Bayerischer Landtag
13. Wahlperiode

Drucksache 13/**390**

07.02.95

Sechzehnter Tätigkeitsbericht des Landesbeauftragten für den Datenschutz

Berichtszeitraum 1994

Der Landesbeauftragte für den Datenschutz
Nr. DSB/1 -510-17

München, 7. Februar 1995

An den
Präsidenten
des Bayerischen Landtags
Herrn Johann Böhm
München

Sechzehnter Bericht über die Tätigkeit des Landesbeauftragten für den Datenschutz

Sehr geehrter Herr Landtagspräsident!

In der Anlage übersende ich gern. Art. 30 Abs. 5 des Bayerischen Datenschutzgesetzes den sechzehnten Bericht über die Tätigkeit des Landesbeauftragten für den Datenschutz.

Mit freundlichen Grüßen

Reinhard Vetter

Inhaltsübersicht Seite

1. Vorbemerkungen

1.1 Der Wechsel im Amt

Am 1. April 1994 habe ich mein Amt angetreten, nachdem der Bayerische Landtag meiner Berufung mit Beschluß vom 9.3.1994 zugestimmt hatte.

Ich bin in den ersten Tagen meiner Amtsführung vielfach gefragt worden, wie ich mir meine Amtsführung vorstelle und welche Position ich zu den Problempunkten vertrete, die mein Vorgänger im Amt, Herr Sebastian Oberhauser, aufgeworfen hat.

Ziel dieses Berichts ist es, auch auf diese Fragen Antwort zu geben. Aus diesem Grund lege ich, ungeachtet des durch die Neufassung des Bayerischen Datenschutzgesetzes eingeführten zweijährigen Berichtsturnus, nunmehr bereits im Dezember 1994 den 16. Tätigkeitsbericht des Bayerischen Landesbeauftragten für den Datenschutz vor. Da es der erste Bericht unter meiner Federführung ist, mögen dem sachkundigen Leser manche Ausführungen als selbstverständlich erscheinen. Ich bitte um Verständnis, daß ich sie zur Standortbestimmung gleichwohl in dieser Form aufgenommen habe.

1.2 Funktion des Datenschutzbeauftragten

Bei der Frage nach der Funktion des Datenschutzbeauftragten sind für mich zwei Punkte entscheidend:

a) Im Gesetzesvollzug ist Datenschutz Aufgabe aller Stellen der vollziehenden Gewalt (Art. 20 Abs. 3 **GG).**

   Das Bayerische Datenschutzgesetz weist deshalb in Art *25* u. a. allen obersten Dienststellen des Staates, den Gemeinden, Gemeindeverbänden und sonstigen der Aufsicht des Staates unterstehenden juristischen Personen die **Pflicht zu, die Beachtung der Vorschriften über den Datenschutz sicherzustellen.** Datenschutz ist also nicht nur Sache des Datenschutzbeauftragten, sondern aller genannten öffentlichen Stellen.

b) Dem Landesbeauftragten für den Datenschutz obliegt nach dem Datenschutzgesetz, Art. 30 Abs. 1 Satz 1 BayDSG, die **Kontrolle** bei den öffentlichen Stellen, daß die Vorschriften über den Datenschutz, d.h. die Bestimmungen zum Schutz des informationellen Selbstbestimmungsrechts des Bürgers, eingehalten werden. Datenschutz ist **Grundrechtsschutz.**

Als Landesbeauftragter für den Datenschutz ist mir damit ein Wächteramt mit der Verantwortung übertragen, durch Kontrollen für den Schutz des informationellen Selbstbestimmungsrechts des Bürgers und damit für seine entsprechenden Grundrechte einzutreten.

Das Gesetz verleiht entsprechend den Ausführungen des Bundesverfassungsgerichts in seinem Volkszählungsurteil (E *65,* 1(46)) zur Bedeutung der Beteiligung unabhängiger Datenschutzbeauftragter für einen effektiven Schutz auf informationale Selbstbestimmung die zur Ausführung dieses Amtes notwendige Unabhängigkeit (Art. 29 Abs. 2 Satz 1 BayDSG).

Das Bayerische Datenschutzgesetz begrenzt meine Kontrollbefugnis allerdings in zwei Punkten:

Soweit personenbezogene Daten in Akten verarbeitet und genutzt werden, ist meine Kontrollzuständigkeit nur bei hinreichenden Anhaltspunkten für eine Rechtsverletzung gegeben (Art. 30 Abs. 1 Satz 2 BayDSG).

Die zweite Einschränkung betrifft die Datenerhebung durch Strafverfolgungsbehörden. Hier ist meine Kontrolle erst nach Abschluß des Strafverfahrens zulässig (Art. 30 Abs. 4 Satz 1 BayDSG); soweit die Datenerhebung gerichtlich überprüft wurde, entfällt die Datenschutzkontrolle (Art. 30 Abs. 4 Satz 2 BayDSG).

Zur Frage, inwieweit bei diesen Einschränkungen eine effektive Kontrolltätigkeit möglich ist, äußere ich mich unten (siehe Ziff. *1.5.* und 1.7).

1.3 Datenschutz und Verwaltungseffektivität - ein Gegensatz?

In Politik und Verwaltung wird - mehr oder weniger und mehr oder weniger offen - gelegentlich der Vorwurf erhoben, Datenschutz behindere die Effektivität der Verwaltung. Für den Polizei- und Strafverfolgungsbereich geistert sogar das böse Wort vom Datenschutz als Tatenschutz (- manchmal verbrämt als ,,Datenschutz darf nicht zum Täterschutz werden"-) durch die Diskussionen.

Diese Vorwürfe sind bei richtigem Verständnis des Verhältnisses von Datenschutz und Verwaltungshandeln unberechtigt:

Mehr als zehn Jahre nach dem Volkszählungsurteil des Bundesverfassungsgerichts sollte heute allgemein akzeptiert sein, und ist es weitgehend auch, daß die Erhebung und Verarbeitung personenbezogener Daten als Grundrechtseingriff einer gesetzlichen Grundlage bedarf.

Begrenzungen des informationellen Selbstbestimmungsrechts durch förmliche Gesetze sind vom einzelnen hinzunehmen, wenn und soweit sie im überwiegenden Allgemeininteresse geboten sind. In diesem Rahmen sind gesetzliche Beschränkungen des informationellen Selbstbestimmungsrechts möglich und notwendig. Der Datenschutz steht diesen notwendigen gesetzlichen Eingriffbefugnissen nicht entgegen. Der Vorwurf, Datenschutz behindere z. B. **die erforderlichen** Vorschriften zur Verbrechensbekämpfung, ist deswegen unberechtigt.

Allerdings muß sich der Gesetzgeber, wie ausgeführt, auf **das Erforderliche beschränken** und die Regelungen müssen verhältnismäßig sein, d.h. der Eingriff darf gegenüber dem angestrebten Erfolg nicht außer Verhältnis stehen.

Bei meinen Stellungnahmen gegenüber den an Gesetzgebungsvorhaben Beteiligten fordere ich die obigen Begren-

zungen ein, soweit aus meiner Sicht Verbesserungen bezüglich des Datenschutzes notwendig sind. Dabei berücksichtige ich die Anforderungen der Praxis.

Die Staatsregierung hat meine Forderungen zu dem am 1.7. in Kraft getretenen Gesetz zur Änderung des Bayerischen Verfassungsschutzgesetzes in vollem Umfang übernommen. Dagegen wurden meine Stellungnahmen zu anderen Gesetzen im Sicherheitsbereich - zu nennen sind hier z. B. das inzwischen in Kraft getretene Verbrechensbekämpfungsgesetz und der Gesetzentwurf der Staatsregierung für ein Ergänzungsgesetz zum Gesetz zur Bekämpfung der Organisierten Kriminalität - nicht, oder jedenfalls bis jetzt nicht berücksichtigt.

Die Frage nach dem Verhältnis von Datenschutz und Verwaltungseffektivität stellt sich auch bei der **Anwendung der Regelungen,** die Vorschriften über die Zulässigkeit und den Umfang von Datenerhebungen und -verarbeitungen enthalten.

Diese Regelungen finden sich nicht nur in allgemeinen oder bereichsspezifischen und -typischen Datenschutzvorschriften (z. B. Bayerisches Datenschutzgesetz, X. Buch Sozialgesetzbuch, oder die Art. 30, 31 Polizeiaufgabengesetz (PAG) und die Datenabgleichsregelung des § 98 a ff. Strafprozeßordnung - Rasterfahndung), sondern auch in **Befugnisnormen, die materiell zu Datenerhebungen** berechtigen, wie z. B. die Art. 13 und 14 PAG (Identitätsfeststellungen, erkennungsdienstliche Maßnahmen) oder zahlreiche Bestimmungen der Strafprozeßordnung, wie z. B. die §§ 81 b (Lichtbilder, Fingerabdrücke) oder 100 a (Überwachung des Fernmeldeverkehrs).

Bei der Anwendung der genannten Bestimmungen, insbesondere bei der Auslegung von unbestimmten Rechtsbegriffen, müssen nach meinem Verständnis die Fachkompetenz der zuständigen Behörden und die Bedürfnisse der Praxis auch von der Seite des Datenschutzes respektiert und in die eigene Meinungsbildung einbezogen werden. Das war in Bayern immer gegeben. Ich werde die Linie eines praxisgerechten, die Notwendigkeiten der Exekutive berücksichtigenden Datenschutzes beibehalten.

Diese Sichtweise ändert nichts an der Wächterfunktion des Datenschutzes. Beispiele hierfür können dem nachfolgenden Bericht entnommen werden.

1.4 Die bei Amtsübernahme bestehenden Problempunkte

Mein Amtsantritt war durch einige ungeklärte Fragen von Gewicht gekennzeichnet.

Mein Vorgänger im Amt hatte zu dem seinerzeitigen Entwurf eines Änderungsgesetzes zum Bayerischen Verfassungsschutzgesetz, durch den u. a. dem Landesamt für Verfassungsschutz die Aufgabe der Vorfeldbeobachtung der Organisierten Kriminalität übertragen werden und durch den das Amt die Befugnis zu technischen Überwachungsmaßnahmen im Schutzbereich des Art. 13 GG erhalten sollte (,,Großer Lauschangriff"), gerügt, daß zum einen die Zielrichtung der technischen Überwachungsmaßnahmen nicht hinreichend bestimmt sei, daß zum anderen der Befugniskatalog für den verdeckten Einsatz besonderer technischer Mittel in Wohnungen nicht abgeschlossen sei. Weiter sei wegen der Beschränkung der Kontrollkompetenz des Datenschutzbeauftragten nach dem Bayerischen Datenschutzgesetz im Aktenbereich eine unabhängige Kontrolle dieser Eingriffe nicht gewährleistet.

Schließlich hatte sich mein Vorgänger im Amt gegen die in Art. 30 Abs. 4 BayDSG enthaltene Begrenzung gewandt, wonach die Kontrollbefugnis des Datenschutzbeauftragten für Datenerhebungen im Strafverfahren auf die Zeit nach Abschluß des Strafverfahrens aufgeschoben ist.

Ich habe die Kritikpunkte zum Änderungsgesetz zum Bayerischen Verfassungsschutzgesetz im wesentlichen geteilt und im Gesetzgebungsverfahren gefordert, zum einen die Zielrichtung der Datenerhebungsmaßnahmen festzulegen, zum anderen durch Streichung des Wortes ,,insbesondere" einen geschlossenen Straftatenkatalog in der Befugnisnorm für die genannten Erhebungsmaßnahmen vorzusehen. Beiden Forderungen wurde, wie oben bereits festgestellt, im Verlauf des Gesetzgebungsverfahrens Rechnung getragen.

Wegen der Kontrollkompetenz in Akten verweise ich auf die nachstehenden Beiträge. Jedenfalls war mir eine Kontrolle des Bereichs der Verarbeitung und Nutzung von durch Maßnahmen nach Art. 6 Abs. 4 BayVSG gewonnenen Daten de facto möglich.

Wegen der mit Fragen der Kontrollbefugnis verbundenen grundsätzlichen Probleme verweise ich wieder auf nachfolgenden Abschnitt 1.5.

Auf die Fragen des Umfangs der Kontrollmöglichkeiten im Justizbereich gehe ich in den darauffolgenden Abschnitten 1.6 und 1.7 ein.

1.5 Kontrollmöglichkeiten von Akten nach dem Bayerischen Datenschutzgesetz

1.5.1 Allgemeines

Das Bayerische Datenschutzgesetz unterwirft in Art. 30 Abs. 1 grundsätzlich die ,,öffentlichen Stellen" der Kontrolle des Landesbeauftragten für den Datenschutz hinsichtlich der Einhaltung der Vorschriften über den Datenschutz. Eine Beschränkung auf ,,Dateien" (oder Karteien) ist in Art. 30 Abs. 1 BayDSG nicht enthalten.

Eine Einschränkung für den Aktenbereich enthält, wie oben bereits ausgeführt, dagegen Art. 30 Abs. 1 Satz 2 BayDSG: Werden Daten ,,in Akten verarbeitet ...,,, kontrolliert der Landesbeauftragte für den Datenschutz nur, wenn ein entsprechender Anlaß vorliegt; dabei gehe ich mit der maßgeblichen Kommentaniteratur - Dammann in

Simitis/Dammann/Geiger/Mallmann/Walz, Kommentar zum BDSG, Anm. 15 zu § 24, und Wilde in Wilde/Ehmann/Niese/Knoblauch, Bayerisches Datenschutzgesetz, Kommentar und Handbuch, Anm. 3 zu Art. 30 - davon aus, daß diese Begrenzung nur dann gegeben ist, wenn die zu kontrollierenden personenbezogenen Daten **ausschließlich** in Akten verarbeitet werden. Werden die genannten Daten sowohl in **Akten wie in Dateien** (oder Karteien) verarbeitet, unterliegt auch die Verarbeitung dieser Daten **in Akten ohne Beschränkung auf die genannten Anlässe** meiner Kontrolle.

Ich habe meine Prüfungen nach diesen Maßstäben durchführen können.

1.5.2 Grundsätzliche Stellungnahme zu dieser Regelung

Diese Regelung des BayDSG, die der des Bundesdatenschutzgesetzes entspricht, ermöglicht bei vorgenannter Auslegung im allgemeinen sachgerechte und effektive Kontrollen, da die Aktenbestände immer mehr über Dateien erschlossen werden. In diesen Fällen kann die Datenverarbeitung in den Dateien und in dem Umfang, in dem die Daten auch in den Dateien enthalten sind, auch in den Akten kontrolliert werden, ohne daß es hierfür eines besonderen Anlasses bedarf. Das Gleiche muß meines Ermessens für Erkenntnisse von datenschutzrechtlicher Relevanz gelten, die mir bei dieser Gelegenheit zur Kenntnis gelangen.

1.5.3 Kontrollfragen im Sicherheitsbereich

Vorweg kann ich betonen, daß mich bei meinen Prüfungen die Sicherheitsbehörden, sowohl das Landesamt für Verfassungsschutz wie auch die von mir geprüften Pohzeistellen, in jeder möglichen Weise unterstützt haben. Diese Bereitschaft möchte ich an dieser Stelle ausdrücklich hervorheben.

Wie ich unten näher ausführen werde, ist nicht gewährleistet, daß alle Maßnahmen im Sicherheitsbereich für die m. E. aus verfassungsrechtlichen Gründen die Kontrolle durch ein unabhängiges Organ sichergestellt sein muß (vgl. das G 10-Urteil des Bundesverfassungsgerichts in E 67, 154 *(185))* - das sind im wesentlichen solche Eingriffe, die den Bürger erheblich berühren, die ihm vielfach nicht mitgeteilt werden und für die deshalb ein anderweitiger Rechtsschutz nicht besteht -, durch Dateien erschlossen sind. Nach dem Wortlaut des Bayerischen Datenschutzgesetzes könnte ich in diesen Fällen eine Kontrolle in den Aktenbeständen nur dann vornehmen, wenn ein entsprechender Anlaß gegeben ist. Ein derartiger Anlaß wird für mich in aller Regel aber nicht vorliegen, da wegen der verdeckten Verarbeitung weder Bürgerbeschwerden noch sonstige konkrete Hinweise gegeben sein werden.

Damit auch in diesen Fällen die notwendige Kontrolle nicht nur tatsächlich durchgeführt werden kann, sondern **auch auf sicheren rechtlichen Grundlagen steht, müßte zumindest für die genannten Bereiche meine Kontrollzuständigkeit auch auf Akten ausgedehnt werden, und zwar unabhängig davon, ob die entsprechenden Daten auch in Dateien verarbeitet werden.**

Eine entsprechende Abgrenzung wird allerdings sehr schwierig sein, so daß sich für mich schon die Frage stellt, ob es nicht zweckmäßiger wäre, wie in der ganz überwiegenden Mehrzahl der anderen Länderdatenschutzgesetze, die Einschränkungen für die Aktenkontrolle überhaupt fallen zu lassen.

1.6 Kontrolle der Staatsanwaltschaften

1.6.1 Allgemeines

Ich habe in mehreren Gesprächen mit dem Staatsministerium der Justiz die bei meiner Amtsübernahme strittig erscheinenden Fragen erörtert. Dabei konnte in wichtigen Punkten Einvernehmen über Verfahrensweisen bei Prüfungen erzielt werden, die den aus meiner Sicht bestehenden Prüfungsnotwendigkeiten gerecht werden.

Insbesondere besteht Einvernehmen darüber, daß mir die nach meiner Einschätzung für die Prüfung erforderlichen Akten in vollem Umfang zur Verfügung gestellt werden.

Die Frage der Prüfkompetenz in Akten konnte noch nicht abschließend erörtert werden, ich bin jedoch zuversichtlich, daß weitere Gespräche eine Annäherung in Richtung der vorstehend vertretenen Positionen bringen wird.

Im einzelnen verweise ich auf den Beitrag unter Nr. 7.3.1.

1.6.2 Prüfungserfahrung

Zusammenfassend kann ich hier feststellen, daß ungeachtet der im Hinblick auf die Aktenkontrolle noch bestehenden unterschiedlichen Betrachtungsweisen die praktische Prüfung einer Staatsanwaltschaft im erforderlichen Umfang durchgeführt werden konnte. Auch hier möchte ich die Bereitschaft der Staatsanwaltschaft hervorheben, mich bei der Prüfung in jeder Weise zu unterstützen.

1.7 Begrenzung der Kontrollzuständigkeit der Datenerhebung im Strafverfahren

Wie bemerkt sieht Art. 30 Abs. 4 BayDSG u.a. vor, daß die Kontrolle von Datenerhebungsmaßnahmen im Strafverfahren bis zu dessen Abschluß aufgeschoben ist

Ich sehe in dieser Regelung, die sich in keinem anderen deutschen Datenschutzgesetz findet, eine wesentliche Einschränkung der datenschutzrechtlichen Kontrollmöglichkeiten, die zum einen die Rechte des Betroffenen -bei dem es sich keineswegs immer um einen Straftäter handeln muß - erheblich beeinträchtigt, und für die zum anderen eine sachliche Notwendigkeit für mich nicht ersichtlich ist.

Die Kontrolle der Erhebungsmaßnahmen wird wegen der langen Dauer vieler Ermittlungsverfahren erheblich auf-

geschoben, eine gerichtliche Kontrolle findet vielfach schon deswegen nicht statt, weil zahlreiche Ermittlungsverfahren ohne gerichtliche Entscheidung eingestellt werden.

Die für die Regelung vorgetragenen Gründe der Effektivität des Strafverfahrens können aus meiner Sicht durch eine entsprechende Kontrollgestaltung und Formulierung der Mitteilung an den Betroffenen ausgeräumt werden. Ich habe zu diesen Fragen das Gespräch mit dem Staatsministerium der Justiz begonnen. Auch hierzu verweise ich im einzelnen auf nachstehenden Beitrag.

1.8 Schwerpunkte des Tätigkeitsberichts

Schwerpunkte des Berichts und meiner Tätigkeit, für deren Vorbereitung, Unterstützung und Wahrnehmung in laufenden Angelegenheiten ich meiner Geschäftsstelle danke, waren die Durchführung von Beratungen und Prüfungen, die Bearbeitung von Einzelfragen, teils auf Anfragen von Bürgern, teils auf Hinweise in der Presse hin, und schließlich Stellungnahmen im oder in Vorbereitung von Gesetzgebungsverfahren. Daneben habe ich an der 48. Konferenz der Datenschutzbeauftragten des Bundes und der Länder in Potsdam, sowie an der 16. Konferenz der Internationalen Datenschutzbeauftragten in Den Haag teilgenommen.

Ausführungen dazu sind im vorliegenden Tätigkeitsbericht aufgenommen, soweit sie über den Einzelfall hinaus von Bedeutung sind. Dabei weise ich darauf hin, daß der Tätigkeitsbericht auch als Kompendium dienen soll, das bei auftretenden Zweifelsfragen in der Praxis herangezogen werden kann. Auch diese Funktion war bei der Entscheidung maßgebend, welche Abschnitte in den Tätigkeitsbericht aufzunehmen waren.

1.8.1 .Beratungstätigkeit, Behandlung von Einzelfällen

Ich habe die Beratungstätigkeit bewußt an den Anfang dieses Abschnitts gestellt. Ich halte die Beratung für einen außerordentlich wichtigen Schwerpunkt unserer Tätigkeit. Rechtzeitige Beratung verhilft vielfach zu Lösungen, die sowohl den Erfordernissen des Datenschutzes, wie auch den Bedürfnissen der praktischen Verwaltung gerecht werden. Unnötige Konflikte können hier vielfach schon im Ansatz vermieden werden.

Es gibt natürlich auch Fälle, in denen die Absichten der Anfragenden bzw. die uns mitgeteilte oder bekanntgewordene Verwaltungspraxis mit den Anforderungen des Datenschutzes, d. h. des Rechts auf informationelle Selbstbestimmung, in Widerspruch stehen. Hier trägt unsere Beratung dazu bei, Verletzungen des informationellen Selbstbestimmungsrechts zu vermeiden.

Als Beispiele der Beratungstätigkeit und der Vielfalt von Einzelfällen nenne ich hier:

Im technischen Bereich ist von besonderer Bedeutung zum einen die Beratung bei Einrichtung von Datenverarbeitungskomponenten. Besonderes Schwergewicht wurde auf Fragen des Datenaustausches in öffentlichen Netzen gelegt. Zu nennen ist hier ein Pilotprojekt in der Steuerverwaltung, bei dem Daten der Einkommensteuer-erklärung von den steuerberatenden Stellen an die Rechenzentren der Finanzverwaltung automatisiert übermittelt werden. Meine Beteiligung ergab, daß dieses Projekt den Notwendigkeiten des Datenschutzes Rechnung trägt, einzelne meiner Vorschläge wurden übernommen.

Das technische Referat meiner Geschäftsstelle gibt im übrigen Hinweise zu baulichen und organisatorischen Maßnahmen, mit denen dazu beigetragen werden soll, daß Mängel insbesondere bei der Datensicherheit von Anfang an vermieden werden.

Nicht minder wichtig ist die Beratung im rechtlichen Bereich:

So habe ich, wie in früheren Jahren, durch meine Geschäftsstelle wiederum zu Datenschutzfragen bei medizinischen Forschungsprojekten Stellung genommen. Teils handelte es sich um die ausreichende Anonymisierung von Daten, die nicht personenbezogen benötigt wurden, teils um Fragen des Zugangs zu personenbezogenen Patientendaten (s. a. *15.* TB Nr.2.2).

Besonderes Interesse der Bürger bezog sich naturgemäß wiederum auf die Zulässigkeit der Speicherung ihrer Daten in polizeilichen Dateien oder auf die Zulässigkeit von Abfragen aus polizeilichen Dateien. Hier hat sich als Problem ergeben, daß in der Protokolldatei der Polizei kein Hinweis auf den Grund der polizeilichen Abfrage angegeben ist. Das erschwert die Kontrolle der Rechtmäßigkeit der Abfrage. Ich habe deshalb vorgeschlagen, **in Zukunft entsprechende Hinweise** aufzunehmen.

Als bedeutenderen Einzelfall erwähne ich hier das Anfertigen von Aufnahmen von Versammlungsteilnehmern durch die Polizei. Ich habe entsprechend § 12 a Versammlungsgesetz gefordert, daß nur solche Teilnehmer aufgenommen werden dürfen, von denen tatsächliche Anhaltspunkte die Annahme rechtfertigen, daß von ihnen erhebliche Gefahren für die öffentliche Sicherheit und Ordnung ausgehen.

Im Vorfeld der Wahlen 1994 hatte ich zahlreiche Anfragen von Gemeinden und Parteien sowie von Bürgern zur Zulässigkeit der Weitergabe von Meldedaten zur Wahlwerbung. Dazu kamen Anfragen von Bürgern und Gemeinden zu Problemen des Datenschutzes im Gemeinderat, z. B. wegen überflüssiger Mitteilungen von Bürgerdaten in öffentlicher Sitzung, und zur Zulässigkeit von gemeindlichen Umfragen. Häufiger haben sich Bürger über Kfz-Halterabfragen zur Kur- und Fremdenverkehrsbeitragsfestsetzung beschwert.

Ein weiterer Schwerpunkt bei der Beratung von Behörden lag im Bereich Arbeitnehmerdatenschutz/Personalwesen.

Die Anfragen bezogen sich meist auf Unsicherheiten oder Unklarheiten bei der Einführung von automatisierten
- Gleitzeiterfassungsverfahren,
- Telefongesprächsdatenerfassungsverfahren,
- Personalverwaltungssystemen.

In einigen Fällen hatte sich der zuständige Personalrat hilfesuchend an mich gewandt. Die Fälle konnten zufriedenstellend beantwortet werden.

Weiter lag ein Schwerpunkt bei der Beantwortung von Anfragen über den rechtmäßigen Umgang mit Schülerund Elterndaten durch die Schulen.

1.8.2 Prüfungstätigkeit

Wie ich in anderem Zusammenhang zu Sicherheitsbehörden und Staatsanwaltschaft bereits betont habe, ergaben meine Prüfungen, daß bei den von mir besuchten Dienststellen ein hohes Bewußtsein über Wesen und Funktion des Datenschutzes herrscht. Hieraus konnte ich das grundsätzliche Bemühen feststellen, den Notwendigkeiten und Erfordernissen des Datenschutzes Rechnung zu tragen.

Das konnte natürlich nicht ausschließen, daß in einzelnen Punkten, die manchmal durchaus wesentlich waren, die Prüfung datenschutzrechtliche Mängel oder solche der Datensicherheit ergeben hat.

Auch hier beginne ich wieder mit dem technischen Bereich:

Bei der Prüfungstätigkeit in diesem Gebiet habe ich durch mein technisches Referat erneut besonderen Wert auf die Dokumentation der Datenverarbeitung und ihre Revisionsfähigkeit gelegt. Durch Dokumentation und Revisionsfähigkeit wird gewährleistet, daß Eingabe- und Abfrageberechtigungen kontrolliert vergeben werden, und daß die Berechtigung der Verarbeitung und Nutzung kontrolliert werden kann. Dokumentation und Revisionsfähigkeit sind damit Kernvoraussetzungen eines effektiven Datenschutzes.

Ebenfalls, wie in den vergangenen Jahren, mußten auch im Berichtszeitraum vielfach Hinweise zu sonstigen Fragen der Datensicherheit, wie zu Identifikations- und Authentifizierungsverfahren oder zu baulichen Maßnahmen für Räume mit wichtigen DV-Komponenten gegeben werden.

Im rechtlichen Bereich sind als besondere Schwerpunkte zu nennen:

- Die Prüfung der Kassenärztlichen Vereinigung Bayerns und des Datenflusses zwischen Kassenärztlicher Vereinigung und gesetzlicher Krankenversicherung:

  Im Hinblick auf die Einführung der Krankenversicherungskarte (Versichertenchipkarte) durch die Krankenkassen wurde in diesem Jahr begonnen, die Datenerhebung durch die Kassenärztliche Vereinigung bei den Ärzten, die Verarbeitung der erhobenen arzt- und versichertenbezogenen Abrechnungsdaten in der Kassenärztlichen Vereinigung, die Weitergabe von Abrechnungsdaten zu Prüf- und Nachweis-zwecken an die gesetzliche Krankenversicherung, sowie die Verarbeitung dieser Daten bei Ortskrankenkassen zu überprüfen. Dabei ergab sich, daß dies ein sehr umfangreiches und schwierig zu durchdringendes Gebiet ist. Ganz erheblichen Aufwand erzeugt dabei das Nachvollziehen der einzelnen Datenverarbeitungs- und Datenübermittlungsvorgänge anhand der Vorschriften des V. Buches des Sozialgesetzbuches. Das liegt möglicherweise auch daran, daß diese Vorschriften überwiegend erst erlassen wurden, nachdem die entsprechenden Erhebungs-, Verarbeitungs-, Übermittlungs- und Prüfungsvorgänge in der Praxis bereits lange Zeit vollzogen wurden. Hervorzuheben ist die Beanstandung von versichertenbezogenen Datenübermittlungen von der Kassenärztlichen Vereinigung Bayerns an die gesetzlichen Krankenkassen entgegen der Vorschrift des §295 Abs. 2 SGB V, der für die Abrechnung der Vergütung grundsätzlich die fallbezogene, nicht die versichertenbezogene Datenübermittlung vorschreibt (s. unter Nr.3.2.1).

- Im Sicherheitsbereich die Prüfung des Einsatzes sogenannter besonderer Mittel der Datenerhebung und verdeckter Erhebungsmaßnahmen zur Strafverfolgung

  Hierunter sind längerfristige Observation, der verdeckte Einsatz technischer Mittel sowie der Einsatz verdeckter Ermittler zu verstehen. Die Prüfung sollte insbesondere ergeben, inwieweit das neue Bayerische Datenschutzgesetz notwendige Kontrollen ermöglicht. Leider muß ich für die Tätigkeit der Polizei als Strafverfolgungsbehörde feststellen, daß für die genannten Maßnahmen bei meinen Prüfungen kein Prüfansatz nach dem BayDSG gegcben war. Das Ergebnis der besonderen Erhebungsmaßnahmen hatte zum einen teilweise keinen Niederschlag in einer Datei gefunden, zum anderen handelte es sich um Strafverfolgungsmaßnahmen, die von mir wegen des Aufschubs der Datenschutzkontrolle im Strafverfahren nach Art. 30 Abs. 4 BayDSG jedenfalls derzeit nicht aufgegriffen werden konnten.

  Die Voraussetzungen für eine Anlaßkontrolle nach Art. 30 Abs. 1 Satz 2 BayDSG waren nicht gegeben. Maßnahmen im präventiven Bereich (PAG-Maßnahmen) waren bei einer von mir geprüften Stelle in Dateien dokumentiert. Über diese Dateien ergab sich für mich ein Prüfansatz. Ein derartiger Prüfansatz ist aber dann nicht gegeben, wenn die genannten Maßnahmen oder deren Ergebnisse nicht in Dateien dokumentiert werden.

  Damit hat sich gezeigt, daß in diesem besonders sensiblen **Bereich** die geltende Fassung des Bayerischen Datenschutzgesetzes eine **unabhängige Kontrolle nicht in vollem Umfang sicherstellt.** Ich verweise

dazu auf meine Eingangsbemerkungen zur Notwendigkeit der Änderung des Bayerischen Datenschutzgesetzes jedenfalls insoweit.

Im übrigen war auch im Berichtszeitraum wieder die Prüfung der Ordnungsgemäßheit der Datenverarbeitung und -nutzung durch die Polizei allgemein ein Schwerpunkt der Prüfungstätigkeit. Von Einzelpunkten abgesehen haben sich wesentliche Beanstandungen nicht ergeben.

Es ist mir im übrigen ein Anliegen darauf hinzuweisen, daß die regelmäßige Aufnahme des Polizeibereichs als besonderer Schwerpunkt in die Tätigkeitsberichte nicht auf ein besonderes Mißtrauen gegenüber der Polizei zurückzuführen ist. Ein solches Mißtrauen wäre nicht gerechtfertigt. Wie an anderer Stelle bereits betont, bemüht sich nach meinen Erkenntnissen die Polizei grundsätzlich in hohem Maße, die Forderungen und Notwendigkeiten des Datenschutzes zu erfüllen. Die Tatsache des besonderen Schwerpunkts ergibt sich vielmehr aus den Kriterien Umfang der Datenverarbeitung und -nutzung in diesen Bereichen, der Sensibilität der erhobenen Daten sowie der Intensität der Eingriffe und, daraus folgend, dem hohen Interesse der Bürger und der Öffentlichkeit an Fragen des Datenschutzes auf diesem Gebiet.

- Im allgemeinen Verwaltungsbereich wurden zwei Landratsämter, eine kreisfreie Stadt und zwei unmittelbar nachgeordnete zentrale Landesbehörden überprüft. Zu den Ergebnissen verweise ich auf die Einzelfeststellungen.

- Schließlich wurden das Statistische Landesamt und das Staatsarchiv Bamberg kontrolliert. Schwerpunkte waren beim Landesamt die Auswahl der Interviewer bei der Erhebung der statistischen Einzeldaten und beim Staatsarchiv die Frage der Schutzfristen.

  Hinsichtlich der Ergebnisse verweise ich ebenfalls auf die nachstehenden Ausführungen.

Die Wahrung des Rechts auf informationelle Selbstbestimmung ist im öffentlichen Bereich in Bayern im Grundsatz gewährleistet. Notwendig ist eine Verbesserung der Kontrollmöglichkeiten des Datenschutzbeauftragten im Sicherheitsbereich.

1.8.3 Stellungnahmen zu Gesetzgebungsverfahren

Ich habe im Berichtszeitraum zu zahlreichen Gesetzentwürfen Stellung genommen. Neben dem oben bereits behandelten Entwurf zur Änderung des Bayerischen Verfassungsschutzgesetzes waren dies

- im Sozial- und Gesundheitsbereich:

  Stellungnahmen zu Entwürfen für ein Bundeskrebsregistergesetz, Bestattungsgesetz, Transplantationsgesetz, ergänzende landesrechtliche Regelungen zum Schwangeren- und Familienhilferecht des Bundes und zum Gesetz über das öffentliche Versorgungswesen.

  Meine Vorschläge in diesem Bereich wurden für das weitere Gesetzgebungsverfahren aufgenommen, teilweise hat sie der Gesetzgeber überndmmen.

- Im Polizei- und Sicherheitsbereich:

  Stellungnahmen zum inzwischen in Kraft getretenen Verbrechensbekämpfungsgesetz, zum Bayerischen Bundesratsentwurf für ein Ergänzungsgesetz zum OrgKG, zum Entwurf der Bundesregierung für ein Bundeskriminalamtsgesetz und zu Entwürfen der Staatsregierung zur Änderung polizeirechtlicher Vorschriften, sowie zur Anderung des Bayerischen Meldegesetzes.

  Die Staatsregierung hat die datenschutzrechtlich begründeten Vorschläge zum Verfassungsschutzänderungsgesetz übernommen (vgl. Ziff. 6.3). Meine Hinweise zum Verbrechensbekämpfungsgesetz - im besonderen die Forderung nach gesetzlicher Klarstellung, daß mit der erweiterten Abhörmöglichkeit keine Aufgabenerweiterung für den BND verbunden ist - konnten im Vermittlungsverfahren zu dem genannten Gesetz nicht umgesetzt werden. Auf meine zum Entwurf eines OrgKG-Änderungsgesetzes erhobenen Forderungen (insbesondere Verwertungsverbot, Zeugnisverweigerungsrecht bestimmter Personengruppen; vgl. Ziff. 5.9) ist das Justizministerium bisher nicht eingegangen. Im Bereich der Änderung polizeirechtlicher Vorschriften hat die Staatsregierung meine Forderung nach Konkretisierung der örtlichen Erweiterung der polizeilichen Befugnis zur verdachtsunabhängigen Identitätsfeststellung („Durchgangsstraßen") nur teilweise übernommen. Nicht berücksichtigt wurden meine Forderungen, die Kontrollen auf „sonstigen" Durchgangsstraßen von der Entscheidung des Dienststellenleiters abhängig zu machen und den Kontrollzweck auf die Bekämpfung der grenzüberschreitenden Kriminalität von erheblicher Bedeutung zu beschränken. Der Entwurf ist inzwischen in Kraft getreten. Ich werde den Vollzug aufmerksam beobachten.

- Im Justizbereich:

  Stellungnahmen zu einem u.a. von Bayern eingebrachten Bundesratsentwurf für ein Strafverfahrensänderungsgesetz, zu Entwürfen der Bundesregierung für ein Registerverfahrensbeschleunigungsgesetz (Grundbuchrecht), für eine zweite Zwangsvollstreckungsnovelle und für ein Gesetz zum Schuldnerverzeichnis und für die entsprechende Verordnung sowie für das inzwischen im Bundesgesetzblatt veröffentlichte Prozeßkostenhilfeänderungsgesetz.

  Weiter habe ich die in weiten Teilen noch fehlenden übrigen bereichsspezifischen Datenschutz-Regelungen im Justizbereich angemahnt. Im besonderen habe ich

für das vom Staatsministerium der Justiz beabsichtigte zentrale staatsanwaltschaftliche Verfahrensregister (BaySIS) die Schaffung einer besonderen Rechtsgrundlage gefordert.

Das Staatsministerium der Justiz hat meine Vorschläge zu den oben angegebenen Entwürfen im zivilprozeßrechtlichen Bereich übernommen. Nicht angeschlossen hat es sich meinen Vorschlägen zum Strafverfahrensrecht zum Grundbuchrecht, sowie meiner Forderung nach einer besonderen Rechtsgrundlage für BaySIS. Ich betrachte diese Diskussion jedoch noch nicht als abgeschlossen.

Im einzelnen verweise ich auf nachstehende Abschnitte.

1.9 Neues Datenschutzrecht

Das Inkrafttreten des **neuen Bayerischen Datenschutzgesetzes** am 1. März 1994 gibt Anlaß, die wichtigsten Neuerungen nochmals in Erinnerung zu rufen:

- Das Gesetz gilt - wie auch das Bundesdatenschutzgesetz, in erheblichem Umfang nicht nur unmittelbar für die Behörden, sondern auch für Vereinigungen **öffentlicher Stellen** in privater Rechtsform, die Aufgaben öffentlicher Verwaltung wahrnehmen (Art. 2).

- Das Gesetz ist auch auf den Umgang mit personenbezogenen **Daten** in Akten anzuwenden, wobei unter Akten alle Arten dienstlicher Unterlagen zu verstehen sind, wie z.B. auch Bild- und Tonträger, nicht jedoch Vorentwürfe oder Notizen, die nicht Bestandteil eines Vorgangs werden sollen (Art. 4). Die Datenschutzkontrolle in Akten setzt nach dem Gesetz allerdings voraus, daß Anhaltspunkte für Verletzungen des Datenschutzrechts vorliegen (Art. 30), soweit die Daten ausschließlich in Akten und nicht auch in Dateien gespeichert sind.

Über die damit verbundenen Probleme im Sicherheitsbereich habe ich unter Nr.1.5.3 berichtet.

- Die Vorschriften über die **Zulässigkeit** der Datenverarbeitung umfassen nun auch das Erheben personenbezogener **Daten** (Art. 15 und 16) und die Nutzung personenbezogener Daten innerhalb der öffentlichen Stellen (Art. 17).

  Wie in den Datenschutzgesetzen des Bundes und der anderen Länder wurde die **Zweckbindung bei der Nutzung und Verarbeitung der Daten nunmehr** ausdrücklich eingeführt. Notwendige Durchbrechungen des Grundsatzes der Zweckbindung wurden vorgesehen (Art. 17 Abs. 2). Größere Schwierigkeiten werden bei der Umsetzung des Zweckbindungsgrundsatzes auch deshalb nicht erwartet, weil nach der vorherrschenden Gesetzesauslegung auch unter der Geltung des alten BayDSG eine Datenverarbeitung nur zulässig war, soweit sie zur Erfüllung einer Aufgabe objektiv geeignet war und im Verhältnis zu dieser Aufgabe auch angemessen erschien. Bei dieser Angemessenheitsprüfung hatten die bayerischen Behörden die Zweckbindungsfrage mit zu berücksichtigen.
- Die Zulässigkeit **von Online-Datenübermittlun**gen wurde besonders geregelt (Art. 8).
- Die **datenschutzrechtliche Freigabe** blieb erhalten, wurde jedoch vereinfacht. Die Sammlung der freigegebenen automatisierten Verfahren ist nun zusammen mit einem Verzeichnis der eingesetzten Datenverarbeitungsanlagen als **Anlagen- und Verfah**rensverzeichnis bei der Behörde zu führen. Die Meldung zum Datenschutzregister beim Landesbeauftragten für den Datenschutz ist entfallen.

Zum 1. März ist außerdem die **Datenschutzverordnung** in Kraft getreten.

Besonders hervorzuheben sind die dort geregelten Aus**nahmen** von der Verpflichtung zur datenschutzrechtlichen **Freigabe** vor Aufnahme von Verfahren in das **An**lagen**und** Verfahrenverzeichnis. Die Regelung dient der Vereinfachung des Verfahrens.

Im Berichtsjahr ebenfalls in Kraft getreten ist die neue **Vollzugsbekanntmachung zum Bayerischen Daten**schutzgesetz. Sie bindet alle staatlichen Behörden und ist den nichtstaatlichen öffentlichen Stellen zur Anwendung empfohlen.

Die Bekanntmachung regelt die Bestellung des behör**deninternen Datenschutzbeauftragten, insbesondere** die Voraussetzungen hierfür. Außerdem werden die Aufgaben und Pflichten des behördlichen Datenschutzbeauftragten beschrieben, sowie sein Recht, personenbezogene Unterlagen einzusehen. In der Bekanntmachung finden sich außerdem Erläuterungen zur datenschutzrechtlichen **Freigabe** automatisierter Verfahren und zur Aufstellung des Anlagen- **und Verfahrenverzeichnisses.** Schließlich wird dort erläutert, in welcher Weise bei personenbezogenen Daten, die dem Arztgeheimnis unterliegen, oder die in Personalakten oder Akten über Sicherheitsüberprüfung enthalten sind, die Betroffenen auf ihr **Widerspruchsrecht** gegen Kontrollen durch den Landesbeauftragten für den Datenschutz hingewiesen werden müssen.

1.10 Datenschutz bei Datenerhebung und -verarbeitung für Begnadigungsverfahren

Am 1. Juli 1994 ist die Bekanntmachung des Bayerischen Ministerpräsidenten über die im Gnadenverfahren zu beachtenden Grundsätze des Datenschutzes vom *25.* Juni 1994 in Kraft getreten (BayGVBl, Seite 546). Ich wurde vor Erlaß der Bekanntmachung gehört. Gewisse Verbesserungen aus Sicht des Datenschutzes konnten erreicht werden. Ich habe jedoch erklärt, daß bei nächster sich bietender Gelegenheit eine angemessene gesetzliche Regelung im Bayerischen Datenschutzgesetz notwendig ist.

Folgendes liegt dem zugrunde:

Wie im 15. Tätigkeitsbericht kurz dargestellt, gelten die Vorschriften des neuen Bayerischen Datenschutzgesetzes

vom 23.7.1993 ,,nicht für die Ausübung des Begnadigungsrechts" (Art. 2 Abs. 4 BayDSG).

In der Gesetzesberatung hatte der Bayerische Senat die Staatsregierung um Prüfung gebeten

> ,,inwieweit eine einschränkende Geltung des Bayerischen Datenschutzgesetzes insbesondere im Kontrollbereich in den Gesetzestext aufgenommen werden kann" (Senatsdrucksache 30/93 vom 11.02.1993).

Mein Vorgänger im Amt hat im Gesetzgebungsverfahren versucht, die Herausnahme des Begnadigungsverfahrens aus dem Geltungsbereich des BayDSG zu verhindern, hatte damit jedoch keinen Erfolg.

Für die in Vorbereitung der Gnadenentscheidung erfolgende Datenerhebung und -verarbeitung ist jedoch eine den Anforderungen des Bundesverfassungsgerichts im Volkszählungsurteil (BVerfGE *65,1)* nach einer normenklaren gesetzlichen Regelung entsprechende Rechtsgrundlage erforderlich, da nicht in allen Fällen die Einwilligung des Betroffenen vorliegt bzw. vermutet werden kann.

In der Praxis stellt sich zwar die Erhebung, Verarbeitung und Nutzung personenbezogener Daten für das Gnadenverfahren vielfach so dar, daß in einem sehr hohen Prozentsatz der Antrags-Fälle nur Daten über den Gnadenbetroffenen selbst mit seiner zumindest konkludenten Zustimmung erhoben werden bzw. nach dem Beibringungsgrundsatz von ihm erwartet wird, daß er selbst das Nötige vorlegt. Es bleibt jedoch ein Rest von Fällen, in denen personenbezogene Daten auch über andere Personen im Gnadenverfahren benötigt werden. Die mit Gnadensachen befaßten Stellen - in der Regel Justizbehörden - werden daher auch solche Daten erheben, verarbeiten und in seltenen Fällen möglicherweise auch weiter übermitteln.

Die **Bayerische Staatskanzlei und das Bayerische Staatsministerium der Justiz** vertreten den Standpunkt, daß das Erheben, Verarbeiten und Nutzen personenbezogener Daten für das Begnadigungsverfahren, soweit es nicht bereits durch die Einwilligung des Betroffenen gedeckt ist, **nach Art. 47 Abs. 4 Satz 1** der Bayerischen Verfassung erlaubt ist, auch soweit darin Eingriffe in das informationelle Selbstbestimmungsrecht des Antragstellers oder Dritter zu sehen wären. In die Bekanntmachung über die Grundsätze des Datenschutzes im Gnadenverfahren, an der ich wie ausgeführt beteiligt wurde, wurden materielle Grundsätze des Datenschutzes aufgenommen. So ist nach § 3 Abs. 2 der Bekanntmachung die Datenerhebung bei Dritten anstatt beim Betroffenen nur vorgesehen, wenn dadurch überwiegende schutzwürdige Interessen von Betroffenen nicht beeinträchtigt werden. Auch die für das Gnadenverfahren erforderlichen Übermittlungen personenbezogener Daten durch bayerische öffentliche Stellen an die mit Gnadensachen befaßten Stellen sowie erforderliche Übermittlungen personenbezogener Daten der mit Gnadensachen befaßten Stellen an andere Stellen dürfen danach überwiegende schutzwürdige Interessen eines Betroffenen nicht beeinträchtigen. Außerdem enthält die Bekanntmachung das Gebot, die nötigen technischen und organisatorischen Datensicherungsmaßnahmen durchzuführen.

Ich begrüße die Anwendung vorstehender materiellrechtlicher Grundsätze im Gnadenverfallren, bin jedoch der Ansicht, daß Art. 47 Abs. 4 Satz 1 BV als Befugnisnorm für die Datenverarbeitung ohne Einwilligung des Betroffenen nicht ausreicht, da Art. 47 BV über Art und Umfang einer Datenerhebung und -verarbeitungsbefugnis normenklar nichts aussagt.

Ich teile zwar die Auffassung, daß die eigentliche Entscheidung über einen Gnadenerweis nicht durch Rechtsnorm vorgegeben oder eingeschränkt werden darf. Dies meint auch die Entscheidung des Bundesverfassungsgerichts vom 23.04.1969 (E 36, 352ff., 361). Die eine Gnadenentscheidung vorbereitende Erhebung und Verarbeitung personenbezogener Daten ist jedoch der Regelung durch den Gesetzgeber zugänglich und im Hinblick auf die damit verbundenen Eingriffe in das informationelle Selbstbestimmungsrecht auch bedürftig. Den Betroffenen sollte daher der Schutz ihrer Daten durch das Datenschutzgesetz gewährt werden. Dies könnte beispielsweise durch Streichung der oben zitierten Ausnahme in Art. 2 Abs. 4 BayDSG und Einfügung einer Erlaubnis zur Zweckänderung, soweit personenbezogene Daten zur Ausübung des Begnadigungsrechts erforderlich sind, in Art. 17 Abs. 2 BayDSG geschehen. Damit würden nicht nur die Datenflüsse im Zusammenhang mit der Vorbereitung der Gnadenentscheidung einem angemessenen gesetzlichen Schutz unterworfen, sondern auch der Umgang mit personenbezogenen Daten bei den mit Gnadensachen befaßten Stellen außerhalb des Begnadigungsverfahrens geregelt.

1.11 Entwurf einer Datenschutzrichtlinie der Europäischen Union

Die Arbeit am Entwurf der EU-Datenschutzrichtlinie ist im Berichtsjahr weiter fortgeschritten. Das deutsche System der Datenschutzkontrolle sowie die vorgesehenen Meldepflichten gegenüber Kontrollbehörden waren in der Beratung von besonderem Gewicht. Die deutschen Vertreter haben darauf gedrungen, daß das in Deutschland bewährte Kontrollsystem beibehalten werden kann, wonach unabhängige Landesbeauftragte für den Datenschutz (bzw. der Bundesbeauftragte für den Datenschutz) für die Kontrolle der öffentlichen Verwaltung zuständig sind, während die Kontrollen der Privatwirtschaft durch Länderaufsichtsbehörden erfolgt, die in die normale Verwaltungshierarchie mit Ministerverantwortlichkeit eingegliedert sind. Desweiteren wurde gefordert, bürokratische Regelungen in Form von übertriebenen Meldepflichten der Wirtschaft gegenüber den Kontrollbehörden zu vermeiden. Die Richtlinie sollte im Hinblick auf das Subsidiaritätsprinzip den Umfang der Meldepflichten den Mitgliedsstaaten überlassen.

Die Gruppe ,,Wirtschaftsfragen/Datenschutz" des Rates der EU hat 1994 einen Entwurf für einen gemeinsamen Standpunkt erarbeitet, der vom Binnenmarktrat Anfang 1995 angenommen werden soll.

Der Deutsche Bundestag hat im Sommer 1994 in einer Stellungnahme beschlossen:

,,Das im Vertrag von Maastricht verankerte Subsidiaritätsprinzip ist strikt anzuwenden. Es dürfen nur solche Datenschutzfragen in der Richtlinie geregelt werden, die zwingend notwendig EU-einheitlich geregelt werden müssen. In diesem Rahmen soll der in der Bundesrepublik Deutschland erreichte Datenschutzstandard erreicht werden. Es muß sichergestellt werden, daß das höhere deutsche Datenschutzniveau auch nach Inkrafttreten der Richtlinie beibehalten werden kann."

Die Entschließung der Datenschutzbeauftragten zum Richtlinienentwurf ist im *15.* Tätigkeitsbericht als Anlage 1 abgedruckt.

1.12 Behördenzusammenlegung und Privatisierung von Behördentätigkeiten, für die personenbezogene Daten erhoben oder verarbeitet werden

Die Bayerische Staatsregierung hat im Berichtsjahr Beschlüsse über die Zusammenlegung von Behörden und die Privatisierung von Behördentätigkeiten gefaßt, um die Verwaltung zu vereinfachen und Aufgaben abzubauen. So sollen die Gesundheitsämter und die Veterinärämter jeweils mit den Landratsämtern zusammengelegt werden. Aufgaben aus dem Bereich der Wasserwirtschaftsämter sollen privatisiert werden. Auf Anregung aus dem Beirat beim Landesbeauftragten für den Datenschutz habe ich mich an die Bayerische Staatskanzlei, das Innen-, das Sozial- und das Umweltministerium gewandt und auf datenschutzrechtliche Probleme hingewiesen, die bei Behördenzusammenlegung oder Privatisierung von Behördentätigkeiten gelöst werden müssen.

Zur Zusammenlegung der **Gesundheitsämter** mit den **Landratsämtern** habe ich um Mitteilung darüber gebeten, wie der Schutz von personenbezogenen Daten künftig bewerkstelligt wird, die dem Gesundheitsamt bzw. seinen Mitarbeiterinnen und Mitarbeitern freiwillig anvertraut oder im Rahmen freiwilliger Begutachtung bekannt wurden. Für solche Daten sieht Art. 6 des Bayerischen Gesundheitsdienstgesetzes ein grundsätzliches Verwertungsverbot vor, das bisher durch besondere organisatorische Maßnahmen bereits innerhalb des Gesundheitsamtes abgesichert wurde. Entsprechende Maßnahmen sind nach der Zusammenlegung innerhalb des Landratsamtes besonders notwendig. Das Sozialministerium hat die Notwendigkeit solcher organisatorischen Vorsorge grundsätzlich. anerkannt.

Fragen einer organisatorischen Arbeitsabgrenzung können sich aber auch beim Vollzug von Gesetzen stellen, die von der Existenz von Gesundheitsamt und Kreisverwaltungsbehörde als zweier unterschiedlicher Behörden ausgehen, wie das Bundesseuchengesetz oder das Unterbringungsgesetz.

Bei Privatisierung von Behördentätigkeiten muß berücksichtigt werden, daß auf die Erhebung und Verarbeitung personenbezogener Daten künftig andere Datenschutzvorschriften anzuwenden sind als bisher. Während Datenerhebung und -verarbeitung bei Behörden durch das Bayerische Datenschutzgesetz oder durch bereichsspezifische Vorschriften geregelt sind, ist auf die Verarbeitung personenbezogener Daten von Bürgern durch eine Privatfirma das Bundesdatenschutzgesetz (BDSG) anzuwenden:

Das Bundesdatenschutzgesetz bezieht sich bei privaten Stellen nur auf Daten, die in **Dateien** verarbeitet werden, während für Behörden das Datenschutzgesetz auch auf die Aktendatenverarbeitung Anwendung findet. Änderungen ergeben sich auch bei der **Datenerhebung,** da diese für Privatfirmen nicht detailliert geregelt ist.

Außerdem ist die **Zweckbindung personenbezogener** Daten für private Stellen aufgrund des Bundesdatenschutzgesetzes lockerer als bei Behörden. So können private Stellen beispielsweise Anschriften von Personen mit Angaben über Zugehörigkeiten zu Berufsgruppen grundsätzlich vermarkten (§ 28 Abs. 2 BDSG), was Behörden nicht gestattet ist. Außerdem findet die **Datenschutzkontrolle bei einer privaten datenverarbeitenden** Stelle nicht von Amts wegen statt, wie bei Behörden, sondern nach dem BDSG nur bei einem entsprechenden Anlaß.

Sobald bekannt ist, welche behördlichen Tätigkeiten im Rahmen der Privatisierungsmaßnahmen künftig von privaten Stellen abgewickelt werden sollen, muß geprüft werden, ob sich aus dieser Änderung wesentliche Nachteile für Bürger ergeben, deren Daten mit den Aufgaben an private Stellen zur Abwicklung übergehen. Ich habe um Unterrichtung über die zur Privatisierung vorgesehenen Tätigkeiten gebeten.

Sozialministerium und Umweltministerium haben zugesichert, mich rechtzeitig über Arbeitsergebnisse zur Zusammenlegung und Privatisierung zu unterrichten. Über den Stand der damit verbundenen Datenschutzfragen werde ich jeweils den Beirat beim Landesbeauftragten für den Datenschutz in Kenntnis setzen.

1.13 Probleme bei der Verwendung von Chipkarten

In zunehmendem Umfang müssen sich die Datenschutzbeauftragten mit Chipkarten und den damit zusamiüenhängenden Datenschutzfragen auseinandersetzen. Die Möglichkeiten, große Datenmengen in den Chips zu speichern, sind faszinierend, die Speicherkapazitäten der Chipkarten werden immer größer. Die Kapazität von Chipkarten legt es deshalb auch nahe, anstelle einer Vielzahl von Plastikkarten nur eine multifunktionale Karte zu

benutzen, die Daten für die verschiedensten Zwecke enthält. Dafür muß das datenschutzrechtliche Problem gelöst werden, daß jeweils nur bestimmte oder vom Karteninhaber gewollte Inhalte der Karte gelesen oder geändert werden. Eine Lösung muß auch dafür gefunden werden, daß der Karteninhaber meist selbst kein Gerät hat, mit dem er den Karteninhalt lesen kann, so daß er auf die Hilfe Dritter angewiesen ist. Auch kann beim Karteninhaber Unsicherheit darüber bestehen, was ein Dritter tatsächlich auf der Karte liest oder ändert. Der Inhaber muß aber darauf vertrauen können, daß Personen oder Stellen, denen er die Karte aushändigt, nur das lesen und ändern können, was er selbst bestimmt. Durch entsprechende Sicherungsmaßnahmen muß daher das nötige Vertrauen bei den Karteninhabern geschaffen werden. Wichtig erscheint aus Datenschutzsicht außerdem stets, daß die Freiwilligkeit der Speicherung und der Verwendung von gespeicherten Daten soweit als möglich erhalten bleibt. Schließlich müssen Benutzerprofile aus Datenschutzsicht soweit wie möglich vermieden werden.

Die Datenschutzbeauftragten haben sich bereits mit einigen Formen von Chipkarten befaßt, wie der Krankenversichertenkarte, die nur dazu dient, die identifizierenden Daten des bisherigen Krankenscheines vorzuhalten, mit sonstigen Gesundheits-Chipkarten (siehe Beschluß der DSB-Konferenz in der Anlage 1) oder mit der Pay-Card zur Abbuchung von Autobahngebühren. Die Bundesvereinigung Deutscher Apothekerverbände hat über ein Projekt zur Einführung einer Patientenchipkarte durch Apotheken unterrichtet. Die Prüfung dieses Verfahrens ist noch nicht abgeschlossen.

Ich werde die Entwicklung in diesem Bereich mit besonderer Aufmerksamkeit beobachten.

2. Gesundheitswesen

2.1 Medizinische Forschung und Datenschutz

2.1.1 Forschungsgeheimnis

Nicht nur für die Sammlung und Auswertung von personenbezogenen Daten über Krebserkrankungen wäre ein rechtlicher Schutz solcher Daten ,,wie beim Arzt" durch Weitergabe- und Verwertungsverbote wie Zeugnisverweigerungsrecht und Beschlagnahmeschutz eine wichtige Verbesserung (siehe auch den folgenden Beitrag zum Bundeskrebsregistergesetz). Auch bei der Sammlung von Daten über **andere Erkrankungen** zu medizinischen Forschungszwecken würde ein **durch Zeugnisverweigerungsrecht und Beschlagnahmeschutz flankiertes** Forschungsgeheimnis dem wissenschaftlichen Anliegen nach Erhalt der notwendigen personenbezogenen Daten ganz wesentlich entgegenkommen.

Dies würde zum einen die datenschutzrechtliche Situation bei Forschungsprojekten, für die personenbezogene Patientendaten von Kliniken und Krankenhäusern oder Ärzten benötigt werden, verbessern. Sorgen des Datenschutzes richten sich nämlich nicht gegen die Nutzung der Daten durch die Wissenschaft, sondern darauf, daß Wissenschaftler rechtlich nicht genügend dagegen abgesichert sind, daß die bei ihnen gesammelten Daten von anderen Stellen für andere Zwecke in Anspruch genommen werden könnten - etwa zur Verfolgung von Straftaten und Ordnungswidrigkeiten oder zur Steuerveranlagung bzw. -fahndung.

Würde eine ausreichende rechtliche Absicherung durch ein solches ,,Forschungsgeheimnis" bestehen, könnte es aber auch dem Gesetzgeber, insbesondere dem Landesgesetzgeber, leichter fallen, gesetzliche Befugnisse zur Weitergabe von Patientendaten für Zwecke unabhängiger wissenschaftlicher Forschung im medizinischen Bereich zu schaffen und damit medizinische, insbesondere epidemiologische Forschung erheblich zu unterstützen.

Es ist nicht einzusehen, weshalb **Patientendaten** den von Strafgesetzbuch und Strafprozeßordnung **beim behandelnden Arzt** seit langem **geltenden Schutz verlieren** sollten, sobald sie außerhalb dieses geschützten räumiichen und personellen Bereichs für unabhängige wissenschaftliche (epidemiologische) Forschung in Anspruch genommen werden.

Es ist auch nicht einzusehen, weshalb Patientendaten, die für Zwecke unabhängiger wissenschaftlicher Forschung im medizinischen Bereich gesammelt werden, schlechter geschützt sein sollen, als Daten bei Sozialbehörden. Im Bereich dieser Behörden sind durch § 35 Abs. 3 des 1. Buches des Sözialgesetzbuches das Zeugnisverweigerungsrecht und das Beschlagnahmeverbot für den Fall der Unzulässigkeit einer Sozialdatenübermittlung gesetzlich festgelegt.

Da Zeugnispflicht und Beschlagnahmerecht durch Bundesrecht, nämiich das Prozeßrecht für Straf- und Zivilverfahren festgelegt sind, können sie zur Sicherstellung eines Forschungsgeheimnisses auch nur durch Bundesgesetz eingeschränkt werden.

2.1.2 Entwurf für ein Bundeskrebsregistergesetz

Zum Entwurf des zwischenzeitlich beschlossenen Bundesgesetzes über das Krebsregister (BGBl 11994, 5. 3551 ff.) hatte ich erneut Stellung genommen und datenschutzrechtliche Verbesserungen gefordert.

Grundsätzlich ist die vorgesehene anonymisierte Speicherung der Daten von Krebspatienten in der Registerstelle aus Datenschutzsicht positiv zu bewerten. Nach den Regelungen sollen die Daten zwar von Ärzten mit dem Namen des Patienten an eine Vertrauensstelle gemeldet werden. Diese soll sie jedoch verschlüsseln und anonymisiert an die Registerstelle weitergeben, selbst aber nicht speichern. Das Register, das die auszuwertenden Daten speichert, würde also keine Patientennamen erhalten. Eine Reidentifikationsmöglichkeit für Forschungszwecke ist gleichwohl vorgesehen.

Im wesentlichen hatte ich folgende Verbesserungen vorgeschlagen:

1. Der Schutz der Patientendaten in der Vertrauens- und Registerstelle darf nicht schlechter sein, als der Schutz von Patientendaten beim behandelnden Arzt und von Sozialdaten bei Sozialbehörden. Da die **Reidentifizierung** der Daten möglich ist halte ich, wie **bei Arzt und Sozialbehörden, ein Zeugnisverweigerungsrecht** sowie ein **Beschlagnahmeverbot für** die im Gewahrsam des Krebsregisters befindlichen Unterlagen für **erforderlich.** Ich habe vorgeschlagen, wie in § 35 Abs. 3 des 1. Buches des Sozialgesetzbuches für Sozialbehörden festzulegen, daß bei fehlender Übermittlungsbefugnis keine Auskunftspflicht, keine Zeugnispflicht und keine Pflicht zur Vorlegung oder Auslieferung von Schriftstücken, Akten, Dateien oder sonstigen Datenträgern besteht.

2. In besonders gelagerten Einzelfällen kann bereits aufgrund der gespeicherten Daten noch ein unnötiges **Reidentifikationsrisiko bei** der **Registerstelle** bestehen, **denn** dort sollen die epidemiologischen Daten im Klartext gespeichert werden. Es besteht bei kleinen Wohnorten, seltenen Berufen, auffälliger Staatsangehörigkeit u.ä. und bei der Kombination solcher Daten bei der Registerstelle ein unnötiges Risiko der Reidentifizierbarkeit von Betroffenen. Die Vertrauensstelle sollte daher solche **Daten** vor der Übermittlung an die Registerstelle ebenfalls **verschlüsseln**.

3 Vorgesehen ist das Abgleichen personenidentifizierender Daten nach Entschlüsselung von Identitätsdaten für im öffentlichen Interesse stehende Forschungsvorhaben. Meines Erachtens fehlt hier die für den Zweck des Krebsregisters völlig ausreichende **Beschränkung auf medizinische Forschungsvorhaben.**

Ich hielt und halte diese Verbesserungen aus der Sicht der betroffenen Patienten für wichtig. Von der Meldung zum Krebsregister werden auch viele Personen betroffen sein, deren Erkrankung noch im Frühstadium ist und die daher u.U. noch lange Zeit oder vielleicht auch auf Dauer ein im wesentlichen normales Leben führen können. Hierbei würden sie durch eine evtl. Offenlegung ihrer Krankheit aufgrund der genannten, völlig unnötigen datenschutzrechtlichen Mängel besonders unverhältnismäßig belastet. Die vorgeschlagenen Verbesserungen hätten deshalb auch die Akzeptanz des Gesetzes bei den betroffenen Personen wesentlich erhöht. Dem Gesetz hätte dann bestätigt werden können, daß der notwendige Datenschutz in vollem Umfang gewahrt ist.

Das Bayerische Sozialministerium hat aus meinen Forderungen zu 1. und 3. Anträge für den Vermittlungsausschuß von Bundestag und Bundesrat formuliert. Sie wurden jedoch im Vermittlungsausschuß leider nicht berücksichtigt.

2.1.3 Fehlbildungsregister

In Zeitungsberichten über das Auftreten von Mißbildungen bei Neugeborenen in der norddeutschen Küstenregion wurde von Forderungen der Ärzte berichtet, ein Fehlbildungsregister einzuführen.

Bei einem Fehlbildungsregister stellt sich ganz besonders - wie bei anderen Krankheitsregistern - aus Datenschutzsicht die Frage, ob für diesen Zweck künftig Daten personenbezogen erhoben und gespeichert werden sollen und ggf. wie sie vor Zweckentfremdung rechtlich und technisch-organisatorisch zu schützen sind. Meine Nachfrage beim Bayerischen Sozialministerium hat ergeben, daß derzeit von ärztlicher Seite an der Definition der Kriterien gearbeitet wird, die ein solches Register erfüllen soll. Erst danach lasse sich überblicken, welche Art von Daten und ob auch personenbezogene Daten erhoben und gespeichert werden sollen.

In diesem Zusammenhang habe ich an die Datenerhebung über Neugeborene im Rahmen der Bayerischen Perinatal- und Neonatalerhebungen erinnert. In beiden Verfahren werden anonymisiert auf Formularen ärztliche Feststellungen über **Mißbildungen an Neugeborenen** an die Bayerische Ärztekammer zur Auswertung übersandt. Ich habe angeregt zu überprüfen, ob dieses anonyme Verfahren für die angestrebten Zwecke eines Fehlbildungsregisters um weitere Mißbildungsmerkmale ergänzt werden könnte. Wesentlich erscheint mir daran, daß zur Aufhebung der Anonymität der Betroffenen allein die behandelnden Ärzte in der Lage wären und diese durch ihre ärztliche Schweigepflicht an dieser Aufhebung der Anonymität gehindert sind.

Das Sozialministerium will mich auf dem laufenden halten.

2.1.4 Verbesserter Zugang zu Todesbescheinigungen für Forschungszwecke durch Änderung des Bayerischen Bestattungsgesetzes

Der vertrauliche Teil der Todesbescheinigungen enthält medizinische Angaben zur Todesursache, die für Forschungszwecke, insbesondere für epidemiologische Forschung, wie es heißt, von großem Wert sind. Der Bayerische Landtag hat daher durch ein Änderungsgesetz zum Bestattungsgesetz eine Erlaubnis für Auskünfte aus dem vertraulichen Teil von Todesbescheinigungen und für Einsichtnahmen in diese u.a. auch für wissenschaftliche Forschungsvorhaben erteilt. Voraussetzung ist jeweils, daß

- durch sofortige Anonymisierung der Angaben oder auf andere Weise sichergestellt wird, daß schutzwürdige Interessen der verstorbenen Person nicht beeinträchtigt werden oder

- das öffentliche Interesse an der Forschung das schutzwürdige Interesse der verstorbenen Person erheblich übersteigt und der Zweck der Forschung auf andere Weise nicht oder nur mit unverhältnismäßigem Aufwand erreicht werden kann und kein Grund zu der Annahme besteht, daß schutzwürdige Interessen von Angehörigen der verstorbenen Person am Ausschluß der Verarbeitung oder Nutzung überwiegen.

Den Gesundheitsämtern wird ausdrücklich die Erlaubnis erteilt, die Todesbescheinigungen zur Erfüllung ihrer Aufgaben auszuwerten. Diese Verdeutlichung geht auf meine Anregung zurück.

2.2 Entwürfe für ein Transplantationsgesetz

Ziel eines Transplantationsgesetzes ist die Schaffung eines klaren rechtlichen Handlungsrahmens, um bestehende Rechtsunsicherheiten und dadurch bedingte Zurückhaltung bei Ärzten und Pflegepersonen auszuräumen, sowie eine Verbesserung der Zusammenarbeit von Krankenhäusern mit Transplantationszentren.

Soweit bisher aus Vorüberlegungen für ein Transplantationsgesetz erkennbar, werden sich hierbei folgende Datenschutzfragen stellen:

1. Schriftlichkeit der Erklärung zur Organentnahme

   Die Regelung wird neben schwierigen Problemen, die keine Datenschutzfragen sind, auch das informationelle Selbstbestimmungsrecht des künftigen Organspenders und von Angehörigen betreffen, die statt eines Verstorbenen, von dem keine Erklärung vorliegt, befragt werden. Zu prüfen ist, ob hier die Schriftlichkeit der Einwilligung von Angehörigen zu fordern wäre, damit zum Nachweis nicht nur das vorliegt, was vom Arzt dokumentiert wurde. Unsicherheiten über den Inhalt von Erklärungen der Angehörigen würden dann im Originalwortlaut dokumentiert, so daß Zweifelsfälle nicht durch zu knappe Dokumentation unter den Tisch fallen könnten.

2. Identifizierung des Spenders

   Aus fachlichen Gründen wird offenbar angestrebt, daß persönliche Daten des Spenders vor dem Empfänger geheimgehalten werden. Gleichwohl kann sich aber in manchen Fällen die Notwendigkeit einer lückenlosen Rückverfolgung des übertragenen Organs vom Empfänger zum Spender ergeben, etwa um bei einer gesundheitlichen Gefährdung des Empfängers durch das transplantierte Organ rasch geeignete Maßnahmen zum Schutz des Empfängers ergreifen zu können. Es ist wohl nicht auszuschließen, daß dafür in Einzelfällen auch die Identität des Spenders bekanntgegeben werden muß. Ausnahmen von der Geheimhaltung wären aber auch im Hinblick auf die Beweissituation bei Übertragung von Krankheiten durch das Organ auf Empfänger zu prüfen.

3. Datenschutz bei der Organvermittlung

   Bei Stellen, die im Zuge der Vermittlung von Organen personenbezogene Patientendaten erhalten und speichern, muß ein Niveau des Datenschutzes ,,wie beim Arzt", das heißt entsprechend § 203 Abs. 1 Nr. 1 StGB, § 97 StPO (Beschlagnahmeschutz) sichergestellt sein. Dies setzt eine eindeutige Regelung in einem Bundesgesetz voraus. Lediglich eine Anwendbarkeit von Vorschriften des Bundesdatenschutzgesetzes könnte diesen Schutz nicht bewirken.

   Zu denken wäre an eine Regelung analog dem Schutz von Sozialdaten in § 35 des 1. Buches des Sozialgesetzbuches (Sozialgeheimnis, Beschlagnahmeschutz).

4. Schriftliche Einwilligung von Organempfängern in Datenübermittlung an Vermittlungsstellen

   Das Einverständnis des Patienten zur Übermittlung seiner personenbezogener Daten an Organvermittlungsstellen sollte zumindest im Regelfall schriftlich eingeholt werden, damit den Patienten hinreichend bewußt wird, an welche Stellen (z.B. auch im Ausland) seine persönliche Daten übermittelt werden.

2.3 Datenschutzfragen aus dem Bereich von Krankenhäusern

2.3.1 Inkasso/Abrechnung des Krankenhausträgers für privatliquidationsberechtigte Ärzte bei stationärer Behandlung

In einer Eingabe wurde Beschwerde darüber geführt, daß ein Krankenhausträger durch eine eigens dafür eingerichtete Stelle seiner Verwaltung das Inkasso für die Pnvatrechnungen des Chefarztes bei stationärer Behandlung durchführen ließ. Es sei keine ausreichende Einwilligung in die Weitergabe der hierfür benötigten Patientendaten vom Arzt an die städtische Inkassostelle eingeholt worden.

Obwohl der Einwand der mangelnden Einwilligung zutraf, war die Weitergabe der Daten an die städtische Inkassostelle gleichwohl nicht zu beanstanden. Eine Befugnis hierfür lag in § 7 Abs. 3 der **Bundespflegesatzverordnung** (in der Fassung des Gesundheitsstrukturgesetzes vom 18.12.1992). Dort ist in Abs. 3 u.a. festgelegt:

> ,,Ein zu gesonderter Berechnung wahlärztlicher Leistungen berechtigter Arzt des Krankenhauses kann eine private Abrechnungsstelle mit der Abrechnung der Vergütung für die wahlärztliche Leistung beauftragen **oder die Abrechnung dem Krankenhaus-träger überlassen .....**
> Die Übermittlung von personenbezogenen Daten an eine beauftragte Abrechnungsstelle darf nur mit Einwilligung der jeweils betroffenen Patienten erfolgen."

Diese Regelung sieht eine Einwilligung des jeweils betroffenen Patienten nur für den Fall vor, daß eine ,,private Abrechnungsstelle" vom Arzt ,,beauftragt" wird. Keine gesonderte Einwilligung ist dagegen erforderlich, wenn die Ärzte ,,die Abrechnung dem Krankenhausträger überlassen". Hiernach darf der zur gesonderten Berechnung wahlärztlicher Leistungen berechtigte Arzt des Krankenhauses das vollständige Erstellen seiner Privatliquidation ,,dem Krankenhausträger überlassen". Wenn der Arzt, anstatt die vollständige Erstellung seiner Pnvatliquidation einer Stelle des Krankenhausträgers zu überlassen, dieser nur einen Teil der ,,Abrechnung" überträgt, muß dies entsprechend als befugt angesehen werden.

Er kann daher, wie im Beschwerdefall, die zunächst von seiner Sekretärin erstellte Privatliquidation der Inkassostelle des Krankenhausträgers zur Plausibilitätsprüfung und Übersendung zum Inkasso überlassen.

An der geschilderten Rechtslage hat sich durch das Inkrafttreten der geänderten Fassung der Regelung (nun §22 Abs. 3 der Bundespflegesatzverordnung), zum 01.01.1995 nichts geändert.

Ungeachtet der geschilderten Befugnis zur Offenbarung halte ich für sinnvoll, die Patienten auf die Einschaltung des Krankenhausträgers hinzuweisen. Der Eingriff in das informationelle Selbstbestimmungsrecht der Patienten, der in der Weitergabe der Daten liegt, wird dadurch verlängert. Ich habe daher die Stadt gebeten, in dem Text, den die Patienten zu den wahlärztlichen Leistungen erhalten, auf die tatsächliche und rechtliche Situation hinzuweisen.

Da die Bundespflegesatzverordnung Offenbarungsbefugnisse jedoch **nur** für **stationäre** Behandlungen erteilt, muß darauf geachtet werden, daß bei der Einschaltung von Abrechnungsstellen bei **ambulanten** Chefarztbehandlungen, und zwar auch bei der Einschaltung von Abrechnungsstellen des Krankenhauses bzw. Krankenhausträgers, die Einwilligung der betroffenen Patienten eingeholt wird.

2.3.2 Vorsorgliche Anmeldung nach § 121 BSHG bei der falschen Stelle

Ein Patient beschwerte sich darüber, daß ein Krankenhausträger eine - strittige - offene Forderung gegen ihn gem. § 121 Bundessozialhilfegesetz (BSHG) bei der Sozialhilfestelle seiner kreisangehörigen Wohnsitzgemeinde angemeldet hatte.

Nach § 121 BSHG haben hilfeleistende Stellen das Recht und die Pflicht, etwaige Ansprüche aus einer eiligen Behandlung rechtzeitig beim zuständigen Sozialleistungsträger anzumelden. Nach Ablauf der hierfür festzulegenden angemessenen Frist lehnt der Sozialhilfeträger die Kostenerstattung ab. Krankenhäuser müssen daher, wenn sie nicht wissen, ob sie die Kosten erstattet erhalten und wenn die vorgesehene Frist zu verstreichen droht, ihre Forderung vorsorglich beim Sozialhilfeträger anmelden.

Die Übermittlung der erforderlichen Patientendaten mit der **Anmeldung der Forderung nach § 121 BSHG** durch das Krankenhaus kann daher nicht beanstandet werden. Allerdings hätte der Antrag nicht bei der kreisangehörigen Wohnsitzgemeinde des Petenten, sondern beim Sozialamt des Landratsamtes gestellt werden müssen, denn Träger der Sozialhilfe im Bereich kreisangehöriger Gemeinden ist der Landkreis. Die Übermittlung personenbezogener Daten an die Wohnsitzgemeinde statt an das Landratsamt in Zusammenhang mit der Anmeldung der Forderung habe ich daher beanstandet.

2.3.3 Erhebung des Datums „geschieden" bei der Aufnahme in das Krankenhaus

Eine Klinik vertrat die Auffassung, der Patient habe bei der Aufnahme auch anzugeben, ob er ,,geschieden" sei.

Die Daten seien zur Erfüllung der Aufgaben des Krankenhauses erforderlich (Art. 27 Abs. 2 des Bayerischen Krankenhausgesetzes).

Bei geschiedenen Ehegatten bestehen jedoch keine direkten Ansprüche des Krankenhausträgers gegen den anderen, ggf. unterhaltsverpflichteten Ehegatten gem. §1357 BGB mehr. Es besteht lediglich ein Anspruch des Unterhaltsberechtigten gegen den Barunterhaltsverpflichteten gem. §§ 1601 ff. BGB. In diesem Fall kann der Krankenhausträger lediglich den Unterhaltsanspruch unter den Voraussetzungen des § 850 b Abs. 1 Nr.2, Abs. 2 ZPO pfänden. Dies ist jedoch letztlich erst eine Frage der Zwangsvollstreckung. Unter diesem Gesichtspunkt erscheint es nicht ohne weiteres einsichtig, weshalb der Patient bereits beim Abschluß des Behandlungsvertrages eine Ehescheidung offenlegen soll. Diese Frage sollte daher nicht im Aufnahmeformular gestellt werden.

2.3.4 Gemeinsame Poststelle für ärztlichen und Verwaltungsbereich im Krankenhaus

Krankenhausärzte stellen immer wieder die Frage, ob es zulässig sei, daß Post für den ärztlichen Bereich des Krankenhauses von der zentralen Poststelle der Klinik geöffnet wird.

Dazu habe ich jeweils mitgeteilt, daß nicht beanstandet werde, wenn in einem Krankenhaus eine gemeinsame Posteinlaufstelle für den ärztlichen und den Verwaltungsbereich eingerichtet ist, in der die Post geöffnet wird, die an das Krankenhaus oder die Krankenhausverwaltung oder einen medizinischen Bereich des Krankenhauses oder auch zu Händen bestimmter Ärzte adressiert ist. Lediglich Post, die unmittelbar an einen Arzt im Krankenhaus adressiert ist - ,,Herm Dr. X im Krankenhaus - ist diesem ungeöffnet zuzuleiten. Allerdings muß die Poststelle die Post nach dem Öffnen direkt den betreffenden Abteilungen zuleiten. Für unzulässig wurde erachtet, wenn etwa der Verwaltungsleiter sämtliche Post, auch solche für den ärztlichen Bereich, über sich leiten ließe.

Dabei gehe ich davon aus, daß die Mitarbeiter der Poststelle als Gehilfen des Arztes unter § 203 Abs. 1 Nr. 1 i.V.m. Abs. 3 fallen, da sie ,,innerhalb des beruflichen Wirkungskreises eines Schweigepflichtigen eine auf dessen berufliche Tätigkeit bezogene unterstützende Tätigkeit ausüben, welche die Kenntnis fremder Geheimnisse mit sich bringt" (Schönke/Schröder StGB 23. Auflage, § 203, RdNr. 64), so daß ich es nicht für notwendig halte, für verwaltungs- und ärztlichen Bereich separate Posteinlaufstellen vorzusehen.

2.3.5 Bestellung eines Datenschutzbeauftragten in öffentlichen Krankenhäusern

Immer wieder erreichen mich Fragen zur Bestellung eines krankenhausinternen Datenschutzbeauftragten und insbesondere zu seiner Befugnis, personenbezogene Patientendaten zur Kenntnis zu nehmen.

Für öffentliche Krankenhäuser in Bayern gelten, auch wenn sie am Wettbewerb teilnehmen, die Art. 25 ff. des neuen Bayerischen Datenschutzgesetzes (siehe Art. 3 Abs. 1 Satz 3 BayDSG). Danach müssen die obersten Dienststellen des Staates, die Gemeinden, die Gemeindeverbände und die sonstigen der Aufsicht des Freistaats Bayern unterstehenden juristischen Personen des öffentlichen Rechts sowie die privatrechtlichen Vereinigungen, auf die das Datenschutzgesetz gemäß dessen Art. 2 Abs. 2 Anwendung findet, für ihren Bereich die Ausführungen des Datenschutzrechts sowie anderer Vorschriften über den **Datenschutz sicherstellen.** Die Vollzugsbekanntmachung zum Bayer. Datenschutzgesetz legt deshalb für staatliche Stellen eine Pflicht zür **Bestellung behördlicher Datenschutzbeauftragter** fest, die auch für staatliche **Krankenhäuser** gilt, wenn sie über **mehr als 100 Betten** verfügen. Den Gemeinden, Gemeindeverbänden und den sonstigen der Aufsicht des Freistaats Bayern unterstehenden juristischen Personen des öffentlichen Rechts (und zugehörigen Krankenhäusern) und ggf. auch Vereinigungen wird empfohlen, bei Vorliegen der Voraussetzungen ebenfalls behördliche Datenschutzbeauftragte zu bestellen.

Dies wird in der gemeinsamen Bekanntmachung der Bayerischen Staatskanzlei und der Bayerischen Staatsministerien vom 11. März 1994 zum Vollzug des Bayerischen Datenschutzgesetzes näher ausgeführt (AllMBl. Nr.9/94 Seite 251/252).

Die Bekanntmachung geht (unter Nr.3.7) auf das Problem ein, inwieweit behördliche Datenschutzbeauftragte **personenbezogene Daten einsehen** dürfen, die einem Berufs- oder besonderen Amtsgeheimnis, insbesondere dem **Arztgeheimnis** unterliegen. Eine Befugnis zur Einsichtnahme in personenbezogene Daten, die der ärztlichen Schweigepflicht unterliegen, kann nur insoweit bestehen, als die Person, die den behördlichen Datenschutzbeauftragten im Einzelfall diesbezüglich anweisen darf, selbst einsichtnahmebefugt wäre. Die Befugnis ist stets ein abgeleitetes Recht. Sie kann nicht weitergehen als die Befugnis des Anweisenden. Denkbar ist, daß der ärztliche Leiter des Krankenhauses insoweit eine andere (evtl. geringere) Befugnis hat, als der Chef der behandelnden Krankenhausabteilung. Auch kann ein Datenschutzbeauftragter, der lediglich dem Verwaltungsleiter unterstellt ist, nicht von diesem die Weisung erhalten, Unterlagen aus dem ärztlichen Bereich einzusehen.

Aus der Problematik der Kenntnisnahme personenbezogener Patientendaten ergeben sich auch Einschränkungen der Einsatzmöglichkeiten externer Datenschutzbeauftragter im Krankenhaus, zumal zweifelhaft ist, ob sie im Hinblick auf ihren Selbständigenstatus als ,,ärztliche Gehilfen" im Sinne des Strafrechts angesehen werden können, so daß personenbezogene Patientendaten, die ihnen bekannt werden, wohl den Schutz des § 203 Abs. 1 u. 3 StGB verlieren würden. Externe könnten ohne dieses Risiko wohl nur insoweit eingesetzt werden, als sie personenbezogene Daten bei ihrer Tätigkeit nicht zu sehen bekommen. Diese Lösung würde auch dem Interesse des Patienten am ehesten entsprechen. Anderes gilt zur Einsichtsbefugnis, wenn sich ein Patient bei einem - internen oder externen - Datenschutzbeauftragten des Krankenhauses unmittelbar beschwert und dabei in die Überprüfung der Verarbeitung seiner personenbezogener Daten durch diesen einwilligt. Die Einwilligung kann allerdings nicht die jeweilige Qualifikation des Datenschutzbeauftragten als ,,ärztlicher Gehilfe" bewirken, von der die Schutzwirkung des § 203 Abs. 1 und 3 StGB abhängt (s.o.). Hierauf wäre der Patient ggf. hinzuweisen.

2.3.6 Verarbeitung medizinischer Patientendaten im Auftrag des Krankenhauses

Aufgrund der Anfragen zweier Krankenhäuser zu Auftragsdatenverarbeitung sei erneut darauf hingewiesen, daß Art. 27 des Bayerischen Krankenhausgesetzes (früher Art. 26) bei der Erteilung einer Befugnis zur Offenbarung von personenbezogenen Patientendaten i.S. von § 203 Abs. 1 Nr. 1 StGB für Zwecke der Auftrags-Datenverarbeitung folgendermaßen unterscheidet:

- Die Vorschrift erteilt für Patientendaten der Krankenhausverwaltung eine Befugnis zur Datenverarbeitung im Auftrag außerhalb des Krankenhauses, wenn die erforderlichen Schutzmaßnahmen sichergestellt sind und solange keine Anhaltspunkte dafür bestehen, daß durch die Art und Ausführung der Auftragsdatenverarbeitung schutzwürdige Belange von Patienten beeinträchtigt werden.

- Zur Verarbeitung von Patientendaten, die nicht zur verwaltungsmäßigen Abwicklung der Behandlung der Patienten erforderlich sind - dies sind die meisten Daten des ärztlichen Bereichs im Krankenhaus,-, erteilt Art. 27 Abs. 4 BayKrG lediglich eine Befugnis zur Datenverarbeitung im Auftrag **bei einem anderen Krankenhaus. Damit** soll sichergestellt werden, daß der Beschlagnahmeschutz nach der Strafprozeßordnung für die oft sehr sensiblen Patientendaten des ärztlichen Bereichs ,,im Gewahrsam einer Krankenanstalt" (§ 97 Abs. 2 StPO) erhalten bleibt.

Für Daten, die für die verwaltungsmäßige Abwicklung der Behandlung des Patienten erforderlich sind (im wesentlichen die Daten der Krankenhausverwaltung für die Patientenabrechnung) ist die Einschränkung auf andere Krankenhäuser nicht getroffen worden, weil diese Daten ohnehin an Abrechnungsstellen und Krankenkassen weitergeleitet werden müssen.

2.3.7 Übermittlung von Patientendaten an Taxiunternehmer zu Abrechnungszwecken

In einer Eingabe wurde berichtet, daß ein Krankenhaus den Patienten für Transporte per Taxi einen Abrechnungsschein gab, der dem Taxifahrer zur Abrechnung auszuhändigen war. Auf der Rückseite des Scheins befand sich ein Aufkleber mit personenbezogenen Daten des

Patienten, u.a. mit Namen und vollständiger Wohnanschrift. In der Eingabe wurde die Weitergabe dieser personenbezogenen Daten bemängelt.

Die Ermittlung des Sachverhalts ergab, daß die Vordrucke der Fahrtaufträge laut Vorgabe den Namen des Fahrgastes enthalten sollten. Die Adresse wurde durch die an sich nicht vorgesehene Verwendung der im Krankenhaus gebräuchlichen Klebeetiketten mit Patientendaten weitergegeben.

Die Etiketten wurden in einigen Stationen des Krankenhauses für die Taxifahrtaufträge verwendet, obwohl seitens der Krankenhausverwaltung früher bereits auf die Unzulässigkeit dieses Verfahrens hingewiesen worden war Die umgehende Einstellung der Verwendung dieser Etiketten auf Fahrtaufträgen durch alle Stationen des Krankenhauses wurde mir zugesagt.

Die Erörterung mit dem Krankenhaus ergab aber auch, daß die Offenbarung von Patientendaten auf den Fahrtaufträgen weder zu Beförderungs- noch zu Abrechnungszwecken erforderlich ist (Art. 27 Abs. 5 BayKrG). Auch von einer Einwilligung des Patienten in die personenbezogene Datenübermittlung kann nicht ausgegangen werden. Unter Einschaltung der Bayerischen Krankenhausgesellschaft wurde daher erörtert, ob der auf dem Fahrtauftrag vorgesehene Name des Patienten durch die Krankenhaus-Aufnahmenummer ersetzt werden kann. Dies erscheint möglich. Damit würde vermieden, daß insbesondere bei selteneren Namen über Telefonbücher die Wohnanschrift ausfindig gemacht werden kann. Der Fahrtauftrag kann danach so gestaltet werden, daß er für Dritte, abgesehen von der zu Beweiszwecken erforderlichen, aber oft unleserlichen Unterschrift, anonym ist. Das Krankenhaus hat eine entsprechende Änderung zugesagt.

2.4 Gesundheitsämter

2.4.1 Gesundheitsamt - Zusatzfragebogen zur Einschulung

Zusammen mit einer Hochschulklinik hat ein Gesundheitsamt bei der Einschulungsuntersuchung die Eltern gebeten, einen zusätzlichen Fragebogen zur Einschulung auszufüllen. Er enthielt Fragen für eine wissenschaftliche Untersuchung über Probleme der Impfbereitschaft. Von den Fragen her war der Bogen anonym gestaltet. Im Kopf des Bogens sollte jedoch der untersuchende Arzt Daten aus seiner Untersuchung - ohne identifizierende Angaben - eintragen. Zum Zeitpunkt der Einschulungs-Untersuchung war dem Arzt die Identität von Mutter und Kind bekannt.

Zur Sicherung der Anonymität der Erhebung dieser zusätzlichen Daten bei der Einschulung habe ich gefordert, daß erst der Arzt und danach die Mutter den Bogen ausfüllen und die Mutter den Fragebogen nach dem Ausfüllen in einem Kuvert in einen mit dem Siegel der Hochschulklinik verschlossenen Kasten einwirft, der lediglich einen Einwurfschlitz hat und keine Möglichkeit zur Herausnahme des Inhalts ohne Bruch des Siegels bietet. Auf dem Kasten mußte deutlich lesbar angebracht werden, daß der Inhalt für die Hochschulklinik zur wissenschaftlichen Auswertung bestimmt ist. Die Erhebungsbögen werden im Hochschulinstitut vernichtet, sobald sie zur Auswertung nicht mehr erforderlich sind.

2.4.2 Gesundheitsämter - anonyme Schwangerschaftskonfliktsberatung

Das Bundesverfassungsgericht hat im Urteil vom 28.05.1993 zum Schwangerschaftsabbruch in seiner Anordnung folgende Festlegung getroffen:

- Beratung der Schwangeren auf Wunsch anonym

- Erteilung einer auf den Namen der Frau lautenden Bescheinigung über die Tatsache der Beratung und

- Erstellung eines Protokolls über die Beratung, das keine Rückschlüsse auf die Identität der Schwangeren erlaubt, in dem Alter, Familienstand, Staatsangehörigkeit, Zahl der Schwangerschaften, der Kinder und frühere Schwangerschaftsabbrüche festzuhalten und die für den Abbruch genannten wesentlichen Gründe, die Dauer des Gesprächs und die hinzugezogenen weiteren Personen zu vermerken sind.

Die Anonymität der Beratung wurde bei der Beratungsstelle eines Gesundheitsamtes überprüft. Folgende Maßnahmen zur Sicherung der Anonymität wurden dabei als wichtig festgestellt:

1. Bei telefonischer Vereinbarung des Beratungstermins muß bereits auf die Möglichkeit der anonymen Beratung hingewiesen werden. Eine **namentliche Eintragung im Terminkalender** ist zu vermeiden.

2. In der Beratungsstelle müssen ein oder ggf. auch **mehrere Schilder, die auf** das **Angebot einer anonymen Beratung** hinweisen, so aufgehängt werden, daß sie von den Wartenden mit Sicherheit nicht übersehen werden.

3. Jede Beraterin weist vor Beginn des Gesprächs auf die **Möglichkeit der anonymen Beratung** und der Erteilung einer Bestätigung über die Tatsache der Beratung mit Namen hin, wobei auf Wunsch darauf verzichtet wird, daß ein Durchschlag der Bestätigung bei der Beratungsstelle verbleibt.

4. Wenn innerhalb des Rahmens der Beratung nach § 218 StGB auch Fachärztinnen, etwa für genetische Beratung oder Psychologinnen beigezogen werden müssen, kann sich das Problem der **Dokumentation von ärztlichen Feststellungen und Ratschlägen** stellen. Nach den Vorgaben des Bundesverfassungsgerichts muß auch in solchen Fällen die Möglichkeit einer anonymen Beratung sichergestellt bleiben. Durch organisatorische Maßnahmen muß daher ausgeschlossen werden, daß solche Unterlagen von der Beratungsstelle bzw. der Beraterin eingesehen werden können.

5. In seiner Anordnung fordert das Bundesverfassungsgericht, daß das Protokoll „in einer Weise, die **keine Rückschlüsse auf die Identität der Beratenen** erlaubt" abgefaßt wird. Da das Gebot der Wahrung der Anonymität vorgeht, hat die Kennzeichnung bestimmter Merkmale, die nach der Anordnung des Bundesverfassungsgerichts ebenfalls grundsätzlich festzuhalten sind, zu unterbleiben, wenn sie Rückschlüsse auf die Identität der Schwangeren zulassen könnten (z.B. sehr seltene Staatsangehörigkeit verbunden mit ungewöhnlich hoher Kinderzahl o.ä.).

6. Nach Anordnung des Bundesverfassungsgerichts hat die Beratungsstelle der Frau auf Antrag über die Tatsache der Beratung eine **auf ihren Namen lautende,** mit dem Datum des letzten Beratungsgesprächs versehene **Bescheinigung** auszustellen. Nach dem hierzu ergangenen Schreiben des Sozialministeriums an die Beratungsstellen sind von diesen Bestätigungen **Durchschriften für die Beratungsstelle** herzustellen, auf die die beratenden Personen keinen Zugriff haben. Die Aufbewahrung der Durchschrift dient nach dem Schreiben allein dem Schutz der Frau, damit bei Verlust oder Zerstörung durch Dritte vor Aufsuchen des Arztes ohne Probleme eine Zweitschrift ausgestellt werden kann. Auch bei Verlust des Originals bei späteren Rechtsstreitigkeiten bis hin zu Strafverfahren kann dann noch nachgewiesen werden, daß die Frau die Voraussetzungen für einen straffreien Abbruch erfüllt hat.

   Ich habe dieses Verfahren akzeptiert, um die genannten Nachweise zu ermöglichen. Gefordert wurde allerdings, daß **Beratungsprotokolle** von den **Durch**schlägen, die den Namen der Beratenen enthalten, absolut zu **trennen** sind. Dies gilt sowohl für die räumliche Aufbewahrung als auch personell für die Verwaltung bzw. für den Zugriff auf die Unterlagen. Auch inhaltlich darf keine Verbindung zwischen Protokoll und einer bestimmten Beratung und den Bestätigungsdurchschlägen herstellbar sein.

   Das Sozialministerium hat diese Forderung in seine Richtlinien für die Beratungsstellen übernommen. Es hat in seinem Schreiben an die Beratungsstelle außerdem klargestellt, daß eine Beratungsbescheinigung auch dann zu erteilen ist, wenn die Frau die **Aufbewahrung** einer Durchschrift bei der Beratungsstelle verweigert. In diesem Falle entfällt die Herstellung bzw. Aufbewahrung einer Durchschrift bei der Beratungsstelle.

7. Die Beratungsbescheinigungen müssen in einem ausreichend sicheren Behältnis verschlossen **aufbewahrt** werden.

8. Für die **Aufbewahrung** von Protokollen und Durchschlägen der Beratungsbestätigungen müssen **Fristen** noch festgelegt werden. Die Protokolle sollten vernichtet werden, sobald sie für , die Kontrollzwecke, insbesondere im Zusammenhang mit der Wiedererteilung der Anerkennung oder für wissenschaftliche Zwecke oder zur Überprüfung des Verfahrens auf seine Effektivität nicht mehr benötigt werden. Bei den Durchschlägen der Beratungsbescheinigung wird derzeit noch eine 5-jährige Aufbewahrung, wie bei den bisherigen Bestätigungen nach dem Bayer. Schwangerenberatungsgesetz nicht beanstandet, solange noch keine neue gesetzliche Regelung aufgrund des Urteils des Bundesverfassungsgerichts getroffen ist.

2.5 Entwurf für landesrechtliche ergänzende Regelungen zum Schwangeren- und Familienhilfegesetz des Bundes

Der Ministerrat hat im Juli den vom Sozialministerium vorgelegten Eckpunkten zu gesetzlichen ergänzenden Regelungen zum Schwangeren- und Familienhilfegesetz des Bundes zugestimmt. Sie enthalten die landesrechtliche Ergänzung des geplanten bundesrechtlichen Schwangeren- und Familienhilfegesetzes. Nach einer Mitteilung der Staatsregierung handelt es sich um verschiedene ärztliche Berufspflichten und solche Regelungsaufträge des Bundesverfassungsgerichts, deren sich der Bundesgesetzgeber nicht annimmt (Bulletin der Bayerischen Staatsregierung vom 26. Juli 1994, Seite 4).

Kurze Zeit vorher hatte ich den Regelungsentwurf erhalten. Ich hatte dazu im wesentlichen zwei Vorschläge gemacht, die in der Ministerratsvorlage noch Berücksichtigung gefunden haben:

1. Ärzte, die Schwangerschaftsabbrüche durchführen, sollten zu besonderen **Aufzeichnungen** über die **Tatsache** der **Darlegung der Gründe** für das Verlangen der Frau nach Abbruch der Schwangerschaft verpflichtet werden. Ich hatte mich dagegen gewandt, über die Dokumentation der Tatsache der Darlegung hinaus auch die Dokumentation der **dargelegten Gründe** selbst vom Arzt zu fordern. Eine solche erweiterte Dokumentationspflicht läßt sich aus den Gründen des Urteils des Bundesverfassungsgerichts vom 28. Mai 1993 nicht ableiten. Die Feststellung und Beurteilung einer Indikation wird vom Arzt gerade nicht verlangt. Er muß sich die Gründe lediglich für seine eigene Entscheidung darüber, ob er den Abbruch vornimmt, darlegen lassen (Urteilsbegründung Seite 123, 1. e).

2. Nach der Urteilsbegründung (S.127) muß der Gesetzgeber prüfen, ob eine **„Begrenzung** der Zahl der Abbrüche auf einen bestimmten **Anteil** der insgesamt vorgenommenen **ärztlichen Verrichtungen"** und eine „einheitlich festgelegte Höhe der **Vergütung** für einen Schwangerschaftsabbruch", wie in Frankreich, einzuführen ist.

Ich habe hierzu vorgeschlagen, nicht etwa Durchschriften der Gebührenrechnungen aufzubewahren, sondern je Schwangerschaftsabbruch einen pauschalierten Betrag

anzusetzen. Die Verwendung von Zweitschriften würde einen hohen Aufwand erzeugen und trotz sog. faktischer Anonymisierung ein Reidentifizierungsrisiko möglicherweise nicht ausschließen, denn auch auf Zweitschriften werden nähere Umstände wie Diagnose, Gebührenordnungspositionen bzw. GOÄ-Nummern und der Behandlungstag festgehalten. Meine Anregung wird geprüft.

2.6 Alarmierung von Rettungsdienst und Notarzt unter Notruf 112

Im letzten Tätigkeitsbericht hatte ich das Problem dargestellt, daß in Gebieten, in denen keine ständig besetzten Einsatzzentralen der Feuerwehr existieren, eine Alarmierung von Rettungsdienst oder Notarzt über Notruf 112 bei Polizeidienststellen eingeht. Die Vollzugspolizisten, die den Anruf entgegennehmen, sind nach den gesetzlichen Bestimmungen (StPO, PAG) verpflichtet, den Anruf nicht nur an Rettungsdienst oder Notarzt weiterzuleiten, sondern auch ggf. strafverfolgend oder zur Gefahrenabwehr tätig zu werden. In diesen Gebieten macht es die Organisation des Notrufs 112 den Bürgern praktisch unmöglich, sich über diese Notrufnummer vertraulich ausschließlich an Rettungsdienst oder Notarzt zu wenden.

Wie ich inzwischen erfahren habe, besteht voraussichtlich in nächster Zeit keine Möglichkeit, hier eine organisatorische Verbesserung durch Trennung der Bereiche vorzunehmen. Wer vermeiden möchte, daß sein Notruf über Nr. 112 bei der Polizei aufläuft, muß die bayernweit verfügbare Rufnummer 19222 (ggf. mit Vorwahlnummer) wählen, die unmittelbar bei den ständig besetzten Rettungsleitstellen eingeht.

Angesichts dieser Situation halte ich es für erforderlich, in den oben genannten Gebieten die Bevölkerung darüber zu unterrichten, daß alle Anrufe über Notruf 112 bei der Polizei auflaufen (nicht nur die Anrufe über Nr.110) und daß eine unmittelbare Benachrichtigung von Notarzt oder Rettungsdienst ohne Einschaltung der Polizei nur über Nummer 19222 (ggf. mit Vorwahlnummer) möglich ist.

Leider konnte ich das Staatsministerium des Innern nicht von der Notwendigkeit eines solchen Hinweises an die Bevölkerung in den betreffenden Gebieten überzeugen. Das Ministerium ist der Ansicht, dem Bürger werde es in aller Regel und in akuten Notsituationen völlig gleichgültig sein, ob die Polizei den Notruf entgegen nimmt oder eine andere Organisation.

Ich werde das geschilderte Problem im Auge behalten und darüber wieder berichten, sobald sich ein Anlaß ergibt.

2.7 Chipkarten im Gesundheitswesen

Nach § 291 des 5. Buches des Sozialgesetzbuches (SGB V) stellen die gesetzlichen Krankenkassen spätestens bis zum 1. Januar 1995 für jeden Versicherten eine Krankenversichertenkarte aus, die den bisherigen Krankenschein ersetzt. In § 291 Abs. 2 SGB V ist gesetzlich festgelegt, daß die Karte ausschließlich die dort genannten Daten enthalten darf, nämlich:

1. Ausstellende Krankenkasse
2. Namen
3. Geburtsdatum
4. Anschrift
5. Krankenversichertennummer
6. Versichertenstatus
7. Tag des Beginns des Versichertenschutzes
8. bei befristeter Gültigkeit der Karte das Datum des Fristablaufs.

Die gesetzliche Festlegung des Inhalts schließt aus, daß auf der gleichen Karte weitere Daten auf freiwilliger Basis gespeichert werden. Der Grund dafür ist, daß der Versicherte **verpflichtet** ist, die **Karte** beim Arzt und anderen Behandlungen **vorzuzeigen.** Er kann nicht nach freier Entscheidung bestimmen, wer den Karteninhalt liest und verwendet (siehe auch 14. TB 1992, Nr. 3.3, Seite 16).

Von verschiedener Seite wird nun immer wieder ins Gespräch gebracht, auf freiwilliger Basis weitere Daten auf anderen Chipkarten zu speichern, um sie jederzeit verfügbar zu haben, so z.B. ,,Gesundheitskarten" oder ,,Servicekarten", ,,Notfallkarten", ,,A-Cards" und ,,Röntgen-Karten". Die Anschaffung der Karten und Verwendung ist zwar grundsätzlich freiwillig. Manche (außerbayerische) Krankenkassen wollen aber solche Karten einführen und bei Verwendung der Karte Vorteile in Aussicht stellen. Die Freiwilligkeit kann sich dadurch relativieren.

Zur strikten **Trennung** zwischen **gesetzlicher Krankenversichertenkarte** und den verschiedenen Arten **freiwilliger Gesundheitskarten** hat die Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 9./10. März 1994 einen Beschluß gefaßt. Er ist in der **Anlage** zu diesem Tätigkeitsbericht abgedruckt.

Eine Nachfrage bei den zuständigen Verbänden der bayerischen Krankenkassen hat bisher keinen Hinweis darauf erbracht, daß in Bayern von den gesetzlichen Krankenkassen derartige freiwillige Gesundheitskarten geplant sind.

Anzumerken ist noch, daß von Journalisten gelegentlich kritisiert wird, daß auf der gesetzlichen Krankenversichertenkarte keine zusätzlichen Gesundheitsdaten gespeichert werden dürfen. Bei solcher Kritik wird regelmäßig die Verpflichtung des Versicherten übersehen, die Karte mit den ,,Krankenscheindaten" jedem vorzulegen, in dessen Behandlung er sich begibt. Der Versicherte sollte aber nicht gezwungen sein, durch die Kombination von Pflicht-Angaben mit zusätzlichen freiwilligen Krankheitsdaten auf einer einzigen Karte bei deren Vorlage auch Angaben über seinen Gesundheitszustand bekannt zu

geben. Dies sollte seiner freien Entscheidung überlassen bleiben. Der Ausschluß des Speicherus von Gesundheitsdaten auf der gesetzlichen Krankenversichertenkarte dient dem Selbstbestimmungsrecht des Versicherten.

3. Sozialbehörden

3.1 Änderung von Rechtsvorschriften

Aus meiner Sicht ist auf zwei wichtige Änderungen hinzuweisen:

3.1.1 Gesetz zur Änderung des Sozialgesetzbuches - 2. SGBÄndG vom 13.6.1994

Im Berichtszeitraum ist das 2.SGBÄndG vom Bundestag verabschiedet worden und hinsichtlich maßgeblicher datenschutzrechtlicher Bestimmungen am 1.7.1994 in Kraft getreten. In der Neufassung des 2. Kapitels des 10. Buches des Sozialgesetzbuches (SGB X) wurde eine Verweisung auf Vorschriften des BDSG weitestgehend vermieden. Die wesentlichen Bestimmungen, so auch die **Begriffsdefinitionen des BDSG** wurden in den Text des **SGB** übernommen. Der Leser hat nun einen weitgehend geschlossenen Gesetzestext zur Verfügung.

Den Regelungen im 2. Kapitel des SGB X, die sich im wesentlichen mit dem Schutz der Sozialdaten vor unbefugten Übermittlungen befassen, wurden die Begriffsdefinitionen sowie Vorschriften über die Zulässigkeit der Datenerhebung, -verarbeitung und -nutzung vorangestellt. Laut amtlicher Begründung verfolgte der Gesetzgeber dabei eine ,,enge Anlehnung an das BDSG, insbesondere bei der Festlegung der Zweckbindung der Datenverwendung."

SGB-spezifische Übermittlungsregelungen (früher Offenbarungsbefugnisse) behielten ihre jeweiligen Paragraphenziffern und entsprechen überwiegend den bisherigen Regelungen. Unterschiede zum BDSG resultieren aus den speziellen Gegebenheiten des Sozialleistungsrechts. Neu im SGB X eingefügt wurde eine Vorschrift über die Einrichtung automatisierter Abrufverfahren.

Abgerundet wird das 2. Kapitel des SGB X durch die Vorschriften über die besonderen Rechte der Betroffenen, über einen verschuldensunabhängigen Schadensersatzanspruch des Betroffenen bei unzulässiger oder unrichtiger automatisierter Sozialdatenverarbeitung sowie durch Straf- und Bußgeldvorschriften.

Die Neufassung von § 35 SGB 1 und des 2. Kapitels des SGB X erforderte eine Anpassung der datenschutzrechtlichen Vorschriften in den besonderen **Teilen des Sozialgesetzbuches. Ferner wurden im SGB V Ergänzungen** angebracht, deren Notwendigkeit sich aus der Praxis der Krankenversicherung ergeben hat.

Eine Vielzahl von Änderungen ist bei der Verarbeitung personenbezogener Daten durch Sozialbehörden zu beachten. Sie darzustellen würde den Rahmen dieses Berichts jedoch sprengen. Eine **zusammenfassende Darstellung wichtiger Änderungen** kann beim Landesbeauftragten für den Datenschutz angefordert werden.

3.1.2 Vollzugsbekanntmachung zum Bayer. Datenschutzgesetz

Behördlicher Datenschutzbeauftragter, Anlagen und Verfahrensverzeichnis

In der Neufassung der **Vollzugsbekanntmachung zum Bayer. Datenschutzgesetz sind Regelungen über die** Einrichtung behördlicher Datenschutzbeauftragter enthalten. Den Gemeinden, Gemeindeverbänden und sonstigen der Aufsicht des Freistaats Bayern unterstehenden juristischen Personen des öffentlichen Rechts sind die Vorschriften der Vollzugsbekanntmachung zur Anwendung empfohlen. Für die **Sozialversicherungsträger** und ihre Verbände kann sich eine Verpflichtung zur Bestellung von behördlichen Datenschutzbeauftragten aus § 81 Abs. 4 Satz 1 SGB X i.V.m. § 36 BDSG ergeben (VollzBek Nr.3.1).

Nach Art. 27 des Bayer. Datenschutzgesetzes haben bayerische öffentliche Stellen ein Anlagen- und Verfahrensverzeichnis für die automatisierten Verfahren aufzubauen. In das Verfahrensverzeichnis sind auch die automatisierten Verfahren aufzunehmen, mit denen Sozialdaten nach dem Sozialgesetzbuch verarbeitet werden. Sozialversicherungsträger und ihre Verbände führen das Anlagen- und Verfahrensverzeichnis nach Art. 18 Abs. 2 und 3 BDSG (§ 81 Abs. 4 Sätze 1 und 3 SGB X). Eine **Meldung zum Datenschutzregister** beim Landesbeauftragten für den Datenschutz ist im Hinblick auf § 81 Abs. 2 Sätze 2 und 3 SGB X nunmehr auch für bayerische Sozialleistungsträger **nicht mehr erforderlich** (VollzBek Nr.5.1). In das Anlagenverzeichnis sind auch die eingesetzten Datenverarbeitungsanlagen aufzunehmen, mit denen Sozialdaten nach dem Sozialgesetzbuch verarbeitet werden (VollzBek Nr. 5.2).

Nach dem Bayer. Datenschutzgesetz ist die Führung eines Datenschutzregisters beim Landesbeauftragten für den Datenschutz seit 1.8.1993 nicht mehr vorgesehen.

3.2 Gesetzliche Krankenversicherung

3.2.1 Datenübermittlung von der Kassenärztlichen Vereinigung Bayerns an Krankenkassen fallbezogen, nicht versichertenbezogen

Das Sozialgesetzbuch sieht im 5. Buch, das die Vorschriften über die gesetzliche Krankenversicherung enthält (SGB V), in § 295 Abs. 2 vor, daß die Kassenärztlichen Vereinigungen die erforderlichen Angaben über die von den Ärzten abgerechneten Leistungen den Krankenkassen ,,fallbezogen, nicht versichertenbezogen" übermitteln. Nach Abs. 3 der Vorschrift vereinbaren die Spitzenverbände der Krankenkassen und die Kassenärztlichen Bunde svereinigungen in Verträgen das Nähere über Einzelheiten des Datenträgeraustausches.

Im Zuge der noch laufenden datenschutzrechtlichen Überprüfung bei der Kassenärztlichen Vereinigung Bayerns (KVB) wurde ein solcher Vertrag festgestellt, nach dessen § 11 Abs. 2 und 4 für einen Übergangszeitraum eine Datenübermittlung auf einem Papierausdruck nicht nur fallbezogen, sondern durch Hinzufügung von Name, Vorname, Geburtsdatum bzw. Versichertennummer auch versichertenbezogen durchgeführt werden soll. Darüber hinaus sollen nach § 4 Abs. 3 des Vertrages die versichertenbezogenen Behandlungsausweise bei konventionell abrechnenden Ärzten - im Gegensatz zu den mit EDV-abrechnenden Ärzten - weiterhin in einer Sortierung von der KVB an die Krankenkassen übermittelt werden, die der Krankenkasse eine versichertenbezogene Zuordnung von zunächst nur fallbezogen übermittelten Abrechnungsdaten ermöglicht.

Bei der datenschutzrechtlichen Prüfung wurde festgestellt, daß auch bereits vor Abschluß des genannten Vertrages in der vorgenannten Weise versichertenbezogene Daten an die gesetzlichen Krankenkassen übermittelt wurden.

Da somit entgegen § 295 Abs. 2 SGB V den Krankenkassen auf Papierausdruck für die ambulanten Behandlungen Name bzw. Versichertennummer, Geburtsdatum und alle abgerechneten Leistungsdaten mit Diagnosen übermittelt werden, habe ich die Kassenärztliche Vereinigung Bayerns, sowie die Bayerischen Landesverbände der Ortskrankenkassen, der Betriebskrankenkassen und ‚der Innungskrankenkassen zur Stellungnahme aufgefordert und um Vorschläge für Maßnahmen gebeten, mit denen auch für die Dauer des in dem Vertrag vorgesehenen Übergangszeitraums der mit der Regelung in § 295 Abs. 2 SGB V bezweckte Effekt der nur fallbezogenen und nicht versichertenbezogenen Übermittlung sichergestellt werden kann. Ich habe insbesondere vorgeschlagen, auf dem Papierausdruck den Ausdruck des Namens des Versicherten zu unterlassen und allenfalls die Versichertennummer anzugeben und bei KVB und Krankenkassen durch organisatorische Maßnahmen sicherzustellen, daß die personenbezogenen Krankheitsdaten nicht in einer gegen § 295 Abs. 2 SGB V verstoßenden Weise zur Kenntnis genommen oder genutzt werden.

Ich bat die Vorgenannten auch mitzuteilen, welche Daten auf welche Art (Papierausdruck) versichertenbezogen zwischen KVB und Krankenkassen übermittelt werden sollen, sowie zu erläutern, wozu der Versichertenbezug genutzt werden solle und welchen Sinn die Nutzung des Versichertenbezuges während der im Vertragsentwurf vorgesehen Übergangszeit habe, wenn er anschließend auch nach dem Vertragsentwurf entfallen solle. Ich wies darauf hin, daß eine datenschutzrechtliche Beanstandung vorbereitet werde.

Der AOK-Landesverband Bayern legte dar, daß der geplante Vertrag über den Datenaustausch auf Datenträgern zwischen den Spitzenverbänden der Krankenkassen und der Kassenärztlichen Bundesvereinigung erarbeitet worden sei und diese Verbände somit auch für den Inhalt des Vertrages grundsätzlich verantwortlich seien. Sinn der Übergangsregelung des Vertragsentwurfes sei, durch einen Papierausdruck die zu Beginn der Umstellung vom manuellen auf das maschinelle Abrechnungsverfahren notwendigen technischen Voraussetzungen flächendeckend zu schaffen und bestehende Unsicherheiten in den Programmen durch entsprechende Prüfungen abklären zu können.

Mit Schreiben vom 14.11.1994 habe ich dann die Verstöße gegen § 295 Abs. 2 SGB V beanstandet. Die Beanstandung bezieht sich auf die versichertenbezogene Übermittlung der Abrechnungsdaten auf Papierausdrucken durch die KVB an die gesetzlichen Krankenkassen vor Vertragsabschluß und auf die im Vertragsentwurf vorgesehene, gegen § 295 Abs. 2 SGB V verstoßende Übergangsregelung (s.o.). Nicht beanstandet wurde die versichertenbezogene Datenübermittlung, soweit das SGB abweichend vom grundsätzlichen Verbot des § 295 Abs. 2 SGB V eine versichertenbezogene Übermittlung in besonderen Fällen zuläßt, wie z.B. die Übermittlung identifizierender Daten der Versicherten zur Prüfung der Leistungspflicht oder von Leistungsdaten für Stichproben, Einzelfallprüfungen oder Erstattungsansprüche gegen andere Leistungsträger oder Dritte.

Ich ging davon aus, daß es sich bei der bereits praktizierten Datenübermittlung wie bei dem im Datenaustausch-vertrag vorgesehenen Verfahren um zeitlich befristete Übergangsmaßnahmen handelt, die die Umstellung auf das automatisierte Abrechnungsverfahren absichern sollen. Deshalb habe ich trotz Beanstandung davon abgesehen, die sofortige Einstellung dieser versichertenbezogenen Datenübermittlung auf Papierausdrucken zu fordern, wenn jeweils die KVB ihre Bundesvereinigung und die Bayerischen Krankenkassenverbände ihre Bundesverbände auffordern, im Vertrag eine gesetzeskonforme Lösung vorzusehen. Zu beachten ist nämlich, daß durch den zwischen den genannten Bundesstellen zu schließenden Vertrag eine Bindungswirkung eintritt, die die bayerischen Kassen daran hindert, ein anderes Verfahren einzuführen, als es im Vertrag vorgesehen ist. Ob diese Bindungswirkung durch den Verstoß gegen § 295 Abs. 2 SGB V insoweit aufgehoben wird, steht nicht mit hinreichender Sicherheit fest. Es ist deshalb vordringlich, den Vertrag bereits für den Übergangszeitraum gesetzeskonform zu gestalten. KVB und Bayerische Kassenverbände müssen aber gegen ein gesetzeswidriges Verfahren deutlich remonstrieren.

Von den Bayerischen Krankenkassen habe ich gefordert, soweit von der KVB wahrend des Übergangszeitraums Leistungsdaten mit Diagnosen versichertenbezogen übermittelt werden, diese auf Seite der Kassen so zu verarbeiten und zu nutzen, daß die mit § 295 Abs. 2 SGB V gesetzlich vorgesehene Wirkung erhalten bleibt, d.h. den Versichertenbezug, soweit nicht gesetzlich zugelassen, nicht zu nutzen und kein versichertenbezogenes Leistungskonto über ambulante Leistungen aufzubauen.

Außerdem habe ich KVB und Krankenkassenverbänden dringend empfohlen, bei den Datenübermittlungen per Ausdruck zumindest die Namen der Versicherten zu unterdrücken, um unnötige Kenntnisnahmen zu vermeiden. Den Krankenkassen verbleibt die Möglichkeit, den Versicherten anhand der Krankenversichertennummer zu identifizieren, wenn das für die gesetzlich erlaubten Fälle (s.o.) erforderlich ist.

Die Krankenkassen-Landesverbände habe ich gebeten, ihren Krankenkassen die Beanstandungen und die Forderungen mitzuteilen und mich über das Veranlaßte zu unterrichten. Inzwischen erklärten der AOK-Landesverband, der BKK-Landesverband und der Landesverband der Innungskrankenkassen ihre Bereitschaft, den Mitgliedskassen zu empfehlen, die im Rahmen dieser Übergangsregelung erhaltenen Daten so zu behandeln, daß den Vorschriften des SGB V, insbesondere § 295 Abs. 2, Genüge getan werde.

Das Bayerische Sozialministerium hat als Rechtsaufsichtsbehörde die Kassenärztliche Vereinigung Bayerns und die bayerischen gesetzlichen Krankenkassen gebeten, meinen Forderungen baldmöglichst zu entsprechen.

3.2.2 Anforderung von hausärztlichen Attesten „im verschlossenen Umschlag"

Von Betroffenen wurde ich darauf aufmerksam gemacht, daß für den Medizinischen Dienst der Krankenversicherung (MDK) immer wieder Atteste von Hausärzten über gesetzlich Versicherte mit folgendem Hinweis angefordert werden:

> ,,Berichte bitte den Versicherten verschlossen ‚mitgeben"

Meines Erachtens hat jedoch der Versicherte, wenn er im Rahmen seiner Mitwirkung ein von ihm bei seinem Hausarzt besorgtes Attest dem MDK überbringt, ein Recht darauf, vom Inhalt des Attestes Kenntnis zu nehmen. Würde ihm dieses Recht verweigert, könnte nicht von Mitwirkung gesprochen werden, denn dazu gehört nicht nur die Einwilligung in die Untersuchung, sondern auch die Einwilligung in die Weiterleitung des Untersuchungsergebnisses an den MDK. Von einer wirksamen Einwilligung in diese Weiterleitung kann aber schwerlich ausgegangen werden, wenn der Betroffene nicht wenigstens die Gelegenheit zur Kenntnisnahme hatte.

Im übrigen hätte der Versicherte nach § 276 Abs. 3 SGB V i.V.m. § 25 SGB X ohnehin das Recht, das Attest einzusehen, sobald es sich in den Akten des MDK befindet. Eine Ausnahme hiervon käme nur in Fällen des sogenannten therapeutischen Privilegs in Betracht (§ 25 Abs. 2 Satz 2 SGB X). Aber auch in diesen Fällen wird nach § 25 Abs. 2 Satz 4 SGB X das Recht zur Kenntnisnahme ,,nicht beschränkt". Wenn also der Versicherte das Attest beim MDK im Wortlaut lesen und sich auch fotokopieren lassen darf, dann spricht nichts dagegen, daß er den Inhalt bereits vor Übergabe an den MDK zu Kenntnis nimmt.

Im Falle einer Mitteilung, die unter das therapeutische Privileg fallen würde, sollte der Arzt das Attest nicht dem Versicherten zur Weiterleitung übergeben, sondern dem MDK per Post übersenden.

Ich habe daher den AOK Landesverband Bayern gebeten, bei der Anforderung der Atteste für den MDK auf den Satz ,,Bericht bitte den Versicherten verschlossen mitgeben" zu verzichten.

Der AOK Landesverband hat mitgeteilt, daß geplant ist, die Einladungen der Versicherten zu sozialmedizinischen Untersuchungen künftig unmittelbar durch den MDK vornehmen zu lassen. Dabei werde darauf hingewirkt, daß bei den Einladungsschreiben der o.g. Hinweis nicht mehr erfolgt.

3.2.3 Nutzung von Anschriften privat Krankenversicherter durch gesetzliche Krankenkassen

Der 15. Tätigkeitsbericht enthält Ausführungen zu der Frage, ob eine gesetzliche Krankenkasse die Adressen **ihrer Mitglieder** nutzen darf, um diese im Zusammenhang mit **Neugründungen von Betriebskrankenkassen** anzuschreiben.

Nunmehr war die Frage zu beantworten, ob eine Ortskrankenkasse die bei ihr gespeicherten Anschriften **privat Krankenversicherter** nutzen darf, um die von der **Errichtung einer Betriebskrankenkasse** betroffenen privatversicherten Arbeitnehmer anzuschreiben und für die Ablehnung der Betriebskrankenkasse zu werben. Im Ergebnis war die konkret vorgenommene ,,Aufklärung" zu beanstanden, da die Krankenkasse den eigenen Beitragssatz mit dem zu erwartenden kalkulierten Beitragssatz der zu gründenden Betriebskrankenkasse wettbewerbsrechtlich unzulässig verglichen hatte und ihre ,,Aufklärung" mit der Feststellung abschloß: ,,Ihre Entscheidung bei der Abstimmung (über die Frage der Errichtung der BKK) kann deshalb nur lauten: BKK NEIN!"

Dieser Vorfall gab Anlaß, **Inhalt und Grenzen einer sachlichen Information privat versicherter Arbeitnehmer durch eine Ortskrankenkasse** in diesem Zusammenhang zu überprüfen.

Die Ortskrankenkassen verfügen über Anschriften privat Krankenversicherter als Einzugsstelle von Beiträgen zur Renten- und Arbeitslosenversicherung, § 28 h, 28 i Abs. 1 Satz 2 SGB IV.

§ 284 Abs. 3 SGB V erlaubt zwar der Krankenkasse, rechtmäßig erhobene und erfaßte versichertenbezogene Daten für die Zwecke der Aufgaben nach § 284 Abs. 1 SGB V im jeweils erforderlichen Umfang zu verwenden. Soweit es durch Rechtsvorschriften des Sozialgesetzbuches angeordnet oder erlaubt ist, dürfen die genannten Daten auch für andere Zwecke im erforderlichen Umfang Verwendung finden. Im vorliegenden Fall wurden jedoch zum einen keine **versichertenbezogenen** Daten verwendet, die **zum Zwecke** der **Krankenversicherung** erhoben und

erfaßt worden wären. Infolge der Verweisung auf § 284 Abs. 1 SGB V bezieht sich § 284 Abs. 3 SGB V nur auf personenbezogene Daten der bei **der jeweiligen Krankenkasse Versicherten und ausschließlich auf Daten, die für Zwecke der Krankenversicherung** erhoben und erfaßt wurden. § 284 Abs. 3 SGB V ist für eine Aufklärung im geschilderten Zusammenhang daher nicht anwendbar.

Nach **§ 67 c Abs. 1 Satz 1 SGB *X*** ist (u.a.) zum anderen das Nutzen von Sozialdaten durch Sozialleistungsträger zulässig, wenn es zur Erfüllung der in der Zuständigkeit der speichernden Stelle liegenden gesetzlichen Aufgaben nach dem Sozialgesetzbuch erforderlich ist und es für die Zwecke erfolgt, für die die Daten erhoben worden sind. Sind die Sozialdaten bei der Krankenkasse bereits in anderem Zusammenhang gespeichert (hier für den Einzug der genannten Sozialversicherungsbeiträge), dürfen sie gemäß § 67 c Abs. 2 Nr.1 SGB X **für andere Zwecke** nur gespeichert, verändert oder genutzt werden, wenn die Daten für die Erfüllung von Aufgaben nach anderen Rechtsvorschriften des Sozialgesetzbuches als diejenigen, für die sie erhoben wurden, erforderlich sind.

Eine derartige Vorschrift nach dem Sozialgesetzbuch im Sinne des § 67 c Abs. 1 und Abs. 2 Nr.1 SGB X stellt **§ 13 SGB 1** dar, dessen Voraussetzungen im gegebenen Fall aber überschritten wurden. Diese Vorschrift enthält eine Verpflichtung der Leistungsträger, im Rahmen ihrer Zuständigkeit ,,die Bevölkerung" über die Rechte und Pflichten nach dem Sozialgesetzbuch **aufzuklären.** Hiervon erfaßt wird eine allgemeine und abstrakte Un-,terrichtung der von Rechten und Pflichten nach dem Sozialgesetzbuch in einem bestimmten Zusammenhang möglicherweise betroffenen, in der Regel im einzelnen nicht bekannten Personen. Sofern ein solcher Personenkreis allerdings eingrenzbar und bekannt ist, kann im Einzelfall eine ,,Aufklärung der Bevölkerung" ausnahmsweise auch einmal in einem Anschreiben an einzelne ,Betroffene in Betracht kommen.

Die maßgeblichen Berechtigungen nach dem Sozialgesetzbuch, über welche die Ortskrankenkassen im Rahmen des § 13 SGB 1 auch Mitglieder privater Krankenversicherungen aufklären dürfen, finden sich den in §§ 148 Abs. 2 Satz 1, 257 Abs. 2 Satz 2 SGB V. Sobald eine Betriebskrankenkasse errichtet wird, wäre letztere für den Personenkreis privat Krankenversicherter bei unterstellter Versicherungspflicht zuständig. Der vom Arbeitgeber gezahlte Zuschuß zur privaten Krankenversicherung beträgt dann nur noch die Hälfte des Beitrags, den der Beschäftigte fiktiv an die Betriebskrankenkasse zu entrichten hätte (höchstens jedoch die Hälfte des Betrages, den er für seine Krankenversicherung tatsächlich zu zahlen hat). Da die Errichtung einer BKK für den Arbeitgeber nur von Interesse ist, wenn der kalkulierte allgemeine Beitragssatz dieser BKK niedriger ausfällt als derjenige der örtlich zuständigen Krankenkasse, besteht für die **ebenfalls über die Errichtung einer BKK abstimmungsberechtigten privatversicherten Arbeit-nehmer** ein konkretes Risiko der Senkung ihres Beitragszuschusses durch den Arbeitgeber und somit das Risiko finanzieller Einbuße. Da nicht mit Sicherheit davon ausgegangen werden kann, daß jeder Arbeitgeber seinerseits die privat versicherten Arbeitnehmer hinreichend gezielt auf diese Zuschußminderung hinweist, besteht ein Aufklärungsbedarf seitens der Betroffenen im Sinne des § 13 SGB 1.

Die Ortskrankenkasse darf dabei **jedoch den Rahmen einer objektiven und sachlich gehaltenen Aufklärung** nicht sprengen. Sofern diese Grenzen eingehalten werden, ist die Nutzung der Anschriften privat Krankenversicherter durch die Ortskrankenkassen zur Versendung dieser Information durch die genannten Vorschriften des Sozialgesetzbuchs gedeckt.

Im gegebenen Fall wurden diese Grenzen aber aus den eingangs genannten Gründen überschritten.

Das Staatsministerium für Arbeit und Sozialordnung, Familie, Frauen und Gesundheit hat vorstehende Rechtsauffassung geteilt.

3.3 Sozialhilfe

3.3.1 Abgleich von Daten von Sozialhilfeempfängern mit Kfz-Zulassungsdaten - § 117 Abs. 3 BSHG

Durch das Gesetz zur Umsetzung des Förderalen Konsolidierungsprogramms (FKPG) vom 23.6.1993 wurde §117 Bundessozialhilfegesetz (BSHG) neu gefaßt. Die Vorschrift soll dazu beitragen, daß die mißbräuchliche Inanspruchnahme von Sozialhilfeleistungen unterbleibt oder aufgedeckt wird.

Aus dem Kreise der Datenschutzbeauftragten ist die Frage aufgeworfen worden, ob und in welchem Umfang zwischen Sozialamt und Kfz-Zulassungsstelle nach §117 Abs. 3 BSHG Daten automatisiert abgeglichen werden dürfen, insbesondere für die bis zum Inkrafttreten der Vorschrift angesammelten , Altfälle. Teilweise wird die Ansicht vertreten, es sei nur ein nicht automatisierter Ab-gleich einzelner Antragsfälle bei entsprechendem Anfangsverdacht zulässig.

Nach § 117 Abs. 3 BSHG sind die Träger der Sozialhilfe befugt, ,,zur Vermeidung rechtswidriger Inanspruchnahme von Sozialhilfe Daten von Personen, die Leistungen nach diesem Gesetz beziehen, bei anderen Stellen ihrer Verwaltung, bei ihren wirtschaftlichen Unternehmen und bei den Kreisen, Kreisverwaltungsbehörden und Gemeinden zu überprüfen, soweit diese für die Erfüllung dieser Aufgaben erforderlich sind." Die Träger der Sozialhilfe dürfen für die Überprüfung nur die in § 117 Abs. 1 Satz 2 BSHG genannten Daten übermitteln. Die ersuchte Stelle darf dagegen nur die in § 117 Abs. 3 Satz 3 BSHG enumerativ genannten Daten übermitteln; sie ist zur Auskunft verpflichtet und hat die ihr im Rahmen der Überprüfung übermittelten Daten nach Vornahme der Auskunft unverzüglich zu löschen. Dies bedeutet z.B., daß die Kfz-Zulas-

sungsstelle im Rahmen des § 117 Abs. 3 Satz 3 Buchstabe f BSHG nur übermitteln darf, ob ein Hilfeempfänger Kraftfahrzeughalter ist. Sonstige Daten, wie Fahrzeugtyp, amtliches Kennzeichen und Baujahr des Pkw dürfen aufgrund dieser Vorschrift nicht mitgeteilt werden.

Zu der Frage des zulässigen Umfangs der Überprüfung von Daten nach § 117 Abs. 3 BSHG kann m.E. aus dieser Vorschrift nicht zwingend abgeleitet werden, daß eine Datenüberprüfung nur manuell, nur im Einzelfall und nur bei Vorliegen eines Anfangsverdachts zulässig wäre, d.h. eineDVunterstützte Abfrage bzw. ein automatisierter Datenabgleich mehrerer Fälle (z.B. der Altfälle) unzulässig wäre.

Zwar setzt eine Abfrage im manuellen wie im maschinellen Verfahren für einzelne wie für gesammelte Fälle voraus, daß die Patenüberprüfung für die Erfüllung der Aufgaben des Trägers der Sozialhilfe **erforderlich ist** Die Bedingung der ,,Erforderlichkeit" führt jedoch nicht dazu, die Überprüfung der bis zum Inkrafttreten des §117 Abs. 3 BSHG aufgelaufenen **Altfälle** in zusammengefaßter Form mit DV-Unterstützung auszuschließen. Sie bewirkt vielmehr, daß in die Datenüberprüfung keine Fälle einbezogen werden dürfen, in denen die Überprüfung nach Kenntnis des Sozialhilfeträgers nicht erforderlich ist (etwa wenn höchst unwahrscheinlich ist, daß Antragsteller überhaupt Eigentümer eines verwertbaren Kfz sind, wie z.B. Kinder, Schwerstbehinderte oder sehr alte Sozialhilfebezieher). Die Erforderlichkeit der Überprüfung kann sich aus Erfahrungen der Sozialhilfebehörde ergeben, etwa wenn Eigentum an Kraftfahrzeugen öfters verschwiegen wird.

Die unterschiedliche Formulierung der Absätze 1 und 2 des § 117 BSHG im Vergleich zu dessen Absatz 3 erschwert zwar die Auslegung des Abs. 3. Aus der Tatsache, daß nur in den Absätzen 1 und 2 von automatisiertem Datenabgleich die Rede ist, aber den Umkehrschluß zu ziehen, daß bei der Datenüberprüfung nach Absatz 3 ein maschineller Abgleich ausgeschlossen wäre, ist lediglich eine theoretische Möglichkeit der Interpretation, jedoch keine zwingende Schlußfolgerung.

Eine materielle Belastung Betroffener aus einem automatisierten Abgleich mit dem Kfz-Halterbestand ist im Grunde nicht feststellbar: Die zusammengefaßte Überprüfung durch das Gegeneinanderlaufenlassen von Datenbeständen der Kfz-Zulassungsstelle und des Sozialamtes im Stapelverfahren kann so gestaltet werden, daß die Kfz-Zulassungsstelle keinerlei Kenntnis aus irgendwelchen Daten des Sozialamtes erhält.

Aus meiner Sicht kann aus § 117 BSHG kein generelles Verbot eines automationsunterstützten Datenabgleichs in den Fällen des § 117 Abs. 3 BSHG abgeleitet werden.

3.3.2 Angabe des Verwendungszwecks „Sozialleistungen" auf Überweisungsträgern und Schecks

In der Vergangenheit ist bei Sozialhilfe-Zahlungen immer wieder kritisiert worden, wenn auf Überweisungsaufträgen oder Schecks Hinweise wie ,,Sozialleistung" o.ä. angebracht wurden, denn das Geldinstitut erfährt auf diese Weise von der Tatsache oder gar von der Art der Sozialleistung. Als Argument für solche Angaben wurden die Zuordenbarkeit von Zahlungen bei Erhalt mehrerer Sozialleistungen sowie Erwägungen zum Pfändungsschutz angeführt. Nun hat das **Bundesverwaltungsgericht** im Urteil vom 23. Juni 1994 entschieden, daß die Angabe **„Sozialleistung"** auf dem Überweisungsträger zur Aufgabenerfüllung grundsätzlich nicht erforderlich und daher in der Regel **unzulässig ist.** (Urteil des Bundesverwaltungsgerichts vom 23. Juni 1994, Nr. SC 16.92).

Das Bundesverwaltungsgericht führt aus, der Anspruch auf Wahrung des Sozialgeheimnisses nach § 35 Abs. 1 Satz 1 SGB 1 bestehe auch in bezug auf die Angabe des Verwendungszwecks der im bargeldlosen Zahlungsverkehr erbrachten Sozialhilfeleistungen. Bei der Preisgabe der Eigenschaft von Bezügen als ,,Sozialleistung" sei schon wegen der damit verbundenen Offenbarung des wirtschaftlichen Status eines Leistungsempfängers ein Geheimhaltungsinteresse anzuerkennen. Die Angabe des Verwendungszwecks auf den Überweisungsträgern sei eine Offenbarung i.S. des § 35 Abs. 1 Satz 1 SGB 1.

Hier ist anzumerken, daß der Ersatz der Bezeichnung Offenbarung" durch ,,Übermittlung" durch das 2.SGB-Änderungsgesetz an der rechtlichen Bewertung nichts ändert, da es sich nach wie vor um eine Mitteilung an das mit der Durchführung des Überweisungsauftrags befaßte Geldinstitut handelt, was i.S. der Begriffsbestimmungen des Datenschutzrechts eine Übermittlung darstellt.

Die Voraussetzung einer zulässigen Offenbarung nach dem hier in Frage kommenden § 69 Abs. 1 Nr.1 SGB X sind nach den Ausführungen des BVerwG in der Regel nicht erfüllt. Unter dem Blickwinkel des Pfändungsschutzes nach §§ 54, 55 SGB 1 könne sich der Hilfeempfänger zwar für den Pfändungsschutz entscheiden und zu diesem Zweck der Mitteilung des Bezuges von ,,Sozialleistungen" auf dem Überweisungsträger zustimmen. Entscheide er sich aber gegen die Bezeichnung einer Leistung als Sozialleistung, so müsse er die Nachteile, die sich daraus bei der Anwendung der §§ 54, 55 SGB 1 (Pfändungsschutz) für ihn ergeben könnten, hinnehmen. Nur in seltenen Einzelfällen werde es erforderlich sein, die Zahlung als Sozialleistung zu bezeichnen, um zu vermeiden, daß Doppelzahlungen notwendig werden.

Aus meiner Sicht wäre anstelle der Bezeichnung als ,,Sozialleistung" die Angabe eines Aktenzeichens sinnvoll, um exakt festzulegen, um welche Sozialleistung es sich bei der Überweisung oder dem Scheck handelt. Das Aktenzeichen müßte neutral, d.h. für die Bank nicht aussagefähig, gestaltet sein. Die Überweisung könnte als ,,Zahlung" bezeichnet werden, um der Bank möglichst keinen inhaltlichen Hinweis zu geben.

Das Bayerische Sozialministerium hat in einem Schreiben Hinweise zur Umsetzung dieses Urteils bei den Sozialbehörden gegeben.

Bei Datenschutzkontrollen werde ich bei Sozialleistungen die Bezeichnung auf Überweisungsträgern und Schecks besonders prüfen.

3.4 Jugendamt

3.4.1 Datenerhebung des Amtspflegers über Unterhaltspflichtige gemäß § 68 Abs. 1 Satz 1 SGB VIII beim Arbeitgeber

Ein Jugendamt bat um Überprüfung, ob ein Amtspfleger/Unterhaltsbeistand **den Arbeitgeber** eines Unterhaltspflichtigen **um Auskunft** über dessen Lohn oder Gehalt **bitten dürfe,** wenn der Betroffene seiner Auskunftspflicht nach § 1605 BGB nicht nachkomme. Angesichts der zunehmenden Anzahl von Pflegschaften und Beistandschaften würde es für die Verwaltung immer problematischer, die Alternative eines langwierigen gerichtlichen Auskunftsklageverfahrens gegen den Unterhaltspflichtigen wahrzunehmen. Des weiteren werde die Verwaltung für die Dauer des Klageverfahrens ggf. durch die Zahlung von Unterhaltsvorschußleistungen oder Sozialhilfe belastet.

Zunächst ist auch weiterhin einer **Datenerhebung beim Betroffenen** (Unterhaltspflichtigen) **Vorrang einzuräumen**, da diese Form der Datenerhebung den **geringstmöglichen Eingriff** in das informationelle Selbstbestimmungsrecht darstellt. Dem Betroffenen wird damit die Möglichkeit gegeben, gemäß § 1605 BGB selbst Auskunft über seine Einkünfte und sein Vermögen zu erteilen, soweit dies zur Feststellung eines Unterhaltsanspruchs durch den Amtspfleger/Unterhaltsbeistand erforderlich ist. Auch kann der Betroffene selbst über die Höhe der Einkünfte Belege bzw. Bescheinigungen des Arbeitgebers einholen und vorlegen.

Daneben kann der Unterhaltspflichtige bei der Aufforderung zur Auskunftserteilung (§1605 BGB) darauf hingewiesen werden, daß er seiner Auskunftspflicht **auch durch Einwilligung** in die Datenerhebung beim Arbeitgeber und dessen Auskunftserteilung **nachkommen** kann. Die Verpflichtung, Daten vorrangig beim Betroffenen zu erheben, wird durch den Hinweis auf die genannte Mitwirkungsalternative nicht in Frage gestellt.

Kommt der Betroffene der Auskunftsverpflichtung jedoch weder durch eigene Auskunftserteilung noch durch Erteilung der o.g. Einwilligung nach, stellt sich die Frage, ob eine Datenerhebung **unmittelbar beim Ar**beitgeber auch **ohne Einwilligung des Betroffenen** datenschutzrechtlich zulässig ist oder ob stattdessen der Zivilrechtsweg beschritten werden muß.

§ 68 Abs. 1 Satz 1 SGB VIII trifft keine Bestimmungen über die Verfahrensmodalitäten bei der Datenerhebung durch den Amtspfleger/Unterhaltsbeistand. Der Wortlaut der Norm schließt somit eine Datenerhebung unmittelbar beim Arbeitgeber ohne Einwilligung des Betroffenen nicht aus. Unter Zugrundelegung der Ausführungen des Bundesverfassungsgerichts zur Verfassungsmäßigkeit von Gesetzen, die das informationelle Selbstbestimmungsrecht des Betroffenen einschränken (BVerfGE 65,1), zeigt sich jedoch, daß § 68 SGB VIII und der darin enthaltene Freiraum bezüglich der Datenerhebung und -verarbeitung einer verfassungskonformen Auslegung und Begrenzung bedürfen, um unverhältnismäßige Eingriffe in das informationelle Selbstbestimmungsrecht der Betroffenen zu vermeiden. Dieser verfassungskonformen Auslegung des § 68 SGB VIII bedarf es insbesondere, weil gemäß § 61 Abs. 2 SGB VIII für den Sozial-datenschutz im Rahmen der Tätigkeit des Jugendamts als Amtspfleger/Beistand nur § 68 SGB VIII gelten soll.

Auch wenn § 62 Abs. 3 und 4 SGB VIII somit nicht unmittelbar anwendbar sind, wird sowohl durch diese Norm als auch durch andere bereichsspezifische Vorschriften (wie die § 97 a Abs. 4 SGB VIII, 67 a und 74 SGB X bzw. § 13 BDSG und Art. 16 BayDSG als allgemeine datenschutzrechtliche Vorschriften) ersichtlich, daß der Gesetzgeber grundsätzlich davon ausgegangen ist, bei fehlender Mitwirkung des Betroffenen und beim Vorliegen jeweils weiterer Voraussetzungen dürfe zu Gunsten der Erfüllbarkeit von Aufgaben der öffentlichen Verwaltung im überwiegenden Allgemeininteresse das Grundrecht auf informationelle Selbstbestimmung durch eine Datenerhebung bei Dritten insoweit eingeschränkt werden. Es ist nicht ersichtlich, weshalb Sozialdaten nach § 68 SGB VIII einen höheren Datenschutz genießen sollten als ihn die §§ 67 a Abs. 2 Nr.2 b bb, 66 SGB X sowie § 62 Abs. 3 Nr.3 SGB VIII gewährleisten. Diese Vorschriften stellen eine Ausprägung des verfassungsrechtlichen Grundsatzes des Verhältnismäßigkeit dar, der auch für die verfassungskonforme Auslegung des § 68 SGB VIII geeignet ist.

Eine Datenerhebung im Bereich des § 68 SGB VIII bei Dritten wird somit für zulässig erachtet, wenn die Erhebung beim Betroffenen einen unverhältnismäßigen Aufwand erfordern würde und **keine Anhaltspunkte dafür bestehen, daß schutzwürdige Belange des Betroffenen beeinträchtigt werden.**

Einen **unverhältnismäßigen Aufwand** im o.g. Sinne erfordern weitere Versuche der **Datenerhebung unmittelbar beim Betroffenen** nach meiner Auffassung dann, wenn der Betroffene über die **Auskunftspflicht** nach § 1605 BGB gegenüber dem unterhaltsberechtigten Kind bzw. dem Amtspfleger/Unterhaltsbeistand **unterrichtet** worden ist, unter **Hinweis** auf die vom Amtspfleger/Unterhaltsbeistand bei fehlender oder bei nicht ausreichender Auskunft vorgesehene **Datenerhebung unmittelbar beim Arbeitgeber** zur Auskunft bis zu einem bestimmten Termin **gemahnt** wurde und dieser Auskunftspflicht **nicht oder nicht ausreichend nachgekommen** ist

Diese Voraussetzungen wurden den Kriterien der §§ 97 a Abs. 4 Satz 2 und 3 SGB VIII und § 76 SGB X nachgebildet. Angesichts der Androhung geplanter Datenerhebung beim Arbeitgeber und der erfolgten Fristsetzung hat der Auskunftspflichtige die Möglichkeit, entweder seiner Auskunftspflicht nachzukommen oder dem Jugendamt

Gesichtspunkte zu unterbreiten, warum eine Datenerhebung beim Arbeitgeber seine **schutzwürdigen Belange beeinträchtigen** würde. Bleibt der Auskunftspflichtige dagegen trotz obiger Informationen gegenüber dem Jugendamt untätig, kann die Datenerhebung unmittelbar beim Arbeitgeber in der Regel als verhältnismäßig und damit auch erforderlich angesehen werden. Dann ist auch nicht mehr anzunehmen, daß **schutzwürdige** Belange des Auskunftspflichtigen durch die Datenerhebung beeinträchtigt würden. Ausnahmen hiervon wären denkbar, wenn eine Beeinträchtigung solcher Belange auch ohne ausdrücklichen Vortrag durch den Auskunftspflichtigen auf Grund eines amtsbekannten besonderen Sachverhalts angenommen und deshalb auch berücksichtigt werden muß.
§ 1605 BGB gibt einen **Anspruch auf Auskunft** ausschließlich gegen den Unterhaltsschuldner und nicht auch **gegen dessen Arbeitgeber.** Diese Tatsache ist insbesondere zu beachten, wenn die Datenerhebung beim Arbeitgeber ohne Einwilligung des Betroffenen erfolgt. Der Amtspfleger/Unterhaltsbeistand hat deshalb den **befragten Arbeitgeber ausdrücklich darauf hinzuweisen, daß**

- dessen Antwort **freiwillig** erfolgt (vergl. Art. 16 Abs. 4 BayDSG, § 13 Abs. 4 BDSG und § 67 a Abs. 4 SGB X) und daß

- er als Arbeitgeber in **eigener Verantwortung** nach den jeweils für ihn geltenden datenschutzrechtlichen Bestimmungen **zu prüfen hat,** ob die freiwillige **Auskunftserteilung rechtlich zulässig** ist.

Bei Zweifeln am Vorliegen einer der beschriebenen Zulässigkeitsvoraussetzungen ist die Datenerhebung unmittelbar beim Arbeitgeber unzulässig, so daß ggf. auf eine gerichtliche Durchsetzung der Auskunftsverpflichtung des Betroffenen zurückgegriffen werden muß.

3.4.2 Informantenschutz - Beschlagnahme von Unterlagen bei Sozialleistungsträgern

Sozialleistungsträgern und Jugendämtern stellt sich immer wieder die Frage, ob es sich bei Name und Anschrift sowie beim Inhalt evtl. vorliegender Schriftstücke eines **Behördeninformanten** um **Sozialdaten** im Sinne des SGB *X* handelt und inwieweit Bürger **Informantenschutz** genießen, die sich an einen Sozialleistungsträger oder ein Jugendamt wenden und ihm z.B. Erkenntnisse über eine Kindesmißhandlung, über Sozialleistungsmißbrauch o.ä. mitteilen. Die Frage stellt sich vor allem, wenn in seltenen Fällen solche Schriftstücke bei diesen Stellen im Zuge eines Ermittlungsverfahrens der Staatsanwaltschaft durch Gerichtsbeschluß beschlagnahmt werden.

Da es sich bei den personenbezogenen Daten eines Behördeninformanten um ,,Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person handelt, die von einer in § 35 SGB 1 genannten Stelle im Hinblick auf ihre Aufgaben nach dem Sozialgesetzbuch erhoben, verarbeitet oder genutzt werden", sind diese Daten gemäß § 67 Abs. 1 Satz 1 SGB *X* Sozialdaten. Dies gilt für **Name und Anschrift des Informanten** und für den **Informationsinhalt.** Diese Daten unterliegen daher dem besonders geschützten Sozialgeheimnis nach § 35 SGB 1, dessen Vorschriften als spezialgesetzliche Regelungen den §§ 94, 98 und 161 StPO vorgehen (§ 35 Abs. 3,2 SGB 1).

Eine wesentliche Problematik des Informantenschutzes ist, ob der Sozialleistungsträger bzw. das Jugendamt die Daten des Informanten von sich aus oder auf Ersuchen der Staatsanwaltschaft zwecks Verwendung in einem staatsanwaltschaftlichen Ermittlungsverfahren an die Strafverfolgungsbehörden übermitteln darf. Das Ermittlungsverfahren wird sich je nach Fallgestaltung gegen den Informanten selbst richten, z.B. bei einer Falschinformation, oder gegen den vom Informationsinhalt Betroffenen, wobei die Informantendaten evtl. als Zeugendaten angefordert werden.

Zu prüfen waren die rechtlichen Möglichkeiten einer Datenübermittlung einerseits nach den Vorschriften zur Übermittlung im Interesse der Übermittlungsempfänger (§§ 68 u. 73 SGB X) und andererseits nach der Vorschrift zur Übermittlung zur Aufgabenerfüllung der Sozialbehörde (§ 69 SGB X).

Eine Übermittlungsbefugnis nach den **§§ 68 bzw. 73 Abs. 2 SGB X** ist in bezug auf den Inhalt der Information nicht gegeben, da der abschließende Katalog übermittlungsfähiger Daten in diesen Vorschriften eine Übermittlung des **Inhalts** der Mitteilung des Informanten ausschließt. Auch der Vor- und Familienname bzw. die Anschrift des Behördeninformanten dürfen danach selbst im Falle eines Ersuchens der Staatsanwaltschaft nicht übermittelt werden, da sonst gleichzeitig unzulässigerweise das Merkmal ,,Behördeninformant in der bezeichneten Angelegenheit" übermittelt würde.

Auch wenn kein Verbrechen vorliegt ist jedoch eine Übermittlung von Sozialdaten des Behördeninformanten **ohne Beschränkung auf Katalogdaten** seit der Neufassung des § 73 **Abs. 1 SGB X** zulässig, soweit sie zur Durchführung eines Strafverfahrens **wegen einer sonstigen Straftat von erheblicher Bedeutung** erforderlich ist. Dies muß jeweils im **Einzelfall** entschieden werden. In der Regel muß **bei Vergehen** die Beschränkung des Datenflusses auf die Katalogdaten des § 72 Abs. 1 Satz 2 SGB *X* eingehalten werden, die Übermittlung des Datums ,,Behördeninformant" müßte hier ausscheiden. Erst bei Vergehen in der Größenordnung z.B. von Straftaten gegen die sexuelle Selbstbestimmung und anderen solchen mit der Folge eines hohen materiellen oder immateriellen Schadens darf eine ,,sonstige Straftat von erheblicher Bedeutung" gesehen werden (vgl. Bericht des Ausschusses für Arbeit und Sozialordnung, BT Drs. 12/6334 vom 02.12.1993). Bei dieser Bewertung ebenfalls zu berücksichtigen sind die Auswirkungen des Eingriffs in das allgemeine Persönlichkeitsrecht des Opfers (z.B. des sexuell mißhandelten Kindes oder eines zu Unrecht

Beschuldigten bei einer Falschanzeige durch den Behördeninformanten).

Sollen die Sozialdaten eines Behördeninformanten **durch ein Jugendamt** an die Staatsanwaltschaft übermittelt werden, ist ggf. der besondere Vertrauensschutz nach den Vorschriften des 4. Kapitels im SGB VIII zu berücksichtigen.

In manchen Fällen wird eine Übermittlung der Sozialdaten eines Behördeninformanten an die Staatsanwaltschaft durch die Sozialbehörde auf der Rechtsgrundlage des **§ 69 SGB X** und damit **einschließlich des Inhalts der Behördeninformation** zulässig sein. Die maßgeblichen Kriterien sind die Erforderlichkeit der Übermittlung für die **Erfüllung einer gesetzlichen Aufgabe der übermittelnden Stelle nach dem Sozialgesetzbuch** bzw. für die Durchführung eines damit **zusammenhängenden** gerichtlichen Verfahrens **einschließlich eines Strafverfahrens.** In diesem Zusammenhang verstehe ich unter ,,Strafverfahren" nicht erst das gerichtliche Strafverfahren, sondern bereits das Ermittlungsverfahren durch die Staatsanwaltschaft.

Im Einzelfall kann zulässig sein, daß es der Sozialleistungsträger/das Jugendamt **als Erfüllung seiner gesetzlichen Aufgaben** nach dem SGB betrachtet, von sich aus eine Strafanzeige **gegen den Behördeninformanten zu** erstatten oder eine bereits durch einen Dritten (z.B. den Betroffenen) erstattete derartige Strafanzeige durch Datenübermittlung zu unterstützen. Dies gilt etwa, wenn dem Sozialleistungsträger/Jugendamt erkennbar ist, daß der Informant die Behörde wider besseres Wissen oder besonders leichtfertig falsch informiert hat. Hier gilt es nämlich, sowohl die Behörde als auch die Betroffenen vor den Auswirkungen derartiger Anzeigen zu schützen. Das Problem der Erkennbarkeit solcher leichtfertiger oder vorsätzlich falscher Behördeninformationen ver-kenne ich dabei nicht.

Sofern sich die **Information** gegenüber einem Sozialleistungsträger/Jugendamt als **falsch** herausstellt, **muß diese Behörde** entscheiden, ob sie eine **Strafanzeige** gegen **den Informanten** durch eine Sozialdatenübermittlung **unterstützt,** weil sie darin nach § 69 SGB X **die Erfüllung einer gesetzlichen Aufgabe nach dem SGB** sieht. Ein diesbezügliches Übermittlungsersuchen der Staatsanwaltschaft kann die Sozialbehörde nicht zur Datenübermittlung verpflichten. Nicht die Staatsanwaltschaft, sondern das Sozial- bzw. Jugendamt hat auf Grund seiner Ermittlungen genügend Informationen, um den Sachverhalt umfassend beurteilen und eine Entscheidung über das VorliegenlNichtvorliegen einer diesbezüglichen gesetzlichen Aufgabe nach dem SGB treffen zu können. Besonders deutlich wird dies, wenn vom **Ju**gendamt über die Sozialdatenschutzregelungen des SGB X hinaus bereichsspezifische Regelungen zum besonderen Vertrauensschutz im 4. Kapitel des SGB VIII zu beachten sind. Ferner muß jede **Sozialbehörde ihrer** Verantwortung auf Grund der gesetzlichen Übermittlungsgrundsätze nach § 67 d Abs. 2 SGB X gerecht werden. Die Verantwortung der Staatsanwaltschaft **für die Richtigkeit ihrer Angaben** in dem Ersuchen läßt die **Verantwortlichkeit der Sozialbehörde für die Zulässigkeit der Übermittlung** nicht entfallen.

Das Bayer. Staatsministerium der Justiz beurteilt die Rechtslage hinsichtlich § 69 Abs. 1 Nr.2 SGB X anders. Sofern die Voraussetzungen dieser Vorschrift gegeben sind (Erforderlichkeit der Übermittlung für die Durchführung eines staatsanwaltschaftlichen/gerichtlichen Verfahrens im Zusammenhang mit der Aufgabenerfüllung durch einen Sozialleistungsträger), bewirke das Auskunftsrecht der Staatsanwaltschaft gemäß § 161 StPO, daß sich die Übermittlungsmöglichkeit nach § 69 Abs. 1 Nr.2 SGB X zu einer Übermittlungspflicht ver-dichte. Dieser Auffassung kann ich mich aus den genannten Gründen nicht anschließen. Diese **Verdichtung sagt nämlich nichts dauiiber, ob die gesetzlichen Voraussetzungen der Übermittlung gegeben sind. Die Verantwortung hierfür trägt die Sozialbehörde. Ein Auskunftsverlangen seitens der Staatsanwaltschaft entbindet die Sozialbehörde nicht von der Pflicht, eigenverantwortlich die Tatbestandsvoraussetzungen der Übermittlungsbefugnis zu prüfen und nach dem Ergebnis dieser Überprüfung zu handeln.**

Unstreitig besitzt dagegen **der Richter** die Kompetenz, Sozialdatenübermittlungen nach **§ 73** Abs. 1 und 2 SGB X anzuordnen (§ 73 Abs. 3 SGB X). Allerdings kann der Sozialleistungsträger/das Jugendamt die Einlegung einer Beschwerde nach § 304 StPO und eine Antragstellung auf Aussetzung der Vollziehung gemäß § 307 Abs. 2 StPO in Erwägung ziehen, wenn auf Grund seiner eigenen Schlüssigkeitsprüfung Zweifel an der Rechtmäßigkeit der Datenübermittlung und damit des gerichtlichen Beschlusses bestehen.

Auf demselben Wege kann gegen eine Beschlagnahme von Informantenschreiben (§§ 94, 98 StPO) vorgegangen werden. Dies gilt auch, sofern die Beschlagnahme nicht auf einer Übermittlungsanordnung des Richters nach § 73 Abs. 3 SGB X beruht, sondern auf einer von der Staatsanwaltschaft angenommenen sonstigen Sozialdatenübermittlungsbefugnis nach dem SGB X, deren Voraussetzungen vom Sozialleistungsträger bzw. dem Jugendamt jedoch für nicht gegeben erachtet werden.

3.5 Versorgungsämter

3.5.1 Ausgabe von Schwerbehindertenausweisen durch Wohnsitzgemeinde - Unterschriftenliste

In einer kreisangehörigen Gemeinde war es üblich, daß Schwerbehinderte, 4ie ihren Ausweis in der Gemeindeverwaltung abholten, den Empfang auf einer Liste bestätigen mußten. Auf dieser Liste konnten sie lesen, wer vor ihnen einen Ausweis erhalten hatte, wer also ebenfalls als Schwerbehinderter anerkannt worden war.

Diese Unterschriftenlisten wurde ohne Rechtsgrundlage geführt. Wer den Schwerbehindertenausweis abholt, hat dies auf einem Quittungsformular zu bestätigen. Das Formular geht an das zuständige Amt für Versorgung und Familienförderung zurück. Bei der Gemeinde ist eine Unterschriftenliste über die ausgehändigten Ausweise nicht zu führen.

Unzulässig war selbstverständlich auch die Verfahrensweise, durch die andere Schwerbehinderte erfuhren, wer vorher bereits seinen Ausweis abgeholt hatte.

Auf meinen Hinweis hat die Gemeinde diese Verfahrensweise eingesteut.

3.5.2 Einwilligungsformulare der Ämter für Versorgung und Familienförderung

Die Ämter für Versorgung und Familienförderung lassen die Antragsteller zusammen mit den Anträgen auf Anerkennung als Schwerbehinderter stets auch Einwilligungen für Datenübermittlungen durch Arzte unterschreiben, mit denen die Ärzte auch von der Schweigepflicht entbunden werden. Im Antragsformular für die Anerkennung als Schwerbehinderter wird dem **Antragsteller freigestellt, bestimmte Gesundheitsstörungen** von seinem Antrag und damit von dem Verfahren über die Anerkennung der Schwerbehinderung **auszunehmen.**

Das Formular, mit dem anschließend von Ärzten die benötigten Unterlagen über den Antragsteller eingeholt wurden, **enthielt eine solche Unterscheidung jedoch nicht.** Auf meine Anregung hin wird das Landesamt für Versorgung und Familienförderung seine Formblätter „Arztanfrage" **nunmehr so ändern,** daß in diesen Fällen der angeschriebene Arzt darauf hingewiesen wird, daß zu einer bestimmten Gesundheitsstörung keine Befunde zu übersenden sind, weil der Antragsteller sie nicht als Behinderung anerkannt haben will.

4. Bayerische Versicherungskammer - Gesetz über das öffentliche Versorgungswesen

In einem Gesetzentwurf der Staatsregierung über das öffentliche Versorgungswesen war vorgesehen, „die öffentlichen Stellen" zu berechtigen und zu verpflichten, an die von der Versicherungskammer verwalteten Versorgungsanstalten personenbezogene Daten von Berufsangehörigen und Hochschulabsolventen zu übermitteln, soweit sie erforderlich sind, um das Bestehen einer Pflichtversicherung oder Pflichtmitgliedschaft nach diesem Gesetz festzustellen oder zu überprüfen (Drucksache 12/14624 - Seite 8).

Ich teilte daraufhin dem Vorsitzenden des Rechts- und Verfassungsausschusses des Bayerischen Landtags, dem Bayerischen Staatsministerium des Innern und der Bayerischen Versicherungskammer mit, daß ich es als problematisch ansehe, daß **alle** öffentlichen Stellen berechtigt und verpflichtet werden sollen, personenbezogene Daten zu liefern, ohne daß auf etwaige schutzwürdige Interessen Betroffener am Ausschluß einer solchen Übermittlung Rücksicht zu nehmen wäre.

Die Bayerische Versicherungskammer hat daraufhin in Abstimmung mit dem Innenministerium einen geänderten Text vorgeschlagen, der bereichsspezifisch festlegt, welche öffentliche Stelle welche Daten an die betreffende Versorgungsanstalt übermittelt. Diese Beschränkung auf bestimmte, für die Feststellung oder Überprüfung einer Pflichtmitgliedschaft oder Pflichtversicherung bei einer Versorgungsanstalt erforderliche Daten habe ich begrüßt und den Vorschlag dem Vorsitzenden des Rechts- und Verfassungsausschusses des Bayerischen Landtags zugeleitet.

Die konkretisierten Datenübermittlungsvorschriften finden sich nunmehr für die Bayerische Ingenieurversorgung-Bau in Art. 29, für die Bayerische Rechtsanwalts-versorgung in Art. 31 und für den Bayerischen Versorgungsverband in Art. 38 des Gesetzes über das öffentliche Versörgungswesen vom *25.* Juni 1994 (GVBl. Nr.16 Seite 466 ff.). Die entsprechende Datenübermittlung an die Bayerische Architektenversorgung wurde bereits zu einem früheren Zeitpunkt in Art. 37 des Bayerischen Architektengesetzes festgelegt (i.d.F. der Bekanntmachung vom 26.11.1990, GVBl. Seite 513 ff.).

5. Polizei

5.1 Schwerpunkte

Schwerpunkte meiner Tätigkeit im Polizeibereich waren

- **allgemeine Kontrollen** von Dateien und Karteien, insbesondere von Dateien zur Gefahrenabwehr und Strafverfolgung (sog. GAST-Dateien), der Datei „Polizeiliche Sachbearbeitung/Vorgangsverwaltung-Verbrechensbekämpfung (PSV)", der „Arbeitsdatei PIOS-Innere Sicherheit (APIS)", des „Kriminalaktennachweises (KAN)", der „Arbeitsdatei organisierte Kriminalität (ADOK)", des „Grenzaktennachweises (GAN)", der „Arbeitsdatei Rauschgiftszene München (RG-Szene M)" und der Kartei „Psychisch Kranke - psychisch Gestörte"
- Prüfung neuer bzw. überarbeiteter Errichtungsan**ordnungen** für polizeiliche Dateien (Grenzaktennachweis-GAN, Spudok-Datei „Grenzpolizeiliche Kfz.-Fahndung", Arbeitsdatei „Polizeilich relevante An- und Verkaufsgeschäfte-PAVER", Arbeitsdatei „Rauschgift-Szene München", Arbeitsdatei „Kfz.-Verschiebung", Arbeitsdatei PIOS-Innere Sicherheit-APIS)
- Prüfung von **Dateimeldungen** (Erkennungsdienstdatei, Verantwortlichendateien, Vermißtenkartei, Fahrraddatei, Lagedateien)
- Mitwirkung im **Arbeitskreis Sicherheit**
- Auswertung der **Protokolldatei** (Abfragen im Zentralen Verkehrsinformationssystem-ZEVIS, im Informationssystem der Bayerischen Polizei (IBP), in

INPOL-Bund Dateien, im Ausländerzentralregister-AZR und in der Einwohnerdatei)
- Bürgereingaben

5.2 Allgemeine Prüfungen

Allgemeine Querschnittsprüfungen habe ich bei folgenden Polizeibehörden vorgenommen:

- Bayerisches Landeskriminalamt
- Polizeipräsidium München
- Polizeipräsidium Mittelfranken mit der Polizei-/Kriminaldirektion Nürnberg
- Polizeipräsidium Unterfranken mit den Polizeidirektionen Würzburg und Aschaffenburg.

Aufgrund des Kontrollergebnisses kann ich feststellen, daß die bayerischen Polizei dem Datenschutz einen **hohen Stellenwert** einräumt und datenschutzrechtliche Verstöße die Ausnahme bilden. Besonders hervorheben möchte ich, daß die Polizei nach meinen Erkenntnissen den Datenschutz als Bürgerrecht begreift und ihn nicht als Behinderung einer effektiven Polizeiarbeit ansieht. Das gleiche gilt für die große Bereitschaft der Polizei, mich bei der Prüfung aktiv zu unterstützen.

5.2.1 Kriminalaktennachweis (KAN)

Die Auflösung des Regional-KAN (vgl. *15.* Tätigkeitsbericht, Nr.4.1.4) ist noch nicht abgeschlossen. Bei der von mir geprüften Polizeidirektion Nürnberg war mit der Auflösung aus technischen Gründen noch nicht begonnen ,worden, während bei einer Polizeidirektion in Unterfranken die Auflösung zum Prüfungszeitpunkt unmittelbarbevorstand. Die noch vorhandenen Regional-KAN-Akten wurden ausgesondert und die entsprechenden Nachweise in der Datei gelöscht, soweit ihre Übernahme nicht für den Landes-KAN vorgesehen ist. So werden grundsätzlich alle Straftaten, die bisher im Regional-KAN gespeichert waren, automatisiert in den Landes-KAN übernommen ,und sind damit landesweit abrufbar. Im übrigen richtet sich die Speicherung im KAN nach den Richtlinien über personenbezogene polizeiliche Sammlungen und der Errichtungsanordnung für die Datei KAN, die allerdings noch der Überarbeitung bedarf. Die Kriminalakten derjenigen Regional-KAN-Bestände, für die eine Speicherung im Landes-KAN nicht vorgesehen ist, wurden einzeln von polizeilichen Sachbearbeitern geprüft und ggf. in der polizeilichen Vorgangsverwaltung erfaßt. Wurde bei dieser Einzelfallprüfung festgestellt, daß eine weitere Aufbewahrung bzw. Speicherung nicht mehr notwendig war, erfolgte die Löschung.

Festgestellte Mängel

Die KAN-Dateien der von mir geprüften Polizeidienststellen vermittelten einen **gut geführten Eindruck.** Nur in einigen Fällen konnte ich die **weitere Erforderlichkeit der Speicherung personenbezogener Daten anhand** der eingesehenen Akten nicht nachvollziehen.
Lücken aus datenschutzrechtlicher Sicht bestanden auch bei der Fristenvergabe für die **Speicherung von Kindern.** Hier konnte ich in einigen Fällen feststellen, daß die im PAG vorgeschriebene Speicherungsdauer von 2 Jahren teilweise um mehr als 2 Jahre überschritten wurde, ohne daß eine entsprechende **Begründung** in der Kriminalakte - wie in Art. 38 Abs. 3 Satz 1 PAG i. V. m. Ziffer 7.3 Dienstanweisung zum KAN vorgesehen - dokumentiert war. Ich habe die betroffene Polizeidienststelle gebeten, die Einzelfälle zu prüfen, ggf. zu ergänzen bzw. zu löschen und die übrigen Speicherungen von Kindern auf diesen Mangel hin zu überprüfen.

Bei der Überprüfung der sog. **personengebundenen Hinweise (PHW)** stellte ich bei der Vergabe des **PHW „geisteskrank"** fest, daß die eingesehenen Akten teilweise nur vage, auf allgemeine Feststellungen basierende, Mutmaßungen über den Gesundheitszustand der gespeicherten Person enthielten. In der Gesamtschau der überprüften Akten fanden sich zwar Hinweise auf psychische Erkrankungen der betroffenen Personen, jedoch fehlte die gem. Ziffer 4.3 der Dienstanweisung zum KAN vorgeschriebene ärztliche Feststellung in den Unterlagen. Ich habe das Innenministerium um eine Überprüfung der Voraussetzungen der Vergabe des PHW ,,geisteskrank" gebeten. Ein Ergebnis liegt mir noch nicht vor.

5.2.2 Einsatz besonderer Mittel der Datenerhebung zur Gefahrenabwehr

Die Polizei kann insbesondere zur Bekämpfung der organisierten Kriminalität besondere Mittel der Datenerhebung nach Art. 33 PAG einsetzen. Besondere Mittel der Datenerhebung sind

1. die planmäßig angelegte Beobachtung einer Person, die durchgehend länger als 24 Stunden oder an mehr als zwei Tagen durchgeführt werden soll (längerfristige Observation),

2. der verdeckte Einsatz technischer Mittel zur Anfertigung von Bildaufnahmen oder -aufzeichnungen sowie zum Abhören oder zur Aufzeichnung des nichtöffentlich gesprochenen Wortes,

3. der Einsatz von Polizeibeamten unter einer Legende (Verdeckte Ermittler).

Die Kontrolle dieses Bereiches war ein Schwerpunkt meiner diesjährigen datenschutzrechtlichen Prüfungen bei der Polizei. Dabei sollte festgestellt werden, ob das neue Bayer. Datenschutzgesetz **(BayDSG)** in diesem Bereich eine ausreichende datenschutzrechtliche Prüfung zuläßt, da die Kontrolle der Datenerhebung, -verarbeitung und -nutzung ausschließlich in Akten verarbeiteter oder genutzter personenbezogener Daten nur bei Vorliegen hinreichender Anhaltspunkte für Rechtsverletzungen zulässig ist **(Anlaßkontrolle).**

Zur Prüfung der Datenerhebung sowie zur Frage, inwieweit verdeckt durchgeführte Maßnahmen zu einer Datenverarbeitung oder -nutzung in einer **Datei** geführt haben, habe ich folgende Prüfansätze gewählt:

- Auswertung einer Aufstellung der Einsätze besonderer Mittel der Datenerhebung zu präventiven Zwecken, die seit 1990 bei einer bestimmten Polizei-dienststelle durchgeführt wurden und zu Speicherungen in Dateien geführt haben;
- Auswertung bestimmter deliktsbezogener Dateien (z.B. Arbeitsdatei organisierte Kriminalität-ADOK sowie verschiedene GAST-Dateien) auf mögliche Speicherungen, die auf dem Einsatz besonderer Mittel der Datenerhebung beruhen.

Die Auswertung der in der Aufstellung enthaltenen Maßnahmen ergab, daß bei der geprüften Pojizeidienststelle nur ein Einsatz eines Verdeckten Ermittlers zu präventiven Zwecken (Art. 33 Abs. 1 Nr.3 PAG) im Prüfzeitraum durchgeführt worden war. Bei der gleichen Dienststelle waren ferner noch zweimal technische Mittel zum Abhören des nichtöffentlich gesprochenen Wortes (Art. 33 Abs. 1 Nr.2 PAG) eingesetzt worden. Das Ergebnis dieser Einsätze hatte **keinen Niederschlag** in ADOK gefunden. Auch der weitere Prüfungsansatz (Auswertung deliktsbezogener Dateien) brachte keine zusätzlichen Erkenntnisse. Damit ergab sich für mich zu diesen Datenerhebungsmaßnahmen kein Prüfungsansatz über eine Datei, so daß ich auf eine Prüfung der Datenerhebung und Speicherung in den Akten verzichten mußte.

Das Ergebnis der Prüfung zeigt, daß die Beschränkung der Datenschutzkontrolle auf die An1aßkontrolle in dem besonders sensiblen Bereich verdeckter polizeilicher Datenerhebung Räume entstehen läßt, die von einer unabhängigen Kontrolle weitgehend ausgenommen sind.

5.2.3 Dateien zur Gefahrenabwehr und Verfolgung von Straftaten und Ordnungswidrigkeiten - GAST-Dateien

Diese Dateien, die mittlerweile eine wichtige DV-Unterstützung der Polizei darstellen, habe ich in meinem 14. Tätigkeitsbericht (Ziffer 4.11) ausführlich erläutert.

Die Errichtungsanordnung für GAST-Dateien wurde vom Innenministerium überarbeitet und den praktischen Erfordernissen angepaßt. Folgende Änderungen bzw. Ergänzungen sind aus datenschutzrechtlicher Sicht von Bedeutung:

1. Nach der Zweckbestimmung dürfen GAST-Dateien zur Unterstützung der polizeilichen Aufgabenwahrnehmung **nur dann errichtet werden, wenn**

1.1 eine zentrale Anwendung im Informationssystem der Bayerischen Polizei (IBP) für den gleichen Aufgabenbereich (noch) **nicht zur Verfügung steht und**

1.2 der mit der GAST-Datei verfolgte Zweck nur der Aufgabenerledigung im **Zuständigkeitsbereich der errichtenden Dienststelle dient.**

2. Der von einer Speicherung betroffene Personenkreis wurde **erheblich erweitert.** Gespeichert werden können nun neben Beschuldigten, Tatverdächtigen und Betroffenen auch sog. Beauftragte nach Art. 9 PAG, Personen nach Art. 10 PAG (sog. nichtverantwortliche Personen) sowie Opfer, Verletzte, Strafantragsberechtigte, Anzeigeerstatter und Mitteiler. Diese Erweiterung kann hingenommen werden, so lange die Datei ,,Polizeiliche Sachbearbeitung/Vorgangsverwaltung-Verbrechensbekämpfung PSV" noch nicht bei allen bayerischen Polizeidienststellen realisiert ist.

3. Ferner wurde der Hinweis aufgenommen, daß die Errichtungsanordnung den **maximalen Rahmen von** Datenspeicherungen festlegt, so daß entsprechend dem Dateizweck der konkreten Anwendung (GAST-Datei) Beschränkungen geboten sein können (z.B. betroffener Personenkreis, Umfang, Löschungsfristen). Notwendige Beschränkungen sind in der Genehmigung der einzelnen GAST-Datei anzugeben; ggf. ist eine eigene Errichtungsanordnung zu erstellen.

4. Aufgenommen wurde auch ein Hinweis auf **Art 47** Abs. 2 **PAG** (Prüfung der Notwendigkeit der Weiterführung oder Änderung der Datei in angemessenen Abständen) sowie die Verpflichtung, einen **Abdruck der Genehmigung dem Landesbeauftragten für** den **Datenschutz zuzuleiten.** Ich werde dadurch in die Lage versetzt, meiner Kontrollaufgabe in diesem Bereich nachzukommen.

5. Die Polizeipräsidien haben zukünftig sogenannte Dateiverzeichnisse für die in ihrem Bereich vorhandenen Dateien zu führen.

Anhand der mir übersandten Genehmigungen der einzelnen GAST-Dateien wie auch im Rahmen datenschutzrechtlicher Kontrollen bei Polizeidienststellen habe ich die Erforderlichkeit der Dateien, die Rechtmäßigkeit der Datenerhebung und -verarbeitung überprüft.

Im einzelnen gilt dies insbesondere für folgende Dateien:

- Polizeilich relevante An- und Verkaufsgeschäfte - PAVER
- Extremistische Vereine - EXVER
- Skinheads - SKIND
- Erkennungsdienstliche Behandlung -EDBEHANDL
- Observationsmaßnahmen/Einsatz technischer Mittel
- Einsatz Dokumentation VE/noeP
- PAG-Maßnahmen
- Verantwortlichen-/Verständigungsdatei
- Gaststättendatei
- Datei zur Speicherung von PKW-Aufbrüchen
- Vermißtendatei
- Anhaltungsdatei
- Versammiungs- und Veranstaltungsdatei (VKALE)
- Versammlungsleiter- und Verantwortlichendatei (VERER)
- Lagedateien für unterschiedliche Deliktsbereiche (z.B. Glücksspiel)

Folgende **Mängel** bei den Festlegungen für die einzelnen GAST-Dateien habe ich festgestellt:

1. Unzureichend konkretisierte Festlegung der **Zweckbestimmung**
2. Unscharfe Definition des von der Speicherung betroffenen **Personenkreises**
3. Fehlerhafte oder fehlende Regelungen zur Aussonderung der gespeicherten personenbezogenen Daten.

Ich habe die Polizei aufgefordert, die entsprechenden Errichtungsanordnungen zu überarbeiten und den gesetzlichen Vorgaben anzupassen. Bei Nachprüfungen im Rahmen datenschutzrechtlicher Kontrollen konnte ich mich von den Korrekturen überzeugen.

5.3 Bayerisches Landeskriminalamt (BLKA)

Im Berichtsjahr habe ich die Arbeitsdatei PIOS Innere Sicherheit (APIS), die Arbeitsdatei ,,Organisierte Kriminalität" - ADOK und die Datei ,,Rauschgiftszene München" geprüft. Darüber hinaus habe ich versucht festzustellen, ob die Maßnahmen der verdeckten Datenerhebung, wie Observation, Einsatz verdeckter Ermittler und Einsatz technischer Mittel über Dateien erschließbar und überprüfbar sind.

5.3.1 APIS-Prüfung

Wegen der besonderen Abgrenzungsschwierigkeiten habe ich schwerpunktmäßig Speicherungen der neuen APIS-Kategorien ,,**Gefährder**" und **„Kontakt- und Begleitpersonen**" geprüft.

In Einzelfällen waren bei der Speicherung dieser Personengruppen die Vorgaben der Errichtungsanordnung nicht berücksichtigt. So stellte ich fest, daß die in der Errichtungsanordnung vorgeschriebene jährliche Relevanzprüfung (Erforderlichkeit der Speicherung) nicht immer durchgeführt wurde. Dies betraf Vorgänge, die bereits vor Einführung der neuen APIS-Kategorien ohne die Verpflichtung zur jährlichen Relevanzprüfung gespeichert waren.

Ich habe das BLKA aufgefordert, eine **generelle Überprüfung** des Datenbestandes zur Berichtigung der Speicherungsfristen vorzunehmen. Das BLKA hat erklärt, daß nunmehr die Durchführung einer jährlichen Relevanzprüfung bei allen Kontaktpersonen gewährleistet ist.

5.3.2 Besondere Mittel der Datenerhebung

Da ich eine umfassende Kontrollbefugnis nur für personenbezogene Daten besitze, die zumindest auch in Dateiep verarbeitet oder genutzt werden, habe ich aus dem Dateien- und Karteienverzeichnis des BLKA die Dateien ausgewählt, von denen aufgrund der Struktur und des Inhalts anzunehmen war, daß darin entweder die verdeckte Maßnahme selbst oder aufgrund der Maßnahme erhobene Daten ihren Niederschlag gefunden haben. Im einzelnen habe ich folgende sog. GAST-Dateien (vgl. auch Ziff. 5.2.3) herangezogen:

- ,,Observationsmaßnahmen/Einsatz technischer Mittel"
- ,,Einsatz Dokumentation Verdeckter Ermittler"
- ,,PAG-Maßnahmen".

Wie sich herausstellte, handelt es sich bei diesen Dateien nicht um Fachdateien, sondern um **Hilfsmittel zum Nachweis und zur Koordination des Einsatzes besonderer Mittel der Datenerhebung.** Eine fachbezogene Speicherung findet in diesen als Führungs- und Dokumentationshilfe konzipierten Dateien nicht statt. Das hätte mich freilich nicht davon abgehalten, die Speicherung auch in einer solchen Datei als Ansatz für meine Kontrollzuständigkeit anzusehen. Es handelte sich jedoch bei den in den Dateien ,,Observationsmaßnahmen/Einsatz technischer Mittel" und ,,Einsatz Dokumentation Verdeckter Ermittler" gespeicherten Fällen, soweit sie von mir eingesehen wurden, überwiegend um Strafverfolgungsmaßnahmen. Entsprechend dem Zweck der Dateien als aktuelle Aufstellung laufender verdeckter Erhebungsmaßnahmen, war keines der zugrundeliegenden Strafverfahren bereits abgeschlossen. Eine **Kontrolle der Erhebung personenbezogener Daten durch die Polizei als Strafverfolgungsbehörde war deshalb nach dem geänderten Bayer. Datenschutzgesetz (Art. 30 Abs. 4 Satz 1) zu diesem Zeitpunkt nicht zulässig.**
Wegen der Problematik dieser Regelung verweise ich auf den besonderen Beitrag zur Kontrollkompetenz des Landesbeauftragten für den Datenschutz gegenüber der Staatsanwaltschaft (vgl. Ziffer 7.3.1).

5.3.3 Datei Rauschgiftszene München

Die Datei dient der **Unterstützung der polizeilichen Bekämpfung der Rauschgiftkriminalität** (einschließlich der Beschaffungskriminalität) an den deliktsspezifischen Rauschgiftschwerpunkten in München. In ihr sollen Daten gesammelt und bereitgestellt werden, die es ermöglichen,

- deliktsrelevante **Personen zu erkennen,**
- Schwernunktmaßnahmen **zu planen und durchzuführen,**
- Straftaten und Ordnungswidrigkeiten zu verhindern bzw. **zu unterbinden,**
- Delikte der Rauschgiftkriminalität einschließlich der Beschaffungskriminalität effizienter **zu bearbeiten** und
- in sonstigen konkreten Ermittlungsfällen die kriminalpolizeiliche Ermittlungsarbeit **zu unterstützen.**

Nach der Errichtungsanordnung sollen Personen gespeichert werden, die sich an Rauschgiftschwerpunkten **aufhalten, polizeilichen Maßnahmen unterzogen werden** und kriminalpolizeiliche Erfahrungswerte dafür sprechen, daß diese Personen der Rauschgiftszene **zuzuordnen** sind. Beispielhaft werden aufgezählt:

- Tatverdächtige, Beschuldigte und Verurteilte,
- Betroffene und Beteiligte im Sinne des Ordnungswidrigkeitengesetzes,

- Betroffene polizeilicher Maßnahmen als Verantwortliche im Sinne von Art. 7 und 8 PAG sowie
- Drogeninteressenten.

Die Speicherungsdauer beträgt 2 **Jahre** und verlängert sich mit erneutem Kontrolldatum um weitere 2 Jahre.

Die Datenspeicherung erfolgt anhand sog. Erfassungsblätter, die von kontrollierenden Beamten vor Ort ausgefüllt werden. Ich habe mir persönlich das Vorgehen der Polizei bei Kontrollen sowie die Erfassung der personenbezogenen Daten von Kontrollierten auf dem Erfassungsblatt angesehen, um einen unmittelbaren Eindruck über den Ablauf der Kontrolle, die Datenerhebung, vor allem aber über die Rechtmäßigkeit der Speicherung personenbezogener Daten in der Datei gewinnen zu können. Insbesondere ging es mir darum festzustellen, nach welchen Kriterien im konkreten Einzelfall über die Aufnahme der Daten in die Datei entschieden wird. Dabei konnte ich feststellen, daß die **Polizei streng darauf achtet, daß nur die Personen in der Datei gespeichert werden, die tatsächliche Anhaltspunkte dafür bieten, daß sie der Rauschgiftszene zuzuordnen sind.**

In diesem Sinn wurde auf meine Anregung das Erfassungsblatt inhaltlich überarbeitet und entspricht nun datenschutzrechtlichen Anforderungen. Die von mir geforderte entsprechende Überarbeitung der Errichtungsanordnung hat das Innenministenüm bisher abgelehnt. Nach meiner Beurteilung ist in der Errichtungsanordnung der für eine Aufnahme in die Datei vorgesehene Personenkreis nicht hinreichend definiert und begrenzt. Dies gilt vor allem für die Speicherungsvoraussetzung ,,kriminalpolizeiliche Erfahrungswerte". Ich halte es für erforderlich, daß neben dem Aufenthalt an Rauschgift-schwerpunkten nicht subjektive Kriterien wie die vorgenannten ,,Erfahrungswerte", sondern das Vorliegen tatsächlicher Anhaltspunkte für die Zuordnung der betroffenen Personen zur Rauschgiftszene und damit für die Speicherung in der Datei maßgebend sind, wie das in dem Erfassungsblatt des BLKA in der jetzigen Fassung nunmehr vorgesehen ist.

5.4 Polizeipräsidium München

Beim Polizeipräsidium München habe ich in einer mehrtägigen Prüfung folgende Bereiche kontrolliert:

- die Datei PSV mit dazugehörigen Unterlagen
- die erkennungsdienstliche Behandlung von Tatverdächtigen
- die Anhaltungsdatei
- die Kartei ,,Psychisch Kranke oder Psychisch Gestörte"

  sowie
- Abfragen aus der Gewerbedatei der Landeshauptstadt München.

Im Ergebnis habe ich bei der Behörde, abgesehen von einzelnen nicht schwerwiegenden Mängeln, einen hohen Datenschutzstandard festgestellt.

5.4.1 Datei Polizeiliche Sachbearbeitung 1 Vorgangsverwaltung-Verbrechensbekämpfung (PSV)

1. Protokollierung

Die Datei PSV ist zwischenzeitlich bei einer Vielzahl von Polizeidienststellen eingeführt. Die von mir geforderte Protokollierung von Abfragen in der PSV ist bei den Polizeidienststellen des Polizeipräsidiums München bereits realisiert. Protokolliert werden unter der Kennung des Abfragenden Name, Geburtsname, Geburtsdatum, KAN-Nummer und/oder Kraftfahrzeugkennzeichen des Betroffenen für die Dauer von 12 Monaten.

2. Speicherungsdauer

Um festzustellen, ob die Löschung von Strafanzeigen gegen bekannte Täter, die sowohl in der PSV als auch im Kriminalaktennachweis (KAN) nachgewiesen sind, entsprechend der für den KAN festgelegten Aussonderungsfristen erfolgt, habe ich im KAN bereits gelöschte Datensätze auf Bestand in der PSV überprüft.

Ich konnte dazu insgesamt 4 Personendatensätze in der PSV feststellen. Schriftliche Unterlagen bestanden jedoch nur zu einer Speicherung. Zu den übrigen Dateispeicherungen hatte das Polizeipräsidium die Vorgangsakten nach einer Aufbewahrungszeit von 2 **Jahren** aus Platzgründen **vernichtet.**

Die unterbliebenen Löschungen in der PSV wurden vom Polizeipräsidium damit erklärt, daß der turnusmäßig halbjährige Löschlauf in der PSV aus technischen Gründen noch nicht vorgenommen werden konnte. Ich werde mich durch eine Nachkontrolle von der Durchführung der Löschung überzeugen.

Problematisch ist auch die Speicherung in der PSV ohne den erforderlichen Aktenrückhalt, da eine Kontrolle der Rechtmäßigkeit der Speicherung nicht mehr nachvollziehbar ist. Das Polizeipräsidium sagte mir zu, dieses Problem in absehbarer Zeit zu bereinigen, da an der Realisierung einer **„elektronischen Papierablage"** durch Einscannen der Unterlagen in die EDV gearbeitet werde. Zu jeder bestehenden Speicherung in der PSV werde dann die entsprechende Papierunterlage bei Bedarf äusgedruckt werden können. Ich werde die weitere Entwicklung aufmerksam verfolgen und auf eine baldige Lösung drängen.

3. Speicherung von Versammlungsvorgängen

Leider habe ich wie im vorhergehenden Berichtszeitraum feststellen müssen, daß entgegen den Vorgaben der Errichtungsanordnung zur Datei PSV Vorgänge im Zusammenhang mit der polizeilichen Betreuung von Veranstaltungen und Versammlungen gespeichert werden. Ich habe diese Frage daraufhin mit dem Innenministerium erörtert. Dabei wurde grundsätzlich meine Auffassung geteilt, daß die unterschiedslose Speicherung von Versammlungen in der PSV mit der Errichtungsanordnung **nicht übereinstimmt.**

Auch in seiner abschließenden schriftlichen Äußerung geht das Innenministerium davon aus, daß Daten, die im Zusammenhang mit einer Versammlung der Polizei bekannt werden, **grundsätzlich nicht** in der Datei PSV gespeichert werden. Dieser Grundsatz solle nur dann nicht gelten, wenn von vornherein Tatsachen bekannt sind oder konkrete Anhaltspunkte dafür vorliegen, daß bei der Veranstaltung gegen Straf- und Bußgeldvorschriften, insbesondere nach dem Versammiungsgesetz, verstoßen wird oder nachträglich entsprechende Feststellungen getroffen werden. In diesen Fällen liegt, wegen der Notwendigkeit polizeilichen Handelns, ein speicherungswürdiger Vorgang vor.. Seine Aufnahme in die Datei PSV ist deshalb datenschutzrechtlich nicht zu beanstanden.

5.4.2 Anhaltungsdatei

Bei der Polizeunspektion im Münchner Hauptbahnhof wurde die bisherige Anhaltekartei als automatisierte Datei weitergeführt. Die Datei wird auf einem Arbeitsplatzcomputer (APC) auf der Grundlage der Errichtungsanordnung für Dateien zur Gefahrenabwehr und Verfolgung von Straftaten und Ordnungswidrigkeiten (GAST-Verfahren) betrieben.

Die Datei dient der Verhütung und Unterbindung von Straftaten (z.B. Begleitdelinquenz männlicher Prostitution, Hausfriedensbruch) und Ordnungswidrigkeiten (Erregung öffentlichen Argernisses), aber auch deren **Verfolgung** und der in diesem Zusammenhang erforderlichen **Bekämpfung von Geschlechts- und anderen ansteckenden Krankheiten.** Sie dient - auch nach meinen Feststellungen - nicht der Erfassung gleichgeschlechtlichen Sexualverhaltens durch Speicherung homosexuell veranlagter männlicher Personen. Ich habe deshalb die Bezeichnung ,,Homosexuelle" als eine in der Errichtungsanordnung für die Speicherung vorgesehene Kategorie gerügt und eine Überprüfung verlangt. Das Innenministerium hat mitgeteilt, daß insofern eine Klarstellung erfolgt.

In dieser Datei dürfen nur Personen gespeichert werden, die im **Toilettenbereich des Münchner Hauptbahnhofs** angetroffen werden **und** bei denen nach Sachlage angenommen werden kann, daß sie

- die für die **Ausübung der männlichen Prostitution** erforderlichen Kontakte knüpfen oder aufrechterhalten wollen,
- aufgrund allgemeiner polizeilicher Erfahrungswerte im Verdacht stehen, **geschlechtskrank zu sein und Geschlechtskrankheiten weiter zu verbreiten.**

Zugriffsberechtigt sind nur die zuständigen Beamten der Polizeiinspektion im Hauptbahnhof. Eine regelmäßige Datenübermittlung findet nicht statt.

Die **Dauer** der Speicherung richtet sich bei Tatverdächtigen nach den in Art. 37 und 38 PAG festgelegten Fristen. Abweichend davon sind Datensätze über Personen, die in der Datei **nicht** als Tatverdächtige geführt werden, grundsätzlich **auszusondern**, wenn seit der letzten Erkenntnis, die zur Aufnahme in die Datei geführt hat, ein **Jahr** vergangen ist und neue relevante Erkenntnisse nicht aufzunehmen sind. Die Fristberechnung beginnt mit Ende des Jahres, in dem das letzte Ereignis erfaßt worden ist.

Ich habe alle Datensätze, die zum Prüfungszeitpunkt gespeichert waren, überprüft und auch zu einigen Speicherungen die vorhandenen Akten eingesehen. Gravierende Mängel, insbesondere im Hinblick auf die Voraussetzungen für die Erfassung, konnte ich nicht feststellen.

5.4.3 Personenkartei „Psychisch Kranke oder Psychisch Gestörte"

Die Kartei dient der Sammlung und Auswertung von Erkenntnissen über Personen, die psychisch krank oder psychisch gestört sind oder die nach ihrem Auftreten, Verhalten und Persönlichkeitsbild dafür gehalten werden müssen und bei denen der Verdacht besteht, daß sie durch krankheitsbedingte Handlungen die öffentliche Sicherheit und Ordnung stören können.

Zweck und Inhalt der Kartei sowie deren Problematik im einzelnen habe ich bereits in meinem *15.* Tätigkeitsbericht (Ziffer 4.5.6) eingehend dargestellt.

Um mir einen Überblick über den in der Kartei gespeicherten Personenkreis zu verschaffen, habe ich bei meiner erneuten Kontrolle der Datei eine Vielzahl von Speicherungen eingesehen. Nur in wenigen Fälle konnte ich aus den Unterlagen die **Erforderlichkeit** einer polizeilichen Speicherung nicht klar erkennen. Das Polizeipräsidium wird diese Einzelfälle nochmals überprüfen und die Kartei ggf. bereinigen.

Ich habe mit der Polizei darüber gesprochen, wann eine **Störung der öffentlichen Sicherheit und Ordnung im** Sinne der Errichtungsanordnung angenommen werden könne. Dabei habe ich ausdrücklich darauf hingewiesen, daß

- das ,,Beschäftigen" von Behörden (z. B. durch sog. Vielbriefschreiber) oder
- ein ,,psychisch gestörtes Erscheinungsbild"

für die Annahme einer solchen Störung nicht ausreicht.

5.4.4 Erkennungsdienstliche Behandlung von Tatverdächtigen

Bei meiner diesjährigen Prüfung des Polizeipräsidiums München habe ich besonderes Gewicht auf die Kontrolle der **erkennungsdienstlichen Behandlung von Tatverdächtigen** sowie die **Speicherung dieser Unterlagen** für Zwecke des Erkennungsdienstes gelegt.

Prüfungsmaßstab war § 81 b der Strafprozeßordnung (StPO). Dazu hat das Bundesverwaltungsgericht im Jahr 1983 folgende Grundsätze aufgestellt:

„Entsprechend dieser gesetzlichen Zweckbestimmung von erkennungsdienstlichen Maßnahmen nach § 81 b 2.

Alternative StPO bemißt sich die Notwendigkeit der Anfertigung und Aufbewahrung von erkennungsdienstlichen Unterlagen danach, ob der anläßlich des gegen den Betroffenen gerichteten Strafverfahrens festgestellte Sachverhalt nach kriminalistischer Erfahrung angesichts aller Umstände des Einzelfalles - insbesondere angesichts der **Art, Schwere und Begehensweise der dem** Betroffenen im strafrechtlichen Anlaßverfahren zur Last gelegten Straftaten, seiner **Persönlichkeit** sowie unter Berücksichtigung des Zeitraumes, währenddessen er strafrechtlich nicht (mehr) in Erscheinung getreten ist - Anhaltspunkte für die Annahme bietet, daß der Betroffene künftig oder anderwärts gegenwärtig mit guten Gründen als Verdächtiger in den Kreis potentieller Beteiligter an einer noch aufzuklärenden strafbaren Handlung einbezogen werden könnte **und** daß die ed-Unterlagen die dann zu führenden Ermittlungen - den Betroffenen schließlich überführend oder entlastend - fördern könnten."

Die Entscheidung über die erkennungsdienstliche Behandlung für die Zwecke des Erkennungsdienstes und die Dauer der Aufbewahrung erkennungsdienstlicher Unterlagen hängt von den Umständen des Einzelfalles und einer kriminalistischen Prognose der Wiederholungsgefahr ab. Deliktsarten, die von vornherein als Anknüpfungspunkt für eine erkennungsdienstliche Behandlung ausscheiden, gibt es danach nicht. Allerdings schränken der Verhältnismäßigkeitsgrundsatz und die Berücksichtigung des Persönlichkeitsrechts des Betroffenen die Zulässigkeit der erkennungsdienstlichen Behandlung z.B. bei Beleidigungen oder ,,Schwarzfahren" erheblich ein. Hier müssen gerade bei Ersttätern besondere Umstände hinzutreten. Deswegen habe ich gerade erkennungsdienstliche Behandlungen wegen dieser Delikte einer Kontrolle unterzogen. Ferner habe ich auch noch bei den Delikten ,,Falsche Versicherung an Eides Statt" und ,,Unterhaltspflichtverletzung" die ,,Eignung" der erkennungsdienstlichen Unterlagen für eine spätere Strafverfolgung geprüft.

In zwei Fällen konnte ich die **Erforderlichkeit** der erkennungsdienstlichen Behandlung nicht erkennen. In einem weiteren Fall stellte ich eine zu lange Speicherungsdauer fest. Das Polizeipräsidium berichtigte die Speicherungen bzw. sagte eine Überprüfung zu. Das Ergebnis der Überprüfung steht noch aus.

5.4.5 Polizeiliche Abfragen aus der Gewerbedatei der Landeshauptstadt München

Bereits im Mai 1991 beantragte das Polizeipräsidium bei der Landeshauptstadt München eine direkte **Zugriffsbe**rechtigung (sog. Online-Zugriff) auf die automatisierte Gewerbedatei der Landeshauptstadt München. Die Genehmigung erfolgte am 24.11.1993. Solche automatisierte Zugriffsberechtigungen hatte die Polizei bisher nur auf die Dateien Einwohnermeldeamtsverfahren (EWO), Ausländerzentralregister (AZR) und Zentrales Verkehrsinformationssystem (ZEVIS).

Im Gegensatz zu diesen Bereichen ist die Zugriffsbefugnis der Polizei auf die Gewerbedatei nicht spezialgesetzlich für diese Datei geregelt. Ich habe es aber für zulässig gehalten, daß in diesem Fall, in dem weniger sensible personenbezogene Daten zum Abruf bereitstehen, auf die Datenübermittlungsvorschriften und die Regelungen zum automatisierten Abrufverfahren im Polizeiaufgabengesetz (Art. 42 in Verbindung mit Art. 46 PAG) zurückgegriffen wird.

Nach Art. 46 Abs. 1 Satz 1 PAG ist die Einrichtung eines automatisierten Verfahrens, das die Übermittlung personenbezogener Daten durch Abruf ermöglicht, zulässig, soweit dieses Verfahren unter Berücksichtigung der schutzwürdigen Interessen der Betroffenen und der Erfüllung polizeilicher Aufgaben angemessen ist.

Abfrageberechtigt sind im Rahmen ihrer Aufgabenerfüllung **alle** Polizeibeamten des Polizeipräsidiums sowie Angestellte, wenn ihnen solche Aufgaben übertragen wurden oder sie mit der Bedienung von Datenendgeräten beauftragt sind und der jeweilige Abruf auf Weisung eines Polizeivollzugsbeamten erfolgt. Der Polizei steht im automatisierten Abrufverfahren der volle **Datenumfang** (mit Ausnahme des Geburtsnamens der Mutter) entsprechend dem Gewerbeanmeldeverfahren (§14 Gewerbeordnung) zur Verfügung. Es handelt sich dabei um 3 Arten von Daten:

- Personendaten,
- Betriebsdaten und
- sog. ,,historische" Daten.

In 10 Fällen habe ich Abrufe auf ihre **Erforderlichkeit zur polizeilichen Aufgabenerfüllung** überprüft. In einem Fall war das Vorliegen der Erforderlichkeit klärungsbedürftig; hierzu habe ich das Polizeipräsidium um Stellungnahme gebeten. Eine Antwort steht noch aus. In einem weiteren Fall wurde mir mitgeteilt, daß die Ab-frage zu Übungszwecken von einem einzuweisenden Beamten durchgeführt worden sei. Ich bin der Meinung, daß grundsätzlich darauf verzichtet werden sollte, Echt-daten zu Übungszwecken abzufragen. Solche ,,Schulungen" sollten vielmehr mit einem Testdatenbestand durchgeführt werden. Darauf habe ich das Polizeipräsidium hingewiesen.

5.4.6 Überprüfung der Speicherung personenbezogener Daten von Demonstranten vor der Bayerischen Börse in München am 13.2.1991

In meinem 15. Tätigkeitsbericht (Ziffer 4.5.7) hatte ich mitgeteilt, daß eine Teilnehmerin an der Demonstration vor der Bayerischen Börse vom Bayerischen Obersten Landesgericht rechtskräftig vom Vorwurf der Nötigung freigesprochen worden war und ihre polizeilichen personenbezogenen Speicherungen auf meine Initiative hin von der Polizei gelöscht worden waren. Wegen der Speicherung der anderen Demonstrationsteilnehmerinnen hatte ich die Polizei um die Prüfung vergleichbarer Fälle gebeten. Daraufhin hatte die Polizei auch die personen-

bezogenen Daten der Demonstrationsteilnehmerinnen gelöscht, deren Strafverfahren nach § 170 Abs. 2 der Strafprozeßordnung eingestellt worden waren. Im Hinblick auf das Urteil des Bayerischen Obersten Landesgerichts, das in dem Verschließen der Eingangstüre der Börse keine Nötigung gesehen hatte, habe ich bei der Polizei darauf gedrungen, daß - unabhängig vom Ausgang der einzelnen Strafverfahren - auch bei den noch gespeicherten Personen die Erforderlichkeit der Speicherung geprüft wird. Die Polizei teilte mir als Ergebnis ihrer Prüfung nunmehr mit, daß auch die zu den verbliebenen Teilnehmerinnen im Zusammenhang mit der Aktion vor der Bayerischen Börse erstellten Unterlagen **vernichtet** und die Speicherungen **gelöscht** wurden.

5.4.7 Speicherungen im Zusammenhang mit den Vorkommnissen beim Münchner Weltwirtschaftsgipfel 1992

Die aus Anlaß des Weltwirtschaftsgipfels 1992 in München vom Polizeipräsidium München eingerichtete Datei „Münchner Wirtschaftsgipfel 1992 - MWG 92" (vergl. 14. Tätigkeitsbericht Ziff. 4.7.1) zur Bewältigung der polizeilichen Aufgaben im Zusammenhang mit diesem Großereignis wurde zum 1. März 1993 wieder gelöscht. Speicherungen personenbezogener Daten wurden aber als zur polizeilichen Aufgabenerfüllung erforderlich in andere polizeiliche Dateien übernommen.

Bei der letztjährigen datenschutzrechtlichen Prüfung beim Polizeipräsidium München hatte ich festgestellt, daß Personen, die im Zusammenhang mit den Vorgängen am 6. Juli 1992 auf dem Münchner Max-Joseph-Platz wegen Verdachts der versuchten Nötigung, der Verunglimpfung des Staates und seiner Symbole und des Widerstands gegen Vollstreckungsbeamte angezeigt wurden, im KAN gespeichert waren. Datenschutzrechtliche Bedenken gegen die Speicherungen hatte ich nicht geltend gemacht (vgl. *15.* Tätigkeitsbericht Ziff. 4.5.1).

Das Polizeipräsidium München hat mir nunmehr auf Anfrage mitgeteilt, daß von den 479 Ermittlungsverfahren im Zusammenhang mit den Vorkommnissen am Münchner Max-Joseph-Platz und anschließenden Folgeaktionen bisher 285 Verfahren gemäß § 170 Abs. 2 StPO sowie 89 weitere Verfahren gemäß § 170 Abs. 2 i.V.m. §153 Abs. 1 StPO eingestellt worden sind.

Derzeit werden vom Polizeipräsidium München die Auswirkungen der Einstellungen auf die weitere Speicherung der personenbezogenen Daten der von den Verfahren Betroffenen im KAN geprüft. Das Polizeipräsidium München hat bereits von sich aus 11 KAN-Speicherungen gelöscht und mitgeteilt, daß mit weiteren Löschungen zu rechnen sei.

Ich habe beim Polizeipräsidium München mit einer datenschutzrechtlichen Prüfung begonnen, um festzustellen, ob die aus datenschutzrechtlicher Sicht - gem. Art. 38 Abs. 2 Satz 2 PAG sind Daten zu löschen, falls der der Speicherung zugrunde liegende Verdacht entfallen ist - erforderlichen Konsequenzen aus der Beendigung der strafrechtlichen Ermittlungsverfahren gezogen werden. Eine abschließende Bewertung ist mir derzeit wegen teilweise noch offener Ermittlungsverfahren nicht möglich.

5.5 Prüfung der Rechtmäßigkeit von Abfragen im Informationssystem der Bayerischen Polizei (Protokolldatei)

Auch im Berichtszeitraum habe ich wieder die Rechtmäßigkeit von Abfragen in polizeilichen Informationssystemen und in nichtpolizeilichen Informationssystemen, auf die die bayerische Polizei online zugreifen kann, durch anlaßabhängige und anlaßunabhängige Auswertungen der Protokolldaten überprüft.

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

In meinem *15.* Tätigkeitsbericht (Ziffer 4.7.1) bin ich ausführlich auf die Bedeutung der Protokollierung polizeilicher Abfragen aus den polizeilichen und nichtpolizeilichen Informationssystemen sowie Sinn und Zweck meiner regelmäßigen Kontrollen der Abfragen eingegangen. Pressemeldungen über einzelne mißbräuchliche Abfragen durch Polizeibedienstete zeigen, daß die Notwendigkeit besteht, anlaßunabhängige Kontrollen weiter durchzuführen, um Mißbrauch entgegenzuwirken.

Ich habe mir zu diesem Zweck vom Landeskriminalamt **Ausdrucke der Protokolldaten** der ersten 1000 von Bediensteten des Präsidiums der Bayer. Grenzpolizei vorgenommenen Abfragen aktuellen Datums aus den Dateien

- Informationssystem Bayerische Polizei (IBP)
- Zentrales Verkehrsinformationssystem (ZEVIS)
- Einwohnermeldeamtsverfahren (EWO)
- Ausländerzentralregister (AZR)

fertigen lassen. Die Auswertung hat **keine** Hinweise auf mißbräuchliche Dateiabfragen erbracht.

5.5.2 Anlaßabhängige Auswertungen der Protokolldatei

Neben den anlaßunabhängigen Kontrollen habe ich aufgrund konkreter Angaben von Petenten auch anlaßbezogene Auswertungen der Protokolldatei durchgeführt:

1. Ein Petent wandte sich an mich, da ihm von dritter Seite Kopien polizeilicher Dateiausdrucke über Eintragungen zu seiner Person im **Kriminalaktennachweis** (KAN) zugesandt worden waren. Durch Auswertung der Protokolldatei mit dem Namen des Petenten als Suchbegriff konnte ich den Polizeibeamten sowie seine Dienststelle feststellen, der eine Abfrage im KAN veranlaßt hatte. Bei einer ersten Befragung gab der Beamte an, daß ihm der Grund der Abfrage nicht mehr erinnerlich sei. Auch eine Zuordnung der Abfrage zu einem dienstlichen Vorgang war bisher nicht möglich.

Da der Petent neben seiner Eingabe bei mir Strafanzeige bei der Staatsanwaltschaft erstattet hatte, habe ich meine datenschutzrechtliche Prüfung bis zum Abschluß des Ermittlungsverfahrens zurückgestellt.

2. Eine weitere Petition betraf einen Vorfall im Grenzgebiet zwischen Deutschland und Österreich. Dort war ein deutscher Autofahrer von unbekannten Personen angehalten und auf seine Teilnahme an einer Motorsportveranstaltung angesprochen worden. Kurz nach diesem Vorfall rief eine unbekannte Person die Halterin des von ihm geführten Fahrzeugs an und erkundigte sich nach diesem Fahrzeug. Nach dem Beschwerdevorbringen lag eine unzulässige Abfrage aus dem **Zentralen Verkehrsinformationssystem-ZEVIS** nahe. Die von mir veranlaßte Auswertung der Protokolldatei ergab, daß das amtliche Kennzeichen des Petenten am betreffenden Tag in zwei Fällen von Dienststellen der Bayer. Grenzpolizei abgefragt worden war. Die abfragenden Beamten gaben an, sich nicht mehr an das überprüfte Fahrzeug erinnern zu können. Eine abschließende Beurteilung der Rechtmäßigkeit der Dateiabfrage war auch in diesem Fall mit den mir zur Verfügung stehenden Möglichkeiten leider nicht zu erreichen. Ich habe aber das Präsidium der Bayerischen Grenzpolizei über den Vorgang und die von mir gewonnenen Erkenntnisse im Hinblick auf die etwaige Notwendigkeit innerdienstlicher Maßnahmen im einzelnen informiert.

5.5.3 Zusatzprotokollierung von Abfragen im Informationssystem der Bayerischen Polizei

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

Die Protokolldatei dient u.a. dem **Zweck,** innerhalb eines Jahres die Rechtmäßigkeit der Abfragen kontrollieren zu können und so einem möglichen Mißbrauch durch unbefugtes Abfragen und unzulässige Nutzung der dabei gewonnenen Daten vorzubeugen.

Aufgrund eigener Erfahrungen, insbesondere anläßlich meiner regelmäßigen anlaßunabhängigen Protqkollauswertungen (vgl. Ziff. 5.5.1) und von Erkenntnissen anderer Datenschutzbeauftragter, habe ich beim Innenministerium eine **Zusatzprotokollierung** von Abfragen angeregt. Zusätzlich zu den bereits bisher protokollierten Angaben sollten der **Zweck der Abfrage** und ggf. das **Aktenzeichen** des bearbeiteten Vorgangs angegeben und in der Protokolldatei festgehalten werden. Das Innenministerium hat mir mitgeteilt, daß meine Anregung geprüft wird. Ein Ergebnis liegt mir noch nicht vor.

5.6 Anwendung des Polizeiaufgabengesetzes (PAG)

5.6.1 Übermittlung personenbezogener Daten an ausländische Sicherheitsbehörden (Fußballweltmeisterschaft 1994)

Im Rahmen der Vorbereitungen zur Fußballweltmeisterschaft 1994 in den USA haben die amerikanischen Sicherheitsbehörden das Bundesministerium des Innern, das Bundeskriminalamt und das Landeskriminalamt Nordrhein-Westfalen um Unterstützung bereits im Vor-feld der Fußballweltmeisterschaft 1994 durch die Übermittlung personenbezogener Daten sog. ,,Fußballrowdies" gebeten. Gewünscht wurden detaillierte Informationen über Personen, die für die Anstiftung von fußball-bezogenen Gewalttaten bekannt sind oder über die Erkenntnisse aus dem Bereich der allgemeinen Kriminalität vorliegen und die wahrscheinlich anläßlich der Fußball-weltmeisterschaft 1994 in die USA reisen wollten.

Eine entsprechende Mitteilung über die Anfrage wurde vom Landeskriminalamt Nordrhein-Westfalen (zentrale Informationsstelle) u.a. auch an die Landesinformationsstelle Bayern (Polizeipräsidium München) weitergegeben. Dieses hat den Vorgang dem Staatsministerium des Innern zur Entscheidung vorgelegt.

Ich habe mich in einem Schreiben an das Innenministerium zu der erbetenen Datenübermittlung geäußert:

Die gewünschte Übermittlung der personenbezogenen Daten diente nicht der Verfolgung der Betroffenen im Rahmen konkreter Strafverfahren, sondern der Vorbereitung präventiver Maßnahmen amerikanischer Sicherheitsbehörden. Eine solche Datenübermittlung an öffentliche Stellen außerhalb des Geltungsbereiches des Grundgesetzes ist - mangels über- oder zwischenstaatlicher Vereinbarungen - nur zulässig, soweit dies zur Abwehr einer erheblichen Gefahr durch den Empfänger erforderlich ist (Art. 40 Abs. 5 Satz 1 Nr.2 Polizeiaufgabengesetz). Dabei muß es sich um eine **konkrete,** das heißt eine im Einzelfall bestehende erhebliche Gefahr handeln. Diese Voraussetzung habe ich nur dann als erfüllt angesehen, wenn hinreichende tatsächliche Anhaltspunkte bestehen, daß Personen in die USA aus Anlaß der Fußballweltmeisterschaft einreisen wollen, von denen aufgrund der vorliegenden Erkenntnisse bei diesem Ereignis mit

hinreichender Wahrscheinlichkeit Gefahren für bedeutsame Rechtsgüter ausgehen. Ich habe es deshalb für erforderlich gehalten, daß vor einer Datenübermittlung in jedem Einzelfall individuell geprüft wird, ob z.B. wegen der Erkenntnisse über Anstiftung, Planung oder Organisation von Gewalthandlungen von einer solchen Gefahrenannahme ausgegangen werden kann. Eine datenschutzrechtliche Prüfung evtl. Datenübermittlungen habe ich mir vorbehalten.

Darüber hinaus habe ich die Ansicht vertreten, daß eine Datenübermittlung nur unter der Bedingung erfolgen dürfe, daß die übermittelten Daten

- nur zu dem angegebenen Zweck der Gefahrenabwehr im Zusammenhang mit der Fußballweltmeisterschaft genutzt und
- anschließend unverzüglich vollständig gelöscht werden.

Die Einhaltung dieser Bedingungen müsse durch eine schriftliche Zusage des Datenempfängers sichergestellt werden.

Darüber hinaus habe ich angeregt zu prüfen, ob die von der Datenübermittlung betroffenen Personen rechtzeitig in geeigneter Weise davon unterrichtet werden sollten.

Das Innenministerium hat meine Bedenken geteilt. Trotz der grundsätzlich bestehenden Bereitschaft die Sicherheitsbehörden der USA bei der Bewältigung der Sicherheitsprobleme aus Anlaß der Fußballweltmeisterschaft zu unterstützen, hat es deshalb von einer Übermittlung personenbezogener Daten an die US-Sicherheitsbehörden abgesehen.

5.6.2 Datenübermittlungsersuchen der Telekom an die Polizei

Eine Polizeidirektion wandte sich mit der Frage an mich, ob die Telekom nach ihrer Umstrukturierung noch Behörde oder öffentliche Stelle im Sinne von Art. 40 PAG ist und ob einem **Ersuchen um** Bekanntgabe des Wohn- bzw. Aufenthaltsortes eines Schuldners oder um Mitteilung, ob sich ein Schuldner in Haft befindet gemäß Art. 40 Abs. 4 PAG entsprochen werden kann. Die TELEKOM hatte mitgeteilt, daß der Vollstreckungsschuldner laut Auskunft des Einwohnermeldeamtes unbekannt verzogen war.

Der Polizeidirektion habe ich folgende Auskunft erteilt:

Nach Art. 40 Abs. 4 Nr.3 PAG kann die Polizei auf Ersuchen personenbezogene Daten an Behörden oder öffentliche Stellen übermitteln, soweit dies zur Wahrung sonstiger schutzwürdiger Interessen erforderlich ist.

Die Bestimmung des Begriffs öffentliche Stelle in bezug auf Datenübermittlungen richtet sich nach der Legaldefinition des Art. 4 Abs. 2 Satz 2 BayDSG. Danach sind öffentliche Stellen auch die öffentlichen Stellen des Bundes gemäß § 2 des Bundesdatenschutzgesetzes und damit auch die TELEKOM.

Schutzwürdige Interessen im Sinne von Art. 40 Abs. 4 Nr. 3 PAG können alle von der Rechtsordnung als schutzwürdig anerkannten ideellen oder vermögenswerten Interessen, also auch **wirtschaftliche Interessen** sein. Das Interesse der Telekom an der Beitreibung der Gebührenschuld ist als schutzwürdiges Interesse anzusehen. Da eine Beitreibung ohne Kenntnis des Wohn- bzw. Aufenthaltsortes des Vollstreckungsschuldners nicht erfolgversprechend ist, ist die Datenübermittlung auch **erforderlich.**

Die Bekanntgabe des Wohn- bzw. Aufenthaltsortes des Vollstreckungsschuldners bzw. die Mitteilung, ob sich der Schuldner in Haft befindet, durch Polizeibehörden an die Telekom auf deren Ersuchen hin, **halte ich deshalb gemäß Art. 40 Abs. 4 Nr.3 PAG für zulässig.**

5.7 Richtlinien für die Führung personenbezogener polizeilicher Sammlungen (PpS-Richtlinien)

Polizeiinterne Grundlage für die Führung polizeilicher personenbezogener Sammlungen bei den Behörden und Dienststellen der bayerischen Polizei, die nach dem PAG und der StPO bestehenden Befugnisse im einzelnen beschreiben, sind die Richtlinien für die Führung personenbezogener polizeilicher Sammlungen (PpS-Richtlinien). Über diese Richtlinien, die am 01.01.1994 in Kraft getreten sind und die Richtlinien für die Führung kriminalpolizeilicher personenbezogener Sammlungen (KpS-Richtlinien aus dem Jahre 1981) ersetzen, habe ich bereits im *15.* Tätigkeitsbericht (Nr.4.9) ausführlich berichtet. Auf zwei datenschutzrechtliche Forderungen möchte ich wegen ihrer Bedeutung nochmals eingehen:

1. Reduzierung der im Kriminalaktennachweis (KAN) zu speichernden Vorgänge

   Mein Vorgänger im Amt hatte bereits in der Vergangenheit gefordert, Fahrlässigkeitsdelikte nicht mehr in den KAN aufzunehmen. Die PpS-Richtlinien sehen nunmehr vor, daß der Nachweis und die Erschließung der Kriminalakten grundsätzlich über die Datei polizeiliche Sachbearbeitung/Vorgangsverwaltung-Verbrechensbekämpfung (PSV) erfolgen, wenn darin ausschließlich Unterlagen über Sachverhalte geringerer Bedeutung erfaßt sind. Da Straftaten, die fahrlässig begangen wurden, nach den PpS-Richtlinien regelmäßig nur geringere Bedeutung zukommt, wird - zumindestens in den Fällen, in denen **ausschließlich Unterlagen über Fahrlässigkeitsdelik**te (evtl. zusammen mit Unterlagen über andere Fälle geringerer Bedeutung) in der Kriminalakte aufbewahrt werden - **von einer (landesweiten) Speicherung im KAN abgesehen. Der** Forderung des Datenschutzes wurde damit zum Teil entsprochen.

2. Speicherung von Suizidversuchen

   Das Staatsministerium des Innern hat mir zugesagt zu prüfen, in welchen Fällen Selbstmordversuche überhaupt zu einer Speicherung im Landes-KAN

führen sollen. Eine Regelung hierzu und zu anderen Fragen polizeilicher Speicherung wird die Neufassung der Errichtungsanordnung für die Datei KAN enthalten, die ich einer kritischen Prüfung unterziehen werde.

5.8 Änderung der Errichtungsanordnung für den Grenzaktennachweis (EA-GAN)

Die Bayerische Grenzpolizei hat die **Erweiterung der Zugriffsberechtigung** auf den sog. Landesgrenzaktennachweis der Bayerischen Grenzpolizei (Landes-GAN) auf alle bayerische Landespolizeidienststellen vorgeschlagen und eine entsprechend geänderte Errichtungsanordnung für die Datei erstellt.

Grund dafür war eine Änderung des Asylverfahrensgesetzes zum 01.07.1993 mit der den Dienststellen der Bayerischen Landespolizei Befugnisse zur Zurückschiebung von Asylbewerbern eingeräumt wurden, die über sichere Drittstaaten eingereist sind. Bei der Entscheidungsfindung muß die Landespolizei auch auf die im Landes-GAN gespeicherten Informationen (z.B. Zurückweisungen an der Grenze) zugreifen können. Grundsätzliche Bedenken gegen die Zugriffsbefugnis der Landespolizei habe ich deshalb nicht geäußert. Ich habe aber keine Notwendigkeit gesehen, die Zugriffsbefugnis auf alle Informationen des Landes-GAN auszudehnen. Ich habe daher das **Innenministerium gebeten, zu prüfen,** ob der Zugriff durch die Bayerische Landespolizei auf alle GAN-Schlüsselzahlen im Hinblick auf die Änderung ihrer Aufgaben nach dem Asylverfahrensgesetz erforderlich ist.

Das Innenministerium hat daraufhin veranlaßt, daß die Ereignisschlüssel, die nur für die Arbeit der Grenzpolizei bedeutsam sind, für den Zugriff durch die Landespolizei gesperrt werden.

5.9 Entwurf eines Gesetzes zur Ergänzung des Gesetzes zur Bekämpfung des illegalen Rauschgifthandels und anderer Erscheinungsformen der organisierten Kriminalität (OrgKGErgG) und Entwurf eines Gesetzes zur Anderung des Grundgesetzes

Das Staatsministerium der Justiz hat den Entwurf eines Gesetzes zur Ergänzung des Gesetzes zur Bekämpfung des illegalen Rauschgifthandels und anderer Erscheinungsformen der organisierten Kriminalität (OrgKGErgG) sowie den Entwurf eines Gesetzes zur Änderung des Grundgesetzes vorgelegt. Die Einbringung beider Gesetzentwürfe in den Bundesrat wurde in der Sitzung vom 17.05.1994 vom Ministerrat beschlossen. Durch die Gesetzentwürfe soll das straf- und strafverfahrensrechtliche Instrumentarium zur Bekämpfung der organisierten Kriminalität und besonders schwerer Fälle der Eigentums- und Vermögenskriminalität verbessert werden.

Aus datenschutzrechtlicher Sicht geht es dabei in erster Linie um folgende Punkte:

1. Nach Art. 1 des Entwurfs eines Gesetzes zur Änderung des Grundgesetzes sollen Eingriffe in die Unverletzlichkeit der Wohnung sowie Beschränkungen in diesem Bereich künftig auch zur Strafverfolgung zulässig sein.

2. Der OrgKGErgG-Entwurf enthält Regelungen zur technischen Wohnraumüberwachung (optische und akustische Beobachtung und Aufzeichnung im Schutzbereich des Art. 13 Grundgesetz).

Die Erweiterung des strafverfahrensrechtlichen Instrumentariums zur Bekämpfung der organisierten Kriminalität kann wegen der Bedrohung der Gesellschaft durch diese Kriminalitätsform im überwiegenden Interesse der Allgemeinheit hingenommen werden.

Ich habe daher keine grundsätzlichen Bedenken gegen die im Gesetzentwurf vorgesehenen Regelungen zur technischen Wohnraumüberwachung geäußert.

Allerdings darf der Einsatz besonderer technischer Mittel in Wohnungen im Hinblick auf die besondere Eingriffsintensität der Maßnahmen nur unter strengen Voraussetzungen zugelassen werden. Darüber hinaus muß wegen der Notwendigkeit der Kontrolle durch eine unabhängige Instanz die uneingeschränkte Kontrolle der Verarbeitung und Nutzung der durch die Maßnahme gewonnenen Daten durch den Datenschutzbeauftragten sichergestellt sein. Im einzelnen habe ich folgendes gefordert:

1. **Gesetz zur Änderung des Grundgesetzes**

   Der sog. Lauschangriff zur Strafverfolgung darf nur unter engen materiell-rechtlichen Voraussetzungen zugelassen werden. Dies gilt umso mehr, da der vorliegende Gesetzentwurf über den Einsatz technischer Mittel zum Abhören und Aufzeichnen des nicht öffentlich gesprochenen Wortes auch die Herstellung von Lichtbildern und Bildaufzeichnungen zuläßt. Da es sich hier um einen Eingriff in den Kernbereich des Persönlichkeitsrechts handelt, sollte die Ausgestaltung des Eingriffs nicht - wie vorgesehen ist - allein einfachgesetzlichen Regelungen vorbehalten bleiben. Dies gilt sowohl für die Eingriffsvoraussetzungen als auch für die Anordnungskompetenz (Richter-vorbehalt), zumal für den geringeren Eingriff der Durchsuchung ein Richtervorbehalt in Art. 13 Abs. 2 Grundgesetz vorgesehen ist.

   Ich halte es daher für notwendig, die zur Strafverfolgung vorgesehenen Eingriffe in die Unverletzlichkeit der Wohnung auf **Straftaten von erheblicher Bedeutung für die Rechtsordnung zu** beschränken. Sie dürfen **nur durch den Richter, bei Gefahr in Verzug im Vorgriff auf die Entscheidung des Richters auch durch die Staatsanwaltschaft angeordnet werden.**

   Diese Regelung der Anordnungskompetenz sollte ausdrücklich in das Grundgesetz aufgenommen werden.

Durch die Eilkompetenz der Staatsanwaltschaft können Grundrechtseingriffe zwar zunächst ohne eine Prüfung durch eine unabhängige Stelle wie das Gericht vorgenommen werden. Die Staatsanwaltschaft hat allerdings unverzüglich die richterliche Bestätigung zu beantragen. Wird diese nicht erteilt, tritt die Anordnung **außer Kraft.**

Ich habe zum Ausdruck gebracht, dabei davon auszugehen, daß

- eine richterliche Bestätigung auch dann einzuholen ist, wenn sich die Maßnahme - gleich aus welchem Grund - zwischenzeitlich erledigt hat,
- Maßnahmen, deren Bestätigung durch das Gericht wegen Rechtswidrigkeit ihrer Anordnung unterbleibt, sofort einzustellen und erlangte Datenbestände - einschließlich der Daten über Zufallsfunde - zu löschen sind.

Nur unter diesen Voraussetzungen habe ich davon abgesehen, entsprechende gesetzliche Regelungen zu fordern.

Zum Sachstand teilt die Staatsregierung mit, daß der Entwurf derzeit in den Ausschüssen des Bundesrates liege. Zu meinen Vorschlägen hat sich die Staatsregierung noch nicht im einzelnen geäußert.

2. **OrgKGErgG-Entwurf**

2.1 **Verwertungsverbot**

Die Verwendung der durch den Eingriff erlangten personenbezogenen Daten zu Beweiszwecken in anderen Strafverfahren ist nur eingeschränkt zulässig. ‚Als Ermittlungsansatz in anderen Strafverfahren und zur Gefahrenabwehr dürfen sie jedoch - legt man die Rechtsprechung zu § 100 a der Strafprozeßordnung (StPO) zugrunde - genutzt werden. Die besondere Intensität des mit der geplanten Maßnahme verbundenen Grundrechtseingriffs verbietet es jedoch, daß die gewonnenen Erkenntnisse für die Verfolgung jedweder Straftat und die Abwehr jedweder Gefahr verwendet werden. Da nur aufgrund der schwerwiegenden Gefahren der organisierten Kriminalität für den Einzelnen und die Allgemeinheit das Eindringen staatlicher Organe in den Schutzbereich des Art. 13 Grundgesetz zugelassen werden kann, dürfen die dadurch gewonnenen personenbezogenen Informationen zur Verfolgung ‚minderschwerer Straftaten und zur Abwehr von Gefahren ohne erhebliches Gewicht nicht verwertet werden. Die in Art. 13 Grundgesetz verbriefte Unverletzlichkeit der Wohnung darf im Rahmen des Verhältnismäßigkeitsgrundsatzes nur insoweit eingeschränkt werden, als es zur Bekämpfung schwerer Straftaten unerläßlich ist. Diese Auffassung findet ihre Stütze auch in einer Entscheidung des Bundesgerichtshofes aus dem Jahr 1980 zur Telefonüberwachung nach dem G 10-Gesetz. Dort wird u.a. ausgeführt:
„Im Lichte der Verfassung macht es keinen wesentlichen Unterschied, ob derjenige, der von einer Telefonüberwachung betroffen und dadurch in seinem Grundrecht aus Art. 10 Abs. 1 Grundgesetz beeinträchtigt ist, aufgrund der unmittelbar oder nur der mittelbar erlangten Beweismittel strafrechtlicher Verfolgung ausgesetzt wird".

Ich habe daher gefordert, die Verwendung der gewonnenen Daten als Ermittlungsansatz auf bestimmte schwere Straftaten und auf die Abwehr erheblicher Gefahren zu beschränken.

2.2 Zeugnisverweigerungsrecht von Berufsgeheimnisträgern und von Personen, die aus persönlichen Gründen zur Verweigerung des Zeugnisses berechtigt sind

Es fehlen Regelungen zur Verwertbarkeit von Mitteilungen zwischen dem Beschuldigten und Personen, die nach § 52 StPO (Angehörige) oder § 53 Abs. 1 Nr.1 bis 3 b (Berufsgeheimnisträger) zur Verweigerung des Zeugnisses berechtigt sind. Eine solche Regelungslücke ist nicht hinnehmbar. Es kann auch nicht angenommen werden, daß - wie bei dem geringeren Eingriff der Telefonüberwachung - § 97 StPO, der die Beschlagnahmefreiheit solcher Mitteilungen vorsieht, für Berufsgeheimnisträger sinngemäß anwendbar ist, da der Entwurf zwar eine Reihe anderer, **nicht aber diese Bestimmung** für anwendbar erklärt.

Das würde dazu führen, daß die genannten Personengruppen zwar das Zeugnis verweigern und Mitteilungen zwischen ihnen und dem Beschuldigten nicht der Beschlagnahme unterliegen. Vertrauliche Gespräche im Schutz der Wohnung wären dagegen dem Zugriff der Strafverfolgungsbehörden ausgesetzt.

Ich habe daher gefordert, § 97 StPO ausdrücklich für anwendbar zu erklären.

2.3 Jährlicher Bericht des Justizministeriums an eine Kommission

Bei Eingriffen in den Kernbereich der Privatsphäre des Bürgers bedarf es als Korrelativ verstärkter Kontrollen. Neben der gerichtlichen Kontrolle und der Datenschutzkontrolle halte ich einen jährlichen Bericht des Justizministeriums an eine parlamentarische Kommission (wie z.B. PKK, G 10-Kommission, Rechtsausschuß) für einen besonders geeigneten Kontrollmechanismus. Diese Berichtspflicht, die zu einer größeren Transparenz staatlichen Handelns für Parlament und Bürger führt, stärkt zugleich das Vertrauen des Bürgers und fördert die Akzeptanz der zu treffenden Maßnahmen.

2.4 Kontrollbefugnis des Datenschutzbeauftragten

Ich habe in diesem Zusammenhang erneut daraufhingewiesen, daß unter Berücksichtigung der Rechtsprechung des Bundesverfassungsgerichts die Kontrolle der Verarbeitung und Nutzung der Daten, die auf der Grundlage der geplanten Maßnahme gewonnen

werden, durch eine unabhängige Stelle sichergestellt sein muß. Der erhebliche Grundrechtseingriff, der mit der technischen Wohnraumüberwachung verbunden ist, ist mit der Datenerhebung, die der Kontrolle des Gerichts unterliegt, nicht beendet, sondern wirkt bei der weiteren Verwendung der Daten fort. Dies stellt einen zusätzlichen Grundrechtseingriff dar. Die Verarbeitung und Nutzung der Daten unterliegt aber nur dann der richterlichen Kontrolle, wenn die Daten in einem Gerichtsverfahren verwertet werden sollen und der Verarbeitung und Nutzung für die Frage der Verwertung Bedeutung zukommt. Nur dann prüft der Richter, ob die Daten rechtmäßig erhoben, verarbeitet und genutzt wurden. Werden Verfahren gegen die von der Maßnahme Betroffenen durch die Staatsanwaltschaft gar nicht erst eingeleitet oder eingestellt oder finden die Daten für die gerichtliche Entscheidung keine Verwendung, wohl aber für andere Zwecke (z.B. Speicherung zur Gefahrenabwehr), unterliegen die Eingriffe nicht der gerichtlichen Kontrolle. Die Verarbeitung und Nutzung dieser Daten bedarf daher der Kontrolle eines anderen unabhängigen Kontrollorgans. Die notwendige Kontrolle kann durch den Datenschutzbeauftragten sichergestellt werden, der im Gegensatz zur Aufsichtsbehörde die Forderungen des Bundesverfassungsgerichts nach der Unabhängigkeit des Kontrollorgans erfüllt.

Ich meine deshalb, daß die uneingeschränkte Kontrolle der Verarbeitung und Nutzung der durch die geplante Maßnahme gewonnenen Daten durch den Datenschutzbeauftragten möglich sein muß. Dies gilt auch für die **in Akten** verarbeiteten und genutzten Daten.

5.10 Entwurf eines Gesetzes über das Bundeskriminalamt und die Zusammenarbeit des Bundes und der Länder in kriminalpolizeilichen Angelegenheiten (Bundeskriminalamtsgesetz -BKAG-)

Die Bundesregierung hat den Entwurf eines Gesetzes über das Bundeskriminalamt und die Zusammenarbeit des Bundes und der Länder in kriminalpolizeilichen Angelegenheiten (Bundeskriminalamtsgesetz -BKAG) vorgelegt. Der Gesetzentwurf verfolgt das Ziel, das Gesetz über die Einrichtung eines Bundeskriminalpolizeiamtes vom 08. März 1951 in der Fassung vom 29. Juni 1973, zuletzt geändert durch das 1. Gesetz zur Reform des Strafrechts vom 09. Dezember 1974, fortzuentwickeln. Damit soll insbesondere auch dem Urteil des Bundesverfassungsgerichts vom *15.* Dezember 1983 zum Volkszählungsgesetz 1983 Rechnung getragen werden, wonach Beschränkungen des Rechts auf informationelle Selbstbestimmung einer verfassungsmäßigen gesetzlichen Grundlage bedürfen, aus der sich Voraussetzungen und Umfang der Beschränkungen klar und für den Bürger erkennbar ergeben.

Dies ist zu begrüßen. Ich meine aber, daß der Entwurf noch nicht allen datenschutzrechtlichen Anforderungen genügt. Zu wichtigen Einzelfragen vertrete ich folgende Auffassung:

1. **Erhebungskompetenz**

Nach dem Gesetzentwurf kann das Bundeskriminalamt, soweit dies zur Erfüllung seiner Aufgabe als Zentralstelle, insbesondere zur Ergänzung vorhandener Daten erforderlich ist, Daten durch **Ersuchen um Auskünfte, Anfragen oder Einsichtnahmen in Akten bei den Polizeien des Bundes und der Länder erheben.** Bei anderen **öffentlichen und nichtöffentlichen Stellen, bei Polizei- und Justizbehörden sowie sonstigen für die Verhütung und Verfolgung von Straftaten zuständigen öffentlichen Stellen anderer Staaten sowie bei internationalen Organisationen, die mit der Aufgabe der Verhütung und Verfolgung von Straftaten befaßt sind,** kann das BKA unter o.g. Voraussetzungen Daten erheben, wenn eine Erhebung bei den Polizeien des Bundes und der Länder **keinen Erfolg verspricht.**

Dem BKA als Zentralstelle wird damit eine eigene Befugnis zur Datenerhebung eingeräumt. Danach können auch personenbezogene Daten, deren Übermittlung von der Polizei an das BKA nach Landespolizeirecht nicht vorgesehen ist, durch das BKA selbst erhoben werden. Dagegen habe ich - ebenso wie mein Amtsvorgänger - keine verfassungsrechtlichen Bedenken.

Nach Art. 73 Nr.10 Grundgesetz hat der Bund die ausschließliche Gesetzgebung über die Zusammenarbeit des Bundes und der Länder in der Kriminalpolizei sowie für die Einrichtung eines Bundeskriminalpolizeiamtes. Art. 87 Abs. 1 Satz 2 Grundgesetz, der die Schaffung einer Zentralstelle für das polizeiliche Auskunfts- und Nachrichtenwesen, für die Kriminalpolizei und zur Sammlung von Unterlagen für Zwecke des Verfassungsschutzes regelt, unterscheidet zwischen einer **Zentralstelle für das polizeiliche** Auskunfts- **und** Nachrichtenwesen und einer **Zentralstelle zur Sammlung** von Unterlagen zum Zwecke des Verfassungsschutzes. Daraus läßt sich schließen, daß die Zentralstelle für das polizeiliche Auskunfts- und Nachrichtenwesen mehr sein muß als eine Stelle, die auf das **Sammeln** von Unterlagen beschränkt ist. Darüber hinaus hat das Bundeskriminalamt vielfältige Aufgaben, so z.B. das Sammeln und Auswerten aller Nachrichten und Unterlagen für die polizeiliche Verbrechensbekämpfung und auch die Unterstützung der Polizeien der Länder in der Vorbeugungsarbeit zur Verbrechensverhütung. Zur Erfüllung dieser Aufgaben wurde ein Informationssystem geschaffen, das über einen **einheitlichen Standard** verfügen muß, will es diesen Zwecken auch gerecht werden. Dieser Standard muß vom BKA-Gesetz festgelegt werden können. Ansonsten müßte sich die gemeinsame Datensammlung

des Bundes und der Länder am restriktivsten Landesgesetz ausrichten.

2. **Übermittlungskompetenz**

Nach dem Gesetzentwurf erhält das BKA eigene Übermittlungskompetenzen im innerstaatlichen und internationalen Bereich. Bei der Beurteilung erscheint eine differenzierte Betrachtungsweise geboten:

Bei der Datenübermittlung im **innerstaatlichen Bereich** ist zu unterscheiden zwischen Datenübermittlung an

- Polizeien des Bundes und der Länder,
- sonstigen öffentlichen Stellen und
- nichtöffentlichen Stellen.

Während bezüglich der Übermittlung **eigener Datenbestände aus Amtsdateien des BKA gegen die Regelung des Entwurfs keine Bedenken bestehen,** gilt dies für Daten, die **von den Ländern in** Verbunddateien des Bundes und der Länder eingegeben wurden, nicht uneingeschränkt.

Zur Erfüllung seiner Aufgaben als Zentralstelle (Zusammenarbeit des Bundes und der Länder) halte ich die Regelung der Zuständigkeit des BKA für die Datenübermittlungen an **Polizeidienststellen** des Bundes und/oder der Länder für zulässig. Dies ergibt sich bereits aus Art. 73 Nr.10 Grundgesetz, der dem Bund die ausschließliche Gesetzgebung über die Zusammenarbeit des Bundes und der Länder in der Kriminalpolizei überträgt.

Anders ist die Kompetenzzuweisung für die Datenübermittlung an andere öffentliche oder nichtöffentliche Stellen zu beurteilen. Das Recht, als Zentralstelle polizeiliche Daten für die Zusammenarbeit des Bundes und der Länder zu sammeln, umfaßt nicht das Recht, ,,Länderdaten" an andere Stellen weiterzuleiten. Dies setzt grundsätzlich für jeden Einzelfall das Einvernehmen mit den datenbesitzenden Landesbehörden voraus.

Datenübermittlungen des BKA im internationalen Bereich (siehe auch Beitrag EUROPOL Nr. 5.14.1) sind vorgesehen u.a. an Polizei- und Justizbehörden sowie an sonstige für die Verhütung und Verfolgung von Straftaten zuständige öffentliche Stellen anderer Staaten sowie an zwischen- und überstaatliche Stellen, die mit Aufgaben der Verhütung und Verfolgung von Straftaten befaßt sind, soweit dies erforderlich ist zur Erfüllung einer ihm obliegenden Aufgabe

- zur Verfolgung von Straftaten und zur Strafvollstreckung nach Maßgabe der Vorschriften über die internationale Rechtshilfe in strafrechtlichen Angelegenheiten,
- zur Verhütung von Straftaten von erheblicher Bedeutung oder
- zur Abwehr einer im Einzelfall bestehenden erheblichen Gefahr für die öffentliche Sicherheit.

Eine solche Befugnisnorm wäre zumindest für den Bereich der Gefahrenabwehr im Hinblick auf die Regelung der Gesetzeskompetenz im Grundgesetz problematisch.

Nach Art. 73 Nr.10 Grundgesetz hat der Bund u.a. die ausschließliche Gesetzgebung über die Zusammenarbeit des Bundes und der Länder in der Kriminalpolizei, über die Einrichtungen des Bundeskriminalamtes und der **internationalen Verbrechensbekämpfung.** Der Begriff ,,internationale Verbrechensbekämpfung" umfaßt jedoch **nur** die **Strafverfolgung durch** deutsche Behörden auf fremden Ge**biet und** die **Amtshilfe deutscher Behörden auf Er**suchen ausländischer Strafverfolgungsbehörden. Der Bereich der Gefahrenabwehr wird davon **nicht** umfaßt.

Auch aus der Zentralstellenbefugnis kann eine Berechtigung des BKA zur Datenübermittlung ins Ausland zum Zwecke der Gefahrenabwehr ebenfalls nicht abgeleitet werden. Die Zentralstellenbefugnis bezieht sich **auf die polizeiliche Zusammenarbeit des Bundes und der Länder,** also auf die nationale Zusammenarbeit, nicht auf die Zusammenarbeit mit anderen Staaten.

3. **Datenspeicherung**

Nach dem Entwurf können personenbezogene Daten von Personen, die bei einer künftigen Strafverfolgung als Zeugen in Betracht kommen, oder bei denen Anhaltspunkte bestehen, daß sie Opfer einer künftigen Straftat werden könnten, sowie von Kontakt- und Begleitpersonen, Hinweisgebern und sonstigen Auskunftspersonen gespeichert, verändert und genutzt werden, soweit dies zur Verhütung oder zur Vorsorge für die künftige Verfolgung einer Straftat mit erheblicher Bedeutung erforderlich ist.

Damit wird die Speicherung verschiedener Personengruppen einheitlich geregelt, obwohl eine differenzierte Regelung erforderlich wäre. Dies gilt insbesondere für die nach dem Entwurf zulässige Speicherung **potentieller** Zeugen und Opfer. Der Wortlaut der Regelung läßt eine flächendeckende Speicherung ganzer Personengruppen (z.B. Homosexueller, Freier, Pizzeriabesitzer) zu Dies ist aus datenschutzrechtlicher Sicht abzulehnen.

Vorstehende Ausführungen habe ich dem Innenministerium zur Berücksichtigung in den weiteren Verhandlungen zum BKA-Gesetz übermittelt.

5.11 Geldwäschegesetz

Am 29.11.1993 trat das Gesetz über das Aufspüren von Gewinnen aus schweren Straftaten (sog. Geldwäschegesetz - GWG) in Kraft. Das Gesetz dient der effektiven

Verfolgung der Geldwäsche und damit - durch den Versuch des Entzugs finanzieller Ressourcen - der Bekämpfung der organisierten Kriminalität. Es enthält Identifizierungs- und Aufzeichnungspflichten bei Finanztransaktionen, insbesondere für Banken und andere Gewerbe-treibende sowie die Verpflichtung zur Meldung von Verdachtsfällen der Geldwäsche an die Strafverfolgungsbehörden. Zur Verfahrenspraxis haben mir das Bayerische Staatsministerium des Innern und das Bayerische Staatsministerium der Justiz folgendes mitgeteilt:

Anzeigen nach § 11 GWG sollen in Bayern an die Staatsanwaltschaften bei den Oberlandesgerichten und an das Landeskriminalamt erstattet werden. Die Bankenverbände, die Versicherungswirtschaft und die Spielbanken sind entsprechend unterrichtet. Bei den Staatsanwaltschaften werden die Anzeigen unabhängig vom Vorliegen eines Anfangsverdachts im Sinne des § 152 Abs. 2 der Strafprozeßordnung (StPO) wie **eine Strafanzeige in das sog. OJs-Register** eingetragen.

Beim Landeskriminalamt werden die Anzeigen im Rahmen der Vorgangsverwaltung gespeichert. Sofern sich ein Anfangsverdacht für ein Vergehen nach § 261 Strafgesetzbuch (Geldwäsche) ergibt, erfolgt die Speicherung auch in der Vorgangsverwaltung der ermittlungsführenden Polizeidienststelle. Darüber hinaus werden in diesen Fällen, in denen Ermittlungsverfahren eingeleitet werden, Kriminalakten angelegt. Erkenntnisse aus Anzeigen werden auch in die Dateien ADOK oder APOK eingestellt, sofern die in den Errichtungsanordnungen genannten Speicherungsvoraussetzungen vorliegen.

Die Speicherungen durch die Polizei halte ich aus datenschutzrechtlicher Sicht für angemessen. Bei der Staatsanwaltschaft halte ich dagegen eine differenziertere registermäßige Behandlung eingehender Anzeigen nach §11 GWG für erforderlich:

Nach meiner Auffassung unterscheiden sich Anzeigen nach § 11 GWG grundsätzlich von Strafanzeigen, die sich gegen eine bestimmte Person richten: Während eine Strafanzeige vom Willen des Anzeigeerstatters getragen ist, daß der von ihm Beschuldigte für ein bestimmtes Verhalten strafrechtlich zur Verantwortung gezogen wird, sind Institute und Spielbanken von Gesetzes wegen verpflichtet, ihnen verdächtig erscheinende Finanztransaktionen den zuständigen Strafverfolgungsbehörden unverzüglich anzuzeigen. Dieser Unterschied ist auch bei der Speicherung in staatsanwaltschaftlichen Informationssystemen zu berücksichtigen:

Leitet die Staatsanwaltschaft aufgrund einer Anzeige nach dem Geldwäschegesetz wegen bestehenden Anfangsverdachts einer Straftat ein Ermittlungsverfahren ein, stehen einer Eintragung des Verfahrens in das OJsRegister datenschutzrechtliche Gesichtspunkte nicht entgegen. Fehlt es jedoch an einem Anfangsverdacht - die Mitteilung des Geldinstituts muß einen solchen noch nicht begründen -, sollte das Verfahren entweder in ein neu zu errichtendes besonderes Register oder in das Register für allgemeine Rechtssachen (AR-Register) eingetragen werden. Dieser unterschiedlichen registermäßigen Behandlung kommt im Hinblick auf die **geplanten bayern- und bundesweiten staatsanwaltschaftlichen Informationssysteme** auch große praktische Bedeutung zu. Würden alle Anzeigen nach § 11 GWG im OJs-Register eingetragen, wären sie nach Realisierung des im Verbrechensbekämpfungsgesetz (Entwurf) vorgesehenen Systems „Bundes-Sissy" **auch bundesweit abfragbar.**

Ich habe das Staatsministerium der Justiz hierzu um Stellungnahme gebeten. Eine abschließende Äußerung liegt mir noch nicht vor.

5.12 Entwurf eines Gesetzes zur Änderung des Strafgesetzbuches, der Strafprozeßordnung und anderer Gesetze (Verbrechensbekämpfungsgesetz)

Von den Fraktionen im Deutschen Bundestag der CDU/CSU und der FDP wurde der Entwurf eines Gesetzes zur Änderung des Strafgesetzbuches, der Strafprozeßordnung und anderer Gesetze (Verbrechensbekämpfungsgesetz) eingebracht. Dieser Gesetzentwurf wurde zwischenzeitlich vom Deutschen Bundestag beschlossen.

In Art. 12 (Änderung des Gesetzes zu Art. 10 Grundgesetz) werden dem Bundesnachrichtendienst (BND) Befugnisse bei der internationalen Verbrechensbekämpfung eingeräumt. Der BND darf künftig

- zur Erkennung und Begegnung einer Gefahr der Begehung bestimmter Kriminalitätsformen (z.B. Geldfälschung, Geldwäsche, unbefugte Verbringung von Betäubungsmitteln in nicht geringer Menge) die internationalen, nicht leitungsgebundenen Fernmeldeverkehrsbeziehungen überwachen und aufzeichnen.
- die bei der Durchführung dieser Maßnahmen erlangten personenbezogenen Daten zur Verhinderung, Aufklärung oder Verfolgung von bestimmten schweren Straftaten (z.B. Geld- oder Wertpapierfälschung, schwerer Menschenhandel, räuberische Erpressung) an die zuständigen Behörden (z.B. Staatsanwaltschaften) übermitteln.

Grundsätzliche datenschutzrechtliche Bedenken habe ich gegen diese Erweiterung der Befugnisse des BND nicht geäußert. Ich bedauere aber, daß der Bundesgesetzgeber die An?egung nach Klarstellung im Gesetzestext selbst, daß die erweiterte Fernmeldeaufklärung dem Bundesnachrichtendienst nur zur Erfüllung seiner eigenen Aufgaben eingeräumt wird (Beobachtung von Vergehen mit außen- und sicherheitspolitischer Bedeutung im Ausland), nicht aufgegriffen hat. Dies hätte verdeutlicht, daß eine gezielte Erhebung von Daten für polizeiliche Zwecke nicht zulässig ist. Auch der Forderung nach einer wirksamen Kontrollmöglichkeit durch den Datenschutzbeauftragten in diesem sensiblen Bereich wurde leider nicht entsprochen.

Ich teile aber insbesondere die Auffassung nicht, durch die im Gesetzentwurf vorgesehene erweiterte Fernmeldeaufklärung des BND und die Zulässigkeit der Über-

mittlung personenbezogener Daten an andere Behörden werde das Trennungsgebot verletzt, da die organisatorische und informationelle Trennung von BND und Strafverfolgungsbehörden bestehen bleibt und der BND kefne exekutiven Zwangsbefugnisse erhält. Die Strafverfolgung bleibt weiterhin alleinige Aufgabe der Polizei und der sonstigen Strafverfolgungsbehörden.

Allerdings muß auch in Zukunft darauf geachtet werden, daß die geheimdienstliche Informationsmacht und die polizeilichen Exekutivbefugnisse strikt getrennt bleiben. Die Datenschutzbeauftragten des Bundes und der Länder haben deshalb mit meiner Stimme in einem gemeinsamen Beschluß gefordert, beim Vollzug des Gesetzes darauf zu achten, daß nicht gezielt Informationen gesammelt werden, die vom Auftrag des BND nicht umfaßt werden, um die klare Trennungslinie zwischen Nachrichtendienst und Polizeibehörden nicht zu verwischen.

5.13 Gesetz zur Änderung polizeirechtlicher Vorschriften

Der Bayerische Landtag hat am 15.12.1994 das Gesetz zur Änderung polizeirechtlicher Vorschriften beschlossen. Das Gesetz bringt eine erhebliche Ausweitung ereignis- und verdachtsunabhängiger polizeilicher Kontrollmöglichkeiten mit sich. Bisher durfte die Bayerische Polizei solche Kontrollen, für die keinerlei tatsächliche Anhaltspunkte für eine konkrete Gefahr oder die Begehung bestimmter Straftaten vorliegen müssen, nur zur Verkehrskontrolle und zu Verkehrserhebungen (§ 36 Abs. 5 der Straßenverkehrsordnung) sowie im ,,Zollgrenzbezirk" und in Flugplatzbereichen zur Verhütung oder Unterbindung unerlaubter Überschreitung der Landesgrenze (Art. 13 Abs. 1 Nr. 5 PAG) durchführen. Identitätsfeststellungen nach Art. 13 Abs. 1 Nr. 2 PAG (an sog. verrufenen Orten) oder Art. 13 Abs. 1 Nr. 4 (an Kontrollstellen) setzen zumindest Anhaltspunkte für Störungen oder die Begehung der in § 100 a der Strafprozeßordnung genannten schweren Straftaten voraus und sind auf einen engen räumlichen Bereich begrenzt.

Künftig wird die Bayerische Polizei Personenkontrollen - einschließlich der Befugnis zur Durchsuchung von Personen und Sachen - auch in einem 30 Kilometer breiten Streifen entlang der Grenzen sowie auf ,,Durchgangsstraßen" und ,,öffentlichen Einrichtungen des internationalen Verkehrs" zur Verhütung oder Unterbindung der unerlaubten Überschreitung der Landesgrenze oder des unerlaubten Aufenthalts oder zur **Bekämpfung der grenzüberschreitenden Kriminalität** durchführen können.

Begründet werden diese zusätzlichen Befugnisse mit der Notwendigkeit von Ausgleichsmaßnahmen für den im Rahmen der Verwirklichung des Schengener Durchführungsübereinkommens angestrebten Abbau der Binnengrenzkontrollen zwischen den Schengener Vertragsstaaten und dem damit verbundenen Wegfall der ,,Filterfunktion" der Grenzkontrollstellen. Hinzu komme, daß mit dem bevorstehenden Wirksamwerden des Beitritts der Republik Österreich zur Europäischen Union die bayerisch-österreichische Grenze ihren Charakter als Zollgrenze verliere.

Gegen die sowohl örtliche wie sachliche Erweiterung der polizeilichen Befugnis zur verdachtsunabhängigen Identitätsfeststellung habe ich im Hinblick auf die Bedrohung durch die wachsende grenzüberschreitende Kriminalität von erheblicher Bedeutung und die Notwendigkeit der Abwehr unerlaubter Grenzübertritte keine grundsätzlichen datenschutzrechtlichen Bedenken. Allerdings wäre aus meiner Sicht wegen der vom Bundesverfassungsgge richt in seiner Entscheidung zum Volkszählungsgesetz 1983 geforderten **Normenklarheit eine Konkretisierung der Regelung -** soweit die Kontrolle auf **„Durchgangsstraßen"** erweitert wird - erforderlich gewesen. Nach der genannten Entscheidung des Bundesverfassungsgerichts bedürfen Beschränkungen des Rechts auf informationelle Selbstbestimmung einer gesetzlichen Grundlage, aus der sich die Voraussetzung und der Umfang der Beschränkungen klar und für den Bürger erkennbar ergeben. Diese Klarheit muß sich aus dem Gesetz selbst ergeben, Ausführungen in der Begründung genügen nicht. Der **Gesetzentwurf berücksichtigte diese Forderungen** aus meiner Sicht **nicht in ausreichendem** Maße. Insbesondere ist für den Bürger und die Polizei nicht ausreichend klar erkennbar, was unter ,,Durchgangsstraßen" - die Regelung beschränkt sich nicht auf Autobahnen - zu verstehen ist.

Ich hatte deshalb vorgeschlagen, als solche Straßen die **Bundesautobahnen und die Europastraßen als Regelfälle** im Gesetz selbst zu benennen. **Die Staatsregierung hat das übernommen.** Soweit darüber hinaus Straßen in entsprechende Kontrollmaßnahmen einbezogen werden sollen, sollte dies nur zulässig sein, wenn **tatsächliche Anhaltspunkte dafür** vorliegen, daß die **anderen Straßen** ebenfalls diese internationale Verkehrsbedeutung haben und der Einsatz der Maßnahme durch den Dienststellenleiter angeordnet wird. Diese Forderung hat die Staatsregierung nicht übernommen.

Auch der Bayerische Senat sah die Umschreibung derbetroffenen Straßen im Entwurf als ,,Durchgangsstraßen" als nicht präzise genug an, um der Polizei die notwendige Sicherheit zu geben, auf welchen Straßen sie kontrollieren darf und um den rechtsstaatlichen Bedürfnissen zu entsprechen. Er hat deshalb vorgeschlagen, die in der Begründung zum Gesetz genannte Definition (alle Straßenverbindungen des internationalen Verkehrs, die aufgrund ihrer Verkehrsbedeutung für die grenzüberschreitende Kriminalität relevant sind) als eigene Definitionsnorm in das Gesetz selbst aufzunehmen. Die Staatsregierung ist dem gefolgt.

Die geplante Gesetzesänderung geht über den Ausgleich des Wegfalls der bisherigen Kontrollmöglichkeiten an den Binnengrenzen hinaus, indem sie die bisherigen Eingriffsmöglichkeiten der Polizei erweitert. Während bisher

verdachtsunabhängige Identitätsfeststellungen nach Art. 13 Abs. 1 Nr. 5 PAG auf die Bekämpfung unerlaubter Grenzübertritte und auf den Grenzbereich und auf Flugplätze beschränkt waren, soll diese Möglichkeit nunmehr auf große Teile des Straßennetzes des gesamten Staatsgebiets ausgeweitet, auf sämtliche Anlagen des internationalen Verkehrs, also auch auf entsprechende Bahnhöfe und Verkehrsmittel erstreckt und allgemein auf die Bekämpfung der grenzüberschreitenden Kriminalität ausgedehnt werden.

Die in den verdachtsunabhängigen Identitätskontrollen und Durchsuchungen liegenden Eingriffe in den grundgesetzlich geschützten allgemeinen Freiheitsbereich des Bürgers dürfen jedoch nur soweit erfolgen, wie es zum Schutz öffentlicher Interessen unerläßlich ist; dabei ist der Grundsatz der Verhältnismäßigkeit zu beachten. Unter diesen Gesichtspunkten habe ich es zum Ausgleich für die erweiterte Kontrollmöglichkeit für erforderlich gehalten, diese zusätzliche Befugnis der Polizei auf den genannten Durchgangsstraßen nur zur Bekämpfung der grenzüberschreitenden Kriminalität von **erheblicher Bedeutung** im Sinne des Art. 30 Abs. 5 PAG einzusetzen. Eine derartige Begrenzung ist **mir** auch aus polizeilicher Sicht vertretbar erschienen, da der Katalog in Art. 30 Abs. 5 PAG nicht abschließend ist und damit die verdachtsunabhängigen Identitätskontrollen in dem genannten Raum auch zur Bekämpfung von Kriminalitätsbereichen möglich wären, die mit den in Art. 30 Abs. 5 PAG genannten Straftatbeständen vom Gewicht her vergleichbar sind. Auch diese Forderung wurde nicht übernommen. Der Bayerische Landtag hat den Gesetzentwurf in der von der Staatsregierung vorgelegten Fassung beschlossen. Ich werde aufmerksam beobachten, wie sich der Vollzug des Gesetzes in der Praxis gestaltet und ggf. auf meine Forderungen zurückkommen.

5.14 Polizeiliche Zusammenarbeit im Rahmen der Europäischen Union

Auch in diesem Berichtszeitraum habe ich die Entwicklung der europäischen polizeilichen Zusammenarbeit weiter beobachtet. Dabei geht es insbesondere um die Schaffung einer europäischen polizeilichen Zentralstelle.

5.14.1 Europäische Zentralstelle (EUROPOL)

Angesichts der Kriminalitätsentwicklung ist die institutionalisierte polizeiliche Zusammenarbeit und damit die Schaffung einer Europäischen Zentralstelle (EUROPOL) vordringliches Ziel auch der Bundesrepublik Deutschland. Bisher existiert in Den Haag nur ein Kooperationsstab EDU (European Drug Unit), der auf dem Gebiet der Bekämpfung der Drogenkriminalität die Möglichkeit des Informationsaustausches zwischen den Mitgliedstaaten der Europäischen Union bieten soll. Die in einer ,,Ministervereinbarung" vorgesehene Übermittlung der von den Polizeibehörden der Länder in bestimmten Anwendungen des INPOL-Systems gespeicherten Daten stützt sich dabei - mangels einer anderen Rechtsgrundlage - auf die jeweiligen Landespolizeigesetze.

Damit EUROPOL den Status einer internationalen zwischenstaatlichen Organisation mit eigener Rechtspersönlichkeit erhält, bedarf es nach einhelliger Auffassung eines völkerrechtlichen Vertrages (Konvention). Dieser wird zur Zeit von einer Arbeitsgruppe EUROPOL ausgearbeitet. Den Vorsitz der Arbeitsgruppe stellt jeweils der Mitgliedstaat der Europäischen Union, der die halbjährlich wechselnde Präsidentschaft innehat. Die Bundesregierung beabsichtigt, während der deutschen Präsidentschaft im 2. Halbjahr 1994 die Beratungen zum Konventionsentwurf abzuschließen und einen ratifizierungsfähigen Vertragstext vorzulegen.

Im Rahmen der Beteiligung der Länder an den Beratungen zum Konventionsentwurf habe ich u.a. auf folgendes hingewiesen:

Nach dem Konventionsentwurf bezeichnet jeder Mitgliedstaat eine nationale Kontrollinstanz, deren Aufgabe darin besteht, nach Maßgabe des jeweiligen nationalen Rechts die Zulässigkeit der Eingabe in das Informationssystem und der sonstigen Übermittlung personenbezogener Daten an EUROPOL durch den jeweiligen Mitgliedstaat unabhängig zu überwachen und zu prüfen, ob hierdurch die Rechte des Betroffenen verletzt werden. Die Kontrollinstanz hat hierfür Zugriff auf den Bestand des Informationssystems. Nationale Kontrollinstanz der Bundesrepublik Deutschland wird der Bundesbeauftragte für den Datenschutz sein.

Eingaben in das Informationssystem erfolgen ausschließlich über die nationalen Zentralstellen. Das Bundeskriminalamt als nationale deutsche ZentralsteÜe erlangt die notwendigen Informationen zu einem großen Teil von den Polizeibehörden der Länder. Damit werden auch ,,bayerische Daten" über das Bundeskriminalamt an EUROPOL übermittelt.

Notwendig ist daher eine datenschutzrechtliche Kontrolle der Übermittlung ,,bayerischer Daten" an die nationale Zentralstelle. Dazu müßte der bayerische Landesbestand in INPOL-Bund, soweit er an die Zentralstelle zur Weiterleitung an EUROPOL übermittelt wird, gekennzeichnet werden. Dadurch wäre mir eine gezielte Kontrolle der von Bayern für EUROPOL vorgesehenen Daten möglich. Das Innenministerium hat mir zugesichert, daß eine derartige Kennzeichnung des Datenbestandes vorgesehen ist.

Die Datenschutzbeauftragten haben in ihrem Beschluß zu EUROPOL darauf hingewiesen, daß sie von der deutschen Seite eine Klarstellung über die Verantwortung der Länder erwarten. Die Regelungen zur Verarbeitung müssen präzise sein und dem Grundsatz der Verhältnismäßigkeit entsprechen. Beispielsweise erfüllen die in den bisherigen Entwürfen vorgesehenen Befugnisse zur europaweiten Speicherung von Daten unbeteiligter Personen diese Voraussetzungen nicht.

5.15 Anfertigung von Bild- und Tonaufnahmen von Teilnehmern öffentlicher Versammlungen

Anläßlich des Landesparteitages einer Partei fand am Vortag eine Gegenveranstaltung in den Räumen statt, die am folgenden Tag für den Parteitag genutzt werden sollten. Im Zusammenhang mit dieser Veranstaltung lagen den Sicherheitsbehörden konkrete Erkenntnisse vor, wonach linksextremistische Gruppen (Mindestteilnehmerzahl: 100 Personen) mit allen Mitteln versuchen würden, den Parteitag zu verhindern. U.a. sei geplant gewesen, den Tagungsraum nach der Gegenveranstaltung nicht mehr zu verlassen, sondern zu besetzen und Sachbeschädigungen - z.B. durch Verbreiten von Buttersäure - zu begehen, um eine Nutzung für den Parteitag unmöglich zu machen. Von der Polizei wurde am Eingang des Veranstaltungsraumes ein Kameramann postiert, der Bild- und Tonaufnahmen von den im Saal befindlichen Versammlungsteilnehmern anfertigte, die - weil die befürchteten Störungen ausblieben - unmittelbar nach Beendigung des Einsatzes vernichtet wurden.

Ich habe das Innenministerium zur datenschutzrechtlichen Beurteilung der polizeilichen Datenerhebung auf folgendes hingewiesen:

Nach § 12 a Versammlungsgesetz darf die Polizei Bild- und Tonaufnahmen **von Teilnehmern** bei oder im Zusammenhang mit öffentlichen Versammlungen nur anfertigen, wenn **tatsächliche Anhaltspunkte** die Annahme rechtfertigen, daß von ihnen erhebliche Gefahren für die öffentliche Sicherheit oder Ordnung ausgehen.

Jede Datenerhebung nach § 12 a Versammlungsgesetz setzt somit eine gesicherte und auf die Betroffenen bezogene Gefahrenprognose voraus. Es müssen tatsächliche Anhaltspunkte dafür vorliegen, daß von den jeweils **von der Maßnahme betroffenen Personen** erhebliche Gefahren für die öffentliche Sicherheit ausgehen. Maßnahmen der Datenerhebung nach § 12 a Versammlungsgesetz **richten sich nicht gegen die Versammlung als solche, sondern nur gegen Störer.** Unbeteiligte (Nicht-Störer) dürfen nur erfaßt werden, wenn es tatsächlich bzw. technisch unvermeidbar ist.

Diese Einschränkung ist Ausfluß der durch das Grundgesetz gewährleisteten Versammlungs- und Demonstrationsfreiheit. Diese setzt voraus, daß die Versammlungsteilnehmer nicht befürchten müssen, wegen oder anläßlich der Wahrnehmung ihrer Grundrechte staatlicher Überwachung unterworfen und somit möglicherweise Adressaten von für sie nachteiligen Maßnahmen zu werden. Wer damit rechnet, daß die Teilnahme an einer Versammlung behördlich registriert wird und daß ihm dadurch Risiken entstehen können, wird möglicherweise auf eine Ausübung seines entsprechenden Grundrechts (Art. 8 GG) verzichten.

Im vorliegenden Fall lagen der Polizei Erkenntnisse vor, daß aus den Reihen der Teilnehmer erhebliche Gefahren für die öffentliche Sicherheit und Ordnung zu erwarten waren. Die ihr zugegangenen Hinweise ließen allerdings eine nähere Identifizierung der potentiellen Störer nicht zu. Bild- und Tonaufnahmen eines Teils oder aller Versammlungsteilnehmer aufgrund dieser Erkenntnisse waren deshalb unzulässig.

Das Innenministerium hat mir gegenüber dazu die Auffassung vertreten, daß bei Gefahrenerkenntnissen, die „nicht bestimmten Personen zugeordnet werden können, sondern nur einer zunächst nicht näher bestimmten Personengruppe, nämlich z.B. den gesamten Teilnehmern einer Versammlung", Bild- und Tonaufnahmen auch von der gesamten Gruppe gemacht werden können. „Bei dieser Fallgestaltung sind sämtliche Teilnehmer der Versammlung als Verantwortliche im Sinne des § 12 a Versammlungsgesetz anzusehen".

Diese Auffassung steht im Widerspruch zum Gesetzestext und den Kommentierungen. So führt z.B. der Kommentar von Dietel/Gintzel/Kniesel zu § 12 a Versammlungsgesetz folgendes aus: „Die Einfügung von § 12 a in das Versammlungsgesetz steht im politischen Zusammenhang mit der Einführung des strafbewehrten Verbots der Vermummung. Wenn die Polizei auf der Grundlage des § 12 a Abs. 1 Versammlungsgesetz Aufnahmen nur anfertigen können soll, wenn tatsächliche Anhaltspunkte die Annahme rechtfertigen, daß von den Teilnehmern erhebliche Gefahren für die öffentliche Sicherheit und Ordnung ausgehen, so sollte dem Einwand von Versammlungsteilnehmern begegnet werden, ihre Vermummung sei lediglich legitime Verteidigung gegen exzessive Überwachung von Demonstrationen und Versammlungen durch eine unbegrenzt videografierende und registrierende Polizei."

Im Bericht des seinerzeit für den damaligen Gesetzentwurf der Bundesregierung federführenden Rechtsausschusses ist als Begründung zu dem während der Ausschußverhandlungen eingefügten § 12 a Versammlungsgesetz ausgeführt, daß im Hinblick auf diese Normierung „für den friedlichen Demonstrationsteilnehmer keinerlei einsichtige Gründe (existierten), sich zu vermummen, um eine Feststellung seiner Identität zu verhindern".

Der Wille des Gesetzgebers war es damit zu gewährleisten, daß nur solche Versammlungsteilnehmer aufgenommen werden, für die konkrete Anhaltspunkte für unfriedliches Verhalten vorliegen. Umgekehrt folgt daraus, daß Versammlungsteilnehmer, für die solche tatsächlichen Anhaltspunkte nicht vorliegen, nicht aufgenommen werden sollen.

Dieser Wille des Gesetzgebers kommt im Wortlaut des Gesetzes nach meiner Auffassung eindeutig zum Ausdruck. Ich halte deshalb eine entsprechende Verfahrensweise der Polizei für geboten und bin in diesem Sinn an das Staatsministerium des Innern herangetreten.

In den folgenden Gesprächen mit dem Innenministerium konnte bisher eine Übereinstimmung in der grundlegenden Frage des Regelungsgehalts des § 12 a Versammlungsgesetz (Umfang der Eingriffsbefugnis) nicht erzielt werden. Das Innenministerium hat aber in einem Schreiben

zum konkreten Vorgang ergänzend insbesondere auf folgendes hingewiesen:

Aufgrund der konkreten Hinweise auf beabsichtigte massive Störungen sei bereits in der weiteren Umgebung des Tagungsraumes gezielte Aufklärung betrieben worden. Dabei seien ca. 30 Personen erkannt worden, die der linken, teilweise autonomen, gewaltbereiten Szene zugeordnet werden konnten. Diese Personen hätten sich nach Öffnung in den Versammlungsraum begeben und sich dort offensichtlich unter den ca. 500 anwesenden Versammlungsteilnehmern verteilt, weil sie - bis auf 2 Mitglieder der autonomen Szene - nicht mehr lokalisiert hätten werden können.

Im o.g. Schreiben hat das Innenministerium zu seinen Feststellungen zur Durchführung von Bild- und Tonaufzeichnungen, wonach diese nicht auf einen bestimmten Personenkreis beschränkt waren und mit dem Ziel durchgeführt wurden, mögliche Störer zu erkennen und die Einleitung evtl. Strafverfahren zu ermöglichen, weiter ausgeführt: Der Kameramann habe den Auftrag erhalten, dem Einsatzleiter zum Zwecke der Einsatzführung einen Überblick von der Versammlung und deren Verlauf durch Bildübertragung zu vermitteln und erkannte Störer im Versammlungsraum zu lokalisieren. Diesem Auftrag sei der Kameramann nachgekommen, wobei die Aufnahmen aus der Rückansicht der Versammlungsteilnehmer angefertigt worden seien.

Hierzu ist aus datenschutzrechtlicher Sicht folgendes festzuhalten:

Übersichtsaufnahmen, die zur Leitung des polizeilichen Einsatzes, zu Schulungszwecken oder zur Einsatzdokumentation benötigt und nicht mit dem Ziel hergestellt wurden, einzelne Teilnehmer einer Versammlung zu identifizieren, sind nach wohl überwiegender Auffassung nicht nur unter den engen Voraussetzungen des § 12 a Versammlungsgesetz zulässig. Solche Aufnahmen werden deshalb von mir nicht beanstandet. Sie sind gleichwohl aus datenschutzrechtlicher Sicht nicht unbedenklich, wenn ein Personenbezug hergestellt werden kann. Soweit neben den Übersichtsaufnahmen Bildaufnahmen **erkannter potentieller** Störer angefertigt wurden, ist dies durch § 12 a Versammlungsgesetz gedeckt. Andere Versamrnlungsteilnehmer dürfen von solchen Maßnahmen allerdings nur im Rahmen des § 12 a Abs. 1 Satz 2 Versammlungsgesetz betroffen werden. Darüber hinausgehende Eingriffe in ihre Grundrechte auf Versammlungsfreiheit und informationelle Selbstbestimmung durch Videografieren sind auf der Grundlage von § 12 a Versammlungsgesetz nicht zulässig.

Ich werde die Angelegenheit weiter verfolgen.

5.16 Bürgereingaben

Auch in diesem Berichtszeitraum wandten sich wieder Bürger an mich, die eine rechtswidrige Erhebung, Verarbeitung oder Nutzung ihrer personenbezogenen Daten durch die Polizei befürchteten. In den meisten Fällen erwiesen sich diese Befürchtungen als unbegründet. In Einzelfällen habe ich die Verkürzung von Speicherfristen, die Löschung bzw. Berichtigung von Daten und die Vernichtung polizeilicher Unterlagen durch die Polizei gefordert sowie die Weitergabe von Daten gerügt. Die beiden folgenden Vorgänge sind - über den Einzelfall hinaus - von allgemeiner Bedeutung:

1. Aufnahme in die Liste der Abschleppunternehmen

   Ein Petent beantragte die Aufnahme seines Gewerbebetriebes in die bei der Polizei geführte Liste von Abschleppunternehmen. Dies wurde mit der Begründung, er sei unzuverlässig, abgelehnt. Zur Beurteilung der Zuverlässigkeit hatte die Polizei die bei ihr zu dem Petenten im Kriminalaktennachweis gespeicherten Ermittlungsverfahren herangezogen. Dagegen hatte sich der Petent, insbesondere wegen der nach seiner Meinung fehlenden Speicherungsvoraussetzungen und unter Hinweis auf die Tilgungsvorschriften des Bundeszentralregistergesetzes gewandt.

   Meine Überprüfung ergab, daß die Entscheidung der Polizei nicht zu beanstanden war:

   Die Aufnahme in die Liste der Abschleppunternehmen setzt auch voraus, daß Bedenken gegen die Zuverlässigkeit des Bewerbers nicht bestehen. Der Bundesgerichtshof hat dazu u.a. ausgeführt:

   „Zwar darf die Polizei, wie das Berufungsgericht mit Recht ausführt, auch in derartigen Fällen nicht ohne weiteres einen Mitbewerber zugunsten eines anderen zurücksetzen. Wie der erkennende Senat aber bereits in dem vorerwähnten Urteil entschieden hat, stellt nur eine willkürliche Ausschließung eines Unternehmers von Abschleppaufträgen einen rechtswidrigen Eingriff in dessen Gewerbebetrieb dar. Die Polizei muß die Abschleppunternehmer, die sie Kraftfahrern benennt, sorgfältig auswählen. Sie darf nur einen geeigneten Unternehmer benennen und kann deshalb von der Berücksichtigung eines Bewerbers Abstand nehmen, wenn ihr bekannte Umstände zu Bedenken gegenüber seiner Zuverlässigkeit Anlaß geben, während ähnliche Bedenken bei einem Mitbewerber nicht ersichtlich sind. ... Es kann dem beklagten Land nicht zugemutet werden, um des Gleichheitsgrundsatzes willen Schadensersatzansprüche in Kauf zu nehmen.... Zwar mag nicht jeder gegen einen Abschleppunternehmer aufgekommene Verdacht, eine strafbare Handlung begangen zu haben, die Polizei berechtigten, ihn von der Liste der den Verkehrsteilnehmern zu benennenden bzw. zu empfehlenden Unternehmer zu streichen. Eine willkürliche Streichung liegt aber schon dann nicht vor, wenn ihr und damit der Nichtnennung ein nicht offensichtlich unbegründeter Verdacht zugrunde liegt.

   Nach dem Polizeiaufgabengesetz ist die Polizei befugt, personenbezogene Daten, die sie im Rahmen strafrechtlicher Ermittlungsverfahren oder von Personen gewonnen hat, die verdächtig sind, eine

Straftat begangen zu haben, zu speichern, zu verändern und zu nutzen, soweit es zur Gefahrenabwehr, insbesondere zur Vorbeugung und Bekämpfung von Straftaten erforderlich ist. Diese Voraussetzungen für die Speicherung der Ermittlungsverfahren, die der Beurteilung der Zuverlässigkeit des Petenten zugrundeliegen, waren erfüllt. Insbesondere war in keinem der Fälle der Tatverdacht entfallen.

Die Polizei kann die rechtmäßig gespeicherten personenbezogenen Daten nutzen, soweit dies u.a. zur Erfüllung ihrer Aufgaben erforderlich ist (vgl. Art. 38 Abs. 1 Polizeiaufgabengesetz). Die Polizei erfüllt mit der Empfehlung oder Vermittlung von Abschleppunternehmern an Fahrzeugführer zur Beseitigung betriebsunfähiger Kraftfahrzeuge oder zur Hilfeleistung bei Pannen und Unfällen auf Bundesautobahnen auch die ihr vom Polizeiaufgabengesetz zugewiesene Aufgabe der Gefahrenabwehr. Deshalb darf sie bei der Beurteilung der Zuverlässigkeit der Bewerber für die Aufnahme in das Verzeichnis privater Reparatur- und Abschleppbetriebe auf ihre eigenen zu diesem Zweck gespeicherten Erkenntnisse und Unterlagen zurückgreifen. Die Regelungen über die Tilgung von Speicherungen im Bundeszentralregister nach Fristablauf sowie das Verwertungsverbot nach dem Bundeszentralregistergesetz für Eintragungen über Verurteilungen, die im Register getilgt worden sind oder zu tilgen waren, haben wegen der unterschiedlichen Zweckbestimmung (Strafverfolgung/Gefahrenabwehr) keine Auswirkungen auf die Speicherung und Nutzung personenbezogener Erkenntnisse durch die Polizei.

Es war daher zulässig, die im Kriminalaktennachweis und in der Kriminalakte rechtmäßig gespeicherten Informationen über den Bewerber zur Beurteilung seiner Zuverlässigkeit heranzuziehen.

2. Datenerhebung und -speicherung zur polizeilichen Bekämpfung der Rauschgiftkriminalität

In den Sommermonaten wandten sich 3 Petenten an mich, die im Englischen Garten in München an verschiedenen Örtlichkeiten von der Polizei kontrolliert, namentlich erfaßt und zum Teil fotografiert worden waren.

Meine Überprüfung ergab, daß die Polizei in bestimmten Bereichen des Englischen Gartens Personenkontrollen durchführt, um die Entstehung einer offenen Drogenszene und die Begehung von Straftaten zu verhindern. In solche Personenkontrollen waren die Petenten geraten.

Die im einzelnen getroffenen datenschutzrechtlich relevanten polizeilichen Maßnahmen habe ich wie folgt beurteilt:

- Identitätsfeststellung

  Die Polizei kann die Identität einer Person u.a. feststellen, wenn die Person sich an einem Ort aufhält, von dem aufgrund **tatsächlicher Anhaltspunkte** anzunehmen ist, daß dort Personen Straftaten verabreden, vorbereiten oder verüben (Art. 13 Abs. 1 Nr.2 a) aa) PAG).

  Diese Voraussetzungen lagen vor, da sich die betreffenden Bereiche zu einem Treffpunkt von Drogenhändlern und Konsumenten entwickelt hatten un& sich die Petenten zum Zeitpunkt der polizeilichen Kontrolle dort auffiielten.

- **Durchsuchung**

  Die Polizei kann eine Person u.a. dann durchsuchen, wenn diese sich an einem sog. verrufenen Ort auffiält (Art 13 Abs. 1 Nr.2 in Verbindung mit Art. 21 Abs. 1 Nr.3 PAG).

  Auch diese Voraussetzung war erfüllt (vgl. Identitätsfeststellung).

- **Datenabgleich**

  Der Datenabgleich der erhobenen Personalien richtet sich nach Art. 43 Abs. 1 PAG. Danach kann die Polizei personenbezogene Daten mit dem Inhalt polizeilicher Dateien u.a. dann abgleichen, wenn **Tatsachen die Annahme rechtfertigen,** daß dies zur Erfüllung einer bestimmten polizeilichen Aufgabe erforderlich ist. Die Polizei kann ferner im Rahmen ihrer Aufgabenerfüllung erlangte personenbezogene Daten mit dem Fahndungsbestand abgleichen.

  Der Abgleich der personenbezogenen Daten der Petenten diente der Überprüfung der Person und der Feststellung, ob Erkenntnisse über diese vorlagen, somit der Gefahrenabwehr, die der Polizei als gesetzliche Aufgabe übertragen ist. Der Eingriff war daher rechtmäßig.

- **Erkennungsdienstliche Maßnahme (Anfertigen eines Lichtbildes)**

  Nach § 81 b Strafprozeßordnung (StPO) besteht für die Polizei die Möglichkeit, für die Zwecke der Durchführung eines Strafverfahrens oder für die Zwecke des Erkennungsdienstes Lichtbilder und Fingerabdrücke eines Beschuldigten aufzunehmen. Die Vornahme erkennungsdienstlicher Maßnahmen ist nach Art. 14 Abs. 1 PAG auch zulässig, wenn eine nach Art. 13 PAG zulässige Identitätsfeststellung auf andere Weise nicht oder nur unter erheblichen Schwierigkeiten möglich ist.

  Zur Rechtmäßigkeit der betreffenden erkennungsdienstlichen Maßnahme (Anfertigung eines Lichtbildes) war mir eine abschließende datenschutzrechtliche Beurteilung leider nicht möglich. Die zur Beurteilung notwendigen Unterlagen, einschließlich des Lichtbildes, waren von der Polizei bereits vernichtet worden, da keine polizeilichen Erkenntnisse zu den Petenten vorlagen.

Eine genaue Feststellung, auf welcher Rechtsgrundlage und mit welcher Begründung die Anfertigung des Lichtbildes erfolgte, konnte ich deshalb nicht treffen, so daß es mir an einer ausreichenden Entscheidungsgrundlage fehlte.

- **Speicherung und Löschung der personenbezogenen Daten**

  Die Polizei kann personenbezogene Daten in Akten oder Dateien speichern, verändern oder nutzen, soweit dies zur Erfüllung ihrer Aufgaben, zur zeitlich befristeten Dokumentation oder zur Vorgangsverwaltung erforderlich ist (Art. 38 Abs. 1 PAG).

  Zur Überprüfung der Petenten war daher eine Speicherung ihrer Daten in einem sog. Erfassungsbogen zulässig. Da zu den Petenten keine polizeilichen Erkenntnisse vorlagen, wurden, wie mir die Polizei mitgeteilt hat, die Speicherungen vernichtet.

  Die vorübergehende Speicherung eines der Petenten in einer Datei zur Rauschgiftbekämpfung (vgl. auch Ziffer. 5.3.3) halte ich dagegen **nicht für rechtmäßig,** da sie zur polizeilichen Aufgabenerfüllung und zu dem mit der Datei nach der Errichtungsanordnung verfolgten Zweck (Bekämpfung der Rauschgiftsucht) **nicht erforderlich** war. Die Speicherung in der Datei wurde gelöscht.

6. Verfassungsschutz

6.1 Vorbemerkungen

In Bayern wurde der Entwurf eines Gesetzes zur Änderung des Bayerischen Verfassungsschutzgesetzes vorgelegt, der die Einbeziehung des Verfassungsschutzes in die Beobachtung der organisierten Kriminalität und die Verbesserung seines Instrumentariums zur Beobachtung rechtsextremistischer Gruppierungen und Einzeltäter vorsieht. Maßgebend waren dafür folgende Überlegungen:

Die Bedrohung der inneren Sicherheit in Deutschland durch die organisierte Kriminalität hat im Berichtszeitraum erheblich zugenommen. Auch die politischen Veränderungen in den Ländern des früheren Ostblocks haben Auswirkurigen auf die internationale Entwicklung der organisierten Kriminalität gehabt. Die wirtschaftsgeographische Lage Bayerns als Schnittpunkt zum Süden wie zum Osten, begünstigt den Anstieg international verflochtener Kriminalität. Insbesondere sind eine erhöhte Rauschgiftzufuhr aus dem Nahen Osten und Aktivitäten krimineller Organisationen aus Italien und Staaten des früheren Ostblocks festzustellen. Vor diesem Hintergrund erschien es erforderlich, die Möglichkeiten und Erfahrungen aller Sicherheitsbehörden einschließlich des Landesamts für Verfassungsschutz zur präventiven Bekämpfung der ,,Organisierten Kriminalität" zu nutzen.

Dazu wurde dem Landesamt für Verfassungsschutz auch die Befugnis eingeräumt, unter engen Voraussetzungen (Vorliegen tatsächlicher Anhaltspunkte für den Verdacht der Verfolgung von Bestrebungen und Tätigkeiten der organisierten Kriminalität durch Planung oder Begehung bestimmter schwerer Straftaten) im Schutzbereich des Art. 13 des Grundgesetzes Informationen durch den Einsatz besonderer technischer Mittel zu gewinnen.

Die zunehmende Bedeutung des Rechtsextremismus, insbesondere des gewaltorientierten Neonazismus mit seinen ausländerfeindlichen Ausschreitungen, hat ebenfalls zu einer Überprüfung der Befugnisse des Verfassungsschutzes geführt. Es erschien notwendig, das rechtliche Instrumentarium des Landesamtes für Verfassungsschutz zur Vorfeldbeobachtung rechtsextremistischer Gruppierungen und Einzeltäter zu verbessern, vor allem durch Erweiterung der Befugnisse des Verfassungsschutzes zum Einsatz besonderer technischer Mittel im Schutzbereich des Art. 13 des Grundgesetzes (Wohnungen).

Das Änderungsgesetz ist am 01.08.1994 in Kraft getreten. Grundsätzliche Bedenken gegen diese Ausweitung der Aufgaben und Befugnisse des Landesamts für Verfassungsschutz habe ich nicht erhoben. Erforderlich ist jedoch eine ausreichende Datenschutzkontrolle durch unabhängige Kontrollorgane (im einzelnen dazu Ziff. 6.3).

6.2 Auswirkungen des neuen Datenschutzgesetzes auf die Datenschutzkontrolle des Landesamtes für Verfassungsschutz

Im *15.* Tätigkeitsbericht (Ziff. *5.2)* hat mein Vorgänger im Amt darauf hingewiesen, daß die Beschränkung der Kontrolle der in Akten verarbeiteten personenbezogenen Daten auf eine bloße Anlaßkontrolle (Art. 30 Abs. 1 Satz 2 BayDSG) eine Beeinträchtigung des Datenschutzes der Bürger gerade in dem besonders sensiblen Bereich verdeckter Informationsgewinnung durch den Einsatz nachrichtendienstlicher Mittel darstellt.

Ich habe seit meinem Amtsantritt diesem Bereich besondere Beachtung geschenkt, um hier zu einem fachlich begründeten und datenschutzrechtlich vertretbaren Ergebnis zu kommen. Aufgrund von Gesprächen mit dem Staatsministerium des Innern und dem Landesamt für Verfassungsschutz sowie meiner ersten Datenschutzkontrolle des Landesamtes für Verfassungsschutz bin ich der Auffassung, daß bei der Beurteilung der datenschutzrechtlichen Kontrollzuständigkeit zwischen den einzelnen Mitteln verdeckter Datenerhebung zu unterscheiden ist:

1. Maßnahmen nach dem Gesetz zur Beschränkung des Brief-, Post- und Fernmeldegeheimnisses (GbGesetz)

   Solche Maßnahmen dürfen unter den dort genannten Voraussetzungen grundsätzlich nur mit Zustimmung der G 10-Kommission des Bayerischen Landtags angeordnet werden. Die ,,Lücke" in der Datenschutz-

kontrolle wird deshalb durch die Zuständigkeit der G 10Kommission -jedenfalls für die Datenerhebung - ausgeglichen. Für die Datenverarbeitung und -nutzung, die eigenständige Rechtseingriffe darstellen, fehlt es an einer ausdrücklichen gesetzlichen Kontrollkompetenz der G l0-Kommission. Ich bin deshalb bisher davon ausgegangen, daß diese Bereiche zu meiner Kontrollzuständigkeit gehören, da Art. 30 Abs. 3 BayDSG die Kontrolle durch den Landesbeauftragten für den Datenschutz nur für personenbezogene Daten ausschließt, die der Kontrolle durch die G 10-Kommission unterliegen. Der Ausschluß der Kontrolle durch den Landesbeauftragten für den Datenschutz beruht auf der Erwägung, daß wegen der ohnehin durchgeführten Kontrolle durch die G 10-Kommission einen weitere Kontrolle durch den Landesbeauftragten für den Datenschutz nicht notwendig ist. Soweit die GlO-Kommission jedoch keine Kontrolle durchführt, ist Art. 30 Abs. 3 BayDSG verfassungskonform und damit so auszulegen, daß keine kontrollfreien Räume bei der Datenverarbeitung und -nutzung des Landesamtes für Verfassungsschutz bestehen.

Das Landesamt für Verfassungsschutz geht zwar wie ich von der **verfassungsrechtlichen Notwendigkeit einer unabhängigen Kontrolle** aus, sieht diese aber nicht nur für die Datenerhebung, sondern auch für die Datenverarbeitung und -nutzung durch die G 10-Kommission als gewährleistet an. Eine Kontrollzuständigkeit für den Landesbeauftragten für den Datenschutz würde danach im Bereich der G 10-Maßnahmen nicht bestehen.

Ich habe diese Frage im Interesse einer einvernehmlichen Lösung mit dem Vorsitzenden der G 10-Kommission in einem ersten Gespräch erörtert. Die dabei gefundenen Lösungsansätze, die von der grundsätzlichen Kontrollzuständigkeit der G 10-Kommission ausgehen, sollen in einem weiteren Gespräch vertieft werden.

2. Verdeckter Einsatz besonderer technischer Mittel zur Informationsgewinnung in Wohnungen

   Durch die Änderung des Art. 6 BayVSG ist die Möglichkeit der Datenerhebung in Wohnungen, insbesondere für den Bereich rechtsextremistischer Straftäter und der organisierten Kriminalität erweitert worden. Das Landesamt für Verfassungsschutz hat mir bei meiner Prüfung die hierzu erforderlichen Auskünfte gegeben. Wegen der Bezugnahme auf das G 10-Gesetz und das entsprechende Ausführungsgesetz in Art. 6 Abs. 2 Satz 3 BayVSG dürfte auch hier die Zuständigkeit für die Kontrolle der weiteren Verwendung der in Wohnungen erhobenen Daten bei der G 10-Kommission liegen.

3. Observation

   Observationen konnte ich mit Hilfe einer Kartei feststellen und stichprobenweise systematisch überprüfen. Dazu wurden mir die Akten zur Einsichtnahme vorgelegt.

Die beim LIV durchgeführte Datenschutzkontrolle hat mir aber gezeigt, daß **nicht alle Maßnahmen** verdeckter Datenerhebung in einer Datei gespeichert werden. In diesen Fällen steht eine als Ausgangspunkt für meine Prüfung geeignete Datei nicht zur Verfügung.

Damit auch hier die notwendige Prüfung - unabhängig von der Bereitschaft des LIV, mir die erforderlichen Informationen zugänglich zu machen - auf rechtlich sichere Grundlagen gestellt wird, halte ich jedenfalls insoweit eine Ausdehnung der Kontrollbefugnis des Datenschutzbeauftragten auf Akten unabhängig von Dateien für erforderlich.

6.3 Änderung des Bayerischen Verfassungsschutzgesetzes (BayVSG)

Am 01. August 1994 ist das Gesetz zur Änderung des Bayerischen Verfassungsschutzgesetzes in Kraft getreten. Art. 1 Abs. 1 Satz 2 des Gesetzes weist dem Landesamt für Verfassungsschutz (Lfv) neben seiner traditionellen Aufgabe des Schutzes der freiheitlichen demokratischen Grundordnung, des Bestandes und der Sicherheit des Bundes oder eines Landes (Art. 73 Nr.10 Grundgesetz) die für das Amt **neue Aufgabe** zu, **Bestrebungen und Tätigkeiten** der Organisierten Kriminalität (OK) zu beobachten. Damit sollen die Erfahrungen des Verfassungsschutzes, die dieser bei der Beobachtung des Terrorismus und der Spionagebedrohung gewonnen hat, und seine Möglichkeiten in der Zusammenarbeit mit Diensten anderer Länder auch für diesen Bereich genutzt werden (insbesondere **Erkennen von Strukturen im Vorfeld** strafbaren Handelns).

Hierfür wurde das LIV zum verdeckten Einsatz besonderer technischer Mittel im Schutzbereich des Art. 13 GG (,,großer Lauschangriff") berechtigt (Art. 6 Abs. 4 BayVSG neu). Darüber hinaus wurde das rechtliche Instrumentarium zur Beobachtung des Extremismus, insbesondere des Neonazismus erweitert

- durch die Möglichkeit des Einsatzes besonderer technischer Mittel im Schutzbereich des Art. 13 des Grundgesetzes bei Vorliegen tatsächlicher Anhaltspunkte für den Verdacht, daß jemand verfassungsfeindliche Bestrebungen durch die Planung oder Begehung von Straftaten nach den § 129 (Bildung krimineller Vereinigungen), 130 (Volksverhetzung) oder 131 (Aufstachelung zum Rassenhaß) des Strafgesetzbuchs (StGB) verfolgt und
- durch die Herabsetzung der Altersgrenze für die Speicherung personenbezogener Daten über das Verhalten einer Person in Dateien von 16 Jahren auf 14 Jahre.

Sowohl mein Vorgänger im Amt, Herr Sebastian Oberhauser, als auch ich haben im Rahmen der Beratungen dieses Gesetzes mehrfach Stellung genommen:

Grundsätzliche datenschutzrechtliche Bedenken gegen den Auftrag des Landesamtes für Verfassungsschutz, Bestrebungen und Tätigkeiten der Örganisierten Kriminalität zu beobachten, haben wir beide nicht erhoben. Die Erweiterung der Datenerhebungs- und Verarbeitungsbefugnis des Landesamtes für Verfassungsschutz auf das Gebiet der Vorfeldbeobachtung der OK kann wegen der dem Gesetz zugrunde gelegten Gefährdungsannahme, an der zu zweifeln für mich kein Anlaß besteht, im überwiegenden Interesse der Allgemeinheit als gerechtfertigt angesehen werden. Aus meiner Sicht kann dabei die strittige Frage des Bestehens oder Nichtbestehens eines verfassungsrechtlichen Trennungsgebotes zwischen Polizei und Verfassungsschutz dahingestellt bleiben. Es wäre jedenfalls durch die neue Aufgabenzuweisung nicht verletzt: Beide Institutionen bleiben organisatorisch getrennt, vor allem aber erhält das Landesamt für Verfassungsschutz keine polizeilichen Exekutivbefugnisse.

Auch die informationelle Trennung zwischen Polizei und Verfassungsschutz bleibt gewahrt: Die Übermittlungsregelungen der Art. 12- 17 BayVSG bleiben unverändert. Im Hinblick auf die erweiterten Aufgaben des Verfassungsschutzes wird die Menge der zu übermittelnden Informationen zwar ansteigen, ein Informationsverbund zwischen Polizei und Verfassungsschutz folgt daraus aber nicht, da die Informationsübermittlung jeweils aufgabenbezogen sein muß, diese Aufgaben aber auch in Bezug auf die Bekämpfung der OK nach wie vor unterschiedlich sind. Dem LIV obliegt die Vorfeldbeobachtung von Bestrebungen und Tätigkeiten der OK, der Polizei die Prävention und Strafverfolgung. Auch wenn im Hinblick auf die Gefahrenvorsorge als Bestandteil des polizeilichen Gefahrenabwehrauftrags Überlappungen und Parallelitäten der beiden Aufgabenbereiche nicht ausgeschlossen sind, bleibt es doch bei der grundsätzlich unterschiedlichen Aufgabenstellung.

Die Trennung zwischen Polizei und Verfassungsschutz wird deshalb durch den Entwurf nicht in Frage gestellt.

Die verfassungsrechtlichen Bedenken meines Vorgängers und auch meine richteten sich vielmehr dagegen, daß der seinerzeitige Gesetzentwurf **keine ausdrückliche Regelung der Zielpersonen** des verdeckten Einsatzes besonderer technischer Mittel zur Informationsgewinnung im Schutzbereich des Art. 13 des Grundgesetzes enthielt und der **Katalog der** Straftaten, dessen Planung oder Begehung in der Form der organisierten Kriminalität die elektronische Überwachung von Wohnungen rechtfertigen sollte, nicht abgeschlossen, sondern durch das Wort ,,insbesondere" offen war. Beide **Problempunkte** sind **nunmehr bereinigt:** Die Zielrichtung der technischen Überwachungsmaßnahmen ist nunmehr genau umschrieben. Sie darf sich nur gegen den Verdächtigen, Informationsübermittler oder Aufenthaltsgeber richten. Die Regelung entspricht derjenigen des G10Gesetzes und der Strafprozeßordnung für Telefonüberwachungsmaßnahmen. Der Straftatenkatalog ist nunmehr durch Streichung des Wortes ,,insbesondere" und die abschließende Aufzählung der Straftatbestände in sich abgeschlossen.

Gegen die Ausweitung derEingriffsbefugnis des Einsatzes technischer Mittel in Wohnungen auf die Straftatbestände der §§ 129, 130 und 131 StGB habe ich keine datenschutzrechtlichen Bedenken. Im rechtsextremistischen Bereich war eine Welle ausländerfeindlicher Gewalt zu verzeichnen. Die neue Dimension der Bedrohung der inneren Sicherheit durch rechtsextremistische Gewalttäter bedeutet eine ernstzunehmende Gefährdung der freiheitlichen demokratischen Grundordnung und schadet auswärtigen Belangen der Bundesrepublik Deutschland. Die verstärkte Vorfeldbeobachtung solcher extremistischen (gewaltbereiten) Bestrebungen in den Bereich neonazistischer Propaganda hinein halte ich deshalb für sachgerecht.

Auch gegen die Herabsetzung der Altersgrenze für die Speicherung personenbezogener Daten in Dateien bestehen keine datenschutzrechtlichen Bedenken, da sich gezeigt hat, daß die Anhänger politisch extremistischer Bestrebungen, insbesondere des Neonazismus in immer jüngerem Alter ,und mit hoher und massiver Gewaltbereitschaft und -fähigkeit auftreten und deshalb die bisherige Altersgrenze von 16 Jahren die Erfüllung des Auftrages des Verfassungsschutzes behindert.

Sowohl mein Vorgänger im Amt als auch ich haben aber darauf hingewiesen, daß nach den Grundsätzen des Bundesverfassungsgerichts auch **eine ausreichende Kontrolle der Verarbeitung und Nutzung der Daten mögich sein muß,** die durch die in das Grundrecht auf Unverletzlichkeit der Wohnung eingreifenden Maßnahmen gewonnen wurden.

Der tiefe Grundrechtseingriff, der mit Abhörmaßnahmen in Wohnungen verbunden ist, ist mit der Abhörmaßnahme als solcher nicht abgeschlossen. Er setzt sich durch die Verarbeitung und Nutzung der dadurch gewonnenen Daten fort. Angesichts der Tatsache, daß der Betroffene davon - jedenfalls zunächst - nichts erfährt und sich deshalb auch nicht gerichtlich wehren kann, ist auch dieser weitere Gruüdrechtseingriff verfassungsrechtlich nur dann hinnehmbar, wenn die Kontrolle durch ein unabhängiges Kontrollorgan sichergestellt ist.

Unbestritten ist die Zuständigkeit der G1O-Kommission für die Kontrolle der **Datenerhebung** in Wohnungen. Wegen der Speicherung und Nutzung der durch diese Maßnahme gewonnenen personenbezogenen Daten bin ich mit dem Vorsitzenden der G 1O-Kommission im Gespräch (vgl. dazu Ziff. 6.2).

6.4 Generelle Prüfung 1994

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

Prüfungsschwerpunkte waren insbesondere

- Speicherungen im Nachrichtendienstlichen Informationssystem NADIS der Verfassungsschutzbehörden,

- Speicherungen aufgrund von Sicherheitsüberprüfungen,
- Datenerhebung mit nachrichtendienstlichen Mitteln.

Wesentliche Verstöße gegen datenschutzrechtliche Bestimmungen habe ich dabei nicht festgestellt.

6.4.1 NADIS

Mit Inkrafttreten der Änderung des Bayer. Verfassungsschutzgesetzes vom 8.7.1994 darf das Landesamt für Verfassungsschutz auch Jugendliche zwischen 14 und 16 Jahren (bisher erst ab 16 Jahren) in Dateien speichern. Dies halte ich wegen der Tatsache, daß die Anhänger politisch extremistischer Bestrebungen, insbesondere des Neonazismus, in immer jüngerem Alter auftreten, für gerechtfertigt. Die Herabsetzung der Altersgrenze erfordert aber auf der anderen Seite eine besondere Sorgfalt bei der Beurteilung der Speicherungsvoraussetzungen, die der Entwicklungssituation des Jugendlichen Rechnung trägt. Ich habe deshalb bei meiner systematischen Kontrolle von NADIS insbesondere Speicherungen von

- Jugendlichen zwischen 14 und 16 Jahren und
- Jugendlichen zwischen 16 und 18 Jahren

einer gründlichen Prüfung unterzogen. Dabei ging es mir vor allem darum festzustellen, ob ausreichende Erkenntnisse (Art. 7 Abs. 1 BayVSG) für die Speicherungen getroffen und hinreichend dokumentiert waren und ob die Speicherungs- und Überprüfungsfristen eingehalten werden.

Die Prüfung gab keinen Anlaß für eine datenschutzrechtliche Beanstandung.

6.4.2 Sicherheitsüberpräfung

Personen, die eine sicherheitsempfindliche Tätigkeit - insbesondere im öffentlichen Bereich - ausüben sollen, sind vorher einer Sicherheitsüberprüfung zu unterziehen. Für die Sicherheitsüberprüfung fehlt es in Bayern bisher noch an einer bereichspezifischen gesetzlichen Grundlage, wie dem Sicherheitsüberprüfungsgesetz des Bundes. Ihre Durchführung richtet sich nach den Richtlinien für die Sicherheitsüberprüfung im Rahmen des Geheimschutzes. Nach Art. 3 Abs. 2 Nr.1 BayVSG hat das Landesamt für Verfassungsschutz die Aufgabe, an der Sicherheitsüberprüfung von Personen, denen im öffentlichen Interesse geheimhaltungsbedürftige Tatsachen, Gegenstände oder Erkenntnisse anvertraut werden, die Zugang dazu erhalten sollen oder ihn sich verschaffen können, mitzuwirken. Das Landesamt führt im Rahmen der Mitwirkung Sicherheitsüberprüfungsakten, die in einer automatisierten Datei nachgewiesen sind.

Ich habe deshalb auch diesen Bereich stichprobenartig kontrolliert und dabei insbesondere

- den Umfang der Datenerhebung und Datenspeicherung sowie
- die Beachtung der Zweckbindung

zum Prüfungsgegenstand gemacht.

Einen Verstoß gegen datenschutzrechtliche Bestimmungen habe ich dabei nicht festgestellt.

6.4.3 Datenerhebung mit nachrichtendienstlichen Mitteln

In diesem Bereich stand mir als Ausgangspunkt für meine Prüfung eine Kartei über Observationen und Ermittlungen zur Verfügung. Die dort erfaßten Maßnahmen habe ich stichprobenweise überprüft. Neben der Kontrolle der Datenerhebung habe ich besonderes Gewicht auf die Kontrolle der Speicherung der durch die Maßnahmen gewonnenen personenbezogenen Daten gelegt.

Zu einzelnen Speicherungen habe ich das LIV um Stellungnahme gebeten. Ihre Auswertung ist noch nicht abgeschlossen.

6.4.4 Beobachtung der organisierten Kriminalität (OK) durch das Landesamt für Verfassungsschutz

Mit der Änderung des Bayer. Verfassungsschutzgesetzes (Art. 3 Abs. 1 Nr.4) wurde dem Landesamt für Verfassungsschutz die Aufgabe der **Beobachtung von Bestrebungen und Tätigkeiten der OK** neu zugewiesen. Das Landesamt darf auch zur Erfüllung dieser Aufgabe unter den Voraussetzungen des Art. 7 BayVSG personenbezogene Daten in Dateien speichern und verändern. Das gilt auch für die Speicherung in automatisierten Dateien. Das Landesamt hat aber für den **erstmaligen Einsatz einer automatisierten Datei,** in der personenbezogene Daten verarbeitet werden, in einer **Errichtungsanordnung**, die der Zustimmung des Staatsministeriums des Innern bedarf, u.a. den **Zweck der Datei,** den **betroffenen Personenkreis** und die **Speicherungsdauer festzulegen** (Art. 9 Abs. 1 Satz 1 BayVSG). Sollen in eine für die Erfüllung der bisherigen Aufgaben des Landesamtes bestimmten Datei personenbezogene Informationen über die organisierte Kriminalität gespeichert werden, so bedarf es zunächst einer entsprechenden Änderung der Errichtungsanordnung (Art. 9 Abs. 1 Satz 3 BayVSG).

Anläßlich meiner diesjährigen Prüfung beim Landesamt, bei der ich mich auch über die datenschutzrechtlich relevanten Aspekte der Arbeit des Landesamtes in diesem Bereich informiert habe, habe ich die unverzügliche Erfüllung dieser Voraussetzungen gefordert.

Nach Mitteilung des Staatsministeriums des Innern wurde die ergänzende Errichtungsanordnung Ende November genehmigt.

6.5 Auskunftserteilung durch das Landesamt für Verfassungsschutz

Wie ich bereits in meinem 15. Tätigkeitsbericht (vgl. Ziff. 5.3.2) ausgeführt habe, haben die Bürger keinen Anspruch auf Auskunft über die beim Landesamt für Verfassungsschutz (LIV) in Dateien oder Akten gespeicherten Informationen. Hat aber eine Person ein besonderes Interesse an der Auskunft über die zu ihrer Person

gespeicherten Daten, so entscheidet das LIV nach pflichtgemäßem Ermessen über das Auskunftsbegehren (Art. 11 Abs. 1 BayVSG). Hierauf haben die Bürger einen Rechtsanspruch.

Diese Einschränkung der Auskunftserteilung berücksichtigt die besondere Aufgabenstellung des LIV und die grundsätzliche Geheimhaltungsbedürftigkeit von Erkenntnissen des Verfassungsschutzes. Andererseits habe ich darauf hingewiesen, daß an das ,,besondere Interesse" keine zu hohen Anforderungen gestellt werden dürfen. Ausreichend für die Annahme eines ,,besonderen Interesses ist es, wenn der Betroffene über das bei jedem Bürger gleichermaßen vorhandene Interesse an der Speicherung seiner personenbezogenen Daten hinaus ein Interesse darlegt, das eine zusätzliche Bedeutung der Auskunftserteilung für ihn erkennen läßt.

Bei der Prüfung von Entscheidungen des LIV über Anträge auf Auskunftserteilung habe ich einen Fall festgestellt, der zu datenschutzrechtlichen Bedenken Anlaß gibt:

Zwei Funktionäre einer Partei, die derzeit daraufhin überprüft wird, ob sie verfassungsfeindliche Bestrebungen verfolgt, beantragten Auskunft über die zu ihrer Person beim LIV gespeicherten personenbezogenen Daten. Das LIV teilte ihnen mit, daß sie ein besonderes Interesse an der Auskunftserteilung nicht dargetan hätten. Insbesondere sei die Funktionsträgerschaft in dieser Partei allein dafür noch nicht ausreichend. Es müsse eine darüber hinausgehende individuelle Belastung bestehen.

Diese enge Auslegung des Begriffes des ,,besonderen Interesses" kann ich aus datenschutzrechtlicher Sicht nicht teilen. In den vorliegenden Fällen müssen die Betroffenen als Funktionäre einer Partei, die bekanntermaßen überprüft wird, damit rechnen, daß über sie Daten gespeichert sind und diese Speicherungen sich für sie nachteilig auswirken. Diese nicht unbegründete Befürchtung schafft bei dem Betroffenen ein Auskunftsinteresse, das über das ,,normale" Interesse des Bürgers weit hinausgeht. Berufliche oder sonst vergleichbare Nachteile aufzuzeigen, ist nicht Aufgabe des Auskunftsbegehrenden. Es genügt meines Erachtens, wenn damit gerechnet werden muß, daß personenbezogene Speicherungen erfolgen, die Konsequenzen für den Betroffenen haben können.

So reichen für die Annahme eines ,,besonderen Interesses" nach der bisherigen Praxis des LIV z.B. auch Darlegungen des Antragstellers,

- von Mitarbeitern des LIV angesprochen worden zu sein oder
- eine Observierung/sonstige nachrichtendienstliche Tätigkeit gegen seine Person festgestellt zu haben.

Die Eigenschaft als Teil einer beobachteten Bestrebung sei dagegen nicht ausreichend. Der Ausforschung würde Tür und Tor geöffnet, wenn der, der weiß, daß er und seine Organisation beobachtet werden, gerade aus dieser Beobachtung ein besonderes Interesse herleiten könnte, Auskunft hierüber zu erhalten. Es müsse eine darüber hinausgehende individuelle Belastung geltend gemacht werden, z.B. wenn ein solcher Funktionär darlegt, bei einem konkreten Ereignis (z.B. Info-Stand) fotografiert worden zu sein.

Abgesehen davon, daß die gesetzliche Regelung für diese differenzierten, eng gefaßten Auslegungen m.E. keinen Raum läßt, kann ich auch nicht erkennen, warum erst die Feststellung, tatsächlich beobachtet zu werden, ein ,,besonderes Interesse" begründen soll. Bei nicht nur nachgeordneten Funktionären eines Beobachtungsobjektes kann auch ohne konkrete Darlegung angenommen werden, daß diese Personen, die die Bestrebung verkörpern, ebenfalls der Beobachtung unterliegen.

Geheimhaltungsinteressen des Landesamtes für Verfassungsschutz können im Rahmen der Entscheidung über den Auskunftsantrag nach pflichtgemäßem Ermessen berücksichtigt werden. Darüber hinaus ist die Auskunft zu versagen, wenn einer der in Art. 11 Abs. 3 BayVSG genannten Gründe (z.B. Geheimhaltungsinteresse) vorliegen. Damit ist ein ausreichender Schutz der Aufgabenerfüllung des LIV gewährleistet.

Ich habe mich mit dem Staatsministerium des Innern bisher in dieser Frage nicht einigen können. Es besteht weiterer Erörterungsbedarf.

7. Justiz

7.1 Regelungsdefizite im Bereich der Justiz

Auch 11 Jahre nach dem Volkszählungsurteil des Bundesverfassungsgerichts vom *15.* Dezember 1983 werden - insbesondere im Bereich der Strafrechtspflege - nach wie vor sensible personenbezogene Daten ohne die vom Bundesverfassungsgericht geforderten bereichsspezifischen gesetzlichen Grundlagen erhoben und verarbeitet. Zwar sind im Bereich der Zivilrechtspflege durch das Gesetz zur Änderung von Vorschriften über das Schuldnerverzeichnis vom 15. Juli 1994 gesetzliche Grundlagen für die Speicherung im und Auskünfte aus dem Schuldnerverzeichnis geschaffen worden, die datenschutzrechtliche Forderungen berücksichtigen.

Gravierende Lücken aus der Sicht des Datenschutzes bestehen jedoch weiterhin insbesondere in folgenden Bereichen:

- Datenverarbeitung im Strafverfahren, insbesondere in automatisierten Dateien,
- Datenerhebung, -verarbeitung und -nutzung im Strafvollzug,
- Datenübermittlung von Amts wegen durch Gerichte und Staatsanwaltschaften an Gerichte, Behörden und sonstige öffentliche Stellen (Justizmitteilungsgesetz) und die
- Aufbewahrung von Akten, Karteien, Büchern und die Dauer der Speicherung in automatisierten Dateien.

So ist beispielsweise offen, ob und ggf. mit welchem Inhalt Entwürfe zum Strafverfahrensänderungsgesetz und zum Justizmitteilungsgesetz in Kraft treten.

Die Datenschutzbeauftragten des Bundes und der Länder haben deshalb mit meiner Stimme in ihrem Beschluß vom 26./27.09. 1994 den Gesetzgeber angesichts der mit der Datenerhebung, -verarbeitung und -nutzung verbundenen Rechtseingriffe aufgefordert, zum Schutz des Rechts des Einzelnen auf informationelle Selbstbestimmung unverzüglich bereichsspezifische Regelungen der materiellen Voraussetzungen sowie die organisatorischen und verfahrensrechtlichen Vorkehrungen zu schaffen, die der Gefahr einer Verletzung des Persönlichkeitsrechts des Bürgers entgegenwirken.

7.2 Gesetzgebungsverfahren

7.2.1 Entwurf eines Strafverfahrensänderungsgesetzes 1994

Nachdem der Regierungsentwurf eines Strafverfahrensänderungsgesetzes 1989 nur in Teilbereichen Gesetzeskraft erlangt hat (siehe dazu *15.* Tätigkeitsbericht Ziff. 6.2.3) haben die Länder Bayern, Hessen, Nordrhein-Westfalen, Rheinland-Pfalz, Saarland und Thüringen den Entwurf eines Strafverfahrensänderungsgesetzes 1994 (StVÄG 1994) im Bundesrat eingebracht.

Mit dem Entwurf sollen bereichsspezifische Regelungen über die Verwendung von personenbezogenen Informationen, die im Strafverfahren erhoben worden sind und über die Verarbeitung personenbezogener Informationen in Dateien geschaffen werden. Dabei soll die Gewährleistung des Rechts auf informationelle Selbstbestimmung mit den Erfordernissen einer funktionstüchtigen Strafrechtspflege in Einklang gebracht werden. Schwerpunkte sind dabei Regelungen über Akteneinsicht und Dateien in der Strafrechtspflege.

Ich habe zum Gesetzesentwurf gegenüber dem Justizministerium Stellung genommen und insbesondere folgende Forderungen erhoben:

1. § 475 Abs. 1 StPO des Entwurfs sieht vor, daß Privatpersonen Auskünfte aus Akten bzw. Einsicht in die Akten bereits dann erhalten, wenn sie hierfür ein **berechtigtes** Interesse darlegen. Meiner Auffassung nach sollte Privatpersonen Einsicht in Strafakten nur dann gewährt werden, wenn sie ein **rechtliches** Interesse glaubhaft machen können. Die Gewährung von Akteneinsicht bereits beim Vorliegen eines berechtigten Interesses erscheint mir im Hinblick auf das durch das Grundgesetz geschützte Recht auf informationelle Selbstbestimmung zu weitgehend. Dies gilt insbesondere mit Rücksicht auf die Sensibilität der in Strafakten erfaßten personenbezogenen Daten, die zum Teil nicht freiwillig gegeben, sondern mit staatlichen Eingriffsmaßnahmen wie z.B. Durchsuchungen, Observationen oder Telefonüberwachungen erhoben werden.

   Unter den Begriff des „berechtigten Interesses" fällt herkömmlicherweise jedes vernünftigerweise gerechtfertigte Interesse auch nur tatsächlicher, wirtschaftlicher oder wissenschaftlicher Art, das sich nicht auf subjektive Rechte zu gründen oder auf das Verfahren zu beziehen braucht. Dadurch wird einer Vielzahl von nicht am Verfahren beteiligten Personen der Zugriff auf personenbezogene Informationen ermöglicht, die in Strafakten gespeichert sind. Durch die Anknüpfung der Akteneinsicht an das Vorliegen eines **rechtlichen** Interesses wird die Möglichkeit eines Zugriffs sachgerecht auf diejenigen begrenzt, deren Rechtskreis durch die personenbezogenen Informationen unmittelbar berührt ist, wie dies z.B. bei der Verfolgung von Schadensersatzansprüchen, Amtshaftungsansprüchen o.ä. der Fall ist.

2. Nach § 477 Abs. 3 StPO des Entwurfs wird nunmehr zwar eine **Zweckbindung** für die durch die Akteneinsicht erlangten personenbezogenen Informationen festgelegt. Dies halte ich jedoch nicht für ausreichend. Es bedarf darüber hinaus einer Strafbe**wehrung dieser Zweckbindungsregelung,** um einer mißbräuchlichen Verwendung wirksam vorzubeugen. Wie Bürgereingaben belegen, ist der Betroffene bisher weitgehend schutzlos gestellt, wenn die durch Akteneinsicht erlangten personenbezogenen Daten durch den Einsichtnehmenden zweckwidrig verwendet werden. Dies kann schwerwiegende Persönlichkeitsverletzungen zur Folge haben. Diese Problematik stellt sich nicht nur bei Informationen aus Strafverfahren, sondern auch bei Informationen aus anderen gerichtlichen oder behördlichen Verfahren, beispielsweise, wenn im Rahmen von Konkurrentenklagen oder Genehmigungsverfahren Akteneinsicht gewährt wird oder personenbezogene Auskünfte erteilt werden.

   Im Interesse eines ausreichenden präventiven Schutzes vor Mißbrauch habe ich deshalb vorgeschlagen, § 353 d des Strafgesetzbuchs (StGB) durch folgenden Straftatbestand zu ergänzen:

   „entgegen einer gesetzlichen Zweckbindungsregelung personenbezogene Daten, die ihm aus Akten oder Dateien des Gerichts, der Staatsanwaltschaft oder anderer Behörden zur Kenntnis gelangt sind, verwendet."

3. § 485 Abs. 2 StPO des Entwurfs trifft hinsichtlich der **Löschung** gespeicherter Daten eine meines Erachtens **unzureichende** Regelung. Vorgeschrieben ist die Datenlöschung zum einen in den Fällen, in denen die Speicherung unzulässig ist, zum anderen, wenn die Kenntnis der Daten zur Aufgabenerfüllung nicht mehr erforderlich ist.

   Ob Daten im Sinne der zweiten Alternative zu löschen sind, darf nicht der Erkenntnis aus Anlaß einer zufälligen Einzelfallbearbeitung überlassen bleiben. Vielmehr halte ich es für geboten, daß der Gesetzgeber

selbst regelt - wie das z.B. auch in Art. 45 Abs. 2 des Bayerischen Polizeiaufgabengesetzes geschehen ist -, daß innerhalb bestimmter Fristen, die im einzelnen untergesetzlich bestimmt werden können, allgemein geprüft wird, ob nicht die Voraussetzungen für die Datenlöschung bereits erfüllt sind.

In einer gemeinsamen Presseerklärung vom 13.10.1994 haben die Datenschutzbeauftragten des Bundes und von 13 Ländern das StVÄG 1994 als ,,unverhältnismäßige Ermächtigung zu Eingriffen in das Persönlichkeitsrecht" kritisiertunddieLandesregierungenaufgefordert,demGesetzesantrag im Bundesrat nicht zuzustimmen. Zur Begründung wurde im wesentlichen u.a. vorgebracht, der Gesetzentwurf verfehle seinen Anspruch, dem Volkszählungsurteil des Bundesverfassungsgerichts Rechnung zu tragen.

Zusammen mit den Landesbeauftragten für den Datenschutz von Sachsen und Thüringen habe ich mich in einer gemeinsamen Presseerklärung gegen eine Ablehnung des Einbringens des Entwurfs gewandt. Ich halte es für begrüßenswert, wenn durch einen Einbringungsbeschluß des Bundesrats das **Gesetzgebungsverfahren** für die dringend erforderlichen bereichsspezifischen Regelungen im Strafverfahren **endlich in Gang kommt.** Dadurch werden noch keine vollendeten Tatsachen geschaffen. Im weiteren Gesetzgebungsverfahren im Deutschen Bundestag müssen die notwendigen datenschutzrechtlichen Verbesserungen in das Gesetz aufgenommen werden.

Auch im Bereich der Justiz ist es an der Zeit, bereichsspezifische und normenklare Regelungen zum Umgang mit Daten von Beschuldigten, Zeugen und Unbeteiligten so zu fassen, wie das Bundesverfassungsgericht dies schon vor 11 Jahren gefordert hat.

7.2.2 Länderübergreifendes staatsanwaltschaftliches Verfahrensregister

Mit dem Verbrechensbekämpfungsgesetz, das zum 01.12.1994 in Kraft getreten ist, wurden in einem 8. Buch der Strafprozeßordnung (§ 474 ff. StPO) die gesetzlichen Grundlagen für ein zentrales staatsanwaltschaftliches Verfahrensregister, das beim BunJeszentralregister geführt wird (sog. Bundes-SISY), geschaffen.

Das Bundes-SISY dient der Speicherung aller im Bundesgebiet anhängigen Ermittlungs- und Strafverfahren. Zweck des Registers ist es, Strafverfolgungsbehörden insbesondere zu ermöglichen, mehrere gegen eine bestimmte Person anhängige Ermittlungsverfahren zusammenzuführen. Die Staatsanwaltschaften erhalten die erforderlichen Informationen, um parallele Ermittlungen bezüglich des gleichen Sachverhalts, die Durchführung mehrerer Hauptverhandlungen nebeneinander und die Notwendigkeit einer nachträglichen Zusammenführung von Einzelstrafen zu einer Gesamtstrafe zu vermeiden. Darüber hinaus erhalten die Staatsanwaltschaften die erforderlichen Informationen, um über die Frage der Verfahrenseinstellung (beispielsweise gemäß §§ 153, 153 a, 154 StPO) sachgerecht entscheiden zu können.

Die gesetzliche Regelung des Bundes-SISY ist auf die wesentlichen Aussagen zu Zweck und Funktion des Registers beschränkt. Die Festlegungen im einzelnen, z.B. zum betroffenen Personenkreis, zu den Arten der zu verarbeitenden Daten und der Datenübermittlung sollen in einer vom Bundesministerium der Justiz mit Zustimmung des Bundesrates zu erlassenden Errichtungsanordnung getroffen werden. Der Entwurf für eine solche Errichtungsanordnung liegt mir bereits vor. Ich habe gegenüber dem Bayerischen Staatsministerium der Justiz auf einzelne Kritikpunkte hingewiesen:

So ist vorgesehen, daß neben den Personendaten stets auch andere auf die Person beziehbare Merkmale wie ,,besondere körperliche Merkmale, unveränderliche Kennzeichen (Muttermale, Narben, Tätowierungen pp.) oder auch z.B. der Beruf in das Bundes-SISY aufgenommen werden können. Dies findet im Gesetz keine hinreichende Stütze. Gemäß § 474 Abs. 2 Nr.1 StPO dürfen neben den Personendaten des Beschuldigten andere zur Identifizierung geeignete Merkmale nur soweit **erforderlich** aufgenommen werden. Eine entsprechende Einschränkung ist auch in die Errichtungsanordnung aufzunehmen.

Ergänzungsbedürftig erscheint mir die Errichtungsanordnung aber insbesondere bezüglich der nach § 9 des Bundesdatenschutzgesetzes erforderlichen technischen und organisatorischen Maßnahmen. Diese sind in der Errichtungsanordnung konkret zu beschreiben (§ 476 Abs. 5 Ziff. 5 StPO). Dies gilt etwa für Maßnahmen zum Zugangsschutz (durch Identifikations- und Authentisierungsmaßnahmen), zur Datenintegrität insbesondere auf dem Übermittlungsweg (Verschlüsselung des Datensatzes) und zur Protokollierung (Absende- und Empfangsnachweis). Erst wenn eine solche Ergänzung in technischer und organisatorischer Hinsicht erfolgt ist, kann beurteilt werden, ob ausreichende Vorkehrungen zur Datensicherheit getroffen wurden.

Klärungsbedürftig erscheint mir auch, in welchem Umfang Datenübermittlungen von der Registerbehörde an die Staatsanwaltschaften zulässig sind. Der Wortlaut des § 474 Abs. 3 Satz 2 StPO, der den Begriff der ,,Auskunft" verwendet, setzt ein entsprechendes Ersuchen der Staatsanwaltschaft um Auskunft voraus. Spontanübermittlungen der Registerbehörde, das heißt Übermittlungen ohne ein solches Ersuchen an die Staatsanwaltschaften, bei denen ein Verfahren gegen die betroffene Person anhängig ist, wären danach ausgeschlossen. Im Gegensatz dazu sieht der Entwurf einer Errichtungsanordnung Spontanübermittlungen vor.

7.2.3 Aufbau eines zentralen staatsanwaltschaftlichen Verfahrensregisters in Bayern (BAYSIS)

Im *15.* Tätigkeitsbericht (Ziff. 6.4.1) habe ich eingehend über das bei einigen bayerischen Staatsanwaltschaften im Probebetrieb eingesetzte EDV-Verfahren ,,SIJUS-STRAFSTA" berichtet. Das Staatsministerium der Justiz hat mir

nun eine Konzeption für den Aufbau eines zentralen staatsanwaltschaftlichen Verfahrensregisters auf Landesebene (BAYSIS) übersandt, das auf dem Datenverarbeitungsverfahren zur Geschäftsstellenautomation SIJUS-STRAF-STA aufbaut.

Dieses bayerische staatsanwaitschaftliche Informationssystem soll selbständig neben dem im Verbrechensbekämpfungsgesetz vorgesehenen länderübergreifenden staatsanwaltschaftlichen Verfahrensregister (sog. Bundes-SISY) bestehen. Da die tatsächliche Realisierung eines bundesweiten staatsanwaltschaftlichen Verfahrensregisters noch viele Jahre dauern dürfte, hat sich das Staatsministerium der Justiz entschlossen, möglichst rasch ein landesweites bayerisches Informationssystem zu errichten.

7.2.3.1 Grundsätzliche Konzeption des Verfahrens

Aus den Verfahrensregistern der einzelnen Staatsanwaltschaften sollen an das BAYSIS-Register automatisch folgende Daten gemeldet werden:

- Die Personendaten der Hauptbeteiligten (= Beschuldigten),
- Die zuständige Staatsanwaltschaft und das Aktenzeichen,
- Tatzeit(en) und Tatort(e),
- Der Tatvorwurf unter Angabe der Strafbestimmung und der Art der Straftat (z.B. Schlüsselkennzeichen für Straftaten aus dem Bereich der Organisierten Kriminalität),
- Die Einleitung des Verfahrens sowie die Verfahrenserledigung durch Staatsanwaltschaft und Gericht unter Angabe der gesetzlichen Vorschriften,
- Hinweise auf eine ggf. bestehende Datensperre und die Datenlöschung.

Noch nicht festgelegt ist, ob neben Strafverfahren weitere Verfahren an BAYSIS gemeldet werden. Ich gehe davon aus, daß Ordnungswidrigkeitenverfahren, AR-Verfahren (das sind solche aus dem allgemeinen Register der Staatsanwaltschaften) oder Verfahren gegen unbekannte Täter nicht gemeldet werden. Nach Auskunft des Justizministeriums soll nach vorheriger Beteiligung der Praxis zu einem späteren Zeitpunkt geregelt werden, ob und in welchem Umfang ein derartiger Ausschluß erfolgt.

7.2.3.2 Datenübermittlung aus BAYSIS

Die Datenübermittlung aus BAYSIS erfolgt weitgehend automatisch. Wird im EDV-System SIJUS-STRAF-STA einer an BAYSIS angeschlossenen Staatsanwaltschaft ein Verfahren gegen einen Beschuldigten eingetragen, so wird dieses Verfahren automatisch an BAYSIS gemeldet. Im Gegenzug erhält die meldende Staatsanwaltschaft , von BAYSIS eine Liste der dort für den Beschuldigten registrierten Verfahren bzw. eine Fehlanzeige.

Darüber hinaus erhalten alle übrigen Staatsanwaltschaften, bei denen ein - noch unerledigtes - Ermittlungsverfahren gegen den Beschuldigten anhängig ist, ebenfalls eine Mitteilung des neuen Verfahrens. Entsprechendes gilt, wenn sich Änderungen der in BAYSIS gespeicherten Daten ergeben, z.B. dadurch, daß ein Verfahren durch Einstellung gemäß § 170 Abs. 2 StPO erledigt wurde.

Neben dem automatisierten Mitteilungs- und Auskunftsverkehr ist vorgesehen, daß die einzelne Staatsanwaltschaft Anfragen nach Personen und zu Einzelverfahren an BAYSIS richten kann. Für solche Abrufe ist eine Protokollierung vorgesehen. Festgehalten werden dabei die Personennummer der in BAYSIS abgefragten Person, der Zeitpunkt des Abrufs, das Verfahren, zu dem der Abruf vorgenommen wird, und die Namen der anfragenden Behörde und des anfragenden Sachbearbeiters. Die Protokollierung soll aus Kapazitätsgründen möglicherweise nicht alle Anfragen erfassen. Die Aufbewahrungsdauer für die Protokolldaten ist noch nicht bestimmt. Für Anfragen, die zu keinem Treffer führen, ist eine Protokollierung nicht vorgesehen.

7.2.3.3 Löschungsregelungen

Da BAYSIS selbst keine Löschungsfunktionen enthält, muß die Datenlöschung von der für den Datensatz verantwortlichen Staatsanwaltschaft ausgelöst werden. Diese Löschung erfolgt grundsätzlich programmgesteuert durch Eingaben in SIJUS-STRAF-STA.

Als Löschvarianten sind vorgesehen:

- Sofortige Löschung

  Diese findet statt, sofern eine Registereintragung in SIJUS-STRAF-STA etwa wegen Unrichtigkeit gelöscht wird. Eine sofortige Löschung erfolgt auch bei nachträglichen Abgaben, Verbindungen und Abtrennungen innerhalb der Behörde und bei **Einstellung des Ermittlungsverfahrens wegen erwiesener Unschuld.**

- Löschung nach 6-Monatsfrist

  Diese findet statt, wenn von SIJUS-STRAF-STA mitgeteilt wird, daß eine rechtskräftige gerichtliche Entscheidung ergangen ist. Gelöscht wird 6 Monate nach Rechtskraft der gerichtlichen Entscheidung. Damit soll eine Lücke zwischen der Löschung in BAYSIS und der Aufnahme der Entscheidung in das Bundeszentralregister vermieden werden.

- Regellöschungsfrist: 5 Jahre

  Als Regelfall ist vorgesehen, daß eine BAYSIS-Eintragung 60 Monate nach der staatsanwaltschaftlichen Erledigung zu löschen ist. Dies gilt jedoch nicht, wenn zu dem gleichen Beschuldigten noch weitere, nicht löschungsreife Verfahren in BAYSIS vermerkt sind. In diesem Falle wird die Löschung erst vorgenommen, wenn ,,Löschungsreife" für alle Verfahren gegeben ist.

- Löschung nach Ablauf der Aufbewahrungsfrist

Eine sofortige Löschung findet schließlich statt, sobald von SIJUS-STRAF-STA wegen Ablauf der Aufbewahrungsfrist durch eine sog. Folgemitteilung die Löschung des Verfahrensdatensatzes an BAYSIS mitgeteilt wird.

7.2.3.4 Grundsätzliche rechtliche Überlegungen zu BAYSIS

Ich gehe bei der Einführung von BAYSIS von folgenden rechtlichen Überlegungen aus:

Der Einsatz des zentralen Verfahrensregisters der Staatsanwaltschaften in Bayern schränkt das Recht des Betroffenen auf informationelle Selbstbestimmung ein. Solche Einschränkungen sind zwar im überwiegenden Allgemeininteresse hinzunehmen, bedürfen aber einer verfassungsmäßigen gesetzlichen Grundlage, aus der sich Voraussetzungen und Umfang der Beschränkungen klar und für den Bürger erkennbar ergeben und die damit dem Gebot der Normenklarheit entspricht. Eine **bereichsspezifische** gesetzliche Regelung für die Datenverarbeitung ist erforderlich, wenn eine angemessene Regelung durch das allgemeine Datenschutzrecht (BayDSG) nicht möglich ist. Dies ist der Fall bei der Verarbeitung sensibler Daten durch Sicherheits- oder Strafverfolgungsbehörden. Als besonders sensibel gelten personenbezogene Daten, die im Strafverfahren erhoben und zum Zwecke der Strafverfolgung gespeichert werden.

So hat auch der Bayerische Verfassungsgerichtshof in einer Entscheidung vom 09.07.1985 zur Führung polizeilicher Aktensammlungen ausgeführt, daß insoweit der Gesetzgeber die erforderlichen Abgrenzungen zwischen den Rechten des Einzelnen und dem Interesse der Allgemeinheit vorzunehmen habe.

Durch BAYSIS soll ein Verfahren geschaffen werden, das nicht - wie bei SIJUS-STRAF-STA - nur behördenintern, sondern behördenübergreifend alle Ermittlungsverfahren in Bayern erfassen soll. Diese Speicherungen dienen nicht nur der ,,Aktenfindung", sondern der Sachbearbeitung des einzelnen Staatsanwalts, wie der Ausdruck automatisierter Verfahrenslisten zeigt. Mit BAYSIS wird deshalb in erheblich stärkerem Maße in das Recht des Betroffenen auf informationelle Selbstbestimmung eingegriffen. Dieser Bewertung steht auch nicht entgegen, daß § 161 StPO Anfragen und Auskünfte der Staatsanwaltschaften untereinander über dort geführte Verfahren ermöglicht. Die Möglichkeit konventioneller Anfragen und Auskünfte im Wege der Amtshilfe ist nämlich von geringerer Grundrechtsrelevanz als ein landesweites Verfahrensregister, aus dem automatisch Verfahrenslisten mitgeteilt werden bzw. Direktabfragen möglich sind.

Auch das vom Bundesverfassungsgericht in zahlreichen Entscheidungen bestätigte Institut des sog. ,,Übergangsbonus" vermag nach meiner Auffassung ein zentrales Informationssystem der Staatsanwaltschaften in Bayern nicht zu tragen. Die Anwendung dieser Grundsätze setzt nämlich voraus, daß Fälle vorliegen, ,,in welchen eine verfassungsrechtlich **ursprünglich unbedenkliche Maßnahme** aufgrund einer gewandelten Rechtsauffassung oder völlig veränderter tatsächlicher Umstände, die der bisherigen Regelung zugrundelagen, verfassungsrechtlich **bedenklich geworden ist**". Dies bedeutet, daß eine Übergangsfrist nur für solche Maßnahmen gelten kann, die zum Zeitpunkt der Entscheidung des Bundesverfassungsgerichts zum Volkszählungsgesetz 1983 bereits bestanden haben und die im nachhinein durch den Wandel der Rechtsauffassung verfassungsrechtlichen Bedenken begegnen. **Nicht erfaßt sind** jedoch **solche Eingriffe in das Grundrecht** auf informationelle Selbstbestimmung, **die erst neu geschaffen werden sollen.**
Solche Eingriffsmaßnahmen bedürfen vielmehr einer ausreichenden Gesetzesgrundlage.

Neben diesen grundsätzlichen Bedenken habe ich gegenüber dem Justizministerium um Überprüfung gebeten, ob tatsächlich eine Vollspeicherung aller Js-Verfahren erforderlich ist. Gerade bei Delikten geringeren Gewichts, wie etwa Fahrlässigkeitsdelikten, könnte eine Meldung an BAYSIS davon abhängig gemacht werden, ob der sachbearbeitende Staatsanwalt dies aufgrund der Beurteilung des Einzelfalles für erforderlich hält. Darüber hinaus habe ich die Auffassung vertreten, daß aus datenschutzrechtlicher Sicht - im Hinblick auf den geringen Unrechtsgehalt - darauf verzichtet werden sollte, Ordnungswidrigkeiten an BAYSIS zu melden.

Positiv bewerte ich, daß bei Einstellung des Ermittlungsverfahrens wegen erwiesener Unschuld eine sofortige. Löschung der Speicherung in BAYSIS beabsichtigt ist. Ich habe das Justizministerium jedoch darauf hingewiesen, daß ich es für sachgerecht halte, wenn darüber hinaus auch ein Freispruch wegen erwiesener Unschuld und eine rechtskräftige Ablehnung der Eröffnung des Hauptverfahrens wegen erwiesener Unschuld zur sofortigen Löschung führen würden.

7.2.3.5 Haltung des Bayerischen Staatsministeriums der Justiz

Im Gegensatz zu vorgenannten Ausführungen sieht das Justizministerium bis jetzt in Art. 18, 17 Abs. 1 und 2 Nr. 10 BayDSG i.V.m. §§ 152 Abs. 2 und 161 StPO eine hinreichende Rechtsgrundlage für das Datenverarbeitungssystem BAYSIS. Bereichsspezifische Datenschutzregelungen seien nur dann zwingend erforderlich, wenn die Voraussetzungen und der Umfang der Beschränkungen des Rechts auf informationelle Selbstbestimmung ohne solche Regelungen für den Bürger nicht erkennbar seien. Davon könne bei BAYSIS jedoch nicht ausgegangen werden. Aus § 161 StPO ergäbe sich ausdrücklich, daß die Staatsanwaltschaft von allen öffentlichen Behörden zu Zwecken der Strafverfolgung Auskunft verlangen könne. Dies umfasse insbesondere die Auskunft anderer Staatsanwaltschaften über dort geführte Verfahren.

Auch bei Strafverfahren wegen Fahrlässigkeitsdelikten gegen namentlich bekannte Beschuldigte sei eine regelmäßige Meldung an BAYSIS gerechtfertigt, ohne daß es einer Entscheidung des sachbearbeitenden Staatsanwalts über die Meldung im Einzelfall bedürfe.

Ich habe meine rechtlichen Überlegungen nochmals dem Staatsministerium der Justiz übermittelt, eine Antwort hierauf steht noch aus.

7.2.4 Registerverfahrenbeschleunigungsgesetz und EDV-Grundbuch

Bereits im 15. Tätigkeitsbericht (Ziff. 6.2.1) habe ich über das inzwischen (am 25.12.1993) in Kraft getretene Registerverfahrenbeschleunigungsgesetz vom 20.12.1993 berichtet. Mittlerweile wurde am 26.05.1994 die Neufassung der Grundbuchordnung bekannt gemacht. Dort werden im 7. Abschnitt die Landesregierungen ermächtigt, durch Rechtsverordnung ein maschinell geführtes Grundbuch einzuführen. Ergänzend hierzu wurden im 13. Abschnitt der Grundbuchverfügung vorläufige, bis 31.12.1995 befristete nähere Bestimmungen über das maschinell geführte Grundbuch getroffen. Mittlerweile ist die Dritte Verordnung zur Anderung der Verordnung zur Durchführung der Schiffsregisterordnung und zur Regelung anderer Fragen des Registerrechts in Kraft getreten. Sie hebt die Befristung des EDV-Teils der Grundbuchverfügung auf.

Am 07.06.1994 wurde das EDV-System ,,SOLUM-STAR" zur maschinellen Grundbuchführung im Amtsgericht München der Öffentlichkeit vorgestellt. Unabhängig davon habe ich mir bei einem Besuch des Grundbuchamtes einen Eindruck von dem neuen Verfahren verschafft:

Dieses Grundbuchsystem wird von den Landesjustizverwaltungen Bayern, Sachsen, Sachsen-Anhalt und Hamburg entwickelt. In Bayern wird das System SOLUMSTAR zunächst bei dem Amtsgericht München im Probebetrieb eingesetzt. Falls hierbei keine Probleme auftreten, ist der Beginn des Echtbetriebs im Dezember 1994 zu erwarten. Das Bayerische Staatsministerium der Justiz beabsichtigt, SOLUM-STAR nach Maßgabe der finanziellen Voraussetzungen auch bei den übrigen 103 bayerischen Grundbuchämtern einzuführen.

Die Struktur des Grundbuchs und die Einteilung der Grundbuchblätter ändern sich durch SOLUM-STAR nicht. Die vorhandenen Grundbuchbestände werden durch den Einsatz von Scannern erfaßt und in nichtcodierter Form gespeichert. Eintragungen nach dieser Ersterfassung werden mit dem Programmsystem SOLUM erstellt und vor der Abspeicherung mit einer ,,elektronischen Unterschrift" versehen, die Authentizität und Integrität der Eintragungen sicherstellt. Die Eintragungen werden sodann im elektronischen Grundbuch in codierter Form gespeichert.

Grundbucheinsicht im Grundbuchamt wird entweder durch Graphikbildschirme, auf denen der Inhalt der Grundbuchblätter seitenweise angezeigt wird, oder durch Einsicht in einen Ausdruck des Grundbuchblatts gewährt.

Der Erleichterung des Grundstückverkehrs dienen soll ein sog. **automatisiertes Abrufverfahren:**

Damit kann eine bestimmte Gruppe von Einsichtsinteressenten (wie z.B. Notare, Behörden, Banken, Kreditinstitute und Versicherungen) zur Grundbucheinsicht im Online-Verfahren zugelassen werden. Zur Sicherung werden für die Teilnehmer am automatisierten Abrufverfahren besondere systemtechnische Berechtigungen vergeben und vom Programm geprüft.

Banken, Kreditinstitute und Versicherungen in privatrechtlicher Form sind nur eingeschränkt abfrageberechtigt. Sie dürfen nur insoweit Grundbuchdaten abrufen, als sie selbst am betroffenen Grundstück dinglich berechtigt oder von einem dinglich Berechtigten hierzu ermächtigt sind. Die Kontrolle erfolgt durch.die Protokollierung.

Sämtliche Datenabrufe im Online-Verfahren werden im System protokolliert. In der Protokolldatei gespeichert werden Datum, abfragende Stelle, Gemarkung, Grundbuchblattnummer und Aktenzeichen. Soweit der Online-Abruf von Einrichtungen vorgenommen wird, die nur eingeschränkt zum automatisierten Abrufverfahren zugelassenen sind, wird ferner in der Protokolldatei durch Angabe einer Schlüsselzahl gespeichert, welchen Grund der Einsichtnehmende für das Vorliegen seines berechtigten Interesses angegeben hat. Grund dafür ist, daß nur eingeschränkt Abrufberechtigte den Einsichtsgrund (etwa: dingliche Berechtigung) konkret dartun müssen.

Gegen die Konzeption des EDV-Grundbuchs SOLUM-STAR habe ich keine grundsätzlichen datenschutzrechtlichen Bedenken. Erfahrungen im Echtbetrieb bleiben abzuwarten.

Protokollierung der Grundbucheinsicht

Eine Protokollierung ist **nur** für die Einsichtnahme im **automatischen Abrufverfahren** vorgesehen. Soweit die Einsicht in das EDV-Grundbuch im Grundbuchamt selbst oder in das Papiergrundbuch stattfindet, sieht das Staatsministerium der Justiz keine Notwendigkeit für eine Protokollierung. Es hat darüber hinaus auf den für eine Protokollierung erforderlichen Aufwand hingewiesen. Eine Protokollierung der Einsichtnahme in das Papiergrundbuch erfordert entweder die Bereitstellung eines datenverarbeitungsgestützten Verfahrens oder die manuelle Führung von Listen. Beides ist mit nicht unerheblichen finanziellen Belastungen und zusätzlichem Zeitaufwand verbunden. Angesichts des Umstands, daß das Papiergrundbuch ohnehin in absehbarer Zeit nicht mehr weitergeführt wird, erscheint es mir vertretbar, die Forderung nach Protokollierung der Einsicht in das Papiergrundbuch zurückzustellen.

Demgegenüber halte ich es aus datenschutzrechtlicher Sicht für wünschenswert, **daß alle Einsichtnahmen in das maschinell geführte Grundbuch protokolliert** werden, um im Interesse des Betroffenen im Einzelfall feststellen zu können, wer personenbezogene Informationen über ihn erhalten hat und um unberechtigten Einsichtnahmen entgegenzuwirken. Das Justizministerium ist allerdings auch hier der Auffassung, daß der Aufwand für die Protokollierung der Einsichtnahmen zu hoch sei. Vertretbar sei allenfalls die stichprobenartige Protokollierung etwa jedes 10. Einsichtsvorgangs, wenn für die Protokollierung ein zweckmäßiges Verfahren und eine entsprechende EDV-Technik zur Verfügung stehen.

Zumindest eine Auswahlprotokollierung halte ich aus präventiven Gründen für geboten. Damit wird allerdings nicht sichergestellt, daß die einzelne Einsichtnahme bei Bedarf nachvollzogen werden kann. Als Speicherungsdauer für die Protokolldaten sollte mindestens ein Jahr vorgesehen werden. **Ich werde mich dafür einsetzen, daß in die Grundbuchverfiigung eine ausreichende Protokollierungsverpflichtung aufgenommen wird.**

7.2.5 Entwurf einer Zweiten Zwangsvollstrek kungsnovelle - Pfändungs- und Überweisungsbeschluß bei einer Mehrzahl von Drittschuldnern

Die Länder Baden-Württemberg, Bayern und Sachsen hatten dem Bundesrat einen Gesetzesantrag für ein Zweites Gesetz zur Änderung zwangsvollstreckungsrechtlicher Vorschriften vorgelegt. Danach sollte § 829 Abs. 1 der Zivilprozeßordnung (ZPO) um folgenden Satz ergänzt werden:

,,Die Pfändung mehrerer Geldforderungen gegen verschiedene Drittschuldner soll auf Antrag des Gläubigers durch einheitlichen Beschluß ausgesprochen werden."

Dazu hatte ich gegenüber dem Justizministerium wie folgt Stellung genommen:

Die bisherige zwangsvollstreckungsrechtliche Praxis, die die Pfändung von Forderungen gegen mehrere Drittschuldner ohne besondere Rechtsgrundlage in einem Pfändungsbeschluß zusammenfaßt, greift in das Recht auf informationelle Selbstbestimmung der Drittschuldner ein. Diese können dem Pfändungsbeschluß nämlich entnehmen, welche weiteren Drittschuldner aus welchem Rechtsgrund vom Schuldner in Anspruch genommen werden können. Ein Eingriff in das informationelle Selbstbestimmungsrecht des Drittschuldners ist jedoch nur zulässig, soweit er - auch unter Berücksichtigung der schützenswerten Interessen des Betroffenen - sachlich geboten ist. Lediglich geringfügige Verfahrenserleichterungen und Kostengründe können einen solchen Eingriff deshalb nicht rechtfertigen.

Zwischenzeitlich wurde der Gesetzentwurf wie folgt geändert:

,,Die Pfändung mehrerer Geldforderungen gegen verschiedene Drittschuldner soll auf Antrag des Gläubigers durch einheitlichen Beschluß ausgesprochen werden, soweit dies für Zwecke der Vollstreckung geboten erscheint und kein Grund zu der Annahme besteht, daß schutzwürdige Interessen der Drittschuldner entgegenstehen."

Ich meine, daß mit dieser Formulierung den datenschutzrechtlichen Anforderungen zumindest entgegengekommen wurde. Allerdings sollten die Worte ,,geboten erscheint" durch die Worte ,,erforderlich ist" ersetzt werden, um deutlich zu machen, daß die Entscheidung über den Erlaß eines gemeinsamen Pfändungs- und Überweisungsbeschlusses nach einem engen objektiven Maßstab zu erfolgen hat.

7.2.6 Prozeßkostenhilfeänderungsgesetz

Die Bundesregierung hat den Entwurf eines Gesetzes zur Änderung von Vorschriften über die Prozeßkostenhilfe vorgelegt. Dieser enthält in zwei Punkten eine wesentliche **Verbesserung des Datenschutzes.**

So soll § 117 Abs. 2 der Zivilprozeßordnung (ZPO) dahingehend ergänzt werden, daß die dem Antrag der Partei auf Gewährung von Prozeßkostenhilfe beigefügte Erklärung und die Belege über die persönlichen und wirtschaftlichen Verhältnisse (Familienverhältnisse, Beruf, Vermögen, Einkommen und Lasten) **dem Gegner nur mit Zustimmung** der antragstellenden Partei zugänglich gemacht werden.

Darüber hinaus soll § 127 Abs. 1 ZPO, der die Entscheidung über den Antrag auf Prozeßkostenhilfe regelt, um folgenden Satz ergänzt werden:

,,Soweit die Gründe der Entscheidung Angaben über die persönlichen und wirtschaftlichen Verhältnisse der Partei enthalten, dürfen sie dem **Gegner nur mit Zustimmung** der Partei zugänglich gemacht werden."

Der Bundesrat hat sich gegen die Ergänzung des § 127 Abs. 1 ZPO mit dem Argument gewandt, daß dies zu einer Aufspaltung der Entscheidungsgründe und damit zu einer Mehrbelastung der Gerichte führen würde.

Ich kann diese Kritik nicht teilen, zumal in der Praxis die Bewilligung von Prozeßkostenhilfe regelmäßig nicht begründet wird und auch bei den Prozeßkostenhilfe versagenden Entscheidungen nur selten die Notwendigkeit einer Aufspaltung der Entscheidungsgründe auftreten dürfte. Ich habe daher gegenüber dem Staatsministerium der Justiz die im Regierungsentwurf enthaltenen Ergänzungen unterstützt und darauf hingewiesen, daß deren praktische Umsetzung wegen der geringen Zahl der Fälle keinen unzumutbaren Mehraufwand für die Gerichte bedeuten dürfte.

Mittlerweile hat der Bundestag am 10.10.1994 das Prozeßkostenhilfeänderungsgesetz mit **beiden** datenschutzfreundlichen Ergänzungen beschlossen. Die Änderungen traten bereits am 01.01.1995 in Kraft.

7.3 Kontrollen im Justizbereich

7.3.1 Kontrollkompetenz des Landesbeauftragten für den Datenschutz gegenüber der Staatsanwaltschaft (Art. 30 BayDSG)

Nachdem ,bei der Prüfung einer Staatsanwaltschaft im Jahre 1993 unterschiedliche Auffassungen zum Umfang meiner Kontrollkompetenz festzustellen waren, habe ich im Berichtszeitraum in zwei Besprechungen mit dem Justizministerium diese Frage intensiv diskutiert. Dabei konnte in einzelnen Bereichen Einvernehmen, in anderen eine Annäherung oder die Bereitschaft des Justizministeriums zur nochmaligen Überprüfung der Standpunkte erreicht werden.

1. **Kontrolle bei Datenverarbeitung in Dateien**

   Übereinstimmung besteht hinsichtlich meiner Befugnis, jederzeit die Rechtmäßigkeit der Speicherungen in Dateien der Staatsanwaltschaften zu überprüfen. Unbestritten ist nunmehr auch, daß ich bei Dateikontrollen die zu überprüfenden Vorgänge selbst auswählen kann. Sind zur Überprüfung die dazugehörigen Akten erforderlich, werden mir diese vollständig zur Einsichtnahme vorgelegt.

   Hinsichtlich der **Kontrolltiefe** scheint das Justizministerium der Ansicht zuzuneigen, ich sei auf die Prüfung der Frage beschränkt, ob die einzelnen Datenspeicherungen im Akt einen Rückhalt finden (z.B. fehlerhafte Übertragung personenbezogener Daten von der Akte in die Datei).

   Datenschutzkontrolle im Sinne des Art. 30 BayDSG bedeutet nicht nur (formale) Prüfung des Aktenrückhalts der Datenspeicherungen. Prüfungsgegenstand ist vielmehr die Akte selbst, jedenfalls in dem Umfang, in dem die personenbezogenen Daten sowohl in der Datei/Kartei, als auch in der Akte gespeichert sind. Nach den führenden Kommentaren zum Bundesdatenschutzgesetz und zum Bayerischen Datenschutzgesetz kommt es darauf an, ob die Daten **ausschließlich** in Akten verarbeitet werden. Ist dies nicht der Fall, so unterliegt nicht nur der Datenbestand der Datei, sondern auch der entsprechende Datenbestand im Akt der Kontrolle. Das gleiche muß wohl auch für den ,,überschießenden" Datenteil des Akts jedenfalls insoweit gelten, als dieser eng, unmittelbar und untrennbar mit dem auch in der Datei enthaltenen Datenbestand des Aktes zusammenhängt. Auch für diese Daten besteht nach meiner Auffassung die Prüfungskompetenz des Landesbeauftragten für den Datenschutz, ohne daß ein konkreter Anlaß besteht.

   Das bedeutet, daß - entgegen der Ansicht des Justizministeriums - grundsätzlich alle Datenübermittlungen aus Ermittlungsakten oder die Gewährung von Akteneinsicht von mir überprüft werden können. Dabei kann es nicht darauf ankommen, ob alle übermittelten Daten in der Datei gespeichert sind. Es muß genügen, wenn dies jedenfalls für einen Teil der Daten zutrifft. Entscheidend ist auch nicht, ob die Daten tatsächlich aus der Datei oder aus dem Akt übermittelt werden. Dies wird im Einzelfall häufig auch nicht feststellbar sein.

   Meiner Überprüfung unterliegt in den Grenzen des Art. 30 Abs. 4 BayDSG auch die Datenerhebung, wie z.B. Herstellung von Lichtbildern und Bildaufzeichnungen (§100 c Abs. 1 Nr.1 a StPO) oder der Einsatz verdeckter Ermittler (§110 a StPO). Dies gilt jedenfalls, soweit die Maßnahme selbst oder die durch ihren Einsatz erhobenen personenbezogenen Daten Niederschlag in einer Datei gefunden haben. Da dies häufig nicht der Fall sein wird, bin ich bei anlaßunabhängigen Kontrollen dieser verdeckten Datenerhebungsmaßnahmen, die tief in das Persönlichkeitsrecht des Betroffenen eingreifen, erheblich beschränkt (vgl. auch Ziff. *5.3.2).*

2. **Kontrolle bei Datenverarbeitung in Akten (sog. Anlaßkontrolle, Art. 30 Abs. 1 Satz 2 BayDSG)**

   Einvernehmen mit dem Justizministerium besteht darüber, daß ,,hinreichende Anhaltspunkte" im Sinne des Art. 30 Abs. 1 Satz 2 BayDSG für eine Datenschutzkontrolle in Akten jedenfalls in folgenden Fällen vorliegen:

- Eingaben von Bürgern, sofern durch substantuerten Vortrag eine Rechtsverletzung dargetan wird,
- substantuerte Berichte von Presseorganen über konkrete datenschutzrechtlich relevante Sachverhalte in Bayern,
- substantiierte Berichte von Presseorganen über konkrete datenschutzrechtlich relevante Sachverhalte in anderen Ländern, die auch in Bayern vorstellbar sind,
- Erkenntnisse über datenschutzrechtliche Mängel bei einer öffentlichen Stelle in Bayern (z.B. Staatsanwaltschaft), wenn Anhaltspunkte dafür bestehen, daß kein Einzelfall vorliegt.
- Erkenntnisse über datenschutzrechtliche Mängel der Datenverarbeitung in Akten, die bei Gelegenheit einer Dateikontrolle unter Beiziehung der Akte festgestellt wurden (sog. Zufallsfunde).

   Neben ,der Kontrolle der Verarbeitung und Nutzung personenbezogener Daten kann ich auch die Rechtmäßigkeit der Datenerhebung in strafrechtlichen Ermittlungsverfahren überprüfen. Beschränkungen meiner Prüfungskompetenz bestehen nur insoweit, als eine Überprüfung nicht während eines laufenden Strafverfahrens zulässig ist (Art. 30 Abs. 4 Satz 1 BayDSG) und soweit Datenerhebungen gerichtlich überprüft wurden (Art. 30 Abs. 4 Satz 2 BayDSG). Prüfungsmaßstab sind die jeweiligen Erhebungsvorschriften der Strafprozeßordnung, die als bereichsspezifische Datenschutzbestimmungen die Voraussetzungen der Erhebung personenbezogener Daten im

Hinblick auf das Recht auf informationelle Selbstbestimmung regeln.

Bei der Überprüfung der rechtmäßigen Anwendung der Datenschutzvorschriften findet grundsätzlich eine vollständige Kontrolle der rechtlichen Voraussetzungen des Einsatzes der Datenerhebungsmaßnahme (z.B. Vorliegen einer Straftat von erheblicher Bedeutung) statt. Gleichwohl bin ich bereit, der Natur des strafrechtlichen Ermittlungsverfahrens durch datenschutzrechtliches ,,Self-Restraint" Rechnung zu tragen: Soweit nach dem Gesetz Bewertungen oder Einschätzungsprärogativen eine Rolle spielen, werde ich deren besondere Fachkenntnis respektieren. Insoweit werde ich nur auf die Einhaltung der Grenzen der Vertretbarkeit achten.

3. Einschränkung der Kontrollbefugnis durch Art. **30 Abs. 4 Satz 1 BayDSG**

Nach dieser Vorschrift, die in den Datenschutzgesetzen des Bundes und der Länder kein Vorbild hat, sondern einzig in Bayern anläßlich der Neufassung in das Bayerische Datenschutzgesetz aufgenommen wurde, ist die Kontrolle der **Erhebung** personenbezogener Daten durch Strafverfolgungsbehörden erst nach Abschluß des Strafverfahrens zulässig. Auf die damit verbundene Problematik für einen effektiven Datenschutz habe ich das Justizministerium hingewiesen:

Mindestens 80 % der polizeilichen verdeckten Datenerhebung findet nicht im Bereich der Gefahrenabwehr, sondern im Rahmen strafrechtlicher Verfolgung statt. Daher bedeutet das Aufschieben der Überprüfung der Datenerhebung bis zum Abschluß des Verfahrens, daß der besonders sensible Bereich verdeckter Erhebungsmaßnahmen - soweit nicht deren gerichtliche Anordnung vorgesehen ist - in großem Umfang zum Teil Monate oder sogar Jahre für eine externe, unabhängige Kontrolle nicht zugänglich ist. Die zur Begründung dieser Einschränkung vorgebrachten Argumente halte ich nicht für stichhaltig.

Das Argument, es bedürfe einer Kontrolle der Datenerhebung durch den Datenschutzbeauftragten während des Verfahrens nicht, da diese Maßnahmen ohnehin später durch das Gericht kontrolliert würden, ist für die Mehrzahl der Ermittlungsverfahren, die durch Einstellung (vor allem gemäß § 170 Abs. 2 StPO) beendet werden, unzutreffend. In diesen Fällen findet gerade keine gerichtliche Kontrolle statt. Die Überprüfung durch den Datenschutzbeauftragten nach Abschluß des Verfahrens ist oftmals angesichts der langen Dauer des Ermittlungsverfahrens nicht mehr zeitnah möglich.

Auch das weitere Argument, eine Kontrolle durch den Datenschutzbeauftragten würde das laufende Ermittlungsverfahren im Fortgang behindern oder die Ermittlungen gefährden, überzeugt nicht. Dies könnte bei entsprechender Gestaltung der Prüfung vermieden werden. Ebenso könnte ausgeschlossen werden, daß der Petent den Fortgang der Ermittlungen gefährdende Erkenntnisse erlangt, indem zum Ergebnis der Kontrolle etwa nur mitgeteilt wird, daß eine Überprüfung keine Verletzung datenschutzrechtlicher Vorschriften ergeben habe.

7.3.2 Kontrolle einer Staatsanwaltschaft

Im Berichtszeitraum habe ich eine Staatsanwaltschaft geprüft, bei der sowohl das EDV-Verfahren SIJUSSTRAF-StA als auch das für Wirtschaftsstrafsachen vorgesehene EDV-Verfahren COWISTRA eingesetzt wird. Mein besonderes Augenmerk galt bei dieser Prüfung der Durchführung von Mitteilungen in Strafsachen, der Praxis der Gewährung von Einsicht in Strafakten und dem EDV-Verfahren COWISTRA.

Als Ergebnis der Prüfung kann ich feststellen, daß die Staatsanwaltschaft in den geprüften Bereichen dem Datenschutz einen hohen Stellenwert beimißt. Gravierende Verstöße gegen den Datenschutz habe ich nicht festgestellt.

7.3.2.1 Mitteilungen in Strafsachen (MiStra)

Gegenstand der Überprüfung waren Mitteilungen über Angehörige des öffentlichen Dienstes (MiStra Nr.15), über Soldaten der Bundeswehr und Zivildienstleistende (MiStra Nr.20), über Rechtsanwälte (MiStra Nr.23) und über Ausländer (MiStra Nr. 42). Anhand zahlreicher Fälle habe ich überprüft, ob bei den Mitteilungen an den jeweiligen Dienstvorgesetzten, die Rechtsanwaltskammer und an das Ausländeramt den datenschutzrechtlichen Anforderungen entsprochen wird.

In allen überprüften Verfahren lagen die Voraussetzungen (z.B. Erhebung der öffentlichen Klage) für die Mitteilung vor.

Leider ist es dem Bundesgesetzgeber aber immer noch nicht gelungen, die Mitteilungen an Dritte, die für den Betroffenen von erheblicher Tragweite sein können, auf eine bereichsspezifische gesetzliche Grundlage zu stellen. Verwaltungsvorschriften (MiStra) sind auf Dauer hierfür nicht ausreichend. Ich habe deshalb, gemeinsam mit den anderen Datenschutzbeauftragten, den Gesetzgeber aufgefordert, das Versäumte nachzuholen (vgl. Ziff. 7.1).

Die Verfügungen, mit denen vom Staatsanwalt die Mitteilung angeordnet wird, bezeichnen die Adressaten zum Teil nur grob (z.B. ,,an die Stadt" und nicht ,,an den Oberbürgermeister der Stadt"). Ob die Mitteilungen von der Geschäftsstelle ordnungsgemäß ausgeführt wurden, konnte bei der Staatsanwaltschaft nicht überprüft werden, da kein Entwurf der Mitteilung beim Akt verbleibt. Dafür wäre eine Überprüfung beim Empfänger der Mitteilung erforderlich. Da sich erst vor kurzem ein Bürger in einer Eingabe an mich gewandt hatte, weil ein Strafbefehlsantrag einer bayerischen Staatsanwaltschaft dem falschen Dienstherrn

mitgeteilt worden sei, habe ich angeregt, daß in Zweifelsfällen durch den Staatsanwalt klargestellt werden sollte, wer richtiger Adressat der Mitteilung ist.

7.3.2.2 Gewährung von Akteneinsicht

Auch die Gewährung von Akteneinsicht ist bisher nur zum Teil in der Strafprozeßordnung geregelt. Gesetzlich ungeregelt ist nach wie vor die Akteneinsicht durch Personen und Behörden, die am Strafverfahren nicht beteiligt sind. Die Entscheidung über die Gewährung der Akteneinsicht erfolgt hier auf der Grundlage der Richtlinien für das Straf- und Bußgeldverfahren. Diese setzen voraus, daß der Antragsteller ein berechtigtes Interesse an der Einsichtnahme besitzt und sonstige Bedenken nicht bestehen.

Bei einer Reihe von Ermittlungsverfahren habe ich die Rechtmäßigkeit der Gewährung von Akteneinsicht überprüft. Anlaß zu Beanstandungen bestand nicht.

Allerdings bin ich bei der Kontrolle der Akteneinsicht einer AOK als Sozialversicherungsträger, die aufgrund übergegangenen Rechts das Bestehen von Ansprüchen gegen den Schädiger ihrer Versicherten prüfen wollte, auf ein besonderes Problem gestoßen. Der AOK war der komplette Ermittlungsvorgang übersandt worden, in dem **mehrere Strafverfahren** verbunden waren, obwohl das für die Gewährung der Akteinsicht erforderliche berechtigte Interesse der AOK nur für die Straftat vorlag, die zur Schädigung der Versicherten geführt hatte.

Im konkreten Fall lag dem Beschuldigten zunächst nur eine Körperverletzung zur Last, auf die die AOK die Prüfung von Schadensersatzansprüchen stützte. Das Ermittlungsverfahren wurde, da die Geschädigte von ihrem Aussageverweigerungsrecht Gebrauch machte, gemäß §170 Abs. 2 StPO eingestellt. Später zeigte die Geschädigte den Beschuldigten auch wegen eines nachfolgenden Sexualdelikts an. Sie machte nunmehr auch hinsichtlich der früheren Körperverletzung Zeugenangaben. Däs bereits eingestellte Ermittlungsverfahren wegen Körperverletzung wurde sodann wieder aufgenommen, zur neuen Anzeige hinzuverbunden und zur gleichen Akte genommen.

Die Verbindung von Strafverfahren zur sachentsprechenden Strafverfolgung ist ein häufiger Vorgang. Davon können auch eine Vielzahl von Einzelstraftaten (z.B. bei Serienstraftaten) betroffen sein. Ich verkenne nicht, daß die Entscheidung, welche Aktenteile vom berechtigten Interesse des Antragstellers umfaßt sind, für den sachbearbeitenden Staatsanwalt eine erhebliche zusätzliche Arbeitsbelastung darstellen würde. Das gleiche gilt für die Geschäftsstelle, die die Akten trennen müßte. Hinzu kommt, daß sich einzelne Aktenbestandteile (z.B. Mitteilungen der Polizei, Protokolle über Zeugenaussagen, staatsanwaltschaftliche oder gerichtliche Entscheidungen) auf mehrere Straftaten beziehen können.

Ich habe als Lösungsansatz vorgeschlagen, daß die Akteneinsicht grundsätzlich nur auf den konkreten Vorgang, für dessen Kenntnisnahme durch den Antragsteller ein berechtigtes Interesse vorliege, sowie auf die (vollständigen) Entscheidungen von Staatsanwaltschaft und Gericht beschränkt werden sollte, soweit eine entsprechende Aktentrennung mit zumutbarem Aufwand möglich ist. Hierzu habe ich das Justizministerium um Prüfung gebeten. Im konkreten Strafverfahren, das Anlaß zur Prüfung gegeben hatte, wäre eine solche Aktentrennung hinsichtlich der einzelnen Tatvorwürfe wegen ihrer engen Verbindung allerdings nicht möglich gewesen.

7.3.2.3 Anwendung des EDV-Systems COWISTRA

Nach Auskunft der Staatsanwaltschaft nutzt die Wirtschaftsabteilung bisher nur zwei Anwendungsmöglichkeiten von COWISTRA: So werden Mitteilungen über die Abgabe eidesstattlicher Versicherungen und Mitteilungen in Konkursverfahren nach Verfügung des Oberstaatsanwalts in die Datei aufgenommen. Erfaßt werden der Name bzw. die Firma, der/die Geschäftsführer und der Grund der Speicherung. Die Vorgänge werden beobachtet und bei Bestehen eines Anfangsverdachts in das Js-Register (Register für Strafsachen) eingetragen.

Gegen diesen Einsatz von COWISTRA habe ich keine datenschutzrechtlichen Bedenken. Da die Anwendung erst seit etwa 6 Monaten bei der Behörde wieder eingesetzt wird, lagen „löschungsreife" Vorgänge noch nicht vor, so daß die Beachtung der Löschungsfristen einer späteren Prüfung vorbehalten bleibt.

Daneben wird die Datenbankfunktion „Gläubigeranfragen" von den Sachverständigen und der Buchhaltungsfachkraft der Wirtschaftsabteilung genutzt. Damit können Gläubigeraufstellungen bearbeitet, Anschreiben an Gläubiger erfaßt und Fragebogen erstellt werden. Derzeit sind dort ca. 20 Verfahren gespeichert, das älteste aus dem Jahr 1988.

Nach der Freigabe des Programmsystems COWISTRA sind die im Rahmen von Ermittlungsverfahren gespeicherten Daten nach rechtskräftigem Abschluß des Verfahrens zu löschen. Eine Überprüfung ergab, daß auch personenbezogene Daten aus Ermittlungsverfahren gespeichert sind, die bereits vor längerer Zeit abgeschlossen waren. Die Staatsanwaltschaft hat mir mitgeteilt, daß die Daten dieser Verfahren mittlerweile gelöscht worden sind und die Datenlöschung im Bereich des Programms COWISTRA durch Dienstanweisung geregelt wird.

7.3.3 Kontrolle einer Justizvollzugsanstalt

Wie schon im Jahre 1993 habe ich auch im Berichtszeitraum eine datenschutzrechtliche Prüfung einer Justizvollzugsanstalt durchgeführt. Als erfreuliches Ergebnis konnte ich feststellen, daß die Justizvollzugsanstalt dem Datenschutz einen hohen Stellenwert beimißt. Gravierende datenschutzrechtliche Mängel konnte ich nicht feststellen. Folgende Feststellungen sind von allgemeiner Bedeutung:

7.3.3.1 Gefangenenpersonalakten

Mein besonderes Augenmerk galt auch diesmal dem Zugriff auf die Gefangenenpersonalakten. Wie bei den bisher von mir geprüften Justizvollzugsanstalten haben auch in dieser Anstalt alle Vollzugsbediensteten Zugriff auf die Gefangenenpersonalakten aller Gefangenen. Bei Entnahme der Akte verbleibt ein sogenanntes Fehlblatt in der Registratur, in dem der Name des Gefangenen, der Name des die Akte entnehmenden Bediensteten, der Entnahmezweck, das Datum und die Unterschrift des Entnehmenden anzugeben sind. Dieses Fehlblatt wird nach Rückgabe der Akte entfernt, so daß keine Dokumentation darüber gewährleistet ist, wer die Akte eingesehen hat.

Bereits in der Vergangenheit habe ich gefordert, die **Einsichtnahme in Gefangenenpersonalakten auf den Umfang zu beschränken,** der zur jeweiligen Aufgabenerfüllung erforderlich ist. Eine Beschränkung der Zugriffsberechtigung auf bestimmte mit dem Gefangenen befaßte Vollzugsbedienstete hat sich allerdings in der Praxis als nicht durchführbar gezeigt. Auch wenn Stationsbeamten bestimmte Gefangene fest zugewiesen sind, so können doch im Einzelfall auch andere Vollzugsbeamte ein rechtmäßiges Informationsinteresse besitzen. So wird beispielsweise der Nachtdienst nach Auskunft der Anstalt von ständig wechselnden Vollzugsbediensteten verrichtet. Auch diesen Bediensteten muß es im Interesse der Anstaltssicherheit möglich sein, sich etwa über besonders fremd-, flucht- oder selbstgefährliche Gefangene durch Beiziehung der Akten zu unterrichten.

Umso wichtiger erscheint es mir - um einem eventuellen Mißbrauch vorzubeugen -, die **Einsichtnahme bzw.** Entnahme der Gefangenenpersonalakten **schriftlich zu dokumentieren.** Damit dürfte kein unzumutbarer Verwaltungsaufwand verbunden sein, zumal das bereits jetzt bei Entnahme der Gefangenenpersonalakten hinterlegte Fehlblatt nur um Einsichtnahmen ergänzt und für eine spätere Überprüfung des Zugriffs auf die Akte aufbewahrt werden müßte. Hierzu habe ich das Staatsministerium der Justiz um Stellungnahme gebeten. Dieses hat eine Dokumentation der Einsichtnahme/Entnahme von Akten abgelehnt, da damit ein unverhältnismäßiger Verwaltungsaufwand verbunden wäre. Ich werde die Angelegenheit weiter verfolgen.

7.3.3.2 Auskünfte an Vollstreckungsgläubiger

Entsprechend meinen Feststellungen im 15. Tätigkeitsbericht (Ziff. 6.9.2.3) habe ich nochmals überprüft, ob und welche Auskünfte über Gefangene an Gläubiger erteilt werden. In der geprüften Justizvollzugsanstalt besteht hierüber eine Dienstanweisung aus dem Jahre 1987, in der u.a. folgendes bestimmt ist:

- Der Auskunftssuchende hat das **berechtigte** Interesse an der Auskunft zu belegen.
- Der Entlassungszeitpunkt wird nur dann mitgeteilt, falls er innerhalb des nächsten Monats liegt, in den übrigen Fällen wird lediglich die Inhaftierung bestätigt.
- Als Entlassungsanschrift wird nur der Ort angegeben, im übrigen wird der Gläubiger auf die zuständigen Meldebehörden verwiesen.

Ergänzend wurde die Festlegung getroffen, daß die Anstalt Auskünfte nur dann erteilt, wenn das Geburtsdatum des betroffenen Gefangenen vom Auskunftssuchenden mitgeteilt wird.

In Zweifelsfällen wird nach Angaben der Anstalt beim Gefangenen mittels eines Formblatts angefragt, ob er mit der Erteilung der gewünschten Auskunft einverstanden ist.

Dieses Verfahren berücksichtigt in angemessener Weise die datenschutzrechtlichen Belange des Gefangenen. Eine stichprobenartige Überprüfung der erteilten Auskünfte ergab, daß in einem Falle auch das Entlassungsdatum und die vollständige Entlassungsanschrift eines bereits entlassenen Gefangenen an eine Gläubigerbank mitgeteilt wurde. Die Mitteilung von Daten eines bereits entlassenen Gefangenen, halte ich in diesem Umfang für bedenklich. Dies gilt insbesondere für die Mitteilung der Wohnanschrift, nach der der ehemalige Gefangene entlassen wurde. Der Gläubiger sollte an die Meldebehörden verwiesen werden, da die Justizvollzugsanstalt für Auskünfte über den Gefangenen nach dessen Entlassung aus der Anstalt grundsätzlich nicht mehr zuständig ist.

Vorstehende Problematik war auch Gegenstand einer Eingabe von einer anderen Justizvollzugsanstalt. Die dortige Praxis gibt zu Bemerkungen Anlaß (siehe Ziff. 7.9.1).

7.3.3.3 Anstaltsführungen

Nach Auskunft der Justizvollzugsanstalt finden derzeit - entgegen früherer Praxis - nur noch Führungen für Gruppen mit berufsspezifischen Interessen (etwa für Richter, Staatsanwälte, Schöffen usw.) statt. Für allgemein Interessierte, wie etwa Schulklassen, fänden Vorträge, bei denen auch Lichtbilder gezeigt würden, statt. Wolle man eine Zelle besichtigen, werde der betroffene Gefangene zuvor gefragt, ob er mit der Besichtigung einverstanden sei. Zu diesem Zeitpunkt stehe die Besuchergruppe aber bereits vor der Zellentüre.

Ich habe gegenüber der Justizvollzugsanstalt folgenden Verbesserungsvorschlag gemacht:

Wird der Gefangene erst in dem Moment, in dem die Besuchergruppe bereits vor seiner Zellentüre steht, gefragt, ob er gegen eine Besichtigung seiner Zelle etwas einzuwenden habe, so kann er unter einem nicht unerheblichen psychologischen Druck stehen, sich einer Besichtigung nicht zu widersetzen. Der betroffene Gefangene sollte deshalb bereits einige Zeit vor Beginn der Besichtigung gefragt werden. Im übrigen sollten die Gefangenen bei Anstaltsbesichtigungen im Rahmen des Möglichen vorab darüber in Kenntnis gesetzt werden, wann und in welchem

Bereich der Anstalt Führungen stattfinden, so daß es ihnen möglich ist, sich der Besichtigung tatsächlich zu entziehen.

7.4 Offene Versendung von Abgabenachrichten im Strafverfahren

Ein Bürger hat sich an mich gewandt und mir in Ablichtung eine Abgabenachricht übersandt, mit der ihm die Abgabe seiner Strafanzeige durch ein bayerisches Amtsgericht an eine bayerische Staatsanwaltschaft mitgeteilt wird. Aus der Abgabenachricht, die als Postkarte ohne Umschlag zur Post gegeben wurde, ergibt sich neben dem Aktenzeichen des Verfahrens, daß es sich um eine Strafanzeige handelt, wer Beschuldigter ist und wer die Anzeige erstattet hat.

Ich habe das Amtsgericht um Stellungnahme gebeten, weshalb die Abgabenachricht trotz der darin enthaltenen sensiblen personenbezogenen Daten als Postkarte und nicht im verschlossenen Umschlag an den Anzeigeerstatter versandt wurde. Darüber hinaus habe ich das Staatsministerium der Justiz von dem Vorgang in Kenntnis gesetzt.

Das Justizministerium hat mir auf der Grundlage eines Berichts des Direktors des Amtsgerichts mitgeteilt, daß Abgabenachrichten grundsätzlich im verschlossenen Briefumschlag versandt würden. Im vorliegenden Falle habe es sich um ein Versehen des Vertreters des zuständigen Beamten gehandelt. Da die Eingabe jedoch über den Einzelfall hinaus Bedeutung haben könne, **sei sie zum Anlaß genommen worden, die nachgeordneten Behörden darauf hinzuweisen, daß Abgabenachrichten, in denen personenbezogene Daten enthalten sind, aus Datenschutzgründen im verschlossenen Umschlag zu versenden sind.**

Das datenschutzrechtlich erforderliche wurde damit veranlaßt.

7.5 Überwachung des Zahlungseingangs bei Verfahrenseinstellung gern. § 153 a StPO

Bereits in meinem *15.* Tätigkeitsbericht (Ziffer 6.8.4) habe ich mich dagegen ausgesprochen, daß bei Einstellung eines Verfahrens gegen Erfüllung einer Geldauflage zugunsten einer gemeinnützigen Einrichtung regelmäßig in Kauf genommen wird, daß die gemeinnützige Einrichtung nicht nur von dem Strafverfahren, **sondern auch von der Person des Beschuldigten** Kenntnis erlangt.

Das Staatsministerium der Justiz hält diese Datenübermittlung weiterhin unter Berufung auf § 153 a Abs. 1 Nr. 2 StPO für gerechtfertigt. Sofern der Beschuldigte der Verfahrenseinstellung zustimme, rechne er auch mit einer Bekanntgabe seines Namens an den Zahlungsempfänger, so daß von seinem Einverständnis zur Datenübermittlung ausgegangen werden könne.

Diese Auffassung kann ich nicht teilen. Auch die Justizverwaltungen selbst sehen hier einen Handlungsbedarf und wollen die bisherige Praxis durch eine Gesetzesänderung absichern.

Zur datenschutzkonformen Lösung des Problems wurden von den Beauftragten für den Datenschutz im wesentlichen zwei Modelle diskutiert:

Zum einen die sogenannte „Pool-Lösung", die offensichtlich bereits von der Freien Hansestadt Bremen praktiziert und auch von einem Teil der Datenschutzbeauftragten befürwortet wird. Danach sollen Zahlungen des Betroffenen an die Gerichtskasse erfolgen und von dort aus die summenmäßig zusammengefaßten Beträge an die jeweiligen gemeinnützigen Organisationen weitergeleitet werden. Wegen des nicht unerheblichen zusätzlichen Aufwands für die Justizbehörden habe ich Bedenken hinsichtlich der Praktikabilität dieser Lösung.

Ich habe mich deshalb für eine Lösung ausgesprochen, die es dem Beschuldigten freistellt, seinen Namen auf dem Zahlungsbeleg gegenüber der gemeinnützigen Einrichtung anzugeben oder nicht. Schwierigkeiten, die dadurch auftreten können, daß der Beleg für den Zahlungsempfänger nur noch das staatsanwaltschaftliche oder gerichtliche Aktenzeichen trägt und durch Verschreiben oder Zahlendreher Unklarheiten entstehen, sollten durch Rückfragen mit zumutbarem Aufwand beseitigt werden können.

In meiner Auffassung werde ich auch durch die bisherige Praxis bekräftigt. So weist das Justizministerium darauf hin, daß es dem Betroffenen freistehe, eigene Überweisungsformulare zu verwenden und diese so auszufüllen, wie er es für richtig hält. Auch Überweisungsformulare, die von den gemeinnützigen Einrichtungen oder von Staatsanwaltschaft und Gericht zur Verfügung gestellt werden, enthalten noch keine Eintragungen personenbezogener Daten. Eingetragen sind allenfalls die zuständige Staatsanwaltschaft bzw. das Gericht, das Aktenzeichen und die Tatsache, daß es sich um eine Geldauflage handelt. Die übrigen Eintragungen, also insbesondere seinen Namen und seine Anschrift nimmt der Beschuldigte selbst vor, so daß er es in der Hand hat, ob er dem Zahlungsempfänger seinen Namen mitteilt oder nicht.

Ich meine, daß damit den datenschutzrechtlichen Anforderungen Rechnung getragen wird.

7.6 Übersendung von Lichtbildern bei Verkehrs-Ordnungswidrigkeiten

Der Datenschutzbeauftragte eines anderen Landes hat mir mitgeteilt, daß das Innenministerium seines Landes beabsichtige, bei Verkehrs-Ordnungswidrigkeiten - soweit vorhanden - bereits mit der Anhörung des Fahrzeughalters ein Lichtbild des Fahrzeugführers zu übersenden. Dies solle aus Gründen der Verfahrensökonomie und nicht zuletzt zur Verringerung der Einsprüche im Bußgeldverfahren geschehen.

Auf Anfrage hat mir das Staatsministerium des Innern mitgeteilt, daß bei Geschwindigkeitsübertretungen auch in

Bayern bereits vor längerer Zeit versuchsweise die Lichtbilder des Fahrers dem Anhörungsbogen beigegeben wurden. Nach der Bewertung des Staatsministeriums des Innern hat der Versuch jedoch kein positives Ergebnis gebracht. So seien nicht nur höhere Kosten dadurch verursacht worden, daß sämtliche Negative mit den Fahrerfotos hätten entwickelt werden müssen. Darüber hinaus habe das Innenministerium auch datenschutzrechtliche Bedenken gehabt, weil Mitinsassen auf den Lichtbildern erkennbar gewesen seien. Ohnehin würde in etwa 90 bis 95 % aller Fälle die Fahrereigenschaft vom Fahrzeughalter nicht bestritten.

Ich bewerte die Übersendung von Lichtbildern an den Fahrzeughalter wie folgt: Die Übermittlung personenbezogener Daten an nichtöffentliche Stellen setzt nach dem Bayerischen Datenschutzgesetz (Art. 19 Abs. 1 Nr. 1 BayDSG) u.a. voraus, daß die Datenübermittlung zur Erfüllung der Aufgaben der übermittelnden Stelle **erforderlich** ist Da nach der Erfahrung jedoch in der ganz überwiegenden Mehrzahl der Fälle die Fahrereigenschaft nicht bestritten wird und stets die Gefahr besteht, daß personenbezogene Daten Dritter (Mitinsassen im Fahrzeug) bekannt werden, halte ich die regelmäßige Übersendung von Lichtbildern bereits mit dem Anhörungsbogen mangels Erforderlichkeit datenschutzrechtlich für nicht zulässig. Dies habe ich dem anfragenden Kollegen mitgeteilt.

7.7 Zustellung von Pfändungs- und Überweisungsbeschlüssen durch Gerichtsvollzieher

Die Regierung von Mittelfranken hat mir zur Kenntnis gebracht, daß sich Datenschutzbeauftragte und Personalleiter von Unternehmen darüber beschwert hätten, daß Gerichtsvollzieher **Pfändungs- und Überweisungsbeschlüsse** bei Unternehmen zum Zweck der Zustellung **an der Pforte, beim Hausmeister** oder sonstigen Beschäftigten **offen** übergeben würden, statt diese ins Personalbüro zu bringen. Dies sei im Hinblick auf die in den Pfändungs- und Überweisungsbeschlüssen enthaltenen sensiblen Informationen über den Betroffenen nicht mit dem Datenschutzrecht vereinbar. Ich teilte diese Ansicht und habe das Staatsministerium der Justiz hierzu um Stellungnahme gebeten.

Das Justizministerium hat mir mitgeteilt, daß die Geschäftsanweisung für die Gerichtsvollzieher dahingehend geändert worden ist, daß bei der Ersatzzustellung das zuzustellende Schriftstück nur dann nicht verschlossen zu werden braucht, wenn der Ersatzempfänger zur Abgabe der Drittschuldnererklärung befugt ist. Eine offene Übergabe an die oben Genannten scheidet damit regelmäßig aus. Ich begrüße dies als eine deutliche Verbesserung des Datenschutzes bei der Zustellung von Pfändungs- und Überweisungsbeschlüssen.

7.8 Vollzugsmitteilungen durch Notare bei Grundstücksveräußerungen

Ein Bürger brachte mir folgenden Sachverhalt zur Kenntnis:

Der Petent veräußerte einen Teil seines Grundstücks zur Errichtung eines Bürgersteigs an eine bayerische Gemeinde. Er erhielt darauf hin sowohl vom zuständigen Grundbuchamt als auch vom beurkundenden Notariat Mitteilungen über die vollzogenen Grundbucheintragungen. Während das Grundbuchamt nur einen Auszug der den jeweiligen Verkäufer betreffenden Eintragungen übersandte, **wurden vom Notariat auch Grundbucheintragungen betreffend den Nachbarn,** der ebenfalls ein Teilgrundstück an die Gemeinde veräußert hatte, **übermittelt.** Ersichtlich waren auch die jeweiligen Belastungen des Nachbargrundstücks mit Grundpfandrechten.

Ich halte solche ,,gemeinschaftliche" Volizugsmitteilungen, die mehrere gesonderte Erwerbsvorgänge betreffen, für datenschutzrechtlich unzulässig. Auf meine Bitte um Stellungnahme teilte mir das betreffende Notariat mit, daß zwischenzeitlich das dortige Personal angewiesen worden sei, künftig bei zusammengefaßten Vollzugsmitteilungen des Grundbuchamts, die mehrere gesonderte Erwerbsvorgänge betreffen, diese nicht in Kopie an die Beteiligten weiterzugeben, sondern zur Wahrung des Datenschutzes den Urkundenvollzug auf andere geeignete Weise getrennt mitzuteilen.

Ich habe auch die Landesnotarkammer Bayern und das Staatsministerium der Justiz - ohne Personenbezug -vom Sachverhalt unterrichtet und - da diese Praxis möglicherweise auch in anderen bayerischen Notariaten besteht - anheimgestellt, die datenschutzrechtliche Problematik in geeigneter Weise an die Notariate in Bayern heranzutragen. Die Landesnotarkammer Bayern hat in Aussicht gestellt, die Notare auf die Problematik besonders hinzuweisen.

7.9 Gefangeneneingaben

7.9.1 Datenübermittlung durch die Justizvollzugsanstalt an Vollstreckungsgläubiger

Ein Strafgefangener einer bayerischen Justizvollzugsanstalt hat sich an mich gewandt und sich darüber beschwert, daß die Anstalt gegen seinen erklärten Willen ihn betreffende Daten an zwei Gläubiger mitgeteilt habe.

Meine Überprüfung ergab, daß der eine Gläubiger lediglich die Auskunft erhalten hatte, der Petent sitze in der Justizvollzugsanstalt ein und werde in absehbarer Zeit nicht entlassen, dem anderen Gläubiger aber zusätzlich der voraussichtliche Entlassungstermin mitgeteilt worden war. Weitere Auskünfte, insbesondere die Entlassungsanschrift hatte die Anstalt nicht gegeben. Beide Gläubiger hatten ihr Interesse an einer Auskunftserteilung durch Vorlage von Vollstreckungstiteln dargetan.

Die Auskunft an den ersten Gläubiger ist datenschutzrechtlich nicht zu beanstanden. Auch gegen den Willen des Gefangenen war die Justizvollzugsanstalt berechtigt, dem Gläubiger, der ein rechtliches Interesse an einer Auskunftserteilung dargetan hatte, die erteilte Auskunft zu

geben. In dieser Auffassung sehe ich mich durch § 113 Abs. 6 des Referentenentwurfs eines Jugendvollzugsgesetzes bestärkt, wonach von der Anstalt mitgeteilt werden darf, ob sich eine Person in der Anstalt befindet und ob die Entlassung voraussichtlich innerhalb eines Jahres bevorsteht.

Wegen der Mitteilung des voraussichtlichen Entlassungstermins an den zweiten Gläubiger habe ich datenschutzrechtliche Bedenken erhoben. Gerade bei längeren Haftstrafen (ein solcher Fall lag hier offensichtlich vor) dürfen aus der Auskunftserteilung an den Gläubiger ,keine Rückschlüsse auf die Haftdauer möglich sein. Die Mitteilung des Entlassungstermins halte ich deshalb jedenfalls dann für unzulässig, wenn die Entlassung nicht in absehbarer Zeit bevorsteht.
Da das Staatsministerium der Justiz den Standpunkt vertritt, daß Justizvollzugsanstalten den Gläubigern auf Anfrage auch den voraussichtlichen Entlassungstermin mitteilen dürfen, habe ich die Eingabe zum Anlaß genommen, meinen Standpunkt gegenüber dem Justizministerium nochmals zu bekräftigen.
Dabei habe ich auch darauf hingewiesen, daß ich bei der Prüfung einer anderen Justizvollzugsanstalt festgestellt habe, daß dort aufgrund einer entsprechenden Dienstanweisung der Entlassungszeitpunkt nur dann mitgeteilt wird , wenn er innerhalb des nächsten Monats liegt (siehe Prüfung einer JVA, Ziff. 7.3.3.2). Dieses Verfahren sollte auch bei den anderen Justizvollzugsanstalten möglich sein.

Ich werde die Angelegenheit weiter verfolgen.

7.9.2 Anstaltsführungen

Im Berichtszeitraum haben sich zwei Strafgefangene darüber beschwert, daß bei **Führungen in Justizvollzugsanstalten** datenschutzrechtliche Belange der Gefangenen nicht ausreichend berücksichtigt würden.

1. Ein Strafgefangener hat bemängelt, daß die Gefangenen bei Führungen in der Anstalt einer ,,Besichtigung" durch die Besucher ausgesetzt seien und aufgrund der an den Hafträumen angebrachten Namensschilder, auf denen auch die sog. Gefangenenbuchnummer angebracht ist, die Identität und Haftdauer des Gefangenen erkennbar sei. Darüber hinaus sei aufgrund der an der Zelle angebrachten Schilder ,,Arrest" oder ,,Spital" sowohl für Anstaltsbesucher als auch für Mitgefangene ersichtlich, daß ein Gefangener eine Disziplinarmaßnahme verbüße oder in das Anstaltskrankenhaus verlegt worden sei.

   Nach Auskunft der Justizvollzugsanstalt wird bei denjenigen Gefangenen, die dies wünschen, vor Beginn von Anstaltsführungen das Namensschild vom Haftraum entfernt. Falls ein Gefangener Arrest als Disziplinarmaßnahme zu verbüßen habe oder sich im Anstaltskrankenhaus befinde, werde das Namensschild beim Haftraum des Gefangenen abgenommen und **anstelle des Namensschildes** das Schild ,,Arrest" oder ,,Spital" am Haftraum des Gefangenen angebracht. Dadurch sei es den Bediensteten möglich, sofort zu erkennen, wo sich der Gefangene vorübergehend auffällt und z.B. Briefe oder Zeitungen weiterzuleiten sowie insbesondere zu vermeiden, daß die Zelle aus Versehen aufgesperrt wird und die dort befindliche Habe des Gefangenen Dritten zugänglich wird.

   Es ist datenschutzrechtlich zu begrüßen, daß auf Wunsch des Gefangenen bei Anstaltsführungen das Haftraumschild entfernt wird. Hinsichtlich der Schilder ,,Arrest" bzw. ,,Spital" am Haftraum des Gefangenen habe ich die Justizvollzugsanstalt noch um ergänzende Stellungnahme gebeten, weshalb es zur Unterrichtung der Bediensteten nicht ausreiche, wenn auf dem Geschäftszimmer der betreffenden Station vermerkt wird, welcher Gefangene sich in Arrest oder im Spital befindet. Die Anstalt hält die Schilder am Haftraum für erforderlich: Eine Information der Bediensteten durch die Aufzeichnungen in den Stationszimmern sei nicht ausreichend, da sich täglich zahlreiche Änderungen ergäben, die die Beamten nicht immer zuverlässig ,,im Kopf" behalten könnten. Es bedürfe daher eines Hinweises ,,vor Ort", also am Haftraum. Diese Argumentation überzeugt mich. Darüber hinaus habe ich zur Verbesserung des Datenschutzes angeregt, daß die Gefangenen im Falle von Anstaltsbesichtigungen so frühzeitig darüber informiert werden, in welchen Häusern der Anstalt und zu welchem voraussichtlichen Zeitpunkt die Führungen stattfinden, daß sie die Möglichkeit haben, sich einer ,,Besichtigung" tatsächlich zu entziehen. Die Anstalt hat zugesagt, daß künftig entsprechend meinen Vorschlägen verfahren wird.

2. Ein Gefangener einer anderen Justizvollzugsanstalt hat sich dagegen gewandt, daß bei Anstaltsführungen nicht vorher die Namensschilder an den Hafträumen der Gefangenen entfernt worden seien. Darüber hinaus habe eine Besuchergruppe den Fernsehraum der Gefangenen, in dem sich auch Gefangene befunden hätten, ,,in Augenschein genommen".

   Die Anstalt hat dahingehend Stellung genommen, daß ein Abdecken oder Entfernen der Haftraumschilder zu einem unvertretbaren Verwaltungsaufwand führen würde. Außerdem werde darauf geachtet, daß Besichtigungen der Hafträume nur während der Arbeitszeit stattfinden, so daß sich kaum Gefangene in den Zellen aufhalten.

   Ich habe auch diese Justizvollzugsanstalt gebeten, Ort und Zeit von Anstaltsbesichtigungen den Gefangenen vorab rechtzeitig mitzuteilen. Darüber hinaus soll ein Abdecken der Namensschilder am Haftraum vor Anstaltsführungen grundsätzlich auf Wunsch des einzelnen Gefangenen ermöglicht werden. Dies könne ggf. auch durch den jeweiligen Gefangenen selbst erledigt werden.

7.9.3 Untersuchungen im Anstaltskrankenhaus

Ein Gefangener hat sich darüber beschwert, daß bei Untersuchungen im Anstaltskrankenhaus die Trennungstüren zweier benachbarter Behandlungsräume nicht geschlossen würden, so daß Personen im Nebenraum vom Gesprächsinhalt (z.B. Untersuchungsbefunden) Kenntnis nehmen könnten.

Der Leiter der Justizvollzugsanstalt hat dazu mitgeteilt, daß er die Anstaltsärzte gebeten habe, darauf zu achten, daß die Trennungstüre zwischen den beiden Behandlungsräumen während der Untersuchungen nicht geöffnet bleibt.

7.9.4 Briefkontrolle

Im 14. Tätigkeitsbericht (Ziff. 6.8.5.2) habe ich ausführlich über die Praxis bayerischer Justizvollzugsanstalten berichtet, bei auslaufenden Schreiben des Strafgefangenen zur Dokumentation der Briefkontrolle einen Sichtvermerk mit Datumsstempel und Handzeichen des kontrollierenden Bediensteten anzubringen.

Das Justizministerium hat nunmehr mitgeteilt, daß künftig **in der Regel auf Sichtvermerke verzichtet wird,** außer in Anstalten, in denen aufgrund von Sicherheitserwägungen daran festzuhalten ist.

Ich begrüße diese Änderung der Praxis. Ich meine jedoch, daß auch in diesen Fällen im Einzelfall von dem Sichtvermerk abgesehen werden sollte, wenn der Gefangene djes unter Darlegung eines berechtigten Interesses beantragt oder aus dem Inhalt des Schreibens ersichtlich ist, daß ein Sichtvermerk untunlich ist (z.B. bei Bewerbungsschreiben des Gefangenen).

7.9.5 Besucherüberprüfung

Bereits im 14. Tätigkeitsbericht (Ziff. 6.8.6) und erneut im 15. Tätigkeitsbericht (Ziff. 6.9.2.4) habe ich Bedenken gegen die Praxis der Justizvollzugsanstalten hinsichtlich der Überprüfung von Besuchern geäußert: Eine polizeiliche Überprüfung der von Gefangenen auf die Besucherliste gesetzten Personen **ohne deren Wissen** bedarf angesichts des damit verbundenen Eingriffs in das Recht auf informationelle Selbstbestimmung einer ausreichenden gesetzlichen Grundlage, die jedenfalls derzeit nicht besteht.

Ich habe daher gefordert, vorerst wie folgt zu verfahren: Die vom Gefangenen als Besucher benannten Personen werden davon unterrichtet, daß der Gefangene beantragt hat, sie in die Besucherliste aufzunehmen und sie deshalb überprüft werden sollen. Die Besucher können sich sodann entscheiden, ob sie den Gefangenen tatsächlich besuchen wollen und deshalb mit einer Überprüfung einverstanden sind.

Das Justizministerium hat nunmehr zugesagt, daß entsprechend meinen Vorstellungen verfahren wird.

8. Landkreise, Städte und Gemeinden

8.1 Prüfung eines Landratsamtes

Bei der Prüfung eines Landratsamtes mußte ich folgendes feststellen:

1. **Gewerbewesen**

   Im Sachgebiet ,,Gewerbewesen" waren verschiedene Dateien vorhanden, beispielsweise über alle nach §34 c GewO erteilten (Makler-)Erlaubnisse und über alle erteilten Reisegewerbekarten. Zum Zeitpunkt der Prüfung war erst eine Datei daraufhin durchgesehen worden, ob die gespeicherten Datensätze noch zur Aufgabenerfüllung benötigt werden (vgl. Art. 12 Abs.1 Nr.2, Art. 17 Abs. 1 Nr.1 BayDSG). Auch bei **Dateien** ist gemäß der allgemeinen Aussonderungsbekanntmachung (AllMBl Nr.28/1991, Seiten 884 ff.) eine Aussonderung **durchzuführen.**

2. **Verstöße gegen die Datensicherheit**

   - Im Sachgebiet ,,Öffentliche Sicherheit und Ordnung" wurde die Waffenbesitzkartei in einem nichtverschließbaren Holzschrank aufbewahrt, obwohl ein verschließbarer Stahlschrank mit ausreichendem Platz vorhanden war.
   - Bei keinem der verwendeten Personalcomputer, auf denen personenbezogene Daten verarbeitet werden, war eine Zugriffssicherung vorhanden.

     Dieser Mangel ist besonders unverständlich, da ich seit Jahren in meinen Tätigkeitsberichten ausführliche Hinweise zur Sicherheit bei Personalcomputern gebe.

8.2 Übersendung von Sitzungsprotokollen

Ein Landkreis hat mich um datenschutzrechtliche Überprüfung gebeten, ob die Übersendung der Niederschriften über die **öffentlichen und nichtöffentlichen** Sitzungen des Kreistages, des Kreisausschusses und weiterer beschließender Ausschüsse an die Kreistags- bzw. Ausschußmitglieder zulässig sei. Innerhalb des Landratsamtes erfolge eine automatische Zuleitung dieser Niederschriften an die Abteilungsleiter sowie an das Kreisrevisionsamt.

Mit dem Staatsministerium des Innern vertrete ich dazu folgende Auffassung:

1. **Übersendung der Niederschriften über die Sitzungen des Kreistages und seiner Ausschüsse an die Kreisräte**

1.1 **Öffentliche Sitzungen**

Die Landkreisordnung enthält keine Vorschrift, aus der sich eine Pflicht zur Herausgabe von Niederschriften der Sitzungen des Kreistages und seiner Ausschüsse an die Kreisräte ergibt. Art. 48 Abs. 2 Satz 1 der

Landkreisordnung (LKrO) sieht neben dem Einsichtsrecht lediglich vor, daß sich die Kreisräte Abschriften der in **öffentlicher** Sitzung gefaßten **Beschlüsse** erteilen lassen können. Diese Vorschrift legt allerdings nur einen Mindeststandard fest. Der Kreistag ist nicht gehindert, in der Geschäftsordnung zu regeln, daß Abschriften der jeweiligen Niederschriften öffentlicher Sitzungen zur Verfügung gestellt werden.

1.2 **Nichtöffentliche Sitzungen**

Niederschriften über **nichtöffentliche** Sitzungen sind hingegen aus Gründen der Gewährleistung der Geheimhaltung und des Datenschutzes in der Regel nicht geeignet, vervielfältigt und versandt zu werden.

Niederschriften, die Privatgeheimnisse im Sinne des § 203 Abs. 2 des Strafgesetzbuches oder personenbezogene Daten im Sinne des Art. 5 des Bayerischen Datenschutzgesetzes enthalten, dürfen nur dann herausgegeben werden, wenn dies zur Erfüllung der den Mitgliedern zugewiesenen Aufgaben unbedingt erforderlich ist. Da dies in der Regel nicht der Fall ist, kommt die Überlassung von Niederschriften nichtöffentlicher Sitzungen deshalb grundsätzlich nicht in Betracht.

Aber selbst dann, wenn strafrechtliche Bestimmungen nicht entgegenstehen, kann nicht empfohlen werden, Niederschriften nichtöffentlicher Sitzungen an die jeweiligen Mitglieder herauszugeben. Die Mitglieder sind zwar gehalten, über die ihnen bei ihrer ehrenamtlichen Tätigkeit bekannt gewordenen Angelegenheiten Verschwiegenheit zu bewahren (vgl. z.B. Art. 14 Abs. 2 Satz 1 LKrO). Gleichwohl hat sich in der Vergangenheit wiederholt gezeigt, daß trotz dieser Verschwiegenheitspflicht vertraulich zugegangene Unterlagen Dritten zur Kenntnis gelangt sind. Um die schutzwürdigen Interessen, die zur nichtöffentlichen Sitzung geführt haben, nicht zu gefährden, sollten deshalb Protokolle nichtöffentlicher Sitzungen auch in diesen Fällen nicht herausgegeben werden.

Das Informationsrecht der Kreisräte wird damit nicht beschnitten. Kreisräte können jederzeit Einsicht in die Niederschriften, auch der nichtöffentlichen Sitzungen, nehmen (vgl. Art. 48 Abs. 2 Satz 1 LKrO). Zudem kann etwa das Protokoll über den nichtöffentlichen Teil der vorangegangenen Sitzung während der Dauer der Sitzung aufgelegt oder in Umlauf gesetzt werden. Ferner bestehen gegen die Erteilung von Abschriften des Textes des Beschlusses (und nur insoweit) keine Bedenken, wenn die Gründe für die Geheimhaltung weggefallen sind (Art. 46 Abs. 3 LKrO; vgl. auch § 36 Abs. 2 Satz 2 der Mustergeschäftsordnung für Gemeinderäte, IMBek. vom 20.02.1990, AllMBl. 1990, S.291). Durch diese Möglichkeiten ist sichergestellt, daß die Kreisräte über eine ausreichende Informationsgrundlage für eine verantwortungsvolle Ausübung ihres Mandats verfügen.

2. **Übersendung der Niederschriften über Sitzungen des Kreistages und seiner Ausschüsse an Bedienstete des Landratsamtes**

Der Landrat hat (ebenso wie die Kreisräte) über die bei seiner amtlichen Tätigkeit bekannt gewordenen Angelegenheiten Verschwiegenheit zu bewahren (Art. 40 KWBG, Art. 14 Abs. 2 LKrO). Dieser Grundsatz ist auch bei Mitteilungen an Bedienstete zu beachten.

Vom Grundsatz der Verschwiegenheitspflicht sehen die genannten Vorschriften jedoch Ausnahmen vor. Die Verschwiegenheitspflicht besteht danach nicht für ,,Mitteilungen im amtlichen Verkehr" oder für Tatsachen, die offenkundig sind oder ihrer Bedeutung nach keiner Geheirahaltung bedürfen (Art. 14 Abs. 2 LKrO, Art. 40 Abs. 1 KWBG). Im Hinblick auf den allgemeinen Schutzgedanken des Bayerischen Datenschutzgesetzes, der zur Bestimmung des Umfangs der Verschwiegenheitspflicht heranzuziehen ist, ist danach die **Weitergabe personenbezogener Daten insoweit zulässig, als die Kenntnis dieser Daten für die Verwaltung zur Erfüllung ihrer Dienstaufgaben erforderlich ist.** Unter der gleichen Voraussetzung ist die Weitergabe von anderen Daten, die der Geheimhaltung unterliegen, z.B. Betriebs- und/oder Geschäftsgeheimnisse (vgl. Art. 30 BayVwVfG) zulässig. Es bestehen daher keine Einwände, wenn die Protokolle unter Beachtung dieses Grundsatzes an die jeweils zuständigen Abteilungen versandt werden. **Die regelmäßige Weitergabe sämtlicher Protokolle an das Rechnungsprüfungsamt halte ich allerdings nicht für erforderlich und deshalb für unzulässig. Ich** verweise dazu auf die Ausführungen im 14. Tätigkeitsbericht 1992 (Nr. 7.12) und im *15.* Tätigkeitsbericht 1993 (Nr. 11.10).

8.3 Weitergabe der Tagesordnung einer Gemeinderatssitzung an die Presse

Im 14. Tätigkeitsbericht habe ich unter Nr.7.3 dargestellt, daß die Aushändigung der Tagesordnungen öffentlicher Sitzungen an die Presse aus datenschutzrechtlicher Sicht nicht zu beanstanden ist. Eine Stadt fragte nun, aus welchen Gründen die **Tagesordnungen nichtöffentlicher Sitzungen** der Presse **nicht** bekanntgegeben werden dürfen.

Nach Art. 52 Abs. 2 Gemeindeordnung sind die Sitzungen nichtöffentlich, soweit Rücksichten auf das Wohl der Allgemeinheit oder auf berechtigte Ansprüche einzelner dies erfordern. Aus diesen Gründen wird auch die Tagesordnung nichtöffentlicher Sitzungen nicht bekanntgegeben. So könnten bereits aus der bloßen Erwähnung von Beratungsgegenständen (z.B. Flurnamen bei Grundstücksangelegenheiten) in der Bevölkerung Schlüsse auf Pläne

und Absichten der Gemeindeverwaltung gezogen werden und diese gemeindlichen Pläne und Absichten dadurch erschwert oder gar durchkreuzt werden. Ebenso könnten durch die bloße Erwähnung von in nichtöffentlicher Sitzung zu behandelnden Beratungsgegenständen schutzwürdige Belange Privater betroffen sein. Davon abgesehen liegt der Sinn der Bekanntgabe der Tagesordnung darin, daß Gemeindeeinwohner, die an einem Tagesordnungspunkt interessiert sind, bei der Beratung zuhören können. Ist aber die Sitzung bei diesem Tagesordnungspunkt nichtöffentlich, so entfällt dieser Zweck.

8.4 Bekanntgabe von personenbezogenen Daten durch den ersten Bürgermeister in öffentlicher Gemeinderatssitzung

Ein Bürger beschwerte sich, daß der erste Bürgermeister in einer öffentlichen Gemeinderatssitzung nähere Angaben zu seiner Person gemacht hatte. Der Bürger hatte anläßlich einer Bürgerversammlung um eine Stellungnahme zu den Kosten einer Anbindungsstraße von einem Wohngebiet an eine Bundesstraße und zu Presseartikeln gebeten, in denen über die Haltung des ersten Bürgermeisters und des Gemeinderates zu dieser Anbindungsstraße berichtet wurde.

Bei der Behandlung dieser Anfrage in öffentlicher Gemeinderatssitzung teilte der erste Bürgermeister auf einen Zwischenruf hin mit, wer der Anfragende sei, wann der Petent in die Gemeinde zugezogen war und von wem er sein Grundstück erworben hatte. Die Weitergabe der Daten über den Zuzug des Petenten und den Grundstückserwerb war aus dem folgenden Grund unzulässig:

Der erste Bürgermeister ist nach Art. 46 Abs. 2 Gemeindeordnung verpflichtet, die Beratungsgegenstände für den Gemeinderat vorzubereiten. Dies bedeutet u.a., daß er dem Gemeinderat alle Daten und Informationen zu einem Beratungsgegenstand mitteilt, **die für die Beratung und Beschlußfassung des Gemeinderates erforderlich sind.** Für die Behandlung einer Anfrage über die Kosten einer Straße bzw. über die Haltung des Gemeinderates zu einer solchen Straße ist es erforderlich, daß der Gemeinderat über den Namen und die Anschrift des Anfragenden informiert wird, um beurteilen zu können, ob und in welcher Weise er von der Straße betroffen ist. Wie lange der Anfragende bereits in der Gemeinde wohnt oder von wem er sein Grundstück gekauft hat, sind dagegen keine Daten, die zur Beratung und zur Beschlußfassung über eine solche Anfrage erforderlich sind.

8.5 Einsichtnahme in Unterschriftenlisten durch Dritte

In einer Gemeinde wurde gegen die Aufstellung eines Bebauungsplans eine Unterschriftenaktion durchgeführt. In die bei der Gemeinde eingereichten Unterschriftenlisten hat ein interessierter Bürger Einsicht genommen. Zur Rechtfertigung verwies die Gemeinde auf die Auslegung der Wählerverzeichnisse zur öffentlichen Einsichtnahme. Außerdem hat der erste Bürgermeister den Mitgliedern des Gemeinderats die Namen der Unterzeichner der Listen mitgeteilt.

Die Einsichtnahme in die Unterschriftenlisten war nach Art. 4 Abs. 6 Nr.3 b BayDSG eine Übermittlung personenbezogener Daten an Dritte. Die Übermittlung war unzulässig, weil dafür weder eine Rechtsgrundlage gegeben war noch der Betroffene eingewilligt hatte (Art. 15 Abs. 1 BayDSG).

Eine Einwilligung der Unterzeichner der Unterschriftenlisten zur Einsichtnahme durch Dritte in die Listen lag nicht vor. Auch nach Art. 40 Abs. 1 des Gesetzes über Kommunale Wahlbeamte, der als Überprüfungsmaßstab heranzuziehen war, war die Einsichtnahme durch den Dritten in die Unterschriftenlisten nicht zulässig, weil sie im Rahmen des dienstlichen Verkehrs zur rechtmäßigen Erfüllung der gesetzlichen Aufgaben des ersten Bürgermeisters nicht erforderlich war.

Zur Rechtfertigung der Einsichtnahme in die Unterschriftenlisten durch einen Dritten konnte auch nicht auf die Wählerverzeichnisse hingewiesen werden. Anlegung und Auslegung der Wählerverzeichnisse zur öffentlichen Einsichtnahme sind gesetzlich geregelt (vgl. §§ 12 ff. der Landeswahlordnung, §§ 2 ff. der Gemeindewahlordnung). Im Gegensatz zu obiger Unterschriftenliste wird mit der Eintragung in das Wählerverzeichnis nicht eine bestimmte Meinung des eingetragenen Bürgers zu einer kommunalpolitischen Frage kundgetan. Die Eintragung in die Wählerliste stellt damit keinen zu obiger Problematik vergleichbaren Sachverhalt dar.

Die Unterrichtung der Mitglieder des Gemeinderats über die Personen, die sich in die Unterschriftenlisten eingetragen hatten, war hingegen zulässig, weil es sich bei der Aufstellung eines Bebauungsplans um eine Angelegenheit von grundsätzlicher Bedeutung handelt, für die der Gemeinderat zuständig ist (Art. 29 und 37 der Gemeindeordnung).

8.6 Anhörung des Bayerischen Bauernverbandes bei Verfahren nach dem Grundstücksverkehrsgesetz; Weitergabe personenbezogener Daten vom Bayerischen Bauernverband an die Obmänner dieses Verbandes

Eine Stadt hat mich gefragt, ob der Bayerische Bauernverband im Rahmen seiner Anhörung nach dem Grundstücksverkehrsgesetz personenbezogene Daten, insbesondere den Kaufpreis, an die Obmänner des Bauernverbandes weitergeben darf.

Zur Anhörung des Bayerischen Bauernverbandes, der als landwirtschaftliche Berufsvertretung bei genehmigungspflichtigen Geschäften nach § 2 Grundstücksverkehrsgesetz (GrdstVG) vor der Entscheidung über den Genehmigungsantrag nach § 19 GrdstVG zu hören ist, ist es erforderlich, den Organen dieses Verbandes die Unterlagen zur Verfügung zu stellen, die für dessen Stellungnahme notwendig sind. Aus den Unterlagen sind die personen-

bezogenen Daten, die für die Stellungnahme nicht erforderlich sind, durch Schwärzen, Herauskopieren etc. vor der Weitergabe an den Bauernverband zu entfernen. Die Übermittlung des Kaufpreises ist für die Beurteilung eines etwaigen Versagungsgrundes im Sinne von § 9 Abs. 1 Nr.3 GrdstVG (grobes Mißverhältnis von Kaufpreis und Grundstückswert) erforderlich. In den Fällen, in denen nach § 8 GrdstVG die Genehmigung nach dem Grundstücksverkehrsgesetz erteilt werden muß, ist dem Bauernverband weder der Kaufvertrag noch ein Auszug daraus zu übersenden. Es genügt, den Bauernverband von dem Grundstücksgeschäft in Kenntnis zu setzen.

Eine Versagung nach § 9 Abs. 1 Nr.1 GrdstVG, weil die Veräußerung eine ungesunde Verteilung des Grundes und Bodens darstellt, oder Genehmigungsauflagen gemäß §10 Abs. 1 Nr.1 und 2 GrdstVG, das erworbene Grundstück an einen Landwirt zu verpachten und ganz oder teilweise zu angemessenen Bedingungen zu veräußern, kommen nur in Betracht, wenn überhaupt an diesem Grundstück interessierte Landwirte vorhanden sind. Hierzu bedarf es entsprechender Erhebungen der Organe des Bayerischen Bauernverbandes, was zwangsläufig zur Folge hat, daß die dazu nötigen Angaben etwaigen interessierten Landwirten zugänglich gemacht werden müssen (vgl. Art. 19 Abs. 1 Nr.1 BayDSG). Dies gilt auch für den Kaufpreis, da er für ein etwaiges Kaufinteresse entscheidungserheblich ist. Es läßt sich also nicht vermeiden, neben der Lage des Grundstücks, auch den Kaufpreis zu nennen. Allerdings darf der Kaufpreis gegenüber angesprochenen Landwirten nicht genannt werden, wenn diese bereits aus anderen Gründen, etwa wegen der Lage des Grundstücks, kein Interesse zeigen. Die in der Nennung des Kaufpreises liegende Datenübermittlung wäre in diesem Fall nicht erforderlich, damit unzulässig.

Die Erhebungen bei den Landwirten erfolgen durch die Ortsobmänner des Bayerischen Bauernverbandes. Diese sind satzungsmäßige Organe des Bayerischen Bauernverbandes, die die Daten für die Geschäftsstelle des Bayerischen Bauernverbandes nutzen. Gegen die Weitergabe personenbezogener Daten, insbesondere auch des Kaufpreises, vom Bayerischen Bauernverband an seine Ortsobmänner im Vollzug des Grundstücksverkehrsgesetzes bestehen daher unter den o.g. Voraussetzungen aus datenschutzrechtlicher Sicht keine Bedenken.

8.7 Postsendungen für den Umlegungsausschuß

Eine Stadt hat mich um Stellungnahme gebeten, ob die Postsendungen für den Umlegungsausschuß diesem ungeöffnet übergeben werden müssen.

In der Stadt ist der Umlegungsausschuß organisatorisch dem Stadtvermessungsamt zugeordnet. Schreiben an den Umlegungsausschuß gehen in der zentralen Posteinlaufstelle der Stadt ein, werden dort grundsätzlich geöffnet und in die Verteilstelle der Botenzentrale gebracht. Dort werden sie dem Stadtvermessungsamt zugeordnet und mit der gesamten Post des Stadtvermessungsamtes in das Vorzimmer dieser Dienststelle gebracht. Von dort werden die Schreiben, ggf. nach Kenntnisnahme durch den Leiter des Stadtvermessungsamtes, an die Geschäftsstelle des Umlegungsausschusses weitergeleitet.

Schreiben der Regierung und anderer übergeordneter Behörden werden von der Posteinlaufstelle grundsätzlich zunächst dem Referat ,,Oberbürgermeister" zur Kenntnisnahme zugeleitet und von dort entsprechend der Allgemeinen Geschäftsanweisung über das Baureferat an das Stadtvermessungsamt weitergeleitet.

Aus datenschutzrechtlicher Sicht vertrete ich folgende Auffassung:

1. **Öffnen der für den Umlegungsausschuß bestimmten Post in der Posteinlaufstelle der Stadt**

   Der Umlegungsausschuß nach § 46 Abs. 2 BauGB ist ein Organ der Gemeinde, das sich, wie auch die anderen Organe der Gemeinde, der Gemeindeverwaltung bedient (vgl. 11.1 und 11.4 der Richtlinien zum Umlegungsverfahren bei den Gemeinden nach dem Baugesetzbuch, Bekanntmachung des Bayer. Staatsministeriums des Innern vom 12. Dezember 1989, AllMBl 1990 S.4). Die an ihn adressierte Post nimmt die Posteinlaufstelle der Gemeinde entgegen, soweit in der Gemeinde keine andere Regelung besteht. Zum Verfahren bei den eingehenden Sendungen kann die Allgemeine Dienstordnung (ADO), die gem. § 1 für die bayerischen Behörden gilt, herangezogen werden:

   Nach § 9 Abs. 2 ADO ist bei Sendungen mit der Behördenanschrift und dem Zusatz ,,z. Hd. von" sicherzustellen, daß der bezeichnete Empfänger von ihnen Kenntnis erhält. Nach Satz 3 sind Sendungen mit der persönlichen Anschrift eines Behördenangehörigen diesem ungeöffnet auszuhändigen; enthalten sie dienstliche Mitteilungen, muß sie der Empfänger unverzüglich an die Eingangsstelle zurückgeben.

   Aus dem Wortlaut und der Systematik der Vorschrift ergibt sich daher, daß die Eingangsstelle Sendungen mit der persönlichen Anschrift eines Behördenangehörigen an diesen ungeöffnet weiterzureichen hat. Post, die den Zusatz ,,z. Hd. von" enthält, darf geöffnet werden.

   Darüber hinaus ist in weiteren Fällen aus datenschutzrechtlichen Gründen eine ungeöffnete Weitergabe der Post erforderlich. So müssen z. B. Beihilfeanträge, die von außen als solche erkennbar sind, ungeöffnet der Beihilfestelle zugeleitet werden, weil andernfalls Beschäftigte Kenntnis über sensible personenbezogene Daten von Beschäftigten derselben Dienststelle erhalten würden, und dies auch noch über einen längeren Zeitraum. Ungeöffnet bleiben z.B. auch Postsendungen an den Standesbeamten und an Ärzte in Krankenhäusern. Demgegenüber sind keine vergleichbaren schutzwürdigen Belange der Absender

von Schreiben an den Umlegungsausschuß oder Dritter ersichtlich, die einer Offnung dieser Schreiben in der Posteinlaufstelle entgegenstünden.

2. **Kenntnisnahme vom Inhalt von Postsendungen an den Umlegungsausschuß durch das Oberbürgermeisterreferat, das Baureferat und das Stadtvermessungsamt**

Nach Art. 4 Abs. 7 i.V.m. Art. 17 Abs. 1 BayDSG ist eine Kenntnisnahme des Inhalts der eingehenden Sendungen durch Bedienstete der Stadt zulässig, soweit das zu deren Aufgabenerfüllung erforderlich ist. Die Stadt hat die technischen und organisatorischen Maßnahmen zu treffen, daß keine Unbefugten vom Inhalt dieser Sendungen Kenntnis erhalten (Art. 7 Abs. 1 Satz 1 BayDSG).

Der Umlegungsausschuß ist für die Durchführung der Umlegung mit selbständigen Entscheidungsbefugnissen ausgestattet und hat sie in eigener Verantwortung durchzuführen. Er ist insoweit gegenüber dem Gemeinderat und der Gemeindeverwaltung weisungsunabhängig (vgl. § 4 Abs. 1 der Verordnung über die Umlegungsausschüsse und das Vorverfahren in Umlegungs- und Grenzregelungsangelegenheiten vom 18. Januar 1961, GVBl S.7; 11.1 der o.g. Bekanntmachung des Bayerischen Staatsministeriums des Innern). Bedienstete **der Gemeinde dürfen danach vom Inhalt der Sendungen für den Umlegungsausschuß Kenntnis nehmen, wenn sie Funktionen in diesem Ausschuß ausüben bzw. Hilfstätigkeiten für den Ausschuß ausführen** (vgl. 11.4 der o.g. Bekanntmachung des Innenministeriums). Die Postverteilung innerhalb des Umlegungsausschusses regelt dieser in eigener Zuständigkeit. So kann sich z.B. der Vorsitzende des Ausschusses, das ist, wenn nichts anderes geregelt ist, der erste Bürgermeister, den Posteinlauf oder auch nur bestimmte Schreiben vorlegen lassen. Im Hinblick auf die Weisungsunabhängigkeit des Umlegungsausschusses können jedoch Aufsichtsrechte und Leitungsfunktionen innerhalb der allgemeinen Verwaltungshierarchie (z.B. der Leiter eines Amtes über die ihm nachgeordneten Sachgebiete und Dienststellen) die Kenntnisnahme des Inhalts der Schreiben an den Umlegungsausschuß nicht rechtfertigen.

Eine Zuleitung an das Oberbürgermeisterreferat ist somit nur im oben genannten Fall gerechtfertigt; die regelmäßige Zuleitung an die übrigen oben erwähnten Nutzer und Stellen ist dagegen nicht zulässig.

8.8 Abgleich von Gästelisten und Kfz-Halterfeststellung zum Zweck der Kur- bzw. Fremdenverkehrsbeitragsfestsetzung

1. **Abgleich von Gästelisten**

Eine Stadt wollte wissen, ob sie beim örtlichen Kneipp- und Kurverein e.V. personenbezogene Daten über Gäste, z.B. aus Teilnehmerlisten an Ausflugsfahrten und Veranstaltungen, erheben darf, um die Angaben der Beherbergungsbetriebe im Rahmen des Vollzugs der Kur- bzw. Fremdenverkehrsbeitragssatzung auf Vollständigkeit und Richtigkeit zu überprüfen.

Nach Art. 16 Abs. 1 BayDSG ist die Datenerhebung zulässig, wenn ihre Kenntnis zur Erfüllung der in der Zuständigkeit der erhebenden Stelle liegenden Aufgaben erforderlich ist. Die Datenerhebung ist dann zur Aufgabenerfüllung erforderlich, wenn die Kenntnis der Daten zur Erreichung des Zwecks objektiv geeignet und im Verhältnis zum angestrebten Zweck auch als angemessen erscheint. Die personenbezogenen Daten sind darüber hinaus grundsätzlich beim Betroffenen mit seiner Kenntnis zu erheben (Art. 16 Abs. 2 Satz 1 BayDSG). Bei Dritten dürfen sie nur unter den in Art. 16 Abs. 2 Satz 2 BayDSG genannten Voraussetzungen erhoben werden.

Im vorliegenden Fall ist die Datenerhebung durch die Stadt beim örtlichen Kneipp- und Kurverein e.V. bereits nach Art. 16 Abs. 1 BayDSG aus den folgenden Gründen zur Aufgabenerfüllung der Stadt nicht erforderlich:

- **Datenerhebung zum Vollzug der Kurbeitragssatzung**

Ein Abgleich der Gästemeldescheine mit Unterlagen des Kneipp- und Kurvereins e.V. zum Vollzug der Kurbeitragssatzung mag zwar als zusätzliche Maßnahme zu Kontrollen in den einzelnen Beherbergungsbetrieben geeignet sein, um unterlassene Gästeanmeldungen im Einzelfall aufzudecken. Es ist jedoch unangemessen, die Unterlagen des Kneipp- und Kurvereins e.V. mit personenbezogenen Angaben über eine Vielzahl von Gästen verschiedener Beherbergungsbetriebe systematisch auszuwerten, um mögliche Verstöße gegen die Satzung im Einzelfall festzustellen.

Bei einer Einsichtnahme in die Unterlagen des Kneipp- und Kurvereins e.V. würde die Stadt Kenntnis davon erhalten, welche Personen sich mit welchem Anliegen an den Verein gewandt haben, z.B. wer wann, ggf. mit wem, an welcher Ausflugsfahrt und Veranstaltung teilgenommen hat. Der weitaus größte Teil der Betroffenen sind Personen, die sich ordnungsgemäß angemeldet haben und auch solche, die nicht kurbeitragspflichtig sind. Diese Personen haben ein schutzwürdiges Interesse daran, daß ihre personenbezogenen Daten über ihr Urlaubsverhalten nicht ohne ihre Einwilligung erhoben werden. Der von der Stadt mit dem Datenabgleich beim Kneipp- und Kurverein e.V. verfolgte Zweck, Verstöße gegen die Kurbeitragssatzung einzelner anderer Personen bzw. Beherbergungsbetriebe festzustellen, rechtfertigt diesen Eingriff nicht, da die Stadt die Möglichkeit hat, die Daten, die sie benötigt, direkt beim Betroffenen und den Beherbergungsbetrieben zu erheben und vor Ort zu kontrollieren. Eine derartige Verfahrensweise ist angemessen, da nur von den Gästen bzw. Inhabern von

Beherbergungsbetrieben (Vergleichs-) Daten erhoben werden müssen, bei denen Unstimmigkeiten zwischen den Gästemeldescheinen und den tatsächlichen Verhältnissen vor Ort aufgetreten sind.

- **Datenerhebung zum Vollzug der Fremdenverkehrsbeitragssatzung**

  Auch für den Vollzug der Fremdenverkehrsbeitragssatzung ist eine allgemeine Datenerhebung beim Kneipp- und Kurverein e.V. nach Art. 16 Abs. 1 BayDSG zur Aufgabenerfüllung der Stadt nicht erforderlich. Die Stadt würde von Personen Daten zur deren Urlaubsverhalten erheben, obwohl diese Personen nicht beitragspflichtig sind und damit die Angaben - anders als beim Kurbeitrag - nicht einmal direkt zur Kontrolle der Beitragsentrichtung dieser Personen herangezogen werden können. Für die Bemessung der Fremdenverkehrsbeitragsschuld nach der Satzung ist nur die Anzahl der Übernachtungen von Bedeutung. Daten zum Urlaubsverhalten, wie sie die Stadt durch die beabsichtigte Erhebung beim Kneipp- und Kurverein e.V. erhalten würde, sind zum Vollzug dieser Bestimmung nicht erforderlich. Die Stadt hat auch hier im Rahmen des Satzungsvollzugs die Möglichkeit, direkt vor Ort bei den Beherbergungsbetrieben zu kontrollieren.

2. **Kfz-Halterfeststellung**

Aufgrund von Bürgereingaben mußte ich feststellen, daß in einer Gemeinde zum Zwecke der Kurbeitragsfestsetzung anhand auswärtiger Kfz-Kennzeichen die Halter festgestellt wurden.

Eine solche Halterfeststellung ist gemäß § 39 Abs. 3 Straßenverkehrsgesetz unzulässig. Darauf habe ich bereits im 7. Tätigkeitsbericht (Nr.8.5) und im 11. Tätigkeitsbericht (Nr.8.8.2) hingewiesen. Auch das Bayerische Staatsministerium des Innern hat den Fremdenverkehrsgemeinden diese Rechtslage mit Schreiben vom 10.04.1987, Nr. 1B4 - 38024 - 7/3(87), mitgeteilt.

8.9 Mitteilung der Helferstunden vom Landratsamt an die Bau-Berufsgenossenschaft

Die Bau-Berufsgenossenschaft Bayern und Sachsen hat mir folgende Frage zur datenschutzrechtlichen Beurteilung vorgelegt:

Der Berufsgenossenschaft wurden von einem Bauherrn eines unter Denkmalschutz stehenden Gebäudes 42 Stunden für Bauhelfer mitgeteilt. Die Bauhelfer waren bei der Berufsgenossenschaft gegen Unfälle versichert. Beitragspflichtig war der Bauherr.

Die Bau-Berufsgenossenschaft hatte fundierte Zweifel an der Richtigkeit der gemeldeten Helferstunden. Sie wollte nun eine Bestätigung des Landratsamtes, daß der Bauherr auch dort nicht mehr als 42 Helferstunden gemeldet hat. Das Landratsamt konnte im Rahmen der Prüfung der Verwendung von öffentlichen Denkmalschutzmitteln (untere Denkmalschutzbehörde) die Anzahl der geleisteten Helferstunden ermitteln.

Rechtsgrundlage für die Datenübermittlung vom Landratsamt an die Bau-Berufsgenossenschaft ist Art. 18 Abs. 1 i.V.m. Art. 17 Abs. 2 Nr.5 des Bayerischen Datenschutzgesetzes (BayDSG). Danach ist die Übermittlung der Helferstunden an die Bau-Berufsgenossenschaft zulässig, da sie zur Erfüllung der in der Zuständigkeit der Bau-Berufsgenossenschaft liegenden Aufgaben erforderlich ist und Angaben des Betroffenen - des Bauherrn - überprüft werden sollen, weil tatsächliche Anhaltspunkte für deren Unrichtigkeit bestehen (Art. 17 Abs. 2 Nr.5 BayDSG).

Bauhelfer sind gemäß § 539 Abs. 1 Nr.1 RVO in der Unfallversicherung kraft Gesetzes versichert. Die Pflicht zur Beitragszahlung an die Berufsgenossenschaft trifft den Unternehmer, der die Versicherten beschäftigt (§ 723 Abs. 1 Satz 1 RVO). Gemäß § 725 Abs. 1 RVO richtet sich die Höhe der Beiträge nach dem Entgelt der Versicherten und nach dem Grad der Unfallgefahr, sofern nicht Sonderregelungen greifen.

Die Bau-Berufsgenossenschaft benötigt somit korrekte Daten, um die Beitragshöhe für die Versicherung beurteilen zu können.

Da die Datenübermittlung vom Landratsamt an die Bau-Berufsgenossenschaft dazu erfolgen soll, um Angaben des Bauherrn überprüfen zu können, weil tatsächliche Anhaltspunkte für deren Unrichtigkeit bestehen, liegen auch die Voraussetzungen des Art. 17 Abs. 2 Nr.5 BayDSG für eine Datenübermittlung vor.

Ergeben sich darüber hinaus bei der Durchführung des Gesetzes zur Bekämpfung der Schwarzarbeit im Einzelfall konkrete Anhaltspunkte für z.B. Verstöße gegen die Vorschriften der Reichsversicherungsordnung, die von §2 a Abs. 2 Nr.4 des Gesetzes zur Bekämpfung der Schwarzarbeit erfaßt werden, hat das Landratsamt im übrigen von sich aus den jeweiligen Träger der Unfallversicherung zu unterrichten.

8.10 Weitergabe von Adreßdaten zur Durchführung einer Umfrage

Eine Stadt bat mich um Auskunft, ob sie einer Fachhochschule die Adreßda ten der derzeitigen und früheren Abonnenten des Theaters der Stadt übermitteln dürfe. Die Fachhochschule benötige die Daten zur Durchführung einer Umfrage im Rahmen der Erstellung einer Studie über den Rückgang der Theaterabonnements.

Die Übermittlung der Adreßdaten an die Fachhochschule ist zur Durchführung der Umfrage nicht erforderlich. Die von der Fachhochschule vorbereiteten Fragebögen können auch von der Theaterverwaltung an die Abonnenten versandt werden. Diese sind auf die Freiwilligkeit der Teilnahme an der Umfrage hinzuweisen. Die Rücksendung der anonymisierten Fragebögen in einem Briefumschlag

ohne Absender kann dabei auch unmittelbar an die Fachhochschule zur Auswertung erfolgen.

9. Einwohnermeldewesen

9.1 Änderung des Melderechtsrahmengesetzes

Auf die Bekanntmachung der Neufassung des Melderechtsrahmengesetzes (MRRG) vom 24.06.1994 (BGBl 1 S.1430 ff.) und auf folgende Anderungen aufgrund des Ersten Gesetzes zur Änderung des Melderechtsrahmengesetzes vom 11.03.1994 (BGBl 1 S.529ff.) möchte ich hinweisen:

1. **Speicherung von Daten**

   Der Katalog der Daten des Einwohners in § 2 Abs. 1 MRRG, den die Meldebehörden speichern dürfen, wurde in folgenden Punkten geändert:

   - Als akademischer Grad darf nur der Doktorgrad gespeichert werden (Nr.4);
   - in Nr.9 sind nun neben dem gesetzlichen Vertreter die ,,Eltern von Kindern nach Nr. 16" (Kinder bis zu 27 Jahren) genannt. Zu den speicherfähigen Daten (in Klammern) gehört nunmehr auch der Sterbetag;
   - nach Nr. 10 dürfen die Staatsangehörigkeiten (bisher Staatsangehörigkeit) gespeichert werden;
   - nach Nr. 14 dürfen bei Verheirateten zusätzlich zum Familienstand Tag und Ort der Eheschließung gespeichert werden;
   - nach Nr.16 dürfen nunmehr Angaben über Kinder bis zur Vollendung des 27. Lebensjahres gespeichert werden (bisher nur bis zur Vollendung des 18. Lebensjahres).

2. **Meldepflicht in Beherbergungsstätten und Krankenhäuser**

   Die Verpflichtung des Gastes, bei einer Übernachtung in einer Beherbergungsstätte den besonderen Meldeschein auszufüllen, bleibt bestehen. Beherbergte Ausländer haben sich dabei gegenüber dem Leiter der Beherbergungsstätte oder seinem Beauftragten durch die Vorlage eines gültiges Identitätsdokumentes auszuweisen. Der Bund ist mit dieser Änderung vom 15.07.1993 (BGBl IIS. 1010) einerVerpflichtung aus dem Schengener Durchführungsübereinkommen nachgekommen.

   Bestehen bleibt auch die Regelung, daß ein Krankenhausleiter die aufgenommenen Personen in ein Verzeichnis aufzunehmen hat. Die Angaben in diesem Verzeichnis durften bislang von der Polizei u.a. für Zwecke der Gefahrenabwehr ausgewertet und verarbeitet werden. Die neue Regelung in § 16 Abs. 3 MRRG schränkt dies nun insoweit ein, als eine **erhebliche und gegenwärtige Gefahr** vorliegen muß. Außerdem beschränkt diese Vorschrift den Zugriff auf Patientendaten auf eine **Auskunftserteilung im Einzelfall** an die zuständigen Behörden. Nach der bisherigen Regelung war das Verzeichnis für die Polizei zur Einsichtnahme bereitzuhalten.

9.2 Änderung des Wehrpflichtgesetzes (WPflG)

Das Welrrpflichtgesetz in der Fassung der Bekanntmachung vom 14. Juli 1994 (BGBl I Seite 1505) hat folgende Auswirkungen auf die Speicherungs- und Übermittlungspraxis der Einwohnermeldeämter:

1. § 24 a WPflG bewirkt, daß die bisher vorgesehene Speicherung des Kennzeichens ,,Wehrüberwachung" bei den über 32jährigen männlichen Deutschen, die (noch) der Wehrüberwachung unterliegen, im Melderegister entfällt und die Daten dieses Personenkreises nicht mehr nach § 2 2. BMeldeDÜV an die Wehrersatzbehörden übermittelt werden dürfen. Nach der bisher geltenden und durch die Novelle weggefallenen Vorschrift des § 24 Abs. 9 WPflG war die Meldebehörde verpflichtet, dem Kreiswehrersatzamt Änderungen der über 32jährigen Bürger, die nach den Mitteilungen des Kreiswehrersatzamtes noch der Wehrüberwachung unterlagen, zu übermitteln.

   Nach der neuen Regelung des § 24 a WPflG haben die Meldebehörden außerdem die in dieser Vorschrift genannten Daten der männlichen Deutschen ab dem 17. **Lebensjahr** an die Kreiswehrersatzbehörden zu übermitteln. Nach der bisherigen Regelung des § 24 Abs. 9 WPflG mußten die Daten der männlichen Deutschen ab dem 18. Lebensjahr an die Kreiswehrersatzämter übermittelt werden.

2. In § 41 WPflG sind die Worte ,,§ 3 Abs. 1 Satz 1" weggefallen. Dadurch reduziert sich die 2jährige Befreiung von der Wehrerfassung und die entsprechende Fristenüberwachung auf den Personenkreis, der aus den in § 1 Abs. 2 Nr. 3 des Bundesvertriebenengesetzes genannten Gebieten stammt.

9.3 Widerspruchsrechte nach Art. 35 Meldegesetz

Obwohl die Regelungen des Meldegesetzes über Melderegisterauskünfte und die Widerspruchsrechte der Bürger bereits seit über 11 Jahren in Kraft sind und wiederholt in den Tätigkeitsberichten zu diesem Problemkreis Stellung genommen wurde, erreichten mich im Berichtszeitraum immer wieder Anfragen und Beschwerden von Bürgern, deren Daten zu Wahlwerbezwecken an politische Parteien und Wählergruppen oder zur Bekanntgabe von Alters- und Ehejubiläen an die Presse übermittelt wurden oder deren Daten in Adreßbüchern erscheinen. Ich möchte deshalb nochmals auf die Regelung im Meldegesetz (MeldeG) hinweisen:

Art. 35 MeldeG läßt folgende Datenübermittlungen zu:

1. Zum Zwecke der **Wahlwerbung** darf **Parteien und Wählergruppen** im Zusammenhang mit allgemeinen

Wahlen und mit Abstimmungen **innerhalb von sechs Monaten** vor der Stimmabgabe Auskunft aus dem Melderegister über Vor- und Familiennamen, akademische Grade und Adressen von Wahlberechtigten erteilt werden. Die Auskunft kann sich auf bestimmten **Gruppen von Wahlberechtigten** beschränken, für deren **Zusammensetzung das Lebensalter** der Betroffenen bestimmend ist. Die Geburtstage der Wahlberechtigten dürfen dabei jedoch nicht mitgeteilt werden. Die Zusammensetzung der Daten von Wahlberechtigten **nach anderen Suchkriterien** (z.B. ,,alle Neubürger") **ist unzulässig.** Die Auskunft ist nur zulässig, **sofern der Bürger der Datenweitergabe nicht** widersprochen hat (Art. 35 Abs. 1 Satz 3 MeldeG).

2. Eine Melderegisterauskunft über**Alters- oderEhejubiläen** von Einwohnern darf an **Parteien, Wählergruppen, Mitglieder parlamentarischer Vertretungskörperschaften und Bewerber für diese sowie Presse und Rundfunk** erteilt werden. Zulässig ist die Übermittlung von Vor- und Familiennamen, akademischen Graden und Adressen sowie des Tages und der Art des Jubiläums. Auch hier **darf die Auskunft nur erteilt werden, wenn der Betroffene nicht widersprochen hat** (Art. 35 Abs. 2 Satz 1 MeldeG).

3. **Adreßbuchverlagen** darf Auskunft über Vor- und Familiennamen, akademische Grade und Adressen sämtlicher Einwohner erteilt werden, die das 18. Lebensjahr vollendet haben. Auch hier hat der Betroffene das **Recht,** der **Weitergabe** seiner Daten zu widersprechen (Art. 35 Abs. 3 Satz 2 MeldeG).

Gerade die Widerspruchsrechte scheinen vielen Bürgern noch nicht hinreichend bekannt zu sein. **Ich rege daher** - wie schon in früheren Tätigkeitsberichten - **an,** die **Bürger in geeigneter Weise auf ihre Widerspruchsrechte hinzuweisen** (z.B. Amtsblatt, Amtstafel, örtliche Presse, vgl. dazu auch Nr.35.4 der Vollzugsbekanntmachung zum Meldegesetz, MABl 1984 S.177 ff.).

10. Ausländerwesen

Abgleich einer Wählerliste mit der Ausländerdatei zur Durchführung von Ausländerbeiratswahlen

Nach der Satzung einer Stadt über den Ausländerbeirat und der dazu erlassenen Wahlordnung sind u.a. alle diejenigen Ausländer wahlberechtigt, die sich erlaubt in der Bundesrepublik Deutschland auffialten. Die Feststellung des ,,erlaubten Aufenthalts" wollte die Stadt dadurch durchführen (lassen), daß das Landratsamt (Ausländeramt) eine Liste von mehreren hundert Ausländern daraufhin überprüft, ob sich diese Personen ,,erlaubt" in Deutschland auffialten. Die Stadt hat mich gebeten zu prüfen, ob der Datenabgleich zulässig ist.

Die Prüfung hat die datenschutzrechtliche Unzulässigkeit des Abgleichs ergeben. Das Ziel (Feststellung des erlaubten Aufenthalts) kann auf andere Weise erreicht werden.

1. **Rechtslage**

Bei der Satzung der Stadt über den Ausländerbeirat sowie der hierzu erlassenen Wahlordnung handelt es sich um Satzungen, die sich auf die allgemeine Satzungsautonomie des Art. 23 Satz 1 der Gemeindeordnung (GO) stützen. Diese bildet keine Rechtsgrundlage für Satzungen, die in die Grundrechte der Bürger eingreifen (vgl. BayVGH BayVBl 1992, 337, 338). Die Wahlordnung kommt deshalb als Rechtsgrundlage für die Übermittlung personenbezogener Daten vom Landratsamt an die Stadt nicht in Betracht. Nachdem auch das Ausländergesetz für Datenübermittlungen zur Frage des ,,erlaubten Aufenthalts" keine Spezialregelungen enthält, findet als Auffanggesetz das Bayerische Datenschutzgesetz Anwendung.

Nach Art. 18 Abs. 1 BayDSG ist die Datenübermittlung vom Landratsamt an die Stadt zulässig, wenn sie zur Aufgabenerfüllung des Landratsamtes oder der Stadt **erforderlich** ist **und** der **Zweckbindungsgrundsatz** (vgl. Art. 18 Abs. 1 i.V.m. Art. 17 Abs. 1 Nr.2, Abs. 2 bis 4 BayDSG) beachtet wird.

Das Kriterium der Erforderlichkeit braucht hierbei nicht weiter geprüft zu werden, da der Datenübermittlung in jedem Fall der **Zweckbindungsgrund satz** entgegensteht.

Die beim Ausländeramt vorhandenen Datenbestände sind im Rahmen der Zuständigkeit des Ausländeramtes (vgl. § 63 Abs. 1 Ausländergesetz) für aufenthalts- und paßrechtliche Zwecke gespeichert. Die Verwendung der Daten zur Durchführung einer Ausländerbeiratswahl würde also einem anderen Zweck, nämlich der Erfüllung einer anderen Aufgabe dienen; dabei ist eine Datenübermittlung nur unter den Voraussetzungen für eine Durchbrechung der Zweckbindung nach Art. 17 Abs. 2 BayDSG möglich.

- Art. 17 Abs. 2 Nr.3 BayDSG ist nicht einschlägig, da nicht davon ausgegangen werden kann, daß allen Ausländern die Übermittlung ihrer Daten an die Stadt erwünscht ist. Dies gilt insbesondere für die Fälle, in denen sich der Aufenthalt des Ausländers als unberechtigt herausstellt.
- Auch Art. 17 Abs. 2 Nr.1 Alternative 2 BayDSG ist nicht einschlägig, demzufolge (i.V.m. Art. 18 Abs. 1 a.E. BayDSG) eine Übermittlung personenbezogener Daten für andere Zwecke auch dann zulässig ist, wenn eine Rechtsvorschrift dies **zwingend** voraussetzt.

  Als eine solche Rechtsvorschrift kommt die Vorschrift in der Wahlordnung für den Ausländerbeirat der Stadt in Betracht, nach der der ,,erlaubte Aufenthalt" in Deutschland Voraussetzung für die

Teilnahme an der Wahl zum Ausländerbeirat ist, wobei die Feststellung dieses Kriteriums anders als durch einen Datenabgleich beim Ausländeramt nicht möglich sein darf.

Diese Vorschrift ist jedoch nicht hinreichend bestimmt, weil der Begriff ,,erlaubter Aufenthalt" in der Wahlordnung nicht definiert ist (Zweifelsfälle sind z.B. noch nicht verbeschiedene Anträge auf Aufenthaltserlaubnis).

Außerdem entspricht sie nicht dem Verhältnismäßigkeitsgrundsatz, denn an Stelle eines derart umfassenden Datenabgleichs gibt es andere Möglichkeiten (vgl. 2.).

2. **Lösungsmöglichkeiten**

Eine Lösungsmöglichkeit für die satzungsrechtliche Regelung des ,,erlaubten Aufenthalts" und seine Feststellung in der Praxis könnte wie folgt aussehen:

- Der ,,erlaubte Aufenthalt" wird in der Wahlordnung eindeutig im Sinne eines rechtmäßigen Aufenthalts definiert, der dann vorliegt, wenn der Ausländer über eine Aufenthaltsgenehmigung (Aufenthaltsberechtigung, Aufenthaltserlaubnis, Aufenthaltsbewilligung, Aufenthaltsbefugnis) verfügt. Diese hat er durch eine entsprechende Eintragung im Reisepaß oder durch EG-Karte nachzuweisen.

- Die praktische Durchführung könnte dann so geschehen, daß alle im Gemeindegebiet seit einem bestimmten Zeitpunkt gemeldeten volljährigen Ausländer ohne nähere Überprüfung in die Wählerliste für die Wahl des Ausländerbeirats eingetragen werden. Von dieser Eintragung werden sie benachrichtigt, wobei darauf hingewiesen wird, daß tatsächlich wahlberechtigt nur diejenigen Ausländer sind, die eine Aufenthaltsgenehmigung besitzen und diese durch eine entsprechende Eintragung im Reisepaß oder durch die EG-Karte nachweisen können. Die Überprüfung der Aufenthaltsgenehmigung anhand des Paßstempels oder der EG-Karte kann dann bei der Urnenwahl im Wahllokal vorgenommen werden. Eine andere Möglichkeit wäre, eine aus dem Melderegister erstellte ,,Grobwählerliste" dadurch fortzuschreiben daß in das ,,eigentliche" Wählerverzeichnis nur diejenigen Ausländer eingetragen werden, die dies gegenüber der Gemeinde beantragen und die bei diesem Antrag die Aufenthaltsgenehmigung nachweisen. Bei diesem Verfahren wird es den einzelnen Ausländern überlassen, ob sie ihre Daten offenbaren wollen oder nicht.

  Die Durchführungsregelung sollte ebenfalls in der Wahlordnung festgelegt werden.

11. Steuerverwaltung

11.1 Datenschutzvorschriften in der Steuerverwaltung

In meinem 15. Tätigkeitsbericht habe ich mitgeteilt, daß Überlegungen im Bundesministerium der Finanzen bestehen, eine Novellierung der datenschutzrechtlichen Bestimmungen in der Abgabenordnung vorerst zurückzustellen. Ich habe darauf hingewiesen, daß ich nach wie vor Handlungsbedarf sehe.

Die Arbeiten am Gesetz zur Änderung der Abgabenordnung wurden bisher nicht wieder aufgenommen. Der Gesetzgeber hat allerdings in Art. 9 des Gesetzes zur Bekämpfung des Mißbrauchs und zur Bereinigung des Steuerrechts vom 21.12.1993 auch einige Änderungen der Abgabenordnung mit datenschutzrechtlichem Bezug verabschiedet.

So sind die für die Verwaltung der Grundsteuer zuständigen Behörden aufgrund des neu eingefügten § 31 Abs. 3 AO nunmehr berechtigt, die durch das Steuergeheimnis geschützten Namen und Anschriften von Grundstückseigentümern zur Verwaltung anderer Abgaben und zur Erfüllung sonstiger öffentlicher Aufgaben zu verwenden oder den hierfür zuständigen Gerichten, Behörden oder juristischen Personen des öffentlichen Rechts auf Ersuchen mitzuteilen, soweit nicht überwiegende schutzwürdige Interessen des Betroffenen entgegenstehen.

Damit wurde eine praxisgerechte Regelung geschaffen und eine von mir bereits mehrfach erhobene Forderung erfüllt. Ich verweise insoweit auf meinen 13. Tätigkeitsbericht (S.51, Nr.10.1) und meinen 15. Tätigkeitsbericht (S.68, Nr.10.1). Unter Nr.11.2 nehme ich anschließend zu einigen Anfragen in diesem Zusammenhang Stellung.

Weiterhin wurde § 249 Abs. 2 AO dergestalt geändert, daß die Finanzbehörden nunmehr ihnen bekannte, durch das Steuergeheimnis geschützte Daten (z.B. Kontonummern), die sie bei der Vollstreckung von steuerlichen Forderungen verwenden dürfen, auch bei der Vollstreckung anderer Geldleistungen als Steuern nutzen können.

Diese Vorschrift ist insbesondere für die Finanzämter in Bayern von Bedeutung, da diese aufgrund von Art. 25 des Bayerischen Verwaltungszustellungs- und Vollstreckungsgesetzes sämtliche Leistungsbescheide des Staates zu vollstrecken haben.

Ich habe in der Vergangenheit bei der Prüfung von Finanzbehörden auf die Schaffung einer normenklaren Regelung in diesem Zusammenhang gedrungen. Diese Forderung ist nunmehr erfüllt.

Ich bin mit der Mehrzahl der Datenschutzbeauftragten des Bundes und der Länder allerdings der Auffassung, daß in Teilbereichen der Abgabenordnung noch datenschutzrechtlicher Handlungsbedarf besteht. Ich unterstütze deshalb die Erstellung einer Bestandsaufnahme von wün-

schenswerten Änderungen durch den Bundesbeauftragten für den Datenschutz mit dem Ziel, eine Wiederaufnahme der Arbeiten am AO-Änderungsgesetz gegenüber dem Bundesministerium der Finanzen zu erreichen.

11.2 Nutzung von Grundsteuer-Adreßdaten von Gemeinden für andere öffentliche Aufgaben

Unter Nr.11.1 habe ich ausgeführt, daß aufgrund § 31 Abs. 3 AO nunmehr die Nutzung von gemeindlichen Grundsteuer-Adreßdaten für andere öffentliche Aufgaben unter bestimmten Voraussetzungen möglich ist.

Im Berichtszeitraum hatte ich zu mehreren konkreten Anfragen in diesem Zusammenhang Stellung zu nehmen.

Eine Gemeinde wollte preisgünstigen Wohnraum anmieten, um diesen dann an junge Familien oder auch im Tauschverfahren an ältere Gemeindebürger weiterzuvermieten. Um potentielle Vermieter über diese Möglichkeit zu informieren, sollten diese anhand der gemeindlichen Grundsteuer-Adreßdaten entsprechend benachrichtigt werden.

Ich habe im Hinblick auf § 31 Abs. 3 AO gegen das geplante Verfahren keine Bedenken erhoben.

Eine weitere Anfrage zur Auskunftserteilung aus den gemeindlichen Grundsteuer-Adreßdateien habe ich vom **Bayerischen Rundfunk** erhalten.

Der Bayerische Rundfunk ist gemäß § 7 Abs. 1 und 2 Rundfunkgebührenstaatsvertrag (RfgebStV) Gläubiger der Rundfunkgebühren für die in seinem Sendegebiet zum Empfang bereitgehaltenen Rundfunkgeräte. Zur Ermittlung bisher nicht oder nicht vollständig gemeldeter Rundfunkgeräte besteht die Möglichkeit, den Rundfunkteilnehmer und auch Dritte um Auskunft über die den Gebührenanspruch begründenden Tatsachen zu bitten. Dies gilt unter bestimmten Voraussetzungen gemäß § 4 Abs. 6 RfgebStV auch gegenüber Meldebehörden. Ein solcher Weg der Auskunftserteilung ist bei Eigentümern von Ferienhäusern und -wohnungen nicht gangbar, da diese wegen ihrer kurzen Aufenthaltsdauer am jeweiligen Ort nicht meldepflichtig sind. In diesem Fall könnten Namen und Anschriften der Eigentümer jedoch der gemeindlichen Grundsteuerdatei entnommen werden.

Ich halte die Anwendung von § 31 Abs. 3 AO und damit eine Auskunftserteilung im vorliegenden Fall für möglich. Etwaige überwiegende schutzwürdige Interessen der von dem Auskunftsbegehren Betroffenen stehen dem meiner Ansicht nach nicht entgegen.

11.3 Kontrollmitteilungen an das Finanzamt

Zur Sicherung der Besteuerung hat die Bundesregierung aufgrund § 93 a Abgabenordnung die Möglichkeit, durch Rechtsverordnung Behörden und öffentlich-rechtliche Anstalten zu verpflichten, Kontrollmitteilungen über Zahlungen z.B. aus Werk- oder Dienstverträgen an die für die Besteuerung der Zahlungsempfänger zuständigen Finanzämter zu übermitteln.

In meinem 15. Tätigkeitsbericht habe ich mitgeteilt, daß der Bundesfinanzminister durch Erlaß der Mitteilungsverordnung vom 07.09.1993 (MV) von dieser Ermächtigung Gebrauch gemacht hat. Ich habe weiterhin mitgeteilt, daß in der Verordnung die ‚Angabe der Betragshöhe nicht vorgesehen war. Begründet wurde dies mit dem Wortlaut der Ermächtigungsgrundlage. Der Gesetzgeber hat nunmehr im Rahmen des Gesetzes zur Bekämpfung des Mißbrauchs und zur Bereinigung des Steuerrechts §93 a Abs. 1 Satz 2 AO um die Angabe der Betragshöhe erweitert.

§ 8 Abs. 2 MV wurde mit Wirkung vom 01.01.1995 entsprechend geändert.

11.4 Eintragung des Freibetrags für Behinderte auf der Lohnsteuerkarte

Soweit ein Steuerpflichtiger in einem erstmaligen Antrag auf Lohnsteuerermäßigung den Freibetrag für Behinderte gemäß § 33 b EStG geltend macht, wird dieser Freibetrag (ggf. zusammen mit anderen beantragten Beträgen) vom **Finanzamt** auf der Lohnsteuerkarte eingetragen (§ 39aAbs.4aEStG).

Unabhängig davon, ob der Steuerpflichtige in den Folgejahren wiederum einen Antrag auf Lohnsteuerermäßigung stellt, erfolgt während der Geltungsdauer des Behindertenausweises eine Übermittlung des Freibetrags für Behinderte - und damit der Tatsache einer vorhandenen Behinderung - vom Finanzamt an die Wohnsitzgemeinde. Aus dem Formular „Antrag auf Lohnsteuer-Ermäßigung" war diese künftige Datenübermittlung für den Steuerpflichtigen bisher nicht erkennbar.

Es sind durchaus Fälle denkbar, in denen der Steuerpflichtige nicht wünscht, daß der Gemeindeverwaltung die Tatsache seiner Behinderung bekannt wird. Das gleiche gilt gegenüber dem Arbeitgeber bei Eintritt einer Behinderung während eines bestehenden Arbeitsverhältnisses oder bei einem Arbeitsplatzwechsel zum Jahresanfang.

Insbesondere bei kleinen Gemeinden ist die ausschließlich zweckgebundene Nutzung dieser Kenntnis nicht immer gesichert. Darüber hinaus kann der Arbeitgeber von der Höhe eines auf der Lohnsteuerkarte ausschließlich eingetragenen Freibetrages wegen der Behinderung auf ihren Grad zurückschließen. Damit erhält er Informationen, die sich nachteilig für den Arbeitnehmer auswirken können und auf die der Arbeitgeber in vielen Fällen keinen Anspruch hat (vgl. meine Ausführungen im 12. Tätigkeitsbericht unter Nr.10.3).

Das Staatsministerium der Finanzen begründet die o.a. Sachbehandlung mit § 39 a Abs. 2 Satz 1 EStG. Danach hat die Gemeinde nach Anweisung des Finanzamts die Pauschbeträge für Behinderte bei der Ausstellung der Lohnsteuerkarten von Amts wegen einzutragen. Es weist darauf hin, daß es sich bei der Datenübermittlung an die Gemeinden um eine Datenübermittlung innerhalb der Finanzverwaltung handle, da die Gemeinden nach § 39 Abs. 6 EStG insoweit, als sie Eintragungen auf den

Lohnsteuerkarten vorzunehmen haben, örtliche Landesfinanzbehörden seien. Sie unterlägen dem Steuergeheimnis nach § 30 AO. Im übrigen sähe Art. 3 Abs. 2 Nr.2 des Meldegesetzes die Speicherung von Freibeträgen für die Ausstellung von Lohnsteuerkarten vor.

Es wird nicht verkannt, daß das augenblickliche Verfahren in den meisten Fällen eine bürgerfreundliche Lösung darstellt, da nur ein einmaliges Tätigwerden des Steuerpflichtigen notwendig ist.

Meiner Ansicht nach muß aus datenschutzrechtlicher Sicht dem Steuerpflichtigen **zumindest die Möglichkeit eröffnet werden,** der künftigen Datenübermittlung an die Gemeinde zu widersprechen und den Eintrag des Freibetrags auf der Lohnsteuerkarte durch das Finanzamt über einen jährlichen Antrag auf Lohnsteuer-Ermäßigung zu erreichen. Außerdem muß der Vordruck ,,Antrag auf Lohnsteuer-Ermäßigung" um einen Hinweis auf die künftigen Datenübermittlungen an die Gemeinde ergänzt werden.

Im Gegensatz zur Auffassung des Staatsministeriums der Finanzen ist eine Gesetzesänderung für diese datenschutzgerechte Sachbehandlung meines Erachtens nicht erforderlich. In den Fällen, in denen der Steuerpflichtige einer Datenübermittlung widerspricht, muß nur die ,,Anweisung des Finanzamts" (§ 39 a Abs. 2 Satz 1 EStG) zum Eintrag des Freibetrags an die Gemeinde unterbleiben.

Eine ähnliche datenschutzfreundliche Regelung wurde von mir im Zusammenhang mit der Abholung eines neuausgestellten Behindertenausweises erreicht. Hier kann der Bürger inzwischen wählen, ob er den Behindertenausweis bei seiner Heimatgemeinde oder dem zuständigen Versorgungsamt abholt.

Im Hinblick darauf, daß es sich bei dem ,,Antrag auf Lohnsteuer-Ermäßigung" um ein bundeseinheitliches Muster handelt, habe ich den Bundesbeauftragten für den Datenschutz gebeten, gegenüber dem Bundesfinanzministerium zumindest die Aufnahme eines Hinweises auf die künftigen Datenübermittlungen an die Gemeinde in den Vordruck zu erreichen. Diesem Vorschlag wurde inzwischen Rechnung getragen. Das Formular ,,Antrag auf Lohnsteuer-Ermäßigung 1995" enthält einen kurzen Hinweis.

Ich habe außerdem einen darüber hinausgehenden Vorstoß für eine datenschutzgerechte Auslegung von § 39 a Abs. 2 EStG angeregt. Das Staatsministerium der Finanzen unterstützt dieses Vorhaben nicht. Es befürchtet einen erheblichen Verwaltungsmehraufwand. Im Hinblick auf die oben geschilderten möglichen Nachteile für den Betroffenen kann ich mich damit nicht zufriedengeben.

Das Staatsministerium für Arbeit und Sozialordnung, Familie, Frauen und Gesundheit hat meinen Vorstoß befürwortet.

11.5 Datenübermittlung an Kirchensteuerämter

In meinem 15. Tätigkeitsbericht habe ich unter Nr.10.6 ausführlich zur aus datenschutzrechtlicher Sicht unbefriedigenden Praxis der Datenübermittlung von den Finanzämtern an die Kirchensteuerämter bei glaubensverschiedenen Ehen Stellung genommen.

Auch im Berichtszeitraum haben sich in diesem Zusammenhang wieder mehrere Bürger an mich gewandt. Aufgrund neuerer Rechtsprechung des Bundesfinanzhofes erfolgte im Berichtszeitraum auch eine Novellierung des Kirchensteuergesetzes. Bisher wurde bei konfessionsverschiedenen Ehen, d.h. beide Ehegatten gehören verschiedenen umlageerhebenden Religionsgemeinschaften an, die Kirchensteuer aus der Hälfte der gemeinsamen Einkommensteuer berechnet bzw. die Kirchenlohnsteuer je zur Hälfte an beide umlageerhebenden Gemeinschaften entrichtet. Künftig wird dieser sogenannte Halbteilungsgrundsatz durch eine Individualbesteuerung abgelöst und die gemeinsame Einkommensteuer im Verhältnis der Summe der Einkünfte eines jeden Ehegatten aufgeteilt.

Es besteht damit die Gefahr, daß die bisher nur bei glaubensverschiedenen Ehen praktizierte und von mir als nicht datenschutzgerecht empfundene Datenübermittlung der Höhe der Einkünfte des nicht der umlageerhebenden Religionsgemeinschaft angehörenden Ehegatten - zur Ermittlung des v.H.-Satzes durch das Kirchensteueramt -, an die Religionsgemeinschaft des anderen Partners künftig auch bei der Vielzahl der konfessionsverschiedenen Ehen erfolgt.

Ich habe gegenüber dem Staatsministerium der Finanzen deutlich gemacht, daß die Novellierung des Kirchensteuergesetzes keinesfalls zu einer Ausweitung der Datenübermittlungen der Finanzämter an die Kirchensteuerämter führen darf. Ich habe gebeten, bei einer als Folge der Novellierung anstehenden Änderung der ,,Verordnung zur Ausführung des Kirchensteuergesetzes ,wie in anderen Ländern, auch in Bayern den Rechenvorgang der Ermittlung der Bemessungsgrundlage (des Anteils an der gemeinsamen Einkommensteuer) auf die Finanzämter zu verlagern.

Das Staatsministerium der Finanzen hat mir inzwischen mitgeteilt, daß ab 1995 - mit Beginn der Veranlagung 1994 - die Fälle der glaubens- und konfessionsverschiedenen Ehegatten gleich behandelt werden. In den genannten Fällen wird künftig neben der gemeinsam veranlagten Einkommensteuer, der im Abzugsweg erhobenen Kirchensteuer und den Kinderentlastungsbeträgen auch die Summe der jeweiligen Einkünfte beider Ehegatten an die Kirchensteuerämter übermittelt. Meine Befürchtungen wurden damit bestätigt.

Das Staatsministerium der Finanzen sieht durch die Neuregelung Belange des Datenschutzes nicht als verletzt an. Nach Auffassung des Staatsministeriums orientiert sich die derzeitige Regelung am geringstmöglichen Verwaltungsaufwand. Sie sei außerdem für den Steuerbürger

„transparent und bürgerfreundlich". Im übrigen wird festgestellt, daß die Rechtmäßigkeit der bisherigen Handhabung vom Bundesfinanzhof mit Beschluß vom 22.10.1991 ausdrücklich bestätigt worden sei.

Die Rechtmäßigkeit des Verfahrens habe ich bisher auch nie in Zweifel gezogen. Das kann aber nicht bedeuten, daß über eine Verbesserung der datenschutzrechtlichen Situation nicht näher nachgedacht werden darf. Es bleibt unbefriedigend, daß Einkommensdaten von Personen, die in keinerlei Beziehung zu einer Religionsgemeinschaft stehen, eben dieser Religionsgemeinschaft durch eine staatliche Stelle zur Kenntnis gebracht werden.

12. Personalwesen

12.1 Personalaktenrecht

Bereits im 15. Tätigkeitsbericht habe ich darauf hingewiesen, daß der Bundesgesetzgeber das Personalaktenrecht im Bundesbeamtengesetz und im Beamtenrechtsrahmengesetz neu geregelt hat. Die Umsetzung des Rahmenrechts durch Novellierung des Bayerischen **Beamt**engesetzes ist nunmehr durch das Zwölfte Gesetz zur Änderung beamtenrechtlicher Vorschriften vom 23.07.1994 erfolgt. Das Gesetz ist, mit wenigen Ausnahmen, zum 01.08.1994 in Kraft getreten.

Vorrangiges Anliegen des Gesetzes ist, einen gerechten Ausgleich zwischen dem Schutz des Persönlichkeitsrechts des betroffenen Beamten und der Erhaltung und Förderung der Funktionsfähigkeit des Personalaktenwesens herzustellen. Ich war in die Beratungen des Gesetzesentwurfes eingebunden und konnte einige meiner Vorstellungen einbringen.

Das Gesetz enthält u.a. Regelungen zu folgenden Bereichen:

- Zweckbindung der Erhebung von Personalaktendaten,
- Pflicht zur Führung von Personalakten,
- vertrauliche Behandlung des Personalakts,
- Begriff, Inhalt und Zweckbestimmung des Personalakts sowie seine Gliederung und Gestaltung,
- Abschottung des Beihilfeakts,
- Einsicht, Vorlage und Auskunft,
- Entfernung von Vorgängen aus dem Personalakt,
- Dauer der Aufbewahrung von Personalakten,
- automatisierte Verarbeitung und Nutzung von Personalaktendaten.

Die meisten der genannten Vorschriften sind nach meiner Ansicht künftig, auch wenn sie sich nach dem Wortlaut nur auf Beamte beziehen, analog für die nichtverbeamteten Beschäftigten im öffentlichen Dienst gleichermaßen anzuwenden.

Herausgreifen möchte ich Art. 100 b BayBG, der sich mit der Behandlung von Unterlagen über **Beihilfen** befaßt.

Unterlagen über Beihilfen sind nach dieser Vorschrift stets als besonderer, vom übrigen Personalakt getrennt aufzubewahrender Teilakt zu führen.

Sie sollen in einer von der Personalverwaltung getrennten Organisationseinheit bearbeitet werden, was auch eine personelle Trennung einschließt. Das Problem der Führung von Beihilfeakten und ihrer sicheren Verwahrung steht im engsten Sachzusammenhang mit dem Personalaktengeheimnis. Da Beihilfeakten regelmäßig höchst persönliche Daten über Krankheiten, Diagnosen, Behandlungen und Medikationen enthalten, die bei zweckwidriger Verwendung zu spürbaren Nachteilen für den Betroffenen führen können, kommt ihrer Absicherung gegen unbefugte Kenntnisnahme besondere Aufmerksamkeit zu. Die Kenntnisnahme von geschützten Daten ist daher im Rahmen des Beihilfeverfahrens auf das für die Abrechnung unumgänglich notwendige Maß zu beschränken. Dies **erfordert eine strikte organisatorische Trennung der Beihilfeakten,** insbesondere der in ihnen enthaltenen ärztlichen Unterlagen von **den sonstigen Personalakten.**

Die Fassung als Sollvorschrift erfolgte mit Rücksicht auf kleinere personalverwaltende Behörden (insbesondere im kommunalen Bereich), wo ein Sachbearbeiter mit der Bearbeitung von Beihilfevorgängen nicht ausgelastet ist, so daß ihm zwangsläufig noch weitere Aufgaben zugewiesen werden müssen. Hierbei ist darauf zu achten, daß vorrangig Aufgaben zugewiesen werden, die in keinem unmittelbaren Zusammenhang mit der Personalverwaltung stehen.

Eine weitere Möglichkeit der Trennung von Beihilfe- und Personalsachbearbeitung, die insbesondere für kleinere Gemeinden bedeutsam ist, besteht im Abschluß einer Beihilfeversicherung. Die gesetzliche Grundlage hierfür bildet Art. 11 Abs. 2 BayBesG. Träger der Beihilfeverpflichtung bleibt nach wie vor der jeweilige Dienstherr. Lediglich die Festsetzung und Zählung der Beihilfe liegt bei der Beihilfeversicherung, die auch das Risiko trägt und der zur Wahrnehmung ihrer Aufgaben alle Daten, die sonst einer Beihilfestelle zur Verfügung stehen, übermittelt werden müssen.

Das Staatsministerium der Finanzen, das ich um Stellungnahme zur Vereinbarkeit der Vorschriften des neuen Personalaktenrechts mit den Datenübermittlungen an eine Beihilfeversicherung gebeten habe, geht davon aus, daß die Vorschriften für die in der Rechtsform einer Anstalt des öffentlichen Rechts organisierten Beihilfeversicherungen unmittelbar gelten.

Die Rechtslage bei privaten Beihilfeversicherungen halte ich jedoch für unklar. Das Staatsministerium hat den Verband der privaten Krankenversicherungen auf die entsprechenden Vorschriften des BayBG hingewiesen. Die rechtsverbindliche Einhaltung der Vorschriften muß jedoch darüber hinaus durch ein geeignetes Verfahren sichergestellt werden. Ich werde mich deshalb nochmals an das Staatsministerium wenden.

12.2 Ressorteinheitlicher Personalfragebogen

In dem durch das Zwölfte Gesetz zur Änderung beamtenrechtlicher Vorschriften novellierten Art. 100 Satz 2 BayBG wird bestimmt, daß Fragebögen, mit denen

Personaldaten erhoben werden, nun der Genehmigung durch die oberste Dienstbehörde bedürfen. Die Vorschrift ist gemäß § 8 Abs. 2 Nr.2 des Änderungsgesetzes bereits ab 01.01.1994 anzuwenden.

Ich habe dies zum Anlaß genommen, gegenüber den obersten Dienstbehörden anzuregen, einen ressorteinheitlichen Personalfragebogen zu entwickeln.

Im 14. Tätigkeitsbericht (S.69, Nr.11.3) und 15. Tätigkeitsbericht (5. 72, Nr, 11.2) habe ich einige datenschutzrechtliche Kriterien für die Gestaltung eines Personalbogens genannt.

Das Staatsministerium für Unterricht, Kultus, Wissenschaft und Kunst hat, unter Einbindung meiner Geschäftsstelle, bereits unabhängig von der Novellierung des Bayerischen Beamtengesetzes einen ressorteinheitlichen Personalfragebogen entwickelt. Datenschutzrechtliche Belange wurden dabei weitestgehend berücksichtigt.

12.3 Speicherung von Personaldaten auf einem privatem PC

Im Berichtszeitraum haben sich vermehrt Beschäftigte im öffentlichen Dienst an mich gewandt und um datenschutzrechtliche Stellungnahme zur Zulässigkeit der Speicherung und Verarbeitung von Personaldaten durch Dienstvorgesetzte auf deren privaten PC's gebeten.

Ich habe dazu die Auffassung vertreten, daß gegen die Speicherung und Verarbeitung von dienstlichen Personaldaten auf einem privaten PC grundsätzliche dienst- und datenschutzrechtliche Bedenken bestehen. Dies gilt auch, soweit die EDV-Geräte mit in den Dienst gebracht werden.

Art. 100 a BayBG bestimmt Begriff, Inhalt, Zweckbestimmung sowie Gliederung und Gestaltung von Personalakten. Danach ist über jeden Beamten ein Personalakt zu führen, wobei die Verwendung des Singular zum Ausdruck bringt, daß nur ein Personalakt zu führen ist, also bspw. keine geheimen Personalakten geführt werden dürfen. Der Personalakt kann nach sachlichen Gesichtspunkten in Grund- und Teilakten gegliedert werden. Teilakten (bspw. Besoldungsunterlagen) können bei der für den betreffenden Aufgabenbereich zuständigen Dienststelle geführt werden. Nebenakten (Unterlagen, die sich auch im Grundakt oder in Teilakten befinden) dürfen nur geführt werden, wenn personalverwaltende und -beschäftigende Behörde nicht identisch sind oder eine Zuständigkeit mehrerer personalverwaltender Behörden besteht. Nach Art. 100 h BayBG dürfen Personalaktendaten in Dateien nur für Zwecke der Personalverwaltung oder -wirtschaft verarbeitet oder genutzt werden. Bei erstmaliger Speicherung ist dem Betroffenen die Art der gespeicherten Daten mitzuteilen. Ferner sind Dokumentationspflichten vorgesehen.

Die Vorschriften sind nach meiner Meinung analog auch auf die nichtverbeamteten Beschäftigten des öffentlichen Dienstes anzuwenden.

Die genannten Voraussetzungen sind beim vorliegenden Sachverhalt einer Speicherung von Personaldaten auf einem privten PC in der Regel nicht erfüllt. Zudem entsteht, ungeachtet der jeweils gewählten Speicherungsform, eine Nebenpersonalakte, über die der Dienstherr auch nicht die erforderliche volle Verfügungsgewalt erhält.

Problematisch ist auch die Sicherstellung der Einsichtsrechte des Beschäftigten in seinen vollständigen Personalakt, da der Dienstherr vielfach keine Kenntnis über die auf dem privaten PC vorhandenen Daten hat.

Weiterhin ist in diesem Zusammenhang auf Art. 75 a BayPVG hinzuweisen, der u.a. eine Mitbestimmung des Personalrats bei der Einführung und Anwendung von automatisierten Verfahren zur Personalverwaltung vorsieht.

Die Schutzbestimmungen des Dienst-, Datenschutz- und Personalvertretungsrechts stehen somit der Speicherung und Verarbeitung von Personaldaten auf einem privaten PC entgegen.

12.4 Tragen von Namensschildern im öffentlichen Dienst

Eine Beschäftigte in einer Behörde mit einem hohen Maß an Publikumsverkehr hat sich an mich mit der Frage gewandt, ob sie aus datenschutzrechtlichen Gründen das Tragen eines Namensschildes verweigern könne. Die Kenntnisnahme des Namens durch Behördenbesucher ermögliche diesen die Ermittlung ihrer Anschrift und Telefonnummer. Damit seien Belästigungen möglich.

Ich habe zur Frage, in welchem Umfang sich Amtsträger auf Datenschutz oder das Recht auf informationelle Selbstbestimmung berufen können, die nachfolgende Auffassung vertreten.

Dem informationellen Selbstbestimmungsrecht kommt als Ausprägung des allgemeinen Persönlichkeitsrechtes Grundrechtscharakter zu. Wie grundsätzlich jedes Grundrecht handelt es sich aber dabei zunächst um ein Abwehrrecht des Bürgers gegenüber dem Staat.

Auch der öffentlich Bedienstete ist Grundrechtsträger gegenüber seinem Dienstherrn. Allerdings bezieht sich diese Rechtsposition nur auf jenen Bereich, in dem der Bedienstete dem Staat als eigenständiger Träger von Rechten und Pflichten gegenübersteht.

In seiner Eigenschaft als Amtsträger, also als handelndes Organ des Staates, kann der Bedienstete schon begrifflich nicht Grundrechtsträger sein. Hauptinhalt seiner Tätigkeit gegenüber dem Bürger ist der korrekte Aufgabenvollzug entsprechend den Gesetzen und unabhängig von individuellen Eigenschaften des Bediensteten.

Bei der Entscheidung über Informationsübermittlungen an Dritte, die die dienstliche Tätigkeit von Amtsträgern betreffen, ist der Dienstherr dennoch nicht völlig frei. Auf der einen Seite ist die Funktionsfähigkeit des Behördenapparates ein gewichtiges Entscheidungskriterium.

Andererseits ist auch die Fürsorge gegenüber dem Bediensteten ein gewichtiger Gesichtspunkt, der zur Geheimhaltung bestimmter Informationen über den Bediensteten führen kann.

Bei einer Abwägung, ob die Informationsinteressen der von staatlichem Handeln betroffenen Bürger oder die Fürsorge gegenüber dem Bediensteten höher zu werten sind, dürfte eine Geheimhaltung der Identität des Bediensteten nur in Frage kommen, soweit Leben und Gesundheit des Bediensteten (bspw. bei bestimmten exponierten Tätigkeiten) gefährdet oder schwerwiegende Belästigungen zu befürchten sind.

Gegen die Anordnung des Dienstherrn, Namensschilder zu tragen, bestehen unter den genannten Voraussetzungen keine datenschutzrechtlichen Bedenken. Allerdings wird das Informationsinteresse des Bürgers bereits durch die Bekanntgabe des Familiennamens gedeckt sein.

Den Interessen der Bediensteten kann im Beteilungsverfahren des Personalrates nach Art. 76 Bayer. Personalvertretungsgesetz ausreichend Rechnung getragen werden.

12.5 Prüfung einer kommunalen Personalverwaltung

Im Berichtszeitraum haben Mitarbeiter meiner Geschäftsstelle die Personalverwaltung einer Stadt datenschutzrechtlich überprüft. Gegenstand der Kontrolle waren die Erhebung von Personaldaten von Bediensteten und Bewerbern mit Hilfe von Formularen. Ferner wurde ,der Umfang und die Erforderlichkeit der in Personal-Dateien gespeicherten Daten, die aus diesen Dateien erstellten Auswertungen, die Zugriffsregelungen auf Dateien, die neben Dateien geführten manuellen Personalkarteien und Datenübermittlungen aus Dateien und Karteien überprüft. Geprüft wurde ferner die Aufbewahrung und Archivierung von Personalakten, die Bearbeitung von Beihilfeanträgen sowie Umfang und Speicherungsdauer der mittels Telefoncomputersystemen aufgezeichneten Verbindungs- und Gebührendaten.

Es ergaben sich nur geringe Mängel.

Im einzelnen wurden folgende Feststellungen getroffen:

Datenerhebung

Grundlage für die Erhebung von Personaldaten sind in der Regel der vom Betroffenen auszufüllende Personalfragebogen, weitere Fragebögen, bspw. zur Festsetzung des Besoldungsdienstalters sowie die vorgelegten Personenstandsurkunden und Prüfungsnachweise.

Gemäß Art. 16 Abs. 3 BayDSG ist ein Betroffener, wenn bei ihm Daten erhoben werden, auf die Rechtsvorschrift hinzuweisen, die ihn zu Angaben verpflichtet, bzw. auf die Freiwilligkeit, wenn eine solche Pflicht nicht besteht. Dies geschah in den augenblicklich verwendeten Personalfragebögen nicht. Ich habe deshalb gefordert, sie entsprechend zu ergänzen.

Datenübermittlungen im Zusammenhang mit der Einstellung von Bewerbern

Im Zusammenhang mit dem Auswahlverfahren bei Neueinstellungen werden Personaldaten der Bewerber an den Personalrat, die Frauenbeauftragte und den Personalausschuß bzw. ab einer bestimmten Vergütungsgruppe/Besoldungsgruppe an den Stadtrat, übermittelt.

Dem Personalrat wurden nur die zur Aufgabenerfüllung erforderlichen Unterlagen zur Verfügung gestellt (Art. 75 Abs. 1 Nr.1, Art. 69 Abs. 2 Bayerisches Personalvertretungsgesetz).

Hinsichtlich der Datenübermittlungen an die Frauenbeauftragte verweise ich auf meine grundsätzlichen Ausführungen unter Nr.12.6.

Bei der Behandlung von Personalangelegenheiten durch den Stadtrat und seine Ausschüsse ist das Recht auf informationelle Selbstbestimmung der Stellenbewerber zu beachten und gleichzeitig dem Informationsbedürfnis des Stadtrats Rechnung zu tragen. Das bedeutet, daß dem Stadtrat und seinen Ausschüssen personenbezogene Daten von Stellenbewerbern in dem Umfang mitgeteilt werden dürfen, als es zur Beschlußfassung erforderlich ist. Bei der überprüften Stadt erhielt der Stadtrat im Regelfall nur eine Bewerberliste. Dabei konnten die Unterlagen der einzelnen Bewerber nicht eingesehen werden. Es erfolgte vielmehr nur eine Auskunft daraus durch den Oberbürgermeister.

Dieses Verfahren ist aus datenschutzrechtlicher Sicht nicht zu beanstanden. Im Hinblick darauf, daß der erste Bürgermeister regelmäßig nicht verpflichtet ist, in Personalangelegenheiten den Sitzungsteilnehmern vor der Beratung Sitzungsunterlagen zuzusenden, könnte daran gedacht werden, die Unterlagen (Bewerberlisten) ggf. numeriert als Tischvorlage für die Dauer der Sitzung zur Verfügung zu stellen und anschließend wieder einzusammeln.

Umfang und Erforderlichkeit der in Dateien gespeicherten Daten

Es wurde das bei der Stadt verwendete Personalverwaltungssystem PAISY sowie die mittels Telefoncomputer erfolgte Telefondatenverarbeitung überprüft.

Hinsichtlich PAISY ergaben sich bei der von der Stadt verwendeten Version keine datenschutzrechtlichen Anmerkungen.

Für das von der Stadt betriebene Klinikum ergab sich, daß dort eine automatisierte Telefondatenerfassung erfolgte, ohne daß eine Dienstvereinbarung abgeschlossen worden war oder die Zustimmung des Personalrats eingeholt wurde. Die Zielnummer wurde in allen Fällen vollständig ausgedruckt. Dies war auch für die vom Schwesternwohnheim aus den einzelnen Appartements geführten Privatgespräche der Fall.

Der Betrieb eines Telefoncomputers ist nach Art. 75 a Abs. 1 BayPVG mitbestimmungspflichtig. Es empfiehlt sich,

über die getroffenen Regelungen eine Dienstvereinbarung abzuschließen. Ich habe gefordert, insbesondere für die aus dem Schwesternwohnheim geführten Privatgespräche eine datenschutzgerechte Lösung zu vereinbaren. Diese könnte bspw. in einem nur verkürzten Ausdruck der Zielnummer bestehen. Nur im Falle strittiger Abrechnungsfälle sollte ein vollständiger Ausdruck erfolgen.

Karteien
Die Urlaubskartei enthielt in einigen Fällen auch den Grad der Schwerbehinderung. Dieses Merkmal ist zur Aufgabenerfüllung nicht erforderlich. Es genügt die Angabe ,,Zusatzurlaub: ja/nein". Bei der Überprüfung wurden auch Karteikarten aus länger zurückliegenden Urlaubsjahren vorgefunden. Die Stadt wurde gebeten, die Aufbewahrungsdauer der Karteikarten festzulegen. Ich habe darauf hingewiesen, daß nach Art. 100 g Abs. 2 BayBG (in der Fassung eines Zwölften Gesetzes zur Änderung beamtenrechtlicher Vorschriften) für Unterlagen der genannten Art eine Aufbewahrungsdauer von 5 Jahren nach Abschluß des Jahres, in dem die Bearbeitung des einzelnen Vorgangs abgeschlossen wurde, vorgesehen ist.

Aufbewahrung und Aussonderung von Personalakten
Bei einer stichprobenartigen Überprüfung von sowohl in der Besoldungskartei als auch in der jeweiligen Personalakte vorhandenen Merkmalen ergab sich in mehreren Fällen, daß zur Begründung für eine Einstellung oder eine ausgesprochene Beförderung auch Unterlagen über vorhandene Mitbewerber in der Personalakte des Eingestellten oder Beförderten abgelegt waren.

Im Hinblick auf das Einsichtsrecht in die eigene Personalakte habe ich gefordert sicherzustellen, daß der Einsichtnehmende nicht von persönlichen Verhältnissen von etwaigen Mitbewerbern Kenntnis erlangt.

12.6 Vorlage von Bewerberlisten an die Gleichstellungsstelle für Frauen durch die Personalverwaltung

Eine Stadt hat mich um Stellungnahme gebeten, unter welchen Voraussetzungen Bewerbungsunterlagen einer Frauenbeauftragten zur Verfügung gestellt werden können.

Im Einvernehmen mit den Staatsministerien der Finanzen, des Innern und für Arbeit, Sozialordnung, Familie, Frauen und Gesundheit vertrete ich dazu die Auffassung, daß mangels entsprechender gesetzlicher Befugnisnormen ein eigenständiger Anspruch der Frauenbeauftragten auf Überlassung von Bewerberlisten und sonstigen personenbezogenen Unterlagen nicht besteht.

Das Staatsministerium des Innern hat mit Bekanntmachung vom 27.01.1989 (AllMBl Nr.8/1989, S.284) Hinweise für die Arbeit der Gleichstellungsstelle bei den Gemeinden veröffentlicht. Danach steht die Entscheidung über die Gleichstellungsstelle, ihre organisatorische Ordnung und ihr Aufgabenzuschnitt im Ermessen der Gemeinde (Organisationshoheit).

Die anfragende Stadt hat sich nach ihrer besonderen Geschäftsanweisung über die Aufgabe der Frauenbeauftragten dafür entschieden, eine städtische Dienststelle einzurichten, die dem Oberbürgermeister unmittelbar zugeordnet ist. Aufgrund dieser Organisationsform ist die Frauenbeauftragte gegenüber dem Oberbürgermeister weisungsgebunden.

Im Rahmen **seiner eigenen Zuständigkeit für Personalangelegenheiten kann der Oberbürgermeister anordnen,** daß die Personalverwaltung **Bewerberlisten an die Gleichstellungsstelle für Frauen vorlegt.** Die Frauenbeauftragte handelt danach im Auftrag des Oberbürgermeisters; der Umfang der zulässigen Datenoffenbarung an sie wird von diesem Auftrag begrenzt.

Ich empfehle allgemein, den Umfang der bei Neuemstellungen und Neubesetzungen zur Verfügung zu stellenden Unterlagen konkret zu beschreiben.

Hinsichtlich der Einsichtnahme in Personalakten (-daten) bemerke ich, daß mit Rücksicht auf das Personalaktengeheimnis der einsichtnehmende Personenkreis möglichst eng zu halten ist.

Dementsprechend sieht Art. 100 a Abs. 3 BayBG (i.d.E eines Zwölften Gesetzes zur Änderung beamtenrechtlicher Vorschriften) vor, daß Zugang zum Personalakt nur Beschäftigte haben dürfen, die im Rahmen der Personalverwaltung mit **der Bearbeitung von Personalangelegenheiten beauftragt** sind, und nur soweit dies zu Zwecken der Personalverwaltung oder Personalwirtschaft erforderlich ist.

Diese Vorgaben sind bei der Frauenbeauftragten der anfragenden Stadt nicht erfüllt.

Es ist für eine Einsichtnahme in einen Personalakt deshalb ein konkreter Auftrag des Oberbürgermeisters, als Dienstvorgesetzter der Beschäftigten der Stadt, erforderlich. Dabei ist stets auch zu prüfen, ob nicht eine Auskunft oder eine Überlassung von Auszügen bereits zur zugewiesenen Aufgabenerledigung ausreichend ist.

Ich vertrete die Auffassung, daß weitergehende Rechte der Frauenbeauftragten - etwa auf weisungsfreies Handeln oder auf eigenständige Informationsansprüche -wegen des damit verbundenen Eingriffs in das informationelle Selbstbestimmungsrecht der Betroffenen nur durch Landesgesetz geschaffen werden können.

Hinsichtlich der Möglichkeit der Weitergabe von zulässigerweise erhaltenen Informationen durch die Frauenbeauftragte bemerke ich:

Die im Rahmen des Einstellungsverfahrens angefertigten Bewerberlisten werden für eine effektive Organisation des Auswahlverfahrens benötigt. Ihnen kommt Sachaktenqualität zu. Gleiches gilt für Bewerbungsunterlagen.

Die Unterlagen über die externen Bewerber erlangen erst mit der tatsächlichen Einstellung Personalaktenqualität.

Beim Umgang mit den genannten Unterlagen hat die Frauenbeauftragte somit die Vorschriften des Bayerischen Datenschutzgesetzes zu beachten. Daraus folgt, daß die Frauenbeauftragte personenbezogene Informationen an einzelne Mandatsträger oder Gruppierungen nicht weitergeben darf. Das Kontroll- und Informationsrecht und die Entscheidungskompetenz in Personalangelegenheiten des Stadtrats und seiner Ausschüsse bleiben davon unberührt.

12.7 Ermittlung von Fehlzeiten und Mitteilung an den Gemeinderat

Mehrere Zuschriften von Gemeindebediensteten beschäftigten sich mit der Frage, ob es zulässig sei, Krankmeldungen namentlich über einen längeren Zeitraum auszuwerten und die Auswertung personenbezogen dem Gemeinderat mitzuteilen.

In mehreren Entscheidungen stellt das Bundesarbeitsgericht fest, daß Vorschriften des Datenschutzrechts den genannten Auswertungen nicht entgegenstehen. Das Gericht führt aus, daß die Speicherung und Verarbeitung personenbezogener Daten im Rahmen der Zweckbestimmung eines Arbeitsvertragsverhältnisses oder zur Wahrung berechtigter Interessen des Arbeitgebers zulässig ist, wenn kein Grund zu der Annahme besteht, daß dadurch schutzwürdige Belange des Arbeitnehmers beeinträchtigt werden.

Der Zweck eines Arbeitsverhältnisses ist der Austausch von Arbeitsleistung gegen Zahlung von Arbeitsentgelt. Von daher entspricht es einem berechtigten Interesse des Arbeitgebers, festzustellen, inwieweit dieses Austauschverhältnis durch Krankheits- und Fehlzeiten gestört ist. Diesem Interesse kann dadurch genügt werden, daß solche Aussagen und Erkenntnisse ohne Einsatz technischer Hilfsmittel erarbeitet werden, es ist aber auch ein berechtigtes Interesse des Arbeitgebers anzuerkennen, sich diejenigen Kenntnisse, die er berechtigterweise benötigt, in wirtschaftlich sinnvoller Weise schnell und kostengünstig unter Einsatz automatisierter Verfahren zu verschaffen.

Im letzteren Fall ist allerdings das Mitbestimmungs**recht** des Personalrats nach Art. 75 a Abs. 1 BayPVG zu beachten.

Schutzwürdige Belange der Arbeitnehmer machen eine solche Datenverarbeitung nicht von vorne herein unzulässig. Zwar werden durch die genannten Auswertungen auch schutzwürdige Belange der Arbeitnehmer berührt, als der Arbeitgeber Erkenntnisse gewinnen kann, die den Arbeitnehmern - wenn auch berechtigterweise - zum Nachteil gereichen können. Das allein schließt die Datenverarbeitung aber noch nicht aus. Die Grenze für die Zulässigkeit einer Datenverarbeitung ergibt sich vielmehr erst aus einer Abwägung der berechtigten Interessen des Arbeitgebers und der schutzwürdigen Belange des Arbeitnehmers.

Zur Übermittlung von Zusammenstellungen über die Fehlzeiten von Gemeindebediensteten an den Gemeinderat bemerke ich:

Gemäß Art. 29 GO wird eine Gemeinde durch den Gemeinderat verwaltet, soweit nicht der erste Bürgermeister selbständig entscheidet. In die Entscheidungskompetenz des ersten Bürgermeisters fallen insbesondere die laufenden Angelegenheiten und die Dienstaufsicht über die Bediensteten der Gemeinde (Art. 37 GO). Der Gemeinderat ist im Zusammenhang mit den mit einer Gemeinde bestehenden Dienst- und Arbeitsverhältnissen für statusrechtliche Entscheidungen wie Ernennungen, Beförderungen, Entlassungen u.ä. zuständig (Art. 43 GO).

Gegen eine personenbezogene oder -beziehbare Mitteilung der Fehlzeiten bestehen Bedenken, soweit es sich nicht um eine statusrechtliche Entscheidung im konkreten Einzelfall (z.B. eine ins Auge gefaßte Entlassung wegen dauerndem Fehlen) handelt. Die Würdigung von Fehlzeiten dürfte in der Regel Teil der Dienstaufsicht sein, welche, wie bereits erwähnt, vom ersten Bürgermeister auszuüben ist.

Auch außerhalb statusrechtlicher Angelegenheiten mögen Fallgestaltungen denkbar sein, in denen eine personenbezogene Bekanntgabe von Personaldaten an den Gemeinderat zulässig ist (z.B. nach einem Beschluß zur Wahrnehmung des Kontrollrechtes des Gemeinderates über die ordnungsgemäße Amtsführung des Bürgermeisters in Personalangelegenheiten), doch auch hier wäre in erster Linie eine Bekanntgabe der Personalaktendaten nicht an den gesamten Gemeinderat, sondern nur an den Personalausschuß angemessen. Erst als letztes käme eine Behandlung der Angelegenheit in einer aufgrund der Sensibilität der Daten nichtöffentlichen Sitzung des Gemeinderats in Betracht.

12.8 Einsichtnahme des Betroffenen in Sitzungsprotokolle des Personalausschusses

Eine Stadt hat angefragt, ob einem städtischen Mitarbeiter Einsicht in die Niederschrift über eine nichtöffentliche Sitzung des Personalausschusses gewährt werden kann, soweit in dieser Sitzung eine den Mitarbeiter betreffende Personalentscheidung getroffen wurde. Bei den Protokollen handelte es sich um Inhaltsprotokolle, denen auch die Äußerungen der einzelnen Diskussionsteilnehmer zu entnehmen waren.

Im Einvernehmen mit dem Staatsministerium des Innern vertrete ich die Ansicht, daß im Zusammenhang mit dem geschilderten Sachverhalt zu prüfen ist, ob einem (Inhalts-)Protokoll einer nichtöffentlichen Gemeinderatsoder Personalausschußsitzung Personalaktenqualität zukommen kann, mit der Folge, daß dem Betroffenen ein Einsichtsrecht nach Art. 100 d Abs. 2 BayBG (neu) zusteht

oder ob auf dieses Protokoll vielmehr die Vorschriften des Art. 52 Abs. 3, Art. 54 Abs. 3 GO anzuwenden sind.

Das Bundesverwaltungsgericht hat mit Urteil vom 04.08.1975 (NJW 76, 204) entschieden, daß eine Stellungnahme einer Gemeinde zur Personalentscheidung einer anderen Stelle, die mittels eines Gemeinderatsprotokolis abgegeben worden ist, Teil der Personalakte des abgelehnten Bewerbers ist. Das Gericht hat dem Betroffenen dementsprechend ein Einsichtsrecht in das Sitzungsprotokoll zugesprochen, auch soweit darin Vorgänge aufgeführt waren, die Mitbewerber betrafen.

Der vorliegende Sachverhalt ist jedoch anders gelagert. Hier geht es nicht um eine Stellungnahme der Gemeinde in Form eines Sitzungsprotokolls, sondern um eine von der Gemeinde selbst zu treffende Personalentscheidung.

Der (materielle) Personalaktenbegriff umfaßt alle Unterlagen und Vorgänge, die in einem unmittelbaren inneren Zusammenhang mit dem Dienstverhältnis des Beamten stehen. Die Stellungnahme einer Gemeinde zu einer Stellenbesetzung zählt danach zu den Personalakten. Auch das Sitzungsprotokoll, das in dem vom BVerwG entschiedenen Fall diese Stellungnahme der Gemeinde darstellte, zählt zu den Personalakten. Dies muß jedoch nicht ohne weiteres für jedes andere Sitzungsprotokoll geiten, das Beratung und Beschlußfassung in Personalangelegenheiten enthält. Das Inhaltsprotokoll dokumentiert den internen Entscheidungsbildungsprozeß, welcher dem Beschluß des Ausschusses selbst vorausgeht und ihn vorbereitet; dieser Teil ist begrifflich von dem Beschluß selbst zu unterscheiden, der sich auf die Wiedergabe der maßgeblichen Erwägungen beschränken kann.

Für diese Differenzierung spricht auch, daß die Gemeinde anstelle von Inhaltsprotokollen reine Ergebnisniederschriften über die gefaßten Beschlüsse fertigen könnte, so daß durch Einsicht kein Bild aller vom Gemeinderat angestellten Erwägungen zu gewinnen wäre.

Ich vertrete deshalb die Auffassung, daß Teil des Personalakts nur der jeweilige **Beschluß,** nicht aber die Protokollierung der vorangehenden Debatte ist. Für Einsichtnahmen in den Protokollteil, der die Debatte wiedergibt, ist nur die GO anzuwenden (Art. 52 Abs. 3, 54 Abs. 3). Für Einsichtnahmen in den Beschlußteil des Protokolls ist sowohl die GO (Einsichtnahme eines Dritten), als auch das Beamtengesetz (Einsichtnahme als betroffener Beamter) anzuwenden. Nach der GO sind nur die in nichtöffentlicher Sitzung gefaßten Beschlüsse - nicht jedoch auch die Teile der Niederschriften, die die Debatte wiedergeben - der Öffentlichkeit bekanntzugeben, sobald die Gründe für die Geheimhaltung weggefallen sind. Dies ist bei Personalentscheidungen regelmäßig mit der Beschlußfassung der Fall.

Die Nichtöffentlichkeit einer Sitzung dient nicht nur dem Schutz des Betroffenen, sondern auch einer objektiven und unbeeinflußbaren Amtsausübung der Ratsmitglieder. Die durch den Ausschluß der Öffentlichkeit ermöglichte freie und vertrauliche Aussprache würde gefährdet, wenn Stellenbewerber (denen in der nichtöffentlichen Sitzung kein Anwesenheitsrecht eingeräumt ist) Einsicht in das vollständige Inhaltsprotokoll nehmen könnten.

Unabhängig davon bin ich der Auffassung, daß sich ein Einsichtsrecht - sollte es doch ausnahmsweise zu bejahen sein (z.B. weil im Vollzug der Gemeinderatsentscheidung nicht nur auf den Beschluß, sondern auch auf die einzelnen Erwägungen des Gemeinderats und die Niederschrift Bezug genommen wird) - lediglich auf den **Inhalt** einer Außerung, **nicht** aber auf ihren **Urheber** erstrecken könnte. Die Namen von Rednern wären danach vor der Einsichtnahme unkenntlich zu machen, um deren Recht auf vertrauliche, unbefangene Aussprache zu schützen. Diese Erwägungen treffen sowohl für Gemeinderatsentscheidungen als auch für Personalausschußentscheidungen zu.

12.9 Weitergabe von Personalakten an ein gemeindeeigenes Archiv

Eine Gemeinde hat angefragt, ob es aus datenschutzrechtlichen Gründen zulässig ist, Personalakten an das gemeindeeigene Archiv abzugeben und welche Zeiträume dabei zu beachten sind.

Nach Art. 13 Abs. 1 des Bayerischen Archivgesetzes regeln die Gemeinden, Landkreise und Bezirke und die sonstigen kommunalen Körperschaften, Anstalten und Stiftungen des öffentlichen Rechts und ihre Vereinigungen die Archivierung der bei ihnen erwachsenen Unterlagen in eigener Zuständigkeit.

Es gehört zu den Aufgaben jeder kommunalen Körperschaft, für den Geschäftsgang zu sorgen und die dafür notwendigen Einrichtungen zu schaffen. Die kommunalen Körperschaften, Anstalten und Stiftungen des öffentlichen Rechts sind aufgrund der kommunalen Vorschriften in Verbindung mit Art. 13 Abs. 1 und 2 des Bayerischen Archivgesetzes verpflichtet, für die Archivierung ihrer Unterlagen in einem Archiv Sorge zu tragen. Unterlagen sind dem zuständigen Archiv anzubieten, soweit eine Behörde, ein Gericht oder eine öffentliche Stelle diese nicht mehr zur Aufgabenerfüllung benötigt.

Der Abgabe von Personalakten stehen datenschutzrechtliche Vorschriften nicht entgegen. Das Bayerische Datenschutzgesetz ist nur anzuwenden, soweit keine spezialgesetzliche Regelung besteht. Eine solche besteht aber in Art. 13 Abs. 2 i.V.m. Art. 6 Abs. 1 Satz 3 des Bayerischen Archivgesetzes.

Ich habe empfohlen, die Übergabe der Unterlagen entsprechend der Aussonderungsbekanntmachung der Bayerischen Staatsregierung vom 19.11.1991 (Staatsanzeiger 1991 Nr.48) zu dokumentieren.

Für den Zeitpunkt der Übergabe der Personalunterlagen ist Art. 100 g Bayerisches Beamtengesetz i.d.F. eines 12. Gesetzes zur Änderung beamtenrechtlicher Vorschriften zu beachten.

Das Gesetz ist meines Erachtens hinsichtlich der Vorschriften zur Personalaktenführung auch für nicht verbeamtete Bedienstete bei kommunalen Körperschaften analog anzuwenden.

Danach sind Personalakten von der personalaktenführenden Behörde nach ihrem Abschluß noch 5 Jahre aufzubewahren.

13. Gewerbe und Handwerk

13.1 Schaffung von bereichsspezifischen Datenschutzregelunge in gewerberechtlichen Vorschriften

Am 01.01.1994 traten das Gesetz zur Änderung der Handwerksordnung, anderer handwerksrechtlicher Vorschriften und des Berufsbildungsgesetzes vom 20.12.1993 (BGB1 1 S.2256 ff) und Teile des Gesetzes zur Änderung des Gesetzes auf dem Gebiet des Rechts der Wirtschaft vom 21.12.1992 (BGBl 1 S.2133 ff) in Kraft. Inzwischen wurde auch das Gesetz zur Änderung der Gewerbeordnung und sonstiger gewerberechtlicher Vorschriften vom 23.11.1994 verkündet (BGB1 1 S.3475 ff.).

Diese Gesetze schaffen u.a. Rechtsgrundlagen für die Erhebung, Verarbeitung und Nutzung personenbezogener Daten in der Handwerksordnung, der Gewerbeordnung und dem Gesetz zur vorläufigen Regelung des Rechtes der Industrie- und Handelskammern (IHK-G).

Im Gesetz zur Änderung der Gewerbeordnung werden u.a. die **Datenübermittlungen aus den Gewerbeanzeigen**, die jeder Gewerbetreibende nach § 14 Gewerbeordnung zu erstatten hat, geregelt. Die Ergänzung des § 14 Gewerbeordnung (GewO), die am 01.12.1995 in Kraft treten wird, sieht nun u.a. vor, daß die Übermittlung von Name, betrieblicher Anschrift und angezeigter Tätigkeit aus der Gewerbeanzeige an nichtöffentliche Stellen und an öffentlich-rechtliche Unternehmen, die am Wettbewerb teilnehmen, nur dann zulässig ist, wenn der Auskunftsbegehrende ein berechtigtes Interesse an der Kenntnis der zu übermittelnden Daten glaubhaft macht. Die Übermittlung weiterer Daten aus der Gewerbeanzeige ist nur zulässig, wenn der Auskunftsbegehrende ein rechtliches Interesse, insbesondere zur Geltendmachung von Rechtsansprüchen, an der Kenntnis der zu übermittelnden Daten glaubhaft macht und kein Grund zu der Annahme besteht, daß das schutzwürdige Interesse des Gewerbetreibenden überwiegt (§14 Abs. 8 GewO).

In die Handwerksordnung wurden u.a. Regelungen über die Daten, die in der **Handwerksrolle** und in der **Lehrlingsrolle** gespeichert werden dürfen, aufgenommen. Bei der Lehrlingsrolle wurde, wohl durch ein unbeabsichtigtes Versehen, in die Aufzählung der einzelnen Daten die Anschrift des Lehrlings nicht aufgenommen, nur die des gesetzlichen Vertreters. Bei volljährigen Lehrlingen benötigt jedoch die Handwerkskammer diese Anschrift, da die Zustellungen von Briefen über den Betrieb an den Lehrling sowohl aus praktischen Gründen als auch aus datenschutzrechtlicher Sicht nicht wünschenswert ist. Ich halte es daher für vertretbar, bis zu einer Änderung der Handwerksordnung die Speicherung der Adressen von volljährigen Lehrlingen in der Lehrlingsrolle zu dulden.

13.2 Änderung des Schornsteinfegergesetzes

Durch das Gesetz zur Änderung des Schornsteinfegergesetzes vom 20.07.1994 (BGBl I S.1624 ff.) wurden u.a. bereichsspezifische Datenschutzregelungen in das Schornsteinfegergesetz aufgenommen. Dabei handelt es sich vor allem um Regelungen zum Umfang der Daten, die ein Schornsteinfegermeister zu einer Feuerungsanlage aufzuzeichnen und in das Kehrbuch einzutragen hat sowie unter welchen Voraussetzungen Daten aus dem Kehrbuch an Dritte übermittelt werden dürfen. An **nichtöffentliche** Stellen dürfen personenbezogene Daten nur übermittelt werden, soweit der Empfänger ein **rechtliches** Interesse an der Kenntnis der Daten glaubhaft darlegt **und** der Betroffene kein schutzwürdiges Interesse an dem Ausschluß der Übermittlung hat (§19 Abs. 4 Satz 1 Schornsteinfegergesetz). Durch die Voraussetzung, daß ein rechtliches und nicht nur ein berechtigtes Interesse des Empfängers glaubhaft dargelegt werden muß, soll verhindert werden, daß die Aufzeichnungen des Schornsteinfegermeisters nicht auch für Zwecke außerhalb wirklicher Gefährdungen und außergewöhnlicher Belästigungen genutzt werden können. Es sollen z.B. keine Daten über Betreiber privater Kleinfeuerungsanlagen für Werbezwecke und allgemeine Nachbarstreitigkeiten übermittelt werden können.

13.3 Auskünfte über das Vorliegen einer Erlaubnis nach § 34 c Gewerbeordnung (GewO)

Eine Immobilienfirma bat mich um Auskunft, ob ihr das Gewerbeamt der Gemeinde oder des Landratsamts mitteilen dürfe, ob eine Person, mit der sie eine geschäftliche Zusammenarbeit beabsichtigte, im Besitz einer Erlaubnis nach § 34 c GewO (sogenannte Maklererlaubnis) ist. Die Firma begründete ihren Wunsch damit, daß sie künftige Geschäftspartner auf deren Seriosität hin prüfen möchte.

1. **Auskünfte aus den Gewerbeanzeigen nach § 14 GewO**

   In die Gewerbeanzeige nach § 14 GewO, die in Bayern bei den Gemeinden zu erstatten ist, ist bei der Anmeldung eines erlaubnispflichtigen Gewerbes auch einzutragen, ob eine Erlaubnis vorliegt. § 14 GewO regelt nach seiner Änderung durch das Gesetz zur Änderung der Gewerbeordnung und sonstiger gewerberechtlicher Vorschriften vom 23.11.1994 (BGBl I S.3475 ff.), welche Auskünfte aus den Gewerbeanzeigen erteilt werden **können.** Er sieht keinen Rechtsanspruch Dritter auf Mitteilung von Angaben aus den Gewerbeanzeigen vor. Die Unterlagen der

Gemeinde über Gewerbeanzeigen sind kein öffentliches Register. Auskünfte an Privatpersonen aus Gewerbeanzeigen über den Namen, die betriebliche Anschrift und die angezeigte Tätigkeit des Gewerbetreibenden können dann übermittelt werden, wenn der Auskunftsbegehrende ein **berechtigtes Interesse** an der Kenntnis der Daten glaubhaft macht. Die Übermittlung weiterer Daten aus der Gewerbeanzeige, beispielsweise ob eine Erlaubnis vorliegt, ist nur dann zulässig, wenn der Auskunftsbegehrende ein **rechtliches** Interesse, insbesondere zur Geltendmachung von Rechtsansprüchen, an der Kenntnis der zu übermittelnden Daten glaubhaft macht und kein Grund zu der Annahme besteht, daß das schutzwürdige Interesse des Gewerbetreibenden überwiegt (§14 Abs. 8 GewO). Das rechtliche Interesse ist ein Teilbereich des berechtigten Interesses. Das rechtliche Interesse ist an das Vorliegen eines besonderen Rechtsgrundes geknüpft. Es ist anzunehmen, wenn bestehende Unsicherheiten über ein Rechtsverhältnis zu klären sind oder Rechtsansprüche durchgesetzt werden sollen. In der Regel werden Rechtsbeziehungen, z.B. Verträge zwischen dem Betroffenen und der anfragenden Privatperson bestehen. Diese Rechtsbeziehungen können durchaus auch wirtschaftliche Interessen verfolgen. Bloße **vorvertragliche Beziehungen, vor allem auch das Bedürfnis einer Bonitätsprüfung, sind zwar ein berechtigtes, aber kein rechtliches Interesse.** Aus den Gewerbeanzeigen. können daher Auskünfte über eine Erlaubnis nach § 34 c GewO zum Zwecke der vorvertraglichen Prüfung, ob ein möglicher Geschäftspartner seriös ist, nicht erteilt werden. Die Neufassung des § 14 GewO tritt am 01.12.1995 in Kraft.

2. **Auskünfte durch die Erlaubnisbehörde**

Erlaubnisse nach § 34 c GewO werden in Bayern von den Kreisverwaltungsbehörden (Landratsämter und kreisfreie Städte) erteilt. DieUnterlagenderErlaubnisbehörde sind kein öffentliches Register. Wiepersonenbezogene Daten im Zusammenhang mit Erlaubnisverfahren zu erheben, verarbeiten und zu nutzen sind, regelt der mit dem oben genannten Gesetz in die Gewerbeordnung eingefügte § 11 GewO. Danach können nur **öffentliche** Stellen, die aufgrund einer Rechtsvorschrift am Verwaltungsverfahren beteiligt waren, darüber informiert werden, ob eine Erlaubnis erteilt, abgelehnt, widerrufen oder zurückgenommen wurde. Übermittlungen für andere Zwecke sind nur zulässig, soweit die Kenntnis der zu übermittelnden Daten zur Verfolgung von Straftaten erforderlich istodereinebesondere Rechtsvorschrift die Übermittlung vorsieht (§ 11 Abs. 5 GewO). Einebesondere Rechtsvorschrift, die eine Datenübermittlung an Privatpersonen für eine Seriositätsprüfung vorsieht existiert nicht, so **daß die Erlaubnisbehörden dem Bürger die gewünschte Auskunft ebenfalls nicht erteilen dürfen. §** 11 GewO tritt am 01.02.1995 in Kraft.

14. Statistik

14.1 Mikrozensusgesetz

Das Bundesministerium des Innern hat einen ersten Arbeitsentwurf eines ab 1996 geltenden Mikrozensusgesetzes vorgelegt. Der Entwurf sieht eine erhebliche Ausweitung des Fragenkatalogs, insbesondere hinsichtlich des Freizeitverhaltens (Reisen, Ausflüge), vor. Außerdem wird für eine Vielzahl bisher freiwilliger Auskünfte eine Auskunftspflicht vorgesehen.

Ich vertrete dazu die Auffassung, daß sich die Frage nach der fachlichen Notwendigkeit der einzelnen Erhebungsmerkmale einer datenschutzrechtlichen Bewertung entzieht, jedenfalls insoweit, als diese nicht außerhalb jeder Vertretbarkeit liegen.

Kernbereiche des Persönlichkeitsschutzes werden bei den vorgesehenen Fragen nur im Gesundheitsbereich berührt. Der Entwurf sieht die Beantwortung dieser Fragen nur auf freiwilliger Basis vor.

Es ist für mich allerdings nicht nachvollziehbar, für welche Planungsaufgaben des Staates umfangreiche Erhebungen des Freizeitverhaltens - darüber hinaus belegt mit einer Auskunftspflicht - erforderlich sein sollen.

Die Akzeptanz der Erhebung durch den Bürger wird dadurch verschlechtert. Auch die Statistikbehörden weisen mit Nachdruck darauf hin, daß mit den geforderten Erweiterungen die Grenzen des Machbaren deutlich überschritten werden.

Auch wenn es sich um kein Datenschutzproblem im engeren Sinne handeln mag, werde ich das Staatsministerium des Innern bitten, bei Beratung des Gesetzesentwurfs eine deutliche Reduzierung des Erhebungskatalogs und der mit einer Auskunftspflicht belegten Fragen zu befürworten.

14.2 Gebäude- und Wohnungsstichprobe 1993

Nach § 1 Nr.2 i.V.m. § 3 Abs. 2 des Gesetzes über gebäude- und wohnungsstatistische Erhebungen (Wohnungsstatistikgesetz - WoStatG) war nach dem Stand vom 30.09.1993 eine Gebäude- und Wohnungsstichprobe auf repräsentativer Grundlage mit einem Auswahlsatz von 1 v.H. der Wohnungen durchzuführen. Für die Erhebung wurde durch § 9 WoStatG eine Auskunftspflicht angeordnet.

Mitarbeiter meiner Geschäftsstelle haben im Berichtszeitraum die praktische Durchführung der statistischen Erhebung bei den Auskunftspflichtigen bis hin zum Rücklauf der Erhebungsunterlagen beim Bayerischen Landesamt für Statistik und Datenverarbeitung überprüft. Dabei waren von besonderem Interesse die Verfahren über die Auswahl der Erhebungsbeauftragten (Interviewer) und der Auskunftspflichtigen (Ziehung der Stichprobe).

Die Erhebung der statistischen Merkmale erfolgt vor Ort (bei den Haushalten) durch sogenannte Erhebungsbeauftragte im Rahmen einer Befragung.

Nach § 7 Abs. 1 WoStatG hat das Landesamt diese Erhebungsbeauftragten auszuwählen und zu bestellen. Die Erhebungsbeauftragten dürfen nicht in der unmittelbaren Nähe ihrer Wohnung eingesetzt werden. Nach § 14 Bundesstatistikgesetz (BStatG) dürfen Erhebungsbeauftragte darüber hinaus nicht eingesetzt werden, wenn aufgrund ihrer beruflichen Tätigkeit oder aus anderen Gründen Anlaß zur Besorgnis besteht, daß Erkenntnisse aus der Tätigkeit als Erhebungsbeauftragte zu Lasten der Auskunftspflichtigen genutzt werden.

Für die Durchführung der Gebäude- und Wohnungsstichprobe 1993 (GWS 93) wurde in erster Linie auf die für die laufenden Erhebungen im Rahmen des Mikrozensus eingesetzten Interviewer zurückgegriffen. Soweit für bestimmte regionale Bereiche darüber hinaus noch Bedarf bestand, wurden durch Aushang in Gemeindeverwaltungen zusätzliche Mitarbeiter geworben.

Zur Vermeidung von Interessenkonflikten wurden analog zu den für die Durchführung der Volkszählung 1987 entwickelten Grundsätzen keine Finanz- und Polizeibeamte sowie keine Mitarbeiter von Meldebehörden zu Erhebungsbeauftragten bestellt. Eine Speicherung des Datums ,,Beruf" in der eingerichteten Interviewerkartei und -datei erfolgte nicht. Die Abklärung der Sachlage wurde vielmehr in einem persönlichen oder fernmündlichen Gespräch vorgenommen.

,,Unmittelbare Nachbarschaft" liegt nach den für die Durchführung der Volkszählung 1987 entwickelten Grundsätzen vor, wenn Erhebungsbeauftragter und Auskunftspflichtige in der gleichen Straße (dem gleichen Straßenabschnitt) wohnen. Das Landesamt hat durch einen Adressenabgleich im Vorfeld der Erhebung versucht, den nicht zulässigen Einsatz von Interviewern in ihrem unmittelbaren Umfeld auszuschließen. Zusätzlich wurden die zur Tätigkeit als Erhebungsbeauftragte bereiten Personen bei einer Schulung auf die Problematik hingewiesen und gebeten, sich bei Ausgabe der Auswahlbezirke ggf. zu melden, um über einen Bezirkstausch den gesetzlichen Vorgaben Genüge zu tun.

Das vom Landesamt angewandte Verfahren schließt Konflikte nicht von vornherein völlig aus, es macht diese aber sehr unwahrscheinlich und ist aus datenschutzrechtlicher Sicht ausreichend.

Im Anschluß an die bereits erwähnten Interviewerschulungen erfolgte eine schriftliche Verpflichtung gemäß § 1 des Verpflichtungsgesetzes und die Bestellung zum Erhebungsbeauftragten.

Datenschutzrechtliche Bedenken gegen dieses Verfahren habe ich nicht erhoben.

Die Auswahl der Auskunftspflichtigen erfolgte aufgrund einer der gemäß § 15 Abs. *5* Volkszählungsgesetz 1987 nach Abschluß der Volkszählung für Zwecke künftiger Gebäude-, Wohnungs- und Bevölkerungsstichprobenerhebungen gezogenen 20 Vorratsstichproben.

Diese Vorratsstichproben wurden laufend aktualisiert. Bei der Aktualisierung wurde ein Verfahren der direkten Beobachtung der Neubautätigkeit angewandt. Grundlage waren dabei die in der Bautätigkeitsstatistik erfaßten Baugenehmigungen.

Dabei wurde die erste Seite des Erhebungsbogens für Baugenehmigungen für Zwecke der GWS 93 genutzt.

Das zweite Gesetz über die Durchführung von Statistiken der Bautätigkeit und die Fortschreibung des Gebäudestandes vom 27.07.1978 sieht eine solche Nutzung nicht vor. Auch im Bundesstatistikgesetz findet sich dafür keine Rechtsgrundlage. § 16 BStatG, der sich mit der statistischen Geheimhaltung befaßt, bestimmt in Absatz 2, daß die Übermittlung von Einzelangaben zwischen den mit der Durchführung einer Bundesstatistik betrauten Personen und Stellen zulässig ist, soweit dies zur Erstellung der Bundesstatistik erforderlich ist.

Nach Ansicht des Landesamtes ist mit dem Singular ,,der Bundesstatistik" nicht die einzelne Bundesstatistik gemeint, sondern das gesamte Gebäude der Bundesstatistik.

Im Gegensatz dazu vertrete ich die auch durch Kommentarliteratur gestützte Auffassung, daß es sich nur um Daten einer Bundesstatistik handeln darf. § 16 Abs. 2 BStatG sieht die amtliche Statistik nicht als Gesamtheit an, sondern behandelt jede einzelne Bundesstatistik für sich.

Für diese Gesetzesauslegung spricht auch § 15 Abs. 5 Volkszählungsgesetz. Danach ist es möglich, die Ergebnisse der Volkszählung 1987 zur Ziehung sogenannter Vorratsstichproben für Zwecke künftiger Gebäude-, Wohnungs- und Bevölkerungsstichproben zu nutzen.

Desweiteren bestimmt § 15 Abs. 5 Satz 6 Volkszählungsgesetz: ,,Aus der Arbeitsstättenzählung dürfen die statistischen Ämter für Wirtschafts-, Lohn- und Umweltstatistiken, die als **Bundesstatistiken** durchgeführt werden, ... nutzen: Name ...

§ 15 Abs. *5* wäre als überflüssig anzusehen, soweit die Ansicht des Landesamtes, daß bereits § 16 Abs. 2 BStatG den Datenaustausch zwischen einzelnen Statistiken innerhalb des ,,Gebäudes der Bundesstatistik" ermögliche, zutreffend wäre.

Unabhängig davon ist auch zu prüfen, ob die Übermittlung von Hilfsmerkmalen aus der Bautätigkeitsstatistik unter Berücksichtigung des durch § 12 BStatG bestimmten Gebots der frühestmöglichen Trennung von Hilfs-und Erhebungsmerkmalen unzulässig ist.

Nach Ansicht des Landesamtes ist § 12 BStatG nicht einschlägig, da § 16 BStatG die grundlegende Vorschrift sei, welche die Geheimhaltung statistischer Einzelangaben

regele. Nach dieser Vorschrift sei nach Auffassung des Landesamtes die Übermittlung zulässig. Sie könne deshalb nicht nach § 12 BStatG unzulässig sein.

Nachdem ich der Auslegung des Landesamtes zu § 16 Abs. 2 BStatG nicht folgen kann, sehe ich auch einen Verstoß gegen § 12 BStatG als gegeben.

Ich habe mich an den Bundesbeauftragten für den Datenschutz mit der Bitte gewandt, zu klären, ob das geschilderte Verfahren bundesweit angewandt wurde und eine Stellungnahme des Statistischen Bundesamtes einzuholen.

15. Landwirtschaft

15.1 Daten über Landwirtschaftsförderung in einem Landschafts- und Flächennutzungsplan

In dem genehmigten Landschaftsplan und Flächennutzungsplan einer Gemeinde wurden Flächen dargestellt, für die Fördermittel aus dem Kulturlandschaftsprogramm (KULAP) gewährt worden waren. Diese Angaben waren jedoch nicht erforderlich, ihre Bereitstellung durch das Amt für Landwirtschaft und Ernährung war unzulässig.

In dem Plan sind die geförderten Flächen flächenscharf dargestellt. Aufgrund dieser Darstellung konnten Personen mit Ortskenntnissen Bezüge zum Grundstückseigentümer herstellen. Eigentümer konnten im übrigen auch über Kataster und Grundbuch festgestellt werden.

Die Darstellung von Flächen, die in ein Extensivierungsprogramm, z. B. KULAP, oder in Förderprogramme des Staatsministeriums für Landesentwicklung und Umweltfragen einbezogen sind, ist nach Darlegung dieses Ministeriums weder im Landschaftsplan noch im Flächennutzungsplan üblich oder erforderlich. Das Bayerische Staatsministerium für Ernährung, Landwirtschaft und Forsten hat in seiner Stellungnahme festgestellt, daß die Übermittlung solcher Angaben vom Amt für Landwirtschaft zur Darstellung im Landschafts- bzw. Flächennutzungsplan zur Aufgabenerfüllung nicht erforderlich ist. Die Übermittlung und Darstellung dieser Daten in den genannten Plänen verstieß auch gegen den Zweckbindungsgrundsatz.

Die Übermittlung der personenbeziehbaren Daten aus der Teilnahme am Kulturlandschaftsprogramm KULAP durch ein Amt für Landwirtschaft und Ernährung an die Gemeinde wurde daher beanstandet. Die Ämter für Landwirtschaft und Ernährung wurden vom Landwirtschaftsministerium aufgefordert, die Weitergabe der KULAP-Daten - auch gemeindeweise zusammengefaßt - im Rahmen von Stellungnahmen als Träger öffentlicher Belange zu unterlassen.

Die Gemeinde habe ich über die Unzulässigkeit der entsprechenden Angabe im Landschaftsplan und Flächennutzungsplan unterrichtet. Ich habe gefordert, Maßnahmen zu ergreifen, die verhindern, daß diese Angaben aus den Plänen weiterhin unverändert genutzt oder übermittelt werden. Da die Pläne öffentlich, d.h. für jedermann einsehbar sind, müssen zu den betreffenden Flächen Änderungen vorgenommen werden. Die Gemeinde hat eine Korrektur der Pläne zugesichert.

15.2 Einschaltung von Bauernverband und Obmännern nach dem Grundstücksverkehrsgesetz

Siehe hierzu den Beitrag unter Nr. 8.6.

16. Schulwesen

16.1 Weitergabe von Schülernamen

Immer wieder erreichen mich Anfragen, unter welchen Voraussetzungen die Namen von Schülern und Erziehungsberechtigten an außerschulische Institutionen weitergegeben werden dürfen.

Die Frage, ob Schülernamen von einer Schule an Kreditinstitute weitergegeben werden können, beurteilt sich nicht nach dem Bayerischen Datenschutzgesetz (BayDSG), sondern nach der für diesen Bereich bestehenden spezialgesetzlichen Regelung des Bayerischen Gesetzes über das Erziehungs- und Unterrichtswesen (BayEUG). Das BayEUG wurde durch Gesetz vom 25.06.1994 mit Wirkung vom 01.08.1994 neu gefaßt. Art. 85 (bisher Art. 62) regelt die Erhebung und Verarbeitung von Daten. Eine inhaltliche Änderung ist in diesem Zusammenhang nicht erfolgt. Nach Art. 85 Abs. 2 BayEUG ist eine Weitergabe von Daten über Schüler und Erziehungsberechtigte nur zulässig, soweit ein rechtlicher Anspruch auf die Herausgabe der Daten nachgewiesen wird.

Ergänzend zu dieser Vorschrift hat das Staatsministerium für Unterricht, Kultus, Wissenschaft und Kunst noch ,,Erläuternde Hinweise für die Schulen zum Vollzug des Bayerischen Datenschutzgesetzes" erlassen (KWMBl. 89, S.40). Im konkreten Fall ist Nr. 4.4 der Hinweise zu beachten. **Danach** ist es nicht zulässig, **Daten für Werbezwecke weiterzugeben.** Dies gilt auch, soweit nur die Namen der Schüler weitergegeben werden.

Einen vergleichbaren Sachverhalt habe ich in meinem 14. Tätigkeitsbericht unter Nr. 14.4 dargestellt.

16.2 Führen von Krankheitsblättern für Lehrer an Volks- und Sonderschulen

Eine Lehrkraft hat angefragt, ob das Führen von Krankheitsblättern für Lehrer bei Volks- und Sonderschulen auf Schulebene zulässig sei.

Im Einvernehmen mit dem Staatsministerium für Unterricht, Kultus, Wissenschaft und Kunst vertrete ich die Ansicht, daß eine Lehrkraft am ersten Tag ihrer Erkrankung die Schulleitung zu informieren hat. Diese benachrichtigt nach dem dritten Tag der Erkrankung das zustän-

dige staatliche Schulamt und dieses wiederum ab dem fünften Tag die Regierung. Diese Datenweitergabe ist notwendig, da nach dem dritten Tag ein ärztliches Attest beizubringen ist und ab dem fünften Tag die Zuweisung einer Aushilfskraft im Rahmen der mobilen Reserve erfolgen soll. Die Schulleitung selbst hat die Krankheitsmeldung ohne aktenmäßige Erfassung lediglich weiterzuleiten. Das Anlegen von eigenen Krankheitsblättern, dabei handelt es sich begrifflich um Personalnebenakten, ist für die Persönalverwaltungsaufgaben der Schulen nicht notwendig. Die Krankheit der Lehrkraft wird somit grundsätzlich lediglich bei den staatlichen Schulämtern und bei den Regierungen erfaßt.

17. Archivwesen

Datenschutzrechtliche Prüfung von Archiven

Im Berichtszeitraum haben Mitarbeiter meiner Geschäftsstelle ein Staatsarchiv und ein städtisches Archiv datenschutzrechtlich überprüft. Schwerpunkte der Kontrollen waren dabei die Verfahren bei der Abgabe von Archivgut durch öffentliche Stellen sowie bei der Nutzung von Archivgut durch Dritte.

Staatsarchiv

Grundlage für die Nutzung des in den staatlichen Archiven verwahrten Archivguts ist das Bayerische Archivgesetz (BayArchivG) und die Benutzungsordnung für die staatlichen Archive Bayerns (ArchivBO). Nach § 4 ArchivBO ist die Benutzung schriftlich unter Angabe bestimmter persönlicher Daten zu beantragen.

Gegen den vom Staatsarchiv verwendeten, von der Generaldirektion der Staatlichen Archive Bayerns aufgelegten ,,Antrag auf Zulassung zur Archivbenützung", habe ich keine datenschutzrechtlichen Bedenken erhoben.

Gemäß Art. 10 BayArchivG i.V.m. § 5 Abs. 6 ArchivBO ist Archivgut von der Benutzung ausgeschlossen, solange es einer Schutzfrist unterliegt und eine Verkürzung der Schutzfrist nicht erfolgt ist. Über eine Verkürzung von Schutzfristen entscheidet die Generaldirektion der Staatlichen Archive Bayerns (§ 6 Abs. 2 ArchivBO).

Bei dem geprüften Staatsarchiv fällt dessen Leiter die endgültige Entscheidung über die Benützung insbesondere bei zeitgeschichtlichen Benützungsanträgen nach einem persönlichen Beratungsgespräch. Zur Benützung freigegebene Einzelunterlagen sollen von dem mit der Betreuung des Nutzers beauftragten Sachbearbeiter vor einer Vorlage an den Benutzer aus Gründen des Persönlichkeitsschutzes durchgesehen werden.

Bei umfassenden Forschungsvorhaben ist dieses Verfahren aufgrund der Vielzahl der einzusehenden Archivalien aus arbeitstechnischen Gründen nur schwer möglich.

Das Staatsarchiv versucht in diesen Fällen den Benutzer durch eine von diesem zu unterzeichnende ,,Erklärung zur Wahrung der Persönlichkeitsrechte Betroffener und Dritter" zu binden.

In dem Vordruck wird auf die schutzwürdigen Belange Betroffener oder Dritter und auf rechtliche Konsequenzen einer widerrechtlichen Verletzung dieser Belange hingewiesen. Weiterhin verpflichtet sich der Benutzer, Namen von Personen, deren Nennung **für das Benützungsvorhaben** nicht erforderlich ist, bei einer Veröffentlichung so zu anonymisieren, daß eine Identifizierung ausgeschlossen ist.

Das geschilderte Verfahren **gewährleistet nicht zuverlässig** die Einhaltung der in Art. 10 Abs. 3 ÄrchivG genannten Schutzfristen bzw. der schutzwürdigen Belange der Betroffenen oder Dritter. Ich habe deshalb das Bayerische Staatsministerium für Unterricht, Kultus, Wissenschaft und Kunst um Stellüngnahme zu der Vorgehensweise des Staatsarchivs gebeten. Ich halte es für erforderlich, ein den gesetzlichen Auflagen besser entsprechendes Verfahren zu entwickeln, wobei ich nicht verkenne, daß die Überprüfung der Schutzfristen des Art. 10 Abs. 3 ArchivG in der Archivpraxis erheblichen Schwierigkeiten begegnet.

Stadtarchiv

Nach Art. 13 Abs. 1 des Bayerischen Archivgesetzes (BayArchivG) regeln die Gemeinden die Archivierung der bei ihnen erwachsenen Unterlagen in eigener Zuständigkeit.

Es gehört zu den Aufgaben jeder kommunalen Körperschaft, für ihren Geschäftsgang zu sorgen und die dafür notwendigen Einrichtungen zu schaffen (Art. *56* Abs. 2 Gemeindeordnung, GO). Die Gemeinden sind auch nach Art. 57 Abs. 1 GO i.V.m. Art. 13 Abs. 1 und 2 BayArchivG verpflichtet, für die Archivierung ihrer Unterlagen in einem Archiv Sorge zu tragen. Aufgabe der Archive ist es, die bei der Verwaltung für den laufenden Dienstbetrieb nicht mehr erforderlichen, jedoch archivwürdigen Unterlagen zu archivieren.

Für das geprüfte Stadtarchiv wurde bisher keine Satzung erlassen.

Im Archiv werden überwiegend historische Unterlagen aufbewahrt. Vorgänge aus jüngerer Zeit lagern meist noch bei den einzelnen Dienststellen der Stadt, soweit sie nicht bereits vernichtet wurden. Dies deutet darauf hin, daß Art. 12 Abs. 4 und 8 BayDSG bisher nicht ausreichend berücksichtigt wurden. Als Ausfluß dieser Bestimmungen sind die Dienststellen **der Stadt gehalten, in regelmäßigen Abständen nicht mehr zur Aufgabenerfüllung erforderliche Akten auszusondern,** nach Maßgabe einer Archivsatzung dem Stadtarchiv anzubieten und bei Nichtübernahme zu vernichten.

Die Stadt wurde gebeten, eine Rechtsgrundlage für das Stadtarchiv zu schaffen und eine **Satzung zu erlassen.** Darin sind auch Regelungen über die Anbietung von Archivgut zu treffen.

Im Hinblick auf die begrenzten Lagermöglichkeiten des Stadtarchivs habe ich auf die Möglichkeit hingewiesen, Lagerräume der Dienststellen der Stadt als Teil des Stadt-

archivs zu deklarieren. Nachdem die Benutzungsregelungen für staatliche Archive für bestimmtes Archivgut mit Einschränkungen auch für kommunale Archive gelten (Art. 13 Abs. 2 BayArchivG), wären in diesemFall Zugangsregelungen festzulegen, welche einen Zugang der den Lagerraum zur Verfügung stellenden Dienststelle nur im Rahmen der gesetzlichen Vorgaben zulassen.

18. Umweltfragen

Altlastendatenbank beim Landesamt für Umweltschutz

Im Berichtszeitraum habe ich das beim Landesamt für Umweltschutz gemäß Art. 27 Abs. 2 Bayerisches Abfallwirtschafts- und Altlastengesetz (BayAbfAlG) eingerichtete **Altlastenkataster überprüft.**

Die Behörden, Gerichte und sonstigen Stellen des Freistaates Bayern, die Gemeinden, die Landkreise, die Bezirke und die sonstigen juristischen Personen des öffentlichen Rechts haben u.a. dem Landesamt für Umweltschutz die ihnen vorliegenden Erkenntnisse über Altablagerungen und Altstandorte mitzuteilen. Das Landesamt für Umweltschutz erfaßt aufgrund dieser Mitteilungen und aufgrund eigener Erkenntnisse altlastverdächtige Flächen und Altlasten im Altlastenkataster. Mitte der 80er Jahre wurde begonnen, bei den Kreisverwaltungsbehörden die in Frage kommenden Flächen zu erheben. Zwischenzeitlich wurden dem Landesamt ca. 9.900 altlastverdächtige Flächen gemeldet und in das Altlastenkataster aufgenommen.

Im Kataster werden zu einer einzelnen Altlast die örtliche Lage und möglichst genaue Sachangaben gespeichert. In Frage kommen hier beispielsweise Angaben über die abgelagerten Stoffe, über hydrogeologische Verhältnisse, bei bereits aufgetretenen Schäden die Schadensart (z.B. Sickerwasseraustritt) oder die Zuordnung zu einer bestimmten Verursacherkategone (z.B. stillgelegte Gerberei). Dokumentiert werden außerdem Untersuchungs-, Sanierungs- und Überwachungsmaßnahmen. **Personenbezogene Daten von natürlichen Personen** werden dann gespeichert, wenn der (frühere) Betreiber eine natürliche Person ist bzw. mittelbar über die Flurnummer, wenn der Grundstückseigentümer eine natürliche Person ist.

Ausgewertet werden kann das Altlastenkataster nach den Suchkriterien ,,Name der Altlast" bzw. ,,Nummer der Altlast", ,,Priorität" (= Dringlichkeitsstufe, in die eine Altlast hinsichtlich ihrer Untersuchung und Sanierung eingeordnet ist) und ,,Name des Standortes". Das Landesamt wertet die Daten für allgemeine, anonymisierte Veröffentlichungen aus und übersendet in bestimmten Zeitabständen (ein bis zwei Jahre) den zuständigen Kreisverwaltungsbehörden eine genaue Aufstellung und Übersicht der im Altlastenkataster registrierten Flächen für das Gebiet der jeweiligen Kreisverwaltung. Die Kreisverwaltungsbehörden sind nach Art. 28 Abs. 1 BayAbfAlG grundsätzlich für die Überwachung von altlastenverdächtigen Flächen und Altlasten zuständig. Karten können allerdings mit Hilfe des automatisierten Altlastenkataster nicht erstellt werden.

Der Umfang der im Altlastenkataster gespeicherten Daten sowie deren Verarbeitung und Nutzung durch das Landesamt entsprachen Art. 27 Abs. 2 BayAbfAlG, der die Erfassung altlastenverdächtiger Flächen und von Altlasten vorsieht. Wie in anderen Fällen mußte ich allerdings auch hier feststellen, daß das verwendete **Paßwort nicht den datenschutzrechtlichen Anforderungen genügt,** da es mit der Benutzererkennung identisch, vom Namen des Sachbearbeiters abgeleitet war und nur drei Buchstaben umfaßte. Ich weise daher auch in diesem Zusammenhang nochmals auf meine unter Nr.20.2.2 des Vierzehnten Tätigkeitsberichtes (Seite 92) aufgezeigten Sicherheitsgrundsätze bei der Vergabe und Änderung von Paßworten hin.

19. Verkehrswesen

19.1 Prüfung des Verfahrens „SIFLUG" beim Luftamt Südbayern

Im Berichtszeitraum habe ich das Verfahren für die Sicherheitsüberprüfung bei der Ausgabe von Zutrittsberechtigungen an Flughäfen (SIFLUG) beim Luftamt Südbayern überprüft.

In nicht allgemein zugänglichen oder sicherheitsempfindlichen Bereichen des Flughafens München kann nur beschäftigt werden, wer sich einer Sicherheitsüberprüfung unterzieht. Ergibt die Überprüfung keine Bedenken, kann dem Betroffenen ein Flughafenausweis durch die Flughafen München GmbH ausgestellt werden, der ihm den Zutritt zu den o.g. Bereichen erlaubt.

Der Antrag auf Ausstellung eines Flughafenausweises ist vom Betroffenen, bzw. der Firma, die ihn beschäftigt, bei der Flughafen München GmbH einzureichen. Der Antragsteller erklärt sich auf dem Antrag damit einverstanden, daß die nach dem Luftverkehrsgesetz erforderlichen Angaben zu seiner Person an die zuständigen Sicherheitsbehörden zur Durchführung der Sicherheitsüberprüfung weitergeleitet werden. Bestandteil ist auch eine Einverständniserklärung für die Verwendung dieser Angaben beim Bayerischen Landesamt für Verfassungsschutz zur Durchführung der Sicherheitsüberprüfung.

Die Flughafen München GmbH leitet den Antrag dem Luftamt Südbayern zu. Die Aufgabe des Luftamts ist es, zu prüfen, ob gegen die Ausstellung eines Flughafenausweises Bedenken bestehen. Dazu holt es Stellungnahmen des Landesamtes für Verfassungsschutz und des Landeskriminalamtes ein.

Teilen diese beiden Stellen mit, daß bei einem Antragsteller keine Bedenken gegen die Ausstellung eines Ausweises bestehen, teilt das Luftamt dieses Ergebnis der Flughafen GmbH mit.

Teilen das Landeskriminalamt oder das Landesamt für Verfassungsschutz Anhaltspunkte mit, die gegen die Zuverlässigkeit des Antragstellers sprechen (z.B. Vorstrafen) hört das Luftamt den Betroffenen an. Werden im Rahmen der Anhörung die Bedenken gegen die Zuverlässigkeit ausgeräumt, wird der Flughafen München GmbH nur das Ergebnis mitgeteilt, daß gegen die Ausstellung eines Flughafenausweises keine Bedenken bestehen.

Bleiben die Bedenken bestehen, wird die Flughafen München GmbH darüber informiert, daß das Luftamt Südbayern einer Erteilung eines Flughafenausweises nicht zustimmen kann. Über die Gründe wird weder die Flughafen München GmbH noch der Arbeitgeber des Betroffenen vom Luftamt informiert. Es bleibt dem Betroffenen überlassen, ob er seinen Arbeitgeber über die genauen Gründe informieren möchte.

Gegen das Verfahren bestehen aus datenschutzrechtlicher Sicht keine Bedenken. Das automatisierte Verfahren für die Sicherheitsüberprüfung bei der Ausgabe von Zutrittsberechtigungen an Flughäfen (SIFLUG) wurde zum Zeitpunkt der Prüfung nur unterstützend im Rahmen der Antragsbearbeitung eingesetzt, z. B. um die Antragseingänge und die Rückmeldungen der Sicherheitsbehörden zu erfassen. Beanstandet werden mußte allerdings, daß die bisher beim Luftamt Südbayern verwendeten Paßwörter nicht den unter Nr. 20.2.2 meines 14. Tätigkeitsberichtes aufgezeigten Sicherheitsgrundsätzen entsprachen. Das Luftamt Südbayern hat den Verstoß inzwischen behoben. Mittlerweile werden geeignete Paßwörter eingesetzt.

19.2 Prüfung einer Führerscheinstelle und einer KfzZulassungsstelle

Bei der Prüfung einer Führerscheinstelle und einer Kfz-Zulassungsstelle mußte ich folgendes beanstanden:

1. **Datenübermittlungen von der Kraftfahrzeugzulassungsstelle an die Sozialhilfeverwaltung nach §117 Abs. 3 BSHG**

   Wie bereits in dem Beitrag unter Nr. 3.3.1 zu § 117 Abs. 3 BSHG berichtet, darf die Sozialhilfeverwaltung überprüfen, ob der Sozialhilfeempfänger Halter eines Kraftfahrzeuges ist. Bei der von mir geprüften kreisfreien Stadt ließ sich die Sozialhilfeverwaltung jedoch nicht nur die in § 117 Abs. 3 BSHG genannten Daten übermitteln, sondern auch weitere Daten zum Fahrzeug (z. B. Baujahr, Fahrzeugtyp). Für die Übermittlung dieser Fahrzeugdaten besteht weder im § 117 BSHG noch in den straßenverkehrsrechtlichen Vorschriften eine Rechtsgrundlage. Solche Daten dürfen daher von der Zulassungsstelle an die Sozialhilfeverwaltung nicht übermittelt werden, außer der Betroffene hat sein Einverständnis dazu erteilt. Benötigt die Sozialhilfeverwaltung weitere Daten zum Fahrzeug, muß sie diese bei dem als Halter eines Kfz ermittelten Sozialhilfeempfänger selbst erheben, wobei dieser die Pflicht zur Mitwirkung gemäß § 60 ff SGB I hat.

2. **Paßwortvergabe**

   Wie so oft mußte ich auch hier feststellen, daß die Paßwortvergabe nicht den datenschutzrechtlichen Anforderungen entsprach. Die Mitarbeiter der Zulassungsstelle konnten ihr Paßwort nicht selbst ändern, sondern es wurde vom Systemverwalter vergeben. Die Paßwörter wurden außerdem nur selten gewechselt.

   Ich weise daher auch in diesem Zusammenhang auf die unter Nr. 20.2.2 meines 14. Tätigkeitsberichts (Seite 92) aufgezeigten Sicherheitsgrundsätze hin.

19.3 Weitergabe von Kfz-Halterdaten zur Verfolgung von Rechtsansprüchen

1. Ein Bürger wollte wissen, ob die Zulassungsstelle berechtigt war, seine Halterdaten an eine Privatperson zu übermitteln, obwohl er nicht in einen Unfall verwickelt gewesen war und auch kein Eigentum dieser Privatperson beschädigt hatte.

   Bei der Zulassungsstelle hatte ein Rechtsanwalt unter Angabe des amtlichen Kennzeichens um die Übermittlung des Namens und der Anschrift des Halters gebeten. Sein Ersuchen begründete er damit, daß das Fahrzeug am (Datum des Ereignisses) die Grundstückseinfahrt seines Mandanten in (Ort des Geschehens) blockiert habe.

   Nach § 39 Abs. 1 Straßenverkehrsgesetz sind die dort genannten Fahrzeug- und Halterdaten durch die Zulassungsstelle zu übermitteln, wenn der Empfänger unter Angabe des betreffenden Kennzeichens darlegt, daß er die Daten zur Geltendmachung, Sicherung oder Vollstreckung oder zur Befriedigung oder Abwehr von Rechtsansprüchen im Zusammenhang mit der Teilnahme am Straßenverkehr oder zur Erhebung einer Privatklage wegen im Straßenverkehr begangener Verstöße benötigt. Unter Rechtsansprüchen im Zusammenhang mit der Teilnahme am Straßenverkehr fallen auch Ansprüche auf Aufwendungs-, Schadensersatz und Unterlassung. Eine Teilnahme am Straßenverkehr liegt auch vor, wenn das Fahrzeug abgestellt ist. Dabei genügt es, wenn das Fahrzeug auf Privatgrund abgestellt ist und dadurch Rechte anderer verletzt werden (z.B. Eigentum, Besitz am Grundstück). Die Erklärung des Rechtsanwaltes unter Angabe von Zeit und Ort des Geschehens, er benötige die Daten, weil das Fahrzeug die Grundstückszufahrt seines Mandanten blockiert habe, erfüllte diese Voraussetzungen. Die Auskunftserteilung war danach zulässig.

2. Eine Bürgerin fragte mich, ob die Zulassungsstelle einem Gläubiger, der zur Durchsetzung von Unterhaltsleistungen einen Personenkraftwagen des Schuldners pfänden will, eine Auskunft aus dem örtlichen Fahrzeugregister erteilen darf.

Ich habe der Bürgerin mitgeteilt, daß bei der Vollstreckung in das Vermögen eines Schuldners, in welchem sich auch ein Kraftfahrzeug befindet, der Zusammenhang mit der Teilnahme am Straßenverkehr fehlt. Eine Datenübermittlung durch die Zulassungsstelle zu dem o.g. Zweck ist danach nicht zulässig.

20. Medien

Datenschutz im Medienbereich

Mehrere Zuschriften befaßten sich mit dem Inkasso des Teilnehmerentgelts für einen Kabelanschluß. Dieses Inkasso ist mit Wirkung vom 01.01.1994 von der Deutschen Bundespost Telekom auf die Bayerische Medien-Servicegesellschaft übergegangen. Bürger sahen ihr Recht auf informationelle Selbstbestimmung dadurch verletzt, daß die für das Inkasso notwendigen Daten, wie bspw. die Kontonummer, ohne Kenntnis der Betroffenen weitergegeben wurden.

Ich habe darauf hingewiesen, daß zur Sicherstellung des Datenschutzes im Bereich der Bayerischen Landeszentrale für neue Medien, den Medienbetriebsgesellschaften und den Betreibern von Kabelanlagen (ausgenommen die Deutsche Bundespost Telekom) der Präsident der Landeszentrale einen Beauftragten für den Datenschutz berufen hat und aufgrund dieser Regelung (Art. 20 Abs. 4 Bayerisches Mediengesetz) meine Kontrollkompetenz nicht gegeben ist.

Die datenschutzrechtliche Überwachung der Deutschen Bundespost Telekom liegt in der Zuständigkeit des Bundesbeauftragten für den Datenschutz.

21. Technischer und organisatorischer Bereich

21.1 Technische Grundsatzfragen

21.1.1 Situation auf dem DV-Markt

Im Juli1994 wurden die Ergebnisse einer Sicherheitsstudie einer führenden deutschen Fachzeitschrift für Informationssicherheit veröffentlicht. Bemerkenswert war u.a., daß die DV-Anwender der Meinung sind, daß für die Datensicherheit die Risiken aus Software-Defekten eher zunehmen werden, während die Risiken, die durch Hardware-Defekte entstehen können, eher abnehmen sollen. Die zunehmend stabiler werdende Hardware und die immer komplexer und umfangreicher werdenden Software-Programme, die nur noch für einige wenige Experten überschaubar und daher fehleranfälliger als früher sind, prägten wohl diese Meinung.

Auch auf dem DV-Markt fand in den letzten Jahren eine recht stürmische Entwicklung statt: Die Hardware-Bauteile wurden ständig kleiner und zugleich leistungsfähiger. Alle vier Jahre vervierfachte sich die Speicherkapazität der Chips, bei nahezu konstant gebliebenen Preisen für den Endanwender. Bezogen auf die Speicherkapazität und die Verarbeitungsgeschwindigkeit sind heutige Personal Computer mit Großrechnern der 70-er Jahre vergleichbar. Auch die Programmierwerkzeuge wurden mächtiger, was sich besonders in der Leistungsfähigkeit der Computer-Programme im PC-Bereich bemerkbar macht. Im Großrechnerbereich, wo die Programme über Jahrzehnte gewachsen sind, hat die Software diesen Entwicklungsschub aus Kosten- und Kapazitätsgründen nicht erfahren können.

Für die Kontrolle der Datensicherungsmaßnahmen bedeutet das, daß dort, wo die Leistungsfähigkeit geradezu explodierte, die Möglichkeiten sowohl für Risiken der Fehlanwendungen als auch für Sicherheitsmaßnahmen ständigen Änderungen unterworfen sind. Der Weiterbildungsbedarf ist einerseits gestiegen, andererseits muß man bei der begrenzten Personalkapaziät der Kontrollinstanzen vom Universalistentum Abschied nehmen. So wie die Hardware-Hersteller, um die Qualität und Wettbewerbsfähigkeit ihrer Produkte halten zu können, Ko-Operationen mit Partnern (Beispiel: Chip-Herstellung) eingehen, muß sich auch die Datenschutzkontrolle vermehrt das Know-how von externen Spezialisten zu eigen machen. Die Kontrollinstanzen müssen jedoch noch genügend eigenen Sachverstand zur Wertung der oft komplexen Sachverhalte selbst aufbringen.

Der Wettbewerbsdruck läßt es nicht zu, daß sich DV-Hersteller mit instabilen Produkten auf dem Markt behaupten. Der Markt würde schnell reagieren und große Umsatzeinbußen wären die Folge. Viele DV-Hersteller wurden von anderen Unternehmen übernommen oder sind gänzlich vom Markt verschwunden, weil sie der Entwicklung nicht standhalten konnten oder weil sie zur Anpassung ihrer Produkte an die veränderten Bedingungen nicht mehr in der Lage waren. Bei vielen Anwendungsprogrammpaketen mußte aus Kostengründen die Weiterentwicklung und Wartung eingestellt werden. Auf der anderen Seite tun sich ständig neue Anwendungsbereiche auf (z.B. medizinische Datenverarbeitung). Der harte Konkurrenzkampf verträgt es allerdings nicht, schlechte und mangelhaft ausgetestete Hard- und Software auf den Markt zu bringen, so daß diese von vorneherein keine großen Marktchancen hätte.

Insgesamt läßt sich jedoch sagen, daß die heute eingesetzte Hard- und Software trotz der Tatsache, daß sie preiswerter geworden sind, den allgemeinen Qualitätsmaßstäben genügen. Der Anwender muß allerdings aufpassen, daß er sich nicht für den Einsatz eines scheinbar billigeren Konkurrenzprodukts eines sog. DV-Exoten entschließt, der nach einigen Jahren vom Markt verschwunden ist. Die Kosten für eine Migration auf ein anderes, zukunftsträchtigeres System wären dann doch recht beachtlich. Auch umfangreiche Eigenentwicklungen sind heute für den Anwender meist unwirtschaftlich geworden. Viele Anwender haben sich deshalb für Gemeinschaftsentwicklungen entschieden, etwa die Verfahren der AKDB oder die Dachverbände der Krankenversicherungsanstalten (etwa der AOK-Bundesverband bzw. der AOK-Landesverband Bayern). Davon kann auch der

Datenschutzbeauftragte profitieren, denn er braucht nur noch ein Verfahren intensiv zu prüfen und nicht eine Vielzahl von ähnlichen.

21.1.2 Grundsätzliche Überlegungen zu Maßnahmen zum Datenschutz und zur Datensicherheit bei der automatischen Gebührenerhebung auf Autobahnen

Bereits im letzten Tätigkeitsbericht wurde über das Vorhaben des Bundesverkehrministeriums zur automatischen Gebührenerhebung auf Autobahnen berichtet. Im Berichtszeitraum begann nun dazu auf der A 555 zwischen Köln und Bonn ein Feldversuch. Der Bundesbeauftragte für den Datenschutz hatte im April 1994 die Landesbeauftragten für den Datenschutz zu einer Präsentation dieses Feldversuches eingeladen. Mit der Durchführung des Feldversuches, an dem sich 10 Privatfirmen mit unterschiedlicher Technik beteiligen, wurde der TÜV Rheinland und die Firma Heusch/Boesefeldt beauftragt. Die Ergebnisse des Feldversuches dürften Mitte 1995 vorliegen.

Aus der Sicht des Datenschutzes ergeben sich folgende Forderungen:

■ **Allgemeine Forderungen**

Alle zum Einsatz kommenden technischen Geräte müssen der Qualitätssicherungsnorm ISO 9001 genügen. Etwaige Störungen bei den im PKW installierten Geräten müssen dem Benutzer sofort angezeigt werden. Die Anfälligkeit des Funksystems gegen Störungen von außen ist im Feldversuch zu untersuchen und zu bewerten.

Aus datenschutzrechtlicher Sicht ist im Hinblick auf den verfassungsrechtlichen Grundsatz der Erforderlichkeit, d.h. des geringstmöglichen Eingriffs, zu fordern, daß zur Gebührenerhebung und zur Überwachung Verfahren gewählt werden, bei denen **möglichst wenig**, d.h. nur die für die **Zweckerreichung notwendigen** personenbezogenen Daten erhoben werden müssen. Bei der **Gebührenerhebung** ist deshalb nach gegenwärtiger Kenntnis ehereinemWertkartensystem derVorzug zu geben, bei dem sämtliche Vorgänge der Gebührenabbuchung und ggf. auch der -berechnung im Fahrzeug stattfinden und eine Erhebung personenbezogner Daten durch externe Stellen lediglich im Rahmen derÜberwachung inBetrachtkommt. Für die **Überwachung** ist ein Verfahren zu wählen,bei dem nur bei den sog. ,,Schlechtfällen" eine Erhebung und Speicherung personenbezogener Daten stattfindet.
Die zur Gebührenberechnung erhobenen personenbezogenen Daten dürfen nur zu diesem Zweck verwendet werden (strikte Zweckbindung). Das läßt sich am besten durch die Verwendung von Verfahren unterstützen, die für andere Zwecke nicht geeignet sind (Monostruktur).

■ **Technische Aspekte**

Der Arbeitskreis ,,Technik" der Datenschutzbeauftragten des Bundes und der Länder hat Mitte 1994 einstimmig ein Grundsatzpapier erstellt, an dem die einzelnen, in Frage kommenden Verfahren gemessen werden sollen.
Die datenschutzrechtlichen Anforderungen beziehen sich dabei auf folgende Aspekte:
- Möglichkeiten der Anonymisierung
- Vertraulichkeit der erhobenen Daten
- Integrität von Verfahren und Daten
- Transparenz des Verfahrens
- Stabilität der Sicherheitsmaßnahmen gegen Rücknahme.

Das Grundsatzpapier liegt dem Tätigkeitsbericht als Anlage 3 bei.
Im übrigen wurden die beiden für die Autobahngebührenerhebung möglichen Verfahren (prepaid- oder postpaid-Verfahren) im letzten Tätigkeitsbericht ausführlich beschrieben.

21.1.3 Anlagen- und Verfahrensverzeichnis

Das Bayerische Datenschutzgesetz vom 23.7.1993 verlangt nach Art. 27 in Verbindung mit Art. 39 Abs. 4, daß speichernde Stellen, soweit personenbezogene Daten automatisiert verarbeitet werden, bis zum 1.3.1995 dafür ein Anlagen- und Verfahrensverzeichnis (in einigen Datenschutzgesetzen auch als Dateiverzeichnis bezeichnet) aufbauen. Diese beiden Verzeichnisse sollen als Ersatz für das früher zentral beim Landesdatenschutzbeauftragten geführte Datenschutzregister gelten.

Der Inhalt des Verfahrensverzeichnisses richtet sich nach Art. 26 Abs. 2 Bayer. Datenschutzgesetz. Die Angaben, die für die datenschutzrechtliche Freigabe erforderlich sind, werden auch in das Verfahrensverzeichnis übernommen. Der Inhalt des Anlagenverzeichnisses ist im Bayer. Datenschutzgesetz jedoch nicht näher geregelt. Er wurde in einer Verwaltungsvorschrift (gemeinsame Bekanntmachung der Bayer. Staatskanzlei und der Bayer. Staatsministerien vom 11.3.1994) festgelegt.

Nach der Vollzugsbekanntmachung zum Bayerischen Datenschutzgesetz vom 11.3.1994 ist jede Datenverarbeitungsanlage in das Anlagenverzeichnis aufzunehmen, auf der im Verfahrensverzeichnis beschriebene Verfahren ablaufen. Es hat Angaben zu enthalten über

■ die eingesetzte Hardware, wie
- die Anlagenbezeichnung,
- die Rechnerart (Großrechner, Abteilungssystem, PC),
- den Umfang der angeschlossenen Peripherie und
- Informationen über die Vernetzung,

■ die eingesetzte Software, wie
- das Betriebssystem,
- die verwendete Basissoftware (Datenbanksysteme, Abfragesprachen, o.ä.) und
- die Bezeichnung der ablaufenden Verfahren aus dem Anlagenverzeichnis, damit die Verbindung zum Verfahrenverzeichnis hergestellt werden kann.

Das Anlagenverzeichnis muß selbstverständlich auch Hinweise über den Standort einer DV-Anlage vermitteln,

damit der behördliche Datenschutzbeauftragte seine gesetzlich vorgegebenen Kontrollaufgaben wahrnehmen kann. Die Sensibilität der auf einer Anlage ablaufenden Verfahren sollte schließlich ein Anhaltspunkt für die Stärke der Datensicherungsmaßnahmen sein.

Die Bayerische Datenschutzverordnung schränkt jedoch die Aufnahme von Verfahren in das Anlagen- und Verfahrensverzeichnis ein. So brauchen nicht in das Verfahrensverzeichnis aufgenommen zu werden:

- Verfahren, die ausschließlich Zwecken der Datensicherung und der Datenschutzkontrolle dienen, und Verfahren, die nur vorübergehend vorgehalten werden und bei denen die personenbezogenen Daten innerhalb von drei Monaten nach der Inbetriebnahme des Verfahrens gelöscht werden
- Verfahren, die ausschließlich zur Erstellung von temporär gespeicherten Texten dienen
- Registraturverfahren, die ausschließlich dem Auffinden von Vorgängen, Anträgen oder Akten dienen
- Verfahren zur Überwachung von Fristen und Terminen (Terminkalender)
- Telefon-, Telefax- sowie sonstige Kommunikationsund Teilnehmerverzeichnisse
- Zimmer-, Inventar-, Hard- und Software-Verzeichnisse
- Bibliothekskataloge und Fundstellenverzeichnisse und Adreßverzeichnisse, die für die Informationsversendung benötigt werden.

Ganz wesentlich ist, daß Verfahrens- und Anlagenverzeichnis verknüpfbar sind. Deshalb sind ins Anlagenverzeichnis eindeutige Hinweise über die auf der DV-Anlage ablaufenden Verfahren aufzunehmen. Damit das Anlagenverzeichnis nicht so ändernungsintensiv wird, können Angaben über den Software-Versionsstand entfallen, soweit diese Information nicht den Sicherheitsstandard kennzeichnet. Grundsätzlich ist jede DV-Anlage, auf der meldepflichtige personenbezogene Verfahren ablaufen, also auch jeder Personal Computer, einzeln ins Anlagenverzeichnis zu übernehmen. Aus Transparenz- und Vereinfachungsgründen wäre es auch denkbar, für DV-Anlagen (PC-Netz) im gleichen Sachgebiet und mit identischen Aufgaben eine Art Sammelmeldung für das Anlagenverzeichnis zu erstellen.

Für ihre Kunden hat die AKDB geeignete Formblätter für das Anlagen- und Verfahrensverzeichnis entwickelt.

21.1.4 Erfahrungen bei der Einführung der Krankenversicherungskarte

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat am 27.3.1994 einen Beschluß zur Einfuhrung von Chipkarten im Krankenversicherungsund Gesundheitsbereich gefaßt (siehe Anlage).

In Bayern wurden Anfang 1994 von den Krankenkassen der gesetzlichen Krankenversicherung an alle Mitglieder die elektronisch lesbaren Krankenversicherungskarten ausgegeben. Die Krankenversicherungskarte ersetzt das bisherige Versichertenscheckheft. Die Krankenversicherungskarte wird in Bayern wie früher das Versichertenscheckheft, z. B. für die bayerischen AOKs, bei der Fa. Systemform in Prien in Auftragsdatenverarbeitung zentral erstellt und an die Mitglieder versandt.

Sicherheitsgrundsätze

Die Krankenversicherungskarte enthält einen Chip mit 256 Byte Speicherkapazität. Die Speicherkapazität des Chips ist nicht erweiterbar. Gespeichert werden auf Grund der gesetzlichen Gebote in § 291 Abs 2 SGB V lediglich die sog. Versichertengrunddaten:
Name, Anschrift, Geburtsdatum, Krankenkasse, Versicherungsnummer, Versichertenstatus, Tag des Beginns des Versicherungsschutzes und bei befristeter Gültigkeit das Datum des Fristablaufs.
Zur Kontrolle werden für jedermann lesbar auf die Karte folgende Feldinhalte gedruckt: Name, Krankenkassennummer, Versicherungsnummer, Status und Gültigkeitsdatum.
Der Versichertenstatus kennzeichnet, ob der Versicherte selbstversichert, Familienmitglied oder Rentner ist und enthält ein Merkmal zur Zugehörigkeit zum Personenkreis des sog. ,,Risikostrukturausgleich" innerhalb der Krankenkassen, sowie für diesen Personenkreis einen Hinweis auf Rentenbezug.
Eine Manipulation der auf dem Chip gespeicherten Daten würde beim Benutzen der Karte offenkundig.

Auf dem Chip sind die Versichertendaten im variablen Feldformat aufgezeichnet, d.h., am Ende des Speichers bleiben freie Speicherstellen übrig, die theoretisch für andere Zwecke genützt werden könnten. Diese freien Speicherstellen werden bei der Beschreibung auf binär ,,blank" (Leerstellen) gesetzt. Zur Feststellung der Authentität der gespeicherten Daten enthält der Chip eine Prüfsumme, die die Unverfälschtheit der gespeicherten Informationen attestieren soll. In diese Prüfsumme geht auch die Anzahl der vorhandenen Leerstellen ein. Das Prüfsummenverfahren soll allerdings professionellen Manipulationen nicht standhalten (es ist mit der sog. digitalen Unterschrift nicht vergleichbar).

Manipulierte Karten können jedoch von den bei den Ärzten im Einsatz befindlichen Programmen und den entsprechenden Lesegeräten nicht gelesen werden. Das gleiche gilt, wenn auf die Karte zusätzliche Informationen gespeichert würden.

Der Arzt ist nicht befugt, Datenänderungen auf der Chipkarte durchzuführen. Er verfügt obendrein nur über Leseeinrichtungen. Die Krankenkassen können lediglich Adreßdaten verändern. Andere Daten können mit den im Einsatz befindlichen Programmen nicht verändert werden, da die Funktionen nichtprogrammiert wurden. Ändert sich beispielsweise der Versichertenstatus oder der Name, muß eine neue Versichertenkarte ausgegeben werden, weil diese Daten auch auf die Karte gedruckt werden müssen.

Die Kassenärztlichen Vereinigungen empfehlen den Ärzten geprüfte Hard- und Software zu verwenden. Einige Lese-

geräte sind vom BSI zertifiziert worden und garantieren den Mindestsicherheitsstandard nach E2 (ausreichende Sicherheit). Die Software wurde vom Bundesverband der Kassenärztlichen Vereinigungen auf ihre Richtigkeit geprüft. Nichtgeprüfte Hard- und Software darf nicht eingesetzt werden. Es ist davon auszugehen, daß die Kassenärzte die offiziellen DV-Systeme einsetzen, da nur für solche Systeme ein finanzieller Zuschuß gewährt wird.

Mißbrauchsmöglichkeiten

Ein Mißbrauch mit der Krankenversichertenkarte ist - wie bisher schon beim Krankenschein - nicht auszuschließen. Eignet sich beispielsweise jemand eine fremde Krankenversicherungskarte an, kann er sich kostenlos behandeln lassen, sofern der Arzt seine Identität nicht überprüft. Die Folgen von Datenmanipulationen sind aber verhältnismäßig unbedeutend und nicht gravierender, als beim Einsatz des herkömmlichen Versichertenscheckheftes. Trotzdem sind die Kassenärztlichen Vereinigungen und die Krankenkassen aufgerufen, im Rahmen der gesetzlichen Möglichkeiten nach Lösungen zu suchen, den Einsatz der Krankenversichertenkarte sicherer zu machen, um Mißbrauchsmöglichkeiten vorzubeugen oder zu verhindern. Ansätze dazu sind bereits erkennbar.

Erfahrungen

In jeder Krankenkasse steht ein Lesegerät bereit, um den Versicherten zeigen zu können, welche Daten auf seiner Karte gespeichert sind. Von dieser Möglichkeit haben bei den Allgemeinen Ortskrankenkassen bisher nur verschwindend wenig Versicherte Gebrauch gemacht.

Beschwerden von Versicherten sind bei verschiedenen Krankenkassen vereinzelt von solchen Versicherten eingegangen, deren Name aufgrund der Umstellung von Großschreibung auf Groß-Kleinschreibweise unkorrekt auf der Karte aufgedruckt war. Wegen des Einsatzes von Großrechnern ist es bisher immer noch nicht wirtschaftlich lösbar, zwischen den Umlauten ä, ö und ü und den Zeichenfolgen ae, oe oder ue zu unterscheiden. Eine automatische Umsetzung würde auch wieder falsche Schreibweisen liefern, nicht alle Mueller schreiben sich Müller und aus Goethe würde Göthe.

Schließlich hat die Ausgabe der Krankenversichertenkarte auch noch einen wirtschaftlichen Aspekt: Bei der neuen konnten gegenüber der herkömmlichen Lösung Kosten eingespart werden.

21.2 Prüfungstätigkeit

21.2.1 Kontrolle und Beratung

Die Kontrolle der technischen und organisatorischen Datensicherheitsmaßnahmen war wiederum ein Schwerpunkt im Berichtszeitraum.

Folgende **Dienststellen** habe ich nach Art. 7 BayDSG (teilweise i.V.m. § 9 BDSG und Anlage) kontrolliert:

- Anstalt für kommunale Datenverarbeitung in Bayern (AKDB), München (neue Verfahren)
- AKDB, KDZ Regensburg
- AKDB, KDZ Würzburg
- AOK Würzburg
- Bezirk Niederbayern, Landshut
- Handwerkskammer Schwaben, Augsburg
- Kreiskrankenhaus Traunstein
- Landratsamt Mühldorf
- Stadt Dachau
- Stadt Ingolstadt
- Stadt Passau
- Zweckverband Gemeindliche Datenverarbeitung im Landkreis Neu-Ulm, Illertissen.

Die Prüfung bei der AKDB München war schwerpunktmäßig auf die neuen Zugriffsschutzsteuerungsprogramme für die HP3000-, Unix- und PC-Verfahren ausgerichtet.

Bei der Prüfung der AOK Würzburg war einer der Prüfungspunkte die Gewährleistung der Datensicherheit bei der Einführung der neuen Krankenversicherungskarte.

Die Entsorgung von Datenträgern mit personenbezogenem Inhalt habe ich zusätzlich bei etwa 10 bayerischen Dienststellen überprüft.

Schließlich habe ich wieder zahlreiche Dienststellen beraten. Die Zahl der Dienststellen steigt ständig, die im Vorfeld von Um- oder Neubauten ihrer Gebäude oder von EDV-Bereichen Hinweise hinsichtlich notwendiger Datenschutz- und Datensicherheitsmaßnahmen (Zutrittsschutz, Objektsicherung, Katastrophenvorsorge, Entsorgung von Datenträgern) erhalten. Im Zuge der weiter ansteigenden Vernetzung der Rechnerleistung wurde ich auch vielfach gebeten, zur Gewährleistung der Datensicherheit in einem LAN Stellung zu nehmen.

21.2.2 Ergebnisse der Kontrolltätigkeit

Die angespannte Haushaltslage zwingt viele öffentliche Stellen zum Sparen an den Finanzmitteln. Trotzdem bemühten sich alle kontrollierten Dienststellen, die erforderlichen Maßnahmen zum Datenschutz und zur Datensicherheit zu treffen. Auf einige verbliebene Mängel, die entweder übersehen oder deren Behebung zurückgestellt worden war, möchte ich nachfolgend näher eingehen:

Dokumentation der Zugriffsberechtigungen
Bei vielen Dienststellen ist es immer noch üblich, daß Zugriffsrechte aufgrund einer telefonischen Anweisung eingerichtet werden. Eine revisionsfähige Dokumentation der Vergabe von Benutzerberechtigungen ist jedoch nur möglich, wenn eine schriftliche Beantragung der Zugriffsrechte durch die Fachdienststellen vorliegt. Bei der Zuteilung der Benutzerberechtigungen, insbesondere bei der Gestaltung des Verfahrens, sollte auch der behördliche Datenschutzbeauftragte beteiligt werden.

Zusatzsoftware für PC
Bei PC, auf denen sensible personenbezogene Daten verarbeitet werden, ist neben der konsequenten Nutzung der

vorhandenen Sicherheitsmaßnahmen (Abschließen der Geräte oder Diskettenlaufwerke, Einsatz von Boot- oder Setup-Paßwörtern) eine wirksame Zugriffschutzsoftware einzusetzen, um eine unberechtigte Kenntnisnahme der gespeicherten Daten zu verhindern. Der Zugriff auf die Betriebssystemebene muß für den normalen Anwender mit Hilfe dieses Produktes gesperrt werden.

Deaktivierung von Bildschirmplätzen
Bei einem ganztägigen Rechnerbetrieb sind außerhalb der regelmäßigen Dienstzeiten sämtliche nicht benötigte Bildschirmarbeitsplätze vom DV-System zu deaktivieren, um einen unberechtigten Zugriff auf die gespeicherten Daten zu erschweren, zumal dann, wenn bei fehlerhaften Zugriffsversuchen systemseitig keine Sanktionen (z. B. Sperrung der Benutzerberechtigung bzw. des Endgeräts) ergriffen werden können.

Bedienerloses Ausschalten einer MX3OO
Im Bereich der Bayerischen Verwaltung ist der Einsatz von MX3OO-Rechnern der SNI AG weit verbreitet. Häufig müssen diese Rechner noch einige Zeit nach Beendigung der allgemeinen Bürozeit für einzelne Benutzer zur Verfügung stehen. Da viele Dienststellen aus Kostengründen keine zusätzliche Bedienkraft für die verspätete Beendigung des Rechnerbetriebs einstellen können, laufen die Rechner zumeist im (z. T. bedienerlosen) 24-Stunden-Betrieb. Damit steigt natürlich die Gefahr eines unerlaubten Rechnerzugriffs. Die Firma Josef Bauer hat nunmehr einen Schaltcomputer entwickelt, der Rechenanlagen der Serie MX300 zu vorher festgesetzten Zeiten ein- und ausschalten kann. Diese Schaltcomputer werden seit einiger Zeit vor allem im Justiz- und Finanzbereich eingesetzt. Probleme sind bisher nicht bekannt geworden.

Schlüsselverwaltung
Jede Dienststelle muß darauf achten, daß jederzeit nachvollziehbar ist, welcher Mitarbeiter welche Art von Schlüssel (General-, Gruppen- oder Einzelschlüssel) besitzt oder besessen hat. Zu diesem Zwecke muß ein revisionsfähiges Schlüsselverzeichnis geführt werden. Auch für die Aufbewahrung der Zweitschlüssel von Schränken und Schreibtischen ist eine einheitliche Regelung erforderlich. Die Mitnahme des Haus- oder Gruppenschlüssels für einzelne Stockwerke einer Dienststelle durch Mitarbeiter einer Putzfirma sollte tunlichst vermieden werden.

Fremdreinigung
Die Einhaltung des Datenschutzes bei Fremdreinigung hat mich in den letzten Jahren des öfteren beschäftigt. Besonders problematisch erscheint mir dabei die Fremdreinigung in sensiblen Amtsbereichen. Nachdem aufgrund einer Empfehlung durch den Obersten Bayerischen Rechnungshof nunmehr sogar Finanzämter gehalten sind, die Eigenreinigung aus Kostengründen auf Fremdreinigung umzustellen, wird die Gefahr einer unberechtigten Kenntnisnahme von Daten durch Außenstehende weiter wachsen. Zur Entschärfung dieser Gefahr verpflichten die Finanzämter beispielsweise die bei der Reinigungsfirma beschäftigten Personen nach dem Verpflichtungsgesetz (BGBl 11974, 547) auf das Steuergeheimnis. Außerdem findet die Reinigung von Räumen mit sensiblen Unterlagen zu einer Zeit statt, in der Bedienstete das Reinigungspersonal kontollieren können (Vier-Augen-Prinzip).

Eine derartige Regelung wäre auch für andere Behörden erwägenswert. Darüberhinaus muß mit der Reinigungsfirma eine schriftliche Vereinbarung getroffen werden, die den Geschäftsführer der Firma in die Pflicht nimmt, daß sich die bei der Firma beschäftigten und bei der Behörde eingesetzten Personen an die Weisungen der Behörde zu halten haben. Die Behörde sollte außerdem eine aktuelle Aufstellung aller Personen (insbesondere bei Änderungen) erhalten, die für die Reinigung ihrer Räume eingesetzt werden.

Entsorgung von Datenträgern
Auch in diesem Berichtszeitraum wurden wieder eine Anzahl von Behörden speziell hinsichtlich der datenschutzgerechten Entsorgung von Datenträgern mit personenbezogenen Inhalt überprüft. Ich konnte dabei feststellen, daß immer mehr Dienststellen ihre Papierunterlagen mit schutzwürdigen personenbezogenen Daten durch eine beauftragte Firma entsorgen lassen. Eine Polizeidienststelle erlebte dabei eine unangenehme Überraschung, als sie einer Zeitung entnehmen konnte, daß ihre Akten von spielenden Kindern ungeschützt in dem Hof eines Altpapierhändlers direkt an einer Straße gefunden wurden. Ein Teil der personenbezogenen Unterlagen war bereits über den Zaun auf die Straße gefallen. Aus diesem Anlaß bitte ich alle Dienststellen, die eine Datenträgerentsorgung im Auftrag vornehmen lassen, die Kontrollen über die mit der Entsorgung beauftragten Vertragsfirmen zu verstärken, um mögliche Schwachstellen leichter zu erkennen. So sollte sich der Auftraggeber vor einer Vertragsunterzeichnung durch eine Besichtigung vor Ort davon vergewissern, ob die eingesetzten Gerätschaften den Anforderungen der DIN 32757 Teil 1 entsprechen. Bei der Vertragsgestaltung mit den beauftragten Entsorgungsunternehmen sollten schließlich auch das Recht auf unangemeldete Kontrollen bei der Entsorgung und angemessene Vertragsstrafen für den Fall der Verletzung von Datenschutzvorschriften durch das beauftragte Unternehmen vereinbart werden. Die datenschutzgerechte Entsorgung des Papiergutes sollte der Auftragnehmer jeweils schriftlich bescheinigen.

Neben der weiterhin zum Teil fahrlässigen Entsorgung von Papierunterlagen mit personenbezogenem Inhalt bleibt die Entsorgung maschinenlesbarer Datenträger ein Problem für viele Dienststellen und hierbei insbesonders die steigende Anzahl zu vernichtender Streamer Tapes. Ich möchte daher noch einmal darauf hinweisen, daß diese Datenträger entweder physisch vernichtet oder - soweit möglich - durch eine Neuformatierung physikalisch gelöscht werden müssen. Ist die Formatierung wegen eines Defektes nicht

mehr möglich, so müssen andere wirksame Maßnahmen (z. B. Einsatz eines starken Elektromagneten) ergriffen werden.

Kuvertieren von Postsendungen durch Fremdfirmen
Einige Behörden lassen einen Teil ihrer Postsendungen (z. B. Bescheide über die Abfallentsorgungsgebühren) durch Privatfirmen versenden. Dagegen bestehen grundsätzlich keine Bedenken. Ich gehe allerdings davon aus, daß der Auftragnehmer unter besonderer Berücksichtigung der Eignung der von ihm getroffenen technischen und organisatorischen Maßnahmen ausgewählt wird und mit der Privatfirma ein Vertrag geschlossen wird, in dem die erforderlichen Sicherheitsmaßnahmen (Verarbeitungsvorgaben, Transportmaßnahmen, Vollständigkeitskontrolle o.ä.) näher erläutert werden. Im Vertrag sind außerdem Vertragsstrafen vorzusehen, wenn sich der Auftragnehmer weisungswidrig verhalten sollte.

21.3 Technische Einzelfragen

21.3.1 Protokollauswertungen

Die von DV-Benutzern verursachten Systemaktionen werden zur Nachvollziehbarkeit der maschinellen Datenverarbeitung in nahezu allen größeren DV-Systemen automatisch in sogenannten Log-Dateien protokolliert. Dabei wird auch die Berechtigung der Zugriffe und die Art des Zugriffs (lesen, kopieren, verändern, löschen oder übermitteln) auf die Datenbestände überwacht.

Das Wissen der Bediensteten um bestehende Aufzeichnungen und damit um die Möglichkeit umfassender nachträglicher Aufklärung eventueller auch länger zurückliegender Unregelmäßigkeiten trägt wesentlich dazu bei, bereits auf den Versuch eines Mißbrauchs der Datenverarbeitungsprogramme zu verzichten.

Alle anomalen Betriebszustände und Sicherheitsverletzungen an den DV-Anlagen müssen durch eine regelmäßige (tägliche) Auswertung der entsprechenden Log-Dateien festgestellt werden, damit die Dienststelle auf Sicherheitsverletzungen (z. B. Eindringversuchen) und alle anderen Versuchen von unzulässigen Aktionen rechtzeitig reagieren kann.

Da bei Stand-alone-PC von den eingesetzten Betriebssystemen grundsätzlich nichts oder zumindest sehr wenig protokolliert wird, ist im Einzelfall - unter Berücksichtigung der Sensibilität der Daten - zu prüfen, ob bei diesen Rechnern - genauso wie beim Einsatz der meisten Unix-Rechner - die Installation einer geeigneten Zusatzsoftware für die Revisionsfähigkeit der Datenverarbeitung notwendig ist. Wird der PC im Multi-User-Betrieb (Benutzung durch mehrere Personen) eingesezt, ist eine Protokollierung der DV-Aktivitäten grundsätzlich erforderlich. Zur gezielten Auswertung und regelmäßigen Kontrolle der vorhandenen Protokolldatei ist auch bei manchen anderen Rechnern (z.B. HP 3000) der Einsatz einer Zusatzsoftware erforderlich.

Insbesondere müssen bei einer Auswertung von Protokollen folgende Fragen beantwortet werden können:

- Ist gewährleistet, daß nachträglich überprüft und festgestellt werden kann, welche Daten zu welcher Zeit von wem in das DV-System eingegeben worden sind?
- Werden alle (wesentlichen) Aktivitäten der Benutzer (auch des Systemverwalters) aufgezeichnet (Vollständigkeit - kein Überschreiben von Protokolldaten vor ihrer Auswertung)?
- Sind alle Protokollierungen gegen Manipulation (wie Unterdrückung von Nachrichten) und nachträgliche Änderungen (z. B. Löschung von Einträgen) geschützt?
- Werden Zugriffsverletzungen (Fehlverhalten und Mißbrauchsversuche) und die dabei ergriffenen Sanktionen ausgewertet?
- Wird auch der regelmäßige Paßwortwechsel protokolliert (wobei die Paßworte nicht im Protokoll erscheinen dürfen)?
- Wird der Einsatz spezieller Utilities (wie Query-Sprachen, Norton Utilities etc) protokolliert?
- Sind die aufgezeichneten Systemnachrichten hinreichend aussagekräftig (Transparenz auch für Außenstehende)?
- Geben die aufgezeichneten Daten Auskunft über alle Datensicherungsaktivitäten?
- Werden Datenübermittlungen protokolliert (welche Daten zu welcher Zeit an wen)?
- Gestatten die Ablaufdaten Auskünfte über die Wartungsarbeiten, einschließlich der Feruwartung?
- Ist sichergestellt, daß die Protokolle durch eine vorher bestimmte Person in regelmäßigen Zeitabständen ausgewertet werden?
- Ist bei der Auswertung das Vier-Augen-Prinzip gewährleistet?
- Existieren Hilfsprogramme zur Auswertung der aufgezeichneten Ablaufdaten?
- Werden die Protokolle über einen längeren Zeitraum (etwa ein Jahr) archiviert?
- Worauf werden die Protokolle archiviert (Festplatte, Magnetband, Diskette, Streamer Tape, Papier)?

Gemäß Art. 17 Abs. 4 BayDSG ist eine Speicherung von Protokolldaten nur zulässig, wenn sie auch erforderlich sind und ausschließlich zu Zwecken der Datenschutzkontrolle, der Datensicherung oder zur Sicherstellung eines ordnungsgemäßen Betriebes der Datenverarbeitungsanlage dienen. In einer Vereinbarung mit dem Personalrat sollten die Einzelheiten der in diesem Rahmen erfolgenden Auswertungen und ihrer Nutzungen festgelegt werden (wer darf diese wie, mit welchen Hilfsmitteln und zu welchem Zweck auswerten). Hierdurch wird auch gewährleistet, daß das Instrument der Protokollierung nicht zweckentfremdet verwendet wird, etwa für die Durchführung einer unzulässigen Verhaltens- oder Leistungskontrolle der Mitarbeiter.

21.3.2 Sicherheitsmechanismen in Netzwerken

Der Einsatz von Kommunikationsnetzen setzt sich in der öffentlichen Verwaltung immer mehr durch. Viele

Behörden vernetzen ihre Computer zu LAN (Local Area Netzwork) oder WAN (Wide Area Network) bzw. Unterformen dieser Netzarten. Während sich Stand-alone-Systeme ohne Anschlüsse an Netze - zumindest im Großrechnerbereich - relativ leicht absichern lassen, entstehen im Zuge einer Vernetzung - neben den Sicherheitslücken des Netzwerkbetriebssystems - natürlich zusätzliche Sicherheitsprobleme auf und für den Transportweg (z. B. Gefahr einer Abhörung des Netzes). Die Bedrohung des nicht autorisierten Zugriffs auf ein Netz oder der an diesem Netz angeschlossenen Rechner geht im wesentlichen von den Einwahlzugängen oder Gateways zu fremden Netzen aus.

Zur Sicherung der Netzkommunikation ist der Einbau von Sicherheitsmechanismen unbedingt erforderlich. In Frage kommen dabei insbesondere:

Hardware-Zugriffsschutzsysteme

Zwischen dem jeweiligen Rechner oder Endgerät und dem Netzanschluß (Modem) werden Einrichtungen (sog. Black Boxes) geschaltet, die sich zu beiden Seiten hin schnittstellenneutral verhalten. In Zusammenarbeit mit einer entsprechenden Sicherheitseinrichtung auf der Gegenseite sorgen sie für die Sicherung der Netzkommunikation. Der Zugang zum Rechner wird erst nach Anruferidentifikation gewährt, wobei die jeweilige Zugriffsberechtigung überprüft und der Anrufer erst nach Authentisierung durchgeschaltet wird.

Vorteile dieser Lösung sind:

- Die Einrichtungen sind rechner- und betriebssystemunabhängig; sie können auch in heterogenen Netzen verwendet werden.
- Zugriffsschutzsysteme auf Hardware-Basis bieten eine anwendungsunabhängige Sicherheit.

Einsatz kryptographischer Verfahren

Sicherheitsfunktionen gegen unbefugtes Mithören der Kommunikation und unbemerkte Veränderung der übertragenen Daten können auch direkt in das Endgerät integriert werden. Hierbei ist zu entscheiden, in welche der sieben ISO-Schichten diese, in erster Linie kryptographischen Mechanismen integriert werden. So kann z. B. eine ganze Anwendung (Schicht 7), ein Darstellungsprotokoll (Schicht 6) oder auch nur das Transportprotokoll (Schicht 4) kryptographisch gesichert werden.

Man unterscheidet bei der Kryptographie zwischen symmetrischen und asymmetrischen Verfahren. Symmetrische Verfahren arbeiten mit einem Schlüssel für die Verund Entschlüsselung (Privat Key), der allen beim Nachrichtenaustausch beteiligten Partnern bekannt ist. Bei diesem Verfahren ist die Gefahr einer Weitergabe des Schlüssels relativ groß. Das derzeit am weitesten verbreitete symmetrische Chiffnerverfahren ist der 1977 vom amerikanischen National Bureau of Standards (NBS) normierte Data Encryption Standard (DES).

Sicherer sind asymetrischen Verfahren (Public-Key-Verfahren), bei denen ein Schlüsselpaar verwendet wird: ein geheimer privater Schlüssel und ein öffentlicher Schlüssel, der beliebigen Partnern bekannt gegeben werden kann. Mit dem öffentlichen Schlüssel wird die Nachricht verschlüsselt und nur mit dem privaten Schlüssel läßt sich die Nachricht entschlüsseln und zweifelsfrei nachweisen, daß nur der Eigentümer des privaten Schlüssels die Nachricht abgesandt haben kann. Darüberhinaus lassen sich Nachrichten und Dokumente signieren (elektronische Unterschriften), um so deren Integrität sowie deren Herkunft und Empfang einwandfrei nachweisen zu können. Das bekannteste asymetrische Verfahren ist das RSA-Verfahren (benannt nach Rivest, Shamir, Adleman, die es zum ersten Mal vorgeschlagen haben). Es tut der Sicherheit keinen Abbruch, daß ein spezieller, relativ kleiner RSA-Schlüssel (rund 130 Stellen) in den Vereinigten Staaten mit großem, unverhältnismäßig hohem Aufwand entschlüsselt wurde. (Quelle: Orgatec-Beilage der Süddeutschen Zeitung vom 19.10.1994). Schlüssel, die mehr als 200 Stellen umfassen, können derzeit weiterhin als sicher betrachtet werden.

Vorteile dieser Lösung sind:

- Es ist keine zusätzliche Einrichtung erforderlich
- Es ist möglich, bestimmte Daten explizit zu schützen.

Chipkarten

Chipkarten sind ein Insirument zur Anwendung kryptographischer Verfahren in Informationssystemen. Sie enthalten in einer Plastikkarte einen Mikroprozessor und geschützte, auslesesichere Speicher, in denen Verschlüsselungsalgorithmen und andere sicherheitsrelevante Funktionen gespeichert sind. Der System- und Netzzugang erfolgt in zwei Schritten. Zunächst weist der Benutzer durch ein persönliches - jederzeit selbst änderbares -Kennwort (PIN) nach, daß er der rechtmäßige Eigentümer der Chipkarte ist. Anschließend weist die Chipkarte gegenüber dem System über kryptographisch ermittelte Parameter ihre Zugangsberechtigung nach.

Verliert ein Anwender seine Chipkarte, dann kann ein Finder diese ohne Kenntnis der individuellen PIN nicht verwenden.

Chipkarten eignen sich für die Realisierung wichtiger Sicherheitsmaßnahmen in Netzwerken (Zugriffskontrolle, Nachrichtenauthentifikation, Nachrichtenverschlüsselung, elektronische Unterschrift).

21.3.3 Telebox-400

Der Datenaustausch über den Telebox-400-Dienst der Deutschen Bundespost Telekom gewinnt zunehmend an Bedeutung, weil dieser Mailbox-Dienst eine recht interessante Art darstellt, wirtschaftlich Daten auszutauschen. Der Telebox-400-Dienst verfügt in seiner heutigen Ausbaustufe nach der Empfehlung der CCITT X.400 von 1984 über einen gewissen sicherheitstechnischen Grundschutz, der sich allerdings nur auf den Zugangsschutz über Benutzerkennung und Paßwort sowie auf die

Sanktionen nach mehrmaligen ungültigen Zugriffsversuchen in ununterbrochener Folge bezieht.

In einer weiteren Ausbaustufe sollen die Sicherheitsmechanismen der Empfehlung der CCITT X.400 von 1988 zur Verfügung gestellt werden. Dabei handelt es sich in erster Linie um den Einsatz von kryptographischen Verfahren bei der Identifizierung und beim Nachrichtentransport sowie um Maßnahmen zur Verifizierung der Dokumentenechtheit. In der Zwischenzeit hat sich der Anwender um die Realisierung dieser unverzichtbaren Funktionen selbst zu kümmern (siehe dazu „Übermittlung von Steuererklärungsdaten auf elektronischem Weg").

21.3.4 Elektronische Mitteilungssysteme

Neben den Telebox-Anwendungen, bei denen die Telekom die gesamte technische Infrastruktur stellt, gewinnen private elektronische Mitteilungssysteme immer mehr an Bedeutung. In Deutschland existieren auf diesem Gebiet schon über 100 Betreiber, hauptsächlich aus dem Bereich der Privatwirtschaft.

In der bayerischen Staatsverwaltung gibt es zur Zeit einige Projektgruppen, die sich mit dem Aufbau eines Elektronischen Mitteilungssystems befassen. In einer Besprechung des Führungskreises des Projekts „Hochgeschwindigkeitsnetze" wurde am 22.9.1994 eine Projektgruppe „Behördennetz" unter dem Vorsitz der Bayer. Staatskanzlei eingerichtet. Auch der Koordinierungsausschuß „Datenverarbeitung" unterhält seit längerem eine Arbeitsgruppe, die an einige in Deutschland tätige Privatfirmen Preisanfragen bezüglich der Einrichtung eines gemeinsamen Transportnetzes im staatlichen Bereich gerichtet hat. Mit der Organisation einer ressortübergreifenden Kommunikation auf der Basis des X.400-Standards beschäftigt sich auf Initiative des Bayer. Staatsministenum des Innern eine weitere Arbeitsgruppe des Koordinierungsausschusses, die die ersten Ergebnisse (technisches Konzept) Ende des Jahres vorgelegt hat.

Hochgeschwindigkeitsnetze werden überall dort benötigt, wo es um die schnelle Übertragung großer Datenmengen geht. Dazu einige Beispiele: Nutzung der Rechnerkapazität von leistungsfähigen Vektorrechnern im Wissenschaftsbereich, Übertragung von Raster- und Vektorgraphiken, Übertragung von Bewegt-Bildern (Video-Konferenzen), Multimedia-Anwendungen.

In einem Behördennetz sollen neben dem Fernsprechen auch Texte und Dokumente (Bilder, Tabellen) übertragen werden. In der Pilotphase ist zunächst daran gedacht, umfangreiche Texte ohne Personenbezug (etwa Bundesratsangelegenheiten, Sachabstimmungen in der Länderkommunikation, Parlamentsdrucksachen) zu übertragen. Anzumerken ist, daß auch diese Texte vertrauliche Informationen enthalten können. Bei der Übertragung von Texten und Dokumenten sensiblen, personenbezogenen Inhalts sind jedoch bestimmte Sicherheitsstandards einzuhalten, die sich mindestens an dem X.400-Sicherheitsstandard von 1988 orientieren. Im einzelnen handelt es dabei im wesentlichen um folgende Sicherheitsmaßnahmen:

- Zugriffsschutzmaßnahmen (Maßnahmen zur Identifizierung und Authentisierung eines Benutzers)
- Maßnahmen zur Beweissicherung (Empfangsnachweise bei der Zustellung bzw. Empfangsübergabenachweise beim Senden)
- Schutz vor falschen Absendern
- Integrität der übersandten Texte und Dokumente (Signierung mit elektronischer Unterschrift)
- Vertraulichkeit der übersandten Texte und Dokumente (Verschlüsselung mit zertifizierten Schlüsseln)
- Einrichtung einer geschlossenen Benutzergruppe bei Übertragung in öffentlich zugänglichen Netzen
- Eigene Hard- und Software-Komponenten (MTA-Message Transfer Agents) für den elektronischen Mitteilungsdienst (Abschottung des innerbetrieblichen Kommunikationsnetzes).

Bei der Auftragsvergabe an einen privaten Netzanbieter, bei dem unter Umständen Texte zwischengespeichert werden, sind schließlich die Vorschriften des Art. 6 BayDSG über „die Verarbeitung personenbezogener Daten im Auftrag" zu beachten, wonach der Auftragnehmer unter Berücksichügung der Eignung der von ihm getroffenen technischen und organisatischen Maßnahmen sorgfältig auszuwählen ist.

All diese Forderungen werden bisher noch von keinem Anbieter in vollem Unfang erfüllt. Es gibt jedoch Hersteller, die in ihrer Produktpalette verschiedene Systemkomponenten entwickelt haben, die manche Sicherheitsmaßnahmen unterstützen, so daß ich bei der Übertragung personenbezogener Daten auf die Einhaltung dieser Maßnahmen drängen werde.

21.3.5 Risiken für und Erkennung von einem Virenbefall

Im Rahmen meiner Kontrollen und Beratungen weise ich immer wieder auf das Risiko einer Gefährdung der Datenverarbeitung durch Computerviren hin und zeige dabei die nachfolgenden Hauptgefahrenquellen eines Virenbefalls auf:

- Datenträgeraustausch (Fremdprogramme, unlizensierte Software, Raubkopien, Public Domain Programme, Shareware, Test- und Demodisketten)
- Offene Netze (z.B. Mailboxen, in die ausführbare Programme eingestellt werden, oder Hacker, die über Wählleitungen eindringen)
- Software-Einsatz (Anwendungsentwicklung, Software-(Fern)Wartung, Speicherung der Programme im Source Code)
- Hardware-Einsatz (mißbräuchliche Nutzung durch berechtigte Benutzer, unberechtigte Nutzung durch Dritte, Zulassung von Diskettenlaufwerken, freizügige Benutzerberechtigungen).

Zur möglichst schnellen Erkennung eines eventuellen Virenbefalls sollte man auf einige Anzeichen achten, die für Infektionen typisch sind. Dies sind beispielsweise:

- geringere Rechnerleistung
  (Jedes infizierte Programm macht mehr als das, wofür es ursprünglich geschrieben wurde. Es infiziert zum Beispiel andere Programme. Das erfordert zusätzliche Rechnerleistung, worunter die Leistungsfähigkeit des Systems leidet. Da die meisten Virenproduzenten den Ehrgeiz haben, daß ihre Viren jedes Programm nur einmal infizieren soll, muß die Virussequenz jedes Programm daraufüm untersuchen, ob es bereits infiziert ist. Mit zunehmender Verseuchung der Programme muß ein solcher Virus hierzu immer länger suchen, um ein noch nicht infiziertes Programm zu finden. Dies führt ebenfalls zu einem Anstieg der verbrauchten Rechnerleistung.)
- vermehrte Festplatten- und Diskettenzugriffe
- vorher nicht aufgetretene Programmabstürze
  (Nicht jeder Fehler, der während der Arbeit am Computer auftritt und einen Programmabsturz zur Folge hat, ist auf einen Virus zurückzuführen. Es könnte sich auch um einen SoftwareFehler handeln. Stellen sich jedoch Fehler ein, die unter denselben Bedingungen bisher nicht auftraten, ist unbedingt eine Virenüberprüfung zu starten.)
- unbekannte Fehlermeldungen bzw. merkwürdige Bildschirmmeldungen
- unerklärliche Hauptspeicher- bzw. Festplattenverknappung
  (Nach Einbau eines Virus sind die Programme größer als vorher und benötigen folglich mehr Speicherplatz. Speicherresidente Viren fressen langsam aber sicher den freien Hauptspeicherplatz auf.)
- defekte Cluster auf Datenträgern.

21.3.6 Übermittlung von Einkommensteuererklärungsdaten auf elektronischem Weg

Das Bayer. Staatsministerium der Finanzen hat im Zuge möglicher Rationalisierungsmaßnahmen im Steuerfestsetzungsverfahren ein Verfahren entwickelt, bei dem Einkommensteuererklärungsdaten auf elektronischem Weg vom Steuerpflichtigen an das Finanzamt übermittelt werden können. Dazu werden in Pilotversuchen von der Lohnsteuerhilfe Bayern e.V. und von der DATEV e.G. die Daten der Einkommensteuererklärung neben der bisherigen Papierform zusätzlich durch Datenfernübertragung an das zuständige Rechenzentrum der Finanzverwaltung (EDV-Stelle) in München und Nürnberg gesandt. Die elektronische Übertragung erfolgt bei der Lohnsteuerhilfe Bayern e.V. über den Telebox-400-Dienst der Telekom, bei der DATEV e.G. direkt über Wählleitung mit dem Übertragungsverfahren FTAM.

Der Rationalisierungseffekt soll darin bestehen, daß die bisherige Datenerfassung im Finanzamt entfällt bzw. vermindert wird und die elektronisch übertragenen Daten direkt für die Erstellung des Steuerbescheids verwendet werden können.

Das Bayer. Staatsministerium der Finanzen hat mich bei diesem Projekt frühzeitig beteiligt, damit mögliche Sicherheitsrisiken aus der Sicht des Datenschutzes rechtzeitig erkannt und bei der weiteren Verfahrensentwicklung durch entsprechende Sicherheitsmaßnahmen verhindert werden.

Pilotverfahren

An den Pilotverfahren nehmen auf seiten der Finanzverwaltung Finanzämter aus den OF-Bezirken München und Nürnberg sowie die EDV-Stellen der Steuerverwaltung in München und Nürnberg, auf seiten der steuerberatenden Berufe die Lohnsteuerhilfe Bayern e.V. und die DATEV e.G. teil. Maschinell unterstützt wird beim Versuch mit der Lohnsteuerhilfe Bayern e.V. die Abgabe der Einkommensteuererklärung für Arbeitnehmer, beim Versuch mit der DATEV e.G. auch die Einkommensteuererklärung von Unternehmern.

Die Lohnsteuerhilfe Bayern e.V. überträgt die Erklärungsdaten verschlüsselt über eine Wählleitung in die Telebox im Telekom-Rechenzentrum in Mannheim. Die EDV-Stelle ruft die Daten ebenfalls über eine Wählleitung, die zu einem PC geschaltet ist, aus der Telebox ab. Diese Wählleitung ist nur während der Übertragungsbzw. Abrufzeit aktiv geschaltet. Der Zugriff auf die Telebox ist für beide Teilnehmer durch Paßwort abgesichert. Will die EDV-Stelle auf die Telebox zugreifen, muß es sich durch Benutzerkennung und Paßwort authentifizieren. Nach dem Datenabruf muß die EDV-Stelle ein zweites Paßwort eingeben, um die aus der Telebox übertragenen Daten entschlüsseln zu können. Zwischen der Lohnsteuerhilfe und der EDV-Stelle wird ein Ver- und Entschlüsselungspaßwort vereinbart, das im 2-Monatsturnus geändert wird. Die Verschlüsselung bewirkt, daß die Daten, solange sie sich außer Haus befinden (auf Leitung, beim elektronischen Postamt), verschlüsselt und für Außenstehende nicht verständlich sind. Die eingesetzte Software sorgt vor der Verschlüsselung zusätzlich noch für eine Verdichtung der Datenmenge. Beim elektronischen Postamt in Mannheim sind getrennte ,,elektronische Brielkästen" für den Datenempfang (Senden durch die Lohnsteuerhilfe) und für den Datenabruf (durch die EDV-Stelle) eingerichtet. Die datenabgebenden Stellen können auf die Daten im ,,Briefkasten" des Abrufberechtigten nicht mehr zugreifen. Der für den Datenabruf bestimmte ,,Briefkasten" ist nur von der datenempfangenden Stelle (die jeweilige EDV-Stelle der Steuerverwaltung) anwählbar.

Das Datenabrufverfahren läuft menueunterstützt ab. Sind in der Telebox neue, noch nicht abgerufene Daten gespeichert, erhält der Benutzer nach dem Anwählen einen Hinweis (Absender, Empfänger, Datenmenge). Nach dem Abruf werden die Daten in der EDV-Stelle entschlüsselt und entpackt und über eine Diskette zur Weiterverarbeitung auf den Großrechner gebracht (PC und

Host-Rechner sind nicht miteinander verbunden; sog. Vorrechner-Konzept). Dieser Schritt soll später einmal automatisiert ablaufen, wobei dann nur der Host-Rechner abrufberechtigt sein wird, um ein Eindringen über die PC-Wählleitung in das DV-System der EDV-Stelle zu verhindern. 24 Stunden nach Abruf durch die EDV-Stelle werden die verschlüsselten Daten in der Telebox gelöscht.

Beim derzeitigen Verfahrensstand werden zwischen der Lohnsteuerhilfe und der EDV-Stelle über die Telebox nur Berechnungsdaten mit Steuernummer aber keine Daten des Grundinformationsdienstes (persönliche Daten, wie Name und Anschrift) ausgetauscht. Wollten die übermittelten Daten einer Person zugeordnet werden, müßte bekannt sein, wem die übermittelte Steuernummer zugeteilt worden ist Dazu wäre Zusatzwissen aus dem Grundinformationsdienst der Steuererkärung erforderlich. Die Daten des Grundinformationsdienstes erhält das zuständige Finanzamt über die herkömmliche Steuererklärung auf Papier, die bei der jeweiligen Geschäftsstelle der Lohnsteuerhilfe erstellt, mit einer sog. Tele-Nummer, die als Zuordnungsmerkmal für die maschinell übermittelten Daten gilt, versehen und unterschrieben an das Finanzamt geschickt wird. Die über die Telebox übermittelten Daten kann das Finanzamt auf herkömmlichem Weg bei der EDV-Stelle abrufen, mit den Erklärungsdaten vergleichen und zur Berechnung der Einkommensteuer freigeben.

Beim Versuch mit der DATEV e.G. werden die Daten über Wählleitungen vom Steuerberater zur DATEV e.G. und von dort zu den jeweiligen EDV-Stellen der Steuerverwaltung übermittelt. Verschlüsselung und Vorrechner-Konzept entsprechen dem Verfahren der Lohnsteuer-hilfe Bayern e.V.

Das DV-Verfahren zur Unterstützung des Erklärungseingangs soll dann weiterentwickelt werden, wenn eine entsprechende Akzeptanz seitens der Partner festzustellen ist.

Die Steuerverwaltung ist bestrebt, mit wenigen DA-Partnern (DA bedeutet Datenaustausch) einen möglichst großen Kreis von Steuerpflichtigen zu erreichen. Die DA-Partner müssen den Vorgaben der Steuerverwaltung entsprechen. Die Zahl der Partner im maschinellen Verfahren wird deshalb gering sein.

■ **Ergebnisse**

Die Steuerverwaltung hat - soweit erkennbar - alle Möglichkeiten für eine sichere Datenübertragung der Steuererklärungsdaten ausgeschöpft.

Sie setzt eine Zusatzsoftware ein, die eine Verschlüsselung und Komprimierung der Daten ermöglicht und eine Offenbarung dieser Daten durch Unbefugte weitgehend ausschließt. Für den Datenabruf wurde eine eigene Wählleitung angemietet, die nicht über die zentrale Telefonvermittlung läuft. Es wird außerdem sichergestellt, daß der Datenabruf nur aus einer Richtung möglich ist.

Der Wählleitungsanschluß ist nur während des Datenzugriffs aktiviert, so daß fremde Dritte nicht in den PC bzw. Vorrechner der EDV-Stelle der Steuerverwaltung eindringen können.

Gegen dieses DV-Verfahren bestehen aus Gründen der Datensicherheit keine grundsätzlichen Bedenken, soweit das beim gegenwärtigen Verfahrensstand beurteilt werden kann.

Zur Verbesserung der Datensicherheit wurden angeregt:

- der 2-Monatszeitraum für die Gültigkeit eines Ver- und Entschlüsselungspaßwortes sollte verkürzt werden;
- die Länge der Paßworte muß mindestens 6 alphanumerische Zeichen umfassen;
- der PC ist nach dem Datenabruf aus der Telebox stets zu deaktivieren oder abzusperren.

21.3.7 Datenschutzregister

Bereits im 15. Tätigkeitsbericht habe ich darauf hingewiesen, daß durch das Bayerische Datenschutzgesetz vom 23. Juli 1993 die Verordnung über das Datenschutzregister vom 23. November 1978 und Art. 7 des Bayerischen Datenschutzgesetzes vom 28. April 1978 mit Wirkung vom 1. August 1993 außer Kraft getreten ist. Von diesem Zeitpunkt an fielen die Registermeldungen ersatzlos weg. Davon ausgenommen waren aber noch Sozialbehörden, die unter die Regelungen des § 79 des Zehnten Buches des Sozialgesetzbuchs (SGB X) fallen.

Durch das Zweite Gesetz zur Änderung des Sozialgesetzbuchs (2. SGBÄndG) vom 13. Juni 1994 wurde in §81 SGB X die bisherige Regelung des § 79 SGB X dahingehend klargestellt, daß bei öffentlichen Stellen der Länder, die unter § 35 SGB 1 fallen, sich die Aufgaben und Befugnisse der Landesbeauftragten für den Datenschutz nach dem jeweiligen Landesrecht richten. Durch diese Änderung ist auch eine Registermeldung für bayerische Sozialbehörden entfallen (siehe auch unter Sozialbehörden - Änderung von Rechtsvorschriften unter Nr.3.1.1).

Die Zahl der Bürger, die sich schriftlich an mich gewandt und um Auskunft aus dem Datenschutzregister gebeten haben, hat sich im Berichtsjahr weiter verringert.

Als Ersatz für das Datenschutzregister gilt das sog. Anlagen- und Verfahrensverzeichnis, das die speichernden Stellen zum 1. März 1995 eingerichtet haben müssen.

22. Der Beirat

Die Mitglieder des Beirates werden nach Art. 33 Abs. 2 BayDSG für vier Jahre, die Beiratsmitglieder aus der Mitte des Landtags für die Wahldauer des Landtags bestellt. Im Berichtszeitraum gehörten dem Beirat an:

Ordentliche Mitglieder	**Vertreter**
die Landtagsabgeordneten	
- in der 12. Legislaturperiode -	
Franz Brosch	Prof. Dr. Hans Gerh. Stockinger
Alois Braun	Dr. Helmut Müller
Franz Meyer	Wilhelm Wenning
Markus Sackmann	Georg Grabner
Dr. Klaus Hahnzog	Armin Nentwig
Carmen König	Joachim Wahnschaffe
- in der 13. Legislaturperiode (ab der Landtagswahl im Herbst 1994) -	
Franz Brosch	Prof. Dr. Hans Gerh. Stockinger
Rudolf Engelhard	Johannes Neumeier
Alfred Reisinger	Dr. Helmut Müller
Markus Söder	Markus Sackmann
Dr. Klaus Hahnzog	Joachim Wahnschaffe
Franz Schindler	Dr. Thomas Jung
die Senatoren	
Wolfgang Burnhauser	Hartwig Reimann
für die Staatsregierung	
Christian P. Wilde Ministerialrat im Bayer. Staatsministerium des Innern	Hubert Kranz Ministerialrat im Bayer. Staatsministerium der Finanzen
für die Sozialversicherungsträger	
Dr. Ludwig Bergner Erster Direktor der Landesversicherungsanstalt Oberbayern	Gerhard Wunderlich, Direktor, Geschäftsführer des BKK Landesverbands Bayern
für die Kommunalen Spitzenverbände	
Klaus Eichhorn Geschäftsführender Direktor der Anstalt für Kommunale Datenverarbeitung in Bayern	Hanns Herrlitz Direktor der Anstalt für Kommunale Datenverarbeitung in Bayern
für den Verband der Freien Berufe in Bayern e.V.	
Erwin Stein, MdL Präsident der Steuerberaterkammer München	Winfried Wachter Präsidiumsmitglied des Verbandes der Freien Berufe in Bayern e.V.

Den Vorsitz im Beirat führt Franz Brosch, MdL; Stellvertreterin war Carmen König, MdL.Abderl3.Legislaturperiode ist Dr. Klaus Hahnzog, MdL, Stellvertreter.

Der Beirat befaßte sich in seinen Sitzungen am 02.11.1993, 14.12.1993, 15.03.1994, 28.06.1994 und 06.12.1994 insbesondere mit folgenden, Themen:

- Beratung des 16. Tätigkeitsberichtes
- Berichte über Prüfungen und Beanstandungen
- Berichte von Arbeitskreisen und Datenschutzkonferenzen
- Normentwürfe im Sicherheitsbereich (Änderung des Bayerischen Verfassungsschutzgesetzes, Bayerische Bundesratsinitiative für ein Gesetz zur Änderung des OrgKG und Gesetz über die Erprobung einer Sicherheitswacht)
- elektronische Erfassung und Überwachung von Straßenbenutzungsgebühren
- maschinell-geführtes Grundbuch: Protokollierung der Einsichtnahme (mit einem Besuch beim Grundbuchamt München am 15.06.1994)
- Verordnung zum BayDSG

23. Konferenz der Datenschutzbeauftragten des Bundes und der Länder

1994 fanden zwei Konferenzen der Datenschutzbeauftragten des Bundes und der Länder statt.
Schwerpunkte der Erörterung waren:

- Datenschutzfragen im Polizeibereich
- Datenschutzfragen im Bereich des Strafverfahrens
- Datenschutzfragen im Sozialbereich
- Erörterung zum Entwurf der EU-Datenschutzrichtlinie und der ISDN-Richtlinie
- Erörterung zur datenschutzrechtlichen Einordnung von Wartung und Fernwartung automatisierter Verfahren
- Automatische Autobahngebührenerfassung
- Entwurf eines Krebsregistergesetzes
- Datenschutzfragen im Zusammenhang mit Entwürfen für ein Transplantationsgesetz
- Zugriffssperren für automatisiert gespeicherte Beitrags- und Leistungsdaten in der gesetzlichen Krankenversicherung

Mit Zustimmung Bayerns wurden Entschließungen zu folgenden Themen verabschiedet:

- Chipkarten und Automatisierung der Datenverarbeitung in der gesetzlichen Krankenversicherung - Entschließung vom 09./10.03. 1994 (siehe Anlage 1)
- Erörterungen zu Datenschutzfragen bei der Postreform II - Entschließung vom 09./10.03.1994 Verordnung (EG) des Rates über die Tätigkeit der Gemeinschaft im Bereich der Statistik (Bundesrats-Drucksache 283/94) - Entschließung vom 25.08.1994
- Vorschläge zur Überprüfung der Erforderlichkeit polizeilicher Befugnisse und deren Auswirkungen für die Rechte der. Betroffenen - Entschließung vom 26./27.09.1994 (siehe Anlage 2)
- Erörterung datenschutzrechtlicher Defizite im Justizbereich - Entschließung vom 26./27.09. 1994 (siehe Anlage 2)
- Datenschutzrechtliche Anforderung an ein EUROPOL-Übereinkommen - Entschließung vom 26./27.09. 1994 (siehe Anlage 2)
- Art. 12 Verbrechensbekämpfungsgesetz - Trennung von Polizei und Nachrichtendiensten - Entschließung vom 26/27.09.1994 (siehe Anlage 2)

- Erörterung des geänderten Vorschlags für eine europäische Richtlinie zum Datenschutz im ISDN und im Mobilfunknetz vom 13.06.1994 - Entschließung vom 26./27.09. 1994 (siehe Anlage 2)

Gegen die Stimme oder bei Stimmenthaltung Bayerns wurden folgende Entschließungen verabschiedet:

- Vorschläge zu gesetzlichen Regelungen der Informationsverarbeitung im Strafverfahren vom 09./10.03. 1994
- Abbau des Sozialdatenschutzes vom 09./10.03. 1994
- Entwurf eines Gesetzes für ein Ausländerzentralregister vom 09/10.03.1994

Anlage 1: Beschluß der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 09/10. 03.1994

Chipkarten im Gesundheitswesen

Die Datenschutzbeauftragten von Bund und Länder verfolgen die zunehmende Verwendung von Chipkarten im Gesundheits- und Sozialwesen mit kritischer Aufmerksamkeit.

Chipkarte als gesetzliche Krankenversicherungskarte

Die Krankenversicherungskarte, die bis Ende des Jahre in allen Bundesländern eingeführt sein wird, darf nach dem Sozialgesetzbuch nur wenige Identifikationsdaten enthalten. Die Datenschutzbeauftragten überprüfen, ob

- die Krankenkassen nur die gesetzlich zulässigen Daten auf den Chipkarten speichern und
- die Kassenärztlichen Vereinigungen dafür sorgen, daß nur vom Bundesamt für Sicherheit in der Informationstechnik zertifizierte Lesegeräte und vom B undesverband der Kassenärztlichen Vereinigungen geprüfte Programme eingesetzt werden.

Chipkarte als freiwillige Gesundheitskarte

Sogenannte ,,Gesundheitskarten", etwas ,,Service-Karten" von Krankenversicherungen und privaten Anbietern, ,,Notfall-Karten", Apo(theken)-Cards" und ,,Röntgen-Karten" werden neben der Krankenversicherungskarte als freiwillige Patienten-Chipkarte angeboten und empfohlen. Während die Krankenversicherungskarte nach dem Sozialgesetzbuch nur wenige Identifikationsdaten enthalten darf, kann mit diesen ,,Gesundheitskarten" über viele medizinische und andere persönliche Daten schnell und umfassend verfügt werden.

Gegenüber der konventionellen Ausweiskarte oder einer Karte mit einem Magnetstreifen ist die Chipkarten-Technik ungleich komplexer und vielfältig nutzbar. Damit steigen auch die Mißbrauchsgefahren bei Verlust, Diebstahl oder unbemerktem Ablesen der Daten durch Dritte. Anders als bei Ausweiskarten mit Klartext können Chipkarten nur mit technischen Hilfsmitteln gelesen werden, die der Betroffene in der Regel nicht besitzt. So kann er kaum kontrollieren, sondern muß weitgehend darauf vertrauen, daß der Aussteller der Karte und sein Arzt nur die mit ihm vereinbarten Daten im Chip speichern, das Lesegerät auch wirklich alle gespeicherten Daten anzeigt und der Chip keine oder nur eindeutig vereinbarte Verarbeitungsprogramme enthält.

Die Freiwilligkeit der Entscheidung für oder gegen die Gesundheitskarte mit Chipkarten-Technik ist in der Praxis bisweilen nicht gewährleistet. So wird ein faktischer Zwang auf die Entscheidungsfreiheit des Betroffenen ausgeübt, wenn der Aussteller - etwa ein Krankenversicherungsunternehmen oder eine Krankenkasse - mit der Einführung der Chipkarte das bisherige konventionelle Verfahren erheblich ändert, z.B. den Schriftwechsel erschwert oder den Zugang zu Leistungen Karten-Inhabern vorbehält bzw. erleichtert

So stellt beispielsweise eine Kasse ihren Mitgliedern Bonuspunkte in Aussicht, wenn sie auf sog. Aktionstagen der Kasse Werte wie Blutzucker, Sauerstoffdynamik, Cholesterol sowie weitere spezielle medizinische Daten ohne ärztliche Konsultation messen und auf der Karte speichern und aktualisieren lassen. In Abhängigkeit von der Veränderung dieser Werte wird von der Kasse gegebenenfalls ein Arztbesuch empfohlen. Die Vergabe solcher Bonuspunkte widerspricht dem Prinzip der Freiwilligkeit bei der Erhebung der Daten für die PatientenChipkarte. Der Effekt wird noch verstärkt, indem die Kasse die ,,Möglichkeit einer Beitragsrückerstattung" in Aussicht stellt. Die Datenschutzbeauftragten des Bundes und der Länder sehen in dieser Art der Anwendung der Chipkarten-Technik das Risiko eines Mißbrauchs, solange der Inhalt und die Nutzung der Daten nicht mit den zuständigen Fachleuten - wie den Medizinern - und den Krankenkassen abgestimmt ist.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hält für den Einsatz und die Nutzung freiwilliger Patienten-Chipkarten zumindest - vorbehaltlich weiterer Punkte - die Gewährleistung folgender Voraussetzungen für erforderlich:

- Die Zuteilung einer Gesundheitskarte und die damit verbundene Speicherung von Gesundheitsdaten bedarf der schriftlichen Einwilligung des Betroffenen. Er ist vor der Erteilung der Einwilligung umfassend über Zweck, Inhalt und Verwendung der angebotenen Gesundheitskarte zu informieren.
- Die freiwillige Gesundheitskarte darf nicht - etwa durch Integration auf einem Chip - die Krankenversichertenkarte nach dem Sozialgesetzbuch verdrängen oder ersetzen
- Die Karte ist technisch so zu gestalten, daß für die einzelnen Nutzungsarten nur die jeweils erforderlichen Daten zur Verfügung gestellt werden.
- Der Betroffene muß von Fall zu Fall frei und ohne Benachteiligung - z.B. gegenüber dem Arzt, der Krankenkasse oder der Versicherung - entscheiden können, die Gesundheitskarte zum Lesen der

Gesundheitsdaten vorzulegen und ggf. den Zugriff auf bestimmte Daten zu beschränken. Er muß ferner frei entscheiden können, wer welche Daten in seinen Datenbestand übernehmen darf. Der Umfang der Daten, die gelesen oder übernommen werden dürften, ist außerdem durch die gesetzliche Aufgabenstellung bzw. den Vertragszweck der Nutzer beschränkt.
- Der Kartenaussteller muß sicherstellen, daß der Betroffene jederzeit vom Inhalt der Gesundheitskarte unentgeltlich Kenntnis nehmen kann.
- Der Betroffene muß jederzeit Änderungen und Löschungen der gespeicherten Daten veranlassen können.

Die Datenschutzbeauftragten des Bundes und der Länder sprechen sich dafür aus, daß der Gesetzgeber dies durch bereichsspezifische Rechtsgrundlagen sicherstellt.

Anlage 2: Beschlüsse der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 26/27.09.1994

Vorschläge zur Überprüfung der Erforderlichkeit polizeilicher Befugnisse und deren Auswirkungen für die Rechte der Betroffenen

Angesichts der aktuellen Diskussion über die innere Sicherheit weisen die Datenschutzbeauftragten des Bundes und der Länder darauf hin, daß umfangreiche polizeiliche Befugnisse zur Erhebung und Verarbeitung personenbezogener Daten, insbesondere im technischen Bereich, gesetzlich verankert worden sind.

Zum Kreis der Betroffenen zählen dabei nicht nur Personen, gegen die Verdachtsgründe vorliegen, sondern auch nichtverdächtige Kontakt- und Begleitpersonen und Unbeteiligte, deren Schutz nach Auffassung der Datenschutzbeauftragten besonders wichtig ist.

Vor diesem Hintergrund schlagen die Datenschutzbeauftragten vor, den derzeitigen Erkenntnisstand über die Erforderlichkeit polizeilicher Befugnisse zur Erhebung und Verarbeitung personenbezogenen Daten sowie ihre Auswirkungen auf die Rechte der Betroffenen durch folgende Maßnahmen zu verbessern:

1. Die Datenschutzbeauftragten teilen die von einigen Innenministern vertretene Auffassung, daß bloße Angaben über Einsatzzahlen der besonderen Befugnisse zur Datenerhebung nur einen begrenzten Aussagewert haben. Aufschluß über die tatsächliche Praxis, ihre Erforderlichkeit und Verhältnismäßigkeit läßt sich nur durch Überprüfung und Auswertung der einzelnen Einsätze gewinnen. Hierzu müssen unter Beteiligung der Datenschutzbeauftragten und der Wissenschaft, insbesondere der Kriminologie und des Polizeirechts, objektive und nachprüfbare Auswertungskriterien entwickelt werden.

   Die Datenschutzbeauftragten begrüßen daher die In - itiative für eine sog. Rechtstatsachensammlung, die Erhebungen zu polizeilichen Ermittlungsmethoden und Eingriffsbefugnissen durchführen soll. Sie schlagen vor, in diese Rechtstatsachensammlung insbesondere Angaben über den Anlaß einer Datenerhebung mit besonderen Mitteln, die Örtlichkeit und die Dauer der Maßnahme, den Umfang der überwachten Gespräche, den betroffenen Personenkreis sowie die Anzahl der ermittelten, verurteilten, aber auch der entlasteten Personen einzubeziehen. Derartige Aufstellungen wären nicht nur für elektronische Über- ,wachungsmethoden, sondern auch Observationen, den Einsatz verdeckter Ermittler und V-Personen sowie für Rasterfahndungen denkbar.

2. Einige Polizeigesetze verpflichten dazu, zu überprüfen, ob es notwendig ist, bestehende Dateien weiterzuführen oder zu ändern. Dabei soll nicht nur darauf eingegangen werden, ob die Anwendungen, d.h. die Dateien, weiterhin erforderlich sind, sondern auch auf ihren Nutzen sowie auf ihre Schwachstellen und Mängel. Ferner sind Vorschläge zu machen, wie festgestellte Defizite beseitigt oder minimiert werden können.

3. Die Datenschutzbeauftragten gehen davon aus, daß sie bei den Überlegungen zur Rechtstatsachensammlung rechtzeitig beteiligt und die jeweiligen Materialien und Zwischenergebnisse mit ihnen erörtert werden.

Fehlende bereichsspeziflsche gesetzliche Regelungen bei der Justiz

Obwohl seit dem Volkszählungsurteil des Bundesverfassungsgerichts mehr als 10 Jahre vergangen sind, werden im Bereich der Justiz sensible personenbezogene Daten nach wie vor ohne die vom Bundesverfassungsgericht geforderten bereichsspezifischen gesetzlichen Grundlagen erhoben und verarbeitet. Stattdessen sind in den letzten Jahren in zunehmendem Maße automatisierte Verfahren neu eingesetzt worden. Die Eingriffe in das Recht auf informationelle Selbstbestimmung stützen die Justizverwaltungen auf die Rechtsprechung des Bundesverfassungsgerichts zum sog. Übergangsbonus.

Die Datenschutzbeauftragten des Bundes und der Länder weisen im Hinblick.auf die kommende Legislaturperiode den Bundesgesetzgeber erneut darauf hin, daß gesetzliche Regelungen im Bereich der Justiz überfällig sind. Dabei ist nicht die jeweils geübte Praxis zu legalisieren, sondern es muß vorab unter datenschutzrechtlichen Gesichtspunkten geprüft werden, welche Form der Datenerhebung und -verarbeitung in welchem Umfang erforderlich ist. Der zur Zeit dem Bundesrat vorliegende Entwurf eines Strafverfahrensänderungsgesetzes beispielsweise wird datenschutzrechtlichen Anforderungen in keiner Weise gerecht.

Im Bereich der Justiz fehlen ausreichende gesetzliche Regelungen für die

- Datenverarbeitung im Strafverfahren, insbesondere in automatisierten Dateien,
- Datenerhebung, -verarbeitung und -nutzung im Strafvollzug
- Übermittlung von Daten aus den bei Gerichten geführten Registern (z.B. Grundbuch) und deren Nutzung durch die Empfänger,
- Datenübermittlung von Amts wegen durch Gerichte und Staatsanwaltschaften an Gerichte, Behörden und sonstige öffentliche Stellen (Justizmitteilungsgesetz)
- Aufbewahrung von Akten, Karteien und sonstigen Unterlagen sowie die Dauer der Speicherung in automatisierten Dateien.

Eine Berufung auf den sog. Übergangsbonus auf unbegrenzte Zeit steht nicht in Übereinstimmung mit der Rechtsprechung des Bundesverfassungsgerichts. Die Datenschutzbeauftragten halten es deshalb zum Schutz des Rechts des Einzelnen auf informationelle Selbstbestimmung für geboten, wegen der mit der Datenerhebung, Verarbeitung und Nutzung verbundenen Rechts-eingriffe in der neuen Legislaturperiode unverzüglich bereichsspezifische Regelungen der materiellen Voraussetzungen sowie der organisatorischen und verfahrensrechtlichen Vorkehrungen zu schaffen, welche der Gefahr einer Verletzung des Persönlichkeitsrechtes des Bürgers entgegenwirken.

Datenschutzrechtliche Anforderungen an ein Übereinkommen der Mitgliedstaaten der Europäischen Union über die Errichtung eines europäischen Polizeiamtes (Europol)

Die Datenschutzbeauftragten der Länder gehen gemeinsam mit dem Bundesdatenschutzbeauftragten davon aus, daß bei den Verhandlungen mindestens folgende Punkte berücksichtigt werden:

- Das Übereinkommen muß der verfassungsrechtlichen Kompetenzverteilung in Bund und Ländern für die Polizei entsprechen. Die materielle Verantwortung für die Datenverarbeitung muß, soweit die Daten von Landesbehörden erhoben worden sind, weiterhin bei den Ländern liegen. Davon bleiben die Zuständigkeiten und die dazugehörigen Befugnisse des BKA als nationale Stelle für den Informationsverkehr mit EUROPOL unberührt.
- Die Regelungen zur Verarbeitung personenbezogener Daten müssen präzise sein und dem Grundsatz der Verhältnismäßigkeit entsprechen. Beispielweise erfüllen die in den bisherigen Entwürfen vorgesehenen Befugnisse zur europaweiten Speicherung von Daten unbeteiligter Personen diese Voraussetzungen nicht.

Die Datenschutzbeauftragten erwarten, daß die deutsche Seite eine Klarstellung über die Verantwortung der Länder, zum Beispiel durch eine Protokollerklärung zum EUROPOL-Übereinkommen, trifft.

Art. 12 Verbrechensbekämpfungsgesetz zur Trennung von Polizei und Nachrichtendiensten

Geheimdienstliche Informationsmacht und polizeiliche Exekutivbefugnisse müssen strikt getrennt bleiben. Die Datenschutzbeauftragten des Bundes und der Länder stellen mit Besorgnis Entwicklungen fest, die die klare Trennungslinie zwischen Nachrichtendiensten und Pohzeibehörden weiter zu verwischen drohen. Die betrifft vor allem den Einsatz des Bundesnachrichtendienstes nach dem Verbrechensbekämpfungsgesetz:

- Der BND erhält danach bei der Fernmeldeaufklärung auch Befugnisse, die auf eine gezielte Erhebung von Daten für polizeiliche Zwecke hinauslaufen können. Deshalb ist bei dem Vollzug des Gesetzes darauf zu achten, daß nicht gezielt Informationen gesammelt werden, die vom Auftrag des BND nicht umfaßt werden.
- Zwischen nachrichtendienstlichen Vorfelderkenntnissen und polizeilichen Zwangsmaßnahmen ist ein Filter erforderlich, der vor allem Unbeteiligte vor überzogenen Belastungen schützt.

Die Datenschutzbeauftragten fordern, für die Zusammenarbeit von Nachrichtendiensten und Polizei in der Durchführung und Gesetzgebung des Trennungsgebot strikt zu beachten. Dies gilt auch bei der Fernmeldeaufklärung des BND. Eine wirksame Kontrolle durch den Datenschutzbeauftragten in diesem sensiblen Bereich ist auch nach der Rechtsprechung des Bundesverfassungsgericht sicherzustellen.

Geänderter Vorschlag für eine Europäische Richtlinie zum Datenschutz im ISDN und in Mobilfunknet-zen vom 13. Juni 1994 (KOM (94)128 endg. - COD 288)

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder begrüßt es, daß die Europäische Kommission mit der Vorlage des geänderten Vorschlags für eine Richtlinie zum Datenschutz im ISDN ihre Absicht bekräftigt hat, unionsweit bereichsspezifische Regelungen für den Datenschutz in Telekommunikationsnetzen zu schaffen. Es kann kein Zweifel daran bestehen, daß die digitalen Telekommunikationsnetze in der Europäischen Union die rechtlichen und technischen Voraussetzungen für die Liberalisierung der Telekommunikationsmärkte in weiten Bereichen bereits geschaffen haben und mehrere Mitgliedsstaaten, darunter Deutschland, derzeit ihr nationales Telekommunikationsrecht auf die Vorgaben der EU umstellen.

Aus diesem Grund sollte der geänderte Vorschlag für eine ISDN-Richtlinie so bald wie möglich vom Ministerrat und vom Europäischen Parlament abschließend beraten werden. Die Bundesregierung sollte die deutsche Ratspräsidentschaft dazu nutzen, den geänderten Vorschlag für eine ISDN-Richtlinie im Rat behandeln zu lassen.

Dabei sollte sich die Bundesregierung insbesondere für folgende Verbesserungen des Richtlinienvorschlags aus datenschutzrechtlicher Sicht einsetzen:

1. Für Telekommunikationsorganisationen und Diensteanbieter müssen die gleichen gemeinschaftsrechtlichen Regelungen zum Datenschutz gelten. Die Verarbeitung personenbezogener Daten durch Diensteanbieter darf nicht privilegiert werden.

2. Die Beschränkung der Datenverarbeitung auf Zwecke der Telekommunikation sollte wieder in die Richtlinie aufgenommen werden. Der allgemeine Zweckbindungsgrundsatz der Datenschutzrichtlinie läßt die Zweckentfremdung schon bei ,,berechtigten Interessen" der Verarbeiter zu. Das ist angesichts zunehmender Diversifizierung der Aktivitäten von Netzbetreibern und Diensteanbietern eine zu weitgehende Lockerung der Zweckbindung im Telekommunikationsbereich.

3. Das ursprünglich vorgesehene Verbot, personenbezogene Däten zur Erstellung von elektronischen Profilen der Teilnehmer zu nutzen, sollte wieder in die Richtlinie aufgenommen werden.

4. Die Speicherung von Inhaltsdaten nach Beendigung der Übertragung sollte - wie im ursprünglichen Richtlinienentwurf vorgesehen - untersagt werden.

5. Die Vertraulichkeit der Kommunikationsbeziehungen und -inhalte (Fernmeldegeheimnis) sollte - wie es der ursprüngliche Richtlinienvorschlag ebenfalls vorsah - auf Unionsebene garantiert werden.

6. Um eine Harmonisierung des Gemeinschaftsrechts beim Einzelgebührennachweis zu erreichen, sollten konkrete Vorgaben in die Richtlinien aufgenommen werden, z.B. indem den angerufenen Teilnehmern die Aufnahme ihrer Rufnummer in Einzelgebührennachweise freigestellt wird.

7. Im Fall der Anrufweiterschaltung sollte die automatische Information des anrufenden Teilnehmers darüber, daß sein Anruf (z.B. bei einem Arzt) an einen Dritten weitergeschaltet wird, gewährleistet sein.

Die Konferenz begrüßt die im geänderten Vorschlag vorgesehene Kostenfreiheit für die verschiedenen Optionen der Anzeige der Rufnummer des Anrufers und für die Nichtaufnahme von Daten in das Teilnehmerverzeichnis (Telefonbuch).

Diese Vorschläge berücksichtigen das Subsidiaritätsprinzip und beschränken sich auf Änderungen, die zur Gewährleistung der Vertraulichkeit der Kommunikation in der Europäischen Union realisiert werden müssen. Zudem wird die Europäische Union insoweit im Rahmen ihrer ausschließlichen Zuständigkeit tätig. Die Konferenz bittet auch die Entscheidungsträger auf Unionsebene sowie die Datenschutzbehörden der anderen Mitgliedsstaaten diese Anregungen zu unterstützen.

Anlage 3: Kriterienkatalog des AK-Technik vom 22.06.1994 Datenschutzrechtliche Anforderungen an automatisierte Verfahren zur Erhebung von Straßen-benutzungsgebühren (road-pricing-Systeme)

Automatisierte Systeme zur Erhebung von Straßenbenutzungsgebühren können das Recht auf informationelle Selbstbestimmung der Straßenbenutzer beeinträchtigen. Die Verwendung der für die Gebührenabrechnung erhobenen Daten für andere Zwecke würde den Datenschutz beeinträchtigen. Zu befürchten ist insbesondere, daß im Rahmen derartiger Verfahren erhobene personenbezogene Daten zur Erstellung von Bewegungsprofilen genutzt werden könnten. Schließlich würde auch eine Verpflichtung des Straßenbenutzers zu einem lückenlosen Nachweis seiner Bewegungen eine unverhältnismäßige Belastung des Betroffenen bedeuten.

Die Datenschutzbeauftragten des Bundes und der Länder begrüßen es, daß bei dem Feldversuch auf der A 555 auch datenschutzrechtliche Erfordernisse berücksichtigt werden sollen. Sie sind bereit, Vorschläge für eine datenschutzgerechte Gestaltung der Technik, der Organisation und der rechtlichen Rahmenbedingungen in die Entscheidungsfindung einzubringen. Sie gehen davon aus, daß diese Vorschläge in den vor dem Echteinsatz derartiger Systeme notwendigen Abwägungsprozeß (Technik-folgen-Abschätzung) eingehen und zu einer datenschutzfreundlichen Systemgestaltung beitragen. Nur Verfahren mit geringstmöglichem Eingriff in das allgemeine Persönlichkeitsrecht sollten zum Einsatz kommen, d.h. Systeme, bei denen möglichst wenig personenbezogene Daten erhoben werden.

Aus diesen Überlegungen ergeben sich die folgenden datenschutzrechtlichen Anforderungen:

1. Anonymität

Der Grundsatz der ,,datenfreien Fahrt" muß auch künftig gewährleistet sein. Je weniger personenbezogene oder personenbeziehbare Daten erhoben, verarbeitet oder genutzt werden, desto geringer ist auch die Gefahr einer mißbräuchlichen Datennutzung. Aus diesem Grund ist das Anonymitätskriterium die wichtigste Datenschutzanforderung. Jedenfalls sollten bei regelgerechter Straßenbenutzung keine personenbezogenen Daten entstehen. Das bedeutet, daß auch keine Angaben erhoben oder verarbeitet werden, die im Nachhinein die Herstellung des Personenbezugs ermöglichen.

Grundsätzlich bieten Verfahren, bei denen Gebühren im voraus entrichtet werden (Prepaid-Verfahren) bessere Voraussetzungen für die Wahrung der Anonymität als solche Systeme, bei denen zunächst Verkehrsdaten erhoben und dann den Benutzern in Rechnung gestellt bzw. von deren Konten abgebucht werden (Postpaid-Verfahren).

Soweit die Speicherung von Benutzerdaten gleichwohl erforderlich ist (z.B. für den Nachweis der Richtigkeit der

Gebührenerhebung), sollten diese Daten dezentral beim Benutzer gespeichert werden. Die Erhebung von Benutzerdaten im Regelbetrieb durch ,,Erhebungsstellen" und deren Übermittlung an Konzentratoren oder zentrale Abrechnungseinheiten sollte unterbleiben.

Die Überwachung der Gebührenerhebung sollte so gestaltet werden, daß die Identität des Benutzers nur dann aufgedeckt wird, wenn ein begründeter Mißbrauchsverdacht besteht. Die Überwachung, ob ein Mißbrauch vorliegt, sollte grundsätzlich nur stichprobenweise und nicht vollständig erfolgen, da Systeme mit flächendeckender Mißbrauchskontrolle eine Infrastruktur voraussetzen, die für eine vollständige Erfassung auch der regelgerechten Straßenbenutzung ,,zweckentfremdet" werden könnte. Dabei sollte die Kontrolldichte so gering wie möglich sein und könnte sich an der bisherigen Kontrollpraxis bezüglich der Einhaltung von Geschwindigkeitsbegrenzungen orientieren.

2. Vertraulichkeit

Sofern personenbezogene Daten erhoben werden, müssen sie vertraulich behandelt werden. Die unbefugte Kenntnisnahme durch Dritte ist durch technische und organisatorische Maßnahmen auszuschließen. Insbesondere ist folgendes zu gewährleisten:

- Alle Komponenten, die sicherheitsrelevante Informationen austauschen, müssen sich partnerweise gegenseitig authentifizieren.
- Die Identität eines Straßenbenutzers sollte nur bei Mißbrauchsverdacht und nur vom Systembetreiber aufgedeckt werden können.
- Daten, die Aufschluß über die Identität oder den Aufenthaltsort des Benutzers geben, sind durch kryptographische Verfahren gegen eine unbefugte Kenntnisnahme zu sichern.
- Bei dezentraler Datenspeicherung (z.B. auf einer Chip-Karte) darf der Zugang nur nach Eingabe eines benutzerspezifischen Codes möglich sein.
- Soweit personenbezogene Daten bei vermutetem Mißbrauch zentral gespeichert werden, ist zu gewährleisten, daß die Daten von anderen vom Systembetreiber verarbeiteten Daten strikt abgeschottet werden und nach Rechnungbegleichung, bzw. wenn ein Mißbrauch nicht nachgewiesen werden kann, unverzüglich gelöscht werden.
- Die Vertraulichkeit im Verhältnis Fahrzeughalter - Fanrzeugbenutzer muß gewahrt werden (benutzer-statt fahrzeuggebundene Erhebung).

3. Integrität

Es ist zu gewährleisten, daß die richtigen Daten jeweils den richtigen Benutzern zugeordnet werden und keine Über-, Unter- oder Doppelerfassung erfolgt. Der Abbuchungsimpuls darf nicht derart streuen, daß er etwa -z.B. beim Spurwechsel - andere Fahrzeuge erfaßt. Auch bei der Fahrzeug- bzw. Benutzeridentifizierung (z.B. durch Kennzeichenerfassung) im Falle vermuteten Mißbrauchs ist die Zuordnung zu den richtigen Fahrzeugen sicherzustellen.

Alle sicherheitsrelevanten Informationen sind mit geeigneten Verfahren gegen Manipulationen zu schützen.

4. Transparenz

Das gesamte Verfahren muß für die Teilnehmer durchschaubar sein, d.h. die Benutzer müssen die realistische Chance haben, sowohl über den generellen Ablauf als auch über die Datenerhebung und -speicherung im Einzelfall Bescheid zu wissen:

- Bei dezentraler Speicherung sollte der Benutzer nachvollziehen können, welche Entgelte wann wo abgebucht wurden.
- Das System sollte den Benutzer rechtzeitig darauf hinweisen, wenn das Guthaben erschöpft oder für die Abbuchung der Maut zu gering ist.
- Sofern im Rahmen von Überwachungsmaßnahmen eine Aufdeckung der ansonsten geheimen Fahrzeug-identität erfolgt, muß dies für den Fahrzeugbenutzer erkennbar sein.
- Abbuchungen, Funktionsstörungen und Manipulationsversuche müssen dem Benutzer angezeigt werden und sind dezentral (z.B. auf der Chipkarte) revisionssicher zu protokollieren. Über Zusatzeinrichtungen, etwa bei Tankstellen, sollte der Benutzer die Möglichkeit haben, den Speicherinhalt der Protokolldatei auszudrucken und die Buchungsdatensätze anschließend zu löschen.

5. Stabilität gegen die Rücknahme von Datenschutzmaßnahmen

Die Systemkomponenten sind so zu gestalten, daß die Datenschutz- und Datensicherungsfunktionen stabil sind und nicht einseitig durch den Systembetreiber oder durch Dritte zurückgenommen oder unterlaufen werden können. Alle zum Einsatz kommenden Geräte müssen der Qualitätssicherungsnorm ISO 9001 genügen.

Systeme, die eine generelle Videoüberwachung des fließenden Verkehrs voraussetzen, werden abgelehnt, weil sie sich bei nur geringen Modifikationen auf eine Vollkontrolle umstellen lassen