gefahren, sondern eher deren Inkaufnahme dar. Die Datenschutzbeauftragten der Länder und des Bundes und die Datenschutzkommission Rheinland-Pfalz haben in einem gemeinsamen Beschluß in ihrer Konferenz zum Entwurf eines Krebsregistergesetzes die Notwendigkeit der Einwilligung des Betroffenen hervorgehoben und sechs Forderungen aufgestellt, die den Schutz personenbezogener medizinischer Daten in einer Forschungsdatenbank auch rechtlich sichern sollen. Die Notwendigkeit solcher rechtlichen Sicherungen wird besonders wegen der Anziehungskraft, die große Datensammlungen auf verschiedenste Arten von Interessenten ausüben, gesehen (s.a. 4. Tätigkeitsbericht, Nr. 3.6.2, S. 37 - 39).

   Für eine Studie „Luftverunreinigung und Krankenhauseinweisungen" im Rahmen eines Umwelt-Forschungsprojekts an der Ludwigs-Maximilians-Universität München wurde zusammen mit dem hierfür zuständigen Institut der Universität das Muster einer Erklärung ausgearbeitet, die den betroffenen Patienten mit der Bitte um Erteilung ihrer Einwilligung in die Verwendung ihrer Daten für Forschungszwecke vorgelegt werden soll. Zum Schutze der Betroffenen wurde vereinbart, daß die erfaßten Patientendaten ausschließlich für die genannte Studie verwendet werden, daß alle Unterlagen, die eine Identifikation der Patienten ermöglichen,

spätestens nach Abschluß der Studie unverzüglich vernichtet werden und der Landesbeauftragte für den Datenschutz hiervon unterrichtet wird.

In einem anderen Fall, in dem für Forschungszwecke Patientendaten erforderlich waren, konnte dank der Aufgeschlossenheit des Forschungsinstituts zur Lösung der Schweigepflicht-Frage folgende praktikable Lösung gefunden werden: Die Patienten wurden um ihre Einwilligung in die Offenbarung einzelner genau definierter Daten aus den Krankenunterlagen gebeten. Die Forschungsstelle erhielt nicht die Krankenunterlagen ausgehändigt, sondern ein Mitarbeiter des Krankenhauses wählte die erforderlichen Daten aus den Unterlagen aus und teilte sie dem Forscher mit.

Auf Grund eines von einer Krankenhausverwaltung vorgelegten Musters für eine Einwilligung von Patienten bestand Veranlassung auf folgende - auch allgemein interessierenden - Punkte hinzuweisen. Die Erklärung ließ nicht mit ausreichender Sicherheit erkennen, daß die Daten - wie vorgesehen - für wissenschaftliche Zwecke in einem Tumorregister maschinell gespeichert werden sollten. Nach der Rechtsprechung wird eine Einwilligung nur dann als rechtswirksam angesehen, wenn der Einwilligende Wesen, Bedeutung und Tragweite seiner Entscheidung zu erfassen imstande ist. Dies setzt voraus, daß er über den Zweck und Umfang der Datenspeicherung und gegebenenfalls den Empfänger einer Datenübermittlung ausreichend unterrichtet wurde (siehe auch Schönke/Schröder zu § 32 StGB Rdnr. 40). Der vorgelegte Krankenhausaufnahmevertrag enthielt außerdem eine Einwilligungserklärung über die Weitergabe von Patientendaten an den weiterbehandelnden Arzt. Andere evtl. infrage kommende Datenübermittlungen wie an den Krankenhausseelsorger, an Studenten oder Doktoranden waren jedoch nicht angesprochen. Hierzu vertrete ich die Auffassung, daß eine Weitergabe von Patientendaten innerhalb des Krankenhauses mit dem Ziele der medizinischen Versorgung des Patienten im Rahmen des bestehenden Behandlungsvertrages zwischen Arzt oder Krankenhaus und Patient ohne weitere Formalitäten zulässig ist, wenn ein gegenteiliger Wille des Patienten nicht erkennbar ist. Bei Datenübermittlungen für andere als Behandlungszwecke (z.B. für Ausbildung, Fortbildung, Forschung, Überprüfung ärztlicher Prognosen, Krankenhausseelsorge usw.) kann eine konkludente Einwilligung jedoch nicht ohne weiteres unterstellt werden. Im Zweifel ist hierfür die Einholung der ausdrücklichen Einwilligung erforderlich (§ 203 StGB, Art. 13 Bayer. KrHG).

Im Zuge eines Forschungsprojekts einer bayerischen öffentlichen Stelle über behinderte Kinder waren auch Namen und Anschriften der Eltern gespeichert worden. Eine Klinik, in der am Forschungsprojekt beteiligte Kinder behandelt worden waren, forderte die Bekanntgabe von Namen und Anschriften der Eltern aus dem Forschungsprojekt, ohne daß die Einwilligung der Eltern hierzu vorgelegen hätte. Die Zulässigkeit der Übermittlung der Anschriften aus einer Datei der öffentlichen Stelle an die Klinik war nach Art. 18 BayDSG zu beurteilen, da das anfordernde Krankenhaus als öffentliche Stelle, die am Wettbewerb i. S. v. Art. 22 Abs. 1 BayDSG teilnimmt, anzusehen war (siehe auch 3. Tätigkeitsbericht Nr. 3.4.2, S. 20). Beide Varianten des Art. 18 Abs. 1 BayDSG waren nicht erfüllt. Die über den Forschungszweck hinausgehende Bekanntgabe der Namen der Eltern war zum einen zur rechtmäßigen Aufgabenerfüllung des Forschungsinstituts nicht erforderlich. Des weiteren hatte das Krankenhaus zwar ein berechtigtes Interesse an der Kenntnis der Namen der Eltern glaubhaft gemacht. Im konkreten Falle war jedoch zu befürchten, daß durch die Bekanntgabe der Namen der Eltern das Behandlungsverhältnis in negativer Weise beeinflußt würde. Die Übermittlung hätte deshalb schutzwürdige Belange der Betroffenen beeinträchtigt. Sie war daher gem. Art. 4 Abs. 1 BayDSG unzulässig.

5. Verschiedene Fälle von Datenübermittlungen haben in der Vergangenheit zu Erörterungen in der Öffentlichkeit geführt:

   In einem anderen Bundesland war eine zentrale Sammlung psychiatrischer Daten - ohne Einwilligung der Betroffenen -eingerichtet worden. Eine solche Sammlung existiert in Bayern, soweit ich feststellen konnte, nicht. In den verschiedenen Bezirkskrankenhäusern bzw. Universitätskliniken werden Patientendaten auf örtliche Ebene geführt und ggf. wissenschaftlich ausgewertet. Die bayerischen Bezirkskrankenhäuser haben ein Projekt medizinischer Basisdokumentation über die aufgenommenen Patienten dezentral bei den einzelnen psychiatrischen Krankenhäusern der Bezirke in Angriff genommen. Bei einigen Krankenhäusern sind bereits entsprechende Kleinrechner (MehrplatzSysteme) eingerichtet werden. Probleme der Verschwiegenheitspflicht der ärztlichen und nichtärztlichen Geheimnisträger der Bezirkskrankenhäuser bei Abwicklung der personenbezogenen Basisdokumentation im automatisierten Verfahren bei einem Auftragnehmer außerhalb des Krankenhauses wurden damit vermieden (s.a. 2. Tätigkeitsbericht Nr. 4.1.4.2 S. 21).

   Ein zentrales Krebsregister existiert in Bayern nicht. Krebsdatensammlungen sind bisher lediglich bei größeren Kliniken festgestellt worden, wobei Ausgangsbasis die Daten der behandelten Patienten waren. Die Aufnahme von Daten anderer Kranker in solche Register setzt eine Befugnis aus dem jeweiligen Behandlungsvertrag oder aus einer besonderen Einwilligung voraus. In einer ganzen Reihe von Forschungsvorhaben konnte in Zusammenarbeit zwischen Forschern und Landesbeauftragten für den Datenschutz entweder eine Anonymisierung oder eine rechtzeitige Einholung der Einwilligung erreicht werden.

4.2.2 Gesundheitsämter

Aus der Sicht der Datenerhebung und Speicherung läßt sich die Tätigkeit der Gesundheitsämter in 3 Bereiche teilen:

- Der hoheitlich-sicherheitsrechtliche Bereich, z.B. Vollzug des Bundesseuchengesetzes, des Geschlechtskrankheitengesetzes,
- der gutachtliche Bereich mit duldungspflichtigen Gutachten, beispielsweise im Rahmen des Verwahrungsgesetzes oder nicht duldungspflichtigen Gutachten, wie Stellungnahmen zur Einstellung oder Verbeamtung, zur Gewährung von Kuren oder zur Begutachtung von Behinderten,
- die Beratungstätigkeit des Gesundheitsamtes auf freiwilliger Basis, wie z.B. Mütter-, Säuglings-, Suchtberatung.

Im Gesundheitsamt sammelt sich eine große Zahl personenbezogener Daten an, und zwar sowohl über eine Vielzahl der im Zuständigkeitsbereich wohnenden Personen, nämlich die im Schulkindesalter erhobenen Daten aus der Schulgesundheitspflege als auch Daten über die verschiedensten Sachverhalte, wie Röntgenbefunde, Untersuchungen für öffentliche Arbeitgeber, Sachverhalte nach dem Bundesseuchengesetz, Angaben über Behinderte, Mütter, Schwangere, Drogensüchtige u.a.. Über manche Bewohner des Bereichs sind also Informationen vorhanden, die weit in die geschützte Privatsphäre reichen, über die große Mehrzahl allerdings nur sehr wenige Angaben.

Aus der Sicht des Datenschutzes ist vor allem zu prüfen, inwieweit im Gesundheitsamt Angaben, die für einen Zweck erhoben wurden, auch für den Vollzug eines anderen Gesetzes verwendet werden dürfen, ohne Vertrauensverhältnisse oder Schweigepflichten zu verletzen. Hieraus ergeben sich beispielsweise Folgerungen für die Art der Datenaufbewahrung im Amt und für die Frage des zulässigen Umfangs zentraler Karteien. Eine Aufgabenzuweisung dergestalt, daß die Gesundheitsämter alle Angaben zu einer Person zusammenzuführen und gemeinsam zu bewerten hätten, um die verschiedenen übertragenen Aufgaben zu vollziehen, fehlt.

Rechtsgrundlage für die Tätigkeit des Gesundheitsamtes ist derzeit das Gesetz über die Vereinheitlichung des Gesundheitswesens vom 3. Juli 1934 mit den hierzu ergangenen drei Durchführungsverordnungen. Die Vorschriften enthalten nach inzwischen gewandelter Auffassung allerdings im wesentlichen nur Aufgaben- nicht jedoch Befugniszuweisungen. Weitere Aufgaben, aber auch Befugnisse, ergeben sich aus dem Bundesseuchengesetz und dem Geschlechtskrankheitengesetz, dem Bundesozialhilfegesetz, dem Röntgenreihenuntersuchungsgesetz und dem Bayer. Schwangerenberatungsgesetz, aus der Bestattungsverordnung und hinsichtlich der Schulgesundheitspflege aus dem neuen Erziehungs- und Unterrichtsgesetz.

Der Landesbeauftragte für den Datenschutz überprüft in Zusammenarbeit mit einigen Gesundheitsämtern die Sach- und Rechtslage zur Datenspeicherung und -übermittlung. Ziel ist es, praktikable Vorschläge für die Organisation und Handhabung der Datensammlungen im Gesundheitsamt zu erarbeiten.

Eine Eingabe zur Frage der Datenübermittlung zwischen Amtsarzt und Dienstherrn anläßlich der Einstellung im öffentlichen Dienst gab Anlaß, folgendes festzustellen: Die auf Verlangen des Dienstherrn, mit Einverständnis des Betroffenen durchgeführte amtsärztliche Untersuchung steht ebenso wie andere ärztliche Untersuchungen unter dem Gebot der ärztlichen Schweigepflicht (vergleiche Dreher/Tröndle StGB § 203 Rdnr. 8). Eine Durchbrechung der Schweigepflicht setzt eine gesetzliche Befugnis oder die Einwilligung des Betroffenen voraus, wobei im Einzelfall auch konkludentes Handeln des Betroffenen hinreichen kann (vergl. Dreher/Tröndle § 203 StGB Rdnr. 28). Bei Einstellungsuntersuchungen ist von einer konkludenten Einwilligung in die Mitteilung des Untersuchungsergebnisses an den Dienstherrn auszugehen. Der Bewerber, der sich auf das zulässige Verlangen des Dienstherrn hin einer Eignungsuntersuchung unterzieht, weiß, daß die Untersuchung erfolgt, um dem Dienstherrn die Bewertung seiner Eignung mitzuteilen. Indem er sich der Untersuchung unterzieht, erteilt er seine konkludente Einwilligung in diese Mitteilung, so weit sie zur Beurteilung seiner Eignung erforderlich ist. Letzteres bedeutet, daß die Einwilligung auf das erforderliche Maß der Unterrichtung des Dienstherrn durch den Arzt beschränkt ist. Dies ermöglicht es dem Dienstherrn, sich ein Urteil über die Eignung zu bilden und über die Bewerbung zu entscheiden. Die Einwilligung bezieht sich daher auf die Mitteilung des Ergebnisses der Einstellungsuntersuchung, nicht jedoch auf die Übermittlung der Beurteilungsgrundlage des Arztes, die die einzelnen Diagnose- und Anamnesedaten enthält.

Die bayerischen Staatsministerien haben einheitliche Bekanntmachungen erlassen, nach denen bei ärztlichen Untersuchungen in dienstrechtlichen Angelegenheiten in der geschilderten Weise verfahren werden soll. So heißt es z.B. in der Bekanntmachung des Bayer. Staatsministeriums des Innern vom 28.1.1981, daß die Gesundheitsämter den personalbewirtschaftenden Stellen das Untersuchungsergebnis nach dem Formblatt „Gesundheitszeugnis" mitteilen. Ein Formblatt „Beurteilungsgrundlage" mit den Anamnese- und Diagnosedaten verbleibt beim Gesundheitsamt. In das Gesundheitszeugnis ist lediglich eine „zusammenfassende Äußerung zu den Gutachtenfragen und zur Belastbarkeit sowie die Wertung aller Besonderheiten, die sich aus der Vorgeschichte, Untersuchung im Gesundheitsamt und gegebenenfalls ergänzenden Befunden unter Berücksichtigung etwaiger vom Auftraggeber bezeichneter Anforderungen" ergeben, aufzunehmen.

Eine Mitteilung an den (künftigen) Dienstherrn, die darüber hinausgehende Angaben enthielte, ist seit Inkrafttreten der o.g. Bekanntmachungen als unzulässig anzusehen. Außerdem kann nicht angenommen werden, daß sich eine konkludente Einwilligung des Betroffenen auf mehr Angaben erstreckt als nach der Bekanntmachung vorgesehen sind. Dies gilt auch in Fällen, bei denen der Dienstherr den begutachtenden Arzt selbst stellt (z.B. für Personal in Krankenhäusern).

4.2.3 Sozialleistungsträger

Die Sozialleistungsträger, besonders die Krankenkassen, besitzen die größte derzeitig existierende Sammlung von Gesundheitsdaten. Hier treten oft Datenschutzfragen auf. Besondere gesetzliche Datenschutzregelungen sind im Sozialgesetzbuch zu finden.

§ 35 SGB I regelt das „Sozialgeheimnis". Danach hat jeder Anspruch darauf, daß Einzelangaben über seine persönlichen und sachlichen Verhältnisse von den Leistungsträgern als Sozialgeheimnis gewahrt und nicht unbefugt offenbart werden. Leistungsträger sind dabei nicht nur die gesetzlichen Krankenkassen, Ersatzkassen und Rentenversicherungen, sondern beispielsweise im kommunalen Bereich das Sozialamt, die Wohngeldstelle, das Jugendamt, soweit ihnen Aufgaben nach dem SGB übertragen sind. Auch die Aufsichts-, Rechnungsprüfungs- oder weisungsberechtigten Behörden unterliegen dem Sozialgeheimnis.

Die Regelungen gelten auch für die Verbände und Arbeitsgemeinschaften der Sozialleistungsträger, für die Kassenärztliche Vereinigung und die Kassenzahnärztliche Vereinigung Bayerns, da beide Einrichtungen ihre Aufgabe, die ärztliche Versorgung der Bevölkerung sicherzustellen, aus der Reichsversicherungsordnung herleiten.

Von Bedeutung ist, daß nach § 35 Abs. 3 SGB I keine Auskunftspflicht, Zeugnispflicht oder Pflicht zur Vorlegung oder Auslieferung von Schriftstücken, Akten, Dateien oder sonstigen Datenträgern besteht, soweit eine Offenbarung personenbezogener Daten nicht zulässig ist. Zulässig ist eine Offenbarung gem. § 35 Abs. 2 SGB I nur unter den Voraussetzungen der §§ 67 bis 77 des X. Buches des SGB. Auf all diese Offenbarungsvorschriften im einzelnen einzugehen, würde den Rahmen dieser Darstellung sprengen. Unter dem Gesichtspunkt Datenschutz im Gesundheitswesen ist aber hervorzuheben, daß nach § 76 SGB X die Offenbarung personenbezogener Daten, die einer in § 35 SGB I genannten Stellen von einem Arzt oder einer anderen in § 203 Abs. 1 und 3 StGB genannten Person zugänglich gemacht worden sind, nur unter den Voraussetzungen zulässig ist, unter denen diese Person selbst offenbarungsbefugt wäre. Diese Regel wird nach § 76 Abs. 2 SGB X für Offenbarungen, die zum Zwecke der Erfüllung sozialer Aufgaben gem. § 69 SGB I Nr. 1 erforderlich sind, und für Daten, die im Zusammenhang mit einer Begutachtung wegen der Erbringung von Sozialleistung oder wegen Ausstellung einer Bescheinigung zugängig gemacht worden sind, durchbrochen, so daß jedenfalls für Offenbarungen innerhalb des Sozialbereichs das Verbot der Weitergabe von Gesundheitsdaten weithin aufgehoben ist. Doch könnte der Betroffene einer solchen Offenbarung widersprechen, wenn er die sich daraus ergebenden Folgen zu tragen bereit wäre.

In diesem Zusammenhang ist auf eine Auslegungsschwierigkeit hinzuweisen. § 76 Abs. 1 SGB X schränkt die Weitergabe

von Daten ein, die dem Sozialleistungsträger von einem Arzt zugängig gemacht worden sind. Teilweise wird hieraus geschlossen, dies könne nur der Fall sein, wenn der Arzt selbst nicht Beschäftigter des Sozialleistungsträgers sei. Dies würde jedoch zu dem willkürlichen Ergebnis führen, daß medizinische Angaben, die der Sozialleistungsträger vom Hausarzt, einem Krankenhaus oder einem sonstigen außenstehenden Arzt erhalten hat, geschützt wären, während die Angaben, die der Betroffene einem vom Sozialleistungsträger beschäftigten Arzt als Arzt anvertraut hat, von diesem Schutz ausgenommen wären. Demgegenüber steht die Ärzteschaft - wie ich meine zu Recht - auf dem Standpunkt, daß auch der Amtsarzt zur Verschwiegenheit verpflichtet ist, es sei denn, daß dem Betroffenen vor der Untersuchung oder Behandlung bekannt ist oder eröffnet wird, inwieweit die vom Arzt getroffenen Feststellung zur Mitteilung an Dritte bestimmt sind (s.a. § 2 Abs. 5 der Berufsordnung für die Ärzte Bayerns vom 1.1.1978 i.d.F. des Beschlusses des 32. Bayer. Ärztetages vom 14.10.1979). Der 85. Deutsche Ärztetag in Münster am 12.5.1982 hat dies erneut bekräftigt. Danach muß auch der angestellte oder beamtete Arzt gegenüber seinem Arbeitgeber oder Dienstherrn die Schweigepflicht wahren, wenn nicht für den Betroffenen erkennbar ist, daß Zweck der Untersuchung oder Begutachtung eine Mitteilung an den Arbeitgeber oder eine andere öffentliche Stelle ist. Will ein Sozialleistungsträger oder eine andere öffentliche Stelle die von ihrem beamteten oder angestellten Arzt erhobenen Angaben in personenbezogener Form verwerten oder weitergeben, so muß sie daher dafür sorgen, daß der Betroffene vor Beginn der Untersuchung oder Begutachtung Klarheit darüber erlangt, daß er sich nicht einem Arzt anvertraut, sondern einer Behörde Angaben macht.

Grundlage dieser Rechtsauffassung ist einmal der Gesetzeswortlaut in § 76 SGB X; der Tatbestand eines Datenaustausches wird sonst innerhalb des SGB X als Weitergabe oder Offenbaren umschrieben.

Vor allem sind medizinische Daten aber meist besonders sensible Daten, die aus einem Intimbereich stammen, in den grundsätzlich nur der Arzt aufgrund seiner Tätigkeit Einblick erlangt. Den Patienten verbindet mit dem Arzt regelmäßig ein besonderes Vertrauensverhältnis, das besonders geschützt werden muß. Ein solches Vertrauensverhältnis kann zu dem bei einem Leistungsträger beschäftigten Arzt genauso bestehen wie zu einem freipraktizierenden Arzt. Zudem besteht häufig auch mit einem bediensteten Arzt ein Behandlungsverhältnis (z.B. in Rehabilitationskliniken). Sinn und Zweck der Bestimmung des § 76 SGB X sprechen damit ebenfalls für eine umfassende Auslegung.

Die während des Gesetzgebungsverfahrens erstellte Begründung des Bundestags-Ausschusses für Arbeit und Sozialordnung zu § 76 SGB X widerspricht dieser Auffassung nicht. Die dort aufgeführte Fallgestaltung ist beispielhaft und beschreibt die möglichen Formen des „Zugänglichmachens" nicht abschließend.

Die Weitergabe von Patientendaten ist auch in der Neuregelung des § 372 Abs. 5 der Reichsversicherungsordnung (RVO) angesprochen. In der durch das Krankenhauskostendämpfungsgesetz vom 22.12.1981 (BGBl 1 Seite 568) geänderten Fassung lautet diese Bestimmung:

„Die Landesverbände schließen mit Wirkung für ihre Mitgliedskassen mit den Kassenärztlichen Vereinigungen sowie den in Abs. 1 genannten Krankenhäusern oder Vereinigungen von Krankenhäusern Verträge über die Zusammenarbeit zwischen

Ärzten und Krankenhäusern, insbesondere über die Einweisung in geeignete Krankenhäuser und die gegenseitige Unterrichtung und Überlassung von Krankenunterlagen."

Ich vertrete hierzu die Auffassung, daß diese Bestimmung keine Durchbrechung der Regeln der ärztlichen Schweigepflicht in § 203 StGB bzw. Art. 13 Bayer. Krankenhausgesetz gestattet. Meines Erachtens kann die Neuregelung nicht als Rechtsgrundlage für Verträge zwischen Ärzten und Krankenhäusern dienen, in denen eine Offenbarung von Patientendaten durch gegenseitige Unterrichtung und Überlassungvon Krankenunterlagen ohne Einwilligung des Patienten geregelt wird. Auch nach Inkrafttreten der Bestimmung ist die Einwilligung des Patienten - gegebenenfalls im Rahmen des Behandlungsvertrags - unabdingbare Voraussetzung für die Weitergabe von Patientendaten.

Es sind Befürchtungen an mich herangetragen worden, daß den Prüfungsausschüssen gemäß § 373 RVO zur Überwachung der Wirtschaftlichkeit in Krankenhäusern auch personenbezogene geschützte Angaben und Unterlagen von „Nicht-RVO-Mitgliedern" bzw. von Nichtversicherten vorgelegt würden, was gegen die verfassungsrechtlich garantierte Persönlichkeitssphäre verstoße. Meiner Ansicht nach kann eine Regelung der Reichsversicherungsordnung für diesen Personenkreis nicht gelten und entsprechende Auskunftspflichten der Krankenhausärzte gegenüber den Ausschüssen nicht auslösen.

4.2.4 Planungen für größere bzw. zentrale Krankheitsregister

1. Der Bundesminister für Jugend, Familie und Gesundheit hatte 1981 einen „Diskussionsentwurf, Muster eines Gesetzes über ein Krebsregister" durch eine Arbeitsgruppe ausarbeiten lassen. Danach sollte den Ärzten die nicht anonymisierte, sondern personenbezogene Meldung über seinen Krebspatienten an das Krebsregister völlig freistehen, zur Hebung der Motivation der Ärzte sollte eine Vergütung für jede Meldung gezahlt werden, dem Betroffenen selbst sollte jedoch nicht freigestellt werden, ob er mit Namen und Anschrift im Register gespeichert würde, seine Einwilligung sollte nach dem Entwurf grundsätzlich nicht zur Voraussetzung der Meldung gemacht werden. Das Freistellen der Meldung zeigt, daß der Entwurf nicht von einer lückenlosen Meldung aller Krebserkrankungsfälle ausgeht - was ein denkbares Forschungsziel wäre. Es muß daher nach Ansicht der Datenschutzbeauftragten der Länder und des Bundes geprüft werden, inwieweit die Einholung der Einwilligung der Patienten noch eine relevante zusätzliche Beeinträchtigung eines Registers verursachen würde, bevor den Betroffenen ein so erheblicher Eingriff in ihre Privatsphäre, wie eine zentrale personenbezogene Registrierung ihres schweren Krankheitsfalles ohne Einwilligung, zugemutet werden kann. Aus der Prüfung von Krebsregistern in Kliniken, die teilweise aufgrund der Behandlung von Patienten in der Klinik entstanden sind, die jedoch auch Patienten aus anderen Kliniken enthalten, ist bekannt, daß in der überwiegenden Mehrzahl der Fälle die Patienten ihre Einwilligung zu solcher Speicherung erteilen.

   Der Diskussionsentwurf ging davon aus, daß das Register lediglich als Nachweisregister dient, d.h. daß die eigentliche Forschungstätigkeit aufgrund von Daten durchgeführt werden soll, die noch zusätzlich von den Patienten, deren Adressen aus dem Register zu erfahren wären, nachträglich für den jeweiligen Forschungszweck erhoben würden. Voraussetzung für eine solche Patientenbefragung wäre auch nach dem Konzept des Musterentwurfs die vorherige schriftliche Einwilligung des Patienten.

   Die Landesbeauftragten und der Bundesbeauftragte für den Datenschutz haben zu dem Diskussionsentwurf eine Stellungnahme erarbeitet (s. 4. Tätigkeitsbericht, Nr. 3.6.2, S. 37 ff.). Ihre Bedenken und Vorschläge zielen darauf ab, die Freiheit der Forschung in ein ausgewogenes und recht-

die Freiheit der Forschung in ein ausgewogenes und rechtlich abgesichertes Verhältnis zu den grundrechtlich geschützten Belangen der Betroffenen zu bringen. Sinn und Nutzen von Krebsregistern zu beurteilen, ist nicht Aufgabe der Datenschutzbeauftragten. Sie warnten aber nachdrücklich vor der Gefahr, daß die Gesetzgebung zu einem Krebsregister ein erster Schritt zur Errichtung einer Vielzahl anderer Epidemiologieregister werden könnte, und wiesen auf die aus Kreisen der Ärzteschaft bekanntgewordenen erheblichen Zweifel am Nutzen zentraler medizinischer Register hin. Zentrales Anliegen für solche Vorhaben müßte daher eine Weiterentwicklung von Anonymisierungs- und Aggregationsmethoden sein, die Probleme, die sich durch ärztliche Schweigepflicht und Datenschutz ergeben, gar nicht erst aufkommen lassen.

2. Nicht auf die Krebserkrankungen beschränkt, sondern mit dem Ziele, alle bei den gesetzlichen Krankenkassen anfallenden Krankheitsdaten personenbezogen in ein automatisiertes Register zu übernehmen, wird die Konzeption für ein sog. „Mitgliederverzeichnis" nach § 319 a der Reichsversicherungsordnung (RVO) vorbereitet. Der Bundesminister für Arbeit und Sozialordnung hatte im Laufe des Jahres 1981 damit begonnen, durch eine Arbeitsgruppe die bei den Krankenkassen im wesentlichen anfallenden Daten auflisten und zu einem Datenkatalog zusammenstellen zu lassen.

   § 319a Reichsversicherungsordnung (RVO) sieht die Möglichkeit der Einrichtung eines sogenannten Mitgliederverzeichnisses der gesetzlichen Krankenkassen vor, das alle Daten über die Versicherten, somit auch bei den Krankenkassen vorhandene medizinische Daten der Versicherten, zusammenführen würde. Gegenwärtig werden nur die Daten über eine Arbeitsunfähigkeit bzw. einen Krankenhausaufenthalt bei den Krankenkassen bezogen auf die Person des Versicherten in der Leistungskartei geführt.

   Ein - mehr oder weniger zentrales - Mitgliederverzeichnis hätte mit Sicherheit zur Folge, daß die darin gespeicherten Gesundheits- bzw. Krankheitsdaten umfassender genutzt würden, als dies bisher bei der manuellen Führung der Fall ist. Andernfalls wäre der Aufwand eines automatisierten Mitgliederverzeichnisses nicht verständlich. Das Mitgliederverzeichnis würde ein Gesundheitsregister für den größten Teil der Bevölkerung, nämlich die Sozialversicherten, darstellen. Als umfassendes Register würde es daher auch immer mehr zusätzliche Nutzungen anziehen. Fehlende Nutzungsbefugnisse würden nach bisheriger Erfahrung im Lauf der Zeit möglicherweise durch Rechtsänderungen geschaffen. Der Interessenschwerpunkt hinsichtlich der bei den gesetzlichen Krankenkassen für Abrechnungszwecke registrierten Krankheiten und Behandlungen würde sich gegenüber der bisherigen Verwendung für Abrechnungszwecke wesentlich verlagern.

   Die Nutzung zu anderen als Abrechnungszwecken des einzelnen Krankheitsfalles würde die Betroffenen wohl zwingen, sich in erheblichem Umfang vorsorglich um die Richtigkeit der gespeicherten Daten zu kümmern, damit aus Unrichtigkeiten keine Nachteile für ihn entstehen können. Inwieweit dies bei den für Abrechnungszwecke registrierten Arbeitshypothesen und Verdachtsdiagnosen von Ärzten überhaupt möglich ist, muß bezweifelt werden.

   Um nachteilige Wirkungen sonstiger Nutzungen der Daten zu vermeiden, würden zumindest einzelne Betroffene wohl auch zu erreichen versuchen, daß ihr „Gesundheitskonto" möglichst wenig Informationen ausweist. Es würde versucht zu vermeiden, daß Informationen, die z.B. bei der Arbeitsplatzsuche oder seiner Erhaltung oder für den Ruf schädlich werden könnten, in das Register gelangen. Das könnte in Einzelfällen so weit führen, daß wegen Krankheiten, die in den Augen Dritter dem Ruf schädlich sein könnten, der Arzt nicht mehr auf Krankenschein aufgesucht würde oder die Inanspruchnahme des Arztes ganz entfiele, um die Weitergabe von Informationen über die Krankheiten an die Krankenkasse zu vermeiden. Versicherte würden also möglicherweise durch den psychischen Druck der gegenüber der Abrechnungsnutzung erweiterten öffentlichen Anteilnahme in der Entfaltung ihrer Persönlichkeit gehemmt und in ihrem Verhalten manipuliert.

   Es ist zu prüfen, ob eine solche „vollständige" Erfassung von Gesundheitsdaten der Sozialversicherten den verfassungsrechtlichen Grundentscheidungen der Art. 1 Abs. 1 und 2 Abs. 1 des Grundgesetzes entspräche. Das Bundesverfassungsgericht hat in seiner Mikrozensusentscheidung (E 27/5 ff) - wie oben bereits erwähnt - festgestellt, daß es der menschlichen Würde widerspräche „den Menschen zum bloßen Objekt im Staat zu machen" und daß es mit der Menschenwürde nicht vereinbar sei „wenn der Staat das Recht für sich in Anspruch nehmen könnte, den Menschen zwangsweise in seiner ganzen Persönlichkeit zu registrieren und zu katalogisieren, sei es auch in der Anonymität einer statistischen Erhebung, und ihn damit wie eine Sache zu behandeln, die einer Bestandsaufnahme in jeder Beziehung zugänglich ist". Wenn auch die Registrierung „lediglich" der Gesundheitsdaten keine Registrierung der gesamten Persönlichkeit wäre, so würde doch ein die Entfaltungschancen wesentlich beeinflussender Teil der Persönlichkeit registriert und katalogisiert. In dieser Entscheidung wird auch deutlich ausgesprochen, daß eine - wenn auch bewertungsneutrale - Einsichtnahme in den Persönlichkeitsbereich, die „die freie Entfaltung der Persönlichkeit durch den psychischen Druck öffentlicher Anteilnahme zu hemmen vermag", dem Staat versagt sei.

   Da die Registrierung aller Krankheiten eines Versicherten sehr weit in seinen Persönlichkeitsbereich eindringt, sehe ich eine gründliche Auseinandersetzung mit den Grundsätzen dieser Entscheidung bei der Vorbereitung eines zentralen Gesundheitsregisters für geboten an.

3. Zur Anziehungskraft großer Datensammlungen:

   Gerade im Bereich der besonders sensiblen medizinischen Daten muß das eingangs erwähnte Phänomen berücksichtigt werden, daß größere Datensammlungen, die mit einem gewissen Aufwand erstellt wurden und die einen neuen, größeren Überblick über einen bisher schlechter aufbereiteten Bereich geben, eine erhebliche Anziehungskraft auf verschiedene, oft vorher gar nicht erkennbare Interessentenkreise ausüben.

   Aus der Sicht des Datenschutzes sind deshalb für größere medizinische Datensammlungen nicht nur technisch-organisatorische Sicherungsmaßnahmen, sondern auch rechtliche Absicherungen gegen zunächst nicht beabsichtigte, dem eigentlichen Zweck widersprechende Nutzungen zu fordern.

4.3 **Sozialgeheimnis**

4.3.1 Datenübermittlungen im Sozialleistungsbereich

1. In letzter Zeit mehrten sich die Fälle, in denen Krankenhausverwaltungen gegenüber Patienten bei unklarer Kostenträgerschaft auf die Mitwirkungspflicht gemäß § 60 SGB I hinwiesen und Auskunft über Einkommensverhältnisse forderten. Die Krankenhausverwaltungen gingen in solchen Fällen davon aus, daß sie für die Sozialämter tätig werden. Das Bayer. Staatsministerium für Arbeit und Sozialordnung

hat nun klargestellt, daß Krankenhäuser in den genannten Fällen nicht für die Sozialämter tätig werden. Der Hinweis auf die Mitwirkungspflicht scheidet daher aus. Die Datenerhebung - auch hinsichtlich der Zahlungsfähigkeit des Patienten - bleibt Gegenstand des Vertragsverhältnisses mit dem Betroffenen. Soweit öffentliche Krankenhäuser, was die Regel ist, als Wettbewerbsunternehmen im Sinne des Art. 22 Abs. 1 BayDSG anzusehen sind, gilt für sie der dritte Abschnitt des Bundesdatenschutzgesetzes. Danach ist die Speicherung personenbezogener Daten im Rahmen der Zweckbestimmung eines Vertragsverhältnisses zulässig. Da die Angaben des Patienten über seine Einkommensverhältnisse gegenüber dem Krankenhaus somit nicht aufgrund einer verpflichtenden Rechtsnorm zu erhalten sind, ist auf eine der Rechtslage entsprechende Gestaltung der Erhebungsformulare der Krankenhäuser zu achten.

2. Aufgrund einer Beschwerde war zu überprüfen, ob ein Jugendamt im Rahmen der Beratung und Unterstützung eines personensorgeberechtigten Elternteils nach § 51 Jugendwohlfahrtgesetz vom Arbeitgeber die Offenbarung von Einkommensdaten eines säumigen Unterhaltszahlers fordern und die erhaltenen Einkommensdaten ohne weiteres dem personensorgeberechtigten Elternteil offenbaren konnte. Ich habe dazu folgende Auffassung vertreten: Nach § 4 Nr. 3 JWG zählt die Mitwirkung im Vormundschaftswesen gemäß den §§ 37 - 54a JWG zu den Aufgaben des Jugendamts. Da § 27 Abs. 1 SGB I auf die Vorschrift des § 4 JWG verweist, ist die Beratung und Unterstützung des personensorgeberechtigten Elternteils durch das Jugendamt zumindest im weiteren Sinne zu den Sozialleistungen der Jugendhilfe gemäß § 27 SGB I zu zählen. Das Jugendhilferecht kennt nämlich, anders als die übrigen Bereiche des Sozialrechts, einen Katalog von Einzelleistungen und deren präzise Bezeichnungen nicht. Damit sind bei der Beratung und Unterstützung des personensorgeberechtigten Elternteils nach § 51 JWG die Bestimmungen zum Schutz der Sozialdaten, hier insbesondere § 74 Abs. 2 SGB X, zu beachten. Ich vertrete daher die Auffassung, daß in dem Beschwerdefall der säumige Unterhaltszahler vor der Abfrage seiner Einkommensdaten beim Arbeitgeber vom Jugendamt hätte gemahnt werden müssen. Durch die Offenbarung der Tatsache „säumiger Unterhaltszahler" gegenüber dem Arbeitgeber könnten Belange des Betroffenen, die durch § 74 Abs. 2 SGB X geschützt sind, beeinträchtigt werden. Die Weitergabe der Einkommensdaten durch das Jugendamt an den auskunftsberechtigten Elternteil ist zulässig, wenn der Unterhaltspflichtige seiner Auskunftspflicht nicht vollständig nachkommt. Der Betroffene muß daher im Rahmen einer Mahnung auf diese Rechtssituation hingewiesen werden.

3. Aufgrund einer Eingabe wurde festgestellt, daß ein Versorgungsamt aus seinen Unterlagen an ein Finanzamt Auskunft über Krankheitsdaten eines Betroffenen erteilt hatte, die der durch § 76 SGB X auf den Sozialleistungsträger „verlängerten" ärztlichen Schweigepflicht unterlagen. Die Offenbarung war zu beanstanden. Das Amt bedauerte den Vorfall.

   Das Landesversorgungsamt Bayern hat nun Erläuterungen zum 2. Kapitel des SGB X erarbeitet und damit einen wesentlichen Beitrag zur Vermeidung von Rechtsunsicherheiten bei der Ausführung des X. Buches des SGB geleistet. Dies begrüße ich ausdrücklich. Gegen die Erläuterungen zu § 76 SGB X habe ich jedoch erhebliche Bedenken erhoben (s.a. Nr. 4.2.3).

4. Ein Stadtrat hatte eine Kommission für Sozialhilfe zur Überwachung der laufenden Angelegenheiten der Sozialhilfe in außergewöhnlichen Fällen gebildet. Art. 2 Abs. 1 des Gesetzes zur Ausführung des Bundessozialhilfegesetzes sieht zwar die Bildung eines Sozialhilfeausschusses für grundsätzliche und allgemeine Angelegenheiten der Sozialhilfe vor, die Bestimmung enthält aber keinen Hinweis auf die Einrichtung einer Kommission zur Überwachung der laufenden Angelegenheiten der Sozialhilfe. Zu prüfen ist daher, ob die Offenbarung von Sozialdaten durch die städtische Sozialverwaltung an die Mitglieder der Kommission in Erfüllung einer gesetzlichen Aufgabe nach dem Sozialgesetzbuch (§ 69 Abs. 1 Nr. 1 SGB X) erfolgt. Diese Überprüfung ist noch nicht abgeschlossen.

5. Das Bayer. Landesamt für Statistik und Datenverarbeitung hatte eine bayerische Landesversicherungsanstalt um Übermittlung von 5000 Anschriften von Rentenversicherten zur freiwilligen Teilnahme an einer Erhebung gebeten. Einwilligungen der Betroffenen lagen nicht vor. Eine Datenübermittlung aufgrund § 68 SGB X habe ich für unzulässig erachtet, da sich die Amtshilfe ihrem Wesen nach nur auf Einzelfälle, d.h. auf bestimmte Sozialdaten bestimmter einzelner Betroffener bezieht (so auch Begründung des Bundestags-Ausschusses für Arbeit und Sozialordnung - BT Drucksache 8/4022 Seite 84). Ich habe jedoch auf die Möglichkeit hingewiesen, Anschreiben des Landesamts für Statistik und Datenverarbeitung von der Landesversicherungsanstalt selbst an die Versicherten versenden zu lassen. Es steht dann den Angeschriebenen frei, sich gegenüber dem Landesamt für Statistik und Datenverarbeitung zu melden oder dies zu unterlassen. In diesem Falle würde ich in der Nutzung von Versicherten-Anschriften keinen Widerspruch zu den Aufgaben der LVA sehen.

4.3.2 Zuständigkeit zur Datenschutzkontrolle bei der Datenstelle des VDR

Bei der vom VDR in Würzburg eingerichteten Zentralen Datenstelle werden in personenbezogener Form Daten aller rentenversicherten Personen in der Bundesrepublik gespeichert. Hinsichtlich der Datenschutz-Kontrollkompetenz für diese Stelle hatten sich Unklarheiten ergeben. Der Landesbeauftragte für den Datenschutz hat deshalb ein Gutachten über die Rechtsfrage erstellen lassen, welchem Datenschutzbeauftragten die Kontrolle der Datenstelle hinsichtlich der Einhaltung der Datenschutzvorschriften obliegt. Das Gutachten kommt in seiner Zusammenfassung zu folgendem Ergebnis:

„1. Ein Zusammenschluß von Verwaltungsträgern des Bundes- und des Landesrechts ist nur in der Form eines betont schlichten Zweckverbandes möglich, bei dem die Verantwortlichkeiten nach Bundes- und nach Landesrecht gewahrt und auf jede Begründung eines gemeinsamen, den Bereich des Bundes- und des Landesrechts gleichzeitig berührenden Aufsichts- und Interventionsrechts verzichtet wird. Der VDR ist in der Rechtsform eines eingetragenen Vereins des privaten Rechts gebildet worden. Seine Gründung unterliegt insoweit keinen verfassungsrechtlichen Bedenken.

   Als privatrechtlicher Verein unterliegt der VDR keiner Staatsaufsicht. Da aber sämtliche Verbandsmitglieder selbst einer Rechtsaufsicht unterliegen, kann deren Tätigkeit bei der Beschlußfassung innerhalb des Verbandes rechtsaufsichtlich durch die verschiedenen Aufsichtsbehörden beeinflußt werden; deren Zusammenwirken ist erforderlich, um auf einen Verbandsbeschluß einwirken zu können.

2. Vom Gesetz festgelegte Zuständigkeiten können von Verwaltungsträgern weder durch Vertrag noch durch Satzung einem Dritten übertragen werden. Im Rahmen dieses Grundsatzes ist es einem Verwaltungsträger jedoch möglich, bestimmte ihm obliegende Aufgaben mittels Mandat

durch einen Dritten wahrnehmen zu lassen. Die Befassung der Datenstelle des VDR mit bestimmten Obliegenheiten bei der Verarbeitung von Daten durch die Rentenversicherungsträger ist zulässig, doch bleibt die Erfüllung der Aufgaben weiterhin in der Verantwortung der das Mandat gewährenden Rentenversicherungsträger.

3. Eine Übertragung von Zuständigkeiten, die gesetzlich den Rentenversicherungsträgern obliegen, auf eine andere Stelle bedürfte einer mit Zustimmung des Bundesrats ergangenen bundesgesetzlichen Regelung. § 14 der 2.DEVO stellt keine solche Regelung dar. Die Ermächtigungsnormen zum Erlaß der 2.DEVO gewähren dem Verordnungsgeber nicht die Befugnis, eine neue Stelle mit eigenen Befugnissen zu errichten. Weder das Recht, Art und Umfang der Datenspeicherung und des Datenaustausches zwischen den Versicherungsträgern zu bestimmen noch die Ermächtigung, das Nähere über Bearbeitung, Sicherung und Weiterleitung der Angaben sowie die Stelle, der gegenüber die Meldungen abzugeben sind, zu bestimmen, enthalten eine Befugnis, in den Gesetzen festgelegte Zuständigkeiten zu verändern oder zu übertragen. Diese Ermächtigungen stellen für den Erlaß der Verordnung den Rahmen nach Inhalt, Zweck und Ausmaß dar; aus ihm muß vorausgesehen werden können, in welchen Fällen und mit welcher Tendenz von ihnen Gebrauch gemacht werden wird. Die Errichtung einer neuen Stelle mit echten Zuständigkeiten und eine dabei vorzunehmende Zuständigkeitsverschiebung zum Nachteil von Landeskompetenzen kann nicht im Rahmen der genannten Ermächtigungen gesehen werden.

4. Die Datenstelle ist kein Sozialversicherungs„träger" im Sinne des Art. 87 Abs. 2 GG, da sie nur mit der Abwicklung von Teilfunktionen bei der Datenverarbeitung im Rentenversicherungswesen ohne eigene Zuständigkeit befaßt ist. Die genannte Verfassungsvorschrift ist übrigens eine Ausnahmeregelung, die eng auszulegen ist.

5. Die Sozialversicherungsträger und ihre Verbände haben hinsichtlich des Datenschutzes Bundesrecht zu beachten (§ 79 SGB X). Das besagt aber noch nichts über ihre Zugehörigkeit zum Aufgabenbereich des Bundesbeauftragten für den Datenschutz (§ 79 Abs. 3 Satz 2 SGB X).

6. Die der Datenstelle überlassenen Tätigkeiten sind rein technischer Natur, Art und Weise sind im einzelnen rechtlich festgelegt, ein Ermessensspielsraum ist, abgesehen von einigen rein technischen sinnvollen Maßgaben, nicht eingeräumt. Die Datenstelle handelt damit ausschließlich im Rahmen eines Auftrags im Sinne des § 8 BDSG.

7. Öffentliche Stellen, soweit sie personenbezogene Daten im Auftrag verarbeiten, unterliegen ebenfalls der Datenschutzkontrolle. Gegenstand der Kontrolle beim Auftragnehmer ist entsprechend seiner Verantwortung die Einhaltung der Weisungen in datenschutzrechtlicher Hinsicht und die Betriebsweise, die den Datenschutz sicherzustellen hat.

   Für die Kontrolle bei den dem Bundesrecht zugeordneten Stellen ist der Bundesbeauftragte für den Datenschutz, bei den dem Landesrecht zuzurechnenden Stellen die Landesbeauftragten für den Datenschutz zuständig (§ 79 Abs. 3 Satz 2 SGB X).

   Da dem VDR, dem Träger der Datenstelle, Anstalten des Bundes- und des Landesrechts angehören, ist für ihn sowohl der Tatbestand einer Vereinigung bundesrechtlicher Anstalten als auch der Tatbestand einer Vereinigung von Anstalten des Landesrechts gegeben. Würde mit dem Zusammenschluß eine Vereinigung einheitlichen Rechts gewollt sein, so würde dies gegen das Gebot der Wahrung der Zuständigkeiten des Landesrechts verstoßen und wäre nichtig. Ein Zusammenschluß von Verwaltungsträgern des Bundes und der Länder kann verfassungsrechtlich nur dann gerechtfertigt werden, wenn dabei die Verantwortlichkeiten nach Bundes- und nach Landesrecht gewahrt und jede Begründung eines gemeinsamen, den Bereich des Bundes- und des Landesrechts gleichzeitig berührenden Aufsichtsrechts verzichtet wird. Dieser oben bereits angeführte Grundsatz gilt auch hier. Eine Zuständigkeitsregelung für eine in verfassungswidriger Weise gebildete Vereinigung kann nicht aus Bestimmungen des Bundesrechts hergeleitet werden. Die Datenstelle untersteht damit der Datenschutzkontrolle sowohl des Bundesbeauftragten als auch der Landesbeauftragten für den Datenschutz.

8. Die Schwierigkeiten, die sich aus der Vielzahl der nebeneinander bestehenden Zuständigkeiten ergeben, können auf der Länderseite dadurch überwunden werden, daß die Landesdatenschutzbeauftragten ihre Aufgaben durch einen einzigen von ihnen wahrnehmen lassen.

   Eine Wahrnehmung der Kontrollaufgaben des Landesbauftragten durch den Bundesbeauftragten erscheint verfassungsrechtlich bedenklich, da das Grundgesetz eine Übertragung von Landesaufgaben auf Bundesstellen außerhalb der von ihm gesetzten Grenzen nicht zuläßt, sondern eine strikte Einhaltung der Kompetenzordnung von Bund und Ländern fordert. Aus der Tatsache, daß solche Aufgabenübertragungen auf Bundesorgane bereits bestehen, kann nicht auf deren Verfassungsmäßigkeit geschlossen werden. Sollte trotz der grundsätzlichen Bedenken eine Organleihe an den Bundesbeauftragten für Datenschutz für zulässig erachtet werden, so ist dabei die Begründung von Ingerenzrechten der beauftragenden Landesorgane unerläßlich, da sich diese nicht völlig ihrer Zuständigkeiten und Verantwortungen begeben können, die ihnen gesetzlich zugeordnet sind.

   Ein Zusammenwirken des Bundesbeauftragten und eines Landesbeauftragten für den Datenschutz ist möglich. Da es sich hierbei um zwei unterschiedliche Aufgaben handelt, liegt keine Mischverwaltung vor. Eine solche „konzertierte Aktion"/bei der Kompetenzausübung ist die notwendige Folge der sich eng berührenden und teilweise verschränkenden, aber zwingenden Zuständigkeitsverteilung des Grundgesetzes. Diese Zusammenarbeit könnte sich, soweit nicht die eigentliche Willensbildung betroffen ist, auch in Arbeitsteilung vollziehen, wenn die Feststellung von Tatsachen und der Verkehr mit dem VDR - möglicherweise im Wechsel - einem der beiden Datenschutzbeauftragten übertragen wird.

   Die notwendigen Vereinbarungen zwischen den Datenschutzbeauftragten können durch Verwaltungsabkommen von diesen abgeschlossen werden."

4.4 Sicherheitsbereich

Die öffentliche Diskussion des Datenschutzes im Sicherheitsbereich ist im Berichtszeitraum durch den meines Erachtens überflüssigen Streit geprägt worden, ob Sicherheit vor Datenschutz oder Datenschutz vor Sicherheit gehen müsse. Gerade aus dem Bereich der Sicherheitsbehörden ist von prominenter Stelle gefordert worden, daß Datenschutz nicht zum Tatenschutz werden dürfe und Sicherheit der Vorrang vor Datenschutzinteressen des Einzelnen zukomme. Diese Diskussion war schon deshalb unglücklich, weil letzten Endes der Anspruch des einzelnen Bürgers, sich frei entfalten zu können, sowohl voraussetzt, daß er sich vor Verbrechen weitgehend

sicher fühlen kann, als auch verlangt, daß seine Privatsphäre beachtet wird. Eine generelle Abwägung zwischen Datenschutz und Sicherheit ist daher abwegig und kann zu keinen brauchbaren Ergebnissen führen. Daher kann auch ich als Datenschutzbeauftragter nicht für den Datenschutz einen absoluten Vorrang vor den Erfordernissen der öffentlichen Sicherheit verlangen. Falls die notwendige Balance zwischen den berechtigten Belangen der Bürger und der zu ihrem Schutz tätigen Sicherheitsbehörden nicht gewahrt wird, droht Gefahr sowohl für die Institution des Datenschutzes als auch für die Arbeit der Sicherheitsbehörden. An keinem von beiden kann der Bürger interessiert sein.

Allerdings ist ein Streit zwischen Datenschutz und Sicherheit nicht das tatsächliche Problem, das mich auf diesem Feld bewegt. Ich beobachte die zunehmende Automatisierung im Bereich der Sicherheitsbehörden. Es wachsen nicht nur die Anzahl der Dateien, es sind auch zusätzlich Verbesserungen im Verbundnetz der Polizei entstanden, z.B. durch den Einsatz von DISPOL, und zunehmend werden mobile Terminals bei der Polizei eingeführt, die die örtlich unabhängige Abfrage der Dateien gestatten. Dieser technische Fortschritt bei den Sicherheitsbehörden bietet der Polizei zusätzliche Abfrage- und damit auch Kontrollmöglichkeiten. Zwar hat der rechtschaffene Bürger für sich zunächst grundsätzlich nichts zu befürchten, wenn die Polizei diese technischen Möglichkeiten nutzt und beispielsweise den einzelnen Bürger häufiger als bisher einer Kontrolle unter gleichzeitiger Abfrage in polizeilichen Datensammlungen unterzieht. Aber jede Kontrolle hinterläßt zunächst Spuren, wenn auch nur auf den Protokollbändern der Datenverarbeitungsanlagen. Auf diese Weise ist zumindest die Tatsache festgehalten, daß der überprüfte Bürger sich zu einem bestimmten Zeitpunkt bei einer Kontrollstelle aufgehalten oder beispielsweise sein Fahrzeug sich zu einem bestimmten Zeitpunkt an einer bestimmten Stelle befunden hat.

Wenn derzeit diese Kontrollen im Regelfall auf bestimmte Örtlichkeiten, wie etwa die Grenzübergänge, beschränkt sind, so ist durch den Einsatz mobiler Terminals und insbesondere auch durch den Anschluß der Bayer. Polizei an das System ZEVIS eine deutliche Erweiterung der Abfragemöglichkeiten gegeben. Deshalb beobachte ich zumindest diese sich möglicherweise abzeichnende Entwicklung mit Aufmerksamkeit und Sorge. Meines Erachtens ist es daher dringend geboten, zum einen feste und eindeutige Regeln zu schaffen, wann derartige Kontrollen durchgeführt werden dürfen und zum weiteren sicherzustellen, daß die bei diesen Kontrollen entstehenden Spuren auf den Protokollbändern der Computer ausschließlich zu Nachweiszwecken verwendet werden. Nur so kann verhindert werden, daß diese Entwicklung zu einer unerwünschten Überwachung der Bürger führt.

Der freiheitliche Staat zeigt und beweist sich gerade dadurch, daß er dem Bürger unüberwachte Bewegungsfreiheit gewährt.

4.4.1 Prüfungen bei der Polizei

Im Berichtszeitraum habe ich neben einer Vielzahl von Einzelprüfungen aufgrund von Bürgereingaben allgemein bei der Staatsschutzabteilung des Landeskriminalamtes, beim Polizeipräsidium Oberfranken nebst sieben diesem nachgeordneten Polizeidienststellen und beim Polizeipräsidium München sowie bei einer Grenzpolizeistation geprüft.

Schwerpunkte dieser Prüfungen waren u.a.:

1. Aufbewahrung und Führung der Kriminalakten sowie die Einhaltung der neu in Kraft getretenen Richtlinien über kriminalpolizeiliche Sammlungen;
2. Datenübermittlungen und Datenabfragen betreffend Sozialleistungsträger (z.B. AOK), Ausländeramt, Einwohnermeldeamt und Jugendamt;
3. Verwendung von „Handkarteien" (z.B. Dirnen-, Rauschgifttäterkarteien);
4. Prüfung, wie auf Gebieten verfahren wird, aus denen sich bislang einige Probleme gezeigt haben (z.B. Glaubwürdigkeit kindlicher Zeugen, Verwendung von Sammelfernschreiben).

Sämtliche Überprüfungen waren durch eine erfreulich gute Zusammenarbeit, unbürokratische Unterstützung sowie das meinen Mitarbeitern entgegengebrachte grundsätzliche Verständnis für datenschutzrechtliche Belange gekennzeichnet. Die erbetene Einsicht in Unterlagen wurde mir in allen Fällen gewährt. Wesentliche Verstöße gegen datenschutzrechtliche Bestimmungen haben die Prüfungen nicht ergeben. Im einzelnen habe ich jedoch beispielsweise festgestellt, daß Arbeits- oder Suchkarteien unsystematisch und uneinheitlich geführt worden sind. Die nach den Richtlinien über kriminalpolizeiliche Sammlungen zu beachtenden Aussonderungsfristen waren teilweise überschritten, teilweise waren die Fristen nicht ausreichend auf den entsprechenden Unterlagen vermerkt. In einem Fall waren etwa 50 bereits ausgesonderte Altakten im Keller eines anderen Dienstgebäudes gelagert worden und dort offensichtlich in Vergessenheit geraten. Deren endgültige Aussonderung und Vernichtung habe ich verlangt. In einem Fall fehlte es an der nötigen Sicherung der Kartei der Rauschgifttäter. Diese Kartei lag in 4 hölzernen Schubladen völlig ungesichert offen im Raum der Sachbearbeiter, obwohl es sich hierbei um sehr sensible Daten handelt.

Andererseits konnte ich auch vielfach das Bemühen feststellen, dem Datenschutz weitgehend Rechnung zu tragen. So hat beispielsweise das Polizeipräsidium Oberfranken zu den KpS-Richtlinien ergänzende Weisungen erlassen, die bemerkenswert sind. Positiv fiel mir auch auf, daß beispielsweise in der Staatsschutzabteilung des Landeskriminalamtes Akten von besonderer Sensibilität besonders sorgfältig und korrekt geführt werden.

4.4.2 Aktenaussonderung beim Bayer. Landeskriminalamt

Durch die am 1.11.1979 begonnene Sonderaktion zur Bereinigung der kriminalpolizeilichen Aktensammlung des Bayerischen Landeskriminalamtes sind bisher ca. 275.000 Kriminalakten ausgesondert und vernichtet worden. Dadurch hat sich trotz der laufenden Neuzugänge die Zahl der Kriminalakten des Bayerischen Landeskriminalamtes auf rund 578.000 verringert.

Zunächst war als Termin für den Abschluß der Sonderaktion „Aktenbereinigung" Mitte 1983 in Aussicht gestellt worden. Da sich jedoch parallel zu dieser Sonderaktion laufende Arbeiten der Erfassung und Bestandspflege als überraschend personalaufwendig herausgestellt haben, dürfte sich der zunächst vom Bayerischen Landeskriminalamt genannte Termin voraussichtlich um 1 Jahr auf Mitte 1984 verschieben.

4.4.3 Datenübermittlungen

4.4.3.1 von Kfz-Zulassungsstellen an die Polizei

Der Online-Anschluß von Polizeibehörden an Kfz-Zulassungsstellen, die ihren Datenbestand automatisiert führen, wächst. So sind beispielsweise die Daten der in München-Stadt registrierten Kraftfahrzeuge und Kraftfahrzeug-Halter bereits seit 7. August 1972 auf elektronischen Datenträgern in der Kfz-Datei der Landeshauptstadt München gespeichert. Diese Datei enthält sämtliche Personalangaben und Daten, die auch im Kraftfahrzeug-Brief und Fahrzeugschein enthalten sind. Seit längerer Zeit sind auf dem Wege von Direktabfragen über Datensichtstationen und Fernschreiber des Polizeipräsidiums München Feststellungen über KraftfahrzeugHalter und Kraftfahrzeuge möglich.

Die Frage der Zulässigkeit von derartigen Online-Anschlüssen der Polizei an Kraftfahrzeug-Dateien von Zulassungsstellen ist problematisch. Nach § 26 Abs. 5 Straßenverkehrszulassungsordnung erteilen die Zulassungsstellen „im Einzelfall auf Antrag Behörden" Auskunft über die Fahrzeuge, die Halter und die Versicherungen. Diese ausdrückliche Beschränkung auf Datenübermittlungen im Einzelfall und die Tatsache, daß nach den Begriffsbestimmungen des Bayer. Datenschutzgesetzes sämtliche Daten als übermittelt gelten, die zum Abruf bereitgehalten sind (Art. 5 Abs. 2 Nr. 2 BayDSG), führen meines Erachtens grundsätzlich zur Unzulässigkeit derartiger Online-Anschlüsse. Da jedoch bei der Novellierung des Bundesdatenschutzgesetzes die insoweit unglückliche Formulierung des Übermittlungsbegriffes geändert werden sollte - dies würde wohl auch gleichartige Änderungen für das Bayer. Datenschutzgesetz mit sich bringen - habe ich von einer Beanstandung abgesehen. Zu diesem Ergebnis bin ich vor allem deshalb gekommen, weil die Polizei beim einzelnen Datenabruf im Online-Verkehr die abgerufenen Daten für ihre Aufgabenerfüllung benötigt.

4.4.3.2 an Sozialpsychiatrischen Dienst

Von einer Polizeidirektion wurde die Frage an mich herangetragen, wie sich die Polizei zu verhalten habe, wenn seitens der örtlich zuständigen psychiatrischen Betreuungsstelle der Wunsch geäußert werde, die Namen von solchen Bürgern zu erfahren, für die eine psychiatrische Betreuung im vorstationären Bereich angezeigt sein könnte. Dabei denke die psychiatrische Betreuungsstelle insbesondere an solche Fälle, in denen Bürger, die sich an die Polizei wenden, einen offensichtlich geistig verwirrten Eindruck machen.

Die Frage habe ich wie folgt beantwortet:
Sozialpsychiatrische Dienste werden primär unter der Trägerschaft der Freien Wohlfahrtsverbände, daneben auch durch Städte, Landkreise und Bezirke eingerichtet. Die Aufgaben der Sozialpsychiatrischen Dienste (Erkennung, Beratung und Betreuung bei psychischen Störungen) werden im „Ersten Bayerischen Landesplan zur Versorgung psychisch Kranker und psychisch Behinderter" näher beschrieben. Eine Rechtsnorm für diese Aufgaben fehlt. Für die Polizei besteht somit keine Verpflichtung, die Sozialpsychiatrischen Dienste über in Frage kommende Personen entsprechend zu informieren. Eine Übermittlung dieser Art ist wohl auch nicht orginäre Aufgabe der Polizei.

Meines Erachtens sollte sich die Polizei im Regelfall daher darauf beschränken, die betroffenen Bürger auf die Beratungs- und Betreuungsmöglichkeit durch die Sozialpsychiatrischen Dienste hinzuweisen. Eine unmittelbare Mitteilung an einen Sozialpsychiatrischen Dienst über Bürger, die sich zunächst in anderer Sache an die Polizei gewandt haben, kann wohl nur in ganz seltenen Einzelfällen und auch hierbei nur unter Berücksichtigung der schutzwürdigen Belange des Betroffenen entsprechend Art. 18 Abs. 1 BayDSG durch die Polizei erfolgen. Als Auswahlkriterien für diese seltenen Fälle kommen eine erkennbare psychische Störung oder Verhaltensauffälligkeit, eine erkennbare Hilfsbedürftigkeit sowie das Fehlen einer ambulanten oder stationären fachlichen Behandlung in Betracht. Außerdem muß der Betroffene erkennbar nicht in der Lage sein, diese für ihn notwendige Entscheidung selbst zu treffen. Sollte eine dieser Bedingungen nicht vorliegen, so halte ich eine entsprechende Datenübermittlung an eine psychiatrische Betreuungsstelle durch die Polizei für unzulässig.

4.4.3.3 zwischen Polizeibehörden

Zwischen den Polizeibehörden findet ein regelmäßiger Fernschreibverkehr statt. Um die Zahl der Fernschreiben möglichst zu reduzieren, werden vielfach sog. „Sammelfernschreiben" versandt, die inhaltsgleich an verschiedene Bundes- und Landespolizeibehörden adressiert sind. Gegen diese Übung ist grundsätzlich nichts einzuwenden. Allerdings habe ich in einzelnen Fällen festgestellt, daß auf diesen Sammelfernschreiben mehrere Tatkomplexe zusammen mit den Angaben der Tatverdächtigen aufgenommen worden waren, obwohl nur jeweils ein Tatkomplex für die einzelnen im Sammelfernschreiben genannten Adressaten von Bedeutung waren. Auf diese Weise haben Polizeidienststellen von personenbezogenen Ermittlungsvorgängen Kenntnis erlangt, die zu ihrer Aufgabenerfüllung nicht erforderlich waren. Meines Erachtens muß in derartigen Fällen auf Sammelfernschreiben verzichtet und müssen die einzelnen Sachverhalte dem jeweils betroffenen Adressaten in Einzelfernschreiben übermittelt werden.

4.4.4 Vorfälle in Nürnberg

Im 4. Tätigkeitsbericht hatte ich meine Tätigkeiten im Zusammenhang mit den Vorfällen in Nürnberg geschildert. Im Berichtszeitraum hatte sich eine Reihe von Bürgern an mich gewandt, die im Rahmen dieser Vorfälle erkennungsdienstlich behandelt worden waren. Diese Eingaben der Bürger wurden als Antrag auf Vernichtung der erkennungsdienstlichen Unterlagen von mir an das zuständige Landeskriminalamt weitergeleitet. In allen mir bekannten Fällen führte dies zur Vernichtung der erkennungsdienstlichen Unterlagen.

4.4.5 Kostenentscheidungen nach Anträgen auf Vernichtung personenbezogener Daten

Ein Bürger, der beim Landeskriminalamt einen Antrag auf Vernichtung seiner personenbezogener Unterlagen gestellt hatte, hatte mit Ablehnung seines Antrages eine Kostenentscheidung für diese Entscheidung des Landeskriminalamtes erhalten. Zur Rechtmäßigkeit derartiger Kostenentscheidungen ist folgendes festzustellen:

Zwar gewährt Art. 11 Bayer. Datenschutzgesetz unter den dort genannten Voraussetzungen ausdrücklich einen Anspruch auf Löschung personenbezogener Unterlagen. Eine ausdrückliche Kostenregelung hierzu enthält das Bayer. Datenschutzgesetz jedoch nicht. Somit sind für die Geltendmachung eines Anspruchs auf Löschung nach Art. 11 BayDSG die allgemeinen Kostenvorschriften anzuwenden. Daher ist aus datenschutzrechtlicher Sicht die Festsetzung von Kosten bei Ablehnung eines Löschungsantrags grundsätzlich nicht zu beanstanden.

Damit die Bürger, welche die im Datenschutzgesetz genannten Löschungsansprüche geltend machen wollen, über das Kostenrisiko rechtzeitig unterrichtet sind, habe ich das Bayer. Landeskriminalamt gebeten, die Bürger, die einen Antrag auf Vernichtung personenbezogener Unterlagen stellen, zunächst auf die möglicherweise anfallenden Kosten hinzuweisen. Die Antragsteller können ggf. ihren Antrag zurücknehmen, wenn die voraussichtlichen Kosten sie zu sehr belasten würden. Diesem Vorschlag versprach das Landeskriminalamt zu folgen.

4.4.6 Spurendokumentationssysteme

Spurendokumentationssysteme der Polizei sind nach Mitteilung des Bayer. Staatsministeriums des Innern zu dem Zweck geschaffen worden, die Ermittlungsbehörden bei der Bearbeitung umfangreicher Ermittlungsverfahren zu unterstützen. Generell muß es sich dabei um Verfahren handeln, die mit herkömmlichen Mitteln entweder nicht mehr oder nur mit unverhältnismäßig hohem Personalaufwand durchzuführen wären. Mit den automatisierten Spurendokumentationssystemen soll es der Polizei ermöglicht werden, einen Überblick über eine Vielzahl von Hinweisen und Spuren jeder Art zu erhalten. Damit werden bei der einzelnen Anwendung eines Spurendokumen-

tationssystems auch viele personenbezogene Daten von Bürger gespeichert, die - wie zumindest die weiteren Ermittlungen ergeben - weder Verdächtige noch sonst Beteiligte der aufzuklärenden Straftat sind.

Aus datenschutzrechtlicher Sicht ist daher bedeutsam, daß personenbezogene Angaben in Spurendokumentationssystemen so kurzfristig wie möglich gelöscht werden, wenn sie zur weiteren Aufklärung der Straftat nicht mehr erforderlich sind. Dies gilt insbesondere für die Namen der Personen, die aus dem Kreis der potentiellen Verdächtigen nach entsprechenden Recherchen der Polizei eindeutig ausgeschieden sind. Gerade weil es sich bei den Straftaten, zu deren Aufklärung SPUDOK-Verfahren eingesetzt werden, gewöhnlich um schwere Delikte handelt, sollen unschuldige Bürger nicht über die zur Aufklärung notwendige Zeit hinaus mit diesen Straftaten in Verbindung gebracht werden. Dies schließt meines Erachtens aus, daß alle im Rahmen eines SPUDOK-Verfahrens eingespeicherten Daten bis zum Zeitpunkt des rechtskräftigen Urteils gespeichert bleiben. Denn gerade bei schweren Straftaten kann sich das Strafverfahren über viele Jahre hinziehen. Darüber hinaus muß aus datenschutzrechtlicher Sicht sichergestellt sein, daß Zugang zu diesen Spurendokumentationssystemen nur die polizeilichen Sachbearbeiter haben, die mit der Aufklärung der zugrundeliegenden Straftat befaßt sind. Keinesfalls dürfen diese personenbezogenen Datenbestände den übrigen polizeilichen Sachbearbeitern geöffnet werden, solange die Spurendokumentationssystemen vorgehaltenen Daten nicht auf den Kreis der tatsächlich Verdächtigen zurückgeführt worden sind.

Ich bin überzeugt, daß sich hinsichtlich dieser Datenschutzforderungen im jeweiligen Einzelfall eine vernünftige und sachgerechte Lösung finden läßt, die einerseits die Datenschutzbelange beachtet und auch das Interesse an der zügigen Aufklärung der Straftat berücksichtigt.

4.4.7 Meldedienst „Landfriedensbruch und verwandte Straftaten"

Im Berichtszeitraum wurde der Meldedienst „Landfriedensbruch und verwandte Straftaten" von der Konferenz der Innenminister und -senatoren beschlossen. Bayern hat diesen Meldedienst in Kraft gesetzt. In die mit diesem Meldedienst einzurichtende Datei sollen Personen aufgenommen werden, gegen die ein Ermittlungsverfahren wegen Landfriedensbruchs, schweren Hausfriedensbruchs, schweren Gewalttätigkeiten, Plünderungen, besonders gemeingefährliche Straftaten oder wegen der Aufforderung zu solchen Straftaten eingeleitet worden ist, wenn diese Verfahren in einem Zusammenhang mit einer politisch bestimmten öffentlichen Veranstaltung oder einem solchen Aufzug stehen. Ziel des Meldedienstes ist es dabei, durch die zentrale Sammlung und Auswertung von Erkenntnissen bei überregional oder steuernd handelnden Straftätern die entsprechenden Tatzusammenhänge zu erkennen und Hinweise für die Verhütung von derartigen Straftaten zu geben. Während das Bundeskriminalamt diese Daten in einer Zentraldatei führt, haben die Polizeidienststellen der Länder die entsprechenden Daten anzuliefern. Die Speicherungsfrist in dieser Datei beträgt längstens 2 Jahre. Unter besonderen Voraussetzungen können die in dieser Datei gespeicherten Daten kurzfristig auch für die Abfrage im INPOL-Fahndungsbestand bereitgehalten werden.

Grundsätzliche Bedenken bestehen aus datenschutzrechtlicher Sicht gegen diesen Meldedienst nicht. Einige Punkte hätten jedoch meiner Ansicht nach einer näheren Konkretisierung oder inhaltlichen Abänderung in diesem Meldedienst bedurft. So bin ich der Auffassung, daß bei der Aufzählung der meldepflichtigen Straftaten die Formulierung „Straftaten mit Gewalttätigkeiten (aggressiver Einsatz physischer Kraft)" zu allgemein gehalten ist. Hier wäre gerade im Interesse der späteren eindeutigen Sachbearbeitung eine katalogartige Aufzählung der relevanten Straftaten sachdienlich. Des weiteren sollte die durch das BKA vorgesehene Auskunftserteilung meines Erachtens nur auf solche Stellen beschränkt sein, die im Einzelfall mit der Sachbearbeitung des jeweils vorliegenden Straftatenkomplexes betraut sind.

Daher begrüße ich auch die Regelung, daß Daten sofort zu löschen sind, wenn das Verfahren eingestellt wird oder Freispruch erfolgt. Allerdings muß meines Erachtens besser als bisher sichergestellt werden, daß die Polizeibehörden über den Ausgang der entsprechenden Strafverfahren umgehend unterrichtet werden, soll diese Regelung nicht leerlaufen.

Leider bin ich zu spät über den beabsichtigten Beschluß zu diesem Meldedienst unterrichtet worden, so daß meine Anregungen nicht mehr berücksichtigt werden konnten.

4.4.8 Fragebogen zur Beurteilung der Glaubwürdigkeit kindlicher Zeugen

In meinen letzten beiden Tätigkeitsberichten hatte ich darauf hingewiesen, daß einzelne Polizeidienststellen im Rahmen von Ermittlungsverfahren an Schulen Fragebogen zur Beurteilung der Glaubwürdigkeit kindlicher Zeugen versenden. Diese Fragebogen, die teilweise sehr sensible Fragen enthielten, wie etwa nach der körperlichen Entwicklung, nach der geistigen Konstitution, den Auffälligkeiten in sexueller Hinsicht, den häuslichen Einflüssen und zu etwaigen psychischen Entwicklungsstörungen, waren teilweise auch zur Aufklärung von Straftaten eingesetzt worden, in denen Art und Umfang der Fragestellung unverhältnismäßig schien.

Das Bayer. Staatsministerium des Innern hat nun eine Anordnung zur Glaubwürdigkeitsprüfung kindlicher Zeugen mit Hilfe eines Fragebogens erlassen, in der es meinen Anregungen im wesentlichen gefolgt ist. In diesem Zusammenhang hätte ich es allerdings begrüßt, wenn das Bayer. Staatsministerium des Innern die Entwicklung eines für Bayern einheitlichen Fragebogens veranlaßt hätte, um die Beachtung der in der Anordnung genannten Grundsätze sicherzustellen. Für die Zukunft gehe ich davon aus, daß die Polizei derartige Fragebogen im übrigen nur verwendet, wenn Anhaltspunkte für Zweifel an der Glaubwürdigkeit der kindlichen Zeugen vorliegen und die Fragebogen gegenüber der unmittelbaren Zeugeneinvernahme der Lehrer nur zweitrangiges Hilfsmittel sind. Außerdem sollte gewährleistet sein, daß die ausgefüllten Fragebogen so an die Polizei zurückgesandt werden, daß Dritte, wie etwa die Schulleitung oder die Schulverwaltung, von deren Inhalt nicht unberechtigt Kenntnis nehmen können.

Parallel hierzu hatte das Bayer. Staatsministerium für Unterricht und Kultus eine Bekanntmachung erlassen, die den Lehrern Hinweise gibt, wenn an Schulen Straftaten begangen werden (vgl. hierzu unten Nr. 4.11.5.).

4.4.9 Grenzkontrolle

Wie schon in vergangenen Jahren haben sich auch in diesem Berichtszeitraum Bürger mit der Befürchtung an mich gewandt, daß die Tatsache ihres Grenzübertritts besonders festgehalten werde oder daß häufige Überprüfungen darin begründet wären, daß bei den Sicherheitsbehörden besondere Hinweise auf sie vorlägen.

Meine Ermittlungen haben in jedem Einzelfall ergeben, daß die Tatsache, daß beispielsweise ein Betroffener häufiger kontrolliert worden ist, nicht in einer Speicherung in der Personenfahndungsdatei begründet war und es sich hierbei entweder um Zufälligkeiten oder aber um eine Verwechslung mit einer Person gehandelt haben könnte, die zur fraglichen Zeit zur Fahndung ausgeschrieben war. Außerdem dürfte es sich bei manchen der gerügten Kontrollen nach Art und Ablauf der Kontrolle

um Überprüfungen durch Beamte des Zolls gehandelt haben. Soweit hierbei auch Personaldokumente abgelichtet worden sind, ist dies nach den bestehenden Rechtsgrundlagen grundsätzlich zulässig.

4.4.10 Überprüfungen der Besucher von Kernkraftwerken

Die Registrierung von Besuchern in Kernkraftwerken hat Bürger dazu veranlaßt, mich nach der Zulässigkeit dieses Verfahrens und nach der Verwendung der dabei angefallenen Daten zu befragen. Hierzu ist folgendes festzustellen:

Bei der Erfassung von Daten der Besucher in bayerischen Kernkraftwerken handelt es sich um ein Datenschutzproblem im Bereich von Stellen, die ihrer Rechtsform nach nichtöffentliche Stellen sind. Nach meinen Erkundigungen werden alle Kernkraftwerke in Bayern von juristischen Personen des privaten Rechts betrieben. Für den Datenschutz im nichtöffentlichen Bereich sind zunächst nach § 30 Bundesdatenschutzgesetz grundsätzlich die Regierungen als Aufsichtsbehörden zuständig.

Unabhängig von dieser Zuständigkeitsregelung kann ich aber berichten, daß die Kernkraftwerke die Ausweispapiere von Besuchern ablichten, um bei besonderen Vorkommnissen nachträglich den Besucherverkehr überprüfen zu können. Diese Aufzeichnungen werden mindestens 6 Monate aufbewahrt und - von besonderen Vorkommnissen abgesehen - nicht an andere Stellen weitergeleitet. Sobald die Aufzeichnungen nicht mehr benötigt werden, werden sie vernichtet. Mit dieser Vorgehensweise entsprechen die Kernkraftwerke den vom Bayer. Staatsministerium für Landesentwicklung und Umweltfragen und vom Bayer. Staatsministerium des Innern festgelegten Sicherheitsvorkehrungen für Kernkraftwerke. Nach Aussagen des Bayer. Staatsministerium des Innern ist sichergestellt, daß die erhobenen Daten nur für eine nachträgliche Kontrolle bei besonderen Vorkommnissen genutzt und zuverlässig nach Ablauf der 6-Monats-Frist vernichtet werden.

4.4.11 Verfassungsschutz

4.4.11.1 Allgemeines

Aus der Natur der Sache eignet sich die Tätigkeit des Landesamtes für Verfassungsschutz nicht zu einer detaillierten öffentlichen Erörterung. Hieran hat sich auch der Landesbeauftragte für den Datenschutz zu halten. Dies bedeutet jedoch nicht, daß im Bereich des Verfassungsschutzes ein datenschutzfreier Raum besteht. So hat das Bayer. Landesamt für Verfassungsschutz das Datenschutzgesetz uneingeschränkt zu beachten und hat der Landesbeauftragte für den Datenschutz uneingeschränktes Prüfungsrecht nach Art. 28 BayDSG. Gerade weil dem Bürger gegenüber den Verfassungsschutzbehörden nur ein beschränktes Auskunftsrecht über die zu seiner Person gespeicherten Daten zusteht, ist es besonders wesentlich, daß ihm durch Kontrollen des Landesbeauftragten für den Datenschutz eine gewisse Sicherheit hinsichtlich der Rechtmäßigkeit der Datenverarbeitung bei den Verfassungsschutzbehörden gegeben wird.

Bei meiner Tätigkeit habe ich dem Landesamt für Verfassungsschutz zwar kein überproportionales Gewicht eingeräumt, doch bin ich neben einer generellen Prüfung noch zahlreichen Einzelfällen im Detail nachgegangen. Dabei hatte sich gezeigt, daß mir gerade die Prüfung aufgrund von Bürgereingaben einen sinnvollen Einblick in die Tätigkeit des Landesamtes für Verfassungsschutz gewährt hat, soweit datenschutzrelevante Vorgänge betroffen werden. Daher bin ich für Eingaben der Bürger dankbar und bis zu einem gewissen Grade für eine effektive Tätigkeit auch angewiesen.

Die Prüfungskompetenz der Datenschutzbeauftragten war im Berichtszeitraum insbesondere im Bundesbereich Gegenstand öffentlicher Diskussionen. Wegen der Bedeutung, der auch ich einer Prüfung beim Verfassungsschutz beimesse, habe ich vor diesem Hintergrund eingehende Gespräche auch mit dem Bayer. Staatsministerium des Innern geführt. Dabei wurde übereinstimmend festgestellt, daß der Verfassungsschutz vom Gesetzgeber nicht aus meiner Prüfungskompetenz ausgenommen worden und daher dieser Bereich im Rahmen meiner Zuständigkeit vollständig zu kontrollieren ist. Ausdrücklich weise ich darauf hin, daß mir in meinem Zuständigkeitsbereich in Bayern mir die Prüfkompetenz nicht abgesprochen worden ist und ich für meine Prüfungen sämtliche von mir erbetenen Unterlagen erhalten habe.

Um das Ergebnis meiner Prüfungstätigkeit im Berichtszeitraum beim Verfassungsschutz vorwegzunehmen, kann ich mitteilen, daß ich dort keine wesentlichen Verstöße gegen das Datenschutzrecht festgestellt habe. Soweit ich im Einzelfall mit einer Sachbehandlung nicht einverstanden war, ist meinen Vorstellungen in der Regel Rechnung getragen worden. Soweit ich keine Einigkeit mit dem Landesamt für Verfassungsschutz erzielt habe, hatte es sich um Fälle gehandelt, in denen es mir wegen der Besonderheit der Tätigkeit des Verfassungsschutzes schwer gefallen ist, die Zulässigkeit der Datenverarbeitung im Rahmen der gesetzlichen Aufgabenerfüllung eindeutig festzustellen. In derartigen Zweifelsfällen gehe ich grundsätzlich davon aus, daß die zuständige Fachbehörde aufgrund ihrer besonderen Fachkenntnisse den Rahmen der gesetzlichen Aufgabenerfüllung genauer festlegen kann.

Wie ich oben und bereits mehrfach in den früheren Tätigkeitsberichten geäußert habe, besteht nach Art. 8 Abs. 2 Nr. 5 BayDSG gegenüber Verfassungsschutzbehörden kein Auskunftsanspruch. Mit dieser Regelung soll verhindert werden, daß diese Behörden ausgeforscht werden. Der Bayer. Landesbeauftragte für den Datenschutz darf diese Bestimmung nicht umgehen und kann deshalb wegen der Besonderheiten des Verfassungsschutzbereiches keine Aussagen über die Ergebnisse von Einzelüberprüfungen erteilen. Derartige Aussagen müßten - sofern sie sich nicht in einer formelhaften Erklärung erschöpfen - wegen der möglichen Vielfalt der Ergebnisse unterschiedlich ausfallen und könnten deshalb Rückschlüsse auf eine etwaige Datenspeicherung zulassen. Dies würde möglicherweise eine nicht erwünschte Ausforschung erlauben. Bürger, die sich an mich wenden, bitte ich daher jeweils um Verständnis, daß ich Ihnen über das Ergebnis meiner datenschutzrechtlichen Prüfung keine Mitteilung machen kann. Ich kann daher nur versichern, daß ich die Belange des Datenschutzes auch gegenüber dem Landesamt für Verfassungsschutz nachhaltig vertrete und etwa festgestellte Verstöße beanstande. Außerdem ist durch die Unterrichtung des Beirats beim Landesbeauftragten für den Datenschutz über derartige Beanstandungen gem. Art. 29 Abs. 5 Bayer. Datenschutzgesetz Sorge dafür getragen, daß diesen Beanstandungen auch grundsätzlich abgeholfen wird.

4.4.11.2 Feststellungen zur Prüfung

Wie oben bemerkt, habe ich neben einer Reihe von Einzelfallprüfungen das Landesamt für Verfassungsschutz auch zu einer generellen datenschutzrechtlichen Prüfung aufgesucht.

Dabei hat die Überprüfung ergeben, daß die Polizeibehörden dem Landesamt für Verfassungsschutz auf Erkenntnisanfragen grundsätzlich alle bekannt gewordenen Sachverhalte übermitteln, darunter auch solche, bei denen ich keinen Bezug zur Aufgabenerfüllung des Landesamtes für Verfassungsschutz erkennen kann. Diese Erkenntnisse werden vom Landesamt für Verfassungsschutz ohne Beschränkung auf das Aufgabengebiet vollständig an andere Dienststellen übermittelt. Erkenntnisse der Polizei werden mit Fernschreiben oder durch die Übersendung der Anzeigendurchschrift weitergegeben. Für

die entsprechenden Erkenntnisanfragen an die Polizeibehörden hat das Landesamt für Verfassungsschutz ein Formblatt entwickelt. Die darin niedergelegte Fragestellung an die Polizeibehörden ist m. E. zu umfassend und nicht deutlich genug auf die Aufgaben des Landesamts für Verfassungsschutz beschränkt. Nach einer datenschutzgerechten Lösung wird derzeit gesucht.

Zur Löschung von Daten habe ich festgestellt, daß die entsprechenden Löschungsrichtlinien bezüglich der Betroffenen, die ein bestimmtes hohes Alter erreicht haben, weitgehend eingehalten sind. Die daneben nach einem bestimmten Zeitablauf vorzunehmende Aussonderung ist noch nicht abgeschlossen. Einer der überprüften Vorgänge ergab außerdem, daß selbst dann, als der Verdacht eines nachrichtendienstlichen Bezugs vollständig ausgeräumt worden war und als außerdem andere Ämter für Verfassungsschutz die entsprechenden Eintragungen in NADIS gelöscht hatten, das Bayer. Landesamt für Verfassungsschutz den von ihm veranlaßten NADISEintrag nicht gelöscht hatte. Aufgrund meiner Prüfung wurden jedoch die entsprechenden Daten gelöscht und die zugrundeliegenden Erkenntnisse vernichtet.

Als Ergebnis meiner Prüfung habe ich folgende Vorschläge unterbreitet:

Soweit das Landesamt für Verfassungsschutz nach Art. 2 Abs. 2 des Gesetzes über die Errichtung eines Landesamtes für Verfassungsschutz tätig wird, sollte das Landesamt im Regelfall selbst entscheiden, welche der bei in vorgehaltenen Daten an die betroffenen Behörden als gerichtsverwertbar oder für die Entscheidung sonst bedeutsam übermittelt werden. Derzeit muß das Landesamt für Verfassungsschutz sämtliche der ihm bekannten Erkenntnisse dem Staatsministerium des Innern zur dortigen Entscheidung übermitteln. Ganz generell bin ich der Auffassung, daß das Risiko einer unbefugten Kenntnisnahme dieser sensiblen Daten erhöht wird, wenn mehrere Stellen eingeschaltet sind.

Entgegen meiner Auffassung meint das Bayer. Staatsministerium des Innern, daß seine Einschaltung in diesem sensiblen Bereich gerade dem Schutz des Betroffenen diene und eine zusätzliche Filterfunktion erfülle. Seine Einschaltung erhöhe keinesfalls das Risiko einer unbefugten Kenntnisnahme dieser sensiblen Daten.

Die Datenübermittlung von der Polizei an das Landesamt für Verfassungsschutz muß auf die Daten beschränkt werden, die für die Aufgabenerfüllung des Amtes erforderlich sind. Die Übermittlung der Tatsachen beispielsweise, daß gegen einen Betroffenen im Laufe der vergangenen Jahre mehrere Ermittlungsverfahren wegen Diebstahls eingeleitet worden sind und gegen dessen Vater ein Verfahren wegen Blutschande (ohne Hinweis auf den Ausgangs des Verfahrens) bestanden hat, ist grundsätzlich mit der Aufgabenerfüllung des Landesamtes für Verfassungsschutz nicht vereinbar. Insbesondere müßte auch bei der Datenübermittlung verstärkt zwischen der Aufgabenerfüllung nach Art. 2 Abs. 1 und nach Art. 2 Abs. 2 Gesetz über die Errichtung eines Landesamtes für Verfassungsschutz unterschieden werden. Weil das Landesamt für Verfassungsschutz verständlicherweise jedoch nicht dem die Erkenntnisse zusammenstellenden Polizeibeamten mitteilen kann, aus welchem Grund es diese Erkenntnisse benötigt, wäre zu erwägen, diese Datenübermittlung über die jeweils zuständige Staatsschutzdienststelle der Polizei abzuwickeln. Die bei diesen Dienststellen beschäftigten Beamten sind mit den das Landesamt für Verfassungsschutz betreffenden Vorgängen besser vertraut und könnten über den Anlaß der Anfrage zumindest im groben unterrichtet werden.

Sofern das Landesamt für Verfassungsschutz die von der Polizei übermittelten Daten im Einzelfall an andere Stellen weiterleitet, hat es seinerseits zu prüfen, wie weit diese Daten zur Aufgabenerfüllung der empfangenden Stelle erforderlich sind. Eine vollständige Weiterleitung dieser Daten ohne derartige Prüfung - wie bei der Kontrolle teilweise festgestellt - verstößt gegen Grundsätze des Datenschutzrechts und ist auch mit dem Gesetz über die Errichtung eines Landesamts für Verfassungsschutz nicht vereinbar.

Für den Sonderfall der Sicherheitsüberprüfungen, bei denen nach Art. 2 Abs. 2 Gesetz über die Errichtung eines Landesamtes für Verfassungsschutz dieses Amt „mitwirkt", ist zu prüfen, wieweit von der bisherigen Verfahrensweise abzurücken ist. Bislang werden diese Sicherheitsüberprüfungen, auch soweit ausschließlich strafrechtlich relevante Vorgänge in mitten stehen, vom Landesamt für Verfassungsschutz durchgeführt. Tatsächlich können Erkenntnisse, die Straftaten betreffen, für die Entscheidung wesentlich sein, ob einer Person geheimhaltungsbedürftige Tatsachen anvertraut werden können oder ob sie in lebens- oder verteidigungswichtigen Einrichtungen beschäftigt sein kann. Weil dem Landesamt für Verfassungsschutz bei derartigen Sicherheitsüberprüfungen jedoch nur eine Mitwirkung als Aufgabe zugewiesen ist, sollte erwogen werden, die Sammlung strafrechtlich relevanter Erkenntnisse dem Landeskriminalamt zu überlassen. Das Landeskriminalamt könnte die strafrechtlich relevanten Erkenntnisse unmittelbar dem Staatsministerium des Innern zuleiten, wo sie dann mit den entsprechenden ausschließlich verfassungsschutzrelevanten Erkenntnissen des Landesamtes für Verfassungsschutz zusammengeführt und ausgewertet werden könnten. Auf diese Weise würde vermieden, daß allzu viele, lediglich den Bereich der polizeilichen Ermittlungstätigkeit betreffende Vorgänge dem Landesamt für Verfassungsschutz übermittelt würden.

4.4.11.3 Registrierung von Bürgereingaben

Die Wahrnehmung der den Bürgern durch das Bayer. Datenschutzgesetz eingeräumten Datenschutzrechte darf nicht zu Nachteilen für den Bürger führen. Manche Bürger könnten es bereits als nachteilig ansehen, wenn die Tatsache, daß sie sich mit der Bitte um Prüfung in einer Verfassungsschutzangelegenheit an den Datenschutzbeauftragten gewandt haben oder einen Auskunftsanspruch unmittelbar gegenüber dem Landesamt für Verfassungsschutz vorgetragen haben, bei diesem Amt gespeichert würde. Hierzu habe ich folgendes festgestellt:

Zu keinerlei Speicherung und auch zu keinerlei Notierung selbst beim behördeninternen Datenschutzbeauftragten kommt es in allen Fällen, in denen zum Anfragenden keinerlei Unterlagen vorhanden sind. In den übrigen Fällen gilt folgendes:

Wenn der Bürger sich unmittelbar an das Landesamt für Verfassungsschutz gewandt hat, wird der Schriftwechsel mit dem Bürger dort aufbewahrt, um, wie bei anderen Verwaltungsvorgängen auch, einen Nachweis über die Erledigung des Schreibens zu haben. Sofern der Landesbeauftragte für den Datenschutz für einen Bürger nachforscht und Vorgänge zum Anfragenden vorhanden sind, wird die Tatsache der Anfrage grundsätzlich nur beim behördeninternen Datenschutzbeauftragten und in dessen Unterlagen vermerkt. Dieser Vermerk dient ebenfalls nur als Nachweis darüber, daß dieser Bürger sich an den Datenschutzbeauftragten gewandt hat und daraufhin geprüft worden war, ob Unterlagen zu diesem Bürger vorhanden sind. Dieser Nachweis ist für den einzelnen Bürger jedoch nicht belastend, da er in keinem Zusammenhang mit den sonstigen Arbeitsunterlagen des Amtes steht.

4.4.11.4 Umfang der Speicherung beim Landesamt für Verfassungsschutz

Mit dem Landesamt für Verfassungsschutz bin ich hinsichtlich des Umfangs der zu einer Person aufzunehmenden Daten und Informationen einig, daß selbst in den Fällen, in denen dort zu

einzelnen Personen bereits Vorgänge vorhanden sind, nicht alle Lebensäußerungen dieser Person zu speichern sind, wenn diese Lebensäußerungen mit den Aufgaben des Landesamtes für Verfassungsschutz nicht im Zusammenhang stehen. Dies gilt auch dann, wenn diese beispielsweise von Kriminalbeamten einer Staatsschutzabteilung oder von Bediensteten des Landesamtes für Verfassungsschutz gleichwohl festgestellt worden sind. Beim Landesamt für Verfassungsschutz muß vor der Speicherung in jedem Einzelfall geprüft werden, ob die dem Amt mitgeteilten Tatsachen für die Tätigkeit des Amtes relevant sind.

4.4.11.5 Speicherung der Daten von Hotelgästen

Aufgrund der Zeitungsberichte zur Datenspeicherung von Hotelübernachtungen in einem anderen Bundesland habe ich mich über die entsprechende bayerische Praxis unterrichtet. Ohne hier die Einzelheiten des in Bayern gewählten Verfahrens im einzelnen berichten zu können, kann ich jedenfalls mitteilen, daß gegen die bayerische Verfahrensweise aus datenschutzrechtlicher Sicht keine Bedenken bestehen, weil insbesondere der Grundsatz der Verhältnismäßigkeit gewahrt wird.

4.4.11.6 Speicherung von Adoptionsbewerbern

In einer Anfrage an den Bundesbeauftragten für den Datenschutz, die mir dieser zuständigkeitshalber zugeleitet hatte, hat ein Bürger die Frage gestellt, „ob es zutrifft, daß in Bayern Adoptionsbewerber Objekt einer Regelanfrage an das Bayer. Landesamt für Verfassungsschutz bilden, um ihre Eignung festzustellen". Meine Ermittlungen haben eindeutig ergeben, daß in Bayern Adoptionsbewerbungen nicht zum Anlaß einer Regelanfrage an das Bayer. Landesamt für Verfassungsschutz genommen werden.

4.4.11.7 Sicherheitsüberprüfungen

Sicherheitsüberprüfungen sind durchzuführen vor Einstellungen in sicherheitsempfindliche Bereiche der Privatindustrie. Bei solchen Sicherheitsüberprüfungen werden einen Bürger betreffende Auskünfte unmittelbar nur dem Innen- oder dem Umweltministerium mitgeteilt. Diese Ministerien entscheiden ihrerseits, inwieweit das Privatunternehmen hiervon im Einzelfall unterrichtet werden muß.

4.4.11.8 Prüfung der Verfassungstreue im öffentlichen Dienst

Bei den sog. Einstellungsüberprüfungen im öffentlichen Dienst wird nach der Bekanntmachung der Bayer. Staatsregierung vom 27.3.1973 verfahren. Nach meinen Ermittlungen werden Anfragen an das Landesamt für Verfassungsschutz ausschließlich und erst dann gerichtet, wenn die Einstellung des Bewerbers im übrigen feststünde. Mir ist ausdrücklich versichert worden, daß keinesfalls Überprüfungen von sonstigen Bewerbern für den öffentlichen Dienst durchgeführt werden.

4.5 **Rechtspflege**

4.5.1 Anwendbarkeit des Bayer. Datenschutzgesetzes

Kenner des Bayer. Datenschutzgesetzes mögen Zweifel haben, ob dieses Gesetz für das Gebiet der Rechtspflege in Bayern überhaupt Bedeutung besitzt. So ist das Bayer. Datenschutzgesetz, wie auch das Bundesdatenschutzgesetz und alle anderen Landesdatenschutzgesetze, zunächst unmittelbar nur auf die Datenverarbeitung in Dateien anwendbar. Daneben bestimmt Art. 2 Abs. 2 BayDSG, daß besondere Vorschriften über Verfahren der Rechtspflege den Vorschriften des Bayer. Datenschutzgesetzes vorgehen. Schließlich gilt selbstverständlich auch im Bereich der Justiz der Grundsatz, daß Bundesrecht Landesrecht bricht und um Bundesgesetze handelt es sich in erster Linie, die die Tätigkeit der Justizbehörden prägen. Trotzdem gilt das Bayer. Datenschutzgesetz grundsätzlich auch für Verfahren der Rechtspflege. Anders als etwa in den Datenschutzgesetzen einiger Bundesländer ist die Geltung des Bayer. Datenschutzgesetzes nicht auf die Erledigung von Verwaltungsaufgaben durch Gerichte oder Staatsanwaltschaften beschränkt. Die Geltung des Gesetzes erstreckt sich vielmehr grundsätzlich auf die gesamte Tätigkeit der Staatsanwaltschaften und Gerichte, soweit nicht die richterliche Unabhängigkeit berührt wird.

Neben der Tatsache, daß der Begriff „Dateien" auch Karteien umfaßt, die in nicht unerheblichem Maße im Justizbereich Verwendung finden, ist zur Subsidiarität des Bayer. Datenschutzgesetzes gegenüber besonderen Vorschriften über Verfahren der Rechtspflege folgendes zu bemerken:

Die Fassung des Art. 2 Abs. 2 BayDSG folgt in der Terminologie der Vorschrift des § 45 BDSG, weshalb die dort entwickelten Grundsätze weitgehend auch für das Bayer. Datenschutzgesetz anwendbar sind. Eine Vorschrift über Verfahren der Rechtspflege geht dem Bayer. Datenschutzgesetz nur dann vor, wenn sie die gleiche Konfliktslage regelt, die auch der Regelung des Bayer. Datenschutzgesetzes zugrundeliegt. Dies ergibt sich aus der Verwendung des Wortes „besondere" in Art. 2 Abs. 2 BayDSG, das andernfalls überflüssig wäre. Somit verdrängt nur eine deckungsgleiche Regelung das Bayer. Datenschutzgesetz.

Im übrigen bestätigen auch systematische Gründe, daß mit der Regelung in Art. 2 Abs. 2 BayDSG nur der Vorrang von bestimmten Sondervorschriften zu Verfahren der Rechtspflege beabsichtigt ist:

So werden in Art. 2 Abs. 1 BayDSG die Gerichte ausdrücklich und ohne Einschränkung als vom Anwendungsbereich des Bayer. Datenschutzgesetzes erfaßte Stellen genannt. Nach Art. 8 Abs. 2 Nr. 1 BayDSG besteht kein Auskunftsanspruch des Betroffenen gegenüber Gerichten und anderen Einrichtungen der Rechtspflege, soweit diese strafverfolgend, strafvollstrekkend oder strafvollziehend tätig werden. Diese Regelung wäre überflüssig, wenn der Gesetzgeber davon ausgegangen wäre, daß Dateien im Bereich der Rechtspflege im Hinblick auf die Regelung des Art. 2 Abs. 2 BayDSG überhaupt nicht vom Bayer. Datenschutzgesetz erfaßt werden.

Soweit Regelungen in Vorschriften über Verfahren der Rechtspflege eine auch im Bayer. Datenschutzgesetz geregelte Konfliktslage betreffen, haben jedoch nicht die Verfahrensgesetze der Rechtpflege im ganzen Vorrang vor dem Bayer. Datenschutzgesetz. Vorrang haben jeweils nur die Einzelregelungen, die die gleiche Konfliktlage regeln. Im übrigen treten die Verfahrensgesetze wegen des unterschiedlichen Regelungsgehalts mit den datenschutzrechtlichen Bestimmungen zum größten Teil überhaupt nicht in Kollision.

Selbst in den Fällen, in denen das Bayer. Datenschutzgesetz nicht unmittelbar anzuwenden ist, besteht bei der Justiz kein datenschutzfreier Raum. Denn so weit die Speicherung und Übermittlung von Daten durch Gerichte und Staatsanwaltschaften nicht gesetzlich geregelt ist, muß grundsätzlich auf die tragenden Bestimmungen der Verfassung zum Schutz der Persönlichkeit zurückgegriffen werden.

4.5.2 Schuldnerverzeichnis

Das Schuldnerverzeichnis wird vom Amtsgericht geführt. Es ist ein Verzeichnis der Personen, die die eidesstattliche Versicherung über ihr Vermögen abgegeben haben oder gegen die wegen der Nichtabgabe der eidesstattlichen Versicherung Haft angeordnet worden ist.

Zum Schuldnerverzeichnis habe ich mich bereits in meinem 3. und 4. Tätigkeitsbericht geäußert. Hierzu habe ich in erster

Linie zu der beabsichtigten Verordnung über Abschriften aus dem Schuldnerverzeichnis Stellung genommen. In diesem Tätigkeitsbericht wende ich mich den praktischen Erfahrungen mit der nach § 915 Abs. 2 ZPO geregelten Löschungspflicht im Schuldnerverzeichnis zu.

Die Pflicht zur Löschung von Eintragungen im Schuldnerverzeichnis in § 915 Abs. 2 ZPO ist ein guter Beweis dafür, daß der Persönlichkeitsschutz im Bereich des Zivilrechts auch den wirtschaftlich Gestrandeten schon seit langer Zeit zugestanden wird.

Nach § 915 Abs. 2 ZPO sind Eintragungen in das Schuldnerverzeichnis von Amts wegen zu löschen, wenn seit dem Schluß des Jahres, in dem die Eintragung erfolgt ist, 3 Jahre verstrichen sind. Eine vorzeitige Löschung ist auf Antrag des Schuldners dann erforderlich, wenn der Schuldner die Befriedigung des Gläubigers nachweist. Nach § 915 Abs. 2 Satz 2 wird die Eintragung im Schuldnerverzeichnis dadurch gelöscht, „daß der Name des Schuldners unkenntlich gemacht oder das Verzeichnis vernichtet wird".

Bei einer Prüfung in einem großen bayerischen Amtsgericht habe ich festgestellt, daß auf den jahrgangsweise jeweils für einen Betroffenen angelegten Karteikarten zwar das Akten zeichen und das Datum der zu löschenden Eintragungen ge schwärzt werden, diese Schwärzung jedoch nicht ausreicht, die Schrift vollständig abzudecken. Trotz der Einschwärzung bleibt der ehemalige Text zum Großteil lesbar. Außerdem wird der Name des Schuldners solange nicht gestrichen, solange auf der einzelnen Karteikarte noch weitere Eintragungen unge löscht bleiben. Erst wenn alle Eintragungen auf einer Kartei karte gelöscht sind, wird die Karteikarte vernichtet. Offen sichtlich sind auch nach der Löschung von Eintragungen noch Auskünfte über die gelöschten Eintragungen an Dritte erteilt worden.

Ich habe das Amtsgericht darauf hingewiesen, daß diese Art der Löschung im Schuldnerverzeichnis nicht dem durch § 915 Abs. 2 Satz 2 ZPO festgelegten Gebot entspricht. Aus der Formulierung dieser Bestimmung, „daß der Name des Schuldners unkenntlich gemacht oder das Verzeichnis vernichtet wird", ist zu entnehmen, daß gelöschte Eintragungen vollständig unlesbar sein müssen und darüber hinaus keinen Bezug zum Schuldner haben dürfen.

Weil dieses Amtsgericht die Karteikarten des Schuldnerver zeichnisses auf die einzelnen Jahre bezogen anlegt und somit alle innerhalb eines Jahres auf einen Schuldner bezogenen Eintragungen auf einer Karteikarte einträgt, tritt noch ein weiteres Problem auf:

Werden von mehreren Eintragungen nur einzelne gelöscht, bleibt auch bei korrekter Durchführung der Löschung bei einer eventuellen Einsicht in das Verzeichnis deutlich, daß der Schuldner über die noch aktuelle Eintragung hinaus weitere eidesstattliche Versicherungen geleistet hatte oder gegen ihn nach § 901 ZPO die Haft angeordnet worden war. Dies ent spricht meines Erachtens ebenfalls nicht dem Willen des Gesetzgebers in § 915 Abs. 2 Satz 2 ZPO.

Bei dem betroffenen Amtsgericht ist auf meine Vorstellungen hin inzwischen angeordnet worden, daß die Löschung im Schuldnerverzeichnis auf den Karteikarten deutlich und vollständig vollzogen wird.

Darüber hinaus ist die gesamte Schuldnerkartei von mehreren tausend Karteikarten nach den mir vorliegenden Informationen überarbeitet worden. Bei einer Nachschau hat sich inzwischen die korrekte Löschung bestätigt.

Das Bayer. Staatsministerium der Justiz, dem ich den Sachverhalt ebenfalls vorgetragen hatte, teilt meine Auffassung, daß Löschungen im Schuldnerverzeichnis nach § 915 ZPO zu einer vollständigen Unlesbarkeit der zu löschenden Eintragungen führen sollten. Ebenso ist das Justizministerium der Ansicht, daß es nicht unbedenklich sei, wenn auf einer Karteikarte Eintragungen vorgenommen würden, die mehrere Verfahren zur Abgabe der eidesstattlichen Versicherung durch den selben Schuldner betreffen. Es sei beabsichtigt, für das Schuldnerverzeichnis einen einheitlichen Kartenvordruck einzuführen. Dabei könnte zugleich bestimmt werden, daß auf einer Karteikarte nur Einträge vorgenommen werden dürften, die das selbe Verfahren betreffen. Diese Äußerung des Staatsministeriums der Justiz begrüße ich. Ich werde die Angelegenheit weiter verfolgen.

4.5.3 Strafvollzug (Briefüberwachung)

Ein Strafgefangener hat mich darauf hingewiesen, daß die Briefüberwachungsstelle der Justizvollzugsanstalt, in der er in Haft sei, auf der ausgehenden Post einen Sichtvermerk anbringe. Durch diesen Sichtvermerk werde dem Empfänger deutlich, daß der Absender Insasse einer Justizvollzugsanstalt sei, obwohl die neutrale Anschrift der Justizvollzugsanstalt dies selbst nicht deutlich mache. Durch diesen Sichtvermerk fühle er sich in seinen schutzwürdigen Belangen beeinträchtigt. Insbesondere sei seine Resozialisierung gefährdet, weil er keine Kontakte für die Zeit nach seiner Entlassung knüpfen könne, ohne daß der Briefpartner von der Tatsache Kenntnis erlange, daß er in einer Justizvollzugsanstalt einsitze.

Hierzu habe ich folgendes festgestellt: Der von einer Briefüberwachungsstelle der Justizvollzugsanstalt auf der ausgehenden Post angebrachte Sichtvermerk stellt zwar ein „Datum" dar, der Vorgang des Anbringens des Sichtvermerks fällt jedoch gleichwohl nicht unter den Schutzbereich des Bayerischen Datenschutzgesetzes, da dieses Datum nicht aus einer Datei im Sinne des Gesetzes stammt. Da das Bayer. Datenschutzgesetz im vorliegenden Fall nicht unmittelbar anwendbar ist, hat sich die Zulässigkeit der Anbringung des Sichtvermerks nach den allgemeinen Grundsätzen der Rechtmäßigkeit und Verhältnismäßigkeit der Verwaltung sowie nach §§ 28 ff Strafvollzugsgesetz zu beurteilen. Nach § 28 Strafvollzugsgesetz steht den Strafgefangenen ein Recht auf Schriftwechsel zu, der jedoch gemäß § 29 Abs. 3 Strafvollzugsgesetz „aus Gründen der Behandlung oder der Sicherheit oder Ordnung der Anstalt" überwacht werden darf.

Damit ist jedenfalls gegen eine Briefüberwachung durch solche Justizvollzugsanstalten des geschlossenen Vollzugs grundsätzlich nichts einzuwenden. Die betroffene Justizvollzugsanstalt hat im übrigen auf die Überwachung des Schriftwechsels der Strafgefangenen verzichtet, die kurz vor der Entlassung stehen.

Während also die Erforderlichkeit der Überwachung in einer solchen Justizvollzugsanstalt nicht zu bezweifeln ist, stellt sich die Frage, ob auch die Anbringung des Sichtvermerks, der zweifelsohne ein geeignetes Mittel für die Durchführung und Kontrolle der Überwachung darstellt, auch erforderlich ist. Bei der Wahl des Mittels zur Kontrolle der Überwachung ist der Grundsatz der Verhältnismäßigkeit zu beachten, der auch für die Beamten des Strafvollzugs gilt. Hierbei sind die vom Bundesverfassungsgericht (E 35, S. 202/233), vom Bayer. Verfassungsgerichtshof (E 21, S. 32/37) und vom OVG Rheinland-Pfalz (Entscheidung vom 24.7.1980) entwickelten Grundsätze zu beachten. Das hinter der Kontrolle stehende Interesse der Justizvollzugsanstalt an der Aufrechterhaltung der Sicherheit der Anstalt ist abzuwägen mit den schutzwürdigen Interessen des Strafgefangenen an der Geheimhaltung seines derzeitigen Aufenthaltes. Die Rechtmäßigkeit dieser Abwägung, die letztlich das auf Art. 1 Abs. 1 und Art. 2 Abs. 1 Grundgesetz berührende Persönlichkeitsrecht und den Grundsatz der Verhältnismäßigkeit der Verwaltung zum Gegenstand hat, ist in jedem

einzelnen Fall gesondert zu prüfen. Zu dieser Prüfung sind aber in erster Linie die hierfür zuständigen Gerichte berufen. Soweit, wie im vorliegenden Falle geschehen, die gerichtliche Entscheidung bereits vorliegt, ist mir im Hinblick auf die durch Art. 97 Abs. 1 Grundgesetz und Art. 85 Verfassung des Freistaates Bayern garantierte richterliche Unabhängigkeit eine datenschutzrechtliche Bewertung dieser Entscheidungen versagt.

Generell ist jedoch festzustellen, daß das Anbringen eines Sichtvermerks bei der Briefüberwachung in einer Anstalt des geschlossenen Vollzugs nicht grundsätzlich unzulässig ist. Dies gilt insbesondere dann, wenn die Justizvollzugsanstalt die Belange des Einzelfalls berücksichtigt und dann auf das Anbringen eines derartigen Sichtvermerks verzichtet, wenn der Strafgefangene ein berechtigtes Interesse darlegt. Ein solches kann beispielsweise vorliegen, wenn der Strafgefangene kurz vor seiner Entlassung steht und diese unbelastet vorbereiten will. Dies entspricht auch den vom Staatsministerium der Justiz an die Leiter der Justizvollzugsanstalten erteilten Weisungen.

4.5.4 Richtlinien für das Strafverfahren

Die Richtlinien für das Straf- und Bußgeldverfahren (RiStBV) geben dem Staatsanwalt Anleitungen für die Abwicklung von Strafverfahren. Einige Hinweise dieser Richtlinien wenden sich auch an den Richter. In Nr. 185 und 185a wird die Gewährung der Akteneinsicht geregelt. Diese Bestimmungen sind im Berichtszeitraum - ohne meine Beteiligung - geringfügig geändert worden. Die nun vorgesehenen Regelungen des Akteneinsichtsrechts, die datenschutzrechtlich als Datenübermittlungen zu werten sind, können aus der Sicht des Datenschutzes noch nicht völlig befriedigen.

Grundgedanke des Datenschutzes ist es, Datenübermittlungen auf das unbedingt erforderliche Maß zu beschränken. Soweit Datenübermittlungen an Private im Einzelfall vorgenommen werden, sehen die Datenschutzgesetze der Länder und des Bundes eine Abwägung zwischen dem gebotenen Schutz der Privatsphäre und dem Informationsinteresse durch im wesentlichen gleichlautende Bestimmungen vor. So erlaubt der für die Datenübermittlung von der öffentlichen Verwaltung an den privaten Bereich einschlägige Art. 18 Abs. 1 BayDSG die Datenübermittlung unter der Voraussetzung, daß der Empfänger ein berechtigtes Interesse an der Kenntnis der zu übermittelnden Daten glaubhaft macht und dadurch schutzwürdige Belange des Betroffenen nicht beeinträchtigt werden.

=

Auch bei der nicht unter den unmittelbaren Anwendungsbereich des Bayer. Datenschutzgesetzes fallenden Datenübermittlung aus Akten ist eine Abwägung zwischen den Belangen des Betroffenen und dem Informationsinteresse des Außenstehenden grundsätzlich geboten. Dies ergibt sich aus dem in Art. 2 Abs. 1 Grundgesetz verankerten Persönlichkeitsrecht, das dem einzelnen Bürger nach der ständigen Rechtsprechung des Bundesverfassungsgerichts neben dem unantastbaren Intimbereich einen Bereich der privaten Lebensgestaltung einräumt, in dem nur unter Abwägung der betroffenen Interessen und unter strikter Wahrung des Verhältnismäßigkeitsgebotes eingegriffen werden darf. Dieser Schutz kommt auch dem Straftäter zu und selbstverständlich demjenigen, der zwar zunächst beschuldigt, dann jedoch freigesprochen oder gegen den das Verfahren eingestellt worden ist. Die Konkretisierung, die das Abwägungserfordernis im Anwendungsbereich des Bayer. Datenschutzgesetzes in Art. 18 gefunden hat, kann daher auf die Datenübermittlung aus Akten übertragen werden.

Zwar begrüße ich, daß die Regelung in Nr. 185 Abs. 4 Satz 1 RiStBV unverändert geblieben ist, wonach vom Strafverfahren nicht betroffenen Privatpersonen und privaten Einrichtungen die Akteneinsicht grundsätzlich versagt wird. Unter Berücksichtigung dieser Grundsätze ist zu Nr. 185 Abs. 4 Satz 2 RiStBV, der unter bestimmter Voraussetzung die Datenübermittlung aus Strafakten an außenstehende Private regelt, aus datenschutzrechtlicher Sicht jedoch folgendes zu bemerken:

Die verfassungsrechtlich gebotene Abwägung in dieser Bestimmung zwar grundsätzlich vorgesehen, jedoch wird das dem „berechtigten Interesse an der Auskunftserteilung" gegenüberstehende Rechtsgut nicht ausreichend konkretisiert. In dieser Bestimmung sollte daher ausdrücklich klargestellt werden, daß die genannten „sonstigen Bedenken" sich aus den schutzwürdigen Belangen der Betroffenen ergeben. Hierunter fällt nicht nur das schutzwürdige Interesse des Angeklagten, sondern grundsätzlich auch das der sonstigen Verfahrensbeteiligten.

Ich habe daher dem Bayer. Staatsministerium der Justiz in Angleichung an Art. 18 Abs. 1 BayDSG für Nr. 185 Abs. 4 Satz 2 RiStBV folgende Formulierung vorgeschlagen, die die Voraussetzung einer zulässigen Datenübermittlung regeln sollte:

„....., soweit der Empfänger ein berechtigtes Interesse an der Auskunftserteilung glaubhaft macht und dadurch schutz würdige Belange der Betroffenen nicht beeinträchtigt werden".

Um darüber hinaus sicherzustellen, daß die aus einer derartigen Akteneinsicht erlangten Kenntnisse von Privaten oder privaten Einrichtungen nicht für andere Zwecke verwendet werden, habe ich angeregt, eine dem Art. 18 Abs. 5 BayDSG entsprechende Regelung aufzunehmen, damit gewährleistet wird, daß die Unterlagen nur zum angegebenen Zweck verwendet werden.

Auch bei der mit Nr. 185 a RiStBV vorgenommenen Neuregelung der „Akteneinsicht für wissenschaftliche Vorhaben" fehlt es meines Erachtens an einer Abwägung mit den schutzwürdigen Belangen der vom Strafverfahren Betroffenen. Zwar regelt Nr. 185 a Abs. 1 Satz 2 RiStBV, daß die Gewährung von Akteneinsicht mit Auflagen verbunden werden kann und in der Regel die Auflage zu erteilen ist, daß die Akten nicht an Dritte weitergegeben werden dürfen, doch fehlt es hier ebenfalls an einer Art. 18 Abs. 5 BayDSG vergleichbaren strengen Pflicht zur Zweckbindung. Das Verbot der Aktenweitergabe hindert nicht ausdrücklich, daß Daten aus dem Inhalt der Akten an Dritte übermittelt werden. Diese Gefahr besteht insbesondere dann, wenn wissenschaftliche Vorhaben im Bereich von Universitäten durchgeführt werden und eine zunächst nicht absehbare Zahl von Studenten Zugang zu den Akten haben.

Schließlich habe ich angeregt, daß für die Akteneinsicht für wissenschaftliche Vorhaben in Nr. 185 a RiStBV noch weitere Auflagen eingefügt werden sollten:

Den Akten dürfen nur anonymisierte Daten entnommen werden, sofern diese für das Forschungsvorhaben ausreichen. Außerdem müssen die den Akten entnommenen Daten schnellstmöglich, spätestens bei Beendigung des Forschungsvorhabens, gelöscht werden.

Das Bayer. Staatsministerium der Justiz hat in seiner Erwiderung darauf hingewiesen, daß die von mir für notwendig erachtete Interessen- und Güterabwägung bereits in der derzeitigen Vorschrift ausreichend berücksichtigt sei.

Da eine Änderung der Grundsätze für die Akteneinsicht in den Richtlinien für das Straf- und Bußgeldverfahren in dem von mir vorgeschlagenen Sinne von den Justizbehörden offensichtlich nicht beabsichtigt ist, erwarte ich zumindest, daß bei Anwendung der Vorschriften in Nr. 185 und 185 a RiStBV bei der Gewährung des Akteneinsichtsrechts gleichwohl die von mir als notwendig erachtete Güterabwägung vorgenommen wird und daß die Einsichtnehmenden auf die Zweckbindung der Daten hingewiesen und ihnen ggf. entsprechende Auflagen gemacht werden.

4.5.5 Mitteilungen in Strafsachen

Nach der Anordnung über Mitteilungen in Strafsachen (MiStra) unterrichten Gerichte und Staatsanwaltschaften andere Behörden und Stellen über Entscheidungen in Strafsachen. Wie ich bereits in meinen letzten beiden Tätigkeitsberichten mitgeteilt hatte, haben die Datenschutzbeauftragten des Bundes und der Länder Bedenken gegen die derzeitige Praxis der Übermittlung von Entscheidungen in Strafsachen geäußert. In einem hierzu ergangenen Beschluß haben sie festgestellt, daß die MiStra wichtigen Grundentscheidungen des Gesetzgebers und des Bundesverfassungsgerichts zu Fragen des Persönlichkeitsschutzes nicht mehr entspricht.

Der von der Justizministerkonferenz in dieser Angelegenheit eingesetzte Unterausschuß hat seine Arbeit noch nicht abgeschlossen. Derzeit finden auch noch Abstimmungen mit den Ressorts statt über die Erforderlichkeit der einzelnen Mitteilungen. Nach den derzeitigen Zeitplanungen ist etwa Ende 1983 mit einem Ergebnis zu rechnen. Ob daneben der Bund auf dem Gebiet der Mitteilungen in Strafsachen gesetzgeberisch tätig wird, ist mir nicht bekannt.

4.5.6 Mitteilung an den Anzeigeerstatter über Ausgang eines Ordnungswidrigkeitenverfahrens

Ein Bürger hatte sich beklagt, daß ihm als Anzeigeerstatter eine Auskunft über den Ausgang eines Ordnungswidrigkeitenverfahrens unter Hinweis auf das „Datenschutzgesetz" verweigert worden sei.

Ich erfahre immer wieder, daß Auskunftsbegehren von öffentlichen Stellen unter Hinweis auf den „Datenschutz" - meist aus Unkenntnis der Rechtslage und aus der Befürchtung heraus, etwas falsch zu machen - abgelehnt werden. Auch im vorliegenden Fall halte ich die Reaktion der zuständigen Verwaltungsbehörde für nicht sachgerecht und dem Datenschutzgedanken abträglich. Das Bayer. Datenschutzgesetz war im vorliegenden Fall schon deshalb nicht einschlägig, weil die Angaben und Feststellungen über den zur Anzeige gebrachten Verstoß weder in Dateien gespeichert noch aus Dateien übermittelt wurden. Zum anderen gehen besondere Vorschriften über Verfahren der Rechtspflege gemäß Art. 2 Abs. 2 BayDSG dem Bayer. Datenschutzgesetz vor. Vorrangig in diesem Sinne sind die Vorschriften zur Ahndung von Ordnungswidrigkeiten und von Straftaten anzusehen.

Zur Notwendigkeit der Mitteilung an den Anzeigeerstatter im Verfahren nach dem Ordnungswidrigkeitengesetz gilt meines Erachtens folgendes:

Eine Mitteilung an den Anzeigenden ist notwendig, wenn der Anzeigende nicht nur eine Anregung zur Prüfung eines Sachverhalts gegeben hat, sondern mit der Anzeige ersichtlich die Durchführung eines Bußgeldverfahrens gegen den Angezeigten erstrebt hat. Dies folgt aus § 171 Satz 1 StPO, der in Verbindung mit § 46 Abs. 1 OwiG im Ordnungswidrigkeitenverfahren anwendbar ist. Soweit im Einzelfall eine Anzeige nicht aufgenommen werden mußte - etwa weil der Sachverhalt keine Anhaltspunkte für eine Ordnungswidrigkeit enthält - braucht auch die Einstellung nicht mitgeteilt zu werden. Die Angabe der Gründe für die Einstellung des Verfahrens ist, abweichend von § 171 Satz 1 StPO, nicht erforderlich, weil dem Anzeigenden gegen die Einstellung ein gesetzlicher Rechtsbehelf nicht zusteht. Sofern jedoch die Verwaltungsbehörde, bei der Anzeige erstattet worden ist, die Sache an die Staatsanwaltschaft nach § 41 Abs. 1 OwiG abgibt, teilt die Staatsanwaltschaft eine Einstellung des Verfahrens grundsätzlich dem Anzeigeerstatter mit (§ 171 Abs. 1 Satz 1 StPO, Nr. 89 Richtlinien für das Straf- und Bußgeldverfahren). Diese Mitteilungspflicht an den Anzeigeerstatter soll diesem in einem Strafverfahren die Möglichkeit der Klageerzwingung nach § 172 StPO eröffnen. Dieses Klageerzwingungsverfahren sichert das in der Strafprozeßordnung verankerte Legalitätsprinzip. Da für Ordnungswidrigkeiten der Opportunitätsgrundsatz gilt, besteht zwar keine Möglichkeit der Klageerzwingung für den Anzeigenerstatter, er soll jedoch durch die Möglichkeit einer Gegenvorstellung oder Dienstaufsichtsbeschwerde auch im Ordnungswidrigkeitenverfahren auf eine sachgerechte Behandlung seiner Anzeige dringen können. Hierzu muß er über die Einstellung des Verfahrens unterrichtet sein.

Ergeht gegen die Person, gegen die sich die Anzeige gerichtet hatte, ein Bußgeldbescheid oder ein Urteil, so entfällt das Interesse einer Klageerzwingung oder einer Überprüfung des Handelns der Verwaltungsbehörde. Deshalb ist eine Mitteilung an den Anzeigenerstatter über einen derartigen Ausgang des Verfahrens nicht veranlaßt. Aus der Tatsache, daß er keine Mitteilung über eine Einstellung des Verfahrens erhalten hat, kann der Anzeigenerstatter daher grundsätzlich den Schluß ziehen, daß das Verfahren mit einem entsprechenden Bescheid oder Urteil geendet hat.

4.5.7 Kriminologische Zentralstelle

Die Probleme einer Einrichtung der Kriminologischen Zentralstelle und einer etwaigen Übermittlung personenbezogener Daten sind im 4. Tätigkeitsbericht kurz dargestellt. Dabei habe ich auch darauf hingewiesen, daß ich meine diesbezüglichen Bedenken dem Bayer. Staatsministerium der Justiz mitgeteilt und die Bitte geäußert hatte, zu prüfen, inwieweit sichergestellt werden kann, daß die Kriminologische Zentralstelle einer ausreichenden Datenschutzkontrolle unterzogen wird.

Derzeit ist die Kriminologische Zentralstelle noch nicht eingerichtet. Nach einem Beschluß der Ministerpräsidentenkonferenz sollen die Voraussetzungen dafür geschaffen werden, daß die Kriminologische Zentralstelle im Jahre 1984 ihren Betrieb aufnehmen kann. Damit stellen sich die im letzten Tätigkeitsbericht aufgeworfenen Datenschutzprobleme noch nicht. Das Bayer. Justizministerium geht im übrigen davon aus, daß bei Arbeitsaufnahme der Kriminologischen Zentralstelle eine sinnvolle Regelung zur datenschutzrechtlichen Kontrolle getroffen werde, weil auf ein entsprechendes Schreiben, das den anderen Landesjustizverwaltungen zugegangen sei, ein diesbezüglicher Widerstand nicht erkennbar geworden sei.

4.5.8 Persönlichkeitsschutz der Zeugen im Strafprozeß

In einem Verfahren vor einem Münchner Gericht wegen sexueller Straftaten wurden mehrere Zeuginnen zu ihrem Verhältnis zum Angeklagten befragt. Dieser aufsehenerregende Prozeß fand insbesondere in den Medien starke Beachtung. Weil die Öffentlichkeit nicht ausgeschlossen war, mußten insbesondere die Zeuginnen eine Herabwürdigung ihrer Ehre hinnehmen.

Der Rechts- und Verfassungsausschuß des Bayer. Senats hat deshalb folgende Beschlußempfehlung (Senatsdrucksache 37/83) verabschiedet:

„Der Ausschuß schlägt vor, dem Antrag in folgender Fassung zuzustimmen:

Der Senat ersucht die Staatsregierung, die Staatsanwaltschaften anzuweisen, die Vorschriften zum Schutze des Persönlichkeits rechts der Zeugen umfassend zu wahren.

Ferner regt der Senat an, die Prozeßordnungen darauf hin zu überprüfen, ob sie die Persönlichkeitsphäre der Zeugen hinrei chend schützen; ggf. empfiehlt der Senat eine Gesetzesinitiative über den Bundesrat.

Der Senat bittet zu erwägen, in die Regelung des § 172 Nr. 2 GVG ein Antragsrecht des Zeugen aufzunehmen.

Der Senat ersucht die Staatsregierung ferner, die Staatsanwalt schaften anzuweisen, darauf hinzuwirken, daß der Würde des

Gerichts und dem Ansehen der Rechtspflege durch das Benehmen eines Prozeßbeteiligten nicht Abbruch getan wird."

Die Frage des Ausschlusses der Öffentlichkeit habe ich im 4. Tätigkeitsbericht (S. 29) kurz angesprochen. Zwar ist das Bayer. Datenschutzgesetz auf die Durchführung einer gerichtlichen Verhandlung grundsätzlich nicht anwendbar, jedoch steht die Frage des Persönlichkeitsschutzes bei derartigen Hauptverhandlungen besonders stark im Vordergrund. Deshalb begrüße ich die Initiative des Rechts- und Verfassungsausschusses des Bayer. Senats außerordentlich.

4.5.9 Übermittlung von Gerichtsakten

Ein Bürger, gegen den vor einem Landgericht ein Strafverfahren anhängig ist, hat gerügt, daß das mit der Sache befaßte Gericht die ihn betreffenden Strafakten an ein Max-Planck-Institut zur Auswertung übersandt habe. Diesen Vorgang habe ich wie folgt bewertet:

Zunächst ist festzustellen, daß das Bayer. Datenschutzgesetz auf Strafakten und deren Weitergabe unmittelbar nicht anzuwenden ist. Wie ich allerdings schon mehrfach festgestellt habe, besteht auch außerhalb des Geltungsbereichs des Bayer. Datenschutzgesetzes für die Justiz kein datenschutzfreier Raum. Denn soweit die Übermittlung von personenbezogenen Daten durch Gerichte nicht gesetzlich geregelt ist, muß grundsätzlich auf die tragenden Bestimmungen der Verfassung zum Schutz der Persönlichkeit zurückgegriffen werden. So hat das Bundesverfassungsgericht in einer Reihe von Entscheidungen festgestellt, daß das Grundgesetz dem einzelnen Bürger einen unantastbaren Bereich privater Lebensgestaltung gewährt, der der Einwirkung der öffentlichen Gewalt entzogen ist. Das verfassungskräftige Gebot der Achtung der Intimsphäre des Einzelnen hat seine Grundlage in dem durch Art. 2 Abs. 1 Grundgesetz verbürgten Recht auf freie Entfaltung der Persönlichkeit. Bei der Bestimmung von Inhalt und Reichweite dieses Grundrechts ist zu beachten, daß nach der Grundnorm des Art. 1 Abs. 1 Grundgesetz die Würde des Menschen unantastbar ist und von aller staatlichen Gewalt geachtet und geschützt werden muß. Jedoch steht nicht der gesamte Bereich des privaten Lebens unter dem absoluten Schutz dieser Grundrechte. Als gemeinschaftsbezogener und gemeinschaftsgebundener Bürger muß vielmehr jedermann staatliche Maßnahmen hinnehmen, die im überwiegenden Interesse der Allgemeinheit unter strikter Wahrung des Verhältnismäßigkeitsgebotes erfolgen, soweit sie nicht den unantastbaren Bereich privater Lebensgestaltung beeinträchtigen.

Akten eines Strafverfahrens können Tatsachen enthalten, die den grundrechtlich geschützten privaten Lebensbereich eines Angeklagten berühren. Dabei ist jedoch festzustellen, daß sie dem schlechthin unantastbaren Bereich privater Lebensgestaltung, bei dem schon jeder Einblick durch Außenstehende von vorneherein unzulässig wäre, wegen des staatlichen Strafanspruchs nicht zugeordnet werden können. Sofern jedoch in den Akten Vorgänge enthalten sind, die nach Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 Grundgesetz der Geheimhaltung unterliegen, ist eine Übermittlung dieser Akten nur zulässig, wenn die Betroffenen einwilligen oder die Übermittlung unter Beachtung des Verhältnismäßigkeitsgebotes gerechtfertigt ist. Der Grundsatz der Verhältnismäßigkeit verlangt insbesondere die generelle Abwägung zwischen dem Schutz der Privatsphäre des Einzelnen und dem öffentlichen Interesse.

Dieser von der Verfassung gewährleistete Schutz der Privatsphäre wird hinsichtlich der Übermittlung von Strafakten durch Nr. 185 a der Richtlinien für das Straf- und Bußgeldverfahren konkretisiert, die an Stelle der bisherigen Nr. 185 Abs. 3 der Richtlinien getreten ist. Hiernach wird für wissenschaftliche Vorhaben Akteneinsicht nur gewährt, wenn und soweit deren Bedeutung dies rechtfertigt und die Gewähr besteht, daß ein Mißbrauch der erlangten Kenntnisse nicht zu befürchten ist. Außerdem kann die Gewährung der Akteneinsicht mit Auflagen verbunden werden. In der Regel ist dabei die Auflage zu erteilen, daß die Akten nicht an Dritte weitergegeben werden dürfen und daß Hinweise auf Verfahrensbeteiligte oder auf Tatsachen, die zu deren Identifizierung führen können, zu vermeiden sind (vgl. hierzu oben Nr. 4.5.4. meines Tätigkeitsberichtes).

Bei einer Weitergabe von Strafakten an ein Max-Planck-Institut für ausländisches und internationales Strafrecht zur Auswertung für wissenschaftliche Zwecke ist ein Mißbrauch der durch Strafakten erlangten Kenntnisse grundsätzlich nicht zu befürchten. Die im Rahmen der Nr. 185 a der Richtlinien notwendige Abwägung zwischen schutzwürdigen Belangen der Verfahrensbeteiligten und dem öffentlichen Interesse an der wissenschaftlichen Forschung kann im übrigen nur im jeweiligen Einzelfall vorgenommen werden. Ein Primat kommt der Wissenschaft nach herrschender Rechtsprechung hierbei nicht zu (vgl. BVerfGE 57, 70/99).

4.5.10 Weitergabe gerichtlicher Entscheidungen

Im Geschäftsbereich des Bayer. Staatsministeriums der Justiz besteht eine Anordnung, daß im Hinblick auf die besondere Vertraulichkeit in Personalangelegenheiten gerichtliche Entscheidungen in personalrechtlichen Angelegenheiten an andere Gerichte und Behörden, die mit dem Verfahren nicht dienstlich befaßt sind, nur nach Unkenntlichmachung des Namens und anderer, zur Identifizierung geeigneter Merkmale weitergegeben werden dürfen. Mit dieser Anordnung wird den berechtigten Belangen der Verfahrensbeteiligten Rechnung getragen. Denn durch die Weitergabe eines Urteils, die ohne Unkenntlichmachung des Namens und der Beschäftigungsbehörde erfolgt, würden Daten des Privatbereichs der Beteiligten einem Dritten zugänglich gemacht, die grundsätzlich unter den von Art. 1 Abs. 1 und Art. 2 Abs. 1 Grundgesetz geschützten Bereich des allgemeinen Persönlichkeitsrechts fallen. Meines Erachtens sollten grundsätzlich in allen Entscheidungen, die an am Gerichtsverfahren nicht beteiligte Stellen versandt werden, die Namen unkenntlich gemacht werden.

An dieser Bewertung ändert sich auch nichts, wenn eine gerichtliche Entscheidung in öffentlicher Sitzung verkündet wird. Dem in den §§ 169 ff. Gerichtsverfassungsgesetz geregelten Öffentlichkeitsgrundsatz der Verhandlung und Verkündigung liegen rechtsstaatliche Erwägungen zugrunde, nach denen die rechtsprechende Gewalt vor der Allgemeinheit zu wirken hat und den Bürgern die Möglichkeit der Kenntnis des gesprochenen Rechts gegeben wird. Diese Öffentlichkeit ist jedoch auf die Hauptverhandlung beschränkt. Denn während in der mündlichen Verhandlung bei Verkündung des Urteils zwangsläufig die Namen der Verfahresbeteiligten genannt werden müssen, kann das schriftlich niedergelegte Urteil seinen Zweck, neben den Prozeßbeteiligten auch die Öffentlichkeit über die Rechtsprechung zu unterrichten, auch erfüllen, wenn die Namen der Verfahrensbeteiligten unkenntlich gemacht oder nicht genannt werden. So geschieht es im übrigen auch stets bei der Veröffentlichung von Urteilen in amtlichen oder privaten Sammlungen. Schließlich würde eine Weitergabe von Urteilen mit Anführung der Namen der Prozeßbeteiligten auch gegen die dem Beamten in Art. 69 Bayer. Beamtengesetz (für Richter gilt diese Vorschrift nach Art. 2 Abs. 1 Bayer. Richtergesetz ebenfalls) gebotene Verschwiegenheitspflicht verstoßen.

Im Berichtszeitraum ist mir ein Verstoß gegen die vorgenannte Anordnung des Bayer. Staatsministerium der Justiz bekannt geworden. Hierbei hat es sich offensichtlich um ein einmaliges Versehen der betroffenen Geschäftsstelle gehandelt.

4.5.11 Vorlage von behördlichen Akten an Gerichte

Nach § 99 Abs. 1 Satz 1 Verwaltungsgerichtsordnung (VwGO) sind Behörden zur Vorlage von Urkunden oder Akten und zu Auskünften verpflichtet. Somit bemißt sich die Zulässigkeit der Vorlage von Behördenakten in einem verwaltungsgerichtlichen Verfahren nach § 99 VwGO. Das Bayer. Datenschutzgesetz findet im vorliegenden Fall gemäß Art. 2 Abs. 2 keine Anwendung, auch wenn im Einzelfall die angeforderten Unterlagen aus Dateien stammen, weil besondere Vorschriften über Verfahren der Rechtspflege vorgehen.

Allerdings besteht für ein verwaltungsgerichtliches Verfahren auch dann kein datenschutzfreier Raum, wenn das Bayer. Datenschutzgesetz nicht unmittelbar anwendbar ist. Dies habe ich schon mehrfach festgestellt. Deshalb muß auch die Vorlagepflicht nach § 99 Abs. 1 Satz 1 VwGO die berechtigten Interessen der Personen berücksichtigen, zu denen Daten in den angeforderten Verwaltungsakten enthalten sind. Zwar gibt § 99 Abs. 1 Satz 2 VwGO der Behörde unter den dort genannten Voraussetzungen das Recht, die Vorlage von Akten zu verweigern, doch sind dort die „schutzwürdigen Interessen von Beteiligten" als Prüfungsmaßstab nicht ausdrücklich erwähnt.

Ohne hier im einzelnen auf die Interpretation der Vorschrift des § 99 VwGO eingehen zu wollen, darf ich doch auf die vom Bundesverfassungsgericht in seiner „Scheidungsakten" -Entscheidung (BVerfGE 27, S. 344/350 ff) entwickelten Grundsätze hinweisen. Damit ist jedenfalls in all den Fällen, in denen in der Aktenübersendung an das Gericht ein Eingriff in das Persönlichkeitsrecht der Betroffenen liegt, eine Übersendung ohne das Einverständnis der Betroffenen nur dann zulässig, wenn die Übersendung nach dem Verhältnismäßigkeitsprinzip gerechtfertigt ist. In einem derartigen Falle hat die zur Aktenübersendung aufgeforderte Behörde die Prüfung der Verhältnismäßigkeit unter Würdigung aller persönlichen und tatsächlichen Umstände des Einzelfalles vorzunehmen. Bei einer derartigen Abwägung wird die Behörde gegebenenfalls auch in Betracht ziehen, ob dem gerichtlichen Verlangen nicht durch eine Übersendung eines Auszugs der Akten ebenfalls Genüge getan werden kann, wenn hiermit die Beeinträchtigung schutzwürdiger Belange der Beteiligten vermieden wird.

4.6 **Melderecht**

4.6.1 Entwurf eines Bayer. Landesmeldegesetzes

Im Berichtsjahr wurde der Entwurf eines Bayer. Landesmeldegesetzes (ELMG) zur Ausführung des Bundes-Melderechts-Rahmengesetzes (MRRG) vorgelegt. Zu dem von einer Arbeitsgruppe der Innenministerien der Länder früher vorgelegten "Formulierungsvorschlag für ein Landesmeldegesetz" und der Stellungnahme der Datenschutzbeauftragten hierzu finden sich Ausführungen im 4. Tätigkeitsbericht unter Nr. 3.1. Aus meiner Stellungnahme zum Entwurf für ein Bayer. Landesmeldegesetz und der Beratung dieses Entwurfs im Beirat beim Landesbeauftragten für den Datenschutz am 18.5.1982 seien folgende Punkte festgehalten:

- Aus der Sicht des Datenschutzes sind ELMG, wie auch MRRG, zu begrüßen. Eine ganze Reihe von generellen Fragen z.B. zur Datenübermittlung, zur Kontrolle der Datenverarbeitung, zu den kostenfreien Schutzrechten des Bürgers und Einzelfragen, wie die immer wieder „problematisierte" Frage der Jubiläumsdaten, finden weitgehend zufriedenstellende Lösungen. Die Aufgaben der Meldebehörden werden im ELMG abschließend festgelegt. Danach ist es Aufgabe der Meldebehörden, die Identität der Einwohner und ihre Wohnungen festzustellen und nachzuweisen. Hierin liegt eine bewußte Beschränkung und eine Abkehr von einem in früheren Entwürfen zu Bundesmeldegesetzen vorgesehenen umfassenden Einwohnerinformationssystem.

Zu einzelnen Artikeln des Entwurfs:

- Die Speicherung von Aufenthaltsanfragen nach Art. 3 Abs. 2 Nr. 6 ELMG bezieht sich nur auf Personen, die in der Gemeinde einmal gewohnt haben; sie ist auf 2 Jahre befristet. Als Beispiele für festzuhaltende Aufenthaltsanfragen wurden genannt: Das Bundesverwaltungsamt suche Personen, denen finanzielle Hilfe im Ausland gewährt worden sei und die sich, ohne Rückzahlung zu leisten, abgesetzt haben. Die Staatsanwaltschaft suche ausgeschriebene Personen. Auch ehemalige Studenten, die Förderungsmittel bezogen aber nicht zurückbezahlt haben, würden gesucht. Schließlich suche das Jugendamt unterhaltspflichtige Personen.
- Die Speicherung von Seriennummern des Passes und des Personalausweises im Melderegister soll nicht zu einer Erweiterung des Rahmens der für die Identitätsfeststellung zu speichernden Daten führen, da diese durch das MRRG abschließend festgelegt sind. Sie soll auch nicht zu einer Erschließung des Melderegisters über die Personalausweis-Nummer führen, da dies gem. § 3 Abs. 4 und 5 des Bundes-Personalausweisgesetzes unzulässig ist (Verbot der Erschließung von Dateien mit Hilfe der Serien-Nummer). Die Speicherung der Nummer soll vielmehr dazu dienen, festzustellen, ob vorgelegte Ausweispapiere tatsächlich auf die entsprechende Person ausgestellt wurden. Es sei daran erinnert, daß das Verbot der Erschließung von Dateien mit Hilfe der Serien-Nummer verhindern soll, daß diese Serien-Nummern zu Ersatz-Personenkennzeichen werden (siehe auch 3. Tätigkeitsbericht, Nr. 2.1, S. 5/6).
- Nach Art. 3 Abs. 2 Nr. 8 ELMG soll die Tatsache, daß jemand aus den im Bundesvertriebenengesetz näher bezeichneten Gebieten stammt, für Zwecke der Übermittlung dieser Tatsache an den Suchdienst gespeichert werden. § 4 Abs. 2 MRRG sieht die Erhebung der Angabe beim Betroffenen und Übermittlung an den Suchdienst vor. Nach Abschluß der Übermittlung kommt meiner Ansicht nach daher eine Löschung oder zumindest Sperrung dieser Angabe in Frage, da es nach dieser Vorschrift nicht Aufgabe der Meldebehörde ist, außer der Übermittlung an den Suchdienst, Personen, die aus den genannten Gebieten stammen, ohne ihre Einwilligung auf Dauer im Melderegister besonders zu kennzeichnen und ggf. diese Angabe auch an andere Behörden zu übermitteln.
- Art. 3 Abs. 1 und 2 ELMG sehen neben der Speicherung der dort genannten Daten auch die Speicherung von Hinweisen zum Nachweis ihrer Richtigkeit vor. Nach der amtlichen Begründung sind darunter in erster Linie Angaben über Urkunden, andere Nachweise (z.B. ausstellende Behörde, Aktenzeichen, Tag der Ausstellung usw.) und die sonstige Herkunft von Daten zu verstehen. Daraus ergibt sich, daß als Hinweise zwar die entsprechenden Beweismittel, nicht aber deren Inhalt gespeichert werden dürfen. So darf etwa bei Vorliegen von Wahlausschlußgründen zwar das Aktenzeichen der Gerichtsentscheidung, nicht aber der Grund, der zum Wahlausschluß geführt hat (z.B. geistige Gebrechlichkeit), gespeichert werden. Andernfalls würde die Speicherung von Hinweisen zum Festhalten von noch erheblich sensibleren Daten führen, als es das Meldegesetz selbst sonst vorsieht.
- Art. 4 ELMG sieht die Einführung eines Ordnungsmerkmals (OM) für die Verwaltung von Datenbeständen der Meldebehörden vor. Gegenwärtig dient ein entsprechendes OM den an die AKDB angeschlossenen Meldebehörden innerhalb des jeweiligen Regierungsbezirks als eindeutiges Identifizierungsmerkmal eines einzelnen Betroffenen. Wer zwei Wohnsitze innerhalb eines Regierungsbezirks hat, wird also dort nur mit einem OM geführt. Es ist nicht auszuschließen, daß die Verwendung dieses eindeutigen Merkmals auf ganz

Bayern ausgedehnt werden könnte. Aus der Sicht des Datenschutzes war daher eine Auseinandersetzung mit der Frage geboten, ob der Gesetzentwurf Ansätze zur Einführung eines allgemeinen Personenkennzeichens enthielte. Unbestritten ist wohl, daß die Verbreitung eines landesweit eindeutigen OM bei einer Vielzahl von Behörden und privaten Stellen die Entstehung eines „Personenkennzeichens" (PK) bedeuten könnte. Aus der amtlichen Begründung zum ELMG ergibt sich jedoch, daß dies nicht beabsichtigt ist. In Art. 4 ELMG sind auch Einschränkungen vorgesehen, die dies verhindern sollen: OM dürfen vom Empfänger von Meldedaten nur an die jeweilige Meldebehörde übermittelt werden, die Übermittlung von OM an nichtöffentliche Stellen ist unzulässig.

Die Datenschutzbeauftragten der Länder und des Bundes hatten in einem Beschluß ihrer Konferenz gefordert, das OM lediglich zwischen Meldebehörden zu verwenden und an andere Behörden, öffentlich-rechtliche Religionsgesellschaften und private Stellen in keinem Falle zu übermitteln (siehe 4. Tätigkeitsbericht, Nr. 3.1.2, S. 15). Da dieser Forderung im ELMG nicht entsprochen wurde, vielmehr die Verwendung des OM bei Datenübermittlungen an andere öffentliche Stellen oder öffentlich-rechtliche Religionsgesellschaften durch Art. 4 des Entwurfs zugelassen wird, war aus der Sicht des Datenschutzes besonderer Wert darauf zu legen, die Verbreitung des OM durch Stellen, die Meldedaten erhalten, möglichst zu verhindern und die sonstige Erhebung des OM auszuschließen. Im Beirat beim Landesbeauftragten für den Datenschutz bestand darüber Einigkeit, daß ein Verbot der Verwendung des OM für nichtöffentliche Stellen einzuführen sei und daß die Vollzugsbekanntmachung zur Ausführung des Meldesgesetzes eine ausdrückliche Regelung zum Umgang mit OM bei Stellen, die das OM mit Meldedaten erhalten, aufweisen müsse. Ein Verbot der Erhebung des OM durch Behörden - außerhalb der Übermittlung vom Meldeamt zusammen mit Meldedaten - wurde in der Beiratsitzung am 25. Januar 1983, die sich nochmals mit dem ELMG befaßte, gebilligt und am 1.2.1983 vom Berichterstatter in der Sitzung des Rechts- und Verfassungsausschusses des Bayer. Landtags zusammen mit dem Erhebungs- und Nutzungsverbot für nichtöffentliche Stellen in die Gesetzesberatung eingebracht. Dies ist in Art. 4 Abs. 3 und 4 MeldeG nunmehr Gesetz geworden. Es ist aus der Sicht des Datenschutzes wichtig, daß diese Einschränkungen eine weitere Verbreitung des OM und seine Nutzung als Verknüpfungsmerkmal zwischen öffentlichen Stellen und erst recht zwischen privaten Stellen verhindern. Die vom Gesetz erlaubte beschränkte Nutzung des OM durch andere Behördenals Meldeämter und öffentliche Religionsgesellschaften muß daher laufend beobachtet werden.

- Hinsichtlich der Datenschutz-Rechte der Betroffenen stellt die amtliche Begründung zum ELMG nunmehr klar, daß weitergehende Bestimmungen des BayDSG neben den Bestimmungen des Landesmeldegesetzes uneingeschränkt gelten. Dies kann beispielsweise für das nach Art. 10 BayDSG weiter gehende Recht auf Sperrung von Daten und den nach Art. 8 BayDSG weiteren Anspruch auf Auskunft über Stellen, denen Daten in automatisierten Verfahren regelmäßig übermittelt werden, von Bedeutung sein.
- Zur Regelung über die Archivierung von Meldedaten in Art. 12 ELMG wurde im Beirat Einigkeit darüber erzielt, daß in den Fällen, in denen noch nicht löschungsreife Meldedaten an Archive lediglich zur Verwahrung übergehen werden, die Daten im Archiv nur vom Meldeamt und nicht zu sonstigen archivalischen Zwecken genutzt werden dürfen. Solche, beispielsweise aus Platzmangel zur Verwahrung im Archiv gelagerten Daten sind dagegen von Informationen zu unterscheiden, die zur rechtmäßigen Erfüllung der Aufgaben des Meldeamts nicht mehr erforderlich sind und dem Archiv für Archivzwecke zur Übernahme angeboten werden.
- In Art. 20 ELMG, der die Auskunftspflicht des Wohnungsgebers gegenüber dem Meldeamt regelt, wurde aufgrund eines Vorschlags aus der Beratung im Senat klargestellt, daß der Vermieter nicht verpflichtet wird, für die Meldebehörde Daten der Mieter zu speichern.
- Die Befugnis der Polizei, gem. Art. 28 ELMG Einsicht in das von Krankenhäusern zu führende Verzeichnis der Patienten zu nehmen, darf sich nicht auf Fälle der Kleinkriminalität erstrecken. Die Einsichtnahme muß sich am Grundsatz der Verhältnismäßigkeit orientieren. Ordnungswidrigkeiten rechtfertigen eine solche Einsichtnahme in Patientendaten nicht. Dies ergibt sich einmal daraus, daß § 16 MRRG eine Ermächtigung zur Verarbeitung dieser Angaben zum Zwecke der Gefahrenabwehr und der Strafverfolgung oder zur Aufklärung von Schicksalen von Vermißten und Unfallopfern enthält, zum anderen daraus, daß das Bundesverfassungsgericht festgestellt hat, daß eine Einsichtnahme in medizinische Angaben nicht generell mit dem Interesse an der Aufklärung von Straftaten gerechtfertigt werden kann, sondern daß überwiegende Belange des Gemeinwohls dies zwingend gebieten müssen (BVerfGE 32, 83 f). Die Tatsache des Aufenthalts in einem Krankenhaus, insbesondere in einem Spezialkrankenhaus oder in bestimmten Abteilungen von Krankenhäusern, ist in vielen Fällen ein besonders geheimhaltungsbedürftiges medizinisches Datum, das auch der ärztlichen Schweigepflicht unterliegt. Eine Durchbrechung muß sich daher am Verhältnismäßigkeitsgrundsatz orientieren. Im Beirat wurde vom Bayer. Staatsministerium des Innern in Aussicht gestellt, dies in der Vollzugsbekanntmachung zum Meldegesetz ausdrücklich klarzustellen.
- Nach der amtlichen Begründung des Entwurfs werden auch Online-Anschlüsse ans Melderegister als regelmäßige Datenübermittlung gem. Art. 31 Abs. 4 ELMG behandelt. Die Frage der automatischen Protokollierung solcher Abfragen muß noch geklärt werden. Ich gehe davon aus, daß die Einrichtung eines neuen Online-Anschlusses an ein Melderegister ein Verfahren darstellt, daß gem. Art. 26 Abs. 2 BayDSG freizugeben und gem. Art. 26 Abs. 4 BayDSG dem Landesbeauftragten für den Datenschutz rechtzeitig vor Einführung mitzuteilen ist.
- Die Vorschrift des Art. 35 Abs. 1 ELMG, wonach Parteien und Wählergruppen 6 Monate vor der Wahl Einwohneradressen übermittelt werden dürfen, wird wohl auch künftig dazu führen, daß beim Landesbeauftragten für den Datenschutz Beschwerden darüber eingehen, daß von Behörden für Wahlwerbung Adressenmaterial zur Verfügung gestellt wird. Im Beirat beim Landesbeauftragten für den Datenschutz wurde daher vorgesehen, den Betroffenen ein Widerspruchsrecht, ähnlich dem im Falle von Jubiläumsdaten vorgesehenen, einzuräumen, das allerdings nicht auf bestimmte Parteien oder Wählergruppen begrenzt wäre. Der Vorschlag wurde vom Vorsitzenden des Beirats in die Gesetzesberatung im Rechts- und Verfassungsausschuß des Landtags eingebracht und ist so Gesetz geworden.
- Art. 42 ELMG erlaubt der Polizei - bis Ende 1985 - auch außerhalb der Dienstzeit des Meldeamts in das Melderegister selbst Einblick zu nehmen. Im Beirat wurde Einvernehmen darüber erzielt, daß die Polizei bei solchen Einsichtnahmen einen Vermerk hinterläßt, der zu Kontrollzwecken den Vorgang, dessentwegen Einsicht genommen wurde, festzustellen erlaubt, ohne gleichzeitig dem Meldeamt die Person bekannt zu geben, derentwegen Einsicht genommen wurde. Bei Online-Anschluß an Melderegister kann die gleiche Wirkung durch die Protokollierung des Abrufs erzielt werden.

4.6.2 Übermittlung von Meldedaten zu Forschungszwecken

Nach dem noch im Berichtsjahr geltenden Melderecht ergaben sich Fragen, die auch jetzt noch Beachtung verdienen:

- Das Ersuchen eines Jugendamts an die kreisangehörigen Gemeinden, Namen, Geburtsdatum und Anschrift sämtlicher Jugendlicher zwischen 10 und 20 Jahren zum Zwecke einer empirischen Untersuchung zu übermitteln, warf aus der Sicht des Datenschutzes folgende Fragen auf:

  Ziel der Übermittlung der Daten aller, also 100% der Jugendlichen zwischen 10 und 20 Jahren war es, in dem geprüften Fall für eine freiwillige Umfrage wenigstens eine Antwortquote von 5% sicherzustellen. Die hohe Differenz zwischen 5% letztlich benötigten Antworten und 100% angeforderten Anschriften führte zu einer Überprüfung mit dem Ziele der Reduzierung der zu übermittelnden Daten.

  Eine zweite Frage ergab sich aus dem Charakter der Studie als freiwillige Umfrage. Einmal war darauf zu achten, daß die Entscheidung über die freiwillige Teilnahme eine gewisse Reife auf seiten des Befragten erfordert, was bei Jugendlichen zumindest vor Vollendung des 16. Lebensjahres nicht angenommen werden kann. In diesen Fällen war mithin die Entscheidung der gesetzlichen Vertreter herbeizuführen - d.h. diese waren vor allem auch zu benachrichtigen. Außerdem war sicherzustellen, daß die zu interviewenden Jugendlichen bzw. ihre Eltern vor ihrer Entscheidung über die freiwillige Teilnahme an der Befragung auch auf mögliche Folgen aus der Befragung hingewiesen würden, denn sie wurde durch Personal des Jugendamts durchgeführt. Das Jugendamt konnte daher im Einzelfall durch die Erhebung Sachverhalte erfahren, auf die es von Amts wegen zu reagieren gehalten sein könnte - unabhängig davon, ob solche Sachverhalte auch im Fragebogen festgehalten würden oder nicht.

- Bei Meldedatenübermittlung für Befragungsaktionen, die Forschungszwecken dienen, haben sich in mehreren Fällen folgende Gesichtspunkte als wichtig erwiesen:

  . Deutlicher Hinweis auf die Freiwilligkeit der Teilnahme an der Befragung. Einfügen dieses Hinweises an hervorgehobener Stelle im Fragebogen,

  . hinreichende Unterrichtung der Betroffenen über Zweck der Befragung und weitere Verwendung der erhobenen Daten - insbesondere anonymisiert oder nicht anonymisiert -, damit der Betroffene wirklich Gelegenheit hat, seine Entscheidung frei zu treffen,

  . unverzügliche Vernichtung der Daten von solchen Personen, die eine Teilnahme an der Befragung verweigern,

  . Verwendung der Daten nur zur Ausführung des konkret bezeichneten Vorhabens, keine sonstige Verarbeitung oder Weitergabe an Dritte, sowie Vernichtung der personenbezogenen Daten, sobald es der Zweck der Befragung zuläßt,

  . keine Hinweise auf bestimmte befragte Personen in Zusammenstellungen über das Ergebnis der Befragung,

  . möglichst zuverlässige und frühzeitige Anonymisierung von Fragebogen,

  . Unterrichtung der beteiligten Mitarbeiter über die notwendige Geheimhaltung,

  . Überprüfung der Fragebogen darauf, ob etwa trotz Verzichts auf Namen und Anschrift aufgrund anderer erhobener Daten in bestimmten Fällen ein Personenbezug hergestellt werden könnte.

- In einem anderen Fall der Übermittlung von Meldedaten an ein Hochschulinstitut ergab sich die Schwierigkeit, die Verwendung der angeforderten Daten für eine bestimmte Forschungsarbeit möglichst konkret festzulegen, andererseits jedoch dem Meldeamt durch eine zu detaillierte Bezeichnung - im konkreten Falle eines medizinischen Forschungsprojekts - nicht unnötigerweise indirekt Angaben über die Erkrankung oder Behandlung der betroffenen Einwohner mitzuteilen. Die Festlegung des konkreten Forschungsvorhabens erschien erforderlich, weil die Daten nicht zur freien Verfügung der Hochschule, sondern für ein bestimmtes Projekt erbeten und auch nur so zweckbezogen übermittelt werden sollten und weil nur anhand einer solchen Festlegung überhaupt definiert werden kann, was beim Empfänger mit den Daten geschieht, wer sie einsehen und auswerten darf, wann sie gelöscht werden. Auch eine Kontrolle der Datenverarbeitung unter Gesichtspunkten des Datenschutzes wäre sonst kaum möglich. Ich lege daher Wert darauf, daß ein Forschungsprojekt grundsätzlich mit seiner „offiziellen" Bezeichnung gegenüber dem Meldeamt benannt wird. In Abwägung möglicherweise entgegenstehender schutzwürdiger Belange des Betroffenen halte ich es aber im Einzelfall für notwendig, von einer solchen „offiziellen" Bezeichnung abzusehen, wenn dadurch dem Meldeamt beispielsweise „mitgeteilt" würde, der Betroffene habe sich in einer Klinik einer Strahlentherapie unterzogen.

4.6.3 Übermittlung von Meldedaten an Adreßbuchverlage

Die Übermittlung von Meldedaten an Adreßbuchverlage ist weithin üblich. Sie war im früheren Melderecht zunächst nur in der Vollzugsbekanntmachung zum Meldegesetz geregelt. Inzwischen ist Art. 35 Abs. 3 MeldeG zu berücksichtigen. Im Berichtsjahr hatte sich folgende Frage ergeben:

Ein nach Straßen und Häusern gegliedertes Einwohner- bzw. „Straßenverzeichnis" kann Auskunft darüber geben, welche Häuser von Alleinstehenden (insbesondere Frauen) bewohnt werden. Es könnte damit z.B. zur Vorbereitung von Einbruchdiebstählen (oder von Betrug, Raub usw...) leicht zugängliche Informationen geben und dadurch schutzwürdige Belange beeinträchtigen.

Um diesen Bedenken Rechnung zu tragen habe ich auf Anfrage von Gemeinden empfohlen, die beabsichtigte Datenübermittlung etwa wie folgt ortsüblich bekanntzugeben:

„Die Gemeinde beabsichtigt ein Adreßbuch herauszugeben. Dafür sollen Namen und Anschrift (gegebenenfalls auch der Dr.-Titel) aller über 18 Jahre alten Gemeindebürger an den Verlag X übermittelt werden. Die Adreßdaten sollen einmal in alphabetischer Reihenfolge nach Namen und einmal nach Straßen sortiert im Adreßbuch erscheinen. Der Landesbeauftragte für den Datenschutz hat darauf hingewiesen, daß insbesondere bei der Sortierung der Adreßdaten nach Straßen in Einzelfällen schutzwürdige Belange (z.B. alleinstehender Frauen) beeinträchtigt werden können. Gemeindebürger, die aus diesen oder anderen Gründen nicht im Adreßbuch erscheinen wollen, können dies der Stadtverwaltung bis ..... mitteilen".

Art. 35 Abs. 3 des am 1.4.83 inkraft getretenen neuen Bayer. Meldegesetzes sieht im übrigen ein allgemeines Recht vor, der Weitergabe von Daten an Adreßbuchverlage generell zu widersprechen. Auch hierauf könnte in der Bekanntmachung hingewiesen werden.

4.6.4 Übermittlung von Einwohner-Veränderungslisten

Ein Landratsamt hatte von den kreisangehörigen Gemeinden die über die AKDB erstellten Einwohner-Veränderungslisten angefordert, um die darin enthaltenen Angaben entsprechend der Müllgebührensatzung den Müllgebührenbescheiden zugrundezulegen. Die Listen wiesen auch Daten

auf, die zur Erfüllung dieser Aufgaben nicht erforderlich waren wie „Familienstand" und „Religion". Die insoweit unzulässige Datenübermittlung wurde beanstandet. Inzwischen übermitteln die Gemeinden gekürzte Einwohnerveränderungslisten, die lediglich die erforderlichen Daten enthalten.

Dieser klare und auch verhätnismäßig einfach lösbare Einzelfall rechtfertigt die Aufnahme in den Tätigkeitsbericht durch folgenden besonderen Umstand: Das gewählte Verfahren führt dazu, daß beim Landkreis ein - wenn auch verkürztes - Melderegister aufgebaut und fortgeführt wird. Eine solche Einrichtung widerspricht meiner Ansicht nach grundsätzlich der gesetzlichen Aufgabenverteilung, nach der es lediglich Aufgabe der Meldebehörden, nicht jedoch des Landkreises oder anderer Behörden ist, alle Einwohner nach Identität und Wohnung zu registrieren. Die übermittelten Meldedaten sind beim Empfänger - jedenfalls in diesem Fall - lediglich durch die Bestimmungen der Art. 4, 17 und 18 des Bayer. Datenschutzgesetzes geschützt. Die Daten sind auch nicht etwa über das kommunale Abgabenrecht geschützt: Art. 13 Abs. 1 Nr. 1c des Kommunalabgabengesetzes nimmt den Bereich der Müllabfuhrgebühren vom Schutz des „Steuergeheimnisses" (§ 30 AO) aus. Meines Erachtens sollte auch bei der Schaffung von Gebührensatzungen, die an personenbezogene Daten anknüpfen, die Entstehung eines solchen zweiten verkürzten aber zentralen Melderegisters vermieden werden. Soweit mir bekannt ist, können Müllabfuhrgebühren in der Regel nicht nach der jeweils aktuellen Bewohnerzahl, sondern nach anderen Kriterien bemessen werden.

Angesichts der detaillierten Regelungen zur Übermittlung von Meldedaten an öffentliche und private Stellen im Melderechtsrahmengesetz und im neuen Landesmeldegesetz und der eindeutigen Zuweisung der Aufgabe dieser Datenübermittlungen an die gemeindlichen Meldebehörden bin ich außerdem der Auffassung, daß aus derartigen, für ganz bestimmte andere Zwecke zustande gekommenen verkürzten „Melderegistern" nicht anstelle der gemeindlichen Melderegister und möglicherweise unter Umgehung einschränkender Vorschriften des Melderechts, Daten weitergegeben werden dürften. Den rechtlichen Ansatzpunkt für diese Ansicht sehe ich darin, daß nach Art. 17 Abs. 1 BayDSG eine Datenübermittlung nur zulässig ist, wenn sie selbst, also die Übermittlung und nicht nur die Daten, zur Aufgabenerfüllung des Datenempfängers erforderlich ist. Eine Erforderlichkeit der Übermittlung ist zu verneinen, wenn dieselben Daten bei den gesetzlich hierfür vorgesehenen Meldeämtern registriert sind.

4.6.5 Weitere Fälle der Übermittlung von Meldedaten

- Mehrere Anfragen und Eingaben betrafen im Berichtsjahr den Umfang der Daten, die mit sog. „Fremdenscheinen" von Hotels und anderen Beherbergungsstätten erhoben werden. Insbesondere in Gebieten mit intensiverem Fremdenverkehr wird nach meiner Erfahrung der in einer Durchführungsverordnung zum Meldegesetz verbindlich vorgeschriebene Fremdenschein gerne um Daten erweitert, die zur Förderung des Fremdenverkehrs erhoben werden sollen. Ich habe auch in diesen Fällen deutlich gemacht, daß solche erweiterten Fremdenscheine einen ausdrücklichen Hinweis auf die Freiwilligkeit der zusätzlich erbetenen Angaben enthalten müssen.
- Auf verschiedene Anfragen hin habe ich Fremdenverkehrsgemeinden bei der Formulierung einer Einwilligungserklärung zur Veröffentlichung von Gästedaten in der örtlichen Kurzeitung o.ä. beraten. Unabhängig von der Frage, ob für die Veröffentlichung einer solchen „Gruppenauskunft" über gemeldete Personen ein „öffentliches Interesse" angenommen werden kann, ist zu berücksichtigen, daß sie schutzwürdige Belange der Betroffenen nicht beeinträchtigen darf. Solche Veröffentlichungen könnten zum Schaden der Betroffenen ausgewertet werden, da sich aus ihnen ergibt, wer seine Wohnung z.Zt. - möglicherweise unbeaufsichtigt - nicht benützt.
- Ein Vorfall vor der Landtagswahl im Herbst 1982 gibt mir schließlich Veranlassung, nochmals auf die Datenübermittlung aus dem Melderegister an Parteien einzugehen (siehe auch mein 1. Tätigkeitsbericht Nr. 4.1.6 Seite 13). Nach bisherigem und auch nach künftigem Melderecht (siehe oben zum Entwurf des Landesmeldegesetzes) dürfen Anschriften von Wahlberechtigten an Parteien und Wählergruppen während eines halben Jahres vor der Wahl für Zwecke der Wahlwerbung übermittelt werden. Voraussetzung ist mithin ein Zusammenhang mit Wahlen, die Folge eine Zweckbindung für die Wahlen. An Parteien oder Wählergruppen, die sich an der Wahl nicht beteiligen, dürfen mithin Anschriften von Wahlberechtigten nicht übermittelt werden. Trotzdem hatte vor der Landtagswahl 1982 eine Partei bzw. Wählergruppe, die sich an der Wahl nicht beteiligte, von verschiedenen Gemeinden die Anschriften aller Wahlberechtigten erhalten, was zu beanstanden war. Eine Nachfrage bei der für den Sitz der Wählervereinigung zuständigen Datenschutzaufsichtsbehörde (außerhalb Bayerns) ergab, daß von dort keine Möglichkeit gesehen wurde den Verbleib der Wähleranschriften zu überprüfen, da eine konkrete Beschwerde eines betroffenen Einwohners nicht vorlag. § 30 des Bundesdatenschutzgesetzes gibt in der Tat den Datenschutzaufsichtsbehörden keine Befugnis zu Kontrollen privater Stellen vor Ort, wenn eine solche Beschwerde nicht vorliegt. Inzwischen ergeben sich Anhaltspunkte dafür, daß die in dem genannten Fall übermittelten Wähleranschriften nicht für Wahl-, sondern für andere Zwecke verwendet bzw. an einen anderen Nutzer widerrechtlich weitergegeben wurden. In Zweifelsfällen empfiehlt es sich daher, vor Übermittlung von Meldedaten festzustellen, ob diese wirklich zur Wahl erbeten werden.
- In einem anderen Fall hatte das Meldeamt einer Gemeinde der Jugendorganisation einer Partei die Anschriften von Jugendlichen ab 14 Jahren zum Zwecke der Mitgliederwerbung zur Verfügung gestellt. Eine Einwilligung der Jugendlichen bzw. deren gesetzlichen Vertreter lag nicht vor. Die Gruppenauskunft war als unzulässig zu beanstanden.

4.7 **Steuerverwaltung**

4.7.1 Steuerverwaltung, allgemein

Im Berichtsjahr wurde vom Bundesminister der Finanzen der Referentenentwurf eines Gesetzes zur Novellierung der Abgabenordnung vorgelegt. Der Entwurf enthielt einige Änderungen, die Forderungen der Datenschutzbeauftragten der Länder und des Bundes Rechnung tragen, an anderer Stelle jedoch auch Regelungen, die aus datenschutzrechtlicher Sicht nicht unbedenklich sind. Ich würde es begrüßen, wenn in das Novellierungsgesetz eine Klarstellung über die Kontrollbefugnis der Datenschutzbeauftragten im Bereich der Finanzverwaltung aufgenommen würde.

Bedenken habe ich gegen die vorgesehene Änderung des § 16 Abs. 2 Abgabenordnung (AO), wonach die Finanzbehörden im Verwaltungsverfahren in Steuersachen nicht mehr als Dritte im Sinne der Datenschutzgesetze gelten sollen, wenn Verwaltungstätigkeiten unterschiedlichen Finanzbehörden übertragen worden sind. Das Bayerische Datenschutzgesetz sieht in Art. 17 Abs. 3 Satz 2 bezüglich der Finanzämter bereits eine Ausnahme von dem Grundsatz vor, daß als andere Stelle auch Teile derselben Stelle mit anderen Aufgaben angesehen werden. Mit der Einfügung des neuen § 16 Abs. 2 AO würde die Finanzverwaltung vollends von der Anwendung der Datenüber-

mittlungsvorschriften der Datenschutzgesetze freigestellt. Dies ist für die von der Finanzverwaltung verfolgten Zwecke nicht nötig, da der gewollte, in der Begründung erwähnte Informationsaustausch der Finanzbehörden von den Datenschutzgesetzen nicht behindert wird, nach denen die Datenübermittlung stets zulässig ist, wenn sie zur rechtmäßigen Erfüllung der der übermittelnden Stelle oder dem Empfänger zugewiesenen Aufgaben erforderlich ist.

Die Kontroverse bezüglich der Kontrollbefugnis der Datenschutzbeauftragten gegenüber der Finanzverwaltung besteht seit Beginn des Datenschutzes (s. 2. Tätigkeitsbericht Nr. 4.1.8.3, S. 24). Den Datenschutzbeauftragten der Länder wird zum Teil die Einsicht in Steuerunterlagen unter Hinweis auf das Steuergeheimnis verwehrt, da die Finanzverwaltung die in den Datenschutzgesetzen geregelte Kontrollbefugnis der Datenschutzbeauftragten nicht als ausreichende Rechtsgrundlage i. S. des § 30 Abs. 4 AO sieht. Es ist eine unverständliche und paradoxe Lage, daß dem Datenschutzbeauftragten als gesetzlichem Kontrollorgan das Steuergeheimnis entgegengehalten wird, dessen Einhaltung er gerade zu kontrollieren hat. Da in Gesprächen deutlich geworden ist, daß sich das Argument der Finanzverwaltung in den genannten Fällen darauf beschränkt, das Vorhandensein einer ausreichenden gesetzlichen Grundlage anzuzweifeln, sollte eine Gelegenheit zur Änderung der Abgabenordnung genutzt werden, hier eine Klarstellung vorzunehmen. Ich habe dem Staatsministerium der Finanzen daher die Aufnahme einer entsprechenden Regelung in den Katalog des § 30 Abs. 4 AO vorgeschlagen.

Schließlich habe ich Bedenken, das in § 112 Abs. 6 AO vorgesehene allgemeine Auskunftsrecht der Finanzverwaltung gegenüber anderen Behörden als „Amtshilfe" zu bezeichnen, da dies eine Erweiterung des Begriffs der Amtshilfe bedeuten würde, unter dem bisher stets nur die Hilfe im Einzelfall verstanden wurde. Die Regelung des allgemeinen Auskunftsrechts wäre besser bei § 116 AO anzusiedeln, der als Gegenstück zu § 112 Abs. 6 AO die Pflichten der zur Auskunft angehaltenen Gerichte und Behörden regelt. Beide Vorschriften schaffen zusammen die von den Datenschutzbeauftragten der Länder und des Bundes geforderte Rechtsgrundlage für die Kontrollmitteilungsverfahren der Finanzverwaltung im öffentlichen Bereich. Ich begrüße die dabei im Entwurf vorgesehene ausführliche Regelung der Art und des Umfangs der Anzeigepflichten durch Rechtsverordnung unter Beachtung der Grundsätze der Verhältnismäßigkeit und Erforderlichkeit.

4.7.2 Einzelfälle

- Ein Verein hatte von verschiedenen bayerischen Gemeinden auf seine Bitte hin die Anschriften sämtlicher Hundehalter übermittelt erhalten. Die Herausgabe der Adressen verstieß gegen das Steuergeheimnis, da die Angaben aus den Hundesteuerunterlagen stammten. Nach Art. 13 Abs. 1 Nr. 1cdes Kommunalabgabengesetzes dürfen Hundehalterdaten aus Steuerunterlagen jedoch ausschließlich in Schadensfällen an Behörden und Schadensbeteiligte herausgegeben werden. In allen anderen Fällen gelten uneingeschränkt die Vorschriften über das Steuergeheimnis (§ 30 AO), d.h. daß Angaben aus den Steuerunterlagen nur mit Einwilligung der Betroffenen gemacht werden dürfen. Gegenüber dem Verein habe ich die Ansicht vertreten, daß die unzulässigerweise vermittelten Daten vom Verein zu löschen bzw. zu vernichten sind. Ich habe die für den Verein zuständige Datenschutzaufsichtsbehörde für den nichtöffentlichen Bereich verständigt.
- Eine Stadt hatte mich um Stellungnahme zu der Frage gebeten, ob ein Finanzamt Überzahlungslisten mit Erstattungslisten der Stadtkasse austauschen dürfe. Zu prüfen war, ob hierdurch entgegen dem Steuergeheimnis, § 30 AO i.V.m. Art. 13 Abs. 1 Nr. 1c Bayer. Kommunalabgabengesetz, Angaben offenbart würden. Nach § 30 Abs. 4 Nr. 1 AO ist die Offenbarung zulässig, wenn sie der Buchführung eines Steuerverfahrens dient, d.h. soweit im konkreten **Einzelfall** vollstreckbare Rückstände von Steuern vorhanden sind. Der pauschale Abgleich der gesamten Listen ist hingegen mit dem Steuergeheimnis nicht vereinbar.
- s. a. 4.11.10. Nr. 3, zur Datenübermittlung des Finanzamts an das Studentenwerk

4.8 **Statistik und Planung**

4.8.1 Probeerhebung für die Volkszählung 1983

§ 10 des Volkszählungsgesetzes 1983 erlaubte, zur Vorbereitung der Volkszählung Probeerhebungen durchzuführen, bei denen die Erteilung der Auskunft durch die Betroffenen freiwillig war. Für eine solche Probeerhebung wurden Erhebungsbögen für die Vorerhebung der Gebäude, der Arbeitsstätten sowie der Wohnungen und Haushalte verwendet, in denen die Tatsache, daß eine Pflicht zur Ausfüllung dieser Bogen für den Betroffenen nicht besteht, nur im Kleingedruckten unter „Rechtsgrundlage" vermerkt war. Dies genügte meiner Ansicht nach der Vorschrift des § 10 Abs. 5 des Volkszählungsgesetzes 1983 („die Erteilung der Auskünfte bei den Probeerhebungen ist freiwillig") und dem Rechtsgedanken aus Art. 16 Abs. 2 BayDSG nicht, nach dem bei einer freiwilligen Erhebung hierauf deutlich hinzuweisen ist. Ich bin davon überzeugt, daß ein erheblicher Teil der Betroffenen, wenn er das jeweils fett gedruckte Wort „Rechtsgrundlage" liest, ohne weiteres davon ausgeht, daß eine Pflicht zur Beantwortung der Fragen gegeben ist. Ein flüchtiger Blick auf die in den überprüften Erhebungsbogen folgenden Ausführungen, die einige Gesetzeszitate enthalten, scheint diesen Eindruck zu bestätigen. Nur wenige Betroffene werden daher den kleingedruckten Absatz über die Rechtsgrundlagen zu Ende lesen, und dabei auf die Freiwilligkeit der Erhebung stoßen. Der Hinweis auf die Freiwilligkeit müßte ebenso wie andere Hinweise in demungsbogen durch Fettdruck hervorgehoben werden. In dem überprüften Fall war gleichwohl ein Rechtsverstoß nicht anzunehmen, da die Stadt, die den Bogen verwendete, in einem zusätzlichen Anschreiben auf die Freiwilligkeit so hingewiesen hatte, daß dieser Hinweis im übrigen Text nicht unterging. Meiner Ansicht nach war die Pflicht, auf die Freiwilligkeit einer Erhebung deutlich hinzuweisen, schon aus § 10 Abs. 5 Satz 1 Volkszählungsgesetz 1983 herzuleiten.

4.8.2 Kommunale Statistik und Planung

Um mit einem vertretbaren Aufwand wirksame Datensicherungsmaßnahmen im Bereich der kommunalen Statistik und Planung festzulegen, wurde zwei Statistikämtern großer bayerischer Kommunen vorgeschlagen, alle Aufgaben, in denen personenbezogene Daten verarbeitet werden, nach einem einfachen Schema zu protokollieren. Aus diesen Aufzeichnungen sollte klar erkennbar sein, welche Daten zu welchem Zweck verarbeitet wurden und ob das Ergebnis personenbezogene Daten enthielt oder nicht. Die Auswertung aller über den Zeitraum von einem Jahr protokollierten Projekte, bei denen personenbezogene Daten verarbeitet werden, ergab folgendes Ergebnis:

- Nach Wegfall solcher Aufgaben, die sich mit der Fortschreibung und Datenaufbereitung der gespeicherten Bestände befassen, blieben bei der ersten Stelle 45 und bei der zweiten Stelle 17 Projekte übrig, in denen personenbezogene Daten verarbeitet wurden.
- Als Datenquellen dienten in der Regel Einwohnerdaten, Daten aus der Baufertigstellungsstatistik sowie von freiwilligen Erhebungen und Passantenbefragungen.

- In nahezu allen Aufgaben wurde nur eine Datei ausgewertet. In ganz wenigen Fällen wurden Einwohnerdaten und Daten einer Haushaltsbefragung verknüpft, wobei die Verknüpfung nie auf Satzebene vorgenommen wurde, sondern aggregierte, das sind in der Regel anonymisierte, Daten zusammengeführt wurden.
- Nur in ganz wenigen Fällen war das Ergebnis personenbezogen, wenn man davon ausgeht, daß in bestimmten Einzelfällen Rückschlüsse auf bestimmte Personen möglich sind. Beispiele solcher personenbezogener Ergebnisse sind kartographische Darstellungen auf Blockebene und Auswertungen zur Vorberei tung der Volkszählung 1983.

Ich habe beide Stellen gebeten, die Protokollierung der Auswertung personenbezogener Daten für solche Projekte weiterzuführen, in denen Dateien für planerische und fachbezogene Aufgaben ausgewertet werden. Beide Stellen haben sich außerdem bereit erklärt, die Protokollierung dahingehend zu ergänzen, daß Selektionskriterien und der Zweck der Auswertung für Außenstehende aussagefähig dargestellt werden.

Die Untersuchungen machten deutlich, daß keine grundsätzlichen Bedenken gegen die eingesetzten Auswerteverfahren bestehen und daß Verknüpfungen auf Satzebene, soweit erkennbar, nicht stattgefunden hatten. Für derartige Verknüpfungen fehlen einerseits die Fragestellungen aus den entsprechenden Fachämtern, andererseits auch die programmtechnischen Möglichkeiten.

Im übrigen wird darauf hingewiesen, daß außer bei den beiden besuchten Stellen auch in anderen bayerischen Kommunen am Aufbau ähnlicher Systeme gearbeitet wird. Als Datenquellen werden stets das Melderegister und die Baufertigstellungsstatistik genannt. Die vorgesehenen Nutzungs- und Anwendungsmöglichkeiten beschränken sich zunächst auf reine Stapelverarbeitung.

4.9 **Bauwesen**

4.9.1 Übermittlung von Bauherrendaten

- Die im Jahre 1982 in Kraft getretene neue Vorschrift des Art. 84 der Bayerischen Bauordnung (BayBO) macht gesetzlich nicht vorgesehene Veröffentlichungen oder Übermittlungen von Bauherrendaten (z. B. zu Werbezwecken) davon abhängig, daß der Betroffene dem nicht widersprochen hat. Die neue Vorschrift wurde verschiedentlich fälschlicherweise so interpretiert, daß sie die Bezeichnung von Bauvorhaben in der ortsüblich bekanntzumachenden Tagesordnung von Bauausschuß oder Gemeinderatssitzung ausschließe. Dies trifft jedoch nicht zu.

  Bauanträge sind nach wie vor in der ortsüblich bekanntzumachenden Tagesordnung ausreichend zu bezeichnen (Art. 52 Abs. 1 der Bayerischen Gemeindeordnung - GO). Es kann davon ausgegangen werden, daß hierfür in der Regel erforderlich aber auch genügend ist, den Bauort nach Straße, Hausnummer, in seltenen Fällen auch Flurnummer, die Art des Bauvorhabens (z. B. Zweifamilienhaus, Dachgeschoßausbau) und den Namen des Bauherrn in der Tagesordnung bekannt zu geben. Die Angabe des Bauherrn-Namens wird erforderlich sein, um innerhalb der Gemeinde transparent zu machen, wer (z. B. auch juristische Personen sowohl des öffentlichen als auch des privaten Rechts) unter Umständen durch sein Bauvorhaben die vorhandene Struktur beeinflussen oder Bezugsfälle auslösen könnte, aber auch um festzustellen, ob Bauwerber vom Bauausschuß bzw. Gemeinderat gleich behandelt werden. Die Bekanntmachung dieser Daten aufgrund der Gemeindeordnung beruht auf der gleichen Überlegung und Wertentscheidung, die der grundsätzlichen Verpflichtung, Gemeinderat- bzw. Bauausschußsitzungen öffentlich abzuhalten, zugrunde liegt, nämlich die Transparenz des gemeindlichen Handelns für die Bürger sicherzustellen.

  Unter der Voraussetzung, daß berechtigte Ansprüche einzelner nicht berührt sind, sind Bauanträge auch in öffentlicher Sitzung zu behandeln. Insoweit gilt Art. 52 Abs. 2 GO jedenfalls als Rechtsvorschrift im Sinne von Art. 4 Abs. 1 Nr. 1 BayDSG, die eine Bekanntgabe (Übermittlung) der Bauherrndaten während der öffentlichen Gemeinderats- bzw. Bauausschußsitzung erlaubt.

  Bei den nach Art. 52 Abs. 1 GO zur Bezeichnung des Tagesordnungspunktes bekanntzumachenden Daten fehlt allerdings die derzeitige Anschrift des Bauwerbers. Erhebt er keinen Widerspruch gegen die Bekanntgabe von Daten gem. Art. 84 BayBO, ergibt sich darüber hinaus die Möglichkeit, die dort genannten Daten Dritten auch zu Werbezwecken zu überlassen. Der Gesetzgeber hat in Art. 84 BayBO also eine sehr sorgfältige Abwägung zwischen der notwendigen Transparenz im gemeindlichen Bereich und den Interessen des Bauwerbers vorgenommen. Wer aus Anlaß seines Bauantrags an Angeboten von Firmen interessiert ist, die seine Anschrift nutzen wollen, braucht lediglich deren Weitergabe nicht zu widersprechen. Er nimmt dann in Kauf, daß er in irgendeiner Weise mit seinem Bauvorhaben von Interessenten unter Umständen zentral gespeichert wird und seine Anschrift möglicherweise dem sonstigen Adreßhandel zugänglich wird. Wer es ablehnt, mit seinem Bauvorhaben (unter Umständen zentral) gespeichert zu werden oder in den Adreßhandel zu gelangen, braucht lediglich zu widersprechen.
- Im Zuge der Automatisierung des Baugenehmigungsverfahrens einer Stadt waren die vorgesehenen Übermittlungen von Baufallanzeigen an verschiedene andere öffentliche Stellen zu überprüfen. Gegenstand der Überprüfung war dabei die Erforderlichkeit der Datenübermittlung und der erforderliche Datenumfang je Empfänger. Ohne auf die Frage des jeweils zulässigen Datenumfangs einzugehen, sei als Ergebnis kurz wiedergegeben: Für zulässig erachtet wurde die Weitergabe der Baufallanzeige von der städtischen Bauaufsichtsbehörde
  - an die Stadtkämmerei in dem geprüften Fall gem. Art. 17 Abs. 3 BayDSG zum Vollzug der den Gemeinden nach dem Grundsteuergesetz (§§ 1, 25 ff.) und Art. 21 des Bayer. Kommunalabgabengesetzes zugewiesenen Aufgaben bei der Erhebung der Grundsteuer,
  - an das Finanzamt gem. § 17 Abs. 2 Finanzverwaltungsgesetz i.V.m. § 13 Grundsteuergesetz, §§ 19 und 68 ff. Bewertungsgesetz sowie §§ 179 und 184 AO gem. Art. 17 Abs. 1 BayDSG,
  - an die Stadtwerke AG wegen Stromversorgung gem. Art. 18 Abs. 1 BayDSG als Erfüllung der der Stadt durch Art. 83 Abs. 1 der Bayer. Verfassung zugewiesenen Aufgaben der Stromversorgung,
  - an das Stadtreinigungsamt zur Erfüllung der der Gemeinde durch Art. 57 GO zugewiesenen Aufgaben der Müllabfuhr und nach Art. 17 Abs. 1 und 3 BayDSG,
  - an das Vermessungsamt aufgrund der Aufgabenzuweisung in Art. 5 i.V.m. Art. 12 Abs. 4 des Landesvermessungsgesetzes und gem. Art. 17 Abs. 1 BayDSG.

4.9.2 Auswertung der Kaufpreissammlungen nach dem Bundesbaugesetz (BBauG)

Das Bayer. Staatsministerium des Innern erließ im Berichtsjahr eine Änderungsverordnung zur Verordnung über die Gutachterausschüsse, die Kaufpreissammlungen und die Bodenricht-

werte nach dem Bundesbaugesetz. Die ÄnderungsVO zieht die Konsequenz daraus, daß die Nutzung der in den Kaufpreissammlungen gesammelten Daten bisher uneinheitlich war, wobei in Einzelfällen auch die Kenntnisnahme personenbezogener Angaben durch andere Stellen oder Personen ohne besondere Legitimation praktiziert wurde. Der 7. Teil des BBauG, der die Vorschriften über die Kaufpreissammlungen enthält, sieht eine so extensive Nutzung der Angaben aus privatrechtlichen Grundstückskaufverträgen nicht vor. Er enthält vielmehr, als Äquivalent für die Pflicht zur Ablieferung von Abschriften aller Grundstückskaufverträge, die Pflicht der Gutachter zur Geheimhaltung der Angaben aus den Verträgen. Die Änderungsverordnung enthält nun im wesentlichen ein Recht, für Gerichte, für Behörden, die mit der Wertermittlung von Grundstücken befaßt sind, und für amtlich vereidigte Sachverständige in die Kaufpreissammlung Einsicht zu nehmen, sowie ein Recht, für Zwecke der wissenschaftlichen Forschung Auskünfte aus der Kaufpreissammlung zu erhalten. In anderen Bundesländern sind durch die jeweiligen Verordnungen über die Gutachterausschüsse etc. ähnliche Auswertungsmöglichkeiten vorgesehen worden.

Die Bayer. Änderungsverordnung stützt sich auf § 144 Abs. 2 Nr. 1 BBauG, wonach die „Auswertung der Kaufpreissammlung" durch Landesverordnung geregelt werden kann. Der Landesbeauftragte für den Datenschutz hat in den Erörterungen vor Erlaß der Verordnung festgestellt, daß das Bayer. Staatsministerium des Innern davon ausgeht, daß durch den Vollzug der Änderungsverordnung berechtigte Interessen Dritter nicht beeinträchtigt werden dürfen und tatsächlich auch nicht beeinträchtigt werden. Diese Prämisse ist wichtig, weil § 144 Abs. 2 Nr. 1 BBauG meines Erachtens keine konkrete Ermächtigung, eine Offenbarung personenbezogener Daten der Kaufpreissammlung gegenüber dritten Stellen oder Personen zuzulassen, enthält. Anhaltspunkte für den vom BBauG gewollten zulässigen Umfang der Offenbarung personenbezogener Daten aus den gesammelten Kaufverträgen ergeben sich in diesem 7. Abschnitt des BBauG aber aus den Geheimhaltungspflichten der Gutachter und aus § 136 Abs. 5. In dieser Vorschrift wird die Möglichkeit eröffnet, Kaufpreisgutachten mit den darin enthaltenen Einzeldaten an Dritte weiterzugeben, wenn „die berechtigten Interessen der Betroffenen nicht beeinträchtigt" werden. Diese Regelung ist nach Auffassung des Landesbeauftragen für den Datenschutz auch durch ein u.U. erhebliches Interesse der Betroffenen gerechtfertigt, denn das gekaufte oder verkaufte Grundstück stellt in vielen Fällen den Hauptvermögensgegenstand dar, so daß Angaben im Vertrag weitgehend mit Angaben über die Vermögenslage der Betroffenen identisch sind. Solche Angaben sind der Privatsphäre zuzuordnen. Den Finanzämtern sind für Steuerfestsetzung und -erhebung besondere gesetzliche Befugnisse zur Einblicknahme in Vermögensverhältnisse zugewiesen worden. Dementsprechend haben die Finanzämter gem. § 143 a Abs. 4 BBauG auch das Recht auf Einsicht in die Kaufpreissammlung erhalten.

Gegen die Heranziehung des Gedankens aus § 136 Abs. 5 BBauG (Berücksichtigung berechtigter Interessen Betroffener vor Offenbarung personenbezogener Daten an Dritte) ist eingewendet worden, daß sich diese Regelung nach ihrem Standort im Gesetz im Zusammenhang mit der Weitergabe von Kaufpreisgutachten nicht auf die Weitergabe von Daten der Kaufpreissammlung im Zuge der „Auswertung" beziehe. Dem ist jedoch entgegenzuhalten, daß weder die Verordnungsermächtigung zur „Auswertung" der Kaufpreissammlung in § 144 Abs. 2 Nr. 1 BBauG, noch § 143 a Abs. 2 BBauG, in dem der Begriff „Auswerten" mit einer Tätigkeit der Geschäftsstelle des Gutachterausschusses verbunden wird, erkennbar eine Befugnis zur Auswertung der Kaufpreissammlung durch dritte Stellen oder Personen auch für solche Fälle erteilt, in denen diese Kenntnisnahme Dritter als belastender Eingriff berechtigte Interessen der Betroffenen beeinträchtigt. Es ist daher sicherlich sinnvoll und notwendig, den Anwendungsbereich der Änderungverordnung, wie vorgesehen, auf diejenigen Fälle zu beschränken, in denen eine solche Beeinträchtigung berechtigter Interessen der Betroffenen ausscheidet. Ich habe das Bayer. Staatsministerium des Innern gebeten, dies in der vorgesehenen Verwaltungsvorschrift zur Ausführung der Gutachterausschußverordnung ausdrücklich klarzustellen.

In den Erörterungen vor Erlaß der Änderungsverordnung konnten noch - wofür ich dem Staatsministerium des Innern dankbar bin - folgende Verbesserungen aus der Sicht des Datenschutzes eingefügt werden: Der Begriff der Kaufpreissammlung, in die nach der Änderungsverordnung verschiedenen Stellen und Personen Einsicht zu gewähren ist, wurde dahin eingegrenzt, daß nicht die Kaufverträge die Kaufpreissammlung sind, in die Einsicht zu gewähren ist, sondern daraus im erforderlichen Umfang gewonnene und in der Regel als Kaufpreiskartei geführte Angaben. Dies halte ich für wichtig, da Grundstückskaufverträge oft eine Vielfalt von Rechten, Pflichten und familiären Angelegenheiten wiedergeben, die der Privatsphäre zuzurechnen und für die Preisermittlung nicht erforderlich sind. Das Einsichtsrecht wurde außerdem davon abhängig gemacht, daß für jeden konkreten Einzelfall eine sachliche Notwendigkeit besteht. Außerdem wurde eine Zweckbindung der durch Einsichtnahme erlangten Daten für die Empfänger festgelegt.

Die Neuformulierung soll sicherstellen, daß dem Einsichtnehmenden nur diejenigen Karteiblätter oder Daten zur Einsicht zur Verfügung stehen, die im konkreten Einzelfall für den Zweck der Wertermittlung erforderlich sind, daß ihm also nicht die gesamte Kaufpreiskartei mit all den anderen Daten, die für den Einzelfall nicht erforderlich sind, zur Verfügung gestellt wird. Die Oberste Baubehörde hat ihre Bereitschaft erklärt, hierauf noch in einer Verwaltungsvorschrift hinzuweisen.

Die Notwendigkeit der Speicherung von Namen und Anschriften von Personen in der der Einsichtnahme unterliegenden Kaufpreissammlung konnte bisher noch nicht geklärt werden. Ich bin der Auffassung, daß eine solche Notwendigkeit nicht besteht und daß sich Hindernisse gegen das Weglassen von Namen und Anschriften lediglich aus der bisherigen Übung oder den bisher verwendeten Karteikartenformularen ergeben. Die oberste Baubehörde im Bayer. Staatsministerium des Innern hat sich bereit erklärt, diesen Punkt noch zu überprüfen.

Hinsichtlich der Übermittlung zu Forschungszwecken wurde in der Änderungsverordnung klargestellt, daß vor jeder personenbezogenen Datenübermittlung zu prüfen ist, ob die Übermittlung aggregierter oder anonymisierter Daten dem Forschungszweck genügt. Bei der Klärung der Frage, ob im Einzelfall personenbezogene Daten vorliegen, ist zu berücksichtigen, daß nach Art. 5 Abs. 1 BayDSG Daten nicht nur dann personenbezogen sind, wenn sie eine Person mit Namen und Anschrift bezeichnen, sondern auch, wenn aus den sonstigen Angaben eine natürliche Person bestimmbar ist. Demnach wären Angaben, die Flur-Nummern und Gemarkungen einzelner Grundstücke enthalten, personenbezogen, da über Kataster und Grundbuch Eigentümer, Nutzungsberechtigte und Gläubiger bestimmbar sind. Zur Erfüllung des Sachverhalts „personenbezogen" kommt es nicht darauf an, ob der Datenempfänger die Person aus eigenen Unterlagen ohne Hinzuziehung beispielsweise von Kataster und Grundbuch ermitteln kann.

4.10 **Personalwesen**

- In mehreren Eingaben wurde von Beamten die Sorge geäußert, Krankheits- und Diagnosedaten würden im Zuge des

Beihilfeverfahrens Unbefugten zur Kenntnis gelangen. Die Vorschriften des Bayer. Datenschutzgesetzes sind hier überwiegend nicht direkt anwendbar, da sie in der Regel an die Verarbeitung von Daten in Dateien anknüpfen. Das Beihilfewesen wird vielmehr durch die Beihilfevorschriften und die hierzu vom Bayer. Staatsministerium der Finanzen erlassenen Vollzugsbekanntmachungen geregelt. In der Bekanntmachung vom 6.11.1968 wurde ein Rundschreiben des Bundesministers des Innern veröffentlicht, in dem besonders darauf hingewiesen wird, daß Beihilfeanträge nach Nr. 14 Abs. 2 Satz 4 der Beihilfevorschriften vertraulich zu behandeln sind und keine Bedenken bestehen, die Belege dem Beihilfeantrag in einem verschlossenen Umschlag beizufügen und so der Einsichtnahme durch die Beschäftigungsdienststelle - die nicht gleichzeitig Festsetzungsstelle für die Beihilfe ist - zu entziehen. Die nur für die Weiterleitung von Beihilfeanträgen an die Festsetzungsstelle für Beihilfen zuständige Beschäftigungsdienststelle ist nicht berechtigt, die Weitergabe von Beihilfeanträgen von der offenen Vorlage der Belege abhängig zu machen. Im übrigen sind ärztliche Gutachten, die über die Art einer Erkrankung Aufschluß geben, nach Auswertung in einem verschlossenen Umschlag aufzubewahren, sofern sie bei den Beihilfeakten verbleiben.

Diese Regelung war offenbar weder bei den Betroffenen noch bei den Beschäftigungsdienststellen ausreichend bekannt. In einem Fall wurde ein Bediensteter durch die Beschäftigungsdienststelle sogar darauf hingewiesen, daß der dem Beihilfeantrag beigefügte verschlossene Umschlag von der Beschäftigungsdienststelle auf jeden Fall geöffnet werden müsse, um die Vollständigkeit der Belege zu überprüfen. Bei einer solchen Überprüfung ist kaum zu vermeiden, daß auch von Diagnosen und Behandlungsarten Kenntnis genommen wird. Der Einblick in diese medizinischen Daten stellt einen Eingriff in den durch Art. 2 Abs. 1 in Verbindung mit Art. 1 Abs. 1 Grundgesetz geschützten Persönlichkeitsbereich dar. Seine Zulässigkeit setzt, sofern ein Einverständnis des Betroffenen nicht vorliegt, voraus, daß sie bei einer Abwägung, die alle Umstände des Einzelfalls in Betracht zieht, dem Verhältnismäßigkeitsgrundsatz entspricht (Bundesverfassungsgericht E 32, 373/379 ff zur Beschlagnahme einer ärztlichen Karteikarte). Zweifel an dieser Verhältnismäßigkeit ergeben sich m.E. dann, wenn, wie hier, außer der Beihilfefestsetzungsbehörde noch eine weitere Dienststelle Gelegenheit zur Kenntnisnahme der medizinischen Daten erhält - z.B. um die Vollzähligkeit der Belege zu überprüfen. Dies gilt in besonderem Maße für Belege, die sich auf Krankheiten bzw. Behandlungen von Familienangehörigen des Beamten beziehen. Die Gefahr des unbefugten Eindringens in den grundrechtlich geschützten privaten Bereich wird durch die seit 1. Januar 1983 durch die Neufassung des GOÄ vorgeschriebene ausführlichere Bezeichnung von Krankheit und Behandlungsart verstärkt. Ich bin der Auffassung, daß auf Grund der vom Bundesverfassungsgericht entwickelten Grundsätze zum Schutze von Gesundheitsdaten, die Organisation der Beihilfeabrechnung in allen damit befaßten Behörden zu überprüfen ist. Durch organisatorische Maßnahmen muß dabeisichergestellt werden, daß von den Angaben zur Gesundheit sowohl der Angehörigen des Beamten als auch des Beamten selbst ausschließlich eine auf das notwendigste beschränkte Zahl von Beihilfesachbearbeitern Kenntnis erlangen kann. Soweit den Beihilfesachbearbeitern in der Behörde noch andere Aufgaben übertragen sind, dürfte es sich dabei meines Erachtens zur Vermeidung von Interessenkollisionen nur um solche Aufgaben handeln, für die Angaben aus Beihilfeunterlagen nicht genutzt werden können. Im Rahmen der notwendigen organisatorischen Maßnahmen ist besonders auf eine Trennung der Beihilfeanträge und Unterlagen vom allgemeinen Geschäftseinlauf der Behörde und die unmittelbare Zuleitung zum Sachbearbeiter zu achten. Die ausreichende Sicherung der Beihilfeunterlagen gegen Einsichtnahmen Unbeteiligter werde ich bei Datenschutzkontrollen künftig besonders überprüfen.

- Auf Anfrage einer Behörde hatte ich mich mit der Frage auseinanderzusetzen, ob und in welchem Umfang Mandatsträgern des Gemeinderats oder Kreistags zur Vorbereitung von nichtöffentlichen Sitzungen personenbezogene Daten insbesondere Personalunterlagen oder Auszüge aus ihnen - nach Hause - übersandt werden dürfen. Ich halte eine solche Bekanntgabe von personenbezogenen Angaben an Gemeinderats-/Kreistagsmitglieder nur für vertretbar, wenn der Datenumfang auf das unbedingt erforderliche Maß reduziert wird. Da die Empfänger gemäß Art. 20 Abs. 2 GO, Art. 14 Abs. 2 LandkreisO zur Verschwiegenheit verpflichtet sind, haben sie auch im familiären Bereich dafür zu sorgen, daß unbefugte Dritte keine Kenntnis vom Inhalt der geheimzuhaltenden Unterlagen erlangen. Mit dem Bayer. Staatsministerium des Innern, das ich in der Frage um eine Stellungnahme gebeten hatte, halte ich es jedoch für zweckmäßig und vom Standpunkt des Datenschutzes für geboten, aus dem Kreis der beschließenden Organe ein Mitglied zu benennen, das sich innerhalb der Behörde über den Sachverhalt zu informieren und dem Gremium dann zu berichten hätte (vergl. § 4 Abs. 5 der Mustergeschäftsordnung für Gemeinderäte - MABl 1972 S. 311).

  Auch hier ist von dem Grundsatz auszugehen, daß der Umfang der diesem Beauftragten zur Verfügung gestellten Unterlagen auf das unbedingt erforderliche Maß zu begrenzen ist. Z.B. hielte ich die Einsichtnahme in den gesamten Personalakt oder dessen Übergabe an den Beauftragten im Regelfall für unzulässig. Aktenauszüge mit den für die Entscheidung relevanten Daten würden m.E. genügen. Einsicht in Angaben zum Familienstand, die über verheiratet/nicht verheiratet/hinausgehen, sowie beispielsweise über Kinderzahl und Brutto- bzw. Nettoeinkünfte, erscheint mir jedenfalls so lange bedenklich, als für deren Verwertung bei der konkret anstehenden Personalentscheidung keine angemessene Begründung vorliegt.

  Die Einsichtnahme im Amt in die vollständige Personalakte durch den Beauftragten des Ausschusses kann ausnahmsweise dann in Frage kommen, wenn das Gremium z.B. zwischen mehreren Bewerbern für ein wichtiges Amt oder über die Entfernung eines Bediensteten aus dem Dienst zu entscheiden hätte (vergl. Art. 43 GO, Art. 38 LKrO).

  Grundsätzlich findet das Akteneinsichts- und Informationsrecht der Gremien dann seine Grenzen, wenn besondere Rechtsnormen zur Geheimhaltung verpflichten wie z.B. das Steuergeheimnis, das Sozialgeheimnis oder die ärztliche Schweigepflicht.

- In einer Eingabe war Beschwerde darüber geführt worden, daß ein Dienstherr die Vorlage des Bescheides über die Anerkennung der Schwerbeschädigteneigenschaft verlangte. Der Petent vertrat die Auffassung, daß nicht alle im Bescheid enthaltenen Angaben über seine Behinderungen für die Entscheidung des Dienstherrn über seinen möglichen Arbeitseinsatz erforderlich seien. Es gäbe vielmehr Behinderungen, die zwar bei der Berechnung der Minderung der Erwerbsfähigkeit Beachtung fänden, jedoch keine Auswirkungen auf die konkrete Arbeitsfähigkeit hätten und deren Offenbarung im Personalakt für ihn peinlich sei.

  Ich habe das Bayer. Staatsministerium der Finanzen gebeten zu prüfen, ob eine Beschränkung der in den vorzulegenden könne.

4.11 **Schul- und Hochschulverwaltung**

4.11.1 Gesetz über das Erziehungs- und Unterrichtswesen

Das Gesetz über das Erziehungs- und Unterrichtswesen (BayEUG), das das EUG abgelöst hat, ist inzwischen in Kraft getreten. Dankenswerterweise war es mir möglich gewesen, im Gesetzgebungsverfahren meine Überlegungen vorzutragen, denen zumindest teilweise Rechnung getragen worden ist.

Als wesentliche Datenschutzbestimmung regelt Art. 62 BayEUG die Zulässigkeit der Erhebung und Verarbeitung von Daten durch die Schulen (s.a. unten Nr. 2). Zur Schulgesundheitspflege ist in Art. 57 BayEUG entsprechend meiner Forderung im 4. Tätigkeitsbericht (3.5.1) eindeutig festgelegt, wer für die im Rahmen der Schuluntersuchungen angefallenen Daten der Schüler verantwortlich ist. Eine eindeutige Regelung hatte ich bezüglich der Schulgesundheitspflege gefordert, damit Mißverständnisse vermieden und Verletzungen des Arztgeheimnisses verhindert werden. Dabei war es mir insbesondere darauf angekommen, daß geregelt werde, inwieweit die Gesundheitsämter eventuelle im Rahmen der Schuluntersuchungen erkannte Erkrankungen und Leistungseinschränkungen der Schule mitteilen, sofern diese Tatsachen bei Gestaltung und Durchführung des Unterrichts von den Lehrern berücksichtigt werden müssen.

Darüber hinaus war es mir bedenklich erschienen, wenn eine vorgesehene Bestimmung des EUG zur Folge gehabt hätte, daß bei jedem Schüler, der das 14. Lebensjahr vollendet hat, vor Aufnahme an einer Schule eine Anfrage an das Bundeszentralregister gerichtet oder die Vorlage eines Führungszeugnisses verlangt worden wäre. Hierzu hat das Bayer. Staatsministerium für Unterricht und Kultus schriftlich mitgeteilt, daß die in Art. 23 Abs. 2 Satz 2 BayEUG vorgesehene Möglichkeit, ab Jahrgangsstufe 10 die Aufnahme vorbestrafter Schüler abzulehnen, selbstverständlich nicht bedeutet, daß vor der Aufnahme eines jeden über 14 Jahre alten Schülers eine Anfrage an das Bundeszentralregister zu richten ist. Diese Gesetzesbestimmung solle lediglich im Interesse der übrigen Schüler ermöglichen, in extremen Fällen (z.B. bei Rauschgiftdelikten) entsprechend reagieren zu können. Derartige Verfehlungen würden den Schulen in aller Regel ohnehin bekannt; die Schulen wurden von Justizbehörden über derart schwerwiegende Verfahren unterrichtet. Im Hinblick auf diese eindeutige Äußerung des Bayer. Staatsministerums für Unterricht und Kultus habe ich meine Bedenken gegen die entsprechende Regelung zurückgestellt.

In einem früheren Entwurf zum BayEUG war darüber hinaus eine Regelung vorgesehen, die den bisherigen § 83 der Allgemeinen Schulordnung entsprach. Die darin vorgesehene jeweilige Verständigung des Jugendamtes, wenn dem Erziehungsberechtigten angedroht wird, daß die Lehrerkonferenz mit der Frage der Entlassung des Schülers befaßt werden kann, schien mir zu weitgehend. Das nun verabschiedete BayEUG sieht eine derartige Möglichkeit nicht mehr vor.

Aus der Sicht des Datenschutzes werde ich die Anwendung des BayEUG beobachten und prüfen, inwieweit die neuen Regelungen den Datenschutzbelangen von Lehrern und Schülern gerecht werden.

4.11.2 Datenerhebung an Schulen

Zwar gilt das Bayer. Datenschutzgesetz für alle öffentlichen bayerischen Stellen, also auch für die bayerischen Schulen. Sofern jedoch besondere Vorschriften über den Datenschutz oder die Geheimhaltung bei einzelnen Behörden oder Stellen regeln, gehen diese dem Bayer. Datenschutzgesetz vor. Solche besonderen Rechtsvorschriften sind für den Schulbereich das Bayer. Gesetz über das Erziehungs- und Unterrichtswesen (BayEUG) und die Allgemeine Schulordnung (ASchO). Die Datenverarbeitung an Schulen regelt, wie oben bemerkt, seit 1.1.1983 Art. 62 BayEUG, der den bis dahin geltenden und im wesentlichen wortgleichen § 97 a ASchO ersetzt. Diese Bestimmungen sind auch für die Datenerhebung an Schulen einschlägig.

Ich erhalte immer wieder von Schülern und Eltern Fragebogen zugesandt, die an Schulen Verwendung finden, und werde gebeten, diese auf ihre datenschutzrechtliche Zulässigkeit zu überprüfen. Neben der Frage nach dem zulässigen Umfang der in den Fragebogen gewünschten Antworten wurde auch die Frage nach der Verfassungsmäßigkeit der Allgemeinen Schulordnung im Hinblick auf die Bestimmung des § 97 a ASchO gestellt. Mit dem Inkrafttreten des Gesetzes über das Erziehungs- und Unterrichtswesen dürfte sich letzere Fragestellung erledigt haben. Art. 62 Abs. 1 BayEUG erlaubt die Erhebung der Daten, die die Schulen zu ihrer Aufgabenerfüllung benötigen, und verpflichtet gleichzeitig zur Angabe dieser Daten. Zur Information gebe ich im folgenden den Text des Art. 62 Abs. 1 wieder:

> „Zur Erfüllung der den Schulen durch Rechtsvorschriften jeweils zugewiesenen Aufgaben sind die Erhebung und die Verarbeitung von Daten zulässig. Dazu gehören personenbezogene Daten des Schülers und der Erziehungsberechtigten, insbesondere Adreßdaten, schulische Daten, Leistungsdaten sowie Daten zur Vorbildung und Berufsausbildung. Der Betroffene ist zur Angabe der Daten verpflichtet; er ist bei der Datenerhebung auf diese Rechtsvorschrift hinzuweisen."

Obwohl diese Vorschrift eine umfangreiche und für schulische Zwecke auch völlig ausreichende Datenerhebung gestattet, werden dennoch in der Praxis manchmal unzulässig viele Daten erhoben:

So wurden an einer Volksschule mit einem Fragebogen zur Feststellung der Bedürfnisse und Interessen der Schüler/die Kinder befragt,

- ob ihr Vater aus beruflichen Gründen häufig für längere Zeit von zuhause abwesend sei,
- ob die Kinder tagsüber allein zuhause seien,
- ob sie nach der Schule den Haushalt oder ihre Geschwister versorgen müßten.

Im Zusammenhang mit Ermittlungen zu den Wohnverhältnissen wurde gefragt,

- ob das Kind mit seiner Familie wohne, und zwar im eigenen Haus oder zur Miete,
- wieviel Wohnräume zur Verfügung stünden und
- wieviel Personen in dieser Wohnung untergebracht seien.

Im Zusammenhang mit der Freizeit wurde gefragt,

- ob das Kind einen Freund oder eine Freundin habe, mit denen es fast immer zusammen sei,
- ob es Heftchen lese, wenn ja, sollte angegeben werden welche,
- außerdem wurde nach beliebten Fernsehsendungen und nach den Titeln der gelesenen Bücher gefragt.

Mit diesen und einigen anderen Fragen wurden meines Erachtens weit mehr Daten erhoben, als nach § 97 a Abs. 1 ASchO zulässig ist. Zur Aufgabenerfüllung der Schule, beispielsweise zur Führung des Schülerbogens nach § 24 Abs. 2 ASchO, waren diese Angaben nicht erforderlich. Darüber hinaus konnten durch die Beantwortung der Fragen schutzwürdige Belange sowohl der Schüler als auch der Eltern beeinträchtigt werden. Denn der überwiegende Teil der Fragen war geeignet, nicht unerheblich in die durch Art. 1 und Art. 2 Grundgesetz geschützte Privatsphäre der Schülerfamilien einzudringen. Eine derartige Datenerhebung wäre allenfalls mit Einwilligung der Eltern zulässig gewesen. Im übrigen fehlte auf dem Frage-

bogen auch der nach Art. 16 Abs. 2 BayDSG notwendige Hinweise auf die Freiwilligkeit der Angaben.

Unter Bezug auf Art. 30 BayDSG, der die Pflicht enthält, Verstöße gegen das Datenschutzrecht zu beanstanden, habe ich die Schule aufgefordert, dafür Sorge zu tragen, daß die Schülerbefragung in dieser Form ab sofort unterbleibt und die bisher unzulässigerweise erhobenen Daten entsprechend Art. 20 Abs. 4 BayDSG vernichtet werden.

Das zuständige Staatliche Schulamt habe ich darüber hinaus um Feststellung gebeten, ob derartige Fragebogen außer an der zu beanstandenden Volksschule auch an anderen Schulen im Zuständigkeitsbereich Verwendung finden.

Das zuständige Staatliche Schulamt hat mir mitgeteilt, daß es meine rechtliche Beurteilung der Unzulässigkeit der Datenerhebung und der anschließenden Speicherung teilt. Obzwar keine weiteren Schulen bekannt seien, an denen der genannte Fragebogen Verwendung gefunden habe, hat das Staatliche Schulamt zugesagt, daß Sorge dafür getragen werde, daß derartige unzulässige Datenerhebungen künftig unterbleiben.

Auch die beanstandete Volksschule hat mitgeteilt, daß das ausgefüllte Fragebogenmaterial vernichtet sei und die Lehrer über die Rechtslage unterrichtet seien.

Dieser Fall zeigt recht deutlich, daß unzulässige Datenerhebungen im staatlichen Bereich meist nicht in böser Absicht, sondern wie hier zur Unterstützung pädagogischer Bemühungen durchgeführt werden. Aber auch der gute Zweck muß im Rahmen der geltenden Gesetze verfolgt werden. Die an die Eltern gerichtete Bitte um Einwilligung nach entsprechender Aufklärung über das Ziel der Fragebogenaktion und die kritische Bewertung, ob wirklich alle Fragen für den Zweck des Lehrers erforderlich sind, würden sinnvolle Datenerhebungen gestatten.

4.11.3 Mißbräuchliche Anforderung von Schülerdaten

Durch einen Leserbrief bin ich auf das nachfolgende Problem aufmerksam geworden. Eine bayerische Stadt bemühte sich um die Gründung eines Gymnasiums in ihrem Stadtbereich. Weil ein Schulstandort in dieser Stadt offensichtlich politisch stark umstritten war, hatte sich der Bürgermeister dieser Stadt an Eltern von Schülern gewandt, die die 4. und 5. Klassen der Grund- und Hauptschulen in den Nachbargemeinden dieser Stadt besuchten. Um an die Anschriften der Eltern dieser Schüler zu gelangen, erholte ein Bediensteter dieser Stadt bei Nachbargemeinden die Anschriften der in Frage kommenden Eltern. Bei dieser Datenerhebung verweigerte der Bedienstete der Stadt gegenüber dem Einwohnermeldeamt der Gemeinde, in welcher der Beschwerdeführer lebte, trotz ausdrücklicher Frage die Angabe des Grundes für die Datenerhebung. Da in dieser Gemeinde die Kinder der örtlichen Schule das Hallenbad der besagten Stadt besuchten, vermutete der Bedienstete des Einwohnermeldeamtes des Marktes, daß die Adressen in diesem Zusammenhang benötigt wurden. Der Bedienstete der Stadt, der die Daten abfragte, ließ auf entsprechendes Befragen offen, ob diese Vermutung richtig ist.

Da eine Datenübermittlung zu dem von der Stadt tatsächlich beabsichtigten Zweck, nämlich der Werbung für ein neu zu gründendes Gymnasium, unzulässig gewesen wäre, hätte die Datenübermittlung nicht stattfinden dürfen. Zwar ist der Datenschutzverstoß an sich nicht gravierend, weil nicht überwiegende schutzwürdige Belange der betroffenen Eltern beeinträchtigt worden sind, andererseits zeigt die Tatsache, daß sich ein Bürger an eine Zeitschrift gewandt hat, daß derartige zweckwidrige Datenverwendungen das Unbehagen der Bürger an einer nicht mehr durchschaubaren Datenverarbeitung erhöhen.

Der vorliegende Fall war aus der Sicht der Tätigkeit des Landesbeauftragten für den Datenschutz aber deswegen besonders ärgerlich, weil sich der Schriftwechsel mit der betroffenen Stadt auf einen Zeitraum von nahezu einem Jahr hinzog und die Einlassungen auf meine entsprechenden Anfragen äußerst zurückhaltend waren und je nach meinem Erkenntnisstand wechselten. Damit war die Aufklärung des Sachverhalts, wie bemerkt, erst nach einem Jahr möglich. Der Bürgermeister der betroffenen Stadt ist seiner Pflicht nach Art. 28 Abs. 2 BayDSG, mich in der Erfüllung meiner Aufgaben zu unterstützen, somit nur äußerst zögerlich nachgekommen.

4.11.4 Datenübermittlung an außerschulische Stellen

1. Für die Übermittlung von Daten über Schüler und Erziehungsberechtigte von Schulen an außerschulische Stellen gilt als bereichsspezifische Datenschutzbestimmung § 62 Abs. 2 BayEUG. Nach dieser Bestimmung ist die Weitergabe von Daten und Unterlagen über Schüler und Erziehungsberechtigte an außerschulische Stellen untersagt, falls nicht ein **rechtlicher** Anspruch auf die Herausgabe der Daten nachgewiesen wird. Mit dieser restriktiven Bestimmung soll verhindert werden, daß die Daten von Eltern und Schülern, die wegen der Schulpflicht zwangsläufig in der Schule anfallen und der Disposition der Betroffenen insoweit entzogen sind, einem weiteren Personenkreis bekannt werden. Aus der Sicht des Datenschutzes begrüße ich diese Bestimmung, da Schüler wie Eltern sicher sein können, daß ihre Daten weder an andere Behörden noch an die Privatwirtschaft weitergegeben werden.
2. Dieser erfreulichen Seite des schulischen Datenschutzes steht allerdings der Nachteil entgegen, daß Schülerdaten ohne Einwilligung der Betroffenen auch an solche Einrichtungen nicht übermittelt werden können, die caritative oder sonstige soziale Zwecke verfolgen. Caritative oder sonstige soziale Zwecke begründen für sich allein keinen rechtlichen Anspruch auf die Herausgabe dieser Daten. Dieses Ergebnis mag in manchen Fällen nicht befriedigen.

   Einem Caritasverband, der Schülerdaten haben wollte, um der Gefährdung von Jugendlichen mit frühzeitigen präventiven Maßnahmen zu begegnen, und einem Verein, der leistungsschwachen Schülern Nachhilfeunterricht erteilen wollte und hierzu die schulischen Leistungen der Kinder von der Schule erfahren wollte, habe ich als Lösungsvorschlag mitgeteilt, daß aus datenschutzrechtlicher Sicht keine Bedenken gegen die Verteilung eines entsprechenden Merkblattes in den Schulklassen besteht. Allerdings habe ich anheimgegeben, wegen eventueller, der Verteilung entgegenstehender Bestimmungen, sich unmittelbar an das Bayer. Staatsministerium für Unterricht und Kultus zu wenden, das für diese schulrechtliche Frage zuständig ist.
3. Erziehungsberatungsstellen wollten ebenfalls für ihre Aufgabenerfüllung die Beantwortung einer Reihe von Fragen, die sie in einem Fragebogen untergebracht hatten.

   Die Tätigkeit der Erziehungsberatungsstellen ist auf eine Zusammenarbeit mit den zuständigen Jugendämtern und den zuständigen Einrichtungen der freien und öffentlichen Jugend-, Erziehungs- und Familienhilfe ausgerichtet. Rechtsgrundlagen für die Tätigkeit dieser Stellen sind die §§ 4 und 5 des Jugendwohlfahrtsgesetzes und Art. 16 des Bayer. Jugendamtsgesetzes. Die Erziehungsberatungsstellen können erforderlichenfalls auch mit den Einrichtungen des Schulwesens Verbindung aufnehmen. Nach den Richtlinien zur Förderung von Erziehungs-, Jugend- und Familienberatungsstellen (Amtsblatt des Bayer. Staatsministeriums für Arbeit und Sozialordnung Nr. 19/1979, S. A 185) bedarf die Inanspruchnahme der Schulen durch die Erziehungsberatungsstellen aber ausdrücklich der Zustimmung der ratsuchenden Eltern (Bekanntmachung des Bayer. Staatsmini-

steriums für Arbeit und Sozialordnung vom 14.9.1979 - Nr. - VI 4 - 68/58/3 - 36/79, Rdnr. 3.1). Da mir eine entgegenstehende Regelung nicht bekannt ist, ist demnach die Beantwortung der von den Erziehungsberatungsstellen übersandten Fragebogen durch Schulen oder Schulbehörden nur mit Einverständnis der betroffenen Eltern zulässig.

In der vorstehenden Angelegenheit hatte ich im übrigen auch um Prüfung gebeten, ob alle im Fragebogen der Erziehungsberatungsstelle gestellten Fragen zur Beurteilung der Erziehungsprobleme wirklich erforderlich sind. Bei der Abwägung zwischen dem zulässigerweise zu erfragenden Datenumfang und dem Erhebungszweck ist auch der Grundsatz der Verhältnismäßigkeit zu berücksichtigen.

4. Datenübermittlung von Berufsschulen an die Industrie- und Handelskammer sowie an die Handwerkskammer:

   Die Übermittlung der Daten einzelner Schüler von den Berufsschulen an die Industrie- und Handelskammer sowie an die Handwerkskammer ist meines Erachtens zulässig, sofern diese Daten beispielsweise zur Beurlaubung für überbetriebliche Ausbildungsmaßnahmen erforderlich sind. Sofern allerdings die Daten aller Schüler einer Klasse ohne Ausnahme sowohl an die Industrie- und Handelskammer als auch an die Handwerksammer übermittelt werden, ohne daß etwa nach dem Ausbildungsziel der betroffenen Schüler unterschieden wird, bestehen Bedenken. Die erforderliche Einzelfallprüfung unterbleibt bei einer derartigen Sachbehandlung.

5. Schulsparen
   Unter der Bezeichnung „Weitergabe von Schülerdaten an Kreditinstitute" habe ich bereits in früheren Tätigkeitsberichten die Zulässigkeit der Weitergabe von Anschriften der Schulanfänger oder ihrer Eltern an Kreditinstitute behandelt. Die Rechtslage hat sich zwischenzeitlich nicht geändert: Solche Datenübermittlungen ohne Einwilligung der Eltern sind unzulässig; seit 1.1.1983 gilt Art. 62 Abs. 2 BayEUG. Dies hatte das Bayer. Staatsministerium für Unterricht und Kultus bereits in seiner Bekanntmachung vom 4.7.1978 - KMBl. 1978 S. 431, Textziff. 242 und 344 ausdrücklich bekräftigt.

   Trotz dieser eindeutigen Rechtslage habe ich von einem Elternteil die meines Erachtens zuverlässige Information erhalten, daß eine Volksschule zumindest bisher der ortsansässigen Kreissparkasse üblicherweise Listen über Schulanfänger zur Verfügung gestellt habe. Die betroffene Volksschule hatte demgegenüber behauptet, daß lediglich eine Sparkassenangestellte im Beisein des Schulleiters aus den schulischen Unterlagen die Briefumschläge zur Versendung des Werbematerials beschriftet habe. Da in dem vorliegenden Fall eine endgültige Aufklärung kaum mehr zu erwarten ist, habe ich das Bayer. Staatsministerium für Unterricht und Kultus gebeten, die Schulen im Umkreis der betroffenen Schule auf die Rechtslage bezüglich der Weitergabe von Schülerdaten an Kreditinstitute hinzuweisen.

4.11.5 Hinweise an die öffentlichen Schulen zum Verhalten bei strafrechtlich relevanten Vorkommnissen

Die unrichtige Auslegung von Datenschutzbestimmungen ist meiner Erfahrung nach vielfach darauf zurückzuführen, daß die Beteiligten die im Einzelfall zu beachtenden Vorschriften nicht kennen und aus Unsicherheit entweder zu viele Daten übermitteln oder unter falscher Berufung auf den Datenschutz von einer an sich zulässigen Datenübermittlung absehen.

Unter diesem Gesichtspunkt, daß Rechtsunsicherheit bei Datenübermittlungen und eventuell sich daraus ergebende nachteilige Folgen dem Datenschutz zur Last gelegt werden, begrüße ich es ausdrücklich, daß das Staatsministerium für Unterricht und Kultus in seiner Bekanntmachung vom 19.5.1982 (KMBl. S. 83) Hinweise an die öffentlichen Schulen zum Verhalten bei strafrechtlich relevanten Vorkommnissen und zur Beteiligung des Jugendamtes herausgegeben hat. Darin werden die Lehrer und Schulleiter beispielsweise darauf hingewiesen, daß nach Art. 69 Abs. 2 Bayer. Beamtengesetz der Beamte ohne Genehmigung über Angelegenheiten, über die er Verschwiegenheit zu bewahren hat, weder vor Gericht noch außergerichtlich Aussagen oder Erklärungen abgeben darf. Zur Glaubwürdigkeitsprüfung von Kindern und Jugendlichen als Zeugen in Ermittlungs- und Strafverfahren (vgl. hierzu auch Nr. 4.4.8) wird darauf hingewiesen, daß Schulleiter und Lehrer zur Persönlichkeit eines Schülers als Zeugen vernommen werden können. Insoweit sei die Staatsanwaltschaft nach § 161 StPO auskunftsberechtigt. Die Strafverfolgungsbehörden hätten bei der Anforderung von Auskünften jedoch den Grundsatz der Verhältnismäßigkeit zu beachten. Die Strafverfolgungsbehörden würden gutachtliche Auskünfte über Schüler nur bei Ermittlungen wegen schwerwiegender Straftaten einholen und nur solche Fragen stellen, auf deren Beantwortung es für das Ermittlungsverfahren im wesentlichen ankomme. Bei ernsthaften Zweifeln an der Einhaltung dieser Grundsätze hätten Schulleiter oder Lehrer die Schulaufsichtsbehörde sofort zu verständigen.

Soweit in dieser Bekanntmachung, vor deren Erlaß ich gehört worden bin, meine Anregungen nicht vollständig berücksichtigt worden sind, werde ich den Vollzug dieser Bekanntmachung auf eventuelle Gefährdungen des Persönlichkeitsschutzes beobachten.

4.11.6 Jugendgesundheitspflege

1. Gesundheitsfragebogen

   Anläßlich von Schuluntersuchungen und bei gesundheitlichen Untersuchungen in **Kindergärten** werden amtliche Fragebogen verwendet. Gegen diese Fragebogen sind bei mir mehrere Beschwerden von Eltern eingegangen. Die Beschwerdeführer ziehen in Zweifel, ob alle in den Fragebögen erhobenen Daten zur Erfüllung der gesetzlichen Aufgaben der Gesundheitsämter erforderlich sind.

   Das zuständige Staatsministerium für Arbeit und Sozialordnung hatte schon vor längerem angekündigt, daß im Zuge einer fachlichen und organisatorischen Neuregelung der Schulgesundheitspflege die Gesundheitskarten in naher Zukunft umgestaltet und den Anforderungen sowohl der modernen Jugendmedizin als auch des Datenschutzes angepaßt würden. An diesem Verfahren bin ich beteiligt. Die Abstimmung über die nun vorliegenden Entwürfe eines Elternfragebogens und einer Gesundheitskarte ist noch nicht abgeschlossen. Weil manche Fragen sehr weitreichend sind und sehr stark in die Privatsphäre der Eltern eindringen, beispielsweise die Fragen nach „Risikoschwangerschaften" und „Auffälligkeiten bei der Geburt", verlange ich einen überzeugenden Nachweis dafür, daß die Beantwortung der Fragestellungen für die gesundheitliche Beurteilung der Kinder wesentlich ist.

2. Geheimhaltung der Gesundheitsdaten

   Das Bayer. Staatsministerium für Unterricht und Kultus hat sich auf meine Veranlassung erfolgreich darum bemüht, bei den bayerischen **Schulen** für eine datenschutzgerechte Aufbewahrung der Schülergesundheitskarten zu sorgen. Nunmehr müßte gewährleistet sein, daß medizinische Daten ausschließlich dem mit der Schuluntersuchung beauftragten Personal (Schularzt, Helferin) zugänglich sind, das selbstverständlich der ärztlichen Schweigepflicht gem. § 203 Abs. 1 StGB unterliegt. Nach einer heute noch geltenden Entschließung des Kultusministeriums aus dem Jahre 1949

darf nur der Schularzt Auskünfte über die schulärztlichen Feststellungen und den Inhalt der Schulgesundheitskarte erteilen, und zwar

- an Erziehungsberechtigte ohne Einschränkung,
- an Lehrer nur insoweit, als die Kenntnis für den Unterricht und die Erziehung des Schülers erforderlich ist (beispiels weise die Mitteilung über einen Herzfehler an den Sportlehrer).

Durch Art. 57 BayEUG ist dies nun, wie oben (Nr. 1) bemerkt, gesetzlich verankert. Darüber hinaus habe ich mich bereits vor geraumer Zeit an die Staatsministerien für Unterricht und Kultus sowie für Arbeit und Sozialordnung mit der Aufforderung gewandt, die einzelnen Fragen im Schulgesundheitsbogen auf ihre Erforderlichkeit hin zu überprüfen. Insbesondere gilt dies für folgende Fragen:

- Beruf von Vater, Mutter, Pflegeeltern
- Todesursache der Eltern
- Todesursache der Geschwister
- Krankheiten von Eltern und Geschwistern

Das Staatsministerium für Arbeit und Sozialordung hat mir daraufhin mitgeteilt, daß zwar auch künftig nicht auf gezielte anamnestische Fragen verzichtet werden könne, jedoch im Rahmen der zukünftigen Neuregelung der Schulgesundheitspflege auch fachlich zeitgemäße und datenschutzgerechte Änderungen im Fragebogen geplant seien.

3. Bei der Durchführung von Untersuchungen im Rahmen der Schulgesundheitspflege ist mir folgender Sachverhalt bekannt geworden:

   In einer bayerischen Großstadt werden die anläßlich der Schulgesundheitspflege angefallenen Daten von Schülern beim Gesundheitheitsamt geführt. Wenn nun der Schulzahnarzt im Rahmen der Schulgesundheitspflege eine Schule aufsucht, werden vom Gesundheitsamt die entsprechenden Unterlagen an die Schule versandt. Dort werden sie vom Schulleiter an die einzelnen Lehrer weitergegeben, die sie dann anläßlich der Untersuchung durch den Zahnarzt an die einzelnen Schüler verteilen. Sofern in diesen Gesundheitsbogen bereits aus früheren ärztlichen Untersuchungen Daten eingetragen sind, ist bei dieser Sachbehandlung nicht ausgeschlossen, daß die Lehrer Kenntnis vom Inhalt der Gesundheitsbögen nehmen.

   Nach Art. 57 Abs. 1 Satz 1 BayEUG wird die Schulgesundheitspflege von den Gesundheitsämtern in Zusammenarbeit mit der Schule wahrgenommen. Damit hat die Schule eine gewisse Mitwirkungspflicht. Deshalb ist es statthaft, daß das Gesundheitsamt in den Fällen, in denen ein Zahnarzt ohne weiteres Hilfspersonal die Schule zu Untersuchungszwecken aufsucht, die anläßlich der Schulgesundheitspflege angefallenen Unterlagen an die Schulleitung zur dortigen Verteilung versendet. Auch eine Verteilung der einzelnen Unterlagen durch die Lehrer erscheint im Hinblick auf Art. 57 Abs. 1 Satz 1 BayEUG grundsätzlich unbedenklich.

4. Im Zusammenhang mit der jugendzahnärztlichen Hauptuntersuchung hat sich bei der Datenübermittlung ein weiteres Problem gezeigt:

   An bayerischen Schulen und Kindergärten werden im Rahmen der jugendzahnärztlichen Hauptuntersuchung Vordrucke verwendet, die in entsprechenden Entschließungen des Staatsministeriums des Innern festgelegt sind. Diese Vordrucke werden nach der Untersuchung den Schülern mit nach Haus gegeben. Nachdem die Erziehungsberechtigten und der behandelnde Zahnarzt schriftliche Erklärungen über die etwa erfolgte zahnärztliche Behandlung des Kindes abgegeben haben, werden diese Vordrucke über den Klassenlehrer oder über den Kindergarten an den Jugendzahnarzt zurückgegeben. In dieser Aufforderung, das Behandlungsergebnis nicht auf direktem Wege dem Jugendarzt zuzuleiten, sondern den Weg über die Schule zu wählen, sehe ich die ärztliche Schweigepflicht zumindest berührt.

4.11.7 Verwendung des Wortes „Sonderschule" auf Schülerausweisen

Bereits in meinen letzten beiden Tätigkeitsberichten habe ich darauf hingewiesen, daß an Sonderschulen Schülerausweise ausgegeben werden, die den Inhaber als Schüler einer Sonderschule ausweisen. Meinen diesbezüglichen Bedenken hatte das Bayer. Staatsministerium für Unterricht und Kultus zunächst nicht Rechnung getragen.

Inzwischen hat das Bayer. Staatsministerium für Unterricht und Kultus in seiner Bekanntmachung Bezeichnung der Schulen für Behinderte (Sonderschulen) vom 31.8.1982 (KMBl. S. 422) in Nr. 5.2 zu den Schülerausweisen folgendes bestimmt:

> „Durch die Angabe der ausstellenden Schule und durch den Siegelabdruck wird offenbar, daß der Schüler eine Schule für Behinderte besucht. Dies wird vielfach als nicht erforderlich empfunden. Es wird daher auch eine vereinfachte Form des Schülerausweises zugelassen, in der die gesetzliche Bezeichnung der Schule nicht erscheint. Das Dienstsiegel kann in diesem Fall nicht beigedrückt werden. Es ist erforderlich und genügend, wenn der Standort der Schule so angegeben wird, daß die ausstellende Schule ggf. eindeutig identifiziert werden kann."

Mit dieser Regelung ist eine Verbesserung gegenüber der bisherigen Situation eingetreten, da ein ungesiegelter Ausweis nicht mehr sofort erkennen läßt, daß der Schüler eine Sonderschule besucht. Ich habe allerdings dem Bayer. Staatsministerium für Unterricht und Kultus mitgeteilt, daß ich die jetzt getroffene Regelung aus der Sicht des Persönlichkeitsschutzes noch nicht als ganz überzeugend halte. Die Tatsache, daß der Sonderschüler-Ausweis nicht gesiegelt wird, könnte zumindest für Eingeweihte den Inhaber wieder der Minderheit „Sonderschüler" erkennbar zuordnen, obwohl dies als für die Schülerausweise nicht erforderlich anerkannt worden ist. Meinem Vorschlag, Schulen für Behinderte ein neutrales Siegel, und zwar ohne Hinweis auf die Sonderschule, für die Ausstellung der Schülerausweise zur Verfügung zu stellen, ist vom Bayer. Staatsministerium für Unterricht und Kultus unter Hinweis auf die Verordnung zur Ausführung des Gesetzes über das Wappen des Freistaates Bayern abgelehnt worden.

Ich werde das jetzige Verfahren in seinem praktischen Vollzug prüfen und eine Änderung anstreben, wenn sich tatsächlich noch zu vermeidende Nachteile für die Sonderschüler zeigen sollten.

4.11.8 Datenerfassung an Hochschulen

Nach § 4 Hochschulstatistikgesetz werden bei Studenten zum Zwecke der Durchführung einer Bestands- und Verlaufsstatistik folgende Daten erhoben:

1. Angaben zu Person, Staatsangehörigkeit und Wohnsitzen
2. Art, Zeitpunkt und Ort des Erwerbs für Studienberechtigung, Studienverlauf, angestrebter Studienabschluß, Ausbildung der Eltern und deren Stellung im Beruf

Die zu erhebenden Daten decken sich im wesentlichen mit dem Katalog in § 4 Hochschulstatistikgesetz. Ausnahmen gelten jedoch für die Fragen nach Familienstand, Zahl der eigenen Kinder und Konfession. Bei der Frage nach der Aufnahme in das Studierendenverzeichnis wird das Einverständnis des Studierenden erbeten.

Eine entsprechende Nachfrage bei der TU München nach der Erforderlichkeit der zuletzt genannten Fragen ergab, daß die Aufnahme der Frage nach der Konfession deshalb erfolgt sei, damit der staatliche Zuschuß für die Hochschulseelsorge halbwegs gerecht verteilt werden könne. Auf meine Gegenvorstellungen hin wurde von der TU München zugesagt, daß die Fragen nach Familienstand, Zahl der eignen Kinderfession bei Neudruck des entsprechenden Datenerhebungsformulars nicht mehr aufgenommen würden, weil auch von seiten der TU München eine Erforderlichkeit dieser Daten nicht festgestellt werden könnte. Soweit der jetzige Vordruckbestand noch aufgebraucht werde, würde veranlaßt, daß die insoweit erhobenen Daten nicht mehr ausgewertet würden.

Ähnliche Probleme bei der Datenerhebung wurden auch an einer Fachhochschule festgestellt. Zwischenzeitlich wird dort die Konfessionszugehörigkeit über ein gesondertes Blatt erfragt, wobei auf die Freiwilligkeit und die beabsichtigte Verwendung dieses Datums hingewiesen wird. Die in diesem Fall zunächst vorgetragene Behauptung, die erfaßten Informationen über Familienstand und Anzahl der Kinder würden beim Studentenwerk benötigt, hat sich nachträglich als nicht zutreffend herausgestellt.

Ich werde beim Bayer. Staatsministerium für Unterricht und Kultus auf eine Vereinheitlichung der Datenerhebungsbögen bei allen bayerischen Hoch- und Fachhochschulen dringen.

4.11.9 Weitergabe von Studentendaten an Versicherungen

Seit langem beschweren sich immer wieder Studenten und Examenskandidaten, daß sie von Versicherungsvertretern aufgesucht werden, denen die Tatsache der Ablegung eines Staatsexamens, manchmal auch die Einzelergebnisse und die Wohnanschriften, bekannt seien. Leider ist es bis jetzt noch nicht gelungen, die Stellen ausfindig zu machen, von denen möglicherweise unzulässige Datenübermittlungen an die Versicherungen ausgehen. Obwohl ich mit Nachdruck jeder einzelnen Beschwerde nachgehe, sind bislang alle Spuren im Sande verlaufen. Manchmal konnte auch die Einlassung von Versicherungsvertretern nicht widerlegt werden, daß sie die Namen der Studenten oder der Examenskandidaten über öffentliche Aushänge in den Universitäten in Erfahrung gebracht hätten.

Ein besonders eklatanter Fall einer unzulässigen Datenweitergabe, der auch die Presse beschäftigt hat, hat sich bezüglich der Daten der Studenten einer Universität gezeigt. Auch dort hat ein Versicherungsunternehmen mit Studenten unter einer Anschrift Kontakt aufgenommen, die nur der Universitätsverwaltung bekannt gewesen sein konnte. Ein ehemaliger Mitarbeiter dieses Versicherungsunternehmens hat sich in dieser Angelegenheit an meine Geschäftsstelle mit der Behauptung gewandt, er könne beweisen, daß das Versicherungsunternehmen durch Bestechung Studentendaten von der Universität erhalten habe. Der Informant nannte in diesem Zusammenhang auch die Namen von Mitarbeitern der Universität. Als Beweisstücke legte er manuell angefertigte Karteikarten vor, aus denen neben Namen, Geburtsdatum und Anschrift der Studenten auch Fächerverbindungen sowie eventuelle Prüfungswiederholungen ersichtlich waren.

Neben einer Prüfung im Kultusministerium habe ich auch die Organisation der Verwaltung der betreffenden Universität, insbesondere die Planungs- und Organisationsabteilung, die Studentenkanzlei, das Prüfungsamt und das Universitäts-Rechenzentrum durch Mitarbeiter überprüft.

Als Ergebnis meiner Prüfung mußte ich feststellen, daß trotz bestehender Datensicherungsmängel die konkrete Beteiligung von Mitarbeitern der Universität an einer unzulässigen Datenübermittlung an das Versicherungsunternehmen nicht nachgewiesen werden konnte. Gerade der Datenschutzbeauftragte muß sich hüten, nicht völlig abgesicherte Verdachtsmomente gegen einzelne Mitarbeiter zu äußern. Zudem konnte ich nicht mit letzter Sicherheit ausschließen, daß die Datenweitergabe möglicherweise auch durch Stellen außerhalb des Universitätsbereiches erfolgt sein könnte. Um derartige Vorfälle jedoch für die Zukunft möglichst zu verhindern, habe ich die Universität gebeten, unter Berücksichtigung der Vorschriften der Art. 14 (Datengeheimnis) und Art. 15 (technische und organisatorische Maßnahmen) des Bayer. Datenschutzgesetzes insbesondere die Aufbewahrung, die Weitergabe, die Zugriffsberechtigung und die Vernichtung personenbezogener Unterlagen neu zu regeln.

Obwohl es mir bisher, wie gesagt, noch nicht gelungen ist, festzustellen, von welchen Stellen Daten über Studenten und Examenskandidaten an Versicherungsunternehmen weitergegeben werden, bin ich überzeugt, daß es möglich sein wird, durch weitere Hinweise von betroffenen Studenten die undichten Stellen auszumachen. Allerdings bin ich hierzu auf die Unterstützung der betroffenen Studenten angewiesen.

4.11.10 Datenübermittlungen im Zusammenhang mit dem Bundesausbildungsförderungsgesetz

4.11.10.1 Übermittlung von BAföG-Empfängerdaten an das Kultusministerium

Die zum Vollzug des Bundesausbildungsförderungsgesetzes (BAföG) erlassene Darlehensverordnung sieht in § 8 Abs. 1 vor, daß alljährlich die Namen der Auszubildenden, die Darlehensanträge und die Gesamtsumme der gemeldeten Darlehen an das Bundesverwaltungsamt zu melden seien. Nach Art. 7 des Bayer. Ausführungsgesetzes zum Bundesausbildungsförderungsgesetz ist das Bayer. Staatsministerium für Unterricht und Kultus oberste Landesbehörde für Ausbildungsförderung. Ihm steht die Fachaufsicht zu, da die Aufgabe von Kommunen im übertragenen Wirkungskreis wahrgenommen wird.

Das Bayer. Staatsministerium für Unterricht und Kultus hat nun von der Anstalt für Kommunale Datenverarbeitung in Bayern alljährlich die Namen der Auszubildenden und die Darlehensbeträge erhalten. Auf meine datenschutzrechtlichen Bedenken hin hat das Kultusministerium die Leistungsträger als speichernde Stellen sowie die in Frage kommenden Rechenzentren angewiesen, ab sofort auf den Ausdruck der Namen der Darlehensempfänger zu verzichten. Sollte in Zukunft in Einzelfällen aus Beweisgründen die Namensnennung dennoch erforderlich sein, wird sich das Kultusministerium von Fall zu Fall vorher mit meiner Geschäftsstelle absprechen.

4.11.10.2 Abgleich der Darlehensempfänger

Zwischen einigen Bundesländern findet ein Abgleich der Empfänger von BAföG-Leistungen statt. Zu diesem Zweck werden im Datenträgeraustausch entsprechende Informationen zwischen den einzelnen Ländern gegenseitig übermittelt.

Meine Ermittlungen haben ergeben, daß das Land Bayern an dieser länderübergreifenden Kontrolle der BAföG-Leistungsempfänger nicht teilnimmt.

Das Bayer. Staatsministerium für Unterricht und Kultus hat ausdrücklich darauf verzichtet, daß ihm wie bisher jährlich Listen über die Darlehensmeldungen an das Bundesverwaltungsamt übersandt werden. Es hat gebeten, jeweils nur die Gesamtsumme der gemeldeten Darlehen mitzuteilen.

4.11.10.3 Datenübermittlung des Finanzamtes an das Studentenwerk

Das Amt für Ausbildungsförderung eines Studentenwerkes hat im Rahmen der Prüfung, ob die Voraussetzungen zur Gewährung von Leistungen nach dem Bundesausbildungsförderungs-

gesetz gegeben sind, Auskünfte über die Einkommensverhältnisse der Eltern des Antragstellers unter Bezug auf § 47 BAföG vom zuständigen Finanzamt erbeten.

Das Finanzamt hat über die gewerblichen Einkünfte der Eltern des Antragstellers Auskunft erteilt, obwohl diese im fraglichen Veranlagungszeitraum einen Verlust aus ihrem Gewerbebetrieb erzielt hatten. Das Studentenwerk hatte bei seiner Bitte um Auskunft das Finanzamt ausdrücklich darauf hingewiesen, daß nur **positive** Einkünfte angegeben werden dürfen.

Die Rechtslage stellt sich wie folgt dar:

Die vom Studentenwerk angegebene Rechtsgrundlage für die Auskunftsverpflichtung der Finanzbehörden - § 47 Abs. 2 BAföG - war zwischenzeitlich gestrichen worden. Eine Datenübermittlung durch Finanzämter konnte somit nicht mit dieser Rechtsnorm begründet werden.

Nach § 21 Abs. 4 des 10. Buches zum Sozialgesetzbuch (SGB X) ist das Studentenwerk jedoch berechtigt, im Wege der Amtshilfe vom zuständigen Finanzamt Auskunft über die Einkommensverhältnisse der Eltern eines Antragstellers zu verlangen (§ 1 Nr. 1 SGB I). Somit hatte das Studentenwerk, abgesehen von der Angabe einer ungültigen Rechtsgrundlage, mit dem Auskunftsverlangen keine datenschutzrechtlichen Bestimmungen verletzt.

Jedoch hat das Finanzamt durch Übermittlung von Negativeinkünften im vorliegenden Fall unzulässig Daten übermittelt. Das Bayer. Staatsministerium der Finanzen hat mir mitgeteilt, daß es das betroffene Finanzamt besonders auf die genaue Beachtung der Auskunftsersuchen hingewiesen hat. Das Ministerium geht im übrigen davon aus, daß die Mitteilung eines gewerblichen Verlustes an das Studentenwerk ein einmaliges Versehen darstelle. Gleichwohl haben die Oberfinanzdirektionen München und Nürnberg die Finanzämter ihres Zuständigkeitsbereichs mit einer mir in Kopie vorgelegten Verfügung auf die Rechtslage hingewiesen.

Für die Datenübermittlung des Finanzamtes an das Studentenwerk gelten im übrigen die Bestimmungen des Bayer. Datenschutzgesetzes nicht unmittelbar, weil die Auskunft nicht aus Dateien, sondern aus Steuerakten erfolgt ist. Für sie gelten daher andere Schutzbestimmungen (z.B. § 30 Abgabenordnung).

4.12 **Archivwesen**

4.12.1 Neuer Regelungsbedarf

In Archiven werden große Mengen personenbezogener Daten erfaßt, verwahrt, ausgewertet und insbesondere für wissenschaftliche und rechtliche Zwecke nutzbar gemacht. Auch aus der Sicht des Datenschutzes hat sich wegen dieser Fülle personenbezogenen Materials die Notwendigkeit ergeben, für die archivarische Verarbeitung personenbezogener Daten gesetzliche Regelungen zu schaffen. In meinem 4. Tätigkeitsbericht habe ich zum Regelungsbedarf einige Ausführungen gemacht. Ohne diese im einzelnen zu wiederholen, weise ich auf einige Kernbereiche nochmals kurz hin:

- Nach Art. 20 Abs. 1 BayDSG sind unter den dort genannten Voraussetzungen personenbezogene Daten zu sperren. Art. 20 Abs. 3 u. 4 legt Löschungspflichten fest bzw. eröffnet die Möglichkeit der Löschung personenbezogener Daten. Diese Bestimmungen werden den Anforderungen der Archive nicht gerecht.
- Besondere Geheimhaltungsbestimmungen, wie beispielsweise das Arzt-, Sozial- und Steuergeheimnis, werfen Probleme auf bei der Archivierung der hiervon betroffenen Daten.
- Gerade wenn die Archive Daten übernehmen, die bei Anwendung der Datenschutzgesetze der Verwaltung aufgrund Sperrung oder Löschung entzogen wären, muß die Aufgabe der Archive und deren spätere Zusammenarbeit mit der Verwaltung neu durchdacht und geregelt werden. Grundsätzlich ist hierbei, von konkreten Ausnahmen abgesehen, die Trennung von Verwaltung und Archiv anzustreben.
- Um zu verhindern, daß für die Archive interessantes Material wegen bei der Verwaltung auftretender Platzprobleme gelöscht oder sonst ausgesondert wird, sind die Archive zunehmend bereit, Aktenmaterial zur Zwischenlagerung aufzunehmen, noch bevor über die endgültige Archivwürdigkeit entschieden ist. Für derartiges Aktengut ist eine Sonderbehandlung notwendig.
- Schließlich stellen die neuen Informations- und Kommunikationstechniken die Archive vor bisher unbekannte Probleme. Große Datensammlungen im öffentlichen Bereich sind nicht mehr statisch, sondern können sich von Tag zu Tag verändern. Die geänderten Daten sind, weil durch aktuelle Daten ersetzt, nicht mehr vorhanden. Damit läßt sich rückblickend ein früherer Datenbestand nicht mehr feststellen. Dieser Wandel der Daten und Informationen ist für die Archive später nicht mehr nachvollziehbar. Dabei könnte es sich insbesondere um Datensammlungen handeln, die wegen die Gesellschaft derzeit bewegender Erscheinungen (z.B. Befürchtungen wegen terroristischer Gewalttaten) für die Nachwelt von Interesse sein könnten. Gleiches gilt in bestimmtem Maße auch für die Kommunikation zwischen den einzelnen Behörden, die bislang weitgehend auf Papier stattgefunden hat und deshalb festgehalten ist. Eine Datenkommunikation im Online-Verkehr beispielsweise ist nach dem Löschen der entsprechenden Sicherungsbänder nicht mehr feststellbar.

  Die Konferenz der Datenschutzbeauftragten der Länder und des Bundes hat zur Sicherstellung des Datenschutzes im Archivwesen am 27.4.1982 Empfehlungen beschlossen. Sie sind nachstehend wiedergegeben.

Empfehlungen der Konferenz der Datenschutzbeauftragten der Länder und des Bundes zur Sicherstellung des Datenschutzes im Archivwesen vom 27. April 1982

I. Problemstellung:

In den Archivverwaltungen des Bundes, der Länder und der Kommunen wird die gegenwärtige Rechtslage durch Akten- und Benutzungsordnungen, Bekanntmachungen einzelner Ressorts, Verwaltungsvorschriften und einige wenige gesetzliche Regelungen bestimmt. Die Archive verarbeiten mit dem ihnen überlassenen Archivmaterial eine Fülle personenbezogener Daten. Die Abgabe archivwürdigen Materials an die Archive und die Benutzung des Archivguts können zu Kollisionen mit dem geltenden Datenschutzrecht und mit spezialgesetzlichen Geheimhaltungsbestimmungen führen. Für die Tätigkeit der Archive müssen daher Rechtsgrundlagen geschaffen werden, die eine sachgerechte Archivtätigkeit gestatten und das vom Grundgesetz geschützte Recht auf Achtung der Privatsphäre der Betroffenen berücksichtigen.

Aus der Sicht des Datenschutzes ist es notwendig, für die Verarbeitung personenbezogener Daten in Archiven gesetzliche Regelungen zu schaffen, die sich nicht auf Dateien beschränken, sondern alle personenbezogenen Daten einbeziehen. Die Notwendigkeit einheitlicher gesetzlicher Regelungen wird auch nicht dadurch beseitigt, daß in einzelnen Landesdatenschutzgesetzen sogenannte Archivklauseln (vgl. § 16 Abs. 3 BrDSG und § 13 Abs. 4 LDSG Rheinland-Pfalz) aufgenommen worden sind, da diese nur einen Teil der anstehenden Probleme lösen. Die Notwendigkeit einer gesetzlichen Archivregelung ist im übrigen in § 10 Abs. 5 Satz 2 Melderechtsrahmengesetz (MRRG) und in § 12 ELMG

zusätzlich begründet, da diese Regelungen Datenübermittlungen an das zuständige Archiv vorsehen.

II. Unter datenschutzrechtlichem Gesichtspunkt werden in künftigen Archivgesetzen folgende Rechtsgedanken zu berücksichtigen sein:

1. Datenverarbeitung ist nur im Rahmen der rechtmäßigen Aufgabenerfüllung zulässig. Dieser Grundsatz gilt auch für Archive. Die Aufgaben sind daher exakt zu beschreiben.

2. Durch Gesetz ist klarzustellen, daß auszusondernde und zu löschende Daten dem zuständigen Archiv angeboten und gegebenenfalls von diesem übernommen und insoweit die Löschungsregelungen für den Betroffenen sichtbar durchbrochen werden. Gleichzeitig ist sicherzustellen, daß die abgebende Stelle auf Daten im Archiv im Regelfall nicht zugreifen darf, wenn diese Daten ohne Abgabe an das Archiv ausgesondert oder gelöscht wären. Anderes gilt grundsätzlich, wenn das Archiv Materialien für die abgebende Stelle verwahrt (z.B. Grundbücher).

3. Übernimmt ein Archiv noch nicht auszusondernde Altregistraturen als Zwischenarchiv, so handelt es sich um ein Auftragsverhältnis zwischen Archiv und abgebender Stelle. Letztere trägt weiterhin die datenschutzrechtliche Verantwortung. Bei der Zwischenarchivierung darf das Archiv nur nach Weisung der abgebenden Stelle handeln. Für diese Zwischenarchive empfiehlt sich eine besondere Regelung (vgl. hierzu auch § 12 ELMG).

   Neben der Notwendigkeit einer Regelung für Auftrags- und Endarchivierung bedarf es einer besonderen Normierung für die aus rechtlichen Gründen „dauernd aufzubewahrenden" Archivalien. Diese sind im Gesetz möglichst aufzuzählen (z.B. Grundbuchsachen, Personenstandsachen, Notarsachen etc.)

4. Die grundsätzliche Trennung von Verwaltungs- und Archivtätigkeit setzt eine Definition des Archivmaterials voraus. Die Feststellung der Archivwürdigkeit soll konstitutiv für die dauernde Aufbewahrung in all den Fällen sein, in denen eine dauernde Aufbewahrung nicht bereits aus rechtlichen Gründen vorgeschrieben ist. Die Feststellung der Archivwürdigkeit im Einzelfall soll durch das Archiv getroffen werden.

5. Stehen die Daten unter einem besonderen gesetzlichen Geheimnisschutz, so ist die Befugnis, die Daten an das Archiv zu übermitteln, ausdrücklich zu regeln.

6. Bei der Datenspeicherung in den Archiven sind folgende Grundsätze zu beachten:

   a) Tragende Grundsätze der Verfassung und des allgemeinen Rechts (z.B. Achtung der Privatsphäre und des allgemeinen Persönlichkeitsrechts).

   b) Archivgut darf grundsätzlich keine vollständige Übernahme des gesamten in der Verwaltung entstandenen Schriftgutes enthalten; eine totale Übernahme darf allenfalls in Teilbereichen erfolgen.

   c) Unzulässig bei der Verwaltung gespeicherte Daten dürfen grundsätzlich nicht in Archive aufgenommen werden; sie müssen in den Ausnahmefällen, in denen gerade die Tatsache der unzulässigen Speicherung historisch bedeutsam sein kann, bei Übernahme besonders gekennzeichnet werden.

7. Anders als in der Archivpraxis sind im Sinne des Datenschutzes Betroffene alle Personen, von denen in einer Datei oder Akte personenbezogene Daten enthalten sind. Einschränkungen des Datenschutzes für bestimmte Personengruppen (Amtswalter) bedürfen einer selbständigen Regelung.

8. Zur Wahrung ihrer Persönlichkeitsrechte ist den Betroffenen ein Auskunftsrecht von in Dateien gespeicherten personenbezogenen Daten, ein Akteneinsichtsrecht und ein Recht auf Gegendarstellung einzuräumen. Das Recht auf Gegendarstellung ist in den Fällen einzuräumen, in denen falsche personenbezogene Daten einer Entscheidung zugrunde lagen, ein Berichtigungsanspruch aber aus Gründen der historischen Wahrheit ausscheidet.

9. Im Rahmen der organisatorischen Regelungen ist festzulegen, welches Archiv für welche Stelle zuständig ist. Nach Möglichkeit ist für die Übermittlung personenbezogener Daten aus öffentlichen an private Archive zu Lebzeiten des Betroffenen oder dessen naher Angehöriger die schriftliche Einwilligung zu verlangen.

10. a) Die verschiedenen Nutzungsmöglichkeiten zu wissenschaftlichen Auswertungen - insbesondere die Erstellung von Personenprofilen - sind unter Berücksichtigung der Persönlichkeitsrechte zu regeln. Hierbei sind unter Berücksichtigung der informationstechnologischen Entwicklung die Probleme einer vollständigen Erfassung aller Verwaltungsvorgänge und der Profilbildung aufzugreifen, mit denen besondere Gefährdungen verbunden sind. Hinsichtlich der Benutzung der Archivalien sollte nach Benutzergruppen unterschieden werden, z.B. Wissenschaftler, Journalisten, Verwaltungsbedienstete, Betroffener, Rechtsnachfolger, jedermann.

    b) Durch eine Benutzungsregelung ist grundsätzlich sicherzustellen, daß durch die Benutzung der Archive schutzwürdige Belange der Betroffenen nicht verletzt werden. Dies kann beispielsweise dadurch gewährleistet werden, daß die Nutzung bis zu bestimmten Zeitpunkten ausgeschlossen wird. Dabei ist der Beginn solcher Ausschlußfristen genau festzulegen. Aus Gründen der Rechtssicherheit sollte er an das Entstehendsdatum der Vorgänge oder an deren Abschluß anknüpfen. Fristen für einen freien Zugang zu den Archivalien sind so zu bemessen, daß die Beeinträchtigung von Persönlichkeitsrechten grundsätzlich ausgeschlossen ist. Für zeitgeschichtliche Forschung können diese Fristen unter genau festzulegenden Auflagen unterschritten werden.

    c) Eine wissenschaftliche Nutzung vor Ablauf dieser Fristen kann nur für wissenschaftliche Forschung im Rahmen eines konkreten Forschungsprojekts möglich sein. Besteht Grund zu der Annahme, daß überwiegend schutzwürdige Belange eines Betroffenen verletzt werden, ist die Benutzung ausgeschlossen. Die erforderliche Abwägung, insbesondere bei Personen der Zeitgeschichte, sollte durch das jeweilige Archiv vorgenommen werden.

    d) Die Tatsache, daß eine Behörde das Schriftgut abgegeben hat (für sogenanntes klassisches Archivgut), rechtfertigt nicht dessen Rückübermittlung „zur Erfüllung konkreter Verwaltungsaufgaben" (vgl. II.2.).

11. Die Datensicherheitsbestimmungen in den Datenschutzgesetzen sind entsprechend anzuwenden.

12. Die im Rahmen der informationstechnologischen Entwicklung künftig zunehmende Automatisierung der Daten- bzw. Schriftgutverwaltung wird sich auf die Tätigkeit der Archive auswirken. Daher bedürfen Vorgänge, wie die eines Datenträgeraustausches, Kopierens oder

Abgleichens von Datenbeständen für archivische Zwecke einer besonderen rechtlichen Regelung, die den oben genannten Voraussetzungen entspricht.

4.12.2 Archivgesetzgebung

Derzeit wird an Archivgesetzen gearbeitet. Zwischenzeitlich liegen eine Reihe von Entwürfen vor. So hat das Bayer. Staatsministerium für Unterricht und Kultus den Vorentwurf eines Gesetzes über die Sicherung und Nutzung von Archivgut in Bayern (Stand: April 1983) vorgelegt. Ebenfalls bekannt sind der Entwurf eines Bundesarchivgesetzes in der Fassung vom 31.3.1983 und die Tatsache, daß in den Ländern Bremen und Nordrhein-Westfalen an entsprechenden Gesetzesentwürfen gearbeitet wird.

Die Arbeiten an einem Bayer. Archivgesetz begrüße ich außerordentlich. Bereits der bisher vorliegende Entwurf berücksichtigt eine Reihe meiner Anregungen hinsichtlich der Beachtung des Datenschutzes. In diesem Zusammenhang danke ich dem Bayer. Staatsministerium für Unterricht und Kultus und insbesondere der Generaldirektion der Staatlichen Archive Bayerns, daß sie mich frühzeitig von ihren entsprechenden Überlegungen unterrichtet und mich mehrfach beteiligt haben. Auch für die Zukunft bin ich gerne bereit, an den weiteren Arbeiten zum Archivgesetz mitzuwirken.

Gerade im Zusammenhang mit den Gesetzgebungsarbeiten an einem Archivgesetz darf ich auf ein Urteil des OVG Rheinland-Pfalz vom 27.10.1982 - Gz.: 2 A 47/82 hinweisen. Das Gericht hatte sich mit der Frage nach der Zulässigkeit der Einsicht in historische Unterlagen zu befassen, die sich auf einzelne natürliche Personen beziehen, welche vor noch nicht 30 Jahren verstorben sind. Bei der Auseinandersetzung zwischen dem Grundrecht auf Wissenschaftsfreiheit und dem Persönlichkeitsschutz hat das Gericht folgenden Leitsatz veröffentlicht:

„Das Grundrecht der Wissenschaftsfreiheit gewährt kein Recht auf Einsichtnahme in archiviertes amtliches Schriftgut, das sich auf eine einzelne noch lebende oder vor weniger als 30 Jahren verstorbene Person bezieht, wenn diese der Einsichtnahme nicht zugestimmt hat, und bei der Auswertung der Urkunden ihr privater Lebensbereich nicht unberücksichtigt bleibt."

4.12.3 Archivierung von Steuerdaten

Die Zulässigkeit der Weitergabe von Steuerunterlagen an Archive beurteilt sich grundsätzlich nach § 30 Abgabenordnung (AO), der als bereichsspezifische Geheimhaltungsvorschrift das Bayer. Datenschutzgesetz verdrängt. Weil § 30 AO für die Archivierung von Steuerunterlagen keine besondere Regelung enthält, ist meines Erachtens derzeit die Weitergabe von Steuerunterlagen an ein nicht dem Bereich der Steuerverwaltung zuzurechnendes Archiv mithin nur zulässig, wenn diese Weitergabe keine Offenbarung des Steuergeheimnisses bewirkt. Dies könnte beispielsweise durch Anonymisierung der personenbezogenen Angaben in den Steuerakten erfolgen, im übrigen aber auch dadurch, daß die Weitergabe der Steuerunterlagen nur zum Zwecke der Verwahrung beim Archiv unter gleichzeitigem Ausschluß der Möglichkeit der archivischen Auswertung; ein unbefriedigendes Ergebnis. Bei der derzeitigen Rechtslage halte ich daher bei einer Weitergabe von Steuerunterlagen an Archive folgende Maßnahmen für erforderlich:

- Klare Trennung zwischen den zur Verwahrung abgegebenen Steuerunterlagen und den sonstigen beim Archiv vorhandenen archivwürdigen Unterlagen.
- Eine Zugangsregelung, die den Zugang des Amtspersonals des Archivs auf den zur Erfüllung des Verwahrungsauftrags erforderlichen technisch-organisatorischen Umgang mit den Steuerunterlagen beschränkt und im übrigen den Zugang mit dem Ziele der Einsichtnahme nur Angehörigen der Steuerverwaltung in den in § 30 Abs. 4 AO genannten Fällen gestattet.

Eine den Bedürfnissen der Steuerverwaltung und den Archiven gleichermaßen gerecht werdende und die schutzwürdigen Belange der Betroffenen berücksichtigende Regelung sollte durch eine Novellierung des § 30 AO gefunden werden. Im Entwurf eines Bundesarchivgesetzes (Stand: 31. März 1983) ist eine entsprechende Regelung vorgesehen.

4.12.4 Abgabe von Sozialdaten an das Archiv

Im Berichtszeitraum ist die Frage nach der Zulässigkeit der Abgabe von Sozialhilfeakten an ein kommunales Archiv an mich herangetragen worden. Hierzu ist folgendes zu bemerken:

Eine Abgabe von Sozialhilfeakten an ein kommunales Archiv ist eine Offenbarung von Angaben über persönliche und sachliche Verhältnisse von Sozialhilfeempfängern. Eine solche Offenbarung ist nach § 35 Abs. 2 SGB I „nur unter den Voraussetzungen der §§ 67 - 77 des 10. Buches" SGB zulässig. Nach keiner dieser Bestimmungen ist eine Offenbarung von Sozialdaten zu Archivzwecken erlaubt. Inwieweit der Gesetzgeber diese Fragestellung übersehen oder absichtlich nicht geregelt hat, kann ich nicht beurteilen. Jedenfalls hat diese Rechtslage zur Folge, daß Sozialhilfeakten, die lebende Personen betreffen, einem kommunalen Archiv nur dann überlassen werden dürfen, wenn entweder die Betroffenen in die Aktenweitergabe eingewilligt haben, oder die Sozialhilfeakten durch Löschung der identifizierenden Angaben so aufbereitet sind, daß der einzelne Betroffene nicht mehr bestimmbar ist. Sofern der Sozialhilfeempfänger oder die sonstigen Betroffenen verstorben sind, steht Art. 35 SGB I einer Datenübermittlung an das Staatsarchiv meines Erachtens nicht entgegen. Obwohl eine ausdrückliche Regelung im Sozialgesetzbuch zu den Daten Verstorbener fehlt, kann wohl davon ausgegangen werden, daß der Schutz der Sozialdaten entsprechend dem der Datenschutzgesetze mit dem Tod des Betroffenen endet.

Aufgrund dieser Überlegungen rege ich daher an, Sozialhilfeakten an ein kommunales Archiv nur dann abzugeben, wenn die Betroffenen verstorben sind oder ihr Ableben mit hoher Wahrscheinlichkeit anzunehmen ist; z.B. nach theoretischer Vollendung des 100. Lebensjahres. Zum Schutze der Persönlichkeitssphäre etwa noch lebender Verwandter sollte zusätzlich für die Benutzung dieser Daten im Archiv eine Sperrfrist von etwa 30 Jahren eingehalten werden. Die bisherige Verfahrensweise der Landesversicherungsanstalten könnte insoweit entsprechend herangezogen werden.

Allerdings enthalten Akten von Sozialleistungsträgern fast immer auch medizinische Daten. Damit entsteht ein weiteres Problem. Nach § 76 Abs. 1 SGB X ist der Sozialleistungsträger gehalten, medizinische Daten nur unter den Voraussetzungen zu offenbaren, unter denen die in § 203 Abs. 1 und 3 StGB (ärztliche Schweigepflicht) genannten Personen selbst zur Offenbarung befugt wären. Nach § 203 Abs. 4 StGB ist die unbefugte Offenbarung fremder Geheimnisse auch nach dem Tode des Betroffenen strafbar. Die Befugnis zur Offenbarung wird in diesen Fällen daher nur vorliegen, wenn eine ausdrückliche Zustimmung des Betroffenen - etwa ausgesprochen noch vor seinem Tode - oder seine mutmaßliche Einwilligung vorliegt oder aufgrund besonderer Gesetze oder eines Notstandes die Offenbarung erlaubt ist. Derzeit besteht meiner Kenntnis nach eine ausdrückliche gesetzliche Befugnis nicht. Eine solche Befugnis könnte eventuell durch ein künftiges Archivgesetz geschaffen werden. Inwieweit die mutmaßliche Einwilligung des Betroffenen angenommen werden kann, erscheint zweifelhaft. Jedenfalls kann nicht das generelle Vorliegen einer mut-

maßlichen Einwilligung unterstellt werden, um somit die vollständigen Abgaben der Akten an ein Archiv zu rechtfertigen, wenn diese Akten medizinische Daten enthalten.

Die Ausnahmeregelung des § 76 Abs. 2 SGB X über die Weitergabe von Gutachten und Bescheinigungen wegen der Erbringung von Sozialleistungen kann eine Abgabe dieser Unterlagen an ein Archiv nicht rechtfertigen, weil eine derartige Weitergabe nicht dem Vollzug einer gesetzlichen Aufgabe im Sinne des § 69 Abs. 1 Nr. 1 SGB X dienen würde.

Im derzeit vorliegenden Entwurf eines Bundesarchivgesetzes sind entsprechende Regelungen für eine Änderung des Sozialgesetzbuches aufgenommen worden, die die Probleme der Archivierung von Sozialdaten lösen sollen. Weil, wie sich aus dem vorstehenden bereits ergibt, im Sozialleistungsbereich derzeit bei der Behandlung von Archivmaterial eine weitgehende Rechtsunsicherheit besteht und im Einzelfall wohl sehr unterschiedlich verfahren wird, begrüße ich die Absicht, diesen Bereich spezialgesetzlich zu regeln.

4.13 **Forschung**

4.13.1 Allgemeines

Datenschutz und Forschung können in einem Spannungsverhältnis zueinander stehen. Hierauf hatte ich bereits in meinem 4. Tätigkeitsbericht (Nr. 3.6.1) hingewiesen. Im Berichtszeitraum konnte ich feststellen, daß sich in der Diskussion in diesem Bereich eine Versachlichung eingestellt hat. Auf seiten der Forscher wurde erkannt, daß manche Probleme, beispielsweise betreffend die Zulässigkeit einer Weitergabe von medizinischen oder sozialen Daten an Forschungseinrichtungen, nicht grundsätzlich durch das Datenschutzrecht neu aufgeworfen worden sind, sondern durch längst vorhandene Regelungen wie zur ärztlichen Schweigepflicht oder zum Sozialgeheimnis bestehen. Die Datenschutzbeauftragten konnten wohl auch deutlich machen, daß sie von Gesetzes wegen gefordert sind, die Belange des Datenschutzes nachhaltig zu vertreten und nicht aus Böswilligkeit der Forschung Daten vorenthalten wollen. Ich bin daher nach wie vor überzeugt, daß bei gemeinsamer Erörterung der Thematik Datenschutz und Forschung praxisgerechte Lösungen gefunden werden können, wenngleich im Einzelfall eine gewisse Behinderung der Forschung nicht immer vollständig ausgeschlossen werden kann.

4.13.2 Grundsätzliche Forderungen an Forschungseinrichtungen

Soweit für Forschungszwecke von Bürgern Daten erfragt werden, sind bei Forschungen mit anonymisierten Daten folgende Grundsätze zu bedenken:

- Anonyme Befragungen sollen so durchgeführt werden, daß keinerlei Hinweise auf den Befragten, auch nicht auf den Verband oder die Gruppe (z.B. Schulklasse), der der Befragte angehört, miterhoben werden, es sei denn, diese Tatsache ist ausnahmsweise von besonderer Bedeutung für Forschungsprojekte.
- Die Antworten auf einem anonymisierten Fragebogen dürfen nicht Bezugspersonen zu den Interviewten zur Kenntnis gegeben werden, die auf Grund ihres Zusatzwissens Rückschlüsse auf eine konkrete Person ziehen können. Dies gilt beispielsweise im Schulbereich für Lehrer oder Elternbeiratsmitglieder.
- Die ausgefüllten Datenerhebungsbogen und evtl. daraus erstellte Datenerfassungsbelege sind nach der Auswertung so schnell wie möglich zu vernichten.
- Maschinenlesbare Einzeldatensätze, die aus den einzelnen Fragebogen aufgenommen worden sind, sind schnellstmöglich zu anonymisieren oder, soweit es die Auswertung zuläßt zu aggregieren und im letzteren Falle die Einzeldatensätze anschließend sofort zu löschen. Dabei ist Sorge dafür zu tragen, daß nicht auf etwaigen Sicherungsbändern die Einzeldatensätze erhalten bleiben.
- Forschungsprojekte beruhen im Regelfall auf freiwilliger Teilnahme. Erfolgen sie in Form von Interviews, so ist auf die Freiwilligkeit der Teilnahme an der Befragung ausdrücklich vor Durchführung des Interviews hinzuweisen. Sollen dagegen von den Betroffenen selbst Fragebogen ausgefüllt werden, so ist der Hinweis auf die Freiwilligkeit der Datenangabe an hervorgehobener Stelle auf dem Fragebogen anzubringen; dies entspricht Art. 16 Abs. 2 BayDSG. Um die Entscheidung für die Teilnahme an einer Befragung wirklich freiwillig vornehmen zu können, sind insbesondere bei Jugendlichen Inhalt und Zweck der Befragung, deren Auswertung sowie deren weitere Verwendung eindeutig mitzuteilen, damit die Befragten die Auswirkung ihrer Teilnahme an der Befragung überblicken können. Die Betroffenen müssen die Gelegenheit haben, ihre Entscheidung frei zu treffen. Das aber setzt die Einsichtsfähigkeit der Befragten über die Tragweite ihrer Antworten voraus, was ich grundsätzliche erst bei Jugendlichen ab vollendetem 16. Lebensjahr unterstelle.

  Sollte für die Erhebung aller oder bestimmter Daten eine Rechtsgrundlage vorliegen, so ist auch diese im Erhebungsbogen anzugeben; insoweit ist auch auf Nummer 16.4 ff VollzBekBayDSG hinzuweisen. Gerade im letzteren Falle sind im Rahmen der Datenerhebung die Erforderlichkeit der einzelnen zu erfragenden Daten und deren Verhältnismäßigkeit zur Aufgabenerfüllung zu prüfen. Des weiteren muß bei der Forschungseinrichtung sichergestellt sein, daß die erhobenen Daten tatsächlich nur zum angegebenen Zweck verwendet werden. Datenübermittlungen an Dritte werden im Regelfall unzulässig sein.
- Zusammenstellungen über das Ergebnis einer Befragung dürfen keine Angaben enthalten, die auf bestimmte befragte Personen hinweisen oder entsprechende Rückschlüsse erlauben. Dies ist insbesondere dann eingehend zu prüfen, wenn im Kreis der Befragten Personen sind, die von Durchschnittswerten besonders stark abweichen und deshalb Anhaltspunkte einen Rückschluß auf diese Personen gestatten.
- Sollte im Einzelfall notwendig sein, daß die Forschungseinrichtung wegen ergänzender Fragen auf den Einzelnen zurückkommen kann, so sollte zur Verbindung zu dem Befragten moglichst nicht dessen Name gespeichert, sondern evtl. eine Kontrollnummer verwendet werden. Diese kann beispielsweise bei Schülern bei der Schule festgehalten sein, so daß bei der Forschungseinrichtung trotz dieser Rückfragemöglichkeit gleichwohl die Anonymität des Einzelnen gewahrt bleibt.

4.13.3 Jugendliche Forscher

Von der Körber-Stiftung, die einen Schülerwettbewerb „Die Kriegsjahre bis Zusammenbruch" veranstaltet hat, bin ich um Unterstützung gebeten worden, damit die „jugendlichen Forscher", die sich auch mit dem Schicksal der Juden auseinandersetzen sollten, die nötigen Daten erhalten.

Gerade wegen der möglichen Sensibilität der hierbei notwendigen Daten, die im übrigen teilweise unter besondere Geheimhaltungsbestimmungen (§ 61 Personenstandsgesetz, § 30 Abgabenordnung, § 35 Sozialgesetzbuch) fallen dürften, habe ich darauf hingewiesen, daß selbst die Verwertung zulässigerweise erhaltener personenbezogener Daten keine Beeinträchtigung schutzwürdiger Belange der Betroffenen oder auch eventueller Hinterbliebener nach sich ziehen darf. Ich habe deshalb

bei der Körber-Stiftung angeregt, den „jugendlichen Forschern" folgende Datenschutzhinweise zu erteilen:

Die interviewten Personen müssen auf die Freiwilligkeit ihrer Teilnahme an der Befragung unter Angabe über Inhalt und Zweck der Befragung hingewiesen werden.

Namen und Anschriften von Personen, die eine Teilnahme an der Befragung verweigern, sind unverzüglich zu vernichten.

Die erlangten Daten dürfen nur zu dem angegebenen Forschungszweck verwendet und nicht weitergegeben werden. Sie sind nach Abschluß der Befragungsaktion bzw. der Forschungsarbeit zu vernichten.

Eine möglichst frühzeitige Anonymisierung der erhobenen Daten bietet Gewähr gegen die Kenntnisnahme durch Unbefugte.

Zusammenstellungen über das Ergebnis einer Befragungsaktion oder Forschungsarbeit dürfen keine Angaben enthalten, die auf bestimmte Personen hinweisen.

4.14 **Datenschutzprüfung bei Landratsämtern, Städten und Gemeinden**

Im Berichtsjahr wurde die Datenschutzprüfung bei Landratsämtern, Städten und Gemeinden fortgesetzt. (Siehe auch 4. TB Nr. 3.1.9, Seite 17 f.). Wie im Vorjahr wurden die verwendeten Erhebungsvordrucke, die Führung von manuellen Dateien bzw. Karteien und Datenübermittlungen daraus und die Verpflichtung auf das Datengeheimnis gemäß Art. 14 BayDSG geprüft. Die über den Einzelfall hinaus interessierenden Fragen ähneln weitgehend den im Vorjahr festgestellten. Insofern sei auf den 4. Tätigkeitsbericht verwiesen. Darüber hinaus wurde im Berichtsjahr festgestellt:

- Bei einer freiwilligen Umfrage zur Erstellung eines Mietspiegels war entgegen Art. 16 Abs. 2 BayDSG kein deutlicher Hinweis für die Befragten auf die Freiwilligkeit ihrer Angabe vorgesehen.
- Ein „Fragebogen zur Ermittlung des Anspruchs auf Pflegezulage bzw. des Pflegefreibetrages zur Kriegsschadensrente nach dem LAG" enthielt die Frage nach Name und Anschrift des behandelnden Arztes - für Rückfragen über den Gesundheitszustand des Antragstellers. Dies war zu beanstanden, da die Offenbarung von Patientendaten dem Arzt durch § 203 Abs. 1 StGB untersagt ist, wenn nicht eine konkrete, auf den Einzelfall abgestellte ausdrückliche Entbindung von der ärztlichen Schweigepflicht vorliegt. Eine solche Entbindung kann allein in der Bekanntgabe des Arztes nicht gesehen werden.
- Zur Veröffentlichung von Bauherrendaten in der örtlichen Presse wurden unterschiedliche Verfahrensweisen festgestellt. Art. 84 der Bayer. Bauordnung in der Fassung der Bekanntmachung vom 2. Juli 1982 (GVBl. Seite 419) hat diese Frage nun gesetzlich geregelt. (Wegen Einzelheiten siehe unter Nr. 4.9.1 in diesem Tätigkeitsbericht).
- Bei einer Kontrolle wurden in dem Raum, in dem die EDV-Anlage eines Landratsamts untergebracht ist, Standesamtsunterlagen vorgefunden. Ich habe auf die Notwendigkeit der feuer- und einbruchsicheren Unterbringung gemäß § 31 Abs. 1 und 38 Satz 2 der Dienstanweisung für die Standesbeamten (DA) hingewiesen.
- In einem Personalamt wurden Bewerbungsunterlagen, mit Ausnahme der Zeugnisse, auch in den Fällen aufbewahrt, in denen kein Dienst- oder Anstellungsverhältnis zustande gekommen war. Die Lebensläufe erlauben, sich ein Bild von Personen zu machen, mit denen jedoch keine Bindung zu einer Behörde zustande kam. Unbeschadet der Tatsache, daß diese Aktenunterlagen nicht von den materiellen Vorschriften des Bayerischen Datenschutzgesetzes erfaßt werden, habe ich empfohlen in entsprechender Anwendung der Rechtsgedanken des Bayer. Datenschutzgesetzes (Art. 20 Abs. 3 und 4 BayDSG) in diesen Fällen, insbesondere den Lebenslauf und evtl. ausgefüllte Personalfragebögen aber auch sonstige Unterlagen an die ehemaligen Bewerber zurückzugeben oder zu vernichten, sofern nicht eine Aufbewahrung für spätere Stellenbesetzung mit den Betroffenen vereinbart war.
- Bei Kontrollen wurden außerdem verschiedene Arten von Personalfragebögen festgestellt. Da gegen einige der darin enthaltenen Fragen aus der Sicht des Datenschutzes Bedenken bestehen, ist beabsichtigt, diese Datenerhebung generell mit dem Bayer. Staatsministerium der Finanzen und dem Bayer. Staatsministerium des Innern zu erörtern.
- Die Kontrollen zeigten Unsicherheit in der Abgrenzung zwischen Dateien, die lediglich internen Zwecken dienen und daher den materiellen Anforderungen des BayDSG gemäß Art. 1 Abs. 2 Satz 2 BayDSG nicht unterliegen, und den nicht internen Dateien. Interne Dateien dienen grundsätzlich nicht der Information anderer Behörden oder Dienststellen. Bei der Zuordnung muß berücksichtigt werden, daß in den meisten Karteien wenn auch nicht alle, so doch einzelne Daten auch zur Übermittlung an Dritte bestimmt sind, so daß die Datei nicht ausschließlich internen Zwecken dient. Dies gilt beispielsweise für die Waffenkartei (Datenübermittlung an die Polizei), für die Kartei der überwachungspflichtigen Betriebe der Lebensmittelkontrolle (Datenübermittlung an Amtsarzt, Amtstierarzt und u.U. an die Staatsanwaltschaft). Zu berücksichtigen ist, daß als „Übermittlung an Dritte" gemäß Art. 17 Abs. 3 Satz 2 BayDSG auch die Weitergabe von Daten an Teile der öffentlichen Stelle mit anderen Aufgaben oder anderem räumlichen Bereich gilt, d.h., daß die Zulässigkeit einer Datenweitergabe auch in diesen Fällen zu prüfen ist, wobei Art. 17 Abs. 1 BayDSG einer zur Aufgabenerfüllung erforderlichen Weitergabe in der Regel kein Hindernis bereitet. Interne Dateien z.B. sind meiner Erfahrung nach in der Minderzahl. Es empfiehlt sich daher, sämtliche Dateien in eine innerbehördliche Dateien-Inventur einzubeziehen, um anschließend alle nicht rein internen Dateien der Erforderlichkeitsprüfung hinsichtlich der gespeicherten Angaben zu unterziehen (vergl. Nr. 16.3 VollzBekBayDSG).
- In einer Gemeinde wurde aus der Grundsteuerdatei ein Verzeichnis der Hauseigentümer erstellt und an jedermann ausgegeben. Dies verstieß gegen das Steuergeheimnis (§ 30 AO). Zu den mit kommunalen Grundstückskarteien verbundenen Fragen siehe auch 4. Tätigkeitsbericht Nr. 3.1.8 Seite 17.
- Schwierigkeiten bereitet in der Praxis die Frage der Übermittlung von sog. Grunddaten wie Namen, betriebliche Anschrift und angemeldete Tätigkeit Gewerbetreibender aus dem Gewerberegister an Adressbuchverlage. Als Voraussetzung der Übermittlung ist gegenwärtig die ausdrückliche Zustimmung des Gewerbetreibenden anzusehen. Diese liegt aber nur bei einem verhältnismäßig geringen Prozentsatz der Gewerbeanmeldungen vor. Alle Gewerbebetriebe, die vor dem 2.1.1980, dem Zeitpunkt der Einführung des Einwilligungserfordernisses, bereits im Gewerberegister gespeichert waren, deren Inhaber also nicht bei der Anmeldung die Möglichkeit zur Entscheidung hatten, ob Daten an Adressbuchverlage übermittelt werden dürfen, müssen bei einer Datenübermittlung an Adressbuchverlage ausgeklammert werden. Wegen des damit verbundenen Verwaltungsaufwands wird eine nachträgliche Einholung dieser Einwilligung i.d.R. nicht in Betracht gezogen. Zur pragmatischen Lösung der Frage wird in einem mir bekanntgewordenen Fall in der örtlichen Presse ein Aufruf an alle Gewerbetreibenden veröffentlicht,

der Stadt oder dem Verlag eine Mitteilung zukommen zu lassen, wenn eine Aufnahme in das Adressbuch als Gewerbebetrieb gewünscht wird.

Seit 1.4.1983 ist durch Art. 35 Abs. 3 des Bayer. Meldegesetzes insofern eine neue Situation eingetreten, als dort gesetzlich festgelegt wird, daß bestimmte Grunddaten über jeden Einwohner an Adressbuchverlage übermittelt werden dürfen - wenn der Betroffene dem nicht widersprochen hat. Der Gesetzgeber sieht also für den Fall des Melderegisters nicht die Einwilligung, sondern ein Widerspruchsrecht vor. Die Veröffentlichung von Grunddaten aus dem Gewerberegister enthält zwar im Vergleich zu den Grunddaten, die aus dem Melderegister an Adreßbuchverlage übermittelt werden dürfen, noch die Angabe, daß der Betreffende ein bestimmtes Gewerbe betreibt. Andererseits sind Gewerbebetriebe in unserer Wirtschaftsordnung im Regelfall auf Herstellung von Kontakten zu Dritten ausgerichtet und an einer besonderen Geheimhaltung des Gewerbes nicht interessiert. Es liegt deshalb nahe, aus Anlaß der neuen Regelung im Melderecht, die bisherige Regelung zum Gewerberegister zu überdenken und zu prüfen, ob sie gegebenenfalls der melderechtlichen Regelung anzugleichen wäre. Eine Beeinträchtigung schutzwürdiger Belange einer möglicherweise vorhandenen Minderheit von Gewerbebetrieben, die kein Interesse an der Veröffentlichung des Gewerbes haben, könnte durch die Einführung eines Widerspruchsrechts ebenso vermieden werden, wie durch Art. 35 Abs. 3 MeldeG im Falle von Einwohnern, die nicht im allgemeinen Adressbuch erscheinen wollen. Wie auch im Meldewesen, wäre der Gewerbetreibende bei der Anmeldung seines Gewerbes auf sein Widerspruchsrecht hinzuweisen. Für die Altfälle käme ein wiederholter, ortsüblich bekanntzumachender Hinweis auf das Widerspruchsrecht in Betracht. Ich habe dem Bayer. Staatsministerium für Wirtschaft und Verkehr einen entsprechenden Vorschlag unterbreitet.

- Bei der Überprüfung von Landratsämtern fiel auf, daß bei manchen Ämtern ein generelles Gewerberegister aus den von den Gemeinden übermittelten Gewerbeanmeldungen geführt wird, während dies bei anderen Landratsämtern unbekannt ist. Alle Ämter erhalten zunächst von den kreisangehörigen Gemeinden Durchschriften der Gewerbeanmeldungen. Dies dient dem Vollzug verschiedener den Landratsämtern durch besondere Vorschriften übertragener Aufgaben wie z.B. hinsichtlich von Ausländern, von Betrieben, die einer besonderen Erlaubnis durch die Kreisverwaltungsbehörde z.B. nach Gewerbeordnung, Gaststättengesetz, Einzelhandelsgesetz bzw. Überwachung nach dem Lebensmittelgesetz usw. unterliegen. Außerdem hat das Landratsamt aber als Kreisverwaltungsbehörde eine umfassende Zuständigkeit zum Vollzug des Gewerberechts. Es nimmt den Vollzug der Titel II bis IV der Gewerbeordnung wahr. Die sachgerechte Erfüllung dieser Aufgabe - beispielsweise der Verwertung von Tatsachen, die die Zulässigkeit einer Gewerbeausübung infrage stellen könnten gem. § 35 GewO - macht die Kenntnis der angemeldeten Gewerbe im Landratsamt erforderlich. Aus der Sicht des Datenschutzes bestehen daher gegen die Führung von Registern über alle Gewerbetreibenden bei den Landratsämtern keine Bedenken.
- Die Kasse einer Stadt beabsichtigte, sämtlichen anordnungsbefugten Dienststellen eine Liste mit Namen, Anschrift und Kontonummer aller Personen, an die Auszahlungen geleistet wurden oder werden, zur Verfügung zu stellen. Durch eine solche Weitergabe würden jedoch jeder anordnungsbefugten Dienststelle auch die Namen, Anschriften und Kontonummern all der Personen offenbart, an die von anderen Dienststellen der Stadt Zahlungen geleistet wurden, obwohl diese Daten in der Regel zur Aufgabenerfüllung nicht erforderlich sind. Ich habe die Weitergabe dieser vollständigen Liste daher gem. Art. 4 i. V. m. Art. 17 Abs. 1 und Abs. 3 Satz 2 BayDSG für unzulässig erachtet.
- Für eine Stadt hatte ein Hochschullehrer ein Gutachten zur Sozialplanung nach dem Städtebauförderungsgesetz zu erstellen. In seinem Gutachten gab er sämtliche Befragungsergebnisse personenbezogen wieder. Da das Gutachten als Grundlage für die Entscheidung des Stadtrats benötigt wurde, ergab sich die Frage der Zulässigkeit der Offenbarung einer Vielzahl recht ins Detail der wirtschaftlichen Verhältnisse einzelner Betroffener gehender Angaben gegenüber dem Stadtrat. Ich bin hierzu mit dem Bayer. Staatsministerium des Innern der Auffassung, daß auch für die Weitergabe personenbezogener Daten an den Stadtrat als das oberste Gremium der Grundsatz der Erforderlichkeit gilt. Dabei ist eine allgemeine Festlegung nicht möglich. Es kann notwendig sein, Befragungsergebnisse personenbezogen vorzulegen, wenn der Stadtrat über soziale Maßnahmen für eine überwiegende Zahl von Sanierungsbetroffenen zu entscheiden hat (Bereitsstellung von Ersatzwohnraum, Härteausgleich usw.). In vielen Fällen wird es dagegen nicht nötig sein, so z.B., wenn erforderliche soziale Maßnahmen von den zuständigen Ämtern der Stadtverwaltung behandelt werden können, oder der Stadtrat über soziale Maßnahmen in einigen wenigen Fällen zu entscheiden hat. Soweit die „Grundsätze für den Sozialplan" nach § 4 Abs. 2 Städtebauförderungsgesetz, deren Aufstellung auf personenbezogenen Daten beruht, zu den Grundlagen einer Entscheidung z.B. über die Art des städtebaulichen Sanierungskonzepts gehören (z.B. überwiegend Beseitigung von Gebäuden und Neubau oder Instandsetzung oder Modernisierung bestehender Gebäude einschließlich Art und Umfang dieser Maßnahmen), genügen in aller Regel aggregierte Daten, ggf. auch Einzelangaben ohne Nennung von Namen und Anschrift. Es gehört daher zu den Aufgaben des Gutachters, sich mit dem Auftraggeber darüber zu verständigen, welche Gremien und Stellen notwendigerweise das vollständige Datenmaterial und welche ggf. die zusammenfassenden Ergebnisse erhalten und auswerten sollen. Die Darstellung im Gutachten hätte sich hiernach zu orientieren.
- In der Vergangenheit sind offenbar in einigen Fällen Gemeindebedienstete von Auskunfteien u. ä. aufgefordert worden, gegen Entgelt umfangreiche Auskünfte u.a. aus dem Gewerberegister nach einem bestimmten Muster zu erteilen. Ob diesen Ersuchen tatsächlich entsprochen wurde, konnte nicht festgestellt werden. Gleichwohl nehme ich die Vorfälle zum Anlaß, auf die Unzulässigkeit einer solchen „nebenamtlichen" Tätigkeit ausdrücklich hinzuweisen (siehe auch meinen Hinweis im 3. Tätigkeitsbericht, Nr. 3.10.5, S. 29).

4.15 **Einzelfragen**

4.15.1 Erörterung von Petitionen in öffentlicher Sitzung

Der Bayer. Landtag hat seine Geschäftsordnung vom 1.10.1982 (GVBl. S. 587) geändert, um bei der Beratung von Eingaben und Beschwerden das Persönlichkeitsrecht der Petenten besser zu schützen. Diese Änderung begrüße ich außerordentlich.

So lautet der in § 32 der Geschäftsordnung neu eingefügte Absatz 2 wie folgt:

„Abs. 1 gilt auch für die Behandlung von Eingaben und Beschwerden. Der Ausschuß schließt die Öffentlichkeit aus, wenn Rechtsvorschriften die Bekanntgabe von Daten untersagen. Er kann die Öffentlichkeit ausschließen, wenn Umstände aus dem persönlichen Lebensbereich des Beschwerdeführers oder eines Dritten zur Sprache kommen, durch deren öffentliche Erörterungen überwiegende schutzwürdige Interessen verletzt würden."

Auf die entsprechende Bitte eines Landtagsabgeordneten um Stellungnahme zu der Diskussion über einen stärkeren Schutz der Intimsphäre der Petenten hatte ich u.a. folgendes mitgeteilt:

Die Tatsache, daß ein Bürger von seinem Petitionsrecht Gebrauch macht, darf nicht dazu führen, daß er wegen der öffentlichen Erörterung seiner, die Privatsphäre berührenden Vorgänge Nachteile erleidet.

In der Wertordnung des Grundgesetzes ist die Menschenwürde der oberste Wert. Der Staat darf durch keine Maßnahme, selbst nicht durch ein Gesetz, die Würde des Menschen verletzen oder sie sonst über die in Art. 2 Abs. 1 Grundgesetz gezogenen Schranken hinaus in ihrem Wesensgehalt antasten. Dem Menschen in der Gemeinschaft der Bürger kommt somit ein sozialer Wert - und Achtungsanspruch zu. Mit der Menschenwürde wäre es nicht zu vereinbaren, wenn der Einzelne wie eine Sache behandelt würde, die einer Bestandsaufnahme in jeder Beziehung zugänglich wäre (s.o. BVerfGE, 27 S. 1/6). Im freiheitlich demokratischen Rechtsstaat kommt dem Parlament als einer der tragenden Gewalten besondere Bedeutung zu. Wegen dieser Bedeutung haben die Bürger in ihrer Gesamtheit ein berechtigtes Interesse, über die Arbeit des Parlaments unterrichtet zu werden.

Für die Frage einer zulässigen öffentlichen Erörterung der von einem Bürger dem Ausschuß für Eingaben und Beschwerden vorgetragenen Sachverhalte ist daher immer dann, wenn durch diese Eingabe die Privatsphäre des Bürgers berührt wird, abzuwägen zwischen dem Interesse des Einzelnen am Schutz seiner Privatsphäre und dem Informationsinteresse der Öffentlichkeit an den Vorgängen im Parlament. Zwar trägt der einzelne Petent durch seine Eingabe an das Parlament selbst dazu bei, daß er Person eines gewissen Öffentlichkeitsinteresses wird, doch kann bei einem Bürger, der nicht Person der Zeitgeschichte ist, nicht von vorneherein ein Vorrang des Informationsinteresses der Öffentlichkeit an der Arbeit des Petitionsausschusses gegenüber dem Schutz der Privatsphäre des Einzelnen angenommen werden. Zwar muß der Einzelne „als gemeinschaftsbezogener und gemeinschaftsgebundener Bürger" (BVerfGE 27, S. 344/351) staatliche Maßnahmen hinnehmen, wegen der zentralen Bedeutung des Persönlichkeitsrechts ist hierbei jedoch der Grundsatz der Verhältnismäßigkeit strikt zu beachten. Nach diesem mit Verfassungsrang ausgestatteten Grundsatz sind Eingriffe in die Privatsphäre nur dann und insoweit zulässig, als sie zum Schutz öffentlicher Interessen unerläßlich sind. Das heißt, daß der Einbruch in die persönliche Sphäre nicht weitergehen darf, als eine angemessene Befriedigung des Informationsinteresses der Öffentlichkeit dies zwingend erfordert (vergl. BVerfGE 35, S. 202/232). Maßgeblich ist hier die Bedeutung, die der vom Petenten vorgetragene Sachverhalt für die Öffentlichkeit hat.

Als Maßstab zur Beurteilung, inwieweit Vorgänge dem besonders schützenswerten privaten Bereich zuzuordnen sind, können die gesetzlichen Geheimhaltungspflichten herangezogen werden. Selbst wenn der Landtag im einzelnen nicht Adressat dieser Vorschriften ist, kann aus ihnen abgeleitet werden, daß die geschützten Vorgänge nicht für die breitere Öffentlichkeit geeignet sind. Sofern ohne Vorliegen besonderer Geheimhaltungsbestimmungen dennoch im konkreten Einzelfall davon ausgegangen werden kann, daß durch die öffentliche Erörterung der mit der Petition im Zusammenhang stehenden Vorgänge schutzwürdige Belange des Petenten beeinträchtigt werden können, scheint mir für die Beurteilung, ob eine öffentliche Erörterung zulässig ist, die Heranziehung der Grundsätze des § 172 Nr. 2 GVG angebracht. Diese Bestimmung regelt den Ausschluß der Öffentlichkeit in Gerichtsverhandlungen, wenn „Umstände aus dem persönlichen Lebensbereich eines Prozeßbeteiligten oder Zeugen .....zur Sprache kommen, durch deren öffentliche Erörterung überwiegend schutzwürdige Interessen verletzt würden".

Bei Erörterung von dem schutzwürdigen privaten Bereich eines einzelnen zuzuordnenden Vorgängen dürfte ein überwiegendes öffentliches Interesse an einer der Allgemeinheit zugänglichen Sitzung im Regelfall nicht anzunehmen sein. Anderes gilt nur, wenn der vom Petenten vorgetragene Sachverhalt an sich von herausragender Bedeutung für die Öffentlichkeit ist oder der Petent durch den Vorgang bereits eine einer Person der Zeitgeschichte vergleichbare Position erreicht hat. Selbst im letzteren Falle müssen die Schutzbedürfnisse des Petenten besonders sorgfältig abgewogen werden, weil sogar Vorgänge, die beispielsweise wegen früherer Veröffentlichungen allgemein bekannt sind, zu schützen sind, wenn dadurch die weitere Entwicklung der Persönlichkeit des einzelnen gefährdet würde (vergl. BVerfGE 35, S. 202/233).

Bei der vorstehend genannten Abwägung zwischen Schutz der Privatsphäre und dem Interesse der Öffentlichkeit unter Beachtung des Verhältnismäßigkeitsgrundsatzes ist darüber hinaus zu berücksichtigen, daß im Regelfall dem Öffentlichkeitsinteresse auch dadurch entsprochen werden kann, daß die Petition ohne Nennung der auf eine bestimmte Person hindeutenden Angaben erörtert wird. Soweit letzteres möglich ist, wäre eine Erörterung unter Nennung des Petenten im Regelfall unverhältnismäßig. Fälle, in denen das öffentliche Interesse an einer Erörterung unter Nennung des Namens des Petenten für die Öffentlichkeit von solcher Bedeutung ist, daß sie die persönlichen Belange des Petenten übertreffen, dürften die Ausnahme sein.

Auch die Tatsache, daß der Betroffene selbst mit seiner Petition den Anstoß gegeben hat, Vorgänge zu erörtern, die seinen persönlichen Lebensbereich berühren oder seine persönliche Angelegenheit betreffen, kann nicht als Einwilligung zur Erörterung in öffentlicher Sitzung gewertet werden. Zum einen wird mancher Bürger nicht wissen, daß die Anrufung des Petitionsausschusses eine öffentliche Erörterung zur Folge haben kann, zum anderen mag sich mancher Bürger den möglichen Auswirkungen einer öffentlichen Erörterung nicht bewußt sein. Im übrigen würde der Betroffene bei zwingender öffentlicher Erörterung vor die Wahl gestellt, entweder auf sein Petitionsrecht oder auf den Schutz seiner Privatsphäre zu verzichten.

Zwar sind in der nun beschlossenen Änderung der Geschäftsordnung für den Bayer. Landtag nicht alle meine Überlegungen berücksichtigt worden, ich begrüße sie als eine Stärkung des Persönlichkeitsschutzes der Petenten gleichwohl. Im übrigen wird für den tatsächlichen Schutz der Privatsphäre der Petenten eine dessen schutzwürdige Belange berücksichtigende Anwendung dieser Vorschriften wesentlich sein.

4.15.2 Datenübermittlung von Kfz-Zulassungsstellen

Die Auskunftserteilung durch die Kfz-Zulassungsstellen an Behörden oder an Stellen außerhalb des öffentlichen Bereichs, z.B. an Versicherungen, Rechtsanwälte und Privatpersonen, bemißt sich nach § 26 Abs. 5 Straßenverkehrszulassungsordnung. Danach ist die Erteilung einer Auskunft über die Fahrzeuge, die Halter und die Versicherungen im Einzelfall an Behörden auf deren Antrag und bei anderen Stellen bei Darlegung eines berechtigten Interesses statthaft. Diese Bestimmung der Straßenverkehrszulassungsordnung geht für diese Datenübermittlung, als solche ist die Auskunft zu werten, als spezialgesetzliche Regelung den Vorschriften des Bayer. Datenschutzgesetzes nach Art. 2 Abs. 2 BayDSG vor. Wenn auch nicht ausdrücklich erwähnt, so ist jedoch auch bei einer Auskunftserteilung nach § 26 Abs. 5 Straßenverkehrszulassungsordnung für die Zulässigkeit einer Datenweitergabe an Behörden Voraussetzung, daß die datenempfangende Behörde diese Daten

für ihre Aufgabenerfüllung benötigt. Bei einer Auskunft an sonstige Stellen sind neben dem berechtigten Interesse dieser Personen auch die schutzwürdigen Belange der Betroffenen - soweit erkennbar - bei der Auskunftserteilung zu berücksichtigen.

Telefonische Auskünfte sind hierbei als Form der Datenübermittlung grundsätzlich problematisch, sofern der Anrufer nicht amtsbekannt ist. Denn hier besteht generell die Gefahr, daß ein Unbefugter Daten erlangt. Für eine sachgerechte Auskunftserteilung empfiehlt es sich, wie dies teilweise auch Praxis ist, die Identität des Auskunftsersuchenden festzustellen, seine Auskunftsgründe festzuhalten und einen entsprechenden Vermerk über die Auskunft in die Fahrzeugakte aufzunehmen, um gegebenenfalls dem Betroffenen gegenüber einen Nachweis führen zu können. Sollte im Einzelfall der Kfz-Zulassungsstelle bekannt sein, daß hinsichtlich der Daten des Betroffenen - beispielsweise im Meldeamt - eine Auskunftssperre besteht, so sollte vor einer eventuellen Auskunftserteilung unbedingt das Einverständnis des Betroffenen eingeholt werden. Da dieser Fall die Ausnahme sein dürfte, ist in einer solchen Vorgehensweise keine wesentliche Beeinträchtigung der Dienstgeschäfte zu sehen. Das Problem besteht in derartigen Fällen wohl eher darin, inwieweit die Kfz-Zulassungsstelle von einer derartigen Auskunftssperre beim Einwohnermeldeamt erfährt. Besteht hier kein ausreichender Informationsaustausch zwischen Einwohnermeldeamt und Kfz-Zulassungsstelle, kann die Sperrung der Daten des Betroffenen beim Einwohnermeldeamt durch die Auskunftserteilung über die Kfz-Zulassungsstelle zumindest teilweise umgangen werden.

Manche Kfz-Zulassungsstellen überlassen außerhalb der Dienstzeit der zuständigen Polizeibehörde einen Schlüssel für den Zugang zur Kfz-Zulassungsstelle. Hiergegen habe ich grundsätzlich keine Bedenken, wenn sichergestellt ist, daß die Einsichtnahme in die Unterlagen der Kfz-Zulassungsstelle nur im berechtigten Einzelfall erfolgt. Um dies zu gewährleisten, sollte der Dienststellenleiter der Polizeibehörde den Erhalt des Schlüssels bestätigen und festlegen, wer über den Schlüssel verfügen darf. Außerdem wäre es auch aus Gründen der Nachprüfbarkeit zweckmäßig, wenn bei der Polizei Tag und Zeit der jeweiligen Aus- und Rückgabe des Schlüssels, die schlüsselempfangende Person und der Fall, der Anlaß zur Nachschau gibt, in einer entsprechende Kladde festgehalten würden. Die Kenntnisnahme weiterer zur Aufgabenerfüllung nicht notwendiger Daten durch die Polizei in der Kfz-Zulassungsstelle ist nach Möglichkeit durch geeignete Maßnahmen zu unterbinden. Solange dies aus organisatorischen oder technischen Gründen nicht möglich ist, darf der Polizeibeamte solche Informationen grundsätzlich nicht verwerten.

5. Bericht zur Datenschutzkontrolle im technischen und organisatorischen Bereich

5.1 Technische und organisatorische Grundsatzfragen

5.1.1 Datensicherung und moderne Technologie

Durch die Miniaturisierung der Bauelemente wurden die Computer kleiner, dabei trotzdem ständig leistungsfähiger und billiger. So können heute auf einem Silizium-Plättchen (Chip) der Größe von einigen Quadratmillimetern mehr als 64 000 Speicherzellen untergebracht werden. Diese hochintegrierten Schaltkreise ermöglichen Schaltgeschwindigkeiten, die im Bereich von Nano-Sekunden, also dem Milliardstelteil einer Sekunde, liegen. Durch diese technologischen Fortschritte steigt auch im öffentlichen Bereich die Zahl der dezentralen Systeme ständig.

Durch eine einseitige Berichterstattung ist nun vielfach der falsche Eindruck entstanden, „der Datenschutz" wende sich gegen die technologischen Fortschritte auf dem Gebiet der Computertechnik, insbesondere in der Weiterentwicklung der automatisierten Datenverarbeitung. Infolge der modernen Technologie können in der Tat größere Datenmengen gespeichert und auch verknüpft werden, so daß sich das Gefahrenpotential erhöht. Bei unsachgemäßer Handhabung entstehen somit größere Gefahrenmomente und möglicherweise größerer Schaden, als es bei der Beibehaltung der bisherigen Verfahren der Fall wäre. Mit meinen Mitarbeitern werde ich diese Entwicklungen kritisch beobachten und rechtzeitig auf die Gefahrenquellen bei Fehlverhalten hinweisen müssen.

Neue Techniken - das darf nicht übersehen werden - eröffnen aber auch neue Dimensionen bei der Kontrolle der Datenverarbeitung, weil nicht nur personenbezogene Daten, sondern auch Daten über den Ablauf der Datenverarbeitung problemlos gesammelt und schnell ausgewertet werden können. Der Datenschutz muß diese Möglichkeit nutzen und kann deshalb Äußerungen entgegentreten, die ihm von vorneherein Technikfeindlichkeit und Unaufgeschlossenheit gegenüber neuen Technologien unterstellen. Nutzen für den Datenschutz können so zum Beispiel intelligente Sicherheitsanlagen, wie Einbruch-, Brand- und Überfallmeldeanlagen, bieten. Diese sind heute durch weniger Bauteile sicherer im Betrieb und ermöglichen es zusätzlich festzustellen, wo ein Alarm ausgelöst wurde. Sie können bei Sicherheitsverletzungen sogar Art und Größe des Eindringlings analysieren.

Auf Grund des technischen Fortschrittes auf dem Gebiet der elektronischen Datenverarbeitung zeichnen sich deshalb für die kommenden Jahre auf dem Gebiet der Technik für den Datenschutz folgende Schwerpunkte ab:

Der Datenschutzbeauftragte muß in der Lage sein, Gefahren und Risiken moderner Computer-Technologien rechtzeitig zu erkennen und zu beurteilen. Dazu ist es notwendig, den Erfahrungsaustausch mit den Herstellern zu verstärken. Mit einigen Herstellern wurden bereits Gespräche über neue Produkte und deren Datensicherungskomponenten sowie deren Verbesserungsmöglichkeiten geführt. Besondere Beachtung verdienen die Entwicklung der Mikrocomputer und der Personal-Computer. Gerade hier sind nicht nur im Zuge der Büroautomation in den nächsten Jahren beachtliche Zuwachsraten zu erwarten. Diese Aufgabe wird allerdings dadurch erschwert, daß derartige Systeme heute von einer Vielzahl von Firmen angeboten werden, und die Personalkapazität meiner Geschäftsstelle nur begrenzt ist. Wenngleich sich solche Systeme in ihrem Leistungsumfang ähnlich sind, unterscheiden sie sich doch hinsichtlich ihres logischen Konzeptes und ihrer technischen Realisierung. Darüber hinaus werden Mikrocomputer, ja sogar Textsysteme, immer häufiger an Großrechner (Hostrechner) angeschlossen, was die Verfügbarkeit zusätzlicher Datensicherungsmaßnahmen notwendig macht. Daraus ergibt sich ein weiterer Schwerpunkt bei der Arbeit des Datenschutzbeauftragten, nämlich die Analyse moderner Vermittlungstechniken. In den kommenden Jahren sind auch hier durch neue Technologien grundlegende Änderungen zu erwarten. Dies gilt besonders für die von verschiedenen Herstellern und der Deutschen Bundespost im Rahmen der Neuen Medien vorgesehene Kommunikationssysteme. Eine Reihe von Problemen zeichnet sich schon jetzt bei der Gewährleistung des Zugriffschutzes der in Konzentratoren und Zentralen gespeicherten Daten und der allgemeinen Datensicherheit auf dem Übertragungsweg ab. Im Zusammenhang damit tauchen die Fragen der Verschlüsselung und der Authentifikation auf, die zwar allgemein bekannt sind, im öffentlichen Bereich jedoch bisher - wohl auch wegen der damit verbundenen Kosten - nur vereinzelt gelöst wurden. Gerade der Einsatz von Teletex durch die Bundespost wird sicher Fragen nach der Datensicherheit auf den Leitungswegen auslösen, da hier Nachrichten im genormten 7-Bit-ISO-

Code übertragen werden, was ihre Umsetzung in Klartext für Außenstehende problemlos gestattet.

Ein weiterer Schwerpunkt datenschützender Tätigkeit in der Zukunft wird die Nachprüfbarkeit einzelner Verfahrensschritte bei der automatisierten Datenverarbeitung sein. Hier muß ohne großen manuellen Aufwand festgestellt werden können, zu welcher Zeit welche Dateien von welchem Benutzer automatisiert verarbeitet wurden. Eine solche Prüfung ist nur durchführbar, wenn sie maschinell unterstützt wird. Maschinell aufgezeichnete JobAccount- und Ablaufprotokolldaten sind in diesen Fragenkomplex mit einzubeziehen. Die neuen Technologien werden eine wirtschaftliche Realisierbarkeit dieser Forderungen sicher begünstigen. Schließlich wird die Transparenz der Datenverarbeitung durch den Einsatz eines maschinellen Dokumentationssystems (DATA-Dictionary) erhöht, in dem Verfahren, Computerläufe, Dateien sowie deren Zugriffsberechtigung zu bestimmten Dateien und die Verfügungsgewalt über sie beschrieben werden.

5.1.2 Grundsatzfragen der datenschutzrechtlichen Freigabe nach Art. 26 Abs. 2 und 4 BayDSG

Nach Art. 26 Abs. 2 BayDSG ist der erstmalige Einsatz von automatisierten Verfahren, mit denen personenbezogene Daten verarbeitet werden, hinsichtlich der Datenarten und der regelmäßigen Datenübermittlung durch die oberste Dienstbehörde oder die von ihr ermächtigte Behörde schriftlich freizugeben. Von dieser Entscheidung ist der Landesbeauftragte für den Datenschutz nach Art. 26 Abs. 4 BayDSG unverzüglich zu unterrichten. Hierüber wurde früher bereits regelmäßig berichtet.

Die Zahl der datenschutzrechtlichen Freigaben hat sich in den letzten Jahren ständig erhöht. Da der Landesbeauftragte für den Datenschutz in der Regel lediglich von der bereits erfolgten Freigabe Kenntnis erhält, ist allerdings unbekannt, wie hoch der Prozentsatz der Verfahren ist, bei denen aufgrund der datenschutzrechtlichen Prüfung vor Freigabe Änderungen in Verfahren notwendig wurden.

Neben den im 4. Tätigkeitsbericht (Nr. 3.9.1, Seite 43 f) aufgezählten Angaben sollte die Freigabemitteilung auch Aussagen über die Speicherungsdauer der Daten enthalten. Schließlich sollte aus dem Speicherungszweck und den Datenarten die Sensibilität der verarbeiteten Daten ersichtlich werden.

Wie wir immer wieder feststellen, fehlen bei vielen Freigabemitteilungen wichtige Informationen für notwendige Nachprüfungen. Art. 26 Abs. 4 BayDSG muß daher so verstanden werden, daß auch wichtige Entscheidungsgrundlagen, die zu der Freigabe-Entscheidung geführt haben, mitgeteilt werden. Rechtlich ist die insoweit notwendige Unterrichtung des Landesbeauftragten für den Datenschutz im übrigen auch im Rahmen der allgemeinen Unterstützungs- und Auskunftspflicht der Verwaltung aus Art. 28 Abs. 2 BayDSG begründet.

5.2 Prüfung der technischen und organisatorischen Maßnahmen des Datenschutzes

5.2.1 Rückblick

Im Bayerischen und Bundesdatenschutzgesetz traten die Bestimmungen bezüglich der technischen und organisatorischen Maßnahmen (z.B. Art. 15 BayDSG) erst am 1.1.1979 in Kraft, um den einzelnen Stellen einen gewissen Zeitraum zu gewähren, die notwendigen Maßnahmen festzulegen und einzuführen. Mit der Prüfungstätigkeit habe ich im Herbst 1979 bei einigen größeren Rechenzentren begonnen. In den zurückliegenden drei Jahren wurden bei ungefähr 100 Stellen die technischen und organisatorischen Maßnahmen zum Datenschutz überprüft. Auch hier ist ein Rückblick angebracht.

Bei den ersten Prüfungen stellte ich bei den einzelnen Stellen wegen der mangelnden Erfahrung Unsicherheiten bei der Auswahl der zu treffenden Maßnahmen fest. Einige Stellen hatten zum damaligen Zeitpunkt überhaupt nur Provisorien eingeführt und warteten erst die Ergebnisse der Überprüfung ab. Andere Stellen hingegen engagierten sich und konnten bereits mit recht wirkungsvollen Lösungen aufwarten. Gravierende Mängel im Gesamtkonzept der technisch-organisatorischen Maßnahmen zum Datenschutz waren weniger häufig anzutreffen. Die Kontrollen im Berichtszeitraum zeigten aber auch, wie mühsam es ist, Datenschutzverständnis in alle Amtsstuben zu tragen und wie schwierig es zudem bei der gegenwärtigen Haushaltslage ist, Mittel für Maßnahmen des Datenschutzes bewilligt zu erhalten. Denn nur in Ausnahmefällen ist es möglich, durch organisatorische Maßnahmen, die keine finanziellen Mittel erfordern, den gewünschten Schutzzweck zu erreichen. Oft lassen sich aber vorhandene Ressourcen umsetzen, so daß zusätzliche Kosten vermieden werden können. Wegen der gegenwärtigen Haushaltslage generelle Abstriche an den Sicherheitsvorkehrungen zu machen, halte ich aber nicht für vertretbar.

In den meisten Fällen wurden meine Anregungen und Forderungen zur Verbesserung und Gewährleistung der Datensicherung bereitwillig aufgenommen. Besonders hervorheben möchte ich die Stadt Lindau, die in vorbildlicher Weise die Sicherung ihres Rechenzentrums und auch in anderen Amtsbereichen die Erfordernisse der technisch-organisatorischen Maßnahmen zum Datenschutz zur vollen Zufriedenheit gelöst hat. In einigen Fällen, in denen größere bauliche Veränderungen notwendig waren, habe ich zwar die Schwachstellen aufzeigen können, Xe Bese Xigung dieser Mißstän X Xäßt allerdings wegen des damit verbundenen Kostenaufwands noch immer auf sich warten. Trotzdem bin ich der Meinung, daß, gemessen an den beispielsweise bedeutenden Mietkosten, die die Datenverarbeitungsanlagen monatlich verursachen, die Mittel für eine ordnungsgemäße Datensicherung aufzubringen sein müßten. Von einem Rechenzentrum einer bestimmten Größe an ist - um nur einige Beispiele zu nennen - sicherzustellen, daß das Magnetbandarchiv gegen den Zugriff Unbefugter geschützt und die Datenerfassung nicht im inneren Sicherheitsbereich durchgeführt wird, auch wenn dazu besondere Geräte notwendig sind. In einem größeren Rechenzentrum, das für verschiedene öffentlichen Stellen unterschiedliche Aufgaben abwickelt, wird meist eine Vielfalt von personenbezogenen Daten gespeichert und verarbeitet, so daß sich im inneren Sicherheitsbereich nur solche Personen aufhalten dürfen, die einen unmittelbaren Bezug zur Maschinenbedienung haben. Datenerfassungskräfte und Benutzer haben im inneren Sicherheitsbereich nichts zu suchen. Unzureichende Übergangslösungen über einen Zeitraum von drei und mehr Jahren sind aus der Sicht des Datenschutzes untragbar und lassen sich auch damit nicht begründen, daß die Rechenzentren später einmal in Neubauten, für die manchmal die Bauplanung noch nicht begonnen hat, verlagert werden.

Ausgesprochen zeitaufwendig gestaltet sich die Überwachung des Vollzugs der Prüfungsbemerkungen. Verletzungen von Vorschriften über den Datenschutz müssen nach Art. 30 Abs. 1 BayDSG beanstandet und ihre Behebung in angemessener Frist gefordert werden. Meine Mitarbeiter sind bei der Suche nach wirksamen und geeigneten Mitteln zur Sicherstellung der technischen und organisatorischen Maßnahmen zum Datenschutz stets behilflich. Die angestrebten Lösungen finden auch meistens die Zustimmung der einzelnen Stelle. Daß die Behebung von Kleinigkeiten manchmal nicht mit dem ursprünglich zugesagten Nachdruck vorangetrieben wird, ist aber unverständlich. Im großen und ganzen läßt sich jedoch sagen, daß die Forderungen hinsichtlich der technischen und

organisatorischen Maßnahmen zum Datenschutz von den einzelnen Stellen erfüllt werden.

5.2.2 Ergebnisse der Kontrollen

Im Berichtszeitraum wurden Kontrollen bei Städten und Gemeinden, bei Landratsämtern, im medizinischen Bereich, im Universitätsbereich und bei einem großen Service-Rechenzentrum durchgeführt. Obwohl das Problembewußtsein hinsichtlich der technischen und organisatorischen Maßnahmen zum Datenschutz in den vergangenen Jahren gewachsen ist, traf ich auch im Berichtszeitraum bei den Kontrollen immer wieder auf Fälle, bei denen notwendige Sicherungen, meist unbewußt, unterblieben.

- Am häufigsten wurden Mängel bei der Aufbewahrung von perso nenbezogenen Daten, die manchmal sogar Diagnosedaten aus dem medizinischen Bereich enthielten, festgestellt. Dieser Umstand ist umso überraschender, da viele Stellen eigene Datenschutzbeauftragte bestellt haben, die dieses Problem eigentlich hätten erkennen müssen. Zu bemängeln war ferner die allzu großzügige Übung, Schränke und Amtszimmer nach Dienstschluß nicht abzuschließen. Zudem fehlten meistens auch wirksame Schlüsselregelungen. - Archivräume, in denen eine Vielzahl personenbezogener Daten aufbewahrt werden, waren unzureichend gesichert. In besonders sensiblen Bereichen empfiehlt es sich, einen Nachweis für die Archivbenutzung zu führen.
- Bei der automatisierten Datenverarbeitung traten immer noch Mängel bei der Zugangssicherung auf. Fluchtwege sind wirklich nur für den Ernstfall gedacht und sollten nicht aus Bequemlichkeit täglich benützt werden. Rechenzentren, in denen sensible Daten verarbeitet werden, sind so abzusichern, daß gewaltsame Zutrittsversuche entdeckt werden können.

Je größer ein Rechenzentrum ist, um so mehr muß dafür getan werden, daß Benutzer Datenverarbeitungsprogramme nur berechtigt zur Ausführung bringen können. Bei Abweichungen vom normalen Produktionsablauf, z.B. für Sonderauswertungen, sind besondere Sicherheitsvorkehrungen notwendig. Grundsätzlich empfiehlt es sich jedoch, die Systemaufzeichnungen regelmäßig auf Abweichungen hin zu untersuchen. Leider bieten die Hersteller dafür nicht die gewünschte Unterstützung, so daß die Betreiber großer Rechenzentren bei der Lösung des Problems oft auf sich allein gestellt sind, d.h. die entsprechende Software selbst entwickeln müssen.

Die Kontrollen haben aber auch gezeigt, daß überall dort, wo Beauftragte für den Datenschutz bestellt waren, die ihre Aufgabe auch ernst nahmen, eine Reihe von technischen und organisatorischen Maßnahmen eingeführt waren, die den Datenschutz wesentlich unterstützten. Dem Datenschutzbeauftragten muß genügend Zeit für seine Aufgaben als Datenschutzbeauftragter eingeräumt werden. Ein behördeninterner Datenschutzbeauftragter sollte sich in erster Linie mit der Schulung der Bediensteten sowie der Definition und Einführung von Datenschutzmaßnahmen befassen. Er sollte ein internes Register über alle automatisiert und manuell geführten Dateien führen, die Wirksamkeit der Datensicherungsmaßnahmen überwachen und jede Möglichkeit zur Weiterbildung nützen, damit er seiner gewiß nicht leichten Aufgabe gerecht werden kann.

5.2.3 Erwartungen bei den zukünftigen Kontrollen

Obwohl die Erfahrung gezeigt hat, daß in der automatisierten Datenverarbeitung weniger Mängel als bei der manuellen Datenverarbeitung festzustellen sind, erwarte ich mir bei den kommenden Kontrollen der technischen und organisatorischen Maßnahmen zum Datenschutz, daß die einzelnen Stellen, sofern sie ein eigenes Rechenzentrum betreiben,

- den Zugang und Abgang des Rechenzentrumspersonals geregelt haben,
- die Trennung von Programmierung und Produktionsbetrieb, soweit möglich, einhalten,
- einen wirksamen Zugriffschutz vorsehen, in den nicht nur Dateien, sondern auch Programme einbezogen sind,
- wirksame Regelungen getroffen haben, daß Ergebnisse aus der automatisierten Datenverarbeitung zuverlässig an die fachlich zuständige Stelle gelangen und
- über eine Dokumentation der Verfahren, der Maschinenbedienung und der Systemgenerierung verfügen, die für fachkundige Dritte aussagefähig ist.

An organisatorischen Maßnahmen sowie bei der Verarbeitung manueller Dateien erwarte ich von den einzelnen Stellen, daß

- die personellen Zuständigkeiten für Angelegenheiten des Datenschutzes schriftlich geregelt sind,
- beim internen Datenschutzbeauftragten Übersichten über alle Dateien vorliegen,
- die Einhaltung der Regelungen für den Zugang zu den Amtsbe reichen gewährleistet ist, sowie Regelungen über die Aufbe wahrung, Bearbeitung und Übermittlung von personenbezogenen Daten bestehen und
- letztlich auch die Vernichtung ausgesonderter Unterlagen mit personenbezogenen Daten so geregelt ist, daß diese von Unbefugten nicht mehr verwendet werden können.

Dabei ist stets darauf zu achten, daß bei der Festlegung der technischen und organisatorischen Maßnahmen zum Datenschutz ein gewisses Augenmaß eingehalten wird und die Verhältnismäßigkeit zum Schutzzweck gewahrt bleibt. Welche seltsame Blüten falschverstandener Datenschutz treiben kann, zeigt folgendes Beispiel: Ein Rechenzentrum befindet sich im Untergeschoß eines Gebäudes, vor dem ein Parkplatz angelegt ist, auf dem auch Bedienstete anderer Bereiche derselben öffentlichen Stelle ihre Kraftfahrzeuge abstellen konnten. Dieser Parkplatz wurde nun für die Bediensteten der anderen Amtsbereiche aus Datenschutzgründen gesperrt, weil angeblich diese Personen vom Parkplatz aus durch die Fenster personenbezogene Daten, die am Drucker ausgedruckt werden, zur Kenntnis nehmen könnten. Hinzuzufügen ist, daß der Parkplatz an einer öffentlichen Straße liegt und für jedermann begehbar ist.

Abschließend wird festgestellt, daß auch in den kommenden Jahren mit der Prüfungstätigkeit verstärkt fortgefahren werden muß, da bisher nur ein verhältnismäßig kleiner Teil der bedeutenden Rechenzentren besucht wurde, der Stand der Technik sich stetig weiterentwickelt und bereits besuchte Rechenzentren durch zu erwartende Umkonfigurierung und Umorganisation sich von ihrer ursprünglichen Form unterscheiden werden.

5.3 Technische und organisatorische Maßnahmen zum Datenschutz

5.3.1 Planung von Datensicherungsmaßnahmen

Erfreulicherweise wird meine Geschäftsstelle bei Neubaumaßnahmen immer häufiger um gutachtliche Stellungnahme zu baulichen Datensicherungsmaßnahmen gebeten. Grundsätzlich besteht zwar keine Verpflichtung, bei Neubaumaßnahmen den Landesbeauftragten für den Datenschutz einzuschalten, die Erfahrung hat jedoch gezeigt, daß sich im Planungsstadium Erfordernisse des Datenschutzes billiger und leichter berücksichtigen lassen. Mehrkosten durch den Datenschutz treten häufig gar nicht auf, zumindest sind sie gemessen an der Bausumme zu vernachlässigen.

Um über die notwendigen Datensicherungsmaßnahmen im Einzelfall Ratschläge erteilen zu können, wird neben einem detaillierten Bauplan, eine Baubeschreibung und Angaben über die Ausstattung von Türen und Fenstern benötigt. Aus den Plänen muß auch die Lage der Räume hervorgehen, in denen personenbezogene Daten aufbewahrt und verarbeitet werden. Insbesondere handelt es sich dabei um solche Räume, in denen ADV-Systeme und Bildschirme aufgestellt werden sollen. Außerdem sind Archive, Zentralregistraturen und solche Amtsbereiche, in denen sensible personenbezogene Daten aufbewahrt werden, zu kennzeichnen.

Bei der Festlegung der Maßnahmen zur Zugangssicherung bestehen grundsätzlich zwei Möglichkeiten: Entweder wird der gesamte Amtsbereich gesichert, was in manchen Fällen sicher notwendig sein kann, oder man bildet innerhalb des Amtsbereiches in sich geschlossene Sicherheitszonen, was sich für die Mehrzahl der Behörden anbieten wird.

Bei der Einführung von Datensicherungsmaßnahmen ist sehr darauf zu achten, daß die Maßnahmen untereinander abgestimmt sind. Der Einbau von einbruchhemmendem Glas der Stufe 2 (mittlere Einbruchshemmung) in Zugangstüren wäre sinnlos, wenn Türrahmen, Verankerungen und Schloß nicht eine vergleichbare Sicherheit böten. Genauso mangelhaft wäre es, nur die Türen eines bestimmten Bereiches zu sichern und die Fenster im Sicherungskonzept unberücksichtigt zu lassen.

Bei der Einrichtung dezentraler ADV-Systeme sind folgende Grundregeln, die über bauliche Maßnahmen hinausgehen, zu beachten:

- Die Zahl der Zutrittsberechtigten ist überschaubar zu halten;
- die Räume, in denen solche Systeme aufgestellt werden, sollten sich möglichst nicht im Erdgeschoß eines Gebäudes befinden und durch massive Wände von den übrigen Bereichen getrennt sein;
- für die Aufbewahrung von maschinell lesbaren Datenträgern, wozu auch die der Sicherungsbestände zählen, sind Metallschränke mit Sicherheitsschloß vorzusehen;
- bei Betriebsbereitschaft der ADV-Anlage auch außerhalb der üblichen Dienstzeit (z.B. bei bedienerlosem Betrieb) sind an den angeschlossenen Datensichtstationen Zugriffssicherungen gegen Unbefugte vorzusehen und das Rechenzentrum gegen unberechtigten Zutritt zu sichern.

5.3.2 Orientierungshilfen für technische und organisatorische Maßnahmen zum Datenschutz

Über Art und Umfang von technischen und organisatorischen Maßnahmen zum Datenschutz existieren bekanntlich keine allgemeinen Vorschriften. Häufig werde ich nach solchen Regelungen gefragt. So sehr einheitliche Konzepte von der Prüfbarkeit her zu begrüßen wären, um so mehr würde ein starres Regelungsgefüge den Ermessensspielraum bei der Auswahl von wirksamen Datensicherungsmaßnahmen einschränken. Gerade im technischen Bereich gibt es oft mehrere gleichwertige Möglichkeiten, um einen bestimmten Sicherungszustand zu erreichen.

Der Katalog für technische und organisatorische Maßnahmen zum Datenschutz (Datensicherungskatalog), dessen versuchsweise Anwendung der Staatliche Koordinierungsausschuß Datenverarbeitung in seiner Sitzung am 30.7.1980 empfohlen hat, stellt zwar eine wertvolle Orientierungshilfe für Datensicherungsmaßnahmen bei Großrechenzentren dar, deckt aber nur zu einem kleinen Teil die datenverarbeitenden Stellen ab, an die sich der Art. 15 Bayer. Datenschutzgesetz bzw. § 6 Bundesdatenschutzgesetz richten. In allen Anwendungsbereichen bewährt hat sich hingegen bei der Festlegung von Datensicherungsmaßnahmen das Schutzstufenkonzept. Dieses Konzept- das soll hier noch einmal deutlich gemacht werden - ist keine Erfindung des Datenschutzes. Vertraulichkeits- und Sicherheitsstufen gab es schon früher in der öffentlichen Verwaltung und in der Privatwirtschaft. Das Schutzstufenkonzept soll in erster Linie dem Gesichtspunkt der Verhältnismäßigkeit von Datensicherungsmaßnahmen Rechnung tragen. Zwar sind alle personenbezogenen Daten schutzwürdig, nur der Aufwand, sie zu sichern, kann verschieden hoch angesetzt werden. Bei Mißbrauch von sensiblen Daten ist die Beeinträchtigung des Betroffenen in der Regel größer als bei unsensiblen Daten. Die Sensibilität der Daten richtet sich nicht nur nach den einzelnen Datenarten, sondern auch wesentlich nach dem Umfeld, in dem sich die Datensammlung befindet und danach, mit welchen Dateien diese verknüpft werden kann.

Das Schutzstufenkonzept wurde deshalb auch auf Datenbestände übertragen, die nicht auf Großrechnern verarbeitet werden. So wurden Orientierungshilfen für technische und organisatorische Maßnahmen beim Einsatz von dezentralen Systemen und bei der Verarbeitung von Dateien in nicht automatisierten Verfahren zusammengestellt. Je nach Einsatzart und -ort ist zu prüfen, ob die dort aufgeführten Maßnahmen sinnvoll und nützlich sind. Sie sind daher stets als Anregungen zu verstehen. Konkrete Aussagen über die Art von Sicherungsmaßnahmen lassen sich in vielen Fällen besser am konkreten Einzelfall festlegen, als in einer allgemeinen Richtlinie, die die Gesamtheit aller Fälle abzudecken versucht. Die Orientierungshilfe für technische und organisatorische Maßnahmen bei der Verarbeitung von Dateien in nichtautomatisierten Verfahren gliedert sich nach den möglichen Arbeitsschritten, die bei der Verarbeitung von personenbezogenen Dateien auftreten können, nicht nach den zehn Kontrollen des Art. 15 BayDSG bzw. § 6 BDSG. Als Beispiele für solche Arbeitsschritte seien das Anlegen und Bearbeiten oder das Aufbewahren von Dateien angeführt. Diese Gliederung hat den Vorteil, daß sie für Personen ohne ADV-Kenntnisse, die wir in diesen Bereichen in der Regel antreffen, geläufiger ist.

In diesem Zusammenhang sei die Arbeitsgruppe Datenschutz in der Benutzervereinigung SCOUT e.V. (Siemens-Computer-User-Team) erwähnt, die von einem Mitarbeiter meiner Geschäftsstelle geleitet wird und sich u.a. mit dem Problem der Nachprüfbarkeit des Ablaufs der Datenverarbeitung beschäftigte. Diese Arbeitsgruppe stellte einen Katalog von technischen Hilfsmitteln zur Überwachung einer ordnungsgemäßen Anwendung der Datenverarbeitungsprogramme zusammen. Einige der dort aufgezählten Hilfsmittel stehen bereits als Betriebssystemfunktionen zur Verfügung, manche Maßnahmen sind organisatorischer Art, die Mehrzahl der Vorschläge aber wird vom Hersteller nicht unterstützt. Eine Umfrage bei Rechenzentrumsleitern der Mitgliedsfirmen ergab, daß die meisten der fehlenden Hilfsmittel ins Betriebssystem integriert werden sollten.

5.3.3 Zugangskontrolle in Rechenzentren

In vielen Rechenzentren werden Daten gespeichert und verarbeitet, deren Mißbrauch die gesellschaftliche Stellung und die wirtschaftlichen Verhältnisse der Betroffenen - zum Teil erheblich - beeinträchtigen kann (Schutzstufe D, Datensicherungskatalog vom 30.7.1980). Dies gilt insbesondere für Rechenzentren, in denen eine Vielzahl von Bediensteten mit unterschiedlichen Aufgaben beschäftigt ist.

Es hat sich gezeigt, daß eine wirkungsvolle Zugangskontrolle nur mit einem automatischen Zugangskontrollsystem, das sowohl Zu- als auch Abgänge aufzeichnet, zu verwirklichen ist. Diese Aufzeichnungen sollen dabei aus Gründen des Datenschutzes lediglich als Nachweis der An- und Abwesen-

heit der im Rechenzentrum Beschäftigten dienen und die sonst üblichen manuell geführten Anwesenheitsaufzeichnungen im Rechenzentrum ersetzen. Bei den Überprüfungen solcher Rechenzentren habe ich deshalb stets eine Anwesenheitsaufzeichnung gefordert.

5.3.4 Maschinelle Verwaltung des Magnetbandarchivs

Die Bemühungen, die Computerhersteller zur Entwicklung wirksamer Dienstprogramme für die Verwaltung von Magnetbandarchiven zu bewegen, blieben bisher erfolglos. Viele Anwender, die umfangreiche Magnetbandarchive unterhalten, haben Eigenlösungen entwickelt, die zwar den gewünschten Zweck erfüllen, jedoch vielfach wartungsintensive Insellösungen darstellen.

In den vergangenen Jahren konnte durch die Entwicklung der Festplatte die Speicherkapazität von Magnetplatten ständig erhöht werden, so daß in modernen Großrechenzentren die Verarbeitung von Magnetbändern im laufenden Betrieb heute ständig abnimmt. Magnetbänder werden hauptsächlich noch für die tägliche Sicherung, die Auslagerung von Archivbeständen und für den Datenträgeraustausch benützt. Da Sicherungs- und Auslagerungsläufe nur zu ganz bestimmten Zeiten durchgeführt werden, stellt die Vollständigkeitskontrolle des Magnetbandarchivs in solchen Fällen kein zentrales Problem mehr dar. Magnetbandanforderungen im laufenden Betrieb beschränken sich in der Regel auf Arbeitsbänder, für die im allgemeinen ein gesonderter Bestand vorgehalten wird. Diese Tendenz spricht eigentlich dagegen, daß die Computerhersteller noch ein Magnetbandverwaltungssystem entwickeln werden.

Zur Frage der Organisation eines Magnetbandarchivs vertrete ich die Auffassung, daß aus der Sicht des Datenschutzes eine nummernorientierte Organisation des Magnetbandarchivs besser ist als eine dateiinhaltbezogene, weil aus einer neutralen Nummer nicht direkt auf die Datei und somit auf die Sensibilität der gespeicherten Daten geschlossen werden kann. Bei einer dateiorientierten Organisation läßt der Dateiname in den meisten Fällen Rückschlüsse auf das Verfahren und somit auf die Sensibilität der zu verarbeitenden Daten zu. Trotzdem gibt es auch Fälle, wo eine dateiorientierte Organisation Vorteile haben kann.

5.3.5 Maßnahmen zur Verbesserung des Zugriffsschutzes

In einer ADV-Anlage werden in der Regel personenbezogene Daten aus verschiedenen Aufgabenbereichen und unterschiedlicher Sensibilität gespeichert und verarbeitet. Moderne ADV-Systeme bieten für die Bearbeitung dieser Datenbestände Bildschirmgeräte an, so daß der Sachbearbeiter vom Schreibtisch aus die automatisiert gespeicherten Daten unmittelbar abfragen und bearbeiten, in vielen Fällen auch neue Daten direkt in das System eingeben kann. Es ist kein System dieses Funktionsumfanges bekannt, das nicht in irgendeiner Art und Weise einen gewissen Schutz gegen unberechtigten Zugriff gewährleistet. Das Sicherheitskonzept solcher Systeme besteht meistens darin, daß in einer Sicherheitsmatrix definiert wird, welche Benutzer mit welcher Anwendung (Transaktion) auf welcher Datenstation arbeiten können. In jeder Anwendung (Transaktion) ist außerdem festgelegt, welche Datei oder welcher Dateiausschnitt gelesen oder verändert werden kann. Für die Anzahl der möglichen Transaktionen, die in einem solchen System definiert werden können, gibt es keine spürbaren Begrenzungen. Viele Systeme führen für Kontrollzwecke automatische Aufzeichnungen (sogenannte LogProtokolle), aus deren periodischer Auswertung erkennbar wird, welche Benutzer mit welcher Häufigkeit welche Transaktionen aufgerufen haben, oder von welchem Bildschirm welche Transaktionen wie häufig aufgerufen wurden.

Zur Verbesserung der Datensicherungsmaßnahmen sollten die Betreiber solcher Systeme aus der Sicht des Datenschutzes grundsätzlich folgende Gesichtspunkte beachten:

- Moderne Bildschirmsysteme gestatten über die sogenannte Menue-Technik eine einfache Benutzerführung. Über benutzer spezifische Menues läßt sich steuern, daß jeder Benutzer nur die Anwendungen angezeigt bekommt, für deren Aufruf er berechtigt ist.
- Ein Schutz der Benutzerkennworte läßt sich nur dann erreichen, wenn diese in unregelmäßigen Zeitabständen geändert werden.
- Die automatisch mitgeführten Aufzeichnungen erfüllen nur dann ihren Zweck, wenn sie regelmäßig ausgewertet werden, damit Abweichungen vom laufenden Betrieb rechtzeitig entdeckt werden.

Vielfach wird gefordert, daß Bildschirmgeräte, wenn sie innerhalb einer Sitzung längere Zeit inaktiv sind, vom System automatisch in den sogenannten LOGOFF-Status zurückgesetzt werden. Eine inaktive Zeit wird von den Befürwortern dieser Forderung meist so gedeutet, daß der Benutzer das Bildschirmgerät verlassen hat, ohne sich vom System abzumelden. Da der Benutzer die Verarbeitung aber nur über seine individuelle Benutzerkennung erreicht hat, könnten Unberechtigte sich in solchen Fällen den aktiven Zustand des Bildschirmes zu nutze machen und beispielsweise einen gespeicherten Datenbestand abfragen oder sogar Datensätze verändern. Die Hersteller großer ADV-Systeme bieten keine Standards an, die dieses Problem befriedigend lösen. Es sind auch keine Anzeichen dafür erkennbar, daß eine solche zusätzliche Sicherung systemseitig unterstützt wird. In den meisten Fällen würde eine solche Funktion den Arbeitsablauf zu sehr behindern. Gerade dort, wo der Sachbearbeiter den Bildschirm bei der Fallbearbeitung benötigt, sind verfahrensbedingt durchaus längere „Denkpausen" üblich. Ein Zurücksetzen des Benutzers in den Ausgangszustand würde in solchen Fällen unnötigen System-Overhead bedeuten. Trotzdem bieten Hersteller kleinerer Systeme, etwa von Textsystemen, die Funktion des Zurücksetzens in den Ausgangszustand an, wenn der Bildschirmbenutzer bei der Funktionsauswahl längere Zeit nicht reagiert. Die Zeitspanne ist meist vom System standardmäßig vorgegeben, der Betreiber kann die Dauer dieser Zeitspanne aber ändern. In einem solchen Fall kann diese Funktion durchaus als sinnvoll erscheinen. Wie in anderen Fällen auch, ist bei der Entscheidung, ob das Vorhandensein dieser Funktion gefordert werden kann, stets das Umfeld, in dem ein ADV-System eingesetzt wird, mit zu berücksichtigen.

5.3.6 Versand von Unterlagen mit personenbezogenen Daten

Beim Versand von Unterlagen mit personenbezogenen Daten hat man grundsätzlich zwischen dem Versand von Unterlagen an den Betroffenen und dem Versand von einer Vielzahl von Fällen, beispielsweise vom Rechenzentrum an die speichernde Stelle, zu unterscheiden.

Als Versandart zwischen der speichernden Stelle und dem Betroffenen wird in der Regel die Briefdrucksache oder der Brief in Betracht kommen. Ob eine Sendung als Brief oder Briefdrucksache zuzustellen ist, hängt neben den postalischen Bestimmungen von der Sensibilität der Unterlagen ab, da Art. 15 Abs. 1 BayDSG auf die Verhältnismäßigkeit zwischen Aufwand und angestrebtem Schutzzweck ausdrücklich hinweist. Nicht nur die augenblickliche Haushaltslage zwingt die Verwaltung überall dort Geldmittel einzusparen, wo dies sachgerecht und vertretbar erscheint, sondern auch die Grundsätze ordnungsgemäßen Verwaltungshandelns verlangen unter Berücksichtigung von Angemessenheit und Verhältnismäßigkeit Sparsamkeit bei der Verwendung von Steuergeldern im

Verwaltungsvollzug. Es ist deshalb angebracht, für die Auswahl einer Datensicherungsmaßnahme auch eine Risikoanalyse durchzuführen. Dazu zwei Beispiele: Den Versand der Verbrauchsgebührenabrechnung als Briefdrucksache mit Punktverschluß halte ich in der Regel für ausreichend. Hingegen sind Lohnsteuerkarten in verschlossenem Briefumschlag zuzustellen, was auch von der Finanzverwaltung angeordnet worden ist.

Der Versand einer Datei, die eine Vielzahl von personenbezogenen Fällen beinhaltet, ist anders zu beurteilen, da sich, je höher die Fallzahl ansteigt, in der Regel auch das Gefährdungspotential erhöht. Liegen Daten in visuell lesbarer Form vor, wie es in einer EDV-Liste oder auf einem Mikro-Fiche der Fall ist, ist das Risiko einer unbefugten Nutzung größer, als wenn die Daten in codierter Form auf einem magnetisierbaren Datenträger aufgezeichnet sind. Nur in den wenigsten Fällen sind magnetisch aufgezeichnete Daten, die im Datenträgeraustausch von Rechenzentrum zu Rechenzentrum oder von der Datenerfassung zum Rechenzentrum gesandt werden, ohne Zusatzinformationen auswertbar. Zur Identifizierung wird meist ein internes Ordnungsmerkmal benötigt, so daß für Außenstehende ein konkreter Personenbezug schwer herzustellen ist. Bei der Festlegung von Datensicherungsmaßnahmen darf daher dieser Gesichtspunkt der Auswertbarkeit solcher Datenträger nur über ein besonderes Zusatzwissen nicht außer Acht gelassen werden. Wird für den Versand von sensiblem Datenmaterial, wie beispielsweise aus dem Sozial- oder medizinischen Bereich, der Postweg gewählt, gilt als Versandart der Wertbrief oder das Wertpaket mit Einzelnachweis in der Regel als ausreichend sicher. Nur in Ausnahmefällen wird man dieser Versandart den eigenen Kurierdienst vorziehen, nämlich dann, wenn der Transportweg in eigener Verantwortung kontrolliert werden muß. Der Kurierdienst erzielt aber nur die gewollte Wirkung, wenn das zu transportierende Gut dem Empfänger oder dessen Vertreter auch persönlich, in Fällen von besonders sensiblen Dateien sogar gegen Quittung, ausgehändigt wird. Bei der Einteilung des Kurierdienstes ist daher darauf zu achten, daß der Empfänger erreichbar ist.

5.3.7 Datenverarbeitung im Auftrag

In einigen Fällen mußte ich feststellen, daß manche Behörden bei der Datenverarbeitung außer Haus allzu sorglos vorgehen. In den meist mit Privatfirmen abgeschlossenen Verträgen fehlen Vereinbarungen über den Datenschutz und die notwendigen technischen und organisatorischen Datensicherungsmaßnahmen. Fünf Jahre nach Inkrafttreten der Datenschutzgesetze kann man Unkenntnis der Datenschutzbestimmungen nicht mehr als Rechtfertigung gelten lassen. Häufig erkennen öffentliche Auftraggeber, übrigens überwiegend aus dem kommunalen Bereich, nicht die Gefahren, die bei der Verarbeitung personenbezogener Daten im Auftrag entstehen können. Art. 3 Abs. 1 Bayer. Datenschutzgesetz verlangt vom Auftraggeber eine sorgfältige Auswahl des Auftragnehmers unter besonderer Eignung der von ihm getroffenen technischen und organisatorischen Maßnahmen zum Datenschutz.

Vor Vertragsabschluß sind daher dem Auftragnehmer grundsätzlich keine personenbezogenen Daten, auch nicht für Testzwecke, zu überlassen. Für vorbereitende Testläufe können jedoch, wie bei der Programmierung in eigener Verantwortung, solche Daten zur Verfügung gestellt werden, die keinen Rückschluß auf bestimmte Personen zulassen. Es hat sich allerdings gezeigt, daß Behörden ohne Datenverarbeitungserfahrung bei der Erstellung signifikanter Testdaten im allgemeinen überfordert sind. Dieses Problem läßt sich eigentlich nur dadurch lösen, daß auch die vorbereitenden Maßnahmen vertraglich geregelt werden.

Häufig fehlt in den Verträgen der Hinweis, daß die zur Verfügung gestellten personenbezogenen Daten ausschließlich für den Vertragsgegenstand genützt und an Dritte nur nach Weisung des Auftraggebers übermittelt werden dürfen. Bei Vertragsbeendigung sind alle Daten entweder zu löschen bzw. zu vernichten, oder an den Auftraggeber zurückzugeben. Darunter fallen selbstverständlich auch alle für die Datenverarbeitung notwendig gewordenen Kopien, Eingabebelege und Auswertungen, unabhängig auf welchem Datenträger diese aufgezeichnet sind.

5.3.8 Organisatorische Sicherungsmaßnahmen bei der Abwicklung des Publikumsverkehrs

Vor zwei Jahren besuchte ein Mitarbeiter eine Behörde, um dort die Datensicherungsmaßnahmen zu überprüfen. Diese Behörde baut nun einen Amtsbereich um, der viel Publikumsverkehr aufweist. Obwohl die Schalterhalle erhalten bleibt, wird nach den mir vorliegenden Plänen streng darauf geachtet, daß im normalen Schalterbetrieb Dritte über Art und Inhalt des Gesprächs zwischen Schalterbeamten und dem einzelnen Behördenbesucher nichts erfahren. Der Wartebereich wurde in einiger Entfernung von den Schaltern eingerichtet und die Schalter gegeneinander durch Sicht- und Schallblenden abgeschirmt. Darüber hinaus werden Diskretionsschalter angeboten, die sich außerhalb der Publikumszone befinden. Diese Vorgehensweise halte ich für beispielhaft und empfehlenswert.

Von Besuchern einer anderen Behörde wurde jedoch darüber geklagt, daß Wartende wegen mangelnder Schallisolation Patientengespräche sowie das jeweils folgende Diktat des Befundes verfolgen und verstehen konnten. Die betroffene Behörde schaffte zwischenzeitlich Abhilfe.

Im Rahmen eines lückenlosen Sicherungskonzepts sind auch in solchen Fällen organisatorische Maßnahmen gegen unbefugte Kenntnisnahme von personenbezogenen Daten zu treffen.

5.3.9 Datensicherungsmaßnahmen im medizinischen Bereich

In Ergänzung der Ausführungen im Dritten Tätigkeitsbericht (Textziff. 3.11.2), die sich in erster Linie auf manuelle Verfahren bezogen, werden im folgenden einige Orientierungshilfen für Datensicherungsmaßnahmen bei der automatisierten Verarbeitung von Patientendaten gegeben:

Grundsätzlich ist darauf zu achten, daß die in Art. 13 Abs. 4 Bayer. Krankenhausgesetz vorgezeichnete Trennung von Verwaltungs- und medizinischen Daten im Krankenhaus durchgeführt wird.

Die Gesamtheit der Datensicherungsmaßnahmen soll darauf abzielen, daß der Kreis der in die medizinischen Datensammlungen einsichtnehmenden Personen klein und überschaubar, d.h. im Bereich der behandelnden Ärzte und ihrer Gehilfen, bleibt. In automatisierten Verfahren läßt sich durch Benutzerkennwörter und Aufzeichnungen über die Verarbeitung von Patientendaten eine wirksame Zugriffskontrolle und die Überprüfung der Datenverarbeitung verwirklichen.

Die Zahl der Verfahren, in denen Diagnosedaten gespeichert und verarbeitet werden, ist allerdings noch gering. Die wenigen Fälle befinden sich fast ausschließlich im Universitätsbereich. Da in der Forschung für Korrelationsanalysen und Verlaufsstatistiken die Kenntnis von identifizierenden Merkmalen, wie Name und Adresse des Patienten, in aller Regel bedeutungslos ist, werden Name und Adresse des Patienten meistens in einer eigenen, physisch von den Diagnosedaten getrennten Datei gespeichert. Diese Segmentierung bewirkt eine Erschwerung der Zuordnung von Name und Adresse zu Diagnosedaten. Die Adreßdatei läßt sich gegen den Zugriff Unbefugter durch technische oder auch organisatorische Maßnahmen schützen, viel-

fach wird diese Datei gar nicht im Rechner gespeichert. Am besten ist es, diese Datei nicht im direkten Zugriff zu halten. Darüber hinaus ist die Gefahr eines Mißbrauchs einer reinen Anschriftendatei, die keinen Aufschluß über Art der Erkrankung des Betroffenen enthält, wesentlich geringer. Sollte im Einzelfall eine Zusammenführung von Adreß- und Diagnosedaten im automatisierten Verfahren erforderlich sein, kann dies technisch beispielsweise über ein internes Ordnungsmerkmal erfolgen. In manchen Fällen ist eine solche Zuordnung dann denkbar, wenn die Auswertung oder Überwachung der Diagnosedaten ergibt, daß zum Beispiel für eine Vorladung zu einer Vorsorgeuntersuchung ein Zugriff auf die Adreßdaten erforderlich ist.

Schließlich ist darauf zu achten, daß personenbezogene Unterlagen mit medizinischen Daten, die zur Vernichtung anstehen, unmittelbar durch Bedienstete der speichernden Stelle vernichtet werden. Die Vernichtungsart ist unerheblich, wenn sichergestellt ist, daß danach eine Kenntnisnahme durch Unberechtigte ausgeschlossen ist.

5.4 **Technische Einzelprobleme**

5.4.1 Fernwartung von Datenverarbeitungssystemen

Im Vierten Tätigkeitsbericht wurde unter der Textziffer 3.12.5 ausführlich über das Konzept der Hersteller zur Fernwartung von Datenverarbeitungssystemen berichtet und eine Reihe von Grundsätzen aufgestellt, die aus der Sicht des Datenschutzes gewährleistet sein müssen.

Die Analyse einiger Fernwartungssysteme der Hersteller zeigte, daß Befürchtungen, Hersteller könnten ohne Wissen des Kunden auf dessen Daten zugreifen, nicht der Wirklichkeit entsprechen, da stets vom Kunden einer ADV-Anlage Art und Umfang der Fernwartung festgelegt werden. Insgesamt fiel bei den technischen Kontrollen auf, daß viele Betreiber von Großrechenzentren, wenn überhaupt, dann nur von dem Teil der Fernwartung Gebrauch machen, der sich auf die Wartung im Hardware-Bereich bezieht. Große Rechenzentren ziehen die Wartung vor Ort der Fernwartung vor, da sie meistens über eigene Wartungstechniker des Herstellers verfügen.

Der Bundesminister des Innern veröffentlichte am 18.11.1982 die Ergebnisse einer Anwender-Umfrage zur Fernwartung. Von den knapp 160 Stellen, die sich an der Umfrage beteiligten, setzen lediglich 31% die Fernwartung ein. Die Akzeptanz scheint geringer zu sein, als es die Hersteller erhofften. Ein Fall von Mißbrauch ist nicht bekanntgeworden. Für viele Stellen hat die Wartung vor Ort - vor allem der Systemsoftware - nach wie vor eine sehr große Bedeutung. Bei einem DV-Hersteller soll sogar eine Trendwende bei der Fernwartung im Software-Bereich festzustellen gewesen sein: Das Konzept einer unmittelbaren Analyse von Softwarefehlersymptomen und Speicherauszügen durch die Fernwartungszentrale über Datenfernverarbeitung würde nicht weiterverfolgt, sondern durch eine „fernunterstützte" telefonische Softwarewartung beim Kunden ersetzt. Diese Vorgehensweise sei für den Kunden effektiver und für den Hersteller kostengünstiger. Gefahren durch die Fernwartung werden weniger hinsichtlich einer Offenbarung personenbezogener Daten gesehen, sondern darin, daß Dritten ein unkontrollierter Einblick in das Betriebsgeschehen, z.B. in die Systemauslastung, gewährt wird, was nicht nur zum Nutzen des Kunden ausgewertet werden kann. Schließlich wurden als Gründe gegen den Einsatz der Fernwartung auch noch geltend gemacht, daß Dritte die Fernwartungszentrale unberechtigt simulieren könnten und daß die Prüf- und Diagnoseprogramme gegen Mißbrauch nicht genug änderungssicher sind, was sich aber durch einen Paßwortschutz der Wartungssoftware erschweren läßt.

Grundsätzlich ist klarzustellen, daß im Rahmen der Fernwartung keine benutzereigenen Anwendungsprogramme untersucht werden. Treten Fehlersituationen im Betriebssystem und in der betriebssystemnahen Software auf, werden die Fehlerinformationen (einige wenige Bytes) in besonderen Systembereichen gesammelt, auf die die Fernwartung im Bedarfsfall zugreift. Diese Informationen enthalten keine Kundendaten und unterliegen deshalb nicht den Datenschutzgesetzen. Die Fernwartung greift für ihre Analysen nahezu ausschließlich auf den Hauptspeicherbereich zu, die Peripherie, z.B. Festplatten mit Kundendaten, wird nicht benötigt. Durch spezielle Diagnose-Programme ist die Wartung nämlich in der Lage, im Hauptspeicher Ein/Ausgabe-Prozesse zu simulieren. Komplette Hauptspeicherauszüge, die im laufenden Betrieb Kundendaten enthalten können, werden wegen der langen Übertragungszeiten ohnehin nicht zur Fernwartungszentrale übertragen. Im übrigen ist die Fernwartung hauptsächlich als vorbeugende Wartung zu sehen.

Für den Fall, daß für die Erklärung einer Fehlerursache der Zugang zu Kundendaten, wozu auch personenbezogene Daten gehören können, notwendig ist, eignen sich die Komponenten der Fernwartung weniger gut, so daß man in diesen Fällen die lokale Wartung vorzieht.

Aus der Sicht des Datenschutzes ist bei Einsatz der Fernwartung im Hardware- und im Software-Bereich darauf zu achten, daß Art und Umfang der Fernwartung so beschrieben sind, daß die Unterlagen für sachverständige Dritte verständlich sind. Die notwendigen technischen und organisatorischen Maßnahmen zum Datenschutz, wie sie im 4. Tätigkeitsbericht auf Seite 51 beschrieben sind, sind zu treffen und allen Beteiligten so bekannt zu machen, daß sie im Bedarfsfall die gewünschte Wirkung erzielen.

5.4.2 Registrierung von Gesprächsdaten bei Nebenstellenanlagen im Fernsprechverkehr

Zur Kostenstellenzuordnung von Dienstgesprächen und zur Abrechnung von Privatgesprächen werden im Fernsprechverkehr in zunehmendem Maße technische Einrichtungen eingesetzt, die Gesprächsdaten festhalten. Die aufgezeichneten Gesprächsdaten lassen sich entweder durch einen eigenen Gebührencomputer oder gegebenenfalls durch die vorhandene ADV-Anlage auswerten.

In der Regel werden folgende Gesprächsdaten aufgezeichnet:

- Rufende Nummer (Nebenstelle, Amtsleitung)
- Zielnummer
- Zeitpunkt des Gesprächs
- Gebühreneinheiten
- Kennzeichnung des Gesprächs (dienstlich/privat)

Einige Anbieter ermöglichen auch die Erfassung einer Kostenstelle oder eines identifizierenden Merkmales (Paßwort).

Für den Nebenstelleninhaber ist es in vielen Fällen äußerst hilfreich, wenn bei den Abrechnungen die Zielnummer mitausgedruckt wird, da er meistens nur anhand dieses Merkmales nachprüfen kann, ob er das ihm angelastete Ferngespräch auch geführt hat. Eine Überprüfung ist dann umso wichtiger, wenn mehrere Personen ein- und dieselbe Nebenstelle benutzen.

Die Untersuchung der meist verbreiteten Gebührenabrechnungssysteme hat gezeigt, daß die Standardkonfiguration die Aufzeichnung aller Gesprächsdaten vorsieht. Einige Hersteller bieten in Nachfolgeversionen aber auch Systeme an, bei denen der Umfang der aufzuzeichnenden Daten durch den Anwender, wie die verstümmelte Aufzeichnung der Zielnummer, festgelegt werden kann. Solche Systeme sind jedoch noch wenig verbreitet, da sie erstens teurer sind und

zweitens auch eine kompliziertere Handhabung voraussetzen, was insbesondere für den Einsatz von sogenannten Paßwörtern zutrifft.

Vom Hersteller der im Einsatz befindlichen Systemen kann deshalb von der Seite des Datenschutzes als Standartfunktion grundsätzlich nicht gefordert werden, die Zielnummer verstümmelt aufzuzeichnen. Zum Stand der Technik gehört jedoch die Möglichkeit einige Nebenstellen aus der generellen Aufzeichnung ganz herauszunehmen.

Für die Speicherungsdauer und Auswertung der Gesprächsdaten abzurechnender Privatgespräche sollte gelten:

- Private Ortsgespräche sollen - soweit sie überhaupt abgerechnet werden (viele Stellen sehen davon ab, da der Aufwand zu hoch ist) - auf den Abrechnungsunterlagen nicht einzeln sondern nur summarisch ausgewiesen werden.
- Für abrechnungspflichtige private Ferngespräche sollte bei den Auswertungen die Möglichkeit vorgesehen werden, die Zielnummer nicht in ihrer vollen Länge auszudrucken. Zur Kontrolle durch den Betroffenen genügen in der Regel die drei- bis fünfstellige Vorwahl und 2 - 4 Stellen der Rufnummer. Das bedeutet wiederum, daß ein Verfahren ungeeignet ist, das eine feste Anzahl von Stellen der Zielnummer auswirft. Bei Auslandsgesprächen ist es zweckmäßig zusätzlich die Länderkennung auszudrucken. Ist sich ein Betroffener im Zweifel, ob ein ihm angelastetes Gespräch dienstlich oder privat war, läßt sich die volle Zielnummer aus den maschinell gespeicherten Daten ermitteln.
- Nach der Abrechnung sind die aufgezeichneten Gesprächsdaten für private Ferngespräche unverzüglich zu löschen. Differenzfälle müßten gesondert abgewickelt werden. Sie dürfen nicht zum Hinausschieben der Löschung für die übrigen, abgerechneten Fälle dienen.
- Der Abrechnungszeitraum sollte in der Regel nicht länger als ein Monat sein. Auf diese Weise wäre zu erreichen, daß die Gesprächsdaten privater Ferngespräche maximal ein Vierteljahr gespeichert bleiben.

Der Betroffene ist auf alle Fälle vorher über Art und Umfang der Gesprächsdatenerfassung zu unterrichten, damit er gegebenenfalls private Ferngespräche, deren Registrierung er vermeiden möchte, nicht vom Dienstapparat aus führt. Problematisch bleibt jedoch die Registrierung der gewählten Rufnummer beispielsweise in Personal-Wohnheimen von Krankenhäusern, oder in Krankenhäusern hinsichtlich der Patienten, da hier die private Lebensführung im Vordergrund steht und ein Ausweichen auf öffentliche Sprechstellen nicht zugemutet werden kann.

5.4.3 Mikroverfilmung von Unterlagen mit personenbezogenen Daten

Immer häufiger machen Behörden bei der Archivierung von personenbezogenen Unterlagen von dem Medium „Mikrofilm" Gebrauch.

Bevor auf die Probleme der Datensicherung und deren Lösungsmöglichkeiten eingegangen wird, soll das technische Verfahren der Mikroverfilmung, insbesondere als Auftragsdatenverarbeitung, kurz erläutert werden.

Das zu verfilmende Gut wird meist in einem ersten Arbeitsgang von Klammern, Heftschienen und Ordnern befreit. Eine Vollständigkeitskontrolle ist in aller Regel wirkungslos, da der Auftraggeber selbst nicht in der Lage ist, den Nachweis über die Vollständigkeit des zu verfilmenden Gutes zu erbringen. Im übrigen empfiehlt es sich, daß die speichernde Stelle die Aufbereitung des Materials selbst vornimmt, da sie die Unterlagen auch auf deren Archivierungswürdigkeit überprüfen kann. Die Verfilmung erfolgt in einem zweiten Arbeitsgang. Die Erfassungskraft legt jedes zu verfilmende Schriftstück in eine Schiene, von der es automatisch in die Kamera zur Verfilmung eingezogen wird. Filmanfang und Filmende, Berichtigungen und Wechsel in der Person des Aufnehmenden werden auf dem Film markiert. Auf Standardformularen, die mikroverfilmt werden, wird u.a. das Datum der Mikroverfilmung und die Person des Aufnehmenden festgehalten. Schließlich ist es möglich, Vorgangsanfang und Vorgangsende zu kennzeichnen, was sich für die Wiederauffindung eines bestimmten Vorganges als nützlich erweisen kann. Die Kamera enthält ein Zählwerk, so daß die Anzahl der verfilmten Schriftstücke erfaßt wird.

Bei der Simplex-Aufzeichnung wird in der Regel ein Verkleinerungsfaktor von 20 - 24 angewandt. Die Simplexmethode ist nur dann anzuwenden, wenn das Schriftgut überwiegend auf der Vorderseite beschriftet ist. Bei der Duplexaufzeichnungsmethode werden Vorder- und Rückseite des Schriftgutes in einem Kameradurchlauf nebeneinander auf dem Film dargestellt. Der Verkleinerungsfaktor beträgt hier 30 - 50. Mit Spezialkameras läßt sich ein Verkleinerungsfaktor von 150 erzielen; auf einem quadratischen Mikrofilmstück von 4 x 4 cm sind dann ca. 1250 DIN A 4-Seiten aufgezeichnet (Ultrafiche). Die belichteten Filme werden anschließend in einem Entwicklungsgerät bearbeitet. Jeder Film wird nach der Entwicklung auf Vollständigkeit und Lesbarkeit überprüft. Bei der Lesbarkeitskontrolle wird das Gesamtbild geprüft und werden keine Einzelinformationen gelesen.

Das Medium Mikrofilm bietet außerdem die Möglichkeit, Filme ohne besondere Schwierigkeiten preiswert zu vervielfältigen. Duplikate können im Kontaktverfahren auf Silber- oder auf Diazo-Filmen hergestellt werden. Sind die auf Mikrofilm aufgezeichneten Informationen über Jahrzehnte oder unbefristet aufzubewahren, sollte nur der Silberfilm Verwendung finden. Von Diazo-Filmen lassen sich im Kontaktverfahren keine Duplikate gleicher Wiedergabequalität herstellen. Hingegen verändern auch Diazo-Fiches bei entsprechender Aufbewahrung ihre Qualität kaum.

Bei der Mikroverfilmung handelt es sich in der Regel um Auftragsdatenverarbeitung im technischen Sinne. Die rechtliche Einordnung dieses Vorgangs ist noch nicht endgültig geklärt. Bei der Mikroverfilmung ist demnach, sofern personenbezogene Daten in Dateien verarbeitet werden, entsprechend Art. 3 BayDSG der Auftragnehmer unter besonderer Berücksichtigung der Eignung der von ihm getroffenen technischen und organisatorischen Maßnahmen sorgfältig auszuwählen. Nach der Vollzugsbekanntmachung zum Bayer. Datenschutzgesetz Nr. 3.3 vom 12.9.1978 sollen im Regelfall öffentliche Stellen Aufträge zur Datenverarbeitung an Private nur dann vergeben, wenn die Daten nicht sensibler Art sind. Angaben über gesundheitliche Verhältnisse werden als sensible Daten betrachtet.

Unbeschadet der Klärung der rechtlichen Fragen, die mit einer eventuellen Offenbarung von Angaben im Zuge von Mikroverfilmung zusammenhängen, gebe ich zu den technisch-organisatorischen Maßnahmen zum Datenschutz folgende Anregungen:

- Führt eine andere Stelle die Verfilmung durch, ist eine schriftliche Regelung zugrunde zu legen. In einem solchen Vertrag ist für den Fall, daß Daten unbefugt zur Kenntnis genommen oder verwendet werden, eine empfindliche Vertragsstrafe zu vereinbaren.
- Falls eine Verfilmung vor Ort ausscheidet, sollte das Material, um Transportrisiken zu vermeiden, durch Bedienstete der Behörde zur Verfilmung angeliefert und nach der Verfilmung wieder abgeholt, also nicht dem Auftragnehmer zur Vernichtung belassen werden. Um möglichem Mißbrauch bei der Vernichtung des verfilmten Aktengutes vorzubeugen,

sollte die Behörde das überflüssig gewordene Aktengut in eigener Verantwortung vernichten.

- Es ist zu prüfen, ob die Verfilmung besonders sensiblen Materials durch einen behördeneigenen Bediensteten ständig überwacht werden könnte, was auch die Vollständigkeitskontrolle unterstützen würde.
- Bei der Aufzeichnung auf Mikrofilm ist darauf zu achten, daß die gängigen Konventionen eingehalten werden, wie Kennzeichnung von Filmanfang und -ende bzw. Vorgangsanfang und -ende, Aufzeichnung des Verfilmungsdatums mit Name des Verfilmenden.
- Ein unbefugtes Kopieren des Filmmaterials ist ebenfalls unter Vertragsstrafe zu stellen. Vom Auftragnehmer sind Maßnahmen zu fordern, die eine unbefugte Duplizierung des Filmmaterials weitgehend ausschließen.
- Bei der Auswahl der Verfilmungsfirma ist zu berücksichtigen, daß mit zunehmender Ortsferne der Firma das Risiko einer Zuordnung von personenbezogenen Daten zu bestimmten Personen erfahrungsgemäß abnimmt.
- Werden medizinische oder ähnlich sensible Daten verfilmt, ist zu prüfen, ob die Verfilmung nicht von der speichernden Stelle selbst oder einer anderen öffentlichen Stelle vorgenommen werden kann.

6. Datenschutzregister

Die Zahl der zum Datenschutzregister gemeldeten automatisierten Dateien stieg bis zum Ende des Berichtszeitraums weiter an. Bis 1. Oktober 1982, dem Redaktionsschluß des 1. Nachtrags zur Übersicht über das Datenschutzregister, hatten 3 676 öffentliche Stellen insgesamt 12 341 Dateien gemeldet. Gegenüber dem Vorjahr bedeutet das bei den Dateien wie auch bei den speichernden Stellen eine Zunahme von ca. 9%. Die relative Zunahme ist gegenüber dem Vorjahr (12% bzw. 11%) damit leicht gesunken, die Gesamtzahl der Eingänge blieb seitdem in etwa konstant, so daß auch im Jahre 1983 mit einem weiteren Anstieg der Meldungen zu rechnen ist.

Als Beilage zum Bayer. Staatsanzeiger Nr. 44 vom 5.11.1982 wurde erstmalig ein Nachtrag zur Übersicht über den Inhalt des Datenschutzregisters veröffentlicht. Dieser Erste Nachtrag ergänzt die Übersicht vom 20.11.1981 (Beilage zum Bayer. Staatsanzeiger Nr. 47/1981) und berücksichtigt die Meldungen von speichernden Stellen, die vom 12.10.1981 bis 1.10.1982 eingegangen sind. Eine Neuauflage der Übersicht schien wegen des beträchtlichen Umfangs und der damit verbundenen hohen Druckkosten nicht zweckmäßig.

Bei Bürgeranfragen auf Auskunft über gespeicherte Daten wird dem Petenten eine Zusammenstellung der Dateien übersandt, in denen Daten über ihn gespeichert sein könnten. Diese Zusammenstellung enthält naturgemäß nur einen Bruchteil der zum Datenschutzregister gemeldeten Dateien. Besonders auffallend war, daß sich die Zahl der Bürgeranfragen an das Datenschutzregister gegenüber dem Vorjahr mehr als verdoppelte. Aus den Bürgerzuschriften habe ich im übrigen nach wie vor den Eindruck, daß trotz intensiver Aufklärungsarbeit die landläufige Meinung, der Datenschutzbeauftragte führe oder besitze einen Zugriff auf eine Datei, in der alle Daten über alle Bürger zusammengefaßt sind, immer noch weit verbreitet ist. Für die Arbeit meiner Geschäftsstelle ist das Register von großem Wert. Die Meldungen zum Datenschutzregister stellen für meine Mitarbeiter zur Vorbereitung der Kontrollen nach Art. 15 BayDSG eine wertvolle Hilfe dar. Außerdem ist das Register zusammen mit der Veröffentlichung der Übersicht ein wichtiges Mittel zur Herstellung der Transparenz der ADV der öffentlichen Verwaltung.

Eine Analyse der aus dem Kommunalbereich vorliegenden Meldungen ergibt, daß sich etwa 78% aller bayerischen Gemeinden bei der Abwicklung ihrer Aufgaben der automatisierten Datenverarbeitung bedienen. Besonders hoch ist der ADV-Einsatz im Einwohnerwesen und bei der Berechnung und Zahlbarmachung der Bezüge der Bediensteten. Die Entwicklung auf dem Gebiet der Mikrocomputer läßt erwarten, daß der Umfang der automatisierten Datenverarbeitung im Kommunalbereich weiter zunehmen wird. Dies gilt besonders für das Haushalts-, Kassen- und Rechnungswesen und die kommunalen Steuern, die sich besonders für eine automatisierte Unterstützung anbieten.

Auch im staatlichen Bereich wird die Zahl der dezentralen Kleinrechner in den nächsten Jahren ansteigen. Bei den Landratsämtern werden viele personenbezogene Dateien zur Zeit noch manuell in Form von Karteien geführt, die sich für eine Übernahme auf ein dezentrales ADV-System eignen könnten. In der Kfz-Zulassung laufen Piloteinsätze bei den Landratsämtern in Miesbach, München, Tirschenreuth und Wunsiedel. Im Krankenhausbereich ist zu beobachten, daß die Zahl der dezentral installierten Rechner ständig zunimmt. Zuwachsraten sind außerdem im Schulbereich, bei den Regierungen, bei den Vermessungsämtern und bei den Universitäten zu erwarten. Nahezu unberührt von der automatisierten Datenverarbeitung blieben bislang der Bereich der staatlichen Gesundheitsämter und der Forstbereich. Schließlich werden Kleinrechner zunehmend bei der Abrechnung von Telefongesprächen und für die Personalverwaltung durch die Personalstellen in sogenannten Personalinformationssystemen eingesetzt. Der vermehrte Einsatz von automatisierter Textverarbeitung und die Möglichkeit, auf Textsystemen in beschränktem Maße auch Dateiverarbeitung durchzuführen, wird die Anzahl der automatisierten Dateien, in erster Linie Adreßdateien, überdurchschnittlich anwachsen lassen.

Immer häufiger erreichen meine Geschäftsstelle Meldungen zum Datenschutzregister, die entweder unvollständig sind oder Formulierungen enthalten, die für ADV-Laien und Personen, die mit den Verfahren nicht vertraut sind, keinen Aussagewert enthalten. Gerade bei der Datensatzbeschreibung ist es wichtig, solche Formulierungen für die Datenarten zu wählen, die Anfragende erkennen lassen, welche Daten welcher Sensibilität in bestimmten Verfahren gespeichert und verarbeitet werden. Eine Datenbeschreibung in Form von nicht aussagefähigen Feldnamen, wie sie häufig in den Computerprogrammen verwendet werden, ist für die Meldung zum Datenschutzregister ungeeignet. Außerdem mußte ich feststellen, daß Anwender dezentraler Kleinrechner, die nicht im AKDB-Verbund arbeiten, bei der Ausfüllung der Meldeformulare große Unsicherheiten zeigen, so daß notwendige Rückfragen für meine personell nicht stark ausgestattete Geschäftsstelle eine zusätzliche Belastung darstellen.

7. Datenschutz beim Bayerischen Rundfunk

7.1 Bericht des Datenschutzbeauftragten

Wie bereits in früheren Tätigkeitsberichten dargelegt, ist in Art. 21 des Bayerischen Datenschutzgesetzes das Datenschutzrecht für den Bayerischen Rundfunk gesondert geregelt. Danach ist für die Kontrolle der Einhaltung des Bayerischen Datenschutzgesetzes und anderer Vorschriften über den Datenschutz bei der gesamten Tätigkeit des Bayerischen Rundfunks ausschließlich der Datenschutzbeauftragte des Bayerischen Rundfunks zuständig. Nach Art. 21 Abs.3 Satz 5 BayDSG hat dieser den Organen des Bayerischen Rundfunks jährlich einen Bericht über seine Tätigkeit zu erstatten und diesen dem Landesbeauftragten für den Datenschutz zu übermitteln. Dieser Verpflichtung ist er mit der Vorlage seines 4. Tätigkeitsberichts

für den Zeitraum vom 1. Januar bis 31. Dezember 1982 nachgekommen.

Folgende Schwerpunkte lassen sich diesem 4. Tätigkeitsbericht entnehmen:

Bezugnehmend auf seine Ausführungen im letztjährigen Tätigkeitsbericht über die datenschutzrechtlichen Aspekte eines Personaldatensystems (PDS) berichtet der Datenschutzbeauftragte des Bayerischen Rundfunks über die beabsichtigte Sachbearbeitung der Fehlzeiten der Mitarbeiter mittels EDV. Gegenstand seiner Überprüfung sei insbesondere die Notwendigkeit der Daten für die Sachbearbeitung gewesen; auch die Datensicherheit, insbesondere die Frage der Benutzer-, Zugriffs- und Speicherkontrolle, habe er geprüft. Diese Überprüfungen hätten keine Beanstandungen ergeben. Das Programm Fehlzeiterfassung habe auch seinen ersten Test bestanden. Mit ihm erfolge u. a. die Abrechnung der Essensmarken.

Der Datenschutzbeauftragte berichtet des weiteren über die Rechtsprobleme, die sich im Zusammenhang mit den von der Finanzverwaltung geforderten Kontrollmitteilungen über Honorarzahlungen an freie Mitarbeiter ergäben. Er schlägt ein verändertes Verfahren vor, das ohne zusätzlichen Verwaltungsaufwand zu einer datenschutzgerechten Lösung führe. Danach sollen nunmehr an Stelle der Finanzämter die einzelnen freien Mitarbeiter selber Mitteilungen über die Jahreshonorarabrechnungen erhalten, die inhaltlich den bisherigen Kontrollmitteilungen entsprächen. Die Finanzämter ihrerseits erhielten Listen mit Namen und Adressen der beschäftigten freien Mitarbeiter, jedoch ohne Mitteilung der Besteuerungsgrundlagen. Sofern sich den Finanzämtern hieraus ein Hinweis auf bisher unbekannte Steuerpflichtige ergäbe, können sie von diesen die Jahreshonorarabrechnungen anfordern.

Über die in seinem letzten Tätigkeitsbericht angekündigte Überprüfung der Datensicherheit im Rechenzentrum des Bayerischen Rundfunks durch einen unabhängigen Gutachter teilt der Datenschutzbeauftragte des Bayerischen Rundfunks mit, daß die Überprüfung durch den Technischen Überwachungsverein Bayern e. V. stattgefunden habe. Dieser habe den Stand der Datensicherungsmaßnahmen insgesamt - unter Berücksichtigung von Art und Umfang der gespeicherten Daten - als befriedigend bezeichnet. Die Überprüfung habe lediglich zwei Mängel ergeben: Zum einen sei die Regelung der Reinigung der RZ-Räume nicht akzeptabel, zum anderen konnte auch die Regelung der Entsorgung nicht mehr benötigter Computerlisten mit personenbezogenen Daten nach den im Verlauf der Untersuchung gemachten Feststellungen nicht als befriedigend bezeichnet werden. Der Datenschutzbeauftragte des Bayerischen Rundfunks will mit den angesprochenen Fachabteilungen versuchen, auf eine Beseitigung der Mängel und eine Realisierung der Empfehlungen hinzuwirken.

Unter der Überschrift „Datenschutz und Rundfunkgebühren" teilt der Datenschutzbeauftragte des Bayerischen Rundfunks mit, daß er im Hinblick auf die datenschutzrechtlichen Fragen von Rundfunkteilnehmern bei der Gebührenstelle ein Datenschutzmerkblatt für den Beauftragtendienst angeregt habe. Einige Bürger, die vom Beauftragtendienst der Gebührenstelle aufgesucht worden seien, seien unsicher gewesen, ob und über welche Daten sie dem Beauftragten Auskunft geben müßten.

Nachdem das Merkblatt dem Beauftragtendienst noch in diesem Jahr zur Verfügung stehen werde, sei jeder Beauftragte der Gebührenstelle damit in der Lage, den von ihm aufgesuchten Rundfunkteilnehmern das Merkblatt zu übergeben und somit für eine umfassende Aufklärung über seine und des Teilnehmers Rechte und Pflichten auch in datenschutzrechtlicher Hinsicht zu sorgen.

Der Datenschutzbeauftragte des Bayerischen Rundfunks stellt fest, daß er wiederum in einer Reihe von Einzelfällen entweder auf Anregung einzelner Mitarbeiter, einzelner Abteilungen des Bayerischen Rundfunks oder von Amts wegen tätig geworden sei und hierbei ein Grund zu formellen Beanstandungen nicht habe festgestellt werden können. Seine entsprechenden Hinweise hätten bei den zuständigen Stellen Beachtung gefunden. Es habe sich auch im Berichtszeitraum wieder als ausreichend erwiesen, für die Zukunft Maßnahmen zur Verbesserung des Datenschutzes zu empfehlen. Themen dieser Tätigkeit seien insbesondere gewesen:

- Übermittlung von Daten aus Pressedatenbanken,
- Veröffentlichung der Namen von Gewinnern bei Preisausschreiben und Lotterien.

Zum „Datenschutz bei der GEZ" berichtet der Datenschutzbeauftragte des Bayerischen Rundfunks, daß dies weiterhin ein Schwerpunkt der Tätigkeit der Rundfunkdatenschutzbeauftragten sei. Die von den Landesrundfunkanstalten und dem ZDF getragene GEZ hatten zum 31.12.1982 einen Bestand von 24.158.484 Hörfunkteilnehmern und 21.835.778 Fernsehteilnehmern zu verwalten. Die GEZ führte 4.078.961 Hörfunkteilnehmer des Bayerischen Rundfunks, von denen 260.520 gebührenbefreit waren. Als Fernsehteilnehmer des Bayerischen Rundfunks waren 3.687.355 gemeldet, von denen 195.734 gebührenbefreit waren.

Im Bereich des Bayerischen Rundfunks ergingen 156.632 Gebührenbescheide, gegen säumige Rundfunkgebührenzahler wurden 12.910 Vollstreckungen eingeleitet und gegen Schwarzseher und -hörer wurden 2.281 Anträge auf Verfolgung als Ordnungswidrigkeiten gestellt. Die Gesamtzahl dieser Maßnahmen sei im Vergleich zum Jahr 1981 nicht unbeträchtlich gestiegen, der Bayerische Rundfunk läge mit diesen Zahlen aber noch erheblich unter dem Durchschnitt innerhalb der ARD.

Die GEZ bearbeitet und beantwortet einfache Anfragen und sonstige Routineschriftwechsel selbständig. Im Jahr 1982 war die GEZ mit folgenden auf den Datenschutz bezogenen Anfragen und Reaktionen von Rundfunkteilnehmern befaßt:

11 Ersuchen von Rundfunkteilnehmern um Auskunft über gespeicherte personenbezogene Daten,
1 Anfrage von einem Teilnehmer, ob und ggfs. an wen die GEZ Rundfunkteilnehmerdaten übermittelt,
14 Fragen in Bezug auf die Herkunft von Adreßdaten bzw. die Berechtigung, Adressen bei Einwohnermeldebehörden oder der Deutschen Bundespost zu erfragen,
2 Anfragen bezüglich der Berechtigung, bestimmte Daten beim Teilnehmer zu erheben bzw. zu speichern,
1 Anfrage nach der Verwendung gespeicherter Teilnehmerdaten,
3 Verlangen, die Teilnehmerdaten nach erfolgter Abmeldung zu löschen,
23 Anfragen von natürlichen Personen, Behörden oder sonstigen Institutionen nach Daten Dritter (anderer Rundfunkteilnehmer),
2 Anfragen allgemeiner Art in Bezug auf den Datenschutz bei der GEZ.

Damit hätten die Anfragen mit datenschutzrechtlichem Bezug bei der GEZ im Vergleich im Vorjahr etwas abgenommen.

In seiner Zusammenfassung weist der Datenschutzbeauftragte des Bayerischen Rundfunks darauf hin, daß die Zahl der Auskunftsersuchen und der sonstigen Reaktionen von Rundfunkteilnehmern und Dritten zu Fragen des Datenschutzes sich im Jahre 1982 im Vergleich zum Vorjahr etwas verringert habe. Die Gründe hierfür sieht er insbesondere in einer Verbesserung des Datenschutzes in den vergangenen Jahren beim Rundfunkgebühreneinzugsverfahren. Im übrigen hebt er besonders her-

vor, daß es auch im Jahre 1982 keinen Anlaß für eine förmliche Beanstandung gegeben habe.

7.2 Datenübermittlung an den Bayer. Rundfunk

Mehrfach haben sich Bürger an mich gewandt, die von Beauftragten des Bayer. Rundfunks aufgesucht worden waren oder aber schriftliche Aufforderungen vom Bayer. Rundfunk erhalten hatten, weil sie kein Fernsehgerät angemeldet hätten.

Meine diesbezüglichen Ermittlungen, wie der Bayer. Rundfunk Anschriften von Bürgern erhalte, die nicht Fernsehteilnehmer sind, haben ergeben, daß jedenfalls bei der Landeshauptstadt München eine regelmäßige Übermittlung der Daten aller Zuziehender an den Bayer. Rundfunk nicht erfolgt.

In einzelnen Fällen hatte der Beauftragte für die Einziehung der Rundfunkgebühren beim Bayer. Rundfunk von Gemeinden eine komplette Liste sämtlicher Einwohner ab vollendeten 18. Lebensjahr erbeten. Diese Liste sollte dem Abgleich mit den ihm von der Gebühreneinzugszentrale (GEZ) gelieferten Daten dienen.

Gegen eine derartige generelle Übermittlung von Einwohnerdaten aller über 18-jährigen an den Beauftragten des Bayer. Rundfunks habe ich grundsätzliche datenschutzrechtliche Bedenken. Offensichtlich sollen nämlich über ein sogenanntes „Raster" diejenigen Personen ermittelt werden, die entweder zurecht nicht gebührenpflichtig sind oder die der Gebührenpflicht nicht bzw. nicht ausreichend nachkommen. Meine Bedenken ergeben sich insbesondere daraus, daß die aus dem Raster fallenden Personen als potentielle Nichtzahler eingestuft und entsprechend gespeichert werden könnten. Letzteres muß auf alle Fälle vermieden werden. Außerdem dürfen die zum Zwecke eines Datenabgleichs zur Verfügung gestellten Einwohnerdaten nicht zum Aufbau eines - wenn auch verkürzten - Einwohnerregisters beim Beauftragten des Bayer. Rundfunks führen.

Andererseits verkenne ich grundsätzlich nicht die für den Bayer. Rundfunk bestehende Notwendigkeit, auch die Rundfunkteilnehmer zu erfassen, die bislang ihrer Zahlungspflicht nicht nachkommen.

Zwischenzeitlich sind mir noch weitere Datenanforderungen des Bayer. Rundfunks bekannt geworden; so z.B. Übermittlung sämtlicher Gewerbetreibendendaten aus dem Gewerberegister und Übermittlung der Daten sämtlicher Anschlußnehmer an einer kommunalen Gemeinschaftsantenne. Zweifel über die Zulässigkeit derartiger Datenübermittlungen werden auch nicht durch Art. 5 Abs. 4 Gebührenstaatsvertrag ausgeräumt, weil nach dieser Bestimmung für die Rundfunkanstalten nur ein Auskunftsrecht gegenüber unbekannten Gebührenpflichtigen begründet wird, wenn die begründete Vermutung besteht, daß ein Rundfunkgerät zum Empfang bereitgehalten wird, für das keine Gebühren an die GEZ entrichtet werden.

Die Konferenz der Datenschutzbeauftragten der Länder und des Bundes hat in ihrer Sitzung am 28. September 1982 zur Datenverarbeitung bei der Erhebung von Rundfunkgebühren diesbezüglich folgendes beschlossen:

„Die Informationshilfe öffentlicher Stellen für Rundfunkanstalten zur Feststellung unbekannter Gebührenpflichtiger darf die durch den Gebührenstaatsvertrag festgelegte Kompetenz- und Befugnisordnung nicht unterlaufen. Die Rundfunkanstalten haben nur ein Auskunftsrecht gegenüber unbekannten Gebührenpflichtigen, wenn eine begründete Vermutung besteht, daß ein Rundfunkgerät zum Empfang bereitgehalten wird (Art. 5 Abs. 4 Gebührenstaatsvertrag). Allein aufgrund der Tatsache, daß Personen einer bestimmten Personengruppe zugehören, ist eine solche Vermutung nicht begründet, wenn sonstige Anhaltspunkte fehlen. Deshalb ist die Übermittlung von Namen und Anschrift aller Gewerbetreibender aus dem Gewerberegister einer Gemeinde nicht zulässig, weil die Daten zur rechtmäßigen Aufgabenerfüllung nicht erforderlich sind."

Zur Klärung der anstehenden Probleme habe ich für die nächste Zeit ein Gespräch mit den Beteiligten vereinbart.

7.3 Befreiung von der Rundfunkgebührenpflicht

Im 4. Tätigkeitsbericht hatte ich darauf hingewiesen, daß ich bei Datenschutzkontrollen festgestellt hatte, daß Gemeinden eine sog. „Rundfunkgebührenbefreiungskartei" führen. Als datenschutzrechtlich von Bedeutung habe ich dabei empfunden, daß die Gemeinden neben der Speicherung der Daten bei der Gemeinde jeweils einen Abdruck des Bescheides über die Gebührenbefreiung an die Gebühreneinzugszentrale der Rundfunkanstalten (GEZ) versenden. Bezüglich der Rechtslage zu diesem Problem nehme ich auf meinen 4. Tätigkeitsbericht (S. 45/46) Bezug.

Die Konferenz der Datenschutzbeauftragten hat zu diesem Problem anläßlich ihrer Sitzung am 28. September 1982 folgende Entschließung gefaßt:

„Rundfunkgebührenbefreiung

1. Die Sensibilität der bei der Rundfunkgebührenbefreiung zu berücksichtigenden Sozialdaten erfordert eine eindeutige Aufgabenzuweisung durch Rechtsvorschrift, um den Gefahren einer unzulässigen Mischverwaltung vorzubeugen.
2. Haben die Gemeinden lediglich ein Vorschlagsrecht, sind sie nicht befugt, personenbezogene Daten in Form einer Rundfunkgebührenbefreiungsdatei vorzuhalten, da eine Vielzahl dieser Daten zur Erfüllung eigener Aufgaben der Gemeinden nicht erforderlich ist.
3. Sind die Gemeinden zur Entscheidung über die Gebührenbefreiungspflicht allein zuständig, dürfen die Rundfunkanstalten insbesondere keine unter das Sozialgeheimnis fallenden personenbezogenen Daten erhalten, da sie zur Aufgabenerfüllung nicht erforderlich sind. Es genügt die Mitteilung der Tatsache der Gebührenbefreiung. Dies gilt auch für die Datenweitergabe an GEZ. Die statistischen Auswertungen der GEZ können auch ohne personenbezogenen Meldungen durchgeführt werden."

Bereits in meinem letzten Tätigkeitsbericht hatte ich darauf hingewiesen, daß ich davon ausgehe, daß im Zusammenhang mit der vorgesehenen Novellierung der Verordnung über die Befreiung von der Rundfunkgebührenpflicht (GVBl. 1981, S. 74) das gesamte Verfahren der Rundfunkgebührenpflichtbefreiung und der damit zusammenhängenden Datenspeicherungen sowie -übermittlungen überprüft und ggf. neu geregelt werden. Bislang ist mir von einem Entwurf für diese Novellierung noch nichts bekannt.

Anhang 1: **Die Konferenz der Datenschutzbeauftragten zur Volkszählung 83**
(Beschluß vom 22.3.1983)

1. Die Konferenz beobachtet die wachsende Unruhe in der Bevölkerung über die bevorstehende Volkszählung 83. Die Datenschutzbeauftragten haben Verständnis für die Sorgen der Bürger. Die anhängigen Verfassungsbeschwerden geben Gelegenheit, die Verfassungsmäßigkeit der Volkszählung zu prüfen.

   Das Volkszählungsgesetz weist einige Unklarheiten und Schwachstellen auf. Die Konferenz erinnert deshalb an die schon 1979 von Datenschutzbeauftragten im Laufe des Gesetzgebungsverfahrens vorgebrachten Bedenken. Diese richteten sich vornehmlich gegen die Durchbrechung des Prinzips der Trennung von Statistik und Verwaltungsvollzug, insbesondere

- gegen die Verbindung einer statistischen Erhebung mit der Aktualisierung der Melderegister
- gegen die Übermittlung nicht anonymisierter Volkszählungs daten durch die Statistischen Landesämter an Dritte
- gegen die unklare Reichweite des Benachteiligungsverbotes.

Die Konferenz stellt fest, daß die Volkszählungserhebungsbogen den Bestimmungen des Volkszählungsgesetzes, des Bundesstatistikgesetzes und der Datenschutzgesetze nicht in allen Punkten entsprechen, und zwar weil

- nicht darauf hingewiesen wird, daß jeder Auskunftspflichtige einen eigenen Haushalts- und Wohnungsbogen ausfüllen kann, damit er nicht anderen Auskunftspflichtigen seine personen bezogenen Daten offenbaren muß
- der Hinweis auf das Verbot von Maßnahmen gegen den Auskunfts pflichtigen mißverständlich ist, da nicht jeglicher Nachteil für den Betroffenen ausgeschlossen werden kann
- der Namensteil von den sonstigen Daten nicht abgetrennt werden kann
- nicht auf die Freiwilligkeit derjenigen Angaben hingewiesen wird, zu deren Beantwortung keine Verpflichtung besteht.

2. Die Datenschutzbeauftragten haben sich seit langem bei den für die Durchführung der Volkszählung zuständigen öffentlichen Stellen für die Gewährleistung datenschutzrechtlicher Anforderungen eingesetzt. Die Konferenz begrüßt, daß entsprechende Maßnahmen in einem Teil der Länder bereits vorgesehen sind. Soweit die nachstehenden Anforderungen nicht bereits berücksichtigt sind, fordert die Konferenz:

   - Zähler dürfen nicht in unmittelbarer Nähe ihres Wohngebietes eingesetzt werden,
   - auf den Einsatz von Zählern, bei denen im Hinblick auf ihre dienstliche Tätigkeit Interessenkonflikte nicht auszu schließen sind, sollte verzichtet werden,
   - der Bürger muß auf sein Recht hingewiesen werden, den Volks zählungsbogen bei der Erhebungsstelle im verschlossenen Umschlag direkt zuzuleiten oder abzugeben, wenn er nicht wünscht, daß der Zähler von den Angaben Kenntnis erhält,
   - die Bürger sind darüber aufzuklären, daß niemand verpflichtet ist, seine Daten einem anderen Auskunftspflichtigen zu offenbaren; daher ist jedem Auskunftspflichtigen, sofern er dies verlangt, ein eigener Bogen auszuhändigen,
   - die Bürger müssen darauf hingewiesen werden, daß die Beantwortung der nachstehend genannten Fragen freiwillig ist

     Telefonnummer

     Fragen an Diplomaten und Angehörige ausländischer Streitkräfte, soweit sie über die diesbezügliche Zugehörigkeit hinausgehen

     Gründe für die Nichtzahlung von Löhnen und Gehältern (Arbeitsstättenbogen)

   - den Meldebehörden dürfen nur die zum Melderegistervergleich erforderlichen Daten zur Verfügung gestellt werden; es ist unzulässig, den Meldebehörden den kompletten Erhebungsbogen zugänglich zu machen,
   - eine Berichtigung des Melderegisters darf erst nach einem förmlichen melderechtlichen Verfahren erfolgen, in dem der Bürger Gelegenheit zur Äußerung erhält,
   - die Bürger müssen darüber aufgeklärt werden, daß das Verbot von Maßnahmen gegen den Betroffenen bei Melderegistervergleich kein striktes Verwertungsverbot darstellt, das jegliche Benachteiligung des Betroffenen nach Berichtigung des Melderegisters ausschließt,
   - außer für den Melderegistervergleich dürfen Gemeinden die Einzelangaben aus den Erhebungsbogen nicht für eigene Zwecke verwenden,
   - eine Datenübermittlung im Rahmen des § 9 Abs. 2 - 4 VZG darf nur im Rahmen des Erforderlichen stattfinden. In aller Regel dürfen nur statistische Ergebnisse übermittelt werden. Eine Übermittlung von Einzelangaben, insbesondere von Straße und Hausnummer, ist ausgeschlossen, wenn die Übermittlung aggregierter Daten ausreicht.
   - Im Rahmen von § 9 Abs. 2 VZG dürfen Einzelangaben nur für statistische und planerische Zwecke übermittelt werden. Deshalb läßt das VZG nicht zu, daß z.B. Polizei, Verfassungsschutz, Sozialbehörden und Finanzämter Einzelangaben erhalten.
   - Im Rahmen von § 9 Abs. 3 VZG dürfen den Gemeinden Einzelangaben nur für eine bestimmte statistische Aufbereitung zur Verfügung gestellt werden. Die Übermittlung muß auf die für die jeweilige statistische Aufbereitung erforderlichen Angaben beschränkt werden; dazu gehört in keinem Fall der Name.
   - Die Statistischen Landesämter haben in jedem Einzelfall zu prüfen, ob die angeforderten Daten zur Erfüllung des angegebenen und zulässigen Zwecks erforderlich sind.
   - Der zuständige Datenschutzbeauftragte ist über alle Übermittlungen von Einzelangaben aus der Volkszählung durch die statistischen Ämter des Bundes und der Länder zu unterrichten.
   - Die Erhebungsunterlagen sind nach Übernahme der Daten auf elektronische Datenträger, spätestens jedoch Ende 1984 zu vernichten. Gleichzeitig sind Kennummer und Zählerlistennummer zu löschen.

3. Die Datenschutzbeauftragten werden verstärkt Kontrollen bei der Ausführung des VZG durchführen. Sie werden dabei insbesondere

   - die Erhebung der Daten,
   - das Verfahren des Melderegistervergleichs,.
   - die Aufbewahrung, Auswertung und Vernichtung der Erhebungsunterlagen bei den Statistischen Landesämtern sowie die Übermittlung statistischer Einzelangaben und ihre Verwendung beim Empfänger

   prüfen und die Öffentlichkeit über die Ergebnisse der Prüfungen unterrichten.

   Wird diesen Forderungen der Datenschutzbeauftragten Rechnung getragen, so sind nach ihrer Überzeugung die Sorgen der Bürger im wesentlichen unbegründet.

Stichwortverzeichnis

zum 5. Tätigkeitsbericht des Bayerischen
Landesbeauftragten für den Datenschutz