Bayerischer Landtag
11. Wahlperiode

Drucksache **11/14417**

14. 12. 89

Elfter Tätigkeitsbericht des Landesbeauftragten für den Datenschutz

Berichtszeitraum 1989

Der Landesbeauftragte für den Datenschutz
Nr. DSB/1 – 510 – 12

München, 14. Dezember 1989

An den
Herrn Präsidenten
des Bayerischen Landtags
München

Elfter Bericht über die Tätigkeit des Landesbeauftragten für den Datenschutz

Sehr geehrter Herr Landtagspräsident!

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

Mit vorzüglicher Hochachtung

Sebastian Oberhauser

Inhaltsübersicht

1. Vorbemerkung

1.1 Kontrolltätigkeit

Auch im Berichtszeitraum 1989 lag der Schwerpunkt meiner Tätigkeit bei der Kontrolle bayerischer Behörden. Zahlreiche zum Teil mehrtägige Kontrollen der Rechtmäßigkeit der Datenverarbeitung habe ich durchgeführt: bei vier Gesundheitsämtern, zwei Landesuntersuchungsämtern für das Gesundheitswesen, der Bayerischen Versicherungskammer, acht Betriebskrankenkassen, einem Finanzamt, einem Landwirtschaftsamt, zwei Landratsämtern, einer Regierung, sechs Kommunen, bei Stadtwerken, zwei Gymnasien, einem Amtsgericht, einer Staatsanwaltschaft, einer Kabelgesellschaft, einer Industrie- und Handelskammer, im Bereich von vier Polizeipräsidien bei sieben Polizeidirektionen, bei der Grenzpolizei, beim Landeskriminalamt, beim Polizeipräsidium München und beim Landesamt für Verfassungsschutz.

Ergänzt wurden die allgemeinen Kontrollen durch zahlreiche Überprüfungen bei Behörden aufgrund von Eingaben und Beschwerden von Bürgern.

Hinzu kommen technisch-organisatorische Kontrollen bei siebzehn Rechenzentren und Betreibern von kleineren Datenverarbeitungsanlagen.

1.2 Datenschutz in Bayern gewährleistet

Als erfreuliches Ergebnis meiner Kontrollen im Jahr 1989 kann ich feststellen, daß der Datenschutz in Bayern grundsätzlich gewährleistet ist.

Bei allen bayerischen Behörden habe ich große Bereitschaft zur Zusammenarbeit und zur Einhaltung des Datenschutzes angetroffen. Soweit Mängel und Fehler festzustellen waren, waren diese nicht auf vorsätzliche Verstöße, sondern auf menschliche Unzulänglichkeit zurückzuführen. Gerade die Fülle bereichsspezifischer detaillierter Regelungen macht es manchen Behörden nicht leichter, jeweils alle diese Bestimmungen in der täglichen Praxis zu überblicken und zu beachten.

1.3 Inhalt und Schwerpunkt des 11. Tätigkeitsberichts

Dieser Bericht kann aus Platzgründen nur eine Auswahl aus meiner Tätigkeit im Berichtszeitraum sein.

- Den Schwerpunkt des Berichts bilden die Ergebnisse der durchgeführten **Datenschutzkontrollen**. Im Vordergrund steht wieder die Datenverarbeitung im **Sicherheitsbereich**.
- Die Kontrolle bei den **Gesundheitsämtern** habe ich fortgesetzt und auf die Landesuntersuchungsämter ausgedehnt. Bei diesen Behörden werden besonders sensible Daten der Bürger verarbeitet.
- Fortgesetzt habe ich die Kontrolle der **Einwohnermeldeämter**, die besonders viele persönliche Daten speichern und als Informationszentralen über die Bürger an zahlreiche Behörden regelmäßig Daten liefern. Um so wichtiger ist die Einhaltung des Datenschutzes beim Einwohnermeldeamt, vor allem die Anwendung zuverlässiger Datenverarbeitungsprogramme.
- Ausgeweitet habe ich meine Kontrolltätigkeit auf den Bereich der Wirtschafts- und Landwirtschaftsverwaltung sowie der Bayerischen Versicherungskammer.
- Zu den gesetzlichen Schranken der **Genomanalyse** beim Menschen habe ich meine Vorstellungen präzisiert.
- Im **Medienbereich** fortgesetzt wurde die Diskussion um die Berücksichtigung des Persönlichkeitsrechts bei der Speicherung von Bürgerdaten in den **Mediendatenbanken**. Die notwendige Vorverlagerung des Datenschutzes macht die Rückführung des Medienprivilegs auf seinen Kern unumgänglich. Hierzu habe ich im Rahmen der Novellierung des Bundesdatenschutzgesetzes einen Vorschlag für eine gesetzliche Regelung vorgelegt.

1.4 Neufassung des Bundesdatenschutzgesetzes

Die Bundesregierung hat einen **Gesetzentwurf zur Fortentwicklung der Datenverarbeitung und des Datenschutzes** im Bundestag eingebracht (BT-Drucks. 11/4306). Teil des Entwurfs ist die Neufassung des Bundesdatenschutzgesetzes. Für die Beratungen im Bundesrat habe ich gegenüber dem Staatsministerium des Innern Stellung genommen. Außerdem habe ich an den Beratungen von Arbeitsgruppen der Bundestagsfraktionen von CDU/CSU und SPD sowie an der Anhörung des Innenausschusses des Deutschen Bundestages teilgenommen.

Die **Konzeption** des Gesetzentwurfs, den Schutz der Daten in Dateien und in Akten unterschiedlich auszugestalten und damit je nach Speicherungsart und Nutzungsmöglichkeit der unterschiedlichen Gefährdung der Daten Rechnung zu tragen, halte ich für sachgerecht und angemessen.

Zu einigen Punkten habe ich allerdings noch weitere **Verbesserungen** gefordert:

- Der Begriff der **„Datei"**, der für die Anwendbarkeit des Bundesdatenschutzgesetzes von zentraler Bedeutung ist, muß so erweitert werden, daß er die moderne Entwicklung der Datentechnik berücksichtigt: Als „Datei" sollte jede Sammlung personenbezogener Daten gelten, die **automatisiert ausgewertet** werden kann. Der Grund für die erhöhte Schutzbedürftigkeit von Daten, die in Dateien gespeichert sind, ist die erhöhte Verfügbarkeit, Auswertbarkeit und Nutzbarkeit von Daten in Computern und das damit verbundene erhöhte Risiko fehlerhafter Datenverarbeitung. Für diese Gefährdung ist ohne Belang, ob und wie die Datensammlung im Computer geordnet ist und ob sie umgeordnet werden kann. Entscheidend kommt es darauf an, ob der Datenbestand automationsunterstützt ausgewertet werden kann, so daß die Informationen schneller und auch kostengünstiger zur Verfügung stehen als bei herkömmlicher Datenverarbeitung in Akten. Da immer größere Datenmengen gespeichert werden können und inzwischen auch ganze Dokumente (Briefe, Rechnungen, Fotos, Graphiken oder umfangreiche Akten) als elektronische Faksimiles aufgenommen werden, kann es für den Dateibegriff nicht mehr auf die Art der Anordnung von Daten in Computern, sondern nur noch auf die automatisierte Auswertungsmöglichkeit ankommen. Würde der bisherige enge Dateibegriff fortgeschrieben, so wären Volltextspeicherungen, wie sie zunehmend eingesetzt werden, nicht oder nicht in vollem Umfang vom Gesetz erfaßt und damit auch möglicherweise der Kontrolle des Datenschutzbeauftragten entzogen. Der erweiterte Dateibegriff bedeutet gleichzeitig eine Erweiterung der Kontrollkompetenzen des Datenschutzbeauftragten.

Daten, die in der Bürokommunikation zwischen automatischer und manueller Bearbeitung **wechseln** können, sollten ebenfalls eindeutig unter das Bundesdatenschutzgesetz fallen.

- Die sogenannten **Internen Dateien**, d. h. Karteien, die manuell geführt werden und aus denen keine Daten an Dritte übermittelt werden, sind bisher von der Geltung des Bundesdatenschutzgesetzes weitgehend ausgenommen. Da sie aber die darin enthaltenen Daten gegenüber bloßer Aktenverarbeitung einem erhöhten Zugriffs- und Nutzungsrisiko aussetzen, müssen die Vorschriften über die Berichtigung, Sperrung, Löschung und Kontrolle durch den Datenschutzbeauftragten zumindest für interne Dateien von Behörden anwendbar sein.

- Der **funktionale Behördenbegriff**, der im Bayerischen Datenschutzgesetz gilt mit der Folge, daß die Datenweitergabe auch innerhalb der gleichen Behörde an Sachgebiete, die andere Aufgaben bearbeiten, nur bei Erforderlichkeit zulässig ist, sollte im Bundesdatenschutzgesetz eingeführt werden.

- Wird der Verwendungszweck gespeicherter Daten später verändert, so sollte dem Betroffenen durch eine **Benachrichtigung** hierüber die Chance einer sofortigen Richtigstellung falscher Daten gegeben werden. Da das Gesetz den Behörden in weitem Umfang erlaubt, Daten anstatt beim Betroffenen bei anderen öffentlichen Stellen zu beschaffen, sollte der Betroffene wissen, für welchen neuen Zweck seine Daten Verwendung finden sollen. Nur dann kann er rechtzeitig darauf hinweisen, daß die übermittelten Daten in dem neuen Verwendungszusammenhang zu falschen Beurteilungen oder Entscheidungen führen können. Eine Benachrichtigung des Betroffenen sollte nur dann unterbleiben, wenn die Besonderheiten der neuen Verwaltungsaufgabe oder unverhältnismäßiger Aufwand entgegenstehen.

- Nach der bewährten bayerischen Regelung sollte vor dem Einsatz eines neuen automatisierten Verfahrens eine gesonderte datenschutzrechtliche **Freigabe** durch die oberste Dienstbehörde vorgesehen werden. Damit soll von vornherein ein höherer Grad an Datenschutz erreicht werden. Von der Freigabe sollte der Bundesdatenschutzbeauftragte unterrichtet werden.

- Interessenkonflikte zwischen **Forschung und Datenschutz** sollten nicht von den Forschern, sondern von einer neutralen Instanz entschieden werden. Der Gesetzentwurf sieht vor, daß öffentliche Stellen personenbezogene Daten an Forscher u.a. dann übermitteln dürfen, wenn das öffentliche Interesse an der Forschungsarbeit das schutzwürdige Interesse des Betroffenen erheblich überwiegt. Da die Übermittlung sensibler Daten zu erheblichen Belastungen des Betroffenen führen kann, gleichwohl aber aus der Sicht der Forscher und der das Projekt finanzierenden Stelle das öffentliche Interesse an der Forschung in aller Regel erheblich stärker als das schutzwürdige Interesse des Betroffenen eingeschätzt wird, sollte die Entscheidung, welches Interesse überwiegt, einer neutralen streitentscheidenden Instanz übertragen werden.

- Das **Recht des Betroffenen auf Auskunft** über gespeicherte Daten und auf Begründung der Auskunftsverweigerung ist bei bestimmten Behörden, z.B. den Sicherheitsbehörden ausgeschlossen. Dies kann — wenn überhaupt — im Hinblick auf die Grundrechte auf informationelle Selbstbestimmung (Art. 2 i.V.m. Art. 1 GG) auf gerichtliche Nachprüfung (Art. 19 Abs. 4 GG) nur hingenommen werden, wenn der Betroffene schriftlich auf die Möglichkeit hingewiesen wird, über den Bundesbeauftragten eine Nachprüfung der Datenverarbeitung zu erreichen.

- Die Kontrolle der Verarbeitung von Daten, die einem besonderen **Berufs- oder Amtsgeheimnis**, z.B. dem Steuergeheimnis oder der ärztlichen Schweigepflicht, unterliegen, muß **auch ohne Einwilligung des Betroffenen** möglich sein. Andernfalls wäre eine wirksame Datenschutzkontrolle durch den Bundesbeauftragten zu Lasten der Bürger in nicht hinnehmbarer Weise erschwert bzw. unmöglich. Das Steuergeheimnis ist nicht zum Schutz des Finanzamts, sondern zum Schutz der Bürger da.

- Das nur für den Bundesdatenschutzbeauftragten vorgesehene **Zeugnisverweigerungsrecht** sollte auch zugunsten der Landesbeauftragten für den Datenschutz eingeführt werden.

- Im Bereich der Medien sollte der Persönlichkeitsschutz verbessert und das sog. **Medienprivileg** (weitgehender Ausschluß des Datenschutzes) auf den Kern der Pressefreiheit zurückgeführt werden (siehe unter 21).

1.5 Änderung des Bayerischen Datenschutzgesetzes

Die Rechtsprechung des Bundesverfassungsgerichts und die Erfahrungen beim Gesetzesvollzug machen auch eine Novellierung des Bayerischen Datenschutzgesetzes erforderlich. Im Interesse der Einheitlichkeit des allgemeinen Datenschutzrechts in der Bundesrepublik Deutschland sollte jedoch die Novellierung des Bundesdatenschutzgesetzes abgewartet werden.

1.6 Gesetzentwurf der SPD-Fraktion zur Änderung der Rechtsstellung des Landesbeauftragten für den Datenschutz

Die SPD-Fraktion des Bayerischen Landtags hatte 1988 den Entwurf eines Gesetzes zur Änderung des Bayerischen Datenschutzgesetzes eingereicht. Ziele des Entwurfs waren die Stärkung der Unabhängigkeit des Landesbeauftragten für den Datenschutz und die stärkere Mitwirkung des Landtags bei seiner Bestellung und Überwachung. Hierzu sollte der Landesbeauftragte als oberste Landesbehörde, eingerichtet werden. Er sollte von einer 2/3-Mehrheit des Landtags auf Zeit gewählt werden und der Rechtsaufsicht des Landtagspräsidenten unterstehen.

Der Landtag hat den Entwurf wegen verfassungsrechtlicher Bedenken abgelehnt. Nach meiner Auffassung würde der Vorschlag die Unabhängigkeit des Landesbeauftragten nicht stärken, sondern insgesamt eher schwächen. Seine Unabhängigkeit ist gegenwärtig durch das Datenschutzgesetz und das Beamtengesetz gesichert. Er ist Beamter auf Lebenszeit, weisungsunabhängig und unterliegt nur einer Dienstaufsicht. Diese ist auf dienstliche Fragen beschränkt und umfaßt nicht die Aufsicht über die rechtliche und fachliche Amtsführung.

1.7 Datenschutz in Europa

Der für 1992 angestrebte EG-Binnenmarkt wird neben einem verstärkten Warenverkehr auch zu einem vermehrten Austausch von personenbezogenen Daten über die EG-Bürger führen. Die dynamische Entwicklung der Telekommunikation beschleunigt diesen Trend zu einem **europaweiten Datenaustausch**. Dies wirft für die Zukunft neue Datenschutz-Probleme auf. Hinzu kommt, daß noch kein EG-weiter, dem deutschen Datenschutzrecht vergleichbarer Datenschutz-Standard besteht und einige EG-Länder überhaupt noch kein Datenschutzgesetz besitzen. Deshalb haben die Datenschutzbeauftragten der EG-Länder anläßlich der 11. Internationalen Konferenz der Datenschutzbeauftragten folgende Forderungen erhoben:

- Durch entsprechende Rechtsakte der Europäischen Gemeinschaft sollten die Grundsätze der **Europaratskonvention 108** für alle Mitgliedstaaten ebenso wie für die Institutionen der EG selbst verbindlich gemacht werden.

- Eine unabhängige **Datenschutzkontrollinstanz** sollte eingerichtet werden. Sie sollte die Einrichtungen der EG in allen Datenschutzfragen beraten, die Verarbeitung personenbezogener Daten innerhalb der Einrichtungen der EG kontrollieren, Eingaben von Betroffenen entgegennehmen und mit den nationalen Datenschutzorganen zusammenarbeiten.

1.8 Ausblick

Auch im Jahr 1990 werde ich mein besonderes Augenmerk neben dem **Sicherheitsbereich** auf die Einhaltung des Datenschutzes im **Gesundheitsbereich** richten. Hierzu werde ich auch bei einigen Krankenhäusern Kontrollen durchführen.

In der Gesetzgebung erwarte ich nach der Vorlage des Gesetzentwurfs zur Novellierung des Verfassungsschutzgesetzes noch den Entwurf einer **Novelle zum Polizeiaufgabengesetz**, mit der die Datenverarbeitung der Polizei eine tragfähige Rechtsgrundlage erhalten soll. Bei beiden Vorhaben werde ich mich dafür einsetzen, daß neben der inneren Sicherheit die Persönlichkeitsrechte der Bürger gewahrt bleiben.

Das Bundesverfassungsgericht hat in den letzten Jahren die Bedeutung der Datenschutzbeauftragten für die Gewährleistung des informationellen Selbstbestimmungsrechts der Bürger wiederholt besonders hervorgehoben. Diese Bedeutung nimmt durch den sprunghaften Anstieg der automatisierten Datenverarbeitung ständig weiter zu. Für den Bürger selbst wird es damit schwieriger, sich einen Überblick darüber zu verschaffen, wer welche Daten wo über ihn gespeichert hat und wer welche Daten an welche Stellen weitergibt. Hinzu kommt, daß die Forderung des Bundesverfassungsgerichts nach bereichsspezifischen detaillierten gesetzlichen Regelungen für Eingriffe in das informationelle Selbstbestimmungsrecht zu einer Fülle von Detailregelungen geführt hat und noch weiter führen wird. Die wirksame Kontrolle der Behörden und die im Zug der Rechtsprechung des Bundesverfassungsgerichts gebotene Ausweitung der Kompetenzen des Datenschutzbeauftragten werden in den nächsten Jahren die angemessene **Ausweitung meiner Geschäftsstelle** unumgänglich machen.

2. Gesundheit

2.1 AIDS

Wie schon im Vorjahr habe ich bei meinen Kontrollen besonders auf den Schutz von Daten geachtet, die im Zusammenhang mit AIDS erhoben werden. So wurde in vier Gesundheitsämtern die Abwicklung der **anonymen HIV-Tests** eingehend kontrolliert. Bei den Landesuntersuchungsämtern für das Gesundheitswesen, welche die HIV-Proben untersuchen, habe ich die datenschutzrechtliche Gegenprobe durchgeführt. Als Ergebnis kann ich feststellen, daß sich keinerlei Zweifel an der Anonymität des Verfahrens ergeben haben. Die verwaltungsmäßige Abwicklung der Tests bei den Gesundheitsämtern wurde aufgrund von Empfehlungen aus meinen Prüfungen verbessert. Die Blutproben werden nunmehr von den Gesundheitsämtern **in jedem Fall anonym** an die Landesuntersuchungsämter gesandt, und zwar auch dann, wenn es sich um nichtanonyme AIDS-Tests, wie z. B. bei der Beamteneinstellung, handelt. Im einzelnen siehe unter 2.3. Zu HIV-Speicherungen bei der Polizei siehe unter 5.5.3.

Die im folgenden geschilderten beiden Vorgänge sind über den Einzelfall hinaus von Interesse:

2.1.1 Bekanntgabe von HIV-Testergebnissen am Telefon

In Presseberichten und in einer Eingabe wurde behauptet, Mitarbeiter eines Gesundheitsamtes hätten mehreren Personen, die sich im Rahmen einer Einstellungsuntersuchung freiwillig anonym auf HIV testen ließen, auf deren Anruf das Testergebnis telefonisch mitgeteilt. Die untersuchten Personen hätten am Telefon nicht die ihnen zugeteilte Kenn-Nummer, sondern nur ihren Namen angegeben. Damit war der Vorwurf zu klären, das Gesundheitsamt habe das Datengeheimnis der untersuchten Personen gefährdet, weil die bloße Namensnennung am Telefon kein ausreichender Identitätsnachweis ist.

Bei meinen Ermittlungen im Gesundheitsamt haben sich keine Nachweise dafür ergeben, daß die HIV-Testergebnisse überhaupt auf telefonische Anfrage hin mitgeteilt worden seien. Die Akten des Gesundheitsamtes gaben keinen Anhaltspunkt für eine telefonische Bekanntgabe. Nach Weisung des Leiters des Gesundheitsamtes ist den Mitarbeitern untersagt, am Telefon Auskünfte über das Ergebnis eines HIV-Tests zu erteilen, und zwar unabhängig davon, ob unter Codewort oder Name angefragt wird. Die für die Abwicklung des HIV-Tests zuständigen Mitarbeiter haben sowohl gegenüber dem Leiter des Gesundheitsamtes als auch bei der Datenschutzkontrolle versichert, sie hätten in keinem Fall Betroffenen telefonisch Auskunft über das Ergebnis des HIV-Tests gegeben.

Ein Nachweis für die Behauptungen in der Presse und in der Eingabe konnte trotz Ausschöpfung aller mir nach dem Datenschutzgesetz zur Verfügung stehenden Möglichkeiten nicht erbracht werden.

2.1.2 Meldung von Therapieabbrechern an Gesundheitsamt

Nach dem Bundesseuchengesetz (BSeuchG) ist AIDS eine übertragbare Krankheit (Bekanntmachung des Staatsministeriums des Innern vom 17.5.1987). Intravenös Drogenabhängige gelten als HIV-ansteckungsverdächtig. Vor diesem Hintergrund bat eine Therapieeinrichtung um Prüfung der Frage, ob intravenös Drogenabhängige, welche die Therapie

vorzeitig abbrechen, auf Anforderung dem Gesundheitsamt gemeldet werden dürfen.

Ich habe die Auffassung vertreten, daß eine **namentliche Meldung** der Drogenabhängigen an das Gesundheitsamt nicht zu beanstanden wäre. Hier stehen sich die ärztliche Schweigepflicht nach § 203 StGB und die gesetzliche Verpflichtung gegenüber, dem Gesundheitsamt im Rahmen seiner Ermittlungen nach dem Bundesseuchengesetz die erforderlichen Auskünfte zu geben.

Die Tatsache, daß ein Betroffener intravenös drogenabhängig ist, stellt in der Regel ein Geheimnis dar, das der Schweigepflicht nach § 203 Abs. 1 StGB unterliegt. Dennoch ist die Meldung von drogenabhängigen Therapieabbrechern an das Gesundheitsamt nicht strafbar, wenn eine Befugnis zur Offenbarung besteht. Eine solche Befugnis ergibt sich unmittelbar aus dem Bundesseuchengesetz (BSeuchG): Nach §§ 31 Abs. 1, 32 Abs. 1, 10 Abs. 2 Satz 3 BSeuchG sind Therapieeinrichtungen verpflichtet, den Gesundheitsämtern Auskünfte über Tatsachen zu geben, die zum Auftreten einer übertragbaren Krankheit führen können. Eine solche Tatsache ist die intravenöse Drogenabhängigkeit einer Person. Intravenös Drogenabhängige gelten nämlich gemäß § 2 Nr. 3 BSeuchG als ansteckungsverdächtig. Dieser Ansteckungsverdacht besteht auch dann fort, wenn sich die Drogenabhängigen freiwillig in eine Therapie begeben.

Um jedoch die Therapiearbeit durch Auskunftsverlangen nicht zu beeinträchtigen, hat das Staatsministerium des Innern die Gesundheitsämter angewiesen, die Ermittlungsmaßnahmen so lange auszusetzen, als sich der Ansteckungsverdächtige in der Therapieeinrichtung befindet.

Bei einem intravenös Drogenabhängigen, der seine Therapie abbricht und ohne Erlaubnis die Einrichtung verläßt, entfallen die Gründe, die den vorläufigen Verzicht auf Ermittlungen nach §§ 31 ff BSeuchG ermöglicht haben. Durch sein Verhalten gibt der Therapieabbrecher sogar Anlaß zur Befürchtung, daß er künftig seiner Verantwortung Dritten gegenüber nicht gerecht werde und diese anstecke.

Die Gesundheitsämter sind daher verpflichtet, ab dem Therapieabbruch **Ermittlungen nach § 31 BSeuchG aufzunehmen**, um den Ansteckungsverdacht abzuklären. Hierzu fordern sie von der Therapieeinrichtung nach §§ 31 Abs. 1, 32 Abs. 1, 10 Abs. 2 Satz 3 BSeuchG die namentliche Bekanntgabe der Therapieabbrecher.

Um dem informationellen Selbstbestimmungsrecht der Betroffenen Rechnung zu tragen, habe ich jedoch empfohlen, die Patienten durch einen Hinweis im Aufnahmeprotokoll darüber aufzuklären, daß sie bei Abbruch der Therapie dem Gesundheitsamt namentlich gemeldet werden.

2.2 Gesundheitsämter

Im Berichtszeitraum wurden vier Gesundheitsämter überprüft. Mein Interesse galt besonders den organisatorischen und personellen Maßnahmen zur Einhaltung des **Verwertungsverbotes** nach Art. 6 des Gesetzes über den öffentlichen Gesundheitsdienst (GDG). Nach dieser Vorschrift dürfen Geheimnisse, die dem Gesundheitsamt bei **freiwilliger** Beratung, Untersuchung oder Begutachtung bekannt geworden sind, bei der Erfüllung anderer, insbesondere **hoheitlicher** Aufgaben nicht verwertet werden; eine Ausnahme gilt, wenn der Betroffene einwilligt oder wenn es die Abwehr von Gefahren für Leben oder Gesundheit Dritter erfordert. In diesem Zusammenhang waren nachfolgenden Punkte zu klären:

Zentralkartei

Die Gesundheitsämter führen als Suchkartei zum Wiederauffinden von Vorgängen eine Zentralkartei. Bei manchen Gesundheitsämtern enthielten die Karteiblätter neben den notwendigen Suchmerkmalen allerdings auch **inhaltliche Hinweise** auf bestimmte Erkrankungen oder persönliche Lebensumstände (z. B. „Zeugnis zur Unterbringung im Spastiker-Zentrum", „wegen Eingliederungshilfe", „wegen dauernder Anstaltsunterbringung" oder „Verurteilung wegen Verstoß gegen das Betäubungsmittelgesetz"). Da alle Mitarbeiter die Zentralkartei benützen, erhalten sie somit auch Kenntnis von den in der Zentraldatei vermerkten Informationen aus der freiwilligen Beratung und Begutachtung. Damit besteht die Gefahr, daß diese Informationen — ohne Zustimmung des Betroffenen — für andere Aufgaben des Gesundheitsamtes verwendet werden.

Als vorbeugende Maßnahme zur Sicherstellung des Verwertungsverbotes nach Art. 6 GDG sollte die Zentralkartei nach Auffassung des Staatsministeriums des Innern, die ich teile, als **reine Suchkartei** geführt werden, in der nur formale, zur Wiederauffindung des Vorgangs erforderliche Hinweise, hingegen keine inhaltlichen Vermerke über Beratung oder Begutachtung gespeichert werden. Die Unterlagen über die Beratung oder Begutachtung sollten im jeweils zuständigen Fachbereich aufbewahrt werden. Dessen Mitarbeiter haben dann bei hoheitlichem Tätigwerden des Gesundheitsamtes über die Verwendung von Vorgängen unter Beachtung des Verwertungsverbotes nach Art. 6 GDG zu entscheiden.

Eines der kontrollierten Gesundheitsämter führt eine Zentralkartei, die diesen Anforderungen entspricht. Auf den einzelnen Karteikarten wird unter Verwendung der Ziffern 1 bis 6 angegeben, bei welchem der sechs Sachgebiete Vorgänge über den Betroffenen vorhanden sind. Rückschlüsse auf bestimmte Erkrankungen sind aus der Zentralkartei nicht möglich, weil die Arbeitsbereiche entweder verschiedenartige Tätigkeiten umfassen oder ihrer Art nach keinen Hinweis auf bestehende Krankheiten geben.

Die Regierung von Oberbayern hat den übrigen Gesundheitsämtern ihres Bereichs vorgeschlagen, ihre Zentralkartei entsprechend verschlüsselt zu führen. Diese Verschlüsselung ist allen Gesundheitsämtern zu empfehlen, in denen die Einteilung in Arbeitsbereiche nicht gleichzeitig Hinweise auf Erkrankungen oder gesundheitliche Probleme wie Drogenabhängigkeit oder Behinderung gibt.

Trennung der Aufgabenbereiche am Gesundheitsamt zur Sicherstellung des Verwertungsverbotes nach Art. 6 Abs. 1 GDG

Das Verwertungsverbot muß auch durch Aufgabentrennung innerhalb eines Gesundheitsamtes gesichert werden. Diese Frage war Schwerpunkt der Prüfung eines städtischen Gesundheitsamtes.

Ein und dieselbe Abteilung dieses Amtes nimmt zwar sowohl hoheitliche Aufgaben (Bekämpfung übertragbarer Krankheiten) als auch Beratungsaufgaben nach Art. 11 Abs. 1 GDG (anonyme Aidsberatung) wahr. Diese Aufgaben

sind jedoch verschiedenen Sachgebieten übertragen, die räumlich und personell voneinander getrennt sind. Die Wahrung der Anonymität der Betroffenen in der Aidsberatungsstelle und die Verwendung der anfallenden Daten ausschließlich zu Beratungszwecken innerhalb dieser Stelle war gewährleistet.

Gesundheitszeugnisse und Gutachten (z.B. Gutachten für die Sozialhilfeverwaltung, für Leistungen wie Kur oder Psychotherapie) werden von einem nur für diese Aufgaben zuständigen Sachgebiet erstellt. Akten eines anderen Sachgebietes werden von der Gutachterstelle nur mit schriftlicher Einwilligung des Betroffenen beigezogen. Diese Organisation trägt dem Datenschutz Rechnung.

Die Prüfung ergab allerdings auch, daß in dem für Erwachsenenpsychiatrie und Suchtkrankenfürsorge zuständigen Sachgebiet **„Beratungs"- und Begutachtungsunterlagen in einem einheitlichen Akt** geführt werden. Unterlagen aus einer Beratung, der sich der Betroffene freiwillig unterzieht, und aus einer hoheitlichen Begutachtung sollten zur Sicherung des Verwertungsverbotes nicht im gleichen Akt geführt werden. Während es sich bei den Gutachten um Unterbringungs-, Pflegschafts- und Entmündigungsgutachten handelt, die eindeutig in hoheitlicher Tätigkeit erstellt werden, haben sich hinsichtlich der „Beratung" Zweifel ergeben, ob das Sachgebiet tatsächlich eine typisch gesundheitliche Beratung im Sinne des Art. 11 Abs. 1 GDG vornimmt oder bereits eine Art „Vorbegutachtung", aufgrund derer es entscheidet, ob eine Pflegschaft oder Unterbringung in Betracht kommt. Im letzteren Fall läge eine hoheitliche Tätigkeit vor, mit der Folge, daß gegen die einheitliche Aktenführung keine Einwände zu erheben wären. In diesem Punkt stehe ich mit dem Innenministerium in Verbindung. In diesem Zusammenhang ist zu klären, ob alle Erkenntnisse aus solchen „Beratungen", die einer Begutachtung vorausgehen, für die Erstellung des Gutachtens verwertet werden dürfen.

2.3 Landesuntersuchungsämter für das Gesundheitswesen

Im Berichtszeitraum habe ich beide Landesuntersuchungsämter für das Gesundheitswesen überprüft. Zu ihren Aufgaben gehört insbesondere, in der Gesundheitsvorsorge für Gesundheitsämter und Kreisverwaltungsbehörden Laboruntersuchungen durchzuführen. Aus der Kontrolle ist zu berichten:

Verarbeitung von HIV-Daten:

Die Landesuntersuchungsämter führen HIV-Tests über eingesandte Blutproben durch. Im wesentlichen senden die Gesundheitsämter Proben ein für anonyme HIV-Tests sowie für HIV-Untersuchungen bei der Einstellung von Beamten und bei Anträgen auf Aufenthaltserlaubnis oder Asyl. Ferner senden die ärztlichen Dienste von Strafanstalten und vereinzelt auch Krankenhäuser HIV-Proben ein.

Aus der Sicht des Datenschutzes war von besonderem Interesse, inwieweit hierbei beim Landesuntersuchungsamt personenbezogene Daten anfallen und wie sie dort verwaltet werden. Ein Landesuntersuchungsamt legt seit November 1988 für jede einsendende Stelle eine eigene Liste an. Dort werden **in keinem Fall die Namen** von Betroffenen eingetragen. Das Testergebnis wird dem Untersuchungsantrag des Einsenders über die interne Labornummer des Landesuntersuchungsamtes zugeordnet. Die Einsender selbst bezeichnen die Probanden lediglich mit Code-Nummern. Hierzu waren sie vom Landesuntersuchungsamt aufgefordert worden. Wurde in Einzelfällen trotzdem der Name des Probanden mitgeteilt, etwa bei der Untersuchung eines Beamtenanwärters auf HIV, so hat das Landesuntersuchungsamt den Namen nicht in die Unterlagen übernommen. Auf dem Untersuchungsantrag wurde er unkenntlich gemacht und durch eine Code-Nummer ersetzt, die dem Einsender mitgeteilt wurde. Auf diese Weise entstehen bei diesem Landesuntersuchungsamt keine personenbezogenen Datenbestände über Personen, deren Blut auf HIV getestet wurde.

Bei diesem Landesuntersuchungsamt besteht allerdings noch eine Kartei, in die früher alle HIV-Untersuchungen eingetragen wurden, und zwar bei anonymen Tests mit der Code-Nummer, bei nichtanonymen Tests vielfach auch mit Namen und ggf. Geburtsdatum des Betroffenen.

Zu dieser Kartei habe ich die Auffassung vertreten, daß die Registrierung von Name und Geburtsdaten der Probanden bei HIV-Untersuchungen zur Erfüllung der Aufgaben des Landesuntersuchungsamtes nicht erforderlich und die Kartei daher in einer Sonderaktion zu anonymisieren ist. Die Anonymisierung der HIV-Kartei wurde zugesagt.

Da seit November 1988 nur mehr Listen in anonymer Form geführt werden, habe ich von einer formellen Beanstandung der früheren Registrierung der Namen in der Kartei abgesehen.

Im anderen Landesuntersuchungsamt war eine entsprechende Kartei nicht angelegt worden. Da auch hier in Einzelfällen bei nicht anonymen HIV-Tests Namen auf den Untersuchungsanträgen angegeben waren, habe ich das Amt aufgefordert, von den Einsendern zu verlangen, daß sämtliche HIV-Untersuchungsanträge nur noch mit Code-Nummern und ohne Namensangaben eingesandt werden. Darüber hinaus wies das Staatsministerium des Innern die Gesundheitsämter darauf hin, daß Blutproben zur Untersuchung auf HIV-Antikörper den Landesuntersuchungsämtern **ausnahmslos anonymisiert** zuzuleiten sind. Dies bedeutet, daß auch in Fällen, in denen das Gesundheitsamt keine anonymen HIV-Tests durchführt, wie bei Einstellungsuntersuchungen für Beamte, die HIV-Untersuchungsanträge ohne Namensangabe zu übersenden sind.

Verarbeitung personenbezogener Daten im Bereich Virologie/Serologie

Beide Landesuntersuchungsämter führen virologische und serologische Untersuchungen durch. Für die gleichen Einzeluntersuchungen werden von den Ämtern teils Karteien geführt, teils nicht für erforderlich gehalten. Da die gesetzlichen Aufgaben nach Art. 3 Abs. 1 des Gesundheitsdienstgesetzes bei beiden Landesuntersuchungsämtern gleich sind, habe ich das Staatsministerium des Innern gebeten, mit den Ämtern ein einheitliches Konzept zur Speicherung personenbezogener Daten im Bereich Virologie/Serologie zu erarbeiten. Die Vorarbeiten für ein **einheitliches Datenverarbeitungskonzept** der beiden Landesuntersuchungsämter wurden bereits aufgenommen.

2.4 Datenschutz im Krankenhaus

Zunächst hatte ich beabsichtigt, systematische Datenschutzprüfungen bei Krankenhäusern öffentlicher Träger bereits in den Kontrollplan 1989 aufzunehmen. Dieses Vorhaben mußte ich jedoch bis 1990 zurückstellen, da entgegen der ursprünglichen Planung die Kontrolle der Gesundheits- und Landesuntersuchungsämter vorgezogen wurde.

Honorarabrechnung für ambulante Privatpatienten

Zu folgendem Fall wurde ich um Stellungnahme gebeten:

Ein Krankenhausträger beabsichtigt, von den privatliquidationsberechtigten Ärzten Angaben über deren ambulante Privatpatienten zu verlangen, um die **Abführung der Nebentätigkeitsabgaben kontrollieren** zu können. Vertragsbeziehungen bestehen in diesen Fällen in der Regel nur zwischen Privatpatient und Arzt, nicht jedoch zwischen Patient und Krankenhaus, so daß sie als Rechtsgrundlage für die Übermittlung der Patientendaten an das Krankenhaus ausscheiden. Bei bestimmten Erkrankungen haben die Patienten zudem ein ausgeprägtes Interesse daran, daß ihre Krankheit möglichst wenigen Personen bekannt wird (z.B. positiver HIV-Befund, psychiatrische Probleme, Geschlechtskrankheiten). In solchen Fällen kann nicht angenommen werden, daß die Patienten eine Einwilligung zur Bekanntgabe ihres Namens und weiterer Daten an die Krankenhausverwaltung zur Abrechnung freiwillig erteilen.

Es stellt sich daher die Frage, ob das zum allgemeinen Beamtenrecht gehörende Nebentätigkeitsrecht das Krankenhaus berechtigt, von personenbezogenen **Patientendaten aus einer Nebentätigkeit des Krankenhausarztes** Kenntnis zu nehmen. Ein solches Informationsrecht des Krankenhauses erscheint mir jedenfalls in den Fällen, in denen der Patient ein besonderes Interesse an der Geheimhaltung seines Arztbesuches hat, als unverhältnismäßiger Eingriff in die Privatsphäre des Patienten. Ob der Arzt die Nebentätigkeitsabgaben zuverlässig abführt, kann nämlich auch ohne Bekanntgabe personenbezogener Patientendaten kontrolliert werden. Bei Stellung der Honorarrechnungen könnten Durchschriften als Nachweise für die Abrechnungskontrolle hergestellt werden, die keine Patientennamen enthalten. Die Vollständigkeit der Rechnungsdurchschriften könnte durch Verwendung von durchnumerierten Rechnungsblöcken sichergestellt werden. Schließlich hält auch der Bayerische Kommunale Prüfungsverband **anonymisierte Durchschriften für Zwecke der Rechnungsprüfung** für ausreichend.

In dem eingangs zitierten Fall wollte das Krankenhaus sogar, daß das Honorar unmittelbar auf ein Konto des Krankenhauses anstatt auf ein Konto des Arztes überwiesen wird. Hierdurch würde die Tatsache der ambulanten Privatbehandlung des Einzahlers einer größeren Zahl von Personen bekannt. Eine solche Forderung wäre zur Sicherung der vollständigen Entrichtung der Nebentätigkeitsabgaben auch unverhältnismäßig, da das Krankenhaus gegen die Gehaltsforderung des Arztes aufrechnen könnte.

2.5 Veröffentlichungen der Apothekerkammer

Durch eine Eingabe wurde ich darauf aufmerksam, daß Apothekerkammern personenbezogene Daten von Apothekern zur Veröffentlichung an Fachzeitschriften übermitteln. Veröffentlicht werden neben **Geburtstagen** von Apothekern und Apothekerinnen auch **apothekenrechtliche Vorgänge**, z.B. Eröffnung, Schließung, Verlegung, Übernahme, Kauf und Fortführung einer Apotheke als Eigentümer. Den Publikationen sind Name und Adresse des Jubilars bzw. Name des Apothekenleiters und Anschrift der Apotheke zu entnehmen.

Die Landesapothekerkammer hat ihre Mitglieder inzwischen durch Rundschreiben davon in Kenntnis gesetzt, daß sie einer **Veröffentlichung ihrer Geburtstage widersprechen** können. Informationen über apothekenrechtliche Vorgänge werden dagegen auch künftig ohne Einwilligung der Mitglieder an die Fachzeitschriften weitergegeben. Die Zulässigkeit dieser Übermittlungen ist nach Art. 18 Abs. 1 BayDSG zu beurteilen. Voraussetzung ist danach, daß der Empfänger ein berechtigtes Interesse an der Kenntnis der zu übermittelnden Daten glaubhaft macht und dadurch schutzwürdige Belange des Betroffenen nicht beeinträchtigt werden.

- Bei Eröffnung, Neuerrichtung, Schließung und Verlegung einer Apotheke besteht ein allgemeines berufliches und wirtschaftliches Interesse an der Kenntnis dieser Vorgänge.

  Schutzwürdige Belange der Betroffenen werden durch eine Veröffentlichung nicht beeinträchtigt, da es sich insoweit um Umstände handelt, die von der Öffentlichkeit ohne weiteres wahrzunehmen sind.

- Bei den übrigen publizierten apothekenrechtlichen Vorgängen (Übernahme, Kauf, Fortführung als Eigentümer, Pacht und Verwaltung), die in das Handelsregister einzutragen und bekanntzumachen sind, kann davon ausgegangen werden, daß bei den Lesern der Fachzeitschriften ein **überwiegendes wirtschaftliches Interesse** an der Kenntnis dieser Daten besteht. So wird z.B. beim Tod eines Apothekers eine Verwaltungsgenehmigung nur für einen Zeitraum von zwölf Monaten bewilligt. Interessierte Kammermitglieder können dem Hinweis auf die Verwaltung entnehmen, daß eine Betriebserlaubnis für diese Apotheke frei wird.

- Hingegen will die Landesapothekerkammer den Kauf und die Fortführung einer Apotheke als Eigentümer nur mehr unter der Bezeichnung „Übernahme einer Apotheke" veröffentlichen, um das persönliche Schutzbedürfnis der betroffenen Apotheker zu berücksichtigen.

3. Genomanalyse

Bereits im 10. Tätigkeitsbericht habe ich die Notwendigkeit betont, bei der Anwendung der Genomanalyse in der Medizin, im Arbeits- und Wirtschaftsleben sowie in gerichtlichen Verfahren den Datenschutz strikt einzuhalten. Meine im Bericht skizzierten Vorstellungen habe ich bei einer Veranstaltung der SPD-Landstagsfraktion am 2. Juni 1989 zum Thema „Genomanalyse und Menschenwürde" weiter präzisiert. Diese Überlegungen sind in die Beratungen der Arbeitsgruppe Genomanalyse beim Bundesbeauftragten für den Datenschutz eingeflossen. In einem einstimmigen Beschluß haben die Datenschutzbeauftragten der Länder und des Bundes ihre Forderungen zur Genomanalyse formuliert (Anhang 1).

4. Sozialbehörden

4.1 Rentenreform-Gesetz 1992

Zu dem 1989 im Bundestag eingebrachten Entwurf eines Rentenreform-Gesetzes habe ich mich wiederholt geäußert. In einer Stellungnahme gegenüber dem Staatsministerium für Arbeit und Sozialordnung habe ich umfangreiche Vorschläge zur Verbesserung des Datenschutzes unterbreitet, die vom Ministerium unterstützt wurden. Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat am 05./06. April 1989 Forderungen zum Gesetzentwurf aufgestellt, die weitgehend berücksichtigt wurden. Auf zwei Problempunkte der Reform weise ich besonders hin:

4.1.1 Datenstelle der Rentenversicherungsträger

Die „Datenstelle der Deutschen Rentenversicherung" in Würzburg verwaltet die Stammsatzdatei aller Rentenversicherten mit ca. 63 Millionen Datensätzen zur Aufdeckung und Verhinderung von Mehrfachvergaben von Versicherungsnummern, zur Herstellung von Querverbindungen zwischen verschiedenen Sozialleistungsträgern, zur Steuerung des Datenaustausches und zur Herstellung der Verbindungen zu Rentenversicherungsträgern in der Europäischen Gemeinschaft. Die Datenstelle ist ein Sonderreferat des Verbandes Deutscher Rentenversicherungsträger (VDR). Der VDR ist ein Zusammenschluß aller 22 Träger der gesetzlichen Rentenversicherung in der Bundesrepublik Deutschland in der Rechtsform eines eingetragenen Vereins.

Die Hauptaufgabe der Datenstelle ist bisher in § 14 der 2. Datenerfassungs-Verordnung (2. DEVO) beschrieben. Bis zum Erlaß des Gesetzes bestanden unterschiedliche Rechtsauffassungen zur Frage, ob die Führung der Stammsatzdatei bei der Datenstelle als eigenständige, durch Rechtsnorm zugewiesene Aufgabe oder als **Datenverarbeitung im Auftrag** der einzelnen Rentenversicherungträger anzusehen war. Von der Klärung dieser Frage hing ab,

- wer als speichernde Stelle verantwortlich ist,
- wer als Herr der Daten Anfragen öffentlicher Stellen zu beantworten und Auskunftsansprüche von Bürgern zu erfüllen hat,
- wer zuständige Rechtsaufsichtsbehörde ist,
- welcher Datenschutzbeauftragte Kontrollbefugnisse bei der Datenstelle besitzt.

Ich hatte vorgeschlagen, im Gesetz klarzustellen, daß die Datenstelle nur als Auftragnehmer tätig wird mit der Folge, daß die Verantwortung für die gespeicherten Daten bei den einzelnen Rentenversicherungsträgern verbleibt. Das Staatsministerium für Arbeit und Sozialordnung hat diesen Vorschlag aufgegriffen; er wurde jedoch im weiteren Gesetzgebungsverfahren nicht berücksichtigt. Das Rentenreformgesetz regelt die angesprochenen Fragen immerhin normenklar: es überträgt die Aufgaben nahezu vollständig auf **Bundeseinrichtungen**. Föderalistische Gesichtspunkte blieben unberücksichtigt.

Mit Blick auf die Datenstelle der Deutschen Rentenversicherungsträger weise ich in diesem Zusammenhang darauf hin, daß bei dieser Stelle durch das Gesetz zur Einführung eines Sozialversicherungsausweises auch eine **Zentraldatei aller geringfügig beschäftigten Personen** eingerichtet wird. Damit werden, wenn auch in unterschiedlichen Dateien, nahezu alle erwachsenen Personen in der Bundesrepublik Deutschland zentral erfaßt. Trotz der vorgesehenen Unterstellung der Datenstelle unter die Aufsicht des Bundesministers für Arbeit und Sozialordnung und unter die Kontrolle des Bundesbeauftragten für den Datenschutz bleibt der VDR ein privatrechtlicher eingetragener Verein, der für die Verwaltung der Datenstelle und damit für den umfassendsten personenbezogenen Datenbestand der Bundesrepublik zuständig ist. Legt man die Maßstäbe zugrunde, die sonst an Datenschutz und Datensicherheit im Sozialbereich gelegt werden, fragt man sich wohl zu Recht, ob die gewählte Organisationsform angemessen ist.

4.1.2 Direktabruf von Rentendaten

Während des Gesetzgebungsverfahrens wurde ein Vorschlag eingebracht, nach dem künftig sowohl die von den Rentenversicherungsträgern gespeicherten Daten als auch die Daten der Datenstelle (siehe oben) von einer sehr großen Anzahl von Behörden (alle Träger der Rentenversicherung und Krankenversicherung, Deutsche Bundespost) automatisiert (online) abgerufen werden dürfen. Darüber hinaus soll der Direktabruf auch den entsprechenden ausländischen Stellen ermöglicht werden.

Die datenschutzrechtliche Besonderheit beim Direktabrufverfahren besteht darin, daß letztlich nur die abrufende Stelle bestimmt, welche Daten ihr über wieviele Personen zur Kenntnis gelangen. Die abgebende Stelle kann nur nachträglich über eine stichprobenweise Auswertung von Protokollen feststellen, welche Daten abgerufen wurden. Online-Abrufmöglichkeiten sind zwar aus der Sicht des Datenschutzes nicht grundsätzlich abzulehnen. Ein Online-Anschluß einer großen Zahl von abrufberechtigten inländischen und ausländischen Stellen bei den Rentenversicherungsträgern und bei den zentralen Datenbeständen der Datenstelle der Rentenversicherungsträger schafft jedoch für die Betroffenen ein nicht mehr überschaubares Risiko. Es muß daher Vorsorge dafür getroffen werden, daß Direktabrufverfahren nur dann eingerichtet werden, wenn sie unter Berücksichtigung der schutzwürdigen Interessen der Betroffenen und der Aufgaben der obengenannten Stellen angemessen sind.

Hierzu habe ich vorgeschlagen, daß die Angemessenheit des Online-Anschlusses in einem **Genehmigungsverfahren** überprüft werden soll. In der Genehmigung sollten in Anlehnung an den Regierungsentwurf zum Bundesdatenschutzgesetz festgelegt werden

- Anlaß und Zweck des Abrufverfahrens,
- Datenempfänger,
- Art und Umfang der abrufbaren Daten,
- die für die wirksame Sicherung und Kontrolle erforderlichen technischen und organisatorischen Maßnahmen (z.B. Protokollierungen).

Der Bundesarbeitsminister hat inzwischen zugesagt, daß meine Forderung bei der Novellierung des Bundesdatenschutzgesetzes berücksichtigt wird.

4.2 Entwurf eines Jugendhilfe-Gesetzes

Im Berichtszeitraum habe ich zweimal zu einem Referentenentwurf für ein neues Kinder- und Jugendhilfegesetz Stellung genommen. Die Neufassung des Jugendhilferechts und die Aufnahme in das Sozialgesetzbuch als Achtes Buch sollten zum Anlaß genommen werden, **normenklare**

Vorschriften zum Datenschutz in das Gesetz aufzunehmen. Im einzelnen habe ich mich zu folgenden Punkten geäußert:

Informationsgrundlagen

Aufgaben und Befugnisse der öffentlichen Jugendhilfe im Umgang mit personenbezogenen Daten sind im Gesetz zu beschreiben. Ferner sind Grundsätze für die Datenverwendung zu normieren. In einer Befugnisnorm sind der Umfang der zulässigen Datenerhebung und -speicherung sowie die Zweckbestimmung dieser Daten festzulegen. Dabei ist zu berücksichtigen, daß im Jugendhilferecht abweichend von den übrigen Sozialleistungen nicht in allen Fällen von einer Mitwirkungsbereitschaft der Beteiligten ausgegangen werden kann (z.B. bei Unterhaltspflichtverletzungen, Freiheitsentziehung bei Jugendlichen, drohender Verwahrlosung). Die Auskunftspflichten der Beteiligten sowie Dritter (z.B. Arbeitgeber) sind daher präzise zu regeln.

Wegen der besonderen Sensibilität der Daten sind ergänzend zu § 84 SGB X besondere Aufbewahrungsfristen, etwa im Bereich der Jugendgerichtshilfe, angezeigt.

In die Erkenntnisse über einen Minderjährigen fließen auch eine Vielzahl von Daten aus seiner sozialen Umgebung ein. Deshalb sind nicht nur die Persönlichkeitsrechte des Minderjährigen, sondern auch der Personen seines **sozialen Umfeldes** (Eltern, Geschwister, Freunde usw.) zu berücksichtigen. Besondere Schwierigkeiten können sich beim Anspruch auf Akteneinsicht oder auf Auskunft, aber auch bei der Berichtigung und Löschung von Informationen ergeben. Es sollten deshalb Regelungen gefunden werden, die auch die Persönlichkeitsrechte der Personen aus dem sozialen Umfeld der Minderjährigen im notwendigen und ausreichenden Umfang schützen.

Trennung von Beratung und Eingriffsverwaltung

Der vorliegende Gesetzentwurf sieht für den Regelfall die freiwillige Inanspruchnahme von Leistungen der Jugendhilfe vor. Er räumt der Beratung der Personensorgeberechtigten großen Raum ein. Die in einer Beratung mitgeteilten Geheimnisse dürften durch die beruflichen Verschwiegenheitspflichten des § 203 Abs. 1 Nr. 4 des Strafgesetzbuches geschützt sein.

Das Gesetz sollte allerdings klarstellen, daß Erkenntnisse aus der Beratungstätigkeit bei der sonstigen, insbesondere hoheitlichen Tätigkeit der Jugendämter grundsätzlich nicht ohne **Einwilligung** verwertet werden dürfen. Die Betroffenen sollen sicher sein, daß ihre freiwilligen Angaben später bei der Erfüllung anderer Aufgaben nicht gegen sie verwendet werden können. Ein Verwertungsverbot von Erkenntnissen aus der freiwilligen Beratung ist auch deshalb angezeigt, weil der Gesetzentwurf den Jugendämtern erlaubt, einen Teil ihrer Beratungsaufgaben von den Trägern der freien Wohlfahrtspflege wahrnehmen zu lassen und in diesem Fall den Jugendämtern die Erkenntnisse der freien Wohlfahrtspflege nicht zur Verfügung stehen. Die Verwertung von Erkenntnissen aus der Beratung darf aber nicht davon abhängen, ob die Beratung vom Jugendamt oder von einem Träger der freien Wohlfahrtspflege durchgeführt wurde. Auf die in Art. 6 Gesundheitsdienstgesetz für den öffentlichen Gesundheitsdienst gefundene Lösung habe ich hingewiesen.

Stellung des Amtsvormundes/Amtspflegers

Die verfahrensrechtliche Stellung des Amtsvormundes/Amtspflegers für einen Minderjährigen ist nach geltendem Recht nicht eindeutig festgelegt. Zum einen sind nach § 38 Jugendwohlfahrtsgesetz auf die Amtsvormundschaft und die Amtspflegschaft die Bestimmungen des Bürgerlichen Gesetzbuches anzuwenden. Zum anderen machen derzeit die bestellten Amtsvormünder/Amtspfleger von den Möglichkeiten behördlicher Tätigkeit einschließlich der Amtshilfe durch andere Behörden Gebrauch. Der vorliegende Gesetzentwurf ändert ihre **unklare Rechtsstellung** nicht. Wie bisher stellt sich die Frage, ob die Bestimmungen für das Verwaltungsverfahren und den Schutz der Sozialdaten nach dem Zehnten Buch zum Sozialgesetzbuch für alle Tätigkeiten des Amtsvormundes/Amtspflegers anzuwenden sind. Das neue Gesetz sollte hier Klarheit schaffen.

Ergänzend sei noch angemerkt, daß bei einer Zuordnung der Tätigkeit zum privaten Bereich dem Amtsvormund/Amtspfleger die übrigen Akten des Jugendamtes, des Sozialamtes und der Sozialarbeiter beim Jugendamt nicht mehr zur Verfügung stünden, da dann eine entsprechende Offenbarungsbefugnis (etwa nach § 69 Abs. 1 Nr. 1 SGB X) für diese Stellen fehlen würde. Der Amtsvormund/Amtspfleger wäre vielmehr ausschließlich auf eigene Erhebungen angewiesen. Dies entspricht nicht der gegenwärtigen Praxis.

Ähnliche Zweifelsfragen gilt es bei dem gegenwärtig beratenen Betreuungsgesetz für Volljährige zu klären. Es liegt nahe, für das gesamte Vormundschafts-, Pflegschafts- und Betreuungsrecht **gleichartige Verfahrens- und Datenschutzbestimmungen** vorzusehen, um eine Ungleichbehandlung gleichartiger Lebensvorgänge zu vermeiden.

4.3 Datenerhebung in der Sozialhilfe

Bei Anträgen auf Sozialhilfe sind umfassende **Einkommenserhebungen beim Hilfesuchenden** und bei seinen unterhaltspflichtigen **Angehörigen** erforderlich. Dies empfindet der Betroffene als Belastung mit der Folge, daß immer wieder Beschwerden und Anfragen bei mir eingehen, ob die Angaben zu Recht gefordert werden. Im Berichtsjahr hatte ich zu drei Problemkreisen Stellung zu nehmen.

Einheitliches Antragsformular für Sozialhilfe

Bereits 1984 hatte ich beim Landkreisverband Bayern, beim Verband der Bayerischen Bezirke und beim Bayerischen Städtetag angeregt, einen Musterentwurf für einen Sozialhilfeantrag zu erarbeiten und untereinander abzustimmen. Der Landkreisverband und der Verband der Bayerischen Bezirke haben zwischen 1985 und 1987 weitgehend **inhaltsgleiche Antragsformulare** vorgelegt und zur allgemeinen Verwendung empfohlen; datenschutzrechtliche Bedenken gegen die verlangten Angaben bestehen nicht.

Aufgrund einer Beschwerde mußte ich freilich feststellen, daß ein bayerischer Bezirk im Berichtszeitraum immer noch ein Antragsformular verwendete, das dem Muster seines Verbandes nicht entsprach und datenschutzrechtlich unzulässige Fragen vorsah. Die Fragen bezogen sich auf Angehörige außerhalb des Haushaltes, auf die Gründe für einen Zuzug, auf Kündigungsgründe u.ä.. Darüber hinaus enthielt der Fragebogen eine **allgemeine Ermächtigung** des

Hilfesuchenden zur Auskunft über Bankguthaben sowie eine **allgemeine Entbindung** von der ärztlichen Schweigepflicht.

Ich habe den Bezirk aufgefordert, die Antragsformulare abzuändern. Einwilligungserklärungen dürfen vom Hilfesuchenden nur verlangt werden, wenn klar erkennbar ist, welche Stellen unter welchen Voraussetzungen um Auskunft ersucht werden. Detaillierten Einzelermächtigungen und Entbindungen von der ärztlichen Schweigepflicht ist hierbei der Vorzug zu geben. Meine Rechtsauffassung deckt sich mit der Haltung des Staatsministeriums für Arbeit und Sozialordnung. Der Bezirk hat mir inzwischen mitgeteilt, daß das Formular geändert und die pauschalen Ermächtigungen durch **Einzelermächtigungen** ersetzt wurden.

Der Bayerische Städtetag hält ein einheitliches Antragsmuster nicht für zweckmäßig, da die Anträge auf die örtlichen Verhältnisse abgestellt werden müßten. Dies schließt freilich eine stärkere Vereinheitlichung nicht aus.

Ich werde bei meinen Prüfungen in den Sozialämtern in Zukunft besonderes Augenmerk auf die verwendeten Antragsformulare richten.

Erhebung der Einkommens- und Vermögensverhältnisse bei Unterhaltspflichtigen

Nach § 116 Abs. 1 BSHG haben Unterhaltspflichtige dem Träger der Sozialhilfe über ihre Einkommens- und Vermögensverhältnisse Auskunft zu geben, soweit die Durchführung dieses Gesetzes es erfordert.

Durch zwei Bürgereingaben bin ich auf den Fragebogen eines Bezirkes aufmerksam geworden, in dem nicht nur die Einkommensverhältnisse des Auskunftspflichtigen, sondern auch die **wirtschaftlichen Verhältnisse seines Ehegatten** sowie seiner im Haushalt und auch außerhalb des Haushalts lebenden Angehörigen (Eltern, Kinder u.a.) anzugeben waren. Auch Angaben über bestehende Verbindlichkeiten und Belastungen wurden erfragt.

Mit den Staatsministerien der Justiz und für Arbeit und Sozialordnung vertrete ich die Auffassung, daß für Ehegatten und sonstige Angehörige eines Unterhaltspflichtigen aus § 116 BSHG **keine Auskunftspflicht** abgeleitet werden kann (§ 99 SGB X findet in der Sozialhilfe keine Anwendung). Da sich jedoch der Umfang der Unterhaltspflicht nach § 1601 BGB vermindert, wenn der Unterhaltspflichtige gegenüber mehreren Personen Unterhaltsleistungen zu erbringen hat, liegt es im Regelfall im Interesse des Unterhaltspflichtigen, Angaben über weitere unterhaltsberechtigte Angehörige sowie über bestehende Verbindlichkeiten und Belastungen zu machen. Hierzu ist er aber nicht verpflichtet. Auf die **Freiwilligkeit** der Angaben ist er deshalb hinzuweisen.

Das Erhebungsformular sollte so aufgebaut sein, daß Zweifel über obligatorische und freiwillige Angaben vermieden werden. Der Bezirk hat mir eine Änderung seines Fragebogens zugesichert.

Vorlage einer Verdienstbescheinigung

Ein Landtagsabgeordneter hat mich darauf hingewiesen, die Träger der Sozialhilfe würden für Verdienstbescheinigungen Formulare benutzen, aus denen der Arbeitgeber eines nach dem Sozialhilferecht Unterhaltspflichtigen den Verwendungszweck „Sozialhilfe" erkennen könne. Dies sei nicht notwendig und für den Unterhaltspflichtigen diskriminierend.

Eine Stichprobe bei verschiedenen Trägern der Sozialhilfe hat ergeben, daß die dort verwendeten Vordrucke für Verdienstbescheinigungen nicht landesweit einheitlich gestaltet sind. Die Sozialhilfeträger benutzen verschiedene Vordrucke privater Fachverlage.

Unterhaltspflichtige haben nach § 116 Abs. 1 BSHG dem Sozialhilfeträger Auskunft über ihre Einkommensverhältnisse zu geben. Die Vorlage einer Verdienstbescheinigung des Arbeitgebers dient diesem Zweck. Die äußere Form der Verdienstbescheinigung ist nicht vorgeschrieben. Die Bescheinigung ist im Regelfall vom Unterhaltspflichtigen selbst beizubringen. Dabei ist es nicht erforderlich, daß der Arbeitgeber Kenntnis von der in Frage stehenden Sozialleistung oder Unterhaltspflicht für einen Sozialhilfeempfänger erhält. Entsprechende Hinweise auf dem Vordruck widersprechen daher datenschutzrechtlichen Belangen. Sozialhilfeträger dürfen deshalb nur solche **Vordrucke** verwenden, die keinen Rückschluß zulassen, daß die Bescheinigung einem Sozialhilfeträger vorgelegt werden soll.

Anders verhält es sich allerdings, wenn der Unterhaltspflichtige seiner Pflicht zur Auskunft nicht oder nicht ausreichend nachkommt. In diesen Fällen hat der Träger der Sozialhilfe die Möglichkeit, sich unmittelbar an den Arbeitgeber zu wenden, der insoweit einer Auskunftspflicht unterliegt (§ 116 Abs. 2 BSHG). Zur Begründung seines Auskunftsanspruches hat der Sozialhilfeträger den Anlaß seiner Anfrage zu nennen; die Offenbarung von Sozialdaten wird damit erforderlich im Sinne des § 69 Abs. 1 Nr. 1 SGB X.

4.4 Information des Sozialamtes bei drohender Zwangsräumung

Im Berichtszeitraum hatte ich zu der Frage Stellung zu nehmen, welche Informationen ein Sozialamt bei drohender Zwangsräumung eines Wohnungsmieters erhalten und weitergeben darf.

Unterrichtung der Gemeinde über Räumungsklagen

Aufgrund einer Verwaltungsvorschrift teilen die Zivilgerichte derzeit dem Sozialamt unter bestimmten Voraussetzungen den Eingang einer Räumungsklage mit (Abschnitt IV/1 der Anordnung über Mitteilung in Zivilsachen).

Die eingehenden Meldungen dienen dem Sozialamt als Grundlage für eine Prüfung, ob die drohende Zwangsräumung durch geeignete Maßnahmen abgewendet werden kann und soll (§ 5 BSHG). Im Zuge der notwendigen Aufklärung und Ermittlung des Sachverhaltes kann es notwendig sein, die Gemeinde einzuschalten und über die drohende Obdachlosigkeit in Kenntnis zu setzen (§ 69 Abs. 1 Satz 1 SGB X).

Mit den Staatsministerien des Innern und der Justiz vertrete ich allerdings die Auffassung, daß die Mitteilung **sämtlicher Räumungsklagen** an die Gemeinde im Hinblick auf das informationelle Selbstbestimmungsrecht der betroffenen Wohnungsmieter unzulässig wäre. Zulässig ist die Mitteilung nur, soweit sie im Einzelfall notwendig ist.

Mitteilungen der Vermieter an das Sozialamt

Das Sozialamt einer Großstadt ist an die örtlichen gemeinnützigen Wohnungsgesellschaften mit dem Wunsch herangetreten, möglichst frühzeitig über Wohnungsmieter unterrichtet zu werden, die mit ihren Mietzahlungen in **Rückstand** geraten sind. Eine Wohnungsgesellschaft hat mich um Stellungnahme gebeten, ob sie dieser Bitte nachkommen darf.

Mit dem Staatsministerium für Arbeit und Sozialordnung vertrete ich die Auffassung, daß das Sozialamt **keinen Auskunftsanspruch** gegenüber Vermietern besitzt. Erhält jedoch das Sozialamt trotzdem von einem Vermieter Angaben über Mietverhältnisse, so kann als Rechtsgrundlage für die Datenspeicherung § 5 BSHG herangezogen werden. Nach dieser Bestimmung setzt die Sozialhilfe ein, sobald dem Sozialamt bekannt wird, daß die Voraussetzungen für die Gewährung vorliegen. Ein Antrag des Betroffenen ist hierfür nicht Voraussetzung. Nach § 6 BSHG soll die Sozialhilfe vorbeugend gewährt werden, wenn dadurch eine drohende Notlage ganz oder teilweise abgewendet werden kann.

Nach Auffassung des Staatsministeriums für Arbeit und Sozialordnung können diese allgemeinen Grundsätze der Sozialhilfe als **ausreichende Rechtsgrundlage** für das Sozialamt angesehen werden, sich in einer Großstadt mit gehäuften und verschärften Wohnungs- und Unterbringungsproblemen an die örtlichen gemeinnützigen Wohnungsgesellschaften zu wenden, um Kenntnis von säumigen Mietzahlern zu erhalten. Eine solche Kenntnis ist zweckmäßig, da nach näherer Maßgabe des § 554 BGB bereits ein Mietrückstand von zwei Monatsmieten für eine fristlose Kündigung ausreichen kann. Die Kündigung wird jedoch unwirksam, wenn sich bis zum Ablauf eines Monats nach Eintritt der Rechtshängigkeit des Räumungsanspruches eine öffentliche Stelle (hier: das Sozialamt) zur Befriedigung der offenen Forderung verpflichtet (§ 554 Abs. 2 BGB). Dabei sieht § 15 a BSHG zur Sicherung der Unterkunft Hilfe zum Lebensunterhalt selbst in Fällen vor, in denen nach den allgemeinen Bestimmungen eine Gewährung von Sozialhilfe nicht möglich ist.

Der den genannten Bestimmungen zugrunde liegende Rechtsgedanke einer besonderen Verpflichtung öffentlicher Stellen zur Sicherung der Unterkunft und zur Vermeidung von Obdachlosigkeit ergibt somit, daß entsprechende Bemühungen des Sozialamtes nicht zu beanstanden sind. Ich habe mich der Rechtsauffassung des Staatsministeriums für Arbeit und Sozialordnung angeschlossen.

5. Polizei

5.1 Zur Lage des Datenschutzes

In meinem 10. Tätigkeitsbericht habe ich darauf hingewiesen, daß „die Informationstätigkeit der Polizei **plausibel** und für den Datenschutzbeauftragten **rechtlich nachvollziehbar** sein" muß. Unter diesem Gesichtspunkt habe ich meine intensiven Kontrollen bei bayerischen Polizeibehörden fortgesetzt. Die datenschutzrechtliche Bewertung der polizeilichen Informationstätigkeit ist im Grundsätzlichen wie im Einzelfall nur möglich, wenn die Entscheidung ausreichend durch Unterlagen **dokumentiert** ist.

Erfreulich war die Feststellung, daß die polizeiliche Praxis bei den meisten Dienststellen dieser Forderung zunehmend entspricht.

Im Berichtszeitraum habe ich eine steigende Zahl von **Anfragen** aus der Bevölkerung verzeichnet, aber auch einen Anstieg an Anfragen von Polizeibehörden und Polizeibeamten zu Fragen der Zulässigkeit der Informationsverarbeitung im Einzelfall. Dies zeigt mir, daß der Bürger und die informationsverarbeitenden Stellen **verstärktes Interesse** an der Beantwortung von Fragen des Datenschutzes haben. Auch im Rahmen meiner Prüfungen bei Polizeidienststellen bemerke ich ein zunehmendes Verständnis für das Anliegen des Datenschutzes. Dies zeigt sich letztlich auch daran, daß die Zahl der beanstandeten Fehler weiter abgenommen hat.

Ich stelle weiterhin fest, daß Polizeibehörden ihre Datenbestände zunehmend **eigenen Relevanzprüfungen** unterziehen, um unter Berücksichtigung der Datenschutzprüfungen der letzten Jahre und im Interesse einer effektiveren polizeilichen Arbeit weniger relevante Informationen vorzeitig auszusondern und falsche Daten zu berichtigen. Dies begrüße ich.

Für die nähere Zukunft gewinnt die grenzüberschreitende Verarbeitung polizeilicher Daten wachsende Bedeutung. Ein Beispiel hierfür ist die angestrebte Zusammenarbeit der Polizeibehörden in den Vertragsstaaten des „Schengener Übereinkommens", mit dem die Grenzkontrollen in Zentraleuropa weitgehend aufgehoben werden sollen. Ziel der Datenschutzbeauftragten muß es sein, den zweifelsohne hohen deutschen Datenschutzstandard möglichst auch bei **europaweiter Datenverarbeitung** zu halten.

Das inzwischen erreichte hohe Maß an Datenschutz bei den meisten Polizeibehörden darf in Zukunft aber auch nicht durch das **private Sicherheits- und Überwachungsgewerbe** unterlaufen werden. So habe ich von Plänen erfahren, im privaten Bereich eine Datei zu errichten, in der „Aktivitäten von potentiellen Tätern" im Umfeld von zu schützenden Personen oder Objekten gespeichert werden sollen. Wenn es zu einer bundesweiten Ausdehnung einer solchen Datei kommen sollte, könnten unter Umständen ähnlich sensible Daten wie bei staatlichen Sicherheitsbehörden überregional vorgehalten werden, ohne daß die von der Polizei zu beachtenden strengeren gesetzlichen Regelungen gelten würden. Auf lokaler Ebene könnten umfangreiche Datenspeicherungen Bewegungsbilder von der näheren und ferneren Nachbarschaft vermitteln und gegen völlig Unbeteiligte Verdacht begründen. Auch die Kontrolle durch die Datenschutzbeauftragten wäre ausgeschlossen. Diese im Zuge der Terrorismusbekämpfung sich abzeichnende Entwicklung zu einer Privatisierung von Sicherheitsdaten ohne ausreichenden Datenschutz beobachte ich mit Skepsis und Sorge.

5.2 Novellierung des Polizeiaufgabengesetzes (PAG)

In meinem letzten Tätigkeitsbericht habe ich auf die Notwendigkeit der Novellierung des Polizeiaufgabengesetzes und auf die möglichen Folgen eines Ausbleibens der Novellierung für die polizeiliche Datenverarbeitung hingewiesen. Ich habe Erklärungen der Staatsregierung zitiert, wonach die Novelle zum Polizeiaufgabengesetz dem Landtag so rechtzeitig zugeleitet werden soll, daß die parlamentarischen Beratungen noch vor der Sommerpause 1989 aufgenommen werden können. Der Bayerische

Landtag hat die Staatsregierung aufgefordert, noch in dieser Wahlperiode einen Gesetzentwurf vorzulegen.

5.3 Neue Sicherungsmaßnahmen

Um künftig noch stärker als bisher Fälle einer mißbräuchlichen Nutzung polizeilicher Informationssysteme auszuschließen, hat das Bayerische Landeskriminalamt (BLKA) im Auftrag des Staatsministeriums des Innern den bisherigen **„Anmeldemodus" für polizeiliche Informationssysteme** weiter verbessert. Eine Abfrage z.B. aus INPOL und ZEVIS, ohne daß sich der abfragende Beamte gegenüber dem System ausgewiesen hat, ist nunmehr ausgeschlossen. Folgende Abfragedaten werden beim BLKA automatisch protokolliert:

- Datum und Uhrzeit einer Abfrage,
- Nummer des Datenendgeräts, von dem aus abgefragt wurde,
- Abgefragte Datei,
- Abfragebegriffe,
- personenbezogene Kennung des Abfragenden.

Dieser neue Anmeldemodus mit Protokollierung ist aus dreierlei Sicht vorteilhaft:

- Besteht der Verdacht einer unberechtigten Verwendung von Dateibeständen, kann auf Anordnung des Staatsministeriums des Innern festgestellt werden, ob überhaupt eine Auskunft eingeholt wurde und wer sie veranlaßt hat. Dies dient dem Schutz des Bürgers vor unberechtigten Abfragen und damit letztlich auch vor unberechtigter Verwendung der Daten.

- Durch Protokollierung der Abfragen wird auch die Polizei vor ungerechtfertigten Vorwürfen angeblicher unberechtigter Verwendung von Daten geschützt.

- Außerdem wird der Aufsichtsbehörde und dem Datenschutzbeauftragten die Kontrolle der Zulässigkeit der einzelnen Abfrage möglich.

Wenn in der Fahndungsdatei zur abgefragten Person kein Bestand vorhanden ist, wird die Abfrage nicht protokolliert, damit keine neue Datei entsteht. Im übrigen ist eine Auswertung der Protokolldaten für andere als Kontroll- oder Sicherungszwecke, von Ausnahmen abgesehen, ausgeschlossen.

Ich begrüße diese Form der Protokollierung von Anfragen aus datenschutzrechtlicher Sicht und werde künftig mein Augenmerk darauf richten, ob durch diese Protokollierungen alle Schutz- und Kontrollbedürfnisse gedeckt werden können.

5.4 Bürgereingaben

Im Berichtszeitraum habe ich einen **Anstieg** von Bürgereingaben gegenüber dem Vorjahr registriert. Schwerpunkte dieser Anfragen waren

- vermutete unberechtigte Datenweitergabe durch Polizeibeamte
- Auskünfte aus polizeilichen Dateien
- Speicherungen im kriminalpolizeilichen Aktennachweis (KAN)
- Speicherungen von erhobenen erkennungsdienstlichen Unterlagen.

Die meisten Bürgeranfragen betreffen Speicherungen im **KAN**: Entweder wird die Zulässigkeit der Speicherung an sich in Frage gestellt oder die Anfragen betreffen Vorgänge, die viele Jahre oder teilweise Jahrzehnte zurückliegen. Nach Art. 6 BayDSG kann sich zwar jedermann an den Landesbeauftragten für den Datenschutz mit dem Vorbringen wenden, bei der Verarbeitung seiner personenbezogenen Daten durch öffentliche Stellen würden seine schutzwürdigen Belange beeinträchtigt. Grundsätzlich kann sich jeder Bürger unmittelbar an den Datenschutzbeauftragten wenden, ohne vorher die speichernde Behörde um Auskunft gebeten zu haben. Wenn sich der Anfragende jedoch nicht sicher ist, ob bei einer Polizeibehörde überhaupt eine Speicherung stattgefunden hat, empfehle ich stets, sich zunächst an die örtlich zuständige Polizeidirektion oder das Bayerische Landeskriminalamt als Zentralstelle der bayerischen Polizei zu wenden und dort einen Antrag auf Auskunft zu stellen.

Zur Mehrzahl der Eingaben stelle ich fest, daß keine Speicherungen in polizeilichen Dateien oder Karteien bestehen, keine Kriminalakten vorhanden und die Befürchtungen der Petenten somit unbegründet sind. Wenn hingegen polizeiliche Ermittlungen gegen den Petenten geführt worden sind, prüfe ich Zulässigkeit und Richtigkeit der gespeicherten Daten. Auch in diesen Fällen habe ich **keine gravierenden Datenschutzverstöße** festgestellt. Allerdings rege ich manchmal an, die Daten früher als bisher vorgesehen zu löschen. Dem wird meist entsprochen.

Auch zur Speicherung von **erkennungsdienstlichen Unterlagen**, also zur Speicherung von Hinweisen auf aufgenommene Lichtbilder und Fingerabdrücke, habe ich im Berichtszeitraum einige Anfragen erhalten. Das BLKA hat in diesen Fällen nach entsprechendem Antrag des Betroffenen die Dateispeicherungen gelöscht und die erkennungsdienstlichen Unterlagen und die hierfür angelegten Akten vernichtet. Dies wird dem Antragsteller mitgeteilt. Wendet sich daraufhin der Antragsteller an mich mit der Bitte diese Vernichtung nachzuprüfen, führe ich beim BLKA eine entsprechende Prüfung durch.

5.5 Prüfungen

Prüfungen habe ich im Berichtszeitraum bei folgenden Polizeibehörden vorgenommen:

Landeskriminalamt
Polizeipräsidium Niederbayern/Oberpfalz
mit Polizeidirektion Passau
Polizeipräsidium Mittelfranken
mit den Polizeidirektionen Erlangen und Schwabach
Polizeipräsidium Unterfranken
mit den Polizeidirektionen Würzburg und Schweinfurt
Polizeipräsidium Schwaben
mit den Polizeidirektionen Augsburg und Dillingen
Polizeipräsidium München
Grenzpolizeiinspektion Hof
mit der Grenzpolizeistation Rudolfstein/Autobahn.

Gegenstand dieser größtenteils mehrtägigen generellen Prüfungen am Ort der Dienststelle sind **automatisierte Verfahren**, wie beispielsweise der Kriminalaktennachweis (KAN), aber auch **Karteien** herkömmlicher Art wie die

Staatsschutzkarteien. Die Zulässigkeit der Datenverarbeitung wird anhand von Stichproben unter Beiziehung der Akten geprüft.

Ich lege bei meinen Prüfungen Wert auf die Anwesenheit kompetenter Ansprechpartner, die meine Forderungen und Anregungen aus den geprüften Vorgängen später generell umsetzen können. Vereinzelt festgestellte, offensichtliche Fehler können bei dieser Verfahrensweise sofort korrigiert werden.

5.5.1 Polizeilicher Kriminalaktennachweis (KAN)

Neben dem polizeilichen Fahndungssystem, das alle zur Festnahme ausgeschriebenen Straftäter enthält (Fahndungsdaten), ist der KAN ein weiterer wesentlicher Teil des der bayerischen Polizei zur Verfügung stehenden Informationssystems. Der KAN enthält **Hinweise** auf die **Polizeidienststellen**, die **Kriminalakten** zu einer bestimmten **Person** führen. Bürgereingaben betreffen zumeist Speicherungen in dieser Datei oder eine Kriminalakte, über deren Bestand ein Nachweis im KAN geführt wird. Die Führung einer Kriminalakte über einen Bürger und die Speicherung im KAN sowie die Nutzung dieser Speicherung bedeuten einen erheblichen Eingriff in das informationelle Selbstbestimmungsrecht. Aus diesem Grund werden auch künftig weiterhin regelmäßige Prüfungen dieser Datei notwendig sein.

Die bereits eingangs erwähnte Tendenz zu **polizeiinternen Datenschutzprüfungen** hat ganz generell zu einer deutlichen **Verbesserung der Datenqualität im KAN** geführt. Behördliche Datenschutzbeauftragte und Verantwortliche für den KAN greifen aufgrund früherer Tätigkeitsberichte erkannte fehlerträchtige Bereiche selbst heraus und prüfen die Zulässigkeit der Speicherung im Einzelfall.

Die Speicherung von **Kindern und alten Menschen**, die in den ersten Jahren des KAN teilweise auf erhebliche datenschutzrechtliche Bedenken gestoßen war, entspricht nunmehr den bestehenden Regelungen. Ich habe deshalb mein Hauptaugenmerk beim KAN auf andere Bereiche gelegt:

Speicherungsebenen im KAN

Sog. „KAN-Merker" bewirken, daß Speicherungen nicht nur bayernweit, sondern bundesweit, also von jeder bundesdeutschen Polizeidienststelle abgefragt werden können. Die Zulässigkeit dieses Merkers ist deshalb auf das Zutreffen weniger, in polizeilichen Weisungen abschließend definierter Kriterien beschränkt. **Schwierigkeiten in der Auslegung** bestehen beispielsweise noch hinsichtlich der Begriffe „gewohnheitsmäßige Tatbegehung" und „gewerbsmäßige Tatbegehung". Wie bereits in den Vorjahren festgestellt, sind immer noch Bagatelldelikte wie Ladendiebstähle oder Sachbeschädigungen durch Verwendung dieser Merker bundesweit abfragbar. Eine Person, die wiederholt Ladendiebstähle begangen hat, stiehlt noch nicht automatisch „gewohnheitsmäßig". Eine Person, die sich durch eine Straftat einen materiellen Vorteil verschafft hat, handelt noch nicht unbedingt „gewerbsmäßig", sondern erst, wenn sie mit diesen Straftaten ihren Lebensunterhalt bestreitet. Manche Fehler werden erst nach genauerem Nachdenken nachvollziehbar, wie beispielsweise ein „gewerbsmäßiger Zechbetrug" oder eine „gewerbsmäßige Verletzung der Unterhaltspflicht". Auch scheidet z.B. eine „gewohnheitsmäßige" Begehung von Fahrlässigkeitsdelikten, wie beispielsweise eine fahrlässige Körperverletzung, begrifflich aus.

Sonstige polizeiliche Gefahrenabwehr

Unter diesen Begriff fällt die Speicherung von Sachverhalten, in denen die Polizei nach der ihr gesetzlich zugewiesenen Aufgabe der Gefahrenabwehr oder auf Grund anderer, neben der Strafverfolgung oder der Verfolgung von Ordnungswidrigkeiten zugewiesener gesetzlicher Aufgaben tätig geworden ist, und sie auf Grund bestimmter Tatsachen annehmen kann, daß die Person erneut „polizeilich" in Erscheinung treten wird. Dieser Bereich führt häufiger als andere zu Beanstandungen. Fehler sind beispielsweise:

- Speicherung der Vernehmung eines Zeugen. Polizeiliches Tätigwerden für eine andere Polizeidienststelle führt regelmäßig zu unzulässiger Doppelspeicherung.

- Speicherung des Vollzugs eines Haftbefehls. Die Verhaftung einer zur Festnahme ausgeschriebenen Person gehört nicht in den Nachweis von Kriminalakten. Die Speicherung der Verhaftung im KAN würde regelmäßig zu einer Doppelspeicherung führen.

- Wird beim Abschluß der Ermittlungen festgestellt, daß keine Straftat vorliegt, und keine Gefahr für die öffentliche Sicherheit und Ordnung zu befürchten ist, so dürfen Unterlagen nicht im KAN als Nachweis für ein polizeiliches Tätigwerden unter dem Begriff „sonstige polizeiliche Gefahrenabwehr" nachgewiesen werden.

- Wird eine vormals verdächtige Person rechtskräftig ohne Restverdacht von einem Schuldvorwurf freigesprochen, so sind polizeiliche Ermittlungsunterlagen aus der kriminalpolizeilichen Aktensammlung zu entfernen und entsprechende Eintragungen im KAN zu löschen. Keinesfalls darf eine weitere Aufbewahrung/Speicherung unter dem Begriff sonstige polizeiliche Gefahrenabwehr vorgenommen werden. Gleiches gilt für Verfahrenseinstellungen nach § 170 Abs. 2 Strafprozeßordnung und § 47 Ordnungswidrigkeitengesetz, wenn jeder Verdacht entfallen ist.

Personengebundene Hinweise

Unter dieser Bezeichnung bestehen im KAN besondere Hinweise auf Personen, wenn sie
- zur Eigensicherung der Polizeibeamten,
- zur Einleitung polizeilicher Fahndungen,
- zur Unterstützung polizeilicher Ermittlungen, aber auch
- zum Schutz der betroffenen Person bei polizeilichen Maßnahmen

erforderlich sind.

In den überwiegenden Fällen habe ich bei meinen Prüfungen nach Akteneinsicht die Berechtigung dieser Hinweise bestätigt gefunden. Beanstandungen habe ich beispielsweise ausgesprochen, wenn ein Hinweis auf einen „bewaffneten Straftäter" gespeichert wurde, obwohl dieser die Waffe bei Begehung der Straftat nicht verwendet hatte. Dies ist nach den polizeieigenen Vergabekriterien Voraussetzung für die Speicherung dieses personengebundenen Hinweises.

Prüffristen gespeicherter Daten

Alle im KAN gespeicherten Daten sind nach bestimmten Zeiträumen auf Aussonderung zu prüfen. Bei Kindern, Jugendlichen und Personen über 70 Jahren sieht bereits die Errichtungsanordnung die Vergabe verkürzter Fristen vor. In Fällen von geringer Bedeutung, zu denen auch Antrags- oder Fahrlässigkeitsdelikte, Bagatelldelikte oder Ordnungswidrigkeiten gehören können, muß die Aussonderungsprüfung ebenfalls grundsätzlich nach **kürzerer Frist** erfolgen. Die Einhaltung der vom Sachbearbeiter vergebenen verkürzten Fristen wird automatisch überwacht. Die Löschung kann also nicht mehr „vergessen" werden.

Beanstandungen in diesem Bereich sind zwar die Ausnahme. Allerdings rate ich den Polizeibehörden, ihren Ermessensspielraum bei der Festlegung der Speicherungsdauer stärker als bisher auszunutzen und von der Möglichkeit der Fristverkürzung mehr Gebrauch zu machen.

Berücksichtigung des Verfahrensausgangs

Neben der Löschung von KAN-Daten und der Vernichtung der dazugehörenden Unterlagen wegen Fristablaufs sind Daten dann zu löschen, wenn ein Gericht durch rechtskräftiges Urteil die **Unschuld** des Angeklagten festgestellt hat oder sich auf andere Weise im weiteren Verfahren die Unschuld des Betroffenen herausstellt. Die Löschung setzt voraus, daß die ermittelnde Polizeibehörde **vom Ausgang des Ermittlungsverfahrens Kenntnis** erhält. Um dies zu ermöglichen, übersendet die Polizei an die Staatsanwaltschaft zusammen mit dem Ergebnis der polizeilichen Ermittlungen ein sogenanntes Strafnachrichtenblatt. Die Staatsanwaltschaft ist verpflichtet, der Polizei den Verfahrensausgang mitzuteilen. Trotzdem stelle ich bei meinen Prüfungen immer wieder fest, daß auch in Fällen, in denen die Ermittlungen schon Jahre zurückliegen, der Ausgang des Verfahrens nicht bekannt ist.

Ganz allgemein gilt, daß die Rechtmäßigkeit der Führung einer kriminalpolizeilichen Akte abschließend erst geprüft werden kann, wenn der Verfahrensausgang bekannt ist. So kann nach Kenntnis des Verfahrensausgangs eine Verkürzung der Aussonderungsprüffrist oder eine Änderung in der Bezeichnung der dem Betroffenen zur Last gelegten Straftat oder die Speicherung in einer anderen KAN-Ebene veranlaßt sein. Stelle ich Fälle fest, bei denen der Verfahrensausgang nicht bekannt ist, so lasse ich diesen ermitteln und prüfe danach die Zulässigkeit der Speicherung.

5.5.2 Polizeipräsidium München

In den vergangenen Jahren habe ich bei meinen Prüfungen des Polizeipräsidiums München mehr als bei anderen Polizeipräsidien Datenschutzdefizite festgestellt, über die ich in meinen früheren Tätigkeitsberichten berichtet habe.

Nunmehr betreibt das Polizeipräsidium München die Datenerfassung aus **Altakten** in den automatisierten Kriminalaktennachweis mit Nachdruck. Alle Altakten sollen bis Ende 1990 überprüft sein. Ziel des Polizeipräsidiums ist es ferner, die kriminalpolizeilichen Vorgänge von Vorgängen zu trennen, die der bloßen Dokumentation des polizeilichen Tätigwerdens dienen, im KAN aber die Bürger unnötig belasten könnten. Außerdem sollen diejenigen Vorgänge ausgesondert und vernichtet werden, deren Aufbewahrung nach den Richtlinien für die Errichtung und Führung kriminalpolizeilicher personenbezogener Sammlungen (KpS) nicht mehr zulässig ist. Bereits jetzt zeichnet sich ab, daß diese Überprüfung zu einer wesentlichen **Reduzierung des Kriminalaktenbestandes** führen wird.

Da diese Überarbeitung des Altaktenbestandes und die Datenerfassung im KAN gegenwärtig mit Nachdruck betrieben werden, habe ich dieses Jahr wiederum eine mehrtägige Prüfung beim Polizeipräsidium München durchgeführt. Es war erklärtes Ziel dieser Überprüfung, etwaige Erfassungs-, Bewertungs- und Systemfehler möglichst frühzeitig zu erkennen, um diese gegebenenfalls rechtzeitig abstellen zu können.

Die Prüfung der **Kriminalakten** hat das grundsätzliche Bemühen des Polizeipräsidiums München um Beachtung des Datenschutzes bestätigt.

Zum Teil erhebliche Mängel weist hingegen noch der **Kriminalaktennachweis** auf. Eine falsch übertragene Schlüsselzahl führte zum Beispiel dazu, daß an sich auf Bayern zu beschränkende Dateispeicherungen bundesweit abfragbar waren. Da der Fehler zeitlich begrenzt war und nur bestimmte Fälle betraf, konnte er durch eine manuelle Überprüfung aller in Frage kommenden Datensätze bereinigt werden.

Zu beanstanden sind die noch recht zahlreichen Bewertungsfehler: Immer wieder werden die sog. KAN-Merker (z.B. „gewerbsmäßige" Tatbegehung) trotz eindeutiger Definition in polizeilichen Dienstanweisungen zu Unrecht gesetzt, und damit Vorgänge unnötig bundesweit abrufbar.

Die Zahl der Speicherungen unter dem Begriff „sonstige polizeiliche Gefahrenabwehr" war zu hoch. Es waren zahlreiche Vorgänge gespeichert, die nicht unter diesen Begriff fallen. Probleme bestehen auch bei der Prüfung der Relevanz einer Straftat oder deren Einordnung unter den richtigen Straftatbestand. In zu vielen Fällen, selbst bei kleinsten Bagatelldelikten (Ladendiebstahl im Wert von wenigen DM), wurde die Regelaussonderungsfrist von zehn Jahren vergeben. Letztlich geschehen auch zu viele Erfassungsfehler, also Fehler bei der Übertragung der Daten aus Erfassungsformblättern in den KAN. Weitere organisatorische Maßnahmen in diesem Bereich, insbesondere eine nachhaltige **Schulung** und **Kontrolle des Personals** sind dringend erforderlich.

Für die **Karteien** bestehen inzwischen sog. Feststellungsanordnungen. Sie enthalten neben Hinweisen auf Rechtsgrundlagen für die Karteiführung auch eine Zweckbeschreibung, regeln den aufzunehmenden Personenkreis und die vorgesehene Dauer der Karteispeicherung. Nach diesen Anordnungen sind Karteien mindestens einmal pro Jahr auf auszusondernde und zu vernichtende Daten zu prüfen. Meine Stichproben haben bestätigt, daß diese Prüfungen tatsächlich durchgeführt werden.

Weiterhin habe ich mehrere **SPUDOK-Dateien** geprüft, die nicht für einzelne polizeiliche Ermittlungsverfahren, sondern zur Erledigung bestimmter polizeilicher Aufgaben genutzt wurden. Teilweise waren hier polizeiliche Karteien aufgelöst und in Dateiform weitergeführt worden. Beispiel einer solchen Datei ist die **Datei „Prostitution"**: Die vormalige „Personenkartei Prostitution" ist überarbeitet worden und wird nun in Dateiform fortgeführt. Ein Teil der personenbezogenen Daten konnte wegen „Inaktualität" vernichtet werden, obwohl die an sich zulässige Aufbewahrungsdauer

noch nicht abgelaufen war. In einigen Fällen habe ich beanstandet, daß das Datum, an dem eine Aussonderungsprüfung vorgenommen werden muß, in der Datei in der Weise automatisch vorgegeben worden ist, daß das Datum der Speicherung — und nicht das des **Zeitpunkts des maßgeblichen Ereignisses** — entscheidend für den Fristbeginn war. Dies führte insbesondere bei der Erfassung von Jahre zurückliegenden Fällen zu falschen Fristsetzungen. Aussonderungsprüffristen müssen stets auf den Einzelfall bezogen festgelegt werden. Dies gilt auch bei der Übernahme bestehender Karteien in Dateien. Bereits in der Kartei bestehende Aussonderungsprüffristen müssen beachtet und in der Datei übernommen werden. Inzwischen sind die Fehler bei der Fristberechnung behoben, so daß eine Beeinträchtigung der schutzwürdigen Belange der von der Dateispeicherung Betroffenen verhindert ist.

5.5.3 Bayerisches Landeskriminalamt

Nach Art. 7 des Gesetzes über die Organisation der Bayerischen staatlichen Polizei (POG) ist das Bayerische Landeskriminalamt (BLKA) die zentrale Dienststelle Bayerns für kriminalpolizeiliche Aufgaben. Es ist weiterhin Zentralstelle für die polizeiliche Datenverarbeitung und Datenübermittlung in Bayern und Fernmeldeleitstelle für die polizeiliche Nachrichtenübermittlung. Ihm obliegt es außerdem, z.B. „Nachrichten und Unterlagen für die Verhütung und polizeiliche Verfolgung von Straftaten zu sammeln und auszuwerten und über die Aufbewahrung solcher Unterlagen bei der Polizei für den Einzelfall zu entscheiden". Diese Feststellungen unterstreichen die Bedeutung des BLKA für die polizeiliche Datenverarbeitung und den Datenschutz. Seit Jahren führe ich dort regelmäßige Kontrollen durch. Nicht zuletzt durch meine häufigen Kontakte mit dem BLKA im Rahmen von Prüfungen, Stellungnahmen zu EDV-Vorhaben, aber auch durch Bürgereingaben, sind dort zahlreiche organisatorischen Maßnahmen getroffen worden, die **vernünftig umgesetzter Datenschutz** erfordert. Einzelne festgestellte Fehler lagen wiederum in der menschlichen Unvollkommenheit begründet. Erfassungsfehler, Unkenntnis des einzelnen von bestehenden Vorschriften, aber auch fehlerhafte Ermessensentscheidungen sind zwar letztlich niemals auszuschließen, müssen jedoch stets Ansporn sein, nach weiteren Lösungen zu suchen, um Fehler künftig zu vermeiden.

Prüfungsschwerpunkte meiner diesjährigen mehrtägigen Prüfung beim BLKA waren folgende Bereiche der polizeilichen Datenverarbeitung:

- Arbeitsdatei PIOS innere Sicherheit (APIS) der Staatsschutzabteilung des BLKA
- Aktenhaltung, Kriminalaktennachweis (KAN) und Haftdaten des BLKA
- Arbeitsdatei PIOS organisierte Kriminalität (APOK)
- SPUDOK-Datei „Sondermeldedienst Umweltdelikte".

Arbeitsdatei PIOS innere Sicherheit (APIS)

Die Datei APIS soll als Hilfsmittel zur Verhütung und Aufklärung von Straftaten mit staatsfeindlicher Zielsetzung dienen. Diese Datei habe ich unter verschiedenen Gesichtspunkten wiederum einer stichprobenartigen Prüfung unterzogen. Meine Prüfungsfeststellungen haben zu folgenden Forderungen geführt:

- Die im Einzelfall festgesetzte **Aussonderungsprüffrist** muß anhand polizeilicher Erkenntnisse nachvollziehbar sein. Das ist für APIS entweder das Vorliegen einer konkreten Straftat oder das Vorliegen eines konkreten Verdachts einer Straftat. Die Tatsache des Ablaufs eines Beobachtungszeitraumes, in dem keine strafrechtlich relevanten Erkenntnisse zur Person des Beobachteten angefallen sind, darf nicht Anlaß für eine erneute Speicherung sein.

- In mehreren Fällen habe ich festgestellt, daß dem Landeskriminalamt der **Verfahrensausgang** nicht bekannt war, obwohl die zugrunde liegende Straftat bereits länger zurücklag. Hier muß der Informationsaustausch zwischen Staatsanwaltschaft, örtlicher Kriminalpolizei und Landeskriminalamt verbessert werden.

- Liegen nach Kenntnisnahme von einer **Verfahrenseinstellung** (nach § 170 Abs. 2 StPO) keine konkreten Verdachtsmomente mehr vor, sind die Daten zu löschen. Eine Speicherung in APIS ist von vorneherein unzulässig, wenn die Meldung an das Landeskriminalamt ausdrücklich besagt, daß kein Anhaltspunkt besteht, daß die genannte Person in irgendeiner Weise an einer konkreten Straftat mit Staatsschutzbezug beteiligt war.

- Die **Personalien** der gespeicherten Personen müssen eindeutig festgestellt sein. Sind nur die Kfz-Kennzeichen bekannt, so wird durch eine bloße Halterfeststellung ohne zusätzliche Überprüfung kein ausreichender Identitätsnachweis geführt, der eine Speicherung in APIS rechtfertigt. Denn der Halter muß nicht mit dem Benutzer des Kfz bei einer bestimmten Aktion identisch sein.

- Soweit Daten von **„Gefährdeten"** und **„Geschädigten"** in APIS gespeichert werden, ist besonders zu prüfen, ob eine Speicherung in APIS in jedem Einzelfall erforderlich ist. Hierbei ist die Ernsthaftigkeit einer „Gefährdung" zu berücksichtigen. Eine ausdrückliche Einwilligung zur Datenspeicherung unter dem Begriff „gefährdet" ist insbesondere bei Journalisten erforderlich, wenn keine Schutzmaßnahmen angezeigt waren oder sie keiner Gefährdungsstufe zugeordnet wurden.

- Gerade vor einer Speicherung in APIS ist die **Prüfung der Relevanz in staatsschutzrechtlicher Sicht** notwendig. Daran bestehen Zweifel, wenn es sich bei einem Vorgang offensichtlich um eine regionale Demonstration wegen eines Problems mit eindeutig regionalem Charakter, etwa einer Mülldeponie, handelt und die beteiligten Bürger zumeist Einwohner anliegender Ortschaften sind. Ein staatsschutzrelevantes Motiv im Sinne der APIS-Errichtungsanordnung läßt sich in solchen Fällen selbst bei Ermittlungen wegen Nötigung durch die Blockade von Zufahrtswegen nicht ohne weiteres annehmen.

- Speichernde Stelle bei APIS und damit für die Richtigkeit der Datenverarbeitung verantwortlich ist hinsichtlich der bayerischen APIS-Daten das Bayerische Landeskriminalamt. Um dieser Verantwortung gerecht zu werden, muß das BLKA die eingehenden Meldungen der Staatsschutzdienststellen vor ihrer Speicherung in APIS darauf überprüfen, ob die Voraussetzungen für eine APIS-Speicherung zumindest schlüssig aus ihnen hervorgehen. Das setzt aber voraus, daß die Meldungen der Staatsschutzdienststellen so vollständig sind, daß sie eine eindeutige **Plausibilitätsprüfung** ermöglichen. Un-

berührt davon bleibt die Pflicht der Staatsschutzdienststellen, das Landeskriminalamt von wesentlichen Änderungen in der Sach- und Rechtslage in APIS gespeicherter Vorgänge zu unterrichten.

Unter der Überschrift APIS habe ich im 10. Tätigkeitsbericht auch über die Speicherung von straffällig gewordenen Volkszählungsboykotteuren berichtet. Mit der Löschung aller Datenspeicherungen im Zusammenhang mit der Volkszählung aus der Staatsschutzdatei APIS durch das BLKA am 12.12.1988, also kurz nach Drucklegung meines 10. Tätigkeitsberichts, fanden die Verhandlungen zu diesem Thema ihren Abschluß: Aus polizeilicher Sicht war die „Volkszählung 87" abgeschlossen. Weiter war die Polizei davon ausgegangen, daß ähnliche Vorgänge in absehbarer Zeit nicht bevorstehen. Es bestand deshalb keine Notwendigkeit mehr, die Daten der hier wegen Straftaten erfaßten Personen weiter zu speichern. Eine vorzeitige Löschung sämtlicher im Zusammenhang mit der Volkszählung erfaßten Personendaten und Erkenntnisse wurde vorgenommen. Ich werte dies als Erfolg meiner ständigen Bemühungen, Polizeibehörden im Blick auf die Einhaltung des Datenschutzes frühzeitig zu beraten.

Kurzfristig habe ich im November 1989 die Datei APIS auf mögliche Speicherungen von Namen und Daten der **Gegner von Müllverbrennungsanlagen** und Deponien geprüft. Ich habe dabei festgestellt, daß im APIS-Bestand des BLKA keine derartige Speicherung besteht.

Arbeitsdatei PIOS — Organisierte Kriminalität (APOK)

Diese Datei dient der Aufklärung sowie der vorbeugenden Bekämpfung von Straftaten der organisierten Kriminalität. Mit Hilfe der Datei werden polizeiliche Erkenntnisse und Informationen aus „organisationsverdächtigen" Kriminalitätsbereichen **geordnet, sortiert** und **ausgewertet**. Bereits vor zwei Jahren habe ich die Datei kurz geprüft. Damals waren erst wenige Daten gespeichert, da mit der Erfassung erst kurz vorher begonnen worden war.

Bei dieser Datei handelt es sich um eine sog. Verbunddatei. Dies bedeutet, daß alle Bundesländer in einer gemeinsamen Datei nach gleicher Dateistruktur Daten speichern, und jedes Bundesland für den Inhalt des eigenen Datenbestandes sowohl sachlich als auch rechtlich — und somit auch datenschutzrechtlich — verantwortlich ist. Ein zahlenmäßiger Vergleich der Dateibestände der verschiedenen Bundesländer zeigt, daß in Bayern bei der Bewertung von Sachverhalten hinsichtlich organisierter Kriminalität zurückhaltend vorgegangen wird.

Trotz einer Anzahl von Stichproben mit Einsichtnahme in dazugehörende Unterlagen bestanden in keinem Fall aus datenschutzrechtlicher Sicht Zweifel an der Zulässigkeit der Erfassung. Z.B. wird die Unterscheidung zwischen Beschuldigten- und Verdächtigeneigenschaft durch Verwendung entsprechender Begriffe in der Datei klar getroffen. Sie läßt sich durch die dazugehörenden Ermittlungsergebnisse belegen.

Sondermeldedienst Umweltdelikte

In der SPUDOK-Datei „Sondermeldedienst Umweltdelikte" speichert das BLKA Meldungen von Polizeibehörden über Umweltstraftaten, um „Tatbrennpunkte" und „Tat- und Täterzusammenhänge" zu erkennen und einen landesweiten Überblick über die Umweltkriminalität zu erhalten. Die Datenspeicherung betrifft nur Beschuldigte im Rahmen eines strafrechtlichen Ermittlungsverfahrens und Verdächtige. Die Erfassung beim BLKA erfolgt nach klaren und übersichtlichen Arbeitsanweisungen; die Löschung der Daten ist regelmäßig, spätestens nach fünf Jahren durchzuführen.

Besonderer Beachtung habe ich bei meiner Prüfung der **Relevanz** der vom BLKA gespeicherten Straftaten für den Zweck der Sonderdatei beigemessen. Eine Verunreinigung der Umwelt, ohne daß ein Straftatbestand erfüllt ist, z.B. ein bloßer Verkehrsunfall, bei dem Benzin, Diesel oder Öl das Erdreich verunreinigen oder wenn spielende Kinder ein Ölfaß umstoßen, erfüllt allein noch nicht die Voraussetzungen zur Speicherung in dieser Datei. Hinzukommen muß, daß neben den sonstigen Voraussetzungen für das Vorliegen einer Umweltstraftat der Täter zumindest fahrlässig ein „Umweltdelikt" begangen hat.

Ich habe das BLKA aufgefordert, aus seiner Verantwortung als speichernde Stelle noch kritischer als bisher die Speicherungsvoraussetzungen zu prüfen und zumindest in Zweifelsfällen bei den sachbearbeitenden Dienststellen weitere Informationen einzuholen.

Speicherung von HIV-Infektionen in polizeilichen Informationssystemen

Auf die Voraussetzungen, unter denen ich keine datenschutzrechtlichen Bedenken gegen die Speicherung des personengebundenen Hinweises (PHW) „ANST" (Ansteckungsgefahr) mit dem Zusatz „Vorsicht Blutkontakte" habe, bin ich bereits im 10. Tätigkeitsbericht ausführlich eingegangen.

Die Voraussetzungen einer Speicherung in INPOL hatte ich wie folgt zusammengefaßt:

- Der Betroffene ist bereits in Fahndungsdateien oder im Kriminalaktennachweis gespeichert.
- Nach Sachlage bestehen aus polizeilicher Sicht Anhaltspunkte dafür, daß der Betroffene strafrechtlich oder anderweitig „polizeilich" in Erscheinung treten wird, und die Polizei bei ihren Ermittlungen und sonstigen Maßnahmen im Hinblick auf die HIV-Infektion Vorkehrungen treffen muß.
- Die HIV-Infektion ist ärztlich nachgewiesen.
- Die Polizei hat von der Tatsache der HIV-Infektion in zulässiger Weise Kenntnis erlangt.
- Die für die Speicherung des Hinweises auf die HIV-Infektion verantwortliche Stelle muß erkennbar sein.

Im Berichtszeitraum habe ich die Speicherungen unter dem PHW „ANST" beim Bayer. Landeskriminalamt (BLKA) geprüft.

Das BLKA führt zwar einen nach meinen Feststellungen lückenlosen Nachweis aller von bayerischen Polizeidienststellen veranlaßten und von ihm eingegebenen Speicherungen dieses personengebundenen Hinweises. Allerdings ließen die Meldungen der Polizeidienststellen in zahlreichen Fällen nicht den eindeutigen Schluß zu, daß die Speicherungsvoraussetzungen tatsächlich erfüllt sind. Somit waren die Unterlagen in diesen Fällen zur **Nachprüfung der Plausibilität der Speicherungsvoraussetzungen** nicht geeignet. Weil die Datenerfassung dieses besonders brisanten personengebundenen Hinweises für die bayerischen Poli-

zeibehörden (mit wenigen Ausnahmen) zentral vom BLKA vorgenommen wird, habe ich gefordert, daß die Zulässigkeit einer Speicherung im Einzelfall durch Prüfung der Voraussetzungen nicht nur bei der sachbearbeitenden Stelle, sondern in Form einer Plausibilitätskontrolle **auch** beim BLKA erfolgen soll. Dadurch wird ein doppelter Schutz vor unzulässiger Speicherung erreicht. Auf jeden Fall muß vermieden werden, daß sich sachbearbeitende Stelle und BLKA bei der Prüfung der Eintragungsvoraussetzungen aufeinander verlassen und eine vollständige Prüfung so letztlich unterbleibt.

5.6 Karteien

Staatsschutzkarteien

Auch in diesem Berichtszeitraum habe ich Staatsschutzkarteien geprüft. Bei den geprüften Polizeipräsidien bestehen **Feststellungsanordnungen**, also Anweisungen, die Zweck, Umfang, Inhalt, zulässige Übermittlungen und Aufbewahrungsdauer der Daten enthalten. Die Polizeipräsidien haben einer Empfehlung des Staatsministeriums des Innern Folge geleistet und dem polizeilichen Staatsschutzsachbearbeiter **klare Arbeitsanweisungen** für die Nutzung dieser Karteien an die Hand gegeben. Erfreulicherweise führten diese Anweisungen dazu, daß alle geprüften Staatsschutzkarteien zwischenzeitlich überarbeitet worden waren. Diese Überarbeitung hat in allen Fällen zu einer erheblichen Reduzierung des Karteibestandes geführt. Eine klare Trennung zwischen polizeilichen Erkenntnissen einerseits und Maßnahmen im präventiven (vorbeugenden) und im repressiven (strafverfolgenden) Bereich des polizeilichen Staatsschutzes andererseits wurde hiermit vorgenommen. Auch hat die Festlegung von Aussonderungsfristen dazu geführt, daß einige teilweise Jahre zurückliegende Informationen vernichtet worden sind. Diese polizeilichen Maßnahmen hatten zur Folge, daß die Zahl der von mir festgestellten Fehler gegenüber früheren Jahren deutlich abgenommen hat.

Die Polizeibehörden berichten im übrigen übereinstimmend, daß durch die Reduzierung der Karteibestände auf relevante und aktuelle Fälle eine effektivere Sachbearbeitung ermöglicht wurde.

Karteien in Fachkommissariaten

Bei größeren Kriminalpolizeibehörden sind für die Verfolgung einzelner Straftatenbereiche (z.B. Rauschgiftdelikte, Tötungsdelikte, Sexualstraftaten oder Staatsschutzdelikte) Fachkommissariate eingerichtet. Diese führen häufig Karteien oder automatisierte Dateien über Straftäter aus ihrem speziellen Zuständigkeitsbereich. Soweit in diesen Dateien Informationen zu Strafverfahren geführt werden, hat sich deren **Aussonderungsprüffrist** regelmäßig an der Frist zu bemessen, die der entsprechende Vorgang im kriminalpolizeilichen Aktennachweis (KAN) erhalten hat. Bei meinen Prüfungen lege ich Wert auf die Feststellung, daß sich in diesen Fällen aus der Kriminalakte ein **Hinweis** ergeben muß, daß bei der Fachdienststelle weitere Erkenntnisse vorliegen. Nur hierdurch kann gewährleistet werden, daß beispielsweise bei vorzeitiger Aussonderung einer Kriminalakte bzw. bei vorzeitiger Löschung einer Eintragung im KAN auch die Fachdienststelle zur Löschung der dortigen Unterlagen aufgefordert werden kann.

5.7 Datenspeicherung in Zusammenhang mit der Wiederaufarbeitungsanlage Wackersdorf

Durch die Einstellung der Arbeiten an der Wiederaufarbeitungsanlage in Wackersdorf stellte sich auch aus datenschutzrechtlicher Sicht die Frage, welche Auswirkungen dieser Umstand auf Dateispeicherungen haben kann. Diese sind bei den vier in Frage kommenden Dateien unterschiedlich:

Soweit Speicherungen im kriminalpolizeilichen Aktennachweis (KAN) erfolgten, hat dies für die Betroffenen keine unmittelbaren Auswirkungen: Eine Speicherung im KAN wird nur bei Vorliegen oder Verdacht einer Straftat, letztlich unter Berücksichtigung des jeweiligen Ausgangs des Verfahrens (Urteil) vorgenommen. Wurde oder wird gegen einen Betroffenen ein Strafverfahren geführt, bleibt der Speicherungsgrund (der Verdacht einer Straftat) trotz Einstellung der Arbeiten zur Wiederaufarbeitungsanlage unverändert bestehen. Eine Löschung von Daten erfolgt im Einzelfall nach den generell geltenden Regelungen der KAN-Errichtungsanordnung.

Die SPUDOK-Datei des Bayer. Landeskriminalamtes, die zur **Ermittlung von überörtlich handelnden Tätern** und zur Unterstützung der Aufklärung von Straftaten des Landfriedensbruchs und schweren Landfriedensbruchs eingerichtet worden war, hat ihren Zweck erfüllt. Diese Ermittlungsverfahren konnten aus polizeilicher Sicht abgeschlossen werden. Die weitere Speicherung der Daten war nicht mehr erforderlich; die Datei ist zwischenzeitlich gelöscht worden.

Die SPUDOK-Datei der Polizeidirektion Amberg, eine sog. Ermittlungsdatei mit dem Zweck, strafrechtlich relevante Sachverhalte **zusammenzuführen**, die Bezug zur Wiederaufarbeitungsanlage in Wackersdorf haben, wird nach und nach gelöscht, wenn die polizeilichen Ermittlungsverfahren soweit abgeschlossen sind, daß im Einzelfall nicht mehr mit polizeilichen Ermittlungen gerechnet werden muß. Die Notwendigkeit der Datei wird halbjährlich von der dateiführenden Stelle geprüft und begründet. Eine Sperrung der Datei ist vorgesehen, sobald die polizeilichen Ermittlungsverfahren abgeschlossen sind.

Auch eine weitere SPUDOK-Datei, eine sog. **Ermittlungs- und Verwaltungsdatei** des Polizeipräsidiums Niederbayern/Oberpfalz, mit der Verwaltungsaufgaben der polizeilichen Einsatzleitung erledigt werden, die aber auch als polizeiliches Führungs- und Einsatzhilfsmittel genutzt wird, wurde nach und nach teilweise gelöscht. Die gesamte Datei ist auf Antrag des Polizeipräsidiums Niederbayern/Oberpfalz zum 1.12.1989 gesperrt worden.

5.8 Bayerische Grenzpolizei

Den Zweck des sog. **Grenzaktennachweises** (GAN) habe ich in meinem 10. Tätigkeitsbericht erläutert: Er dient als Nachweissystem der Bayer. Grenzpolizei über grenzpolizeiliche Vollzugsmaßnahmen und über Maßnahmen der grenzpolizeilichen Gefahrenabwehr. Die durchwegs positiven Ergebnisse bei der Prüfung des Grenzaktennachweises in den Vorjahren fanden sich auch 1989 bestätigt.

Die im GAN gespeicherten Daten sind gut dokumentiert, Entscheidungen, z.B. zur Speicherungsdauer, sind somit auch datenschutzrechtlich nachvollziehbar. Zumindest die geprüfte Grenzpolizeiinspektion (in Hof) hat sich auf die Speicherung von grenzpolizeilich relevanten Sachverhalten

beschränkt. So befinden sich im dortigen GAN keine Datensätze mit KAN-Merkern, personengebundenen Hinweisen oder Datensätze über Vermißtenfälle, „sonstige polizeiliche Gefahrenabwehr", Kinder oder Personen über 70 Jahre.

Eine Datengruppe innerhalb des GAN enthält Fälle der Überwachung des **grenzüberschreitenden Omnibus- und Lkw-Verkehrs**. Schwerwiegende Verstöße gegen Vorschriften zum Schutz der Sicherheit im Straßenverkehr, gegen das Güterkraftverkehrsgesetz, das Fahrpersonalgesetz und das Personenbeförderungsgesetz werden hier im GAN gespeichert. Meine Prüfungen haben ergeben, daß, wie dies in der Errichtungsanordnung vorgeschrieben ist, grundsätzlich nur **gravierende Verkehrsdelikte** erfaßt wurden. Vereinzelt habe ich festgestellt, daß bestimmte Vorgänge, für die eine auf zwei Jahre verkürzte Speicherungsdauer vorgesehen ist, mit fünfjähriger Frist versehen worden sind. Diese Fehler wurden umgehend behoben und lagen wohl in Anfangsschwierigkeiten bei der Erfassung in den GAN begründet.

6. Verfassungsschutz

Der Verfassungsschutz dient nach der ausdrücklichen Definition des Grundgesetzes dem „Schutze der freiheitlichen demokratischen Grundordnung, des Bestandes und der Sicherheit des Bundes oder eines Landes". Dem Verfassungsschutz ist deshalb gesetzlich die **Aufgabe** zugewiesen, Informationen über extremistische Bestrebungen und Spionageaktivitäten zu sammeln und auszuwerten. Hierzu gehört auch die Mitwirkung des Verfassungsschutzes bei der Überprüfung von Personen, die an sicherheitsempfindlichen Stellen beschäftigt sind oder denen besonders geheimhaltungsbedürftige Tatsachen anvertraut werden sollen. Damit ist jedenfalls die Tätigkeit des Verfassungsschutzes in erster Linie Erhebung und Verarbeitung personenbezogener Daten. Weil diese Tätigkeit im Einzelfall besonders stark in das Recht auf informationelle Selbstbestimmung eingreifen kann, sind für sie **klare gesetzliche Regelungen notwendig**. Diese sind derzeit in Vorbereitung (siehe 6.3). Außerdem muß in ganz besonderem Maße sichergestellt sein, daß die Datenerhebung und -verarbeitung des Verfassungsschutzes im Rahmen seiner Aufgabenzuständigkeit ablaufen und die einzelnen Daten richtig sind. Zur Richtigkeit der Datenverarbeitung gehört auch, daß diese durch ausreichende Unterlagen plausibel nachvollziehbar ist.

6.1 Bayerisches Landesamt für Verfassungsschutz

Wie in den Jahren zuvor haben auch im Berichtszeitraum beim Landesamt für Verfassungsschutz zahlreiche datenschutzrechtliche Prüfungen stattgefunden. Auch dieses Mal lag ein Schwergewicht auf der **Kontrolle von Einzelvorgängen**, die durch zahlreiche Eingaben von Bürgern veranlaßt waren.

In der überwiegenden Zahl der Fälle waren die Befürchtungen, bei Verfassungsschutzbehörden gespeichert zu sein, völlig unbegründet. Soweit ich in Einzelfällen Speicherungen vorgefunden habe, hat sich in keinem Fall Anlaß zu einer Beanstandung ergeben.

Allerdings konnte ich in manchen dieser Fälle den Erwartungen der Bürger nicht entsprechen. So, wenn es etwa Ziel einer Eingabe war, ein nachteiliges Votum des Landesamtes im Falle einer Sicherheitsüberprüfung abzuändern, jedoch die von mir vorgefundenen Tatsachen das Votum des Verfassungsschutzes zumindest plausibel erscheinen ließen.

Um unnötige Ängste der Bürger abzubauen, empfehle ich dringend, in mehr Fällen als bisher dem Bürger **Auskunft** zu erteilen über die Tatsache, ob über ihn etwas gespeichert ist und ggf. über den Informationsinhalt. Eine solche Transparenz ist geeignet, manches unnötige Mißtrauen gegenüber dem Verfassungsschutz abzubauen. Die Arbeit des Verfassungsschutzes leidet darunter keineswegs. Die Gefahr der Aushorchung und Ausspionierung besteht bei Anfragen nur selten: Meist sind es etwas überängstliche Bürger, die wissen wollen, ob sie vom Verfassungsschutz beobachtet werden.

6.2 Generelle Prüfung

Neben diesen Einzelkontrollen habe ich wiederum eine diesmal sich allerdings über mehrere Tage hinweg erstreckende generelle Prüfung durchgeführt.

Schwerpunkte dieser allgemeinen datenschutzrechtlichen Prüfung waren das nachrichtendienstliche Informationssystem (NADIS), die Abwicklung der Sicherheitsüberprüfungen für die Privatwirtschaft und die öffentliche Verwaltung sowie verschiedene weitere Karteien und Dateien.

6.2.1 NADIS

Wie in den Vorjahren hat die Prüfung von NADIS-Speicherungen keine wesentlichen Datenschutzverstöße erbracht. Die Speicherungen waren grundsätzlich für die Erfüllung der dem Landesamt zugewiesenen gesetzlichen Aufgaben erforderlich.

Allerdings bereitet die Festlegung des **für die Aussonderungsfrist maßgeblichen Datums** weiterhin Schwierigkeiten. Es ist nicht eindeutig und verbindlich definiert und wird deshalb innerhalb der verschiedenen Sachgebiete des Landesamtes nicht einheitlich gehandhabt. Ich habe das Landesamt aufgefordert, für eine einheitliche, an der letzten relevanten Erkenntnis ausgerichteten Vergabe dieses Datums Sorge zu tragen.

Der Nachweis über die Abwicklung von Verwaltungsvorgängen, wie etwa die Beantwortung von Anfragen, sollte grundsätzlich nicht im NADIS, sondern ausschließlich in den entsprechenden Registrierungsunterlagen vorgenommen werden.

6.2.2 Sicherheitsüberprüfungen

Im Jahr 1988 sind neue Richtlinien für die Überprüfung von Personen im Rahmen des **Geheimschutzes** in Kraft getreten. Meine Prüfung der Handhabung der neuen Sicherheitsrichtlinien hat gezeigt, daß die Sicherheitsüberprüfungen aus datenschutzrechtlicher Sicht korrekt abgewickelt werden. Die notwendigen Maßnahmen des Landesamtes für Verfassungsschutz werden auch vollständig und übersichtlich dokumentiert, was die Kontrolle wesentlich erleichtert. Dieses erfreuliche Ergebnis der Anwendung der Sicherheitsrichtlinien entbindet den Gesetzgeber jedoch nicht von der Notwendigkeit, die Rechtsgrundlagen für Sicherheitsüberprüfungen im Bereich des Geheimschutzes zu verbessern.

Für die Sicherheitsüberprüfungen in der **Privatwirtschaft** ist seit Mai 1989 eine bayernweit einheitliche „Einverständniserklärung" zu verwenden. Diese Erklärung ist aus datenschutzrechtlicher Sicht hinreichend klar formuliert. Der zu Überprüfende unterzeichnet sie **vor** Einleitung des Überprüfungsverfahrens. Meinem Wunsch entsprechend enthält sie auch einen Hinweis auf das Recht zur Anrufung des Bayerischen Landesbeauftragten für den Datenschutz.

Meine Kontrolle aller im Jahre 1989 durchgeführten Sicherheitsüberprüfungen, bei denen vom Landesamt Sicherheitsbedenken geäußert worden waren, erbrachte in keinem Fall gravierende Verstöße gegen datenschutzrechtliche Bestimmungen. Ich habe das Landesamt allerdings gebeten, in den internen Unterlagen noch deutlicher herauszustellen, **aufgrund welcher Tatsachen** im jeweiligen Einzelfall Sicherheitsbedenken geäußert werden. Als weitere Verbesserungen habe ich angeregt:

- genauere Beschreibung der vorgesehenen Verwendung des zu Überprüfenden;
- Aktualisierung der Liste von Firmen, an deren Sicherheitsüberprüfung das Landesamt mitwirken soll;
- vor einer Sicherheitsüberprüfung durch das Landesamt sollten alle übrigen Einstellungsvoraussetzungen erfüllt sein;
- klare Dokumentation des Inhalts der dem Sicherheitsbeauftragten der anfragenden Firma mitgeteilten Auskünfte.

6.2.3 Karteien

Die Einrichtung und Führung personenbezogener Karteien beim Landesamt für Verfassungsschutz setzt klare Arbeitsanweisungen und eindeutige Errichtungsanordnungen voraus. Daraus muß der Zweck der Karteien, der zulässige Inhalt, die Beschreibung der Voraussetzungen für die Aufnahme in diese Karteien, die zulässige Nutzung und eine differenzierte Aussonderungsregelung enthalten sein. Grundsätzlich bedürfen die Karteien des Landesamtes für Verfassungsschutz einer ständigen Aktualisierung. Ich habe das Landesamt aufgefordert, die Bereinigung der Extremismuskarteien zügig fortzusetzen. Zur Aufgabenerfüllung nicht oder nicht mehr erforderliche Speicherungen sind zu löschen.

6.3 Entwurf eines Bayerischen Verfassungsschutzgesetzes (BayVSG)

Die Notwendigkeit der Schaffung bereichsspezifischer Datenschutzregelungen für die personenbezogene Datenverarbeitung der Verfassungsschutzbehörden ist unbestritten. Hierauf hatte ich bereits in den letzten Tätigkeitsberichten hingewiesen. Inzwischen liegt ein von der Staatsregierung beschlossener Entwurf eines Bayerischen Verfassungsschutzgesetzes vor. Dieser Entwurf faßt die Rechtsgrundlagen für die Tätigkeit der Verfassungsschutzbehörden in Bayern zusammen. Er regelt u.a. die Beobachtungs- und Mitwirkungsaufgaben des Landesamtes für Verfassungsschutz, die Befugnis des Landesamtes zur Erhebung, Speicherung, Veränderung und Nutzung personenbezogener Daten sowie die Befugnis zur Informationsübermittlung zwischen dem Landesamt und anderen Behörden.

Bei der Vorbereitung des Gesetzentwurfs durch das Staatsministerium des Innern war ich intensiv beteiligt. Ich hatte wiederholt Gelegenheit, meine Vorstellungen mit dem Innenministerium ausführlich zu erörtern. Der überwiegende Teil meiner Forderungen ist in den Gesetzentwurf aufgenommen worden. Ich begrüße insbesondere, daß die für die Beschreibung der **Aufgaben** des Landesamtes wichtigen Begriffe, nämlich die **freiheitliche demokratische Grundordnung** und die gegen sie gerichteten **Bestrebungen**, näher definiert sind. Das gilt auch für die Definition der **nachrichtendienstlichen Mittel** im Gesetz selbst. Auch meine Forderung nach klaren Befugnisregelungen des Landesamtes für die Verarbeitung personenbezogener Daten ist weitgehend erfüllt.

In einigen Punkten sollten der Datenschutz noch weiter verbessert, der Inhalt gesetzlicher Regelungen verdeutlicht und der Rahmen für die Befugnisse der Verfassungsschutzbehörden klarer abgesteckt werden. Das betrifft folgende Bereiche:

Einsatz nachrichtendienstlicher Mittel

Der Einsatz nachrichtendienstlicher Mittel kann im Einzelfall besonders stark in das Recht auf informationelle Selbstbestimmung der Bürger eingreifen. Deshalb sollten im Entwurf des Verfassungsschutzgesetzes folgende Verbesserungen vorgenommen werden:

Bei **Anwendung** nachrichtendienstlicher Mittel sollte über Datenerhebungen, die in ihrer Art und Schwere einer Beschränkung des Brief-, Post- und Fernmeldegeheimnisses gleichkommen, entweder die nach dem G-10-Gesetz zuständige Kommission oder der Landesbeauftragte für den Datenschutz in regelmäßigen Abständen **unterrichtet** werden. Dabei ist insbesondere an sogenannte „Lauschangriffe" mit Hilfe besonderer technischer Geräte zu denken. Das vertraulich gesprochene Wort bedarf eines ausdrücklichen Schutzes vor technisch unterstützten Lauschangriffen, unabhängig davon, ob solche Lauschangriffe innerhalb oder außerhalb des von Art. 13 GG geschützten Bereiches stattfinden.

Ein intensiver Eingriff ist auch die heimliche Photo-, Film oder Videoaufnahme, wenn sich der Betroffene in seinem Privatbereich bewegt. Der hier notwendige Schutz der Bürger soll darin bestehen, daß der Einsatz dieser Mittel von Institutionen außerhalb des Verfassungsschutzes (G-10-Kommission oder Landesbeauftragten für den Datenschutz) nachgeprüft wird.

Die **Nutzung** von Informationen, die durch nachrichtendienstliche Mittel erworben worden sind, sollte in zwei Fällen **begrenzt** werden:

Durch nachrichtendienstliche Mittel **unzulässigerweise** erhobene Daten sollten nur genutzt werden dürfen, wenn dies zur Abwehr einer schwerwiegenden Gefahr für den Bestand des Bundes oder eines Landes oder der verfassungsmäßigen Ordnung erforderlich ist. Bisher regelt der Entwurf nur, unter welchen Voraussetzungen die Erhebung personenbezogener Informationen durch Anwendung nachrichtendienstlicher Mittel unzulässig ist. Es fehlt jedoch ein Hinweis, was mit unzulässig erhobenen Daten geschehen soll.

Die **Nutzung** von Informationen, die durch nachrichtendienstliche Mittel erworben worden sind, sollte weiter für den Fall begrenzt sein, daß beim Einsatz nachrichtendienstlicher Mittel **zulässigerweise** erhobene Informationen anfallen, die aber nicht zum Aufgabenbereich des Verfassungsschutzes gehören und die für gewöhnlich als sog. **Zufallsfunde** bezeichnet werden. Auch hier bietet sich

die entsprechende Anwendung der im G-10-Gesetz getroffenen Nutzungsbeschränkung an, wonach derartige Zufallsfunde nur zur Verhinderung oder Verfolgung einer in § 138 StGB genannten schweren Straftat verwendet werden dürfen.

Erhebung, Verarbeitung und Nutzung von Daten in Akten des Verfassungsschutzes

Die Erhebung, Verarbeitung und Nutzung von personenbezogenen Daten in Akten müssen entsprechend der Forderung des Bayerischen Verfassungsgerichtshofs in seinem Kriminalaktenurteil von 1985 im Gesetz ausdrücklich geregelt werden. Dabei müssen, so der Verfassungsgerichtshof, Abgrenzungen zwischen den Rechten des einzelnen einerseits und den Interessen der Allgemeinheit andererseits vorgenommen werden. Der Gesetzentwurf enthält allgemeine Bestimmungen nur über die Erhebung, Verwendung und Übermittlung, nicht hingegen über die Speicherung und sonstige Nutzung der Daten in Akten. Sicherzustellen ist jedoch eine **lückenlose Regelung der Erhebung, Verarbeitung und Nutzung von Daten in Akten.** In diesem Zusammenhang sollen auch Regelungen über die **Sperrung** und **Löschung** von Daten in Akten geschaffen werden.

Gesonderte Dokumentation der Einsichtnahme in Dateien

Wenn der Verfassungsschutz in Dateien Einsicht nimmt, sollte er hierüber intern einen gesonderten Nachweis führen, damit die Rechtmäßigkeit der Einsichtnahme wirksam kontrolliert werden kann. Die Informationsverarbeitung durch den Verfassungsschutz sollte für den Datenschutzbeauftragten jederzeit transparent nachprüfbar und nachvollziehbar sein.

Solche Dokumentationen sind dem Verfassungsschutz nicht fremd. Sie werden etwa von Art. 31 Abs. 3 Satz 2 MeldeG, Art. 14 Gesetz zur Ausführung des Gesetzes über Personalausweise und das Paßgesetz und Art. 72 Abs. 2 SGB X bereits heute gefordert.

Auskunftsrecht des Betroffenen

Aus dem Recht auf **informationelle Selbstbestimmung** und dem **Rechtsstaatsprinzip** ergibt sich nach meiner Auffassung zwingend, daß dem Betroffenen grundsätzlich ein Recht auf Auskunft auch gegenüber dem Verfassungsschutz zustehen muß. Selbstverständlich darf durch ein derartiges Auskunftsrecht die Arbeit des Verfassungsschutzes in ihrer Wirksamkeit nicht beeinträchtigt werden.

Das bedeutet, daß der Verfassungsschutz in der Regel Auskunft erteilen soll über Vorgänge, die er aus allgemein zugänglichen Quellen entnommen hat (Kandidatur für eine extremistische Partei, öffentliche Veranstaltungen). Gleiches gilt für gerichtsverwertbare Erkenntnisse, die im Rahmen von Sicherheits- oder Einstellungsüberprüfungen angefallen sind, und die bei einem etwaigen Verwaltungsverfahren ohnehin dem Betroffenen oder dessen Anwalt zugänglich gemacht werden müßten. Auch Tatsachen, die in ihn betreffenden Strafverfahren oder Verwaltungsvorgängen angefallen sind und die keinem Auskunftsverbot nach den entsprechenden Verfahrensvorschriften unterliegen, sollten dem Betroffenen auf Antrag mitgeteilt werden.

Schranken für Auskunftsbegehren bestehen dann, wenn
- die Auskunft die ordnungsgemäße Erfüllung der Aufgaben des Verfassungsschutzes gefährden würde,
- die Auskunft die öffentliche Sicherheit oder Ordnung gefährden oder sonst dem Wohle des Bundes oder eines Landes Nachteile bereiten würde, oder
- die Daten oder die Tatsache ihrer Speicherung nach einer Rechtsvorschrift oder ihrem Wesen nach, insbesondere wegen der überwiegenden berechtigten Interessen eines Dritten, geheimgehalten werden müssen, und das Interesse des Betroffenen an der Auskunftserteilung nicht ausnahmsweise im Einzelfall überwiegt.

Schließlich muß die Auskunftserteilung auch dann unterbleiben, wenn ein Auskunftsverlangen erkennbar zu Ausforschungszwecken gestellt wird, der Spionagebereich betroffen ist oder der Quellenschutz entgegensteht. Um ganz generell zu verhindern, daß aus der Ablehnung einer Auskunft der Schluß gezogen werden kann, beim Verfassungsschutz gespeichert zu sein, muß der Verfassungsschutz zur Verhinderung der Ausforschung auch in anderen Fällen zur Verweigerung der Auskunft berechtigt sein. So könnte etwa der Verfassungsschutz ganz grundsätzlich jede 20. Auskunft verweigern. Dies wäre für den Betroffenen auch deshalb hinnehmbar, weil in Fällen der Auskunftsverweigerung ein Hinweis auf die Anrufungsmöglichkeit des Landesbeauftragten für den Datenschutz zu geben und so eine Nachprüfung auch in diesen Fällen gewährleistet ist.

7. Justiz

7.1 Gesetzgebung

Nach dem Volkszählungsurteil sind für die Verarbeitung personenbezogener Daten in vielen Bereichen präzisere Rechtsgrundlagen erforderlich. Der Bundesminister der Justiz hat deshalb im Berichtszeitraum eine Fülle von Gesetzgebungsvorhaben vorgelegt:

7.2 Strafverfahrensänderungsgesetz (StVÄG) 1989

Die Strafprozeßordnung enthält keine ausdrückliche Generalermächtigung zum Eingriff in Individualrechtsgüter. Das Gesetz erteilt den Strafverfolgungsorganen zwar einen umfassenden Auftrag zur Aufklärung und Verfolgung strafbarer Handlungen, folgt aber im übrigen der Methode der Aufzählung einzelner Eingriffsermächtigungen, die nach Maßgabe des Verhältnismäßigkeitsgrundsatzes unterschiedlich ausgestaltet sind.

Dieses Prinzip wie auch die neuere Rechtsprechung des Bundesverfassungsgerichts zum Grundrecht auf informationelle Selbstbestimmung erfordern gesetzliche Grundlagen für **neuartige strafprozessuale Ermittlungsmethoden**. Regelungsbedürftig sind auch einige **hergebrachte** Ermittlungsmethoden und außerdem die **Verarbeitung** und die **Nutzung** personenbezogener Informationen im Strafverfahren, das **Akteneinsichtsrecht**, das bisher im wesentlichen auf der Grundlage von Verwaltungsvorschriften gewährt wird, sowie die Verwendung von personenbezogenen Informationen aus Strafverfahren für die **Gefahrenabwehr**.

Der Entwurf enthält — dies hat eine Entschließung der Konferenz der Datenschutzbeauftragten vom 06.04.1989 ausdrücklich begrüßt

- Datenschutzregelungen und eigenständige Befugnisnormen für besondere Ermittlungs- und Fahndungsmethoden sowie Regelungen zur Verarbeitung personenbezogener Daten und zur Akteneinsicht. Ich verkenne weiterhin nicht, daß der vorliegende Entwurf in einigen weiteren Bereichen datenschutzrechtliche Verbesserungen enthält: So ist nunmehr eine bürgerfreundliche Auskunftsregelung vorgesehen. Die Datensicherheit im Forschungsbereich wurde erhöht. Außerdem wurde der Entwurf auch an die Terminologie der Datenschutzgesetze angepaßt.

  Gleichwohl sind weiterhin eine Reihe **wichtiger Datenschutzforderungen** noch nicht berücksichtigt:

- Die Verarbeitung personenbezogener Daten durch Strafverfolgungsorgane greift ganz erheblich in das Persönlichkeitsrecht der Bürger ein. Daher sollten **Abstufungen** nach dem Grad der Betroffenheit (Beschuldigte, Verdächtige, von Vorfeldermittlungen Betroffene und erkennbar Nichtverdächtige, etwa Geschädigte oder Zeugen) vorgenommen werden, wie sie sich in der polizeilichen Praxis zum Teil schon bewährt haben.

- Es sollte klargestellt werden, daß die vorgesehene **Ermittlungsgeneralklausel** keine Eingriffe gestattet, die in ihrer Eingriffstiefe den nunmehr besonders geregelten gleichkommen oder sie übertreffen. So kann etwa der **Einsatz von V-Leuten** nicht auf die Generalklausel gestützt werden.

- Regelungen über die Datenverarbeitung im Strafverfahren setzen eine **Gesamtkonzeption** über die Informationsverarbeitung bei den Strafverfolgungsbehörden voraus. Notwendig sind insbesondere klare Bestimmungen über die Zusammenarbeit zwischen Staatsanwaltschaft und Polizei. Der vorliegende Entwurf läßt den hierzu notwendigen Konsens noch nicht erkennen.

7.3 Auftragsdatenverarbeitung durch Privatfirma

Ein bayerisches Amtsgericht erledigt die **Neufestsetzung des Regelunterhalts** bei Änderung der Unterhaltssätze zentral für Bayern in einem automatisierten Verfahren. In Abständen von etwa zwei Jahren werden infolge der Erhöhung des Regelbedarfs durch Rechtsverordnung der Bundesregierung sehr viele Anträge auf Neufestsetzung des Regelunterhalts gestellt. Um diesen erhöhten Arbeitsanfall möglichst schnell erledigen zu können, ist einer privaten Firma ein Teil der hierbei notwendigen Datenerfassung übertragen.

Unter datenschutzrechtlichen Gesichtspunkten bestehen grundsätzlich Bedenken, die Erfassung von Justizdaten an private Unternehmen zu vergeben. Wirtschaftliche Gesichtspunkte und Kostenfaktoren dürfen nicht ausschlaggebende Maßstäbe sein.

Datenschutzrechtlich ist dieser Vorgang als Auftragsdatenverarbeitung im Sinn von Art. 3 BayDSG zu werten. Diese Form der Datenverarbeitung bringt besondere Risiken mit sich. So sind die Möglichkeiten des Auftraggebers begrenzt, die Einhaltung datenschutzrechtlicher Vorschriften beim Auftragnehmer sicherzustellen. Sie beschränken sich im wesentlichen auf die vertragliche Festlegung bestimmter Pflichten des Auftragnehmers. Deshalb stellt Art. 3 Abs. 1 Satz 2 BayDSG besondere Anforderungen an die Eignung der vom Auftragnehmer getroffenen technischen und organisatorischen Maßnahmen.

Für die Vergabe von Erfassungsarbeiten sensibler Daten, wie der Leistung von Unterhalt für ein nichteheliches Kind, ergeben sich folgende Konsequenzen:

- Nach Nr. 3.3 der Vollzugsbekanntmachung zu Art. 3 BayDSG sollen Aufträge zur Erfassung sensibler Daten im Regelfall nicht an Private vergeben werden.

  An dieser bewährten Regelung ist festzuhalten. Die Datenerfassung durch die Behörde ermöglicht nämlich eine bessere Kontrolle der Einhaltung der datenschutzrechtlichen Vorschriften, da unmittelbare Kontroll- und Einflußmöglichkeiten hinsichtlich der Auswahl des Personals, der Sicherung der Räume und der Organisation des Arbeitsablaufs bestehen. Es entfällt das Problem der Transportsicherung, das sich bei einer Vergabe der Erfassung an Dritte und dem dadurch notwendig werdenden Transport von Datenträgern stellt. Schließlich verhindert die Eigenerfassung das Entstehen von Mißtrauen beim Betroffenen. Die Möglichkeit, daß Unbefugte Einblick in seine Daten erhalten, liegt aus seiner Sicht bei einer Datenerfassung durch private Stellen näher als bei der Eigenerfassung durch die staatliche Behörde selbst. Die Beschäftigten des Privatunternehmens erscheinen ihm als Außenstehende.

- Nur in Ausnahmefällen kann bei sensiblen Daten die Vergabe der Erfassung an Privatunternehmen in Betracht kommen. Dazu gehören insbesondere plötzlich auftretende Arbeitsspitzen, die kurzfristig bewältigt werden müssen. Sofern dies nicht durch Zurückstellung weniger dringender Arbeiten geschehen kann, können im Interesse einer ordnungsgemäßen, insbesondere auch rechtzeitigen Erfüllung der staatlichen Aufgaben in einem solchen Fall ausnahmsweise die oben geschilderten Bedenken zurückgestellt werden. Voraussetzung ist jedoch, daß auf eine besonders sorgfältige Auswahl und Überwachung des beauftragten Unternehmens geachtet wird, um die geschilderten Risiken möglichst auszuschließen.

Um mich von dem Stand der Datenschutzmaßnahmen zu überzeugen, die bei dieser Erfassung von Justizdaten durch eine Privatfirma getroffen worden sind, habe ich diese aufgesucht. Mit den getroffenen Sicherungsvorkehrungen für den Transport der Daten zwischen Amtsgericht und Privatfirma war ich einverstanden. Zur Datensicherung vor Ort waren allerdings einige Hinweise veranlaßt, damit ein unberechtigter Zutritt zu den Geschäftsräumen der Firma und die versehentliche Weitergabe von Daten an Außenstehende durch nicht völlig gelöschte Magnetbänder verhindert werden. Außerdem sollte der Einsatz von Subunternehmern (Heimarbeiterinnen) für die Datenerfassung ausdrücklich vertraglich untersagt werden, damit eine weitere Verbreitung dieser Unterhaltsdaten verhindert wird. Meine Anregungen wurden überwiegend aufgegriffen. Zwar sind damit meine oben genannten Bedenken zur Auftragsdatenverarbeitung durch eine private Firma nicht vollständig ausgeräumt. Da wegen einer Änderung der Zivilprozeßordnung künftig die Datenerfassung reduziert werden kann und bereits jetzt eine ganze Reihe datenschutzrechtlich wichtiger Maßnahmen — wie etwa Vertragsstrafen — vorgesehen sind, habe ich meine grundsätzlichen Bedenken

gegen die Datenerfassung in diesem speziellen Fall vorläufig zurückgestellt.

7.4 Schuldnerverzeichnis und Schuldnerlisten

Die Amtsgerichte führen nach § 915 Zivilprozeßordnung (ZPO) ein Schuldnerverzeichnis, in das alle Personen eingetragen werden, welche die eidesstattliche Versicherung abgegeben haben, gegen die wegen Nichtabgabe der eidesstattlichen Versicherung Haft angeordnet oder eine Haft von mindestens sechs Monaten Dauer vollstreckt worden ist. Auf Antrag erhält nach § 915 Abs. 3 ZPO **jedermann Auskunft** über das Bestehen oder Nichtbestehen einer Eintragung in das Schuldnerverzeichnis. Der Nachweis eines berechtigten Interesses ist nicht erforderlich.

Darüber hinaus übermitteln die bayerischen Amtsgerichte nach den dafür maßgebenden Bestimmungen (§ 915 Abs. 4 ZPO i. V. m. den dazu ergangenen Ausführungsregelungen) Abschriften aus dem Schuldnerverzeichnis an die Industrie- und Handelskammer für München und Oberbayern, die ihrerseits in 14tägigem Turnus „Vertrauliche Mitteilungen über die Schuldnerverzeichnisse der bayerischen Amtsgerichte" (IHK-Schuldnerlisten) herausgibt. Diese Schuldnerlisten kann derzeit jeder beziehen, der einer berufsständischen Einrichtung angehört und ein berechtigtes Interesse am Bezug glaubhaft macht.

7.4.1 Prüfung des Schuldnerverzeichnisses bei einem Amtsgericht

Die für die Erteilung von Auskünften und Abschriften aus dem Schuldnerverzeichnis maßgebenden Rechtsgrundlagen werden seit längerer Zeit als änderungsbedürftig angesehen. Seit Jahren erreichen mich immer wieder Eingaben von Bürgern, die den Verdacht haben, daß Daten aus dem Schuldnerverzeichnis unzulässigerweise an andere Stellen übermittelt werden.

Die Prüfung bei einem Amtsgericht führte zu folgenden Feststellungen:

- Die zur eindeutigen Identifikation eines Schuldners notwendigen **Mindestdaten** (Namen, Geburtsdaten, genaue Anschrift) werden nicht immer erhoben und fehlen dann im Schuldnerverzeichnis. Dies trifft i.d.R. für den Fall zu, daß die Daten des Schuldners ausschließlich auf den Angaben des Gläubigers beruhen. Das Geburtsdatum und die aktuelle Anschrift des Schuldners sind ihm häufig nicht bekannt. Dies birgt die Gefahr von **Personenverwechslungen**, die zu erheblichen wirtschaftlichen Nachteilen für die Betroffenen führen können. Außerdem haben Stichproben ergeben, daß die Namen der Schuldner teilweise aus den Akten unrichtig in das Schuldnerverzeichnis übertragen worden sind.

- Die Datenübermittlung an die IHK erfolgt auf der Grundlage von im Jahr 1955 vom Bundesminister der Justiz erlassenen Allgemeinen Vorschriften, die datenschutzrechtlichen Ansprüchen nicht genügen. Diese Vorschriften regeln auch das Verzeichnis nach § 107 Konkursordnung (KO). Letztgenannte Vorschrift gibt dem Bundesminister der Justiz jedoch keine Regelungsbefugnis.

- Die **Löschungspraxis** des Amtsgerichts entspricht nicht immer dem § 915 ZPO: Die Löschung personenbezogener Daten erfolgt häufig erst nach fünf, statt nach spätestens drei Jahren.

- Die Art der **Aufbewahrung der Akten** in offenen Regalen und zum Teil in für Besucher zugänglichen Nebenräumen ermöglicht den Zugriff durch Unbefugte und entspricht somit nicht den Anforderungen an die Datensicherheit. Inzwischen sind einige Maßnahmen zur Datensicherung getroffen worden.

7.4.2 Verwendung der Schuldnerlisten durch die IHK

Bei der Prüfung einer IHK traf ich folgende Feststellungen:

- Für die weitere Verwendung der aus dem Schuldnerverzeichnis regelmäßig übermittelten Daten bei der IHK fehlt es an hinreichenden **Rechtsgrundlagen**: Die vorgenannten Allgemeinen Vorschriften sowie § 1 Abs. 1 des Gesetzes zur vorläufigen Regelung des Rechts der Industrie- und Handelskammern, wonach diese für die Förderung der gewerblichen Wirtschaft zu wirken haben, reichen nicht aus.

- Außerdem hat die IHK eine Kartei über sämtliche seit 1949 im Bayerischen Staatsanzeiger veröffentlichten Konkurse ohne Rechtsgrundlage geführt. Die Kartei wurde zwischenzeitlich vollständig vernichtet.

- Die Bedingungen für den Bezug der „Vertraulichen Mitteilungen der IHK über die Schuldnerverzeichnisse der bayerischen Amtsgerichte" berücksichtigen nicht die Fortentwicklung des Rechts: Während derzeit die Schuldnerlisten jeder beziehen kann, der einer berufsständischen Einrichtung wie etwa der Handwerks- oder Rechtsanwaltskammer angehört und ein berechtigtes Interesse am Bezug glaubhaft macht, sollte künftig die **Weitergabe der Schuldnerlisten** stark eingeschränkt werden. Es sind Fälle bekannt geworden, in denen Kredithaie über IHK-Schuldnerlisten Schuldner ausfindig gemacht und noch tiefer in Schulden gestürzt haben. Kontrollen der Bezieher, unter denen sich auch Einzelpersonen befinden, finden nicht statt. Als Konsequenz hieraus ist ein Datenmißbrauch nicht auszuschließen. Vor allem aber ist die rechtzeitige Vernichtung überholter Listen nicht gewährleistet.

- Nach den Bedingungen, welche die IHK für München und Oberbayern mit den Beziehern der Vertraulichen Mitteilungen vertraglich vereinbart, sind u.a. folgende Maßgaben einzuhalten:
  - Verwendung der Mitteilungen nur für eine vertrauliche Auskunftserteilung im Einzelfall;
  - keine Weitergabe der Daten an andere Personen;
  - die Mitteilungen dürfen vom Bezieher nicht abgeschrieben, veröffentlicht, nachgedruckt, anderweitig vervielfältigt oder vertrieben werden; außerdem darf anderen Personen keine Einsicht gewährt werden.

  Diese Bedingungen werden nicht von allen Beziehern eingehalten.

- Nach mir vorliegenden Informationen sollen private Firmen **zentrale Schuldnerverzeichnisse** planen oder bereits einrichten. Dies ist nach meiner Auffassung weder mit dem geltenden Recht noch mit dem derzeit vorliegenden Entwurf eines Gesetzes zur Änderung von Vorschriften über das Schuldnerverzeichnis vereinbar. Es widerspricht grundlegenden Forderungen des Daten-

schutzes, wenn private Firmen zentrale Schuldnerverzeichnisse ohne ausreichende Beschränkungen und Kontrollen führen.

7.4.3 Gesetzentwurf

Der Bundesminister der Justiz hat einen neuen Gesetzentwurf zum Schuldnerverzeichnis vorgelegt. Er enthält in vielen Punkten Verbesserungen gegenüber früher diskutierten Vorschlägen. Allerdings ist auch im neuen Entwurf das Hauptproblem, die **Weitergabe von Schuldnerlisten durch die Abdruckempfänger**, nicht befriedigend gelöst. Meine Bedenken richten sich in erster Linie dagegen, daß eine **effektive Kontrolle** der Einhaltung der Datenschutzvorschriften, vor allem der **Löschung** überholter Eintragungen, nicht gewährleistet ist, wenn die Daten aus dem Schuldnerverzeichnis durch regelmäßige Übermittlungen aller Änderungen zu breit gestreut werden.

Zur Lösung dieses Problems könnte man an ein Verfahren der unmittelbaren Auskunftserteilung im jeweiligen Einzelfall durch die Industrie- und Handelskammern an Mitglieder von Körperschaften des öffentlichen Rechts denken. Damit könnte auf die Übermittlung vollständiger Listen verzichtet werden. Hierdurch könnte der Empfängerkreis schriftlicher Abdrucke aus dem Schuldnerverzeichnis spürbar eingegrenzt und dadurch der Gefahr einer Weitergabe inhaltlich falscher Daten wirksamer begegnet werden.

7.5 Notwendige Novellierung der Strafvollzugsgesetze

In den Strafvollzugsanstalten nimmt die Automatisierung zu. So werden zur Lohnabrechnung der Gefangenen und zur Buchführung über ihre Guthaben sowie zur anstaltsinternen Kommunikation EDV-Verfahren eingesetzt. In automatisierten Verfahren (Datenfernübertragung, Datenträgeraustausch) werden keine personenbezogenen Daten an Dritte weitergegeben. Hingegen übermittelt die Anstalt in manuellen Verfahren **Daten von Gefangenen an andere Behörden** vielfach nur auf der Grundlage der Vollzugsgeschäftsordnung, einer Verwaltungsvorschrift.

Das Strafvollzugsgesetz enthält kaum gesetzliche Regelungen zur Datenverarbeitung. Derzeit bestehen insoweit nur einzelne Verwaltungsvorschriften. Im Hinblick auf das Volkszählungsurteil des Bundesverfassungsgerichts ist jedoch zumindest der Rahmen für die Datenverarbeitung der Justizvollzugsanstalten in einem formellen Gesetz abzustecken. Bemühungen zur Novellierung des Strafvollzugsgesetzes scheiterten bisher an den unterschiedlichen Vorstellungen des Bundesministers der Justiz und der Landesjustizverwaltungen. Ein ebenfalls notwendiges **Jugendstrafvollzugsgesetz** ist derzeit nicht absehbar. Weiterhin erfordern umfangreiche Automationsvorhaben der Justiz im Strafvollzug (Geschäftsstelle, Arbeits- und Wirtschaftsverwaltung, Datenträgeraustausch) bereichsspezifische Regelungen.

Insbesondere folgende Fragen sind regelungsbedürftig:

- Umfang der Datenerhebung und -speicherung, etwa im Aufnahmeverfahren, bei der Vorstellung beim Anstaltsleiter, bei der ärztlichen Untersuchung, hinsichtlich der Notwendigkeit erkennungsdienstlicher Maßnahmen.
- Besonders sensible Daten sollten nicht in der allgemeinen Strafvollzugsakte, sondern beispielsweise in einem Sammelheft aufbewahrt werden. Der Zugriff der einzelnen Bediensteten auf die **Personalakten** sollte differenziert nach ihrer jeweiligen Tätigkeit geregelt werden.
- Die diversen Bücher, Karteien und Dateien, in denen personenbezogene Daten gespeichert sind, sollten auf ihre Notwendigkeit überprüft und reduziert werden. Für die dann noch erforderlichen Datenspeicherungen sind gesetzliche Grundlagen zu schaffen.
- Datenübermittlungen sollten nur auf einer gesetzlichen Grundlage erfolgen.
- Zumindest der Rahmen für die Sicherung und Löschung personenbezogener Daten von Strafgefangenen sollte festgelegt werden.

7.6 Eingaben zu Krankenversicherungen

Wiederum beschwerten sich einige Rechtsreferendare wegen der Weitergabe ihrer Anschrift an Krankenversicherungen. Sie vermuteten die Urheber bei staatlichen Behörden.

Ermittlungen beim Oberlandesgericht, das für die Ausbildung der Referendare zuständig ist, bei dem beim Staatsministerium der Justiz errichteten Landesjustizprüfungsamt, das die Prüfungen abhält, und bei der Universität führten zu folgendem Ergebnis:

Anhaltspunkte dafür, daß Bedienstete des Oberlandesgerichts Anschriften von Bewerbern für den juristischen Vorbereitungsdienst an Versicherungen weiterreichen, haben sich nicht ergeben. Die mit der Bearbeitung der personenbezogenen Daten von Rechtsreferendaren beschäftigten Kräfte werden regelmäßig — letztmals schriftlich im Frühjahr dieses Jahres — darauf hingewiesen, daß die Weitergabe solcher Daten an Versicherungsvertreter oder Vertrauensmänner unzulässig ist. Sämtliche in Frage kommenden Bediensteten haben erklärt, daß diese Hinweise beachtet und eingehalten werden. Anhaltspunkte für die Unrichtigkeit dieser Versicherungen habe ich nicht.

Auch sämtliche Angehörige des Landesjustizprüfungsamts beim Staatsministerium der Justiz haben in dienstlichen Äußerungen erklärt, daß sie keine Auskünfte an Versicherungen erteilen. Versicherungsvertreter hätten auch nicht versucht, Anschriften von Prüfungsteilnehmern zu erhalten.

Die Universität München hat sich wie folgt geäußert:

Universitäten sind nur am mündlichen Prüfungsverfahren zur Ersten Juristischen Staatsprüfung insofern beteiligt, als die zu Prüfern bestellten Professoren eine Mitteilung über Termin und Namen der zu prüfenden Kandidaten erhalten. Anhaltspunkte, daß aus diesem Personenkreis Daten weitergegeben werden, gibt es nicht. Listen der Prüfungskandidaten werden an der Universität nicht ausgehängt.

Namenslisten finden — allerdings ohne Anschriften — allenfalls während des Studiums Verwendung. Möglich ist jedoch, daß ein Versicherungsvertreter Namen von Kommilitonen erhalten hat.

7.7 Forschung

Im Berichtszeitraum war ich wiederum mit einer Reihe von Forschungsvorhaben befaßt, in denen personenbezogene Daten aus den Unterlagen bayerischer Justizbehörden verarbeitet wurden.

Die bedeutsamste Untersuchung, die auf Veranlassung des Bundesministers der Justiz durchgeführt wird, betrifft eine **Strukturanalyse der Rechtspflege**. Hierbei werden die unterschiedlichen Organisationsstrukturen bei Amts-, Finanz- und Verwaltungsgerichten im Hinblick auf unterschiedliche Vor- und Nachteile für Effizienz und Arbeitsfähigkeit der Gerichte untersucht.

Gegen die Untersuchung bestehen keine grundsätzlichen Bedenken, da der öffentlich-rechtliche Dienstherr das Recht hat, personenbezogene Daten (auch durch Dritte) für Untersuchungen dieser Art zu erheben. Die dem Dienstherrn obliegende Sorgfalt, insbesondere im Bereich der Datensicherheit, muß allerdings auch bei den beauftragten Firmen gewährleistet sein. Die Untersuchung kann auf die Weisungsbefugnis des Dienstherrn gestützt werden.

Ich habe das Staatsministerium der Justiz zur Sicherung der Anonymität gebeten, insbesondere auf folgende Maßnahmen zu achten:

- Der Vorgesetzte der jeweils befragten Justizbediensteten darf die Unterlagen nicht erhalten, da ihm eine Reidentifizierung trotz anonym durchgeführter Untersuchung möglich ist.
- Auch die Justizverwaltung sollte keine personenbezogenen Daten erhalten.
- Die Anonymität der Befragten ist bei der Bekanntgabe der Forschungsergebnisse zu gewährleisten. Die veröffentlichten Informationen dürfen keinen Rückschluß auf bestimmte oder bestimmbare Personen zulassen.

Darüber hinaus befaßte ich mich mit einer Reihe weiterer Forschungsvorhaben. Meine Zustimmung habe ich jeweils nur unter Auflagen erteilt:

- Nach Möglichkeit müssen die Betroffenen vor der Teilnahme an der Untersuchung über deren wesentlichen Verlauf unter deutlichem Hinweis auf die Freiwilligkeit der Teilnahme aufgeklärt werden.
- Sämtliche Datenträger (Disketten, Listen, Formblätter u.ä.) sind so aufzubewahren, daß unbeteiligte Dritte hierauf weder Zugriff haben noch vom Inhalt Kenntnis nehmen können.
- Das Forschungsvorhaben darf nicht auch ohne Verwendung personenbezogener Daten durchführbar sein.
- Die am automatisierten Verfahren beteiligten Personen sind vor Aufnahme ihrer Tätigkeit nach Maßgabe von Art. 14 BayDSG auf das Datengeheimnis zu verpflichten.
- Die technischen und organisatorischen Maßnahmen müssen dem Stand der Technik entsprechen.
- Das Datenmaterial darf nur für den Forschungszweck verwendet werden.
- Die Forscher müssen sich bereit erklären, eine datenschutzrechtliche Kontrolle ihrer Arbeit zu ermöglichen.

Der Bundesminister der Justiz beabsichtigt, die Bedingungen der Forschung mit Strafakten dadurch zu verbessern, daß bei der Auswertung der Strafakten zu Forschungszwekken auch die in diesen enthaltenen **Sozialdaten** einbezogen werden dürfen.

8. Regierungen, Landkreise, Städte und Gemeinden

8.1 Datenschutzlücke im Gemeinderat

In meinem letzten Tätigkeitsbericht habe ich das Thema „Datenschutzlücke im Gemeinderat" angesprochen. Ich habe bemängelt, daß der Datenschutz der Bürger verletzt wird, wenn deren persönliche Angelegenheiten in nichtöffentlichen Sitzungen behandelt werden und die Mitglieder kommunaler Vertretungsorgane sich nicht an ihre Verschwiegenheitspflicht halten. Ich habe vorgeschlagen zu prüfen, ob von der Möglichkeit, **Ordnungsgelder** zu verhängen, ausreichend Gebrauch gemacht wird, oder ob eine **Verschärfung** der Gesetzesbestimmungen notwendig ist. Darüber hinaus habe ich eine angemessene Strafvorschrift für notwendig erachtet.

Das Staatsministerium des Innern hat meine Anregung zum Anlaß genommen, die Problematik mit den kommunalen Spitzenverbänden zu erörtern. Es ist dabei zur Auffassung gelangt, das vorhandene rechtliche Instrumentarium reiche aus, eventuellen Verletzungen der Verschwiegenheitspflicht durch Mitglieder kommunaler Vertretungsorgane wirksam vorzubeugen. Mandatsträger machten sich jetzt bereits nach geltendem Recht bei Verletzung der Verschwiegenheitpflicht gem. § 203 und § 353 b StGB strafbar. Es bleibt vorerst abzuwarten, ob bekanntwerdende Verstöße auf Strafanträge der Betroffenen auch zu Verurteilungen führen werden.

8.2 Prüfung von Regierungen

Festgestellte Mängel behoben

In meinem letzten Tätigkeitsbericht habe ich über die Prüfung einer Regierung berichtet. Die seinerzeit dargelegten Mängel betrafen die **Beihilfeverwaltung**, den Umfang einiger **Dateien**, die zu **sorglose Aufbewahrung** der Akten und Karteien (Datensicherheit) sowie die **Telefondatenerfassung** und die **Gleitzeitregelung** für die Beschäftigten.

In allen angesprochenen Bereichen konnte die Regierung inzwischen datenschutzgerechte Lösungen mitteilen. So werden die Beihilfeantragsformulare jetzt mit dem Hinweis versehen, daß die Briefumschläge, in denen die Beihilfeanträge an die Regierung versandt werden, mit dem Wort „Beihilfe" gekennzeichnet werden sollen. Gekennzeichnete Briefumschläge werden dann von der Einlaufstelle ungeöffnet an die Beihilfestelle weitergeleitet. Die Schreibarbeiten in der Beihilfestelle werden in einem gesonderten Raum erledigt, der durch weitere Maßnahmen gegen unbefugtes Betreten gesichert ist. Die Beihilfeunterlagen werden nach Dienstende in einem Stahlschrank unter Verschluß genommen.

Bei der Telefondatenerfassung werden manuelle Aufzeichnungen über dienstliche Ferngespräche nicht mehr geführt. Die bisherigen Aufzeichnungen wurden vernichtet. Bei Privatgesprächen werden Datum, Uhrzeit und die vollständige Telefonnummer beider Teilnehmer gespeichert, wobei die Zielnummer nur für Abrechnungszwecke genutzt und verkürzt ausgedruckt wird. Auf meinen Vorschlag hin erhält jeder Bedienstete in einem verschlossenen Umschlag einen monatlichen Ausdruck.

Prüfung im Berichtszeitraum

Bei der Prüfung einer weiteren Regierung konnte ich folgende Feststellungen treffen:

- Im Bereich **Personalwesen** habe ich zahlreiche Karteien mit einem umfangreichen Datenbestand vorgefunden, welche die einzelnen Sachbearbeiter wegen der zentralen Personalaktenführung für erforderlich hielten, um besoldungs- und statusrechtliche Fragen ohne Beiziehung des Personalaktes bearbeiten zu können. Nach Einführung des automatisierten Personalverwaltungsprogrammes „DIAPERS" werden diese Karteien überflüssig werden. Ich habe auf eine datenschutzgerechte Vernichtung nach Inbetriebnahme von DIAPERS hingewiesen.

- Die „Kartei der Rechtsreferendare" enthielt Daten, die zur Sachbearbeitung nicht benötigt werden, wie Familienstand, Zahl der Kinder, Punktezahl der Stationszeugnisse und Staatsangehörigkeit. Da noch Prüfungsjahrgänge bis zu ca. 20 Jahren zurück aufbewahrt wurden, habe ich eine Aussortierung und Vernichtung dieser alten Karteikarten verlangt.

- Daneben bestehen umfangreiche Bestände an **„Ausgeschiedenen-Karteien"**, die bei den einzelnen Sachbearbeitern aufbewahrt werden. Obwohl des öfteren Rückfragen zu den Arbeitsverhältnissen ehemals Beschäftigter eingehen, ist ein unbegrenztes Vorhalten dieser Datenbestände mit dem Datenschutz nicht vereinbar. Ich habe daher Aussonderungsfristen in entsprechender Handhabung der in DIAPERS vorgesehenen Löschungsfristen angeregt.

- Die bisherige Praxis, **Beihilfeanträge**, die an die Beihilfestelle adressiert oder als Beihilfeanträge von außen erkennbar sind, in der Poststelle öffnen zu lassen, entsprach nicht den vom Staatsministerium des Innern für seinen Geschäftsbereich festgelegten Grundsätzen, wonach die Umschläge nur von den Beihilfestellen geöffnet werden dürfen. In meinem letzten Tätigkeitsbericht hatte ich die gleiche Praxis bei einer anderen Regierung bereits beanstandet.

8.3 Prüfung von Landratsämtern

Prüfung im Berichtszeitraum

Bei der Prüfung eines Landratsamtes stellte ich fest, daß die Organisation der **Beihilfesachbearbeitung** nicht den Anforderungen entspricht, die das Staatsministerium des Innern zum Persönlichkeitsschutz bei Beihilfedaten aufgestellt hat. Nach der bisherigen Organisation wurden nämlich Beihilfeanträge von einem **Personalsachbearbeiter** miterledigt. Dem Gebot der sachlichen und organisatorischen Trennung von Personal- und Beihilfeverwaltung, die auf Sachgebietsleiterebene anzustreben ist, war damit nicht Rechnung getragen.

Im Bereich der **Sozialhilfeverwaltung** wurden alte Karteikarten und Akten zuletzt im Jahre 1974 ausgesondert. Da zur gesetzlichen Aufgabenerfüllung (§ 92 c BSHG) allenfalls eine Aufbewahrungsfrist von 13 Jahren sachgerecht und somit erforderlich ist, habe ich die datenschutzgerechte Vernichtung der über diesen Zeitraum hinaus vorgehaltenen Unterlagen gefordert, soweit nicht die Akten nach dem Bayerischen Archivgesetz an das Bayerische Staatsarchiv abzugeben sind.

Im übrigen war der größte Teil der insgesamt 45 überprüften Karteien nicht zu beanstanden. Allerdings waren verschiedene Karteien und Akten in **nichtabschließbaren Schubläden** oder Schränken aufbewahrt, obwohl ihr sensibler Inhalt die sichere Unterbringung erfordert. Dies betraf zum Beispiel Bußgeldkarteien, Akten über Unterbringungen von Personen nach dem Unterbringungsgesetz, Bodenverkehrsakten mit notariellen Kaufverträgen sowie Handakten der Sozialarbeiterin im Bereich Jugendhilfe. Ich habe das Anbringen bzw. den Einbau von Schlössern gefordert.

Das Landratsamt hat mir mitgeteilt, daß es die Beihilfeverwaltung neu organisieren werde und als Alternative auch den Abschluß einer Beihilfeversicherung erwäge. Wegen der weiteren Forderungen stehe ich mit dem Landratsamt in Verbindung.

Ergebnisse der letztjährigen Prüfung

Bei der Prüfung eines Landratsamtes im Jahre 1988 wurden vor allem Mängel bei der Datensicherheit festgestellt. So befand sich ein Teil der Besoldungsakten in einem **nichtabsperrbaren Schrank**. Darüber hinaus wurden in nichtabschließbaren Karteikästen Karteien mit zum Teil sensiblen Daten (BAFöG-Angaben, Jugendhilfe) verwahrt. Ich hatte diese Unterbringung beanstandet. Das Landratsamt hat zwischenzeitlich Abhilfe geschaffen. Die Besoldungsakten befinden sich jetzt in einem absperrbaren Schrank, dessen Schlüssel nur den Bediensteten zur Verfügung stehen, die im Rahmen ihrer Tätigkeit auf die Akten zugreifen müssen. Auch die Karteien sind jetzt unter Verschluß.

8.4 Prüfungen bei Gemeinden

Der Schwerpunkt der Prüfungen bei Gemeinden lag auf den automatisierten Verfahren im Meldewesen. Zu deren Ergebnissen verweise ich auf 9.2.

8.5 Zuverlässigkeitsüberprüfung im waffenrechtlichen Erlaubnisverfahren

Der Datenschutzbeauftragte einer Stadt hat sich mit der Frage an mich gewandt, ob im Rahmen eines waffenrechtlichen Erlaubnisverfahrens (Erteilung eines Waffenscheins oder einer Waffenbesitzkarte) **Ermittlungen in der Nachbarschaft** des Antragstellers durchgeführt werden dürfen. Die Ermittlungen sehen so aus, daß die Nachbarn des Antragstellers befragt werden, ob er ihres Wissens schon einmal mit der Polizei zu tun gehabt habe und er in geordneten wirtschaftlichen Verhältnissen lebe.

In Übereinstimmung mit dem Staatsministerium des Innern vertrete ich dazu folgende Auffassung:

Das entscheidende Kriterium im Waffenrecht ist die Zuverlässigkeit des Antragstellers. Weist der Antragsteller die erforderliche Zuverlässigkeit nicht auf, muß der beantragte Waffenschein oder die beantragte Waffenbesitzkarte versagt werden. Angesichts des zwingenden Charakters des Versagungsgrundes der Unzuverlässigkeit muß die Erlaubnisbehörde in jedem Fall von Amts wegen prüfen, ob Tatsachen vorliegen, aus denen sich der Mangel der persönlichen Zuverlässigkeit ergibt. Es muß dann auch die Möglichkeit bestehen, im **Einzelfall mit Einverständnis** des Antragstellers eine solche „Umfeldüberprüfung" durchzu-

führen, wenn sich die Zuverlässigkeit auf andere Weise nicht klären läßt.

8.6 Ablichtung und Aufbewahrung von Unterstützungslisten für Wahlen

Das Wahlrecht für Europa-, Bundes- und Landeswahlen sieht vor, daß die gemeindliche Wahlbehörde die Wahlberechtigung der Unterzeichner sogenannter Unterstützungslisten prüft und hierüber zur Vorlage beim Landeswahlleiter eine Bescheinigung ausstellt. Diese Bescheinigung kann auf einem besonderen Vordruck erteilt werden, wird aber in der Regel auf der Unterstützungsliste selbst vorgenommen.

Die Gemeinde hat dabei zu gewährleisten, daß die Bescheinigung für jeden wahlberechtigten Unterzeichner **nur einmal zu einem Wahlvorschlag** erteilt wird.

Anläßlich der letzten Europawahl habe ich in Einzelfällen festgestellt, daß die Gemeinden zum Nachweis, für welchen Bürger eine Bescheinigung erteilt wurde, die Unterstützungslisten ablichteten und aufbewahrten.

Diese Verfahrensweise war unzulässig, weil §§ 32 Abs. 5 Europawahlordnung, 34 Abs. 6 Bundeswahlordnung, 31 Abs. 5 Landeswahlordnung den Gemeinden ausdrücklich untersagen, festzuhalten, für welchen Wahlvorschlag die Bescheinigung bestimmt ist.

Das Staatsministerium des Innern, dem ich die Problematik geschildert habe, hat mir zugesichert, die Gemeinden in den für die nächsten Wahlen neu abzufassenden Wahlanweisungen ausdrücklich darauf hinzuweisen, daß Anfertigung und Aufbewahrung von **Kopien von Unterstützungslisten unzulässig** sind.

In Ergänzung dieser beabsichtigten und von mir begrüßten Wahlanweisung schlage ich den Gemeinden vor, zum Nachweis, daß eine Unterschrift bereits bescheinigt wurde, die Unterzeichner in eine manuell geführte Liste oder Kartei einzutragen oder besser noch in einem alphabetischen Verzeichnis aller Wahlberechtigten (z.B. durch Abhaken) zu kennzeichnen.

Ein zwingendes Gebot des Datenschutzes ist es außerdem, daß nach Ablauf der Frist für die Einreichung der Unterstützungslisten beim Landeswahlleiter **alle** Aufzeichnungen in der Gemeinde **gelöscht** werden.

8.7 Tonbandaufnahmen in Bürgerversammlungen zu Protokollzwecken

Anläßlich einer schriftlichen Landtagsanfrage ist mir bekannt geworden, daß vereinzelt in Bürgerversammlungen Tonbandaufnahmen zu Protokollzwecken gefertigt werden.

Bürgerversammlungen nach Art. 18 Gemeindeordnung dienen der Erörterung gemeindlicher Angelegenheiten. Redebeiträge in Bürgerversammlungen sind zwar als öffentlich gesprochene Worte anzusehen, die nicht nach § 201 Abs. 1 Nr. 1 StGB strafrechtlich geschützt sind.

In Übereinstimmung mit dem Staatsministerium des Innern bin ich aber der Auffassung, daß im Hinblick auf das Recht auf informationelle Selbstbestimmung auch das öffentlich gesprochene Wort nicht schutzlos ist und nicht ohne weiteres von öffentlichen Stellen auf Tonband aufgenommen werden darf. Zumindest müssen die Gemeindebürger wissen, daß ein Tonbandgerät ihre Redebeiträge aufzeichnet.

Das Staatsministerium des Innern hat diesen Fall zum Anlaß genommen, die Gemeinden darauf hinzuweisen, die Teilnehmer von Bürgerversammlungen vor Beginn vom Einsatz eines Tonbandgerätes ausdrücklich zu informieren. Das Innenministerium hat darüber hinaus klargestellt, daß Personen, die mit der Aufnahme ihrer Redebeiträge nicht einverstanden sind, berechtigt sind, das Abschalten des Tonbandgerätes zu verlangen, solange sie reden.

Diese Klarstellung begrüße ich.

8.8 Fremdenverkehr

8.8.1 Gewinnspiele und Preisausschreiben in Fremdenverkehrs und Kurorten

Unter der Überschrift „Schwarz-Gäste mit Spiel entlarvt" berichtete eine bayerische Tageszeitung, daß anhand der Daten von Teilnehmern an einem Gewinnspiel, das der Fremdenverkehrsverein durchführte, festgestellt worden sei, daß etwa 10 v.H. der Gäste von den Beherbergungsbetrieben der Gemeinde zur Festsetzung der Kurbeiträge und Kurtaxen nicht gemeldet worden seien.

Diese Feststellung stützt sich auf einen **Abgleich der Gewinnspielteilnehmerdaten** mit den von den Gästen auszufüllenden Meldescheinen.

Ganz abgesehen davon, daß die Teilnehmer über die mit dem Gewinnspiel verfolgten Zwecke im unklaren gelassen werden (letztlich sind sie Abgabenschuldner, sofern der Beherbergungsbetrieb die von den Gästen vereinnahmten Kurbeiträge nicht an die Gemeinde abführt), halte ich den Abgleich von Gästemeldescheindaten mit den Gewinnspielteilnehmerdaten mit Art. 29 Abs. 1 Satz 2 MeldeG für nicht vereinbar.

8.8.2 Kfz-Halterfeststellung zur Festsetzung des Kurbeitrags/der Kurtaxe

In der Vergangenheit wurde ich immer wieder mit der Frage konfrontiert, ob in Fremdenverkehrsgemeinden zur Überprüfung der Kurbeitrags-/Kurtaxenentrichtung anhand auswärtiger Kfz-Kennzeichen die Halter festgestellt werden dürfen (vgl. auch Nr. 8.5 des 7. Tätigkeitsberichts).

Eine solche Halterfeststellung ist gemäß § 39 Abs. 3 Straßenverkehrsgesetz (StVG) **unzulässig**. Auf das Schreiben des Staatsministeriums des Innern aus dem Jahr 1987, in dem den Fremdenverkehrsgemeinden diese Auffassung ausdrücklich mitgeteilt wird, verweise ich.

8.8.3 Fragebogen zur Struktur- und Wirtschaftsanalyse

Eine Fremdenverkehrsgemeinde versandte an alle Haushalte einen Fragebogen zur „Struktur- und Wirtschaftsanalyse". Der Fragebogen sollte nach Angaben der Gemeinde Grundlage für ein Wirtschaftsgutachten sein, mit dessen Hilfe die Aufnahme der Gemeinde in das Städtebauförderungsprogramm erreicht werden sollte. Ich hatte an der Fragebogenaktion folgendes auszusetzen:

- Eine gesetzliche Pflicht zum Ausfüllen des Fragebogen bestand nicht: Die Gemeinde hätte deshalb auf die **Freiwilligkeit hinweisen** müssen (Art. 16 Abs. 2 BayDSG). Es fand sich jedoch weder im Begleitschreiben

der Gemeinde noch im Fragebogen selbst ein Hinweis darauf, daß die Beantwortung der Fragen freiwillig ist.

- Die Befragten mußten Namen, Vornamen und Straße sowie Hausnummer angeben. Eine Abtrennung dieses „Anschriftenfeldes" vom eigentlichen Fragebogen war nicht vorgesehen.

  Die Gemeinde erklärte dies damit, die Abtrennung des Anschriftenfeldes sei deshalb nicht geplant, weil die aus den Fragebögen resultierenden Ergebnisse innerhalb des Ortes räumlich zugeordnet werden müßten.

  Diese Auffassung überzeugte mich nicht. Für eine räumliche Zuordnung reicht es aus, wenn nur der Straßenname erkennbar ist. Die anderen Angaben, also Name, Vorname und Hausnummer, können unkenntlich gemacht (geschwärzt) werden.

- Einige Fragen waren sehr problematisch. Zum Beispiel wurde nach dem Sanierungs- oder Modernisierungsbedarf am Eigentum gefragt, ferner nach den Räumlichkeiten, die als Gästezimmer/Ferienwohnung verwendet werden können. Andere Fragen an Gewerbebetriebe betrafen durchwegs Betriebsinternas (Personal, Räumlichkeiten, Ausstattung u. ä.).

  In einem Abschnitt „Fragen an Landwirte und Inhaber von landwirtschaftlichen Flächen" wurde die Frage nach dem Alter des Betriebsinhabers gestellt, ferner ob die Hofnachfolge vorhanden, ungewiß, oder nicht vorhanden ist sowie ob der landwirtschaftliche Betrieb in absehbarer Zeit weitergeführt, vergrößert, verkleinert oder ganz aufgegeben wird.

  Ich halte Fragen dieser Art für datenschutzrechtlich nicht akzeptabel, wenn aus dem Fragebogen die Identität des Betroffenen erkennbar ist und die Freiwilligkeit bei einer Befragung nicht eindeutig klargestellt wird.

8.9 Datenübermittlungen

8.9.1 Angebliche Datenweitergabe aus einem Landratsamt

Ein Landtagsabgeordneter hat mich um Überprüfung folgenden Falles gebeten:

Zwischen einem Erfinder und seinem ehemaligen Berater war es zu erbitterten privaten Auseinandersetzungen gekommen. Der Erfinder behauptete, sein ehemaliger Berater hindere ihn seit Jahren an der Vermarktung seiner Ideen. Dieser wiederum hatte gegen den Erfinder beträchtliche finanzielle Forderungen, die der Erfinder nicht befriedigen konnte.

Der Erfinder behauptete nun, sein Kontrahent erhalte vom Landratsamt (Sozialhilfeverwaltung und/oder Kfz-Zulassungsstelle), vom Amtsgericht und vom Fernmeldeamt ständig Informationen über ihn.

Meine Überprüfungen haben diesen Vorwurf nicht erhärten können. Ich habe bei den meiner Aufsicht unterliegenden öffentlichen Stellen (Landratsamt, Amtsgericht) nachgefragt, ob die behaupteten Vorwürfe zutreffen. Diese versicherten mir glaubwürdig, daß aus ihrem Bereich keine Informationen geflossen sind. Diesen Erklärungen war nichts entgegenzusetzen, zumal in vorliegendem Fall viele private Quellen (z.B. Banken, Privatfirmen, Versicherungen, Detektivbüro oder Schutzorganisationen für Gläubiger) in Frage kamen, aus denen Informationen stammen konnten.

8.9.2 Bekanntgabe einer gaststättenrechtlichen Gestattung

In einer Eingabe beschwerte sich ein Vorsitzender eines Sportvereins, der Bürgermeister seiner Gemeinde habe eine seinem Verein erteilte gaststättenrechtliche Gestattung für die Abhaltung eines Vereinsfestes dem örtlichen Gastwirt übergeben.

Der um Stellungnahme gebetene Bürgermeister erklärte, er habe den örtlichen Gastwirt von der gaststättenrechtlichen Gestattung informiert, weil dieser als Grundstückseigentümer Mitbetroffener sei und der Verein das Wasser aus der Wasserversorgung des Gastwirtes beziehe.

Mich konnte diese Stellungnahme nicht überzeugen.

Die Bekanntgabe der gaststättenrechtlichen Gestattung an den örtlichen Gastwirt war weder zur rechtmäßigen Erfüllung der durch das Gaststättengesetz der Gemeinde zugewiesenen Aufgabe erforderlich, noch konnte der Gastwirt ein berechtigtes Interesse an der Kenntnis des Bescheides geltend machen. Die Tatsache, daß er Grundstückseigentümer ist und dem Verein das Wasser liefert, reicht dafür nicht aus. Weder das Gaststättengesetz noch die Allgemeine Verwaltungsvorschrift sieht die Unterrichtung von Grundstückseigentümern oder Wasserversorgungsunternehmen über die Erteilung gaststättenrechtlicher Erlaubnisse vor. Außerdem wurden „schutzwürdige Belange" des Vereins verletzt.

Ich habe dies dem Bürgermeister der Gemeinde mitgeteilt und das Verhalten der Gemeinde gerügt.

8.10 Bauwesen

8.10.1 Gesetzliche Vorkaufsrechte der Gemeinden nach den Vorschriften des Baugesetzbuches (zweistufiges Verfahren)

In meinem letzten Tätigkeitsbericht habe ich mich mit der Frage befaßt, unter welchen Voraussetzungen ein Notar einer Gemeinde zur Ausübung des Vorkaufrechts den gesamten notariellen Kaufvertrag übermitteln darf. Ich habe auf das von der Landesnotarkammer Bayern vorgeschlagene **„zweistufige Verfahren"** zur Ausübung des Vorkaufsrechts der Gemeinden hingewiesen. Dieses Verfahren sieht vor, daß der Notar der Gemeinde zur Prüfung der Frage, ob ein Vorkaufsrecht besteht, zunächst nicht den gesamten notariellen Kaufvertrag übersendet. Vielmehr soll die Gemeinde in einem ersten Schritt über die Umstände unterrichtet werden, die es ihr erlauben zu entscheiden, ob für das verkaufte Grundstück überhaupt ein Vorkaufsrecht besteht. Kommt die Ausübung des Vorkaufsrechts in Betracht, so kann die Gemeinde in einem zweiten Schritt die Übermittlung des vollständigen Inhalts des Kaufvertrages verlangen.

Ich hatte darauf verwiesen, daß allein dieses zweistufige Verfahren dem Grundsatz entspricht, nur die jeweils notwendigen Daten an andere Stellen zu übermitteln. Der Bayer. Gemeindetag hat auf Bitte des Staatsministeriums des Innern seine Mitglieder über das zweistufige Verfahren unterrichtet und die Anwendung unterstützt. Leider hat sich der Bayer. Städtetag diesem Schritt nicht angeschlossen, weil er einen nicht unerheblichen Mehraufwand befürchtet.

Ich bedauere diese Entscheidung, weil ich die Befürchtungen des Städtetags nicht teile.

8.10.2 Weiterleitung von Kaufverträgen durch den Gutachterausschuß an die Gemeinden

Zur Ermittlung von Grundstückswerten bestehen bei den kreisfreien Städten und den Landratsämtern sogenannte Gutachterausschüsse. Diese haben die Aufgabe, auf Antrag Gutachten über den Verkehrswert von bebauten und unbebauten Grundstücken zu erstatten. Dabei sind die Gutachterausschüsse auf die Mitarbeit der Gemeinden angewiesen. Sie benötigen Informationen über den Planungszustand (bebaut, bebaubar, unbebaut u.ä.) der Grundstücke. Zu diesem Zweck leiten sie den Gemeinden Vordrucke zu, in denen die Flurnummer des zu schätzenden Grundstückes angegeben ist. Die **Namen des Käufers und des Verkäufers fehlen**. Auf dieses Verfahren haben sich das Staatsministerium des Innern und ich aus datenschutzrechtlichen Gründen geeinigt.

Ein Arbeitskreis „Kommunalverwaltung" in einem Landkreis wandte sich an mich mit der Bitte, dieses Verfahren zu überprüfen. Die Gemeinden seien auf die Namen der Käufer und Verkäufer angewiesen; ohne diese Angaben könnten sie die vom Gutachterausschuß erbetenen Auskünfte nicht erteilen.

In Übereinstimmung mit dem Staatsministerium des Innern teile ich die Auffassung des Arbeitskreises nicht. Jede Gemeinde muß in der Lage sein, Grundstücke in ihrem Gebiet ohne besonderen Arbeitsaufwand allein an Hand der Flurnummer zu identifizieren und Auskünfte zu erteilen.

8.10.3 Ermittlung von Eigentümernamen bei Vorkaufsrechtsanfrage

Anläßlich einer Eingabe wurde mir folgender Vorfall bekannt:

Ein Architekt kaufte in einer Großstadt einen Häuserkomplex. Wenige Tage später, so der Architekt, waren die Mieter dieser Häuser durch Flugblätter des örtlichen Mietervereins über den Kauf informiert. Der Architekt vermutete die „undichte Stelle" bei der für die Ausübung des Vorkaufrechts zuständigen Stelle der Stadtverwaltung; er argwöhnte, die dortigen Beamten hätten die Angaben an den örtlichen Mieterverein herausgegeben.

Meine Nachforschungen bei der Stadtverwaltung blieben letztlich ergebnislos. Die Beamten bestritten, die Daten über den Verkauf der Häuser weitergegeben zu haben. Ich habe auch den örtlichen Mieterverein, der als private Organisation nicht meiner datenschutzrechtlichen Überwachung unterliegt, gebeten mir mitzuteilen, woher er seine Informationen habe. Der Verein antwortete, er habe die Informationen von einer Privatperson erhalten.

8.10.4 Einsicht in Erschließungsbeitragsabrechnungen

Ein Petent zweifelte die Höhe des von ihm geforderten Erschließungsbeitrages an und erbat bei der Gemeinde Einsicht in die Abrechnungsunterlagen, die ihm auch gewährt wurde. Darüber hinaus verlangte er eine Kopie über die beteiligten Grundstückseigentümer sowie deren Grundstücksgrößen, um die Aufteilung der Kosten rechnerisch überprüfen zu können. Dies lehnte die Gemeinde aus Datenschutzgründen ab.

Im Rahmen des Rechts des Beitragspflichtigen auf fehlerfreie Berechnung des Erschließungsbeitrags halte ich eine Bekanntgabe und schriftliche Mitteilung zumindest der **Gesamtabrechnungsfläche** sowie der erschließungsbeitragsfähigen **Gesamtkosten**, welche nicht personenbezogene Daten sind, für zulässig. Für eine Nachberechnung der Gesamtabrechnungsfläche sind dabei die **Grundstücksgrößen**, zuzüglich bestimmter Zuschläge für besondere Nutzungen maßgebend, so daß auch eine Bekanntgabe dieser Daten geboten sein dürfte. Allerdings dürfen vertraulich zu behandelnde Tatsachen anderer Beitragspflichtiger wie Eigentumsverhältnisse, Adresse, Anteilseigentümer, Nummern von Notarurkunden nicht offenbart werden.

Soweit die erforderlichen Berechnungsunterlagen nicht anonymisiert werden können (z.B. durch Schwärzen von Kopien) empfehle ich eine anonymisierte Zusammenstellung der erforderlichen Daten. Somit kann dem Anliegen einzelner Bürger auf Überprüfung ihrer Beitragsschuld Rechnung getragen werden, ohne daß gleichzeitig sensible Daten anderer Beteiligter preisgegeben werden müssen.

9. Einwohnermeldewesen

9.1 Rechtliche Entwicklung

Der Vollzug des Bayerischen Meldegesetzes hat gezeigt, daß einzelne Regelungen mit Blick auf Bürgerfreundlichkeit und Verwaltungsvereinfachung sowie das informationelle Selbstbestimmungsrecht überarbeitet werden sollten. Die Bundesregierung hat inzwischen den Entwurf zur **Änderung des Melderechtsrahmengesetzes** (MRRG) vorgelegt, der noch in dieser Legislaturperiode im Bundestag verabschiedet werden soll.

Aus datenschutzrechtlicher Sicht ist an diesem Entwurf positiv hervorzuheben, daß künftig die Nutzung von **Patientenverzeichnissen** in Krankenhäusern und ähnlichen Einrichtungen (§ 16 Abs. 3 MRRG) wegen der Sensibilität der Daten erheblich eingeschränkt werden soll.

Beachtenswert ist außerdem, daß künftig der sog. **Familienverband** (Querverweise zwischen Eltern und Kindern) bis zur Vollendung des 27. Lebensjahres der Kinder aufrechterhalten bleiben soll. Damit wird einem starken praktischen Bedürfnis entsprochen.

9.2 Prüfungen

Einer der Schwerpunkte meiner Kontrollen bei Gemeinden ist seit längerem die Prüfung der automatisierten Verfahren für das Meldewesen. Hierbei stelle ich bei von privaten Firmen angebotenen Verfahren immer wieder die gleichen Fehler fest. Um hier eine nachhaltige Verbesserung zu erreichen, weise ich die Gemeinden nochmals auf folgendes hin:

Jede Gemeinde ist für die Richtigkeit ihrer Datenverarbeitung **selbst verantwortlich**. Das gilt auch für die Richtigkeit der von privaten Firmen erworbenen Programme. Mit der Freigabe durch den Gemeinderat übernimmt die Gemeinde diese Verantwortung. Die Freigabe nach Art. 26 BayDSG setzt deshalb eine gründliche Prüfung der Rechtmäßigkeit und Erforderlichkeit der von privaten Firmen angebotenen Programme voraus.

Leider ist auch im Berichtszeitraum festzustellen, daß Gemeinden in Unkenntnis ihrer Verantwortung und im Vertrauen auf die Zusicherung der Herstellerfirmen, daß „sämtliche datenschutz- und melderechtlichen Gesichtspunkte in dem Verfahren berücksichtigt wurden", automatisierte Einwohnermeldeverfahren installieren, die bei einer späteren Überprüfung durch meine Geschäftsstelle in nicht unerheblichem Maße beanstandet werden müssen.

In meinem 10. Tätigkeitsbericht habe ich unter Nr. 7.2.2 (S. 30/31) typische Verfahrensmängel der von mir geprüften automatisierten Einwohnermeldeverfahren aufgelistet. Weitere, im Berichtszeitraum durchgeführte Prüfungen im Einwohnermeldewesen führten zu keinem wesentlich besseren Ergebnis als 1988.

Die von mir beanstandeten Gemeinden haben die Firmen, die ihnen die Programme geliefert haben, aufgefordert, die in den Prüfungsberichten festgehaltenen Verfahrensmängel zu bereinigen. Während die Anbieter mit einem relativ großen Marktanteil aufgrund meiner Feststellungen einzelne Fehler bereinigt haben und sich um weitere Verbesserungen bemühen, reagieren die Softwarehäuser mit verhältnismäßig wenig Kunden (wohl aus Kostengründen) nur äußerst schleppend. Die Folge ist, daß nach wie vor mängelbehaftete Einwohnermeldeverfahren bei den Kommunen eingesetzt werden. Dies gilt insbesondere für die zahlreichen Meldebehörden, die von mir bereits bei anderen Gemeinden geprüfte, mängelbehaftete Programme einsetzen. Deshalb sollten alle Anwender beanstandeter Programme mit Nachdruck bei den Herstellerfirmen die umgehende Korrektur der Programme fordern. Sollten die Fehler und Mängel nicht innerhalb angemessener Frist beseitigt werden, weil die Programmhersteller die Mängel nicht beheben, werde ich nach Art. 30 Abs. 2 Satz 1 BayDSG rechtsaufsichtliche Maßnahmen fordern.

Im folgenden zeige ich nochmals einige typische Mängel in automatisierten Einwohnermeldeverfahren auf, damit das Meldeamtspersonal von sich aus Fehlerquellen erkennen und Folgerungen für das eigene Verfahren treffen kann. Nachteilige Auswirkungen mancher Verfahren und Mängel, vor allem Unvollständigkeiten, können vom Sachbearbeiter verhindert werden.

Kennzeichen Wehrüberwachung

Nach § 24 Abs. 9 Wehrpflichtgesetz i.V.m. § 2 2. BMeldDÜV haben die Meldebehörden dem Kreiswehrersatzamt zum Zwecke der Wehrüberwachung die Daten aller männlichen Deutschen zwischen dem vollendeten 18. und 32. Lebensjahr zu übermitteln. Die Daten älterer Wehrpflichtiger sind nur zu übermitteln, wenn der Meldebehörde von der Wehrersatzbehörde mitgeteilt worden ist, daß sie auch nach Vollendung des 32. Lebensjahres (noch) der Wehrüberwachung unterliegen (Offiziere, Unteroffiziere).

Dies bedeutet, daß nur bei letztgenanntem Personenkreis (über 32 Jahre) eine Kennzeichnung als „der Wehrüberwachung unterliegend" im Meldedatensatz gespeichert werden darf. In der Praxis stelle ich jedoch häufig fest, daß das Kennzeichen „Wehrüberwachung" auch bei 18- bis 32jährigen eingegeben wird (manche Verfahren sehen das entsprechende Datenfeld sogar als „Mußfeld" vor). Die Folge davon ist, daß das Kennzeichen auch nach Vollendung des 32. Lebensjahres gespeichert bleibt, und somit die Daten der Betroffenen weiterhin (unzulässigerweise) an die Wehrersatzbehörde übermittelt werden, obwohl sie der Wehrüberwachung nicht mehr unterliegen.

Zur Bereinigung der Melderegister empfiehlt es sich, eine Liste über sämtliche Personen mit dem Kennzeichen „Wehrüberwachung" auszudrucken und nach einem Abgleich mit dem Kreiswehrersatzamt die erforderlichen Löschungen vorzunehmen. Das Kennzeichen darf nur bei den über 32jährigen gespeichert bleiben, die aufgrund besonderer Mitteilung des Kreiswehrersatzamtes noch der Wehrüberwachung unterliegen.

Verfahrensseitig müßte vor einer Datenübermittlung an das Kreiswehrersatzamt wie folgt geprüft werden:

- männlich?
- deutsch?
- zwischen 18 und 32 Jahre alt?
- oder über 32 Jahre alt und Kennzeichen „Wehrüberwachung" ist gespeichert.

Auch wäre es zu begrüßen, wenn verfahrensseitig die Eingabe des Kennzeichens „Wehrüberwachung" bei Minderjährigen, bei den 18- bis 32jährigen, bei Ausländern sowie bei weiblichen Personen automatisch als unzulässig zurückgewiesen würde.

Von mir hin und wieder festgestellte Kennzeichnungen wie „Zivildienst", „Ersatzdienst", „Zivil-/Katastrophenschutz" usw. sind generell unzulässig. Solche Merkmale sind zu löschen.

Auflösung des Familienverbandes bei Eintritt der Volljährigkeit der Kinder

Nach Art. 3 Abs. 1 Nr. 16 MeldeG i.V.m. Nr. 3.1.4 Abs. 3 VollzBekMeldeG sind im Melderegister die Querverweise zwischen Eltern und Kindern bei Eintritt der Volljährigkeit der Kinder zu löschen. Diese Regelung hat in der Praxis zu Problemen bei der Ermittlung von Erben und Hinterbliebenen geführt.

Die vom Bundesgesetzgeber beabsichtigte Beibehaltung des Familienverbandes bis **zur Vollendung des 27. Lebensjahres** der Kinder habe ich zum Anlaß genommen, meine Forderung nach Löschung der Querverweise bis auf weiteres zurückzustellen.

Löschung von Daten Weggezogener oder Verstorbener (Art. 11 MeldeG)

Art. 11 MeldeG schreibt zwingend vor, daß Daten von Weggezogenen oder Verstorbenen nach Ablauf bestimmter Fristen zu löschen sind.

Bei den überprüften Einwohnermeldeverfahren privater Anbieter fehlten die entsprechenden Routinen. Ich habe deshalb die Gemeinden aufgefordert dafür zu sorgen, daß Daten Weggezogener oder Verstorbener nach Art. 11 Abs. 2 MeldeG gelöscht und die Aussonderung und gesonderte Aufbewahrung (50 Jahre) der Daten nach Art. 11 Abs. 3 MeldeG vorgenommen werden.

Bisher ist mir nur von der AKDB bekannt, daß für den Vollzug des Art. 11 MeldeG ein Verfahren entwickelt worden ist.

Speicherung des gesetzlichen Vertreters

Nach Art. 3 Abs. 1 Nr. 9 MeldeG dürfen Angaben zum gesetzlichen Vertreter im Melderegister gespeichert werden. Eine solche Speicherung kommt sowohl bei Minderjährigen (nichteheliche Kinder, Waisen, aber auch Entmündigungen) als auch bei Volljährigen, z.B. bei Entmündigungen, in Betracht.

Bei Minderjährigen muß bei Erreichen der Volljährigkeit der gesetzliche Vertreter, von einigen Ausnahmen abgesehen, gelöscht werden. Andernfalls entsteht der unrichtige Eindruck, daß der Betroffene etwa aufgrund einer Entmündigung einen gesetzlichen Vertreter habe. Dies kann zur Folge haben, daß er keine Wahlunterlagen erhält oder Schwierigkeiten bei der Beantragung von Ausweispapieren bekommt.

Deshalb ist der gesetzliche Vertreter eines Minderjährigen grundsätzlich bei Eintritt der Volljährigkeit zu löschen (es sei denn, der Betroffene ist entmündigt oder steht auch nach Eintritt der Volljährigkeit unter Pflegschaft).

Die von mir geprüften Meldebehörden habe ich aufgefordert, die entsprechenden Datensätze zu kontrollieren und ggf. zu bereinigen.

Inhalt von „Bemerkungsfeldern"

Zahlreiche von mir überprüfte Einwohnermeldeverfahren sehen sog. Bemerkungsfelder vor, in die der Anwender frei wählbare Texte eingeben kann.

Nicht selten mußte ich feststellen, daß in diesen Feldern Hinweise auf Adoptionen, Wahlausschlußgründe, wie Entmündigung, Pflegschaft, Vormundschaft, sowie andere durch Art. 3 MeldeG nicht gedeckte Daten gespeichert waren.

Ich habe die Meldebehörden darauf hingewiesen, daß in Bemerkungsfeldern ausschließlich melderechtlich zulässige Daten gespeichert werden dürfen, und sie aufgefordert, die Melderegister zu bereinigen.

Zeitliche Begrenzung von Auskunftssperren

Das Melderecht kennt eine Reihe von Auskunfts- und Übermittlungssperren, die dazu dienen, Datenübermittlungen und Auskünfte in bestimmten Fällen an bestimmte Empfänger zu verhindern. Sie gelten mit Ausnahme der „Sperrung der erweiterten Melderegisterauskunft" (Art. 34 Abs. 6 Satz 2 MeldeG) durchwegs unbefristet, nämlich bis zum Widerruf durch den Betroffenen selbst oder bis zur Aufhebung durch die Meldebehörde.

Mehrere automatisierte Einwohnermeldeverfahren sehen im Gegensatz dazu Befristungsdaten bei sämtlichen Auskunfts- und Übermittlungssperren vor. Die betroffenen Meldebehörden habe ich zur Überprüfung und zur Bereinigung der entsprechenden Fälle aufgefordert, damit nicht unberechtigte Auskünfte erteilt werden, die im Einzelfall für den Betroffenen zu ganz erheblichen Nachteilen führen können.

Wahrung des Adoptionsgeheimnisses

Nr. 3.1.5 VollzBekMeldeG schreibt vor, daß bei einer Annahme als Kind (Adoption) im Zusammenhang mit dem neuen Namen weder der vor der Adoption geführte Name noch ein sonstiger Hinweis auf die Adoption im Melderegister gespeichert werden darf (Ausnahme: Erwachsenenadoption).

Tatsächlich stelle ich jedoch immer wieder fest, daß in derartigen Fällen entweder eine Auskunftssperre nach Art. 34 Abs. 7 Nr. 1 MeldeG und/oder der frühere Name des Kindes im Melderegister gespeichert ist. Da diese Daten und Hinweise im Falle einer vollzogenen Adoption mehr verraten als schützen, habe ich die betreffenden Meldebehörden aufgefordert, die Adoptions-Auskunftssperre, die nur im Falle von Volljährigenadoptionen von Bedeutung ist, bei Kindesadoptionen zu löschen. Ebenso habe ich empfohlen, die Annahme als Kind nicht über die Verfahrensfunktion „Namensänderung", sondern z.B. als „Berichtigung" abzuwickeln, weil sonst der frühere Name des Kindes gespeichert bliebe.

Defizit bei der Benachrichtigung über Berichtigungen des Melderegisters (Art. 10 MeldeG)

Nach Art. 10 Satz 2 MeldeG hat die Meldebehörde von Berichtigungen unverzüglich diejenigen Stellen zu unterrichten, denen im Rahmen regelmäßiger Datenübermittlungen (vgl. Art. 31 Abs. 7 MeldeG, 1. und 2. BMeldDÜV, BayMeldeDÜV) die unrichtigen Daten übermittelt worden sind. Diese Bestimmung wird vielfach von den Meldebehörden nicht beachtet. Sie ist auch in den automatisierten Verfahren nicht berücksichtigt.

Beispiele:

a) Wurde ein Sterbedatum eingegeben, so hat dies eine Mitteilung an den Rentendienst der Deutschen Bundespost zur Folge (§ 4 Abs. 1 2. BMeldDÜV). Wird nun zu einem späteren Zeitpunkt das Sterbedatum im Melderegister gelöscht, muß eine Information des Rentendienstes gewährleistet sein.

b) Wird ein Deutscher fälschlicherweise als Ausländer angemeldet, hat dies eine Unterrichtung der Ausländerbehörde zur Folge. Die notwendige Unterrichtung des Kreiswehrersatzamtes unterbleibt dagegen.

Wird die bisher (falsch) gespeicherte ausländische Staatsangehörigkeit auf „deutsch" berichtigt, müßte dies zwingend Auswirkungen auf die Unterrichtung sowohl der Ausländerbehörde als auch des Kreiswehrersatzamtes haben. Gleiches gilt, wenn ursprünglich als Staatsangehörigkeit „deutsch" gespeichert war und der Datensatz später auf die richtige ausländische Staatsangehörigkeit abgeändert wird.

Weitergabe von Meldeschein-Ablichtungen an andere Behörden

Im Falle regelmäßiger Datenübermittlungen an andere öffentliche Stellen sind die Meldedatenübermittlungsverordnungen des Bundes (1. und 2. BMeldDÜV) und die Bayerische Meldedaten-Übermittlungsverordnung (BayMeldeDÜV) zu beachten. Die Datenübermittlung darf nach § 14 Abs. 3 BayMeldeDÜV auch in schriftlicher Form, u.a. mit Hilfe der Meldescheine vorgenommen werden. Durch technische und organisatorische Maßnahmen ist allerdings sicherzustellen, daß der in den Meldedatenübermittlungsverordnungen vorgesehene (zulässige) Datenumfang nicht überschritten wird (z.B. durch Schwärzen der nicht erforderlichen und damit unzulässigen Informationen).

Wiederholt habe ich jedoch festgestellt, daß Meldebehörden Kopien der Originalmeldescheine ohne Beachtung des Art. 14 Abs. 3 BayMeldeDÜV an andere Behörden weiterleiten. Z.B. wurden bei Verwendung eines gemeinschaftlichen Meldescheins (Vater, Mutter, Kinder) auch die Daten der deutschen Familienangehörigen eines Ausländers an die Ausländerbehörde weitergegeben. Ebenso wurden die Daten von Familienangehörigen eines männlichen Deutschen, der der Wehrüberwachung unterliegt, an das Kreiswehrersatzamt übermittelt.

Die Meldebehörden wurden aufgefordert, ihre Datenübermittlungspraxis unverzüglich an die Vorgaben der Meldedaten-Übermittlungsverordnungen anzupassen.

Um den Rahmen dieses Tätigkeitsberichts nicht zu sprengen, konnten nicht alle festgestellten Verfahrensmängel geschildert werden. Interessierten Meldebehörden stelle ich auf Anforderung detailliertere Mängelberichte zur Verfügung.

9.3 Meldedatenübermittlung an politische Parteien und Wählergruppen zum Zwecke der Wahlwerbung (Entscheidungshilfen für die Praxis)

Wie schon bei zurückliegenden Wahlen sind auch anläßlich der Europawahl zahlreiche Fragen zur Übermittlung von Wähleradressen an politische Parteien gestellt worden. Der Beirat beim Landesbeauftragten für den Datenschutz hat hierzu folgenden Beschluß gefaßt:

„Der Beirat beim Landesbeauftragten für den Datenschutz stellt fest, daß die Übermittlung von Wählerdaten an Parteien und Wählergruppen dem Auftrag der Parteien nach Art. 21 Grundgesetz Rechnung trägt.

In Einzelfällen hat es bei Meldebehörden Unsicherheit über die Auslegung der melderechtlichen Bestimmungen gegeben. Daher gibt der Datenschutzbeirat für Auskünfte der Meldebehörden an Parteien und Wählergruppen über Wähleranschriften folgende Hinweise:

1. Über die Herausgabe von Wählerdaten an Parteien und Wählergruppen nach Art. 35 Abs. 1 des Meldegesetzes entscheidet die jeweilige Meldebehörde nach pflichtgemäßem Ermessen. Entscheidet sie sich für die Herausgabe, darf sie die Wähleradressen nur solchen Parteien verweigern, die vom Bundesverfassungsgericht für verfassungswidrig erklärt worden sind.

2. Wählerdaten erhalten nur die Parteien und Wählergruppen, die für die jeweilige Wahl Kandidaten nominiert haben.

   Empfänger von Wählerdaten dürfen bei den Parteien sein

   - die jeweiligen Landesverbände bei allen Wahlen,
   - die Parteigliederungen, aber beschränkt auf deren jeweiligen örtlichen Wirkungsbereich.

   Wählergruppen erhalten die Wähleranschriften für die Wahl und den örtlichen Bereich, in dem sie auftreten.

   Einzelkandidaten, die keiner Partei oder Wählergruppe angehören, erhalten die Daten für ihren Wahlbezirk.

3. Die Wähleranschriften dürfen auf jedem geeigneten Datenträger (z.B. Magnetplatte, Magnetband, Disketten, Papier) und in Datei- oder Listenform übermittelt werden.

4. Von der Meldebehörde erhaltene Daten sind im jeweiligen Verantwortungsbereich (z.B. rechtlich unselbständige Parteigliederungen, Arbeitsgemeinschaften und Jugendorganisationen, Kandidaten) zu belassen und dürfen nicht an Dritte (erlaubt: an Auftragnehmer) weitergegeben werden. Die Datensicherheit ist zu gewährleisten.

5. Die Wählerdaten dürfen nur für Zwecke der Wahlwerbung verwendet werden.

   Der Begriff der Wahlwerbung ist nicht zu eng auszulegen. Zulässig sind etwa die Verwendung zur Ladung zu Wahlveranstaltungen, zu gesellschaftlichen Veranstaltungen der Parteien (z.B. Sommerfeste, Dichterlesungen, Kabaretts usw.), zu Hinweisen auf die Briefwahl, zum Angebot der Beförderung zum Wahllokal und die **beiläufige** Werbung von Mitgliedern oder für Parteipublikationen.

6. Mit den Wählerdaten dürfen kein Datenabgleich und keine Verknüpfung mit anderen Dateien vorgenommen werden. Ausgenommen ist der Datenabgleich mit den Mitgliederdateien.

7. Die von der Meldebehörde erhaltenen Wählerdaten dürfen nicht gemischt mit Adreßdaten anderer Herkunft gespeichert werden.

8. Die Wähleranschriften sind spätestens einen Monat nach der Wahl oder Abstimmung zu löschen.

Das Staatsministerium des Innern wird gebeten, diese Hinweise den Gemeinden mitzuteilen."

9.4 Melderegisterauskünfte über „Altersjubiläen" 18jähriger

Ein Landtagsabgeordneter bat einen Bürgermeister um laufende Mitteilung der Adressen aller 18jährigen, um ihnen zur Volljährigkeit Glückwünsche übermitteln zu können.

Nach Art. 35 Abs. 2 MeldeG darf die Meldebehörde Parteien, Wählergruppen, Mitgliedern parlamentarischer Vertretungskörperschaften und Bewerbern für diese sowie Presse und Rundfunk eine Melderegisterauskunft über **Alters-** und Ehejubiläen erteilen.

Der 18. Geburtstag ist zwar wegen des Eintritts der Volljährigkeit und der damit verbundenen Rechte und Pflichten ein im Leben jedes Bürgers wichtiges Datum, aber kein Altersjubiläum. Vielmehr setzt ein Altersjubiläum nach dem herkömmlichen Sprachverständnis einen jenseits der Mitte des Lebens liegenden „runden" Geburtstag voraus.

Obgleich sich das Meldegesetz nicht abschließend festlegt, welche Alters- und Ehejubiläen übermittelt werden dürfen, kann man sich an § 10 der Bayerischen Meldedatenübermittlungsverordnung orientieren, wonach die Übermittlung von Altersjubiläen jedenfalls ab dem 75. Lebensjahr und von Ehejubiläen ab der Goldenen Hochzeit zulässig ist.

Demzufolge halte ich eine Bekanntgabe der Daten junger Mitbürger, die demnächst volljährig werden, mit Art. 35 Abs. 2 MeldeG nicht für vereinbar.

9.5 Melderegisterauskünfte über Aus- und Übersiedler

In letzter Zeit mehren sich Anfragen der Meldebehörden, ob sie Krankenkassen, Versicherungen und sozialen Einrichtungen etwa zur Mitgliederwerbung Auskunft über Namen und Anschrift von Aus- und Übersiedlern erteilen dürfen.

Ganz abgesehen davon, daß nach Art. 3 MeldeG das Datum Aus- oder Übersiedler im Melderegister nicht gespeichert wird, rechtfertigen Mitgliederwerbung und Einladungen des betroffenen Personenkreises zu (evtl. nicht gewünschten) Betreuungsgesprächen oder -veranstaltungen eine solche Gruppenauskunft ohne Einwilligung der Betroffenen nicht.

9.6 Veröffentlichung von Einwohnerdaten im Adreßbuch

Nach Art. 35 Abs. 3 MeldeG darf die Meldebehörde einem Adreßbuchverlag Auskunft über Namen, Anschrift und akademischem Grad der volljährigen Einwohner geben. In manchen Adreßbüchern erscheinen die Bewohner nicht nur alphabetisch aufgelistet, sondern auch nach Straßen notiert. Das haben einige Wohnungssuchende dazu benützt, aus dem Adreßbuch Namen und Anschrift von mutmaßlich Alleinstehenden herauszusuchen. Sie haben dann telefonischen oder schriftlichen Kontakt mit den Betroffenen aufgenommen, um von ihnen mit ungewöhnlichem Nachdruck Wohnraum in dem „allein" bewohnten Haus zu fordern.

Ich empfehle deshalb erneut, die Gemeindebürger von Zeit zu Zeit in ortsüblicher Weise auf die nach dem Meldegesetz vorgesehenen **Widerspruchsrechte** hinzuweisen. An die in Nr. 35.4 VollzBekMeldeG getroffene Regelung, gerade vor einer Auskunftserteilung an Adreßbuchverlage in ortsüblicher Weise auf das Widerspruchsrecht hinzuweisen, erinnere ich.

9.7 Melderegisterauskunft an Rundfunkbeauftragte

Wiederholt erhielt ich Anfragen von Meldebehörden, ob den Beauftragten des Bayerischen Rundfunks, welche Rundfunk- und Fernsehteilnehmer zu ermitteln haben, die bislang ihrer Zahlungsverpflichtung an die GEZ nicht nachkommen, Auskunft aus dem Melderegister erteilt werden darf (z.B. über alle Zu- und Wegzüge, über alle über 18jährigen oder alle Hochhausbewohner).

Grundsätzlich sind Melderegisterauskünfte an die Rundfunkanstalten (auch an die GEZ) und deren Beauftragte nach Art. 31 MeldeG zu beurteilen (siehe auch Nr. 34.11 VollzBekMeldeG). Danach ist eine Datenübermittlung im Einzelfall zulässig, soweit sie zur rechtmäßigen Aufgabenerfüllung des Rundfunks (der GEZ) erforderlich ist.

Der Datenschutzbeauftragte des Bayerischen Rundfunks hat mitgeteilt, daß in der Praxis die Beauftragten des Bayerischen Rundfunks für ihre Überprüfungstätigkeit Datenkarten über die dem Rundfunk (der GEZ) gemeldeten Rundfunkteilnehmer erhalten. Diese Karten werden von der GEZ straßenweise aufbereitet, so daß der Beauftragte ohne weiteres vor Ort feststellen kann (z.B. über Adreßbücher oder Namensschilder an den Klingeln), welche Bewohner einer Straße noch nicht der GEZ gemeldet sind. Soweit erforderlich, kann der Rundfunkbeauftragte in solchen Einzelfällen bei der Meldebehörde im Rahmen des Art. 31 Abs. 1 MeldeG Auskünfte über diese dem Rundfunk bisher nicht bekannten Personen einholen.

Pauschale Datenübermittlungen über Einwohner bestimmter Wohngebiete oder bestimmter Altersgruppen scheiden daher mangels Erforderlichkeit aus. **Regelmäßige** Datenübermittlungen (z.B. aller Zu- und Wegzüge) sind schon deshalb unzulässig, weil eine entsprechende Ermächtigung in der Bayerischen Meldedatenübermittlungsverordnung fehlt (vgl. Art. 31 Abs. 4 und 5 MeldeG).

9.8 Übermittlung von Einwohner-Veränderungslisten zur Berechnung von Abfall-/Abwasserbeseitigungsgebühren

Obwohl bereits unter Nr. 4.6.4 des 5. Tätigkeitsberichts (1982) ausgeführt wurde, daß die regelmäßige Weitergabe von Meldedaten zum Zwecke der Berechnung von Abfallbeseitigungsgebühren unzulässig ist, fordern die gebührenfestsetzenden Stellen (Landratsämter, Abwasserzweckverbände) von den Meldebehörden immer wieder Einwohnerveränderungslisten, um anhand der Zu- und Abgänge die Gebühren nach dem Personenmaßstab festsetzen zu können.

Solche **regelmäßigen** Datenübermittlungen sind einerseits wegen fehlender Regelung in der Meldedatenübermittlungsverordnung (vgl. Art. 31 Abs. 4 und 5 MeldeG) unzulässig. Andererseits genügen zur rechtmäßigen Aufgabenerfüllung der Festsetzungsbehörden zahlenmäßige Angaben. Die Mitteilung der Namen ist daher nicht erforderlich und deshalb unzulässig.

Hierauf habe ich die betreffenden Behörden erneut hingewiesen und die Löschung der früher erhaltenen Melderegisterdaten gefordert.

9.9 Veröffentlichung der Daten von Zu- und Wegziehenden im kommunalen und im kirchlichen Mitteilungsblatt

Wiederholt habe ich die Bekanntgabe von Daten der Zu- und Wegziehenden in kommunalen Mitteilungsblättern beanstandet, soweit sie ohne Einwilligung der Betroffenen erfolgt ist.

Die Bürger, die nach staatlichem Datenschutzrecht keine Einwilligung erteilt haben, sind überrascht, wenn Kirchengemeinden, denen von den Meldebehörden im Rahmen des Art. 32 MeldeG Meldedaten zur rechtmäßigen Aufgabenerfüllung (dazu zählen seelsorgerische, karitative, kulturelle Zwecke) übermittelt werden dürfen, die Daten der Zu- und Wegziehenden im kirchlichen Mitteilungsblatt (Gemeindebrief) ohne vorherige Einwilligung veröffentlichen.

Da die Religionsgesellschaften nach Art. 140 Grundgesetz i.V.m. Art. 137 Abs. 3 Weimarer Reichsverfassung ihre Angelegenheiten, also auch den Datenschutz, selbständig ordnen und verwalten, habe ich keinen unmittelbaren Einfluß auf die kirchliche Datenverarbeitung. Um jedoch für die betroffenen Bürger eine annehmbare Lösung zu finden, hat sich das Staatsministerium des Innern, dem ich die Angelegenheit vorgetragen habe, bereit erklärt, mit den Kirchen hierüber Gespräche zu führen. Ein Ergebnis steht noch aus.

9.10 Variable Gestaltung von melderechtlichen Aufenthaltsbescheinigungen

Zum Nachweis, daß ein Bürger in der Gemeinde gemeldet ist, stellt die Meldebehörde auf Antrag des Betroffenen eine

sog. Aufenthaltsbescheinigung zur Vorlage bei anderen Behörden (z.B. Kfz-Zulassungsstelle, Nachlaßgericht) aus.

Meinen Feststellungen und einzelnen Beschwerden zufolge werden diese Aufenthaltsbescheinigungen in den automatisierten Einwohnermeldeverfahren grundsätzlich starr nach dem amtlichen Muster mit sämtlichen dort vorgesehenen Daten erstellt, ohne daß dabei nach dem vorgesehenen Zweck unterschieden würde. Z.B. sind Religionszugehörigkeit und der Familienstand zur Vorlage bei der Kfz-Zulassungsstelle nicht erforderlich.

In einigen automatisiert erstellten Aufenthaltsbescheinigungen werden mehr Daten als im amtlichen Muster vorgegeben, ausgedruckt, nämlich „Familienstand seit", „weitere (Neben-)Wohnungen" sowie „minderjährige Kinder". Dies ist nicht von vorneherein unzulässig: Der Betroffene kann sich diese Daten auf ausdrücklichen Wunsch ausdrucken lassen (vgl. Nr. 9.2 der Vollzugsbekanntmachung zum Bayer. Meldegesetz).

Ich habe stets eine **dem jeweiligen Verwendungszweck entsprechende** variable Gestaltung der Aufenthaltsbescheinigung gefordert. Allerdings hat das Staatsministerium des Innern mitgeteilt, daß es eine variable Gestaltung im automatisierten Verfahren wegen des hohen Kosten- und Verwaltungsaufwands nicht für zwingend geboten hält; sowohl Bürger als auch die Meldebehörden hätten die Möglichkeit, Aufenthaltsbescheinigungen je nach ihrem Zweck im manuellen Verfahren zu beantragen bzw. auszustellen. Das Staatsministerium des Innern hat jedoch aufgrund meiner Initiative die Bereitschaft signalisiert, diese Angelegenheit weiter zu verfolgen.

Auch die Anstalt für Kommunale Datenverarbeitung in Bayern (AKDB) hat eine Programmversion mit variabler Gestaltung der Aufenthaltsbescheinigung für 1990 in Aussicht gestellt.

10. Steuerverwaltung

10.1 Datenschutzvorschriften für die Steuerverwaltung

Auf einhellige Ablehnung der Datenschutzbeauftragten stieß ein vom Bundesfinanzminister vorgelegter Referentenentwurf über **bereichsspezifische Regelungen zur Erhebung und Verarbeitung von Daten im Anwendungsbereich der Abgabenordnung**. Danach sollten das Kontrollrecht der Datenschutzbeauftragten auf Daten in Dateien beschränkt, die Datenschutzkontrolle bei Datenübermittlungen (Steuergeheimnis) verhindert und Steuerpflichtigen ein Widerspruchsrecht gegen die Datenschutzkontrolle eingeräumt werden. Eine solche Regelung hätte den gegenwärtigen unbefriedigenden Zustand, der eine Datenschutzkontrolle der Steuerbehörden weitgehend unmöglich macht, im wesentlichen fortgeschrieben.

Der Bundesfinanzminister hat inzwischen auf bereichsspezifische Datenschutzvorschriften im Anwendungsbereich der Abgabenordnung verzichtet.

Nunmehr ist beabsichtigt, hinsichtlich der Kontrollbefugnis der Datenschutzbeauftragten das **Bundesdatenschutzgesetz** (BDSG) anzuwenden. Nach Meinung des Bundesfinanzministers kann damit auf die im Referentenentwurf vorgesehenen Einschränkungen verzichtet werden, wenn sichergestellt sei, daß die Datenschutzbeauftragten das Steuergeheimnis nach § 30 Abgabenordnung zu wahren haben.

Der Verzicht auf bereichsspezifische Regelungen im Anwendungsbereich der Abgabenordnung ist zu begrüßen. Nicht hinnehmbar wäre allerdings, wenn, wie es der derzeitige Entwurf zu § 22 Abs. 2 Nr. 3 BDSG vorsieht, die Datenschutzkontrolle dadurch verhindert würde, daß den Betroffenen vor einer Kontrolle Gelegenheit zum Widerspruch zu geben wäre.

10.2 Datenschutzprüfung bei einem Finanzamt

Im 10.Tätigkeitsbericht habe ich gefordert, die Hürde des Steuergeheimnisses vor Datenschutzkontrollen abzubauen. Nach Ansicht der Steuerverwaltung setzt eine Datenschutzkontrolle, bei der Einsicht in personenbezogene Steuerdaten genommen wird, die Entbindung vom Steuergeheimnis durch den Betroffenen voraus. Die Datenschutzbeauftragten sind hingegen der Auffassung, daß ihr gesetzlicher Kontrollauftrag das Recht zur Einsicht in Steuerdaten bereits enthält. Um festzustellen, welche praktischen Auswirkungen diese Meinungsverschiedenheiten zwischen Steuerverwaltung und Datenschutzbeauftragten über den Umfang der Kontrollbefugnis haben, habe ich ein Münchner Finanzamt geprüft. Vor Beginn der Prüfung stellte sich das Finanzamt auf den Standpunkt, daß meine Prüfungsbeamten in Daten von Steuerpflichtigen erst nach Entbindung vom Steuergeheimnis Einblick nehmen dürfen. Auf Vorschlag der Oberfinanzdirektion München wurde dann ein anonymisiertes Prüfungsverfahren getestet. Dabei zeigte sich, daß ein solches Verfahren in keiner Weise eine geeignete Grundlage für datenschutzrechtliche Prüfungen bei Finanzämtern sein kann.
In dem für diese Prüfung zunächst akzeptierten anonymisierten Verfahren wurde so vorgegangen, daß ein Bediensteter des Finanzamtes die Erläuterungen für Datenspeicherungen, ohne die die Notwendigkeit und Richtigkeit der Speicherung nicht überprüft werden kann, aus Steuerakten vorlas. Einsicht in gespeicherte personenbezogene Daten durften meine Beamten über Bildschirm nur nehmen, wenn keine den Steuerpflichtigen identifizierenden Merkmale angezeigt wurden oder wenn die identifizierenden Daten abgedeckt werden konnten. In DV-Ausdrucken wurden die Namens- und Adreßdaten geschwärzt.

Dieses Verfahren erfordert nicht nur einen erheblichen zeitlichen und verwaltungsmäßigen Aufwand. Vor allem läßt es aber keine Feststellungen zu über eventuelle unzulässige Datenspeicherungen oder Datenübermittlungen aus Dateien, die nur aus Steuerakten erkennbar sind. Eine Kontrolle der Steuerverwaltung durch die unabhängige Kontrollinstanz des Datenschutzbeauftragten findet auf eine solche Weise nicht statt. Eine Einwilligungslösung, wie sie der Steuerverwaltung vorschwebt, bei der die Steuerpflichtigen das Finanzamt vor der Prüfung vom Steuergeheimnis entbinden, ist für die Datenschutzkontrolle nicht praktikabel. Denn vor einer Prüfung kann nicht zuverlässig festgelegt werden, welche Steuerpflichtigen um ihre Einwilligung gebeten werden müßten. Eine wirksame Datenschutzkontrolle läßt sich — abgesehen von Einzelbeschwerden — mit dem geschilderten Verfahren nicht durchführen. Wer die Datenschutzkontrolle über die Steuerverwaltung will, darf sie nicht durch das Steuergeheimnis verhindern.

11. Rechnungsprüfung

Bereits in meinem letzten Tätigkeitsbericht (S. 39) bin ich wegen der Anforderung von Beihilfeunterlagen durch den Obersten Rechnungshof und die Prüfungsämter auf das Verhältnis Rechnungsprüfung und Datenschutz eingegangen. Mehrere im Berichtszeitraum eingegangene Anfragen von Behörden, ob Rechnungsprüfungsämter personenbezogene Daten anfordern dürfen, veranlassen mich, dieses Thema erneut aufzugreifen.

Vorlage von Schülerbögen bei einem Staatlichen Rechnungsprüfungsamt

Der Träger einer privaten Sonderschule wurde vom Staatlichen Rechnungsprüfungsamt zur Vorlage von Schülerbögen aufgefordert, die auch Angaben zur bisherigen Schullaufbahn enthielten. Die Vorlage diente zur Überprüfung der Höhe der staatlichen Zuschüsse zum Personal- und Sachaufwand nach dem Bayer. Schulfinanzierungsgesetz, in die auch Privatschulen unter bestimmten Voraussetzungen einbezogen werden können. Desweiteren sollte an Hand der bisherigen Schullaufbahn der Besuch der „richtigen" Sonderschule überprüft und eine Statistik für spätere Bedarfsberechnungen erstellt werden. Der Schulträger fragte über seinen Spitzenverband an, ob die Übermittlung dieses Schülerbogens zulässig sei.

Hierzu ist anzumerken:

Nach Art. 88 der Bayer. Haushaltsordnung (BayHO) prüft der Oberste Rechnungshof die gesamte Haushalts- und Wirtschaftsführung des Staates einschließlich seiner Betriebe und Sondervermögen oder läßt die Prüfung durch die Staatlichen Rechnungsprüfungsämter vornehmen. Bei Stellen außerhalb der Staatsverwaltung, z.B. Privatschulen, erstreckt sich die Prüfung auf die bestimmungsmäßige und wirtschaftliche Verwendung der staatlichen Zuwendungen und — soweit es der Oberste Rechnungshof für notwendig hält — auch auf die sonstige Haushalts- und Wirtschaftsführung des Empfängers (Art. 91 BayHO).

Nach Art. 95 BayHO hat der Auskunftspflichtige diejenigen Unterlagen vorzulegen, die der Rechnungshof zur Erfüllung seiner Aufgaben für erforderlich hält. Es kommt nicht auf die objektive Erforderlichkeit an. Sie sind ihm auf Verlangen innerhalb einer bestimmten Frist vorzulegen oder seinen Beauftragten zu übersenden.

Bei der Bewertung, welche Unterlagen zur Erfüllung ihrer Pflichten erforderlich sind, ist den Prüfungsämtern ein weiter Beurteilungsspielraum eingeräumt. Prüfungsmethode und -umfang sind im Rahmen der einschlägigen Vorschriften dem pflichtgemäßen **Ermessen der Prüfer** überlassen. Auch besteht für die Prüfer keine Pflicht, vorab den Prüfungsumfang festzulegen, da die Prüfung eine umfassende Kontrolle ermöglichen soll. Dies kann im Einzelfall dazu führen, daß sich der Prüfumfang während der Prüfung ändert oder erweitert, weil an unerwarteten Stellen Unstimmigkeiten auffielen, die aufgeklärt werden müssen.

Namentliche Meldung von verhaltensauffälligen Kindern bei Abrechnung von Personalkostenzuschüssen für Kindergärten

Die Bedienstete eines Kindergartens hat sich mit der Frage an mich gewandt, ob sie die **Namen verhaltensauffälliger** und **sprachgestörter Kinder**, die den Kindergarten besuchen, an ihre Wohnortgemeinde weitergeben darf. Die Gemeinde war für die Bewilligung der staatlichen Zuschüsse zuständig und verlangte die Namen als Nachweis für die Förderung von zusätzlichem Kindergartenpersonal — wohl auch für Zwecke der Rechnungsprüfung. Nach Art. 24 Abs. 2 BayKiG i.V.m. der 3. DVBayKiG kann aus „zwingenden Gründen" zusätzliches Personal als förderungswürdig anerkannt werden, wenn beispielsweise die Betreuung besonders zeitaufwendig ist.

Nach Mitteilung des Staatsministeriums für Unterricht und Kultus, das ich um Stellungnahme gebeten habe, bestehen keine Festlegungen, wie der Nachweis der Erforderlichkeit zu erbringen ist. Jedoch müssen die Gründe im Antrag eindeutig dargelegt werden. Eine Überprüfung der zugrundeliegenden Unterlagen muß möglich sein.

Da die Namen der Kinder in Verbindung mit der jeweiligen Art ihrer Behinderung sehr sensible Daten darstellen, habe ich der Gemeinde nahegelegt, **von der Anforderung von Namenslisten abzusehen** und statt dessen nur die Zahl der Behinderten abzufragen oder nur eine anonymisierte Aufstellung der einzelnen Behinderten anzufordern. Im Einzelfall ist dadurch eine Prüfung beim Träger des Kindergartens nicht ausgeschlossen.

Der Bayerische Oberste Rechnungshof hat mir mitgeteilt, daß eine namentliche Benennung der behinderten Kinder in den Bewilligungsakten aus seiner Sicht nicht erforderlich sei. Es reiche aus, wenn die Anzahl der behinderten Kinder in einem Kindergarten und die Art und Schwere ihrer Behinderung allgemein aufgezeigt sowie pädagogisch und zuschußrechtlich gewürdigt würden.

Die Gemeinde hat mir in der Zwischenzeit mitgeteilt, daß sie künftig von der namentlichen Meldung verhaltensauffälliger Kinder absehen wird.

12. Personalwesen

12.1 Neuordnung des Personalaktenrechts

Der Bundesminister des Innern legte einen Gesetzentwurf zur Neuregelung des Personalaktenrechts im öffentlichen Dienst vor. Dabei sollen die zu erhebenden und zu verarbeitenden Daten auf das erforderliche Maß beschränkt, die Verwendungszwecke der Daten bestimmt und der erforderliche Schutz gegen Zweckentfremdung gewährleistet werden.

Der Gesetzentwurf enthält zahlreiche positive Ansätze. Der innerbehördliche Zugriff auf die Personalakte wird beschränkt, die Vorlage von Personalakten sowie die Auskunft hieraus werden auf das erforderliche Maß reduziert. Dem Beamten soll vor der Aufnahme von belastenden Unterlagen in die Personalakte ein Recht zur Äußerung zustehen. Außerdem sind Regelungen zur Aufbewahrungsdauer vorgesehen.

Der Entwurf sollte jedoch aus datenschutzrechtlicher Sicht in einzelnen Punkten noch verbessert werden.

Bisher ist vorgesehen, daß Beihilfeakten rechtlich Teil der Personalakten sind. Die Beihilfeakte kann im Einzelfall sehr sensible Gesundheitsdaten der Beamten und seiner Angehörigen enthalten. **Beihilfevorgänge** sollten daher nicht zur Personalakte gehören. Damit wäre eine strikte

Abschottung der Beihilfesachbearbeitung von der Personalverwaltung besser zu erreichen.

Überarbeitungsbedürftig erscheint mir auch die vorgesehene Regelung zur automatisierten Verarbeitung personenbezogener Daten von Beamten. Bislang ist nicht vorgesehen, die Datenspeicherung auf die für die gesetzliche Aufgabenerfüllung tatsächlich **erforderlichen Angaben** zu beschränken. Nach der Rechtsprechung des Bundesverfassungsgerichts muß aber der Umfang der Datenspeicherung strikt am Erforderlichkeitsgrundsatz orientiert sein. Vorgesehen ist bisher auch der automatisierte Abruf gespeicherter Daten durch andere Behörden. Dies kann jedoch nur vorgesetzten Personalbehörden gestattet werden. Für andere Behörden und andere Geschäftsbereiche kann ein Online-Abruf von Personaldaten nicht in Frage kommen.

Ich habe das Staatsministerium der Finanzen gebeten, im weiteren Verlauf des Gesetzgebungsverfahrens auf die Berücksichtigung meiner Vorschläge hinzuwirken und mich über den Fortgang zu unterrichten.

12.2 Weitergabe von Personaldaten an Verbände

Aufgrund einer Eingabe hatte ich mich erneut mit der Weitergabe von Personaldaten an Berufsverbände zur Veröffentlichung in einem Beschäftigtenverzeichnis zu befassen. Das Staatsministerium für Ernährung, Landwirtschaft und Forsten hatte vierteljährlich Berufsverbände über **Personalveränderungen** unterrichtet. Übermittelt wurden Namen der Betroffenen, bisheriges und neues Amt.

Wie in früheren Fällen (vgl. 6. Tätigkeitsbericht, Nr. 4.9.8, S. 60/61, und 7.Tätigkeitsbericht, Nr. 11.8., S. 53) habe ich die Auffassung vertreten, daß die Veröffentlichung von personenbezogenen Daten in einem Verzeichnis die Betroffenen in ihren schutzwürdigen Belangen beeinträchtigen kann. Dies ergibt sich aus Beschwerden, die im Zusammenhang mit der Veröffentlichung von Personaldaten durch Beamtenverbände vorgetragen worden sind. Der umfassende Überblick, den ein solches Verzeichnis über einen Berufsstand bietet, ist mit Veröffentlichungen im Staatsanzeiger nicht vergleichbar.

Wie anderen Geschäftsbereichen habe ich auch dem Staatsministerium für Ernährung, Landwirtschaft und Forsten empfohlen, allen betroffenen Beamten Gelegenheit zu geben, vor einer bevorstehenden Veröffentlichung bzw. Datenübermittlung zur Veröffentlichung Kenntnis zu nehmen, damit sie der Weitergabe der eigenen Daten **widersprechen** können. Vor einer Weitergabe von Personaldaten an mehrere möglicherweise konkurrierende Verbände habe ich dagegen die Einholung einer Einwilligungserklärung der Betroffenen gefordert. Nach Mitteilung des Staatsministeriums für Ernährung, Landwirtschaft und Forsten werden Personaldaten an Berufsverbände in Zukunft nur noch bei Vorliegen einer Einwilligungserklärung jeder einzelnen in dem Verzeichnis aufgeführten Person weitergegeben.

Aufgrund einer weiteren Eingabe wurde mir folgender Fall bekannt:

Eine Arbeitsgemeinschaft von Berufsschullehrerverbänden plante Ende 1987 die Neuauflage eines Handbuchs „Die beruflichen Schulen in Bayern". In diesem Handbuch sollten unter der jeweiligen Schule auch die Daten der Berufsschullehrer veröffentlicht werden. Zu diesem Zweck verschickte die Arbeitgemeinschaft an die Schulleitungen der Berufsschulen in Bayern Formblätter (sog. Lehrerverzeichnisse) und bat die Schulleiter, in die Formblätter die Daten der Lehrer an ihrer Schule einzutragen. Die Lehrkräfte sollten zum Zeichen des Einverständnisses mit der Veröffentlichung unterschreiben. Die ausgefüllten Lehrerverzeichnisse sollten dann der Arbeitsgemeinschaft zurückgesandt werden. Einzutragen waren Name, Vorname, ggf. Geburtsname, Dienst-/Amtsbezeichnung, Lehramt und Lehrbefähigung, Geburtsjahr sowie „hauptamtlich/hauptberuflich tätig seit..."

Gegen dieses Verfahren wäre datenschutzrechtlich nichts einzuwenden gewesen, wenn die Namen der Lehrer, die der Übermittlung ihrer Daten nicht zugestimmt haben, in der Lehrerliste **unkenntlich** gemacht worden wären. Einzelne Schulleiter sandten aber an die Arbeitsgemeinschaft auch die Lehrerverzeichnisse mit den Daten derjenigen Lehrer zurück, die ihr Einverständnis hierzu nicht erteilt hatten.

Diese Sachbehandlung habe ich beanstandet. Die Daten der Lehrkräfte, die ihre Zustimmung zur Veröffentlichung nicht gegeben hatten, hätten der Arbeitsgemeinschaft gar nicht erst übermittelt werden dürfen. Korrekt wäre es gewesen, wenn die Schulleiter die Daten der Lehrkräfte, die mit der Veröffentlichung nicht einverstanden waren, unkenntlich gemacht, z.B. ausgelackt hätten, oder eine gesonderte Liste mit ausschließlich den Lehrkräften übermittelt hätten, die mit der Veröffentlichung einverstanden waren.

Ich weise noch einmal nachdrücklich darauf hin, daß die Übermittlung von Daten von Behördenbediensteten an Berufsverbände nicht auf Art. 18 BayDSG gestützt werden kann, da nicht davon ausgegangen werden kann, daß durch die Übermittlung an den Berufsverband und durch die Veröffentlichung in einem Handbuch schutzwürdige Belange der Betroffenen nicht verletzt werden.

13. Gewerbe und Handwerk

13.1 Anpassung des Gewerbe- und Wirtschaftsverwaltungsrechts an die Vorgaben des Volkszählungsurteils vom 15.12.1983

Auch das Gewerbe- und Wirtschaftsrecht ist den Vorgaben des Bundesverfassungsgerichts im Volkszählungsurteil anzupassen. Es fehlt vor allem an gesetzlichen Regelungen zur Verarbeitung , insbesondere zur Übermittlung der von den Gewerbeämtern zwangsweise erhobenen Daten. In Bayern wenden die Gewerbebehörden bisher die „Allgemeine Verwaltungsvorschrift für die Behandlung von Anzeigen nach den §§ 14 und 55 c Gewerbeordnung" an. Nach dem Urteil des Bundesverfassungsgerichts erfordert die Verarbeitung zwangsweise erhobener personenbezogener Daten eine normenklare gesetzliche Regelung. Von besonderer Bedeutung ist dies, wenn Gewerbekarteien automatisiert werden.

In der Vergangenheit habe ich gegenüber dem Staatsministerium für Wirtschaft und Verkehr wiederholt gesetzliche Regelungen gefordert. Inzwischen liegt ein vom Bund-Länder-Ausschuß „Gewerberecht" erarbeiteter vorläufiger Referentenentwurf vor. Für dringend nötig halte ich dabei auch eine **bereichsspezifische Regelung** über die Speicherung, Auswertung und Nutzung von Daten, die gesammelt werden, um die Unzuverlässigkeit „des Gewerbetreibenden

oder einer mit der Leitung des Gewerbebetriebes beauftragten Person in bezug auf dieses Gewerbe..." zu belegen (§ 35 Gewerbeordnung). Im Hinblick auf den schnellen Zugriff und die vielfältigen Auswertungsmöglichkeiten einer automatisierten Datei müssen Speicherung und Nutzung gesetzlich eingeschränkt werden. Die automatisierte Speicherung dieser u.U. sehr sensiblen Daten ist für die Betroffenen eine erheblich stärkere Belastung als das bisherige Sammeln (zunächst nicht überprüfter) Mitteilungen in Akten. Hier könnten sich in unverhältnismäßiger Weise geschäftsschädigende Wirkungen durch die Übernahme von zweifelhaften Angaben in eine Datei ergeben. Außer für den Fall des § 35 GewO gilt dies auch für andere gewerberechtliche Zuverlässigkeitsprüfungen (z.B. im Gaststättengesetz).

In diesem Zusammenhang bestehen noch Meinungsverschiedenheiten darüber, ob die Gewerbebehörden bei ihrer Tätigkeit auch Daten **noch nicht rechtskräftig abgeschlossener gerichtlicher oder gewerberechtlicher Verfahren** oder die Tatsache der Einleitung eines solchen Verfahrens speichern dürfen. Ich halte eine Speicherung auch solcher Daten für sinnvoll und notwendig. Würde man nur rechtskräftige Entscheidungen speichern, so würde eine solche Datei ihren Zweck weitgehend verfehlen. Tatsachen, deretwegen ein Gewerbeuntersagungsverfahren eingeleitet ist, müssen bei der Erteilung von Erlaubnissen, bei denen es auf die Zuverlässigkeit ankommt, auch dann berücksichtigt werden, wenn das Verfahren noch nicht abgeschlossen ist. Selbstverständlich muß aber der Ausgang des Verfahrens berücksichtigt werden, wenn das Verfahren noch nicht abgeschlossen ist.

13.2 Datenübermittlung Gewerbeaufsicht/Umweltbehörden

Das Staatsministerium für Arbeit und Sozialordnung bat mich um Äußerung zu einem Gesetzentwurf zu § 139 b Gewerbeordnung. Danach soll die bisherige Regelung, wonach die Gewerbeaufsichtsbehörden vorbehaltlich der Anzeige von Gesetzwidrigkeiten zur Geheimhaltung der amtlich zu ihrer Kenntnis gelangenden Geschäfts- und Betriebsverhältnisse verpflichtet sind, zugunsten der Umweltbehörden durchbrochen werden (Entwurf eines Dritten Rechtsbereinigungsgesetzes). Aufgrund der neuen Regelung wäre eine **Offenbarung von Geschäfts- und Betriebsgeheimnissen** an die Umweltbehörden „zur Erfüllung von gesetzlich geregelten Aufgaben zum Schutz der Umwelt" zulässig.

Aus datenschutzrechtlicher Sicht bestehen gegen eine bessere Information der Umweltbehörden durch die Gewerbeaufsichtsbehörden keine grundsätzlichen Bedenken. Um dem Betroffenen jedoch Gelegenheit zur Korrektur evtl. falsch übermittelter Daten oder zur Erläuterung mitgeteilter Daten zu geben, habe ich vorgeschlagen, im neuen § 139 b Gewerbeordnung die Umweltbehörden zu verpflichten, den Betroffenen oder Dritte über die Datenübermittlung zu unterrichten, soweit und sobald hierdurch die Aufgabenerfüllung der Umweltbehörden nicht gefährdet wird.

13.3 Datenerhebung für Prüfungszulassung

Eine Handwerkskammer veranstaltete einen Ausbildungskurs für die Erlangung des „Computerscheines A". Im Zusammenhang mit der Zulassung zur Prüfung erreichten mich Beschwerden von Prüfungsteilnehmern gegen Art und Umfang der Daten, die mit dem Prüfungsanmeldeformular erhoben wurden. Die Weigerung, Daten anzugeben, die nach Auffassung der Betroffenen überflüssig waren, habe die Handwerkskammer mit der Androhung der Nichtzulassung zur Prüfung beantwortet.

Die zur Stellungnahme aufgeforderte Handwerkskammer verwies auf die von ihrer Vollversammlung erlassenen „besonderen Rechtsvorschriften" für die Prüfung. Das **Anmeldeformular zur Prüfung** enthielt jedoch neben unbedenklichen Fragen zur Person (Name, Anschrift, Geburtsdatum, Geburtsort, betriebliche Anschrift, telefonische Erreichbarkeit) auch Fragen nach Bankverbindung, Staatsangehörigkeit, ausländischem Wohnsitz und schulischer Vorbildung sowie zum Lebenslauf mit zusätzlichen Angaben zu Familienstand, Eltern, Geschwistern, Wehrdienst und ohne Einschränkung auch zu Schulausbildung, Berufsausbildung und beruflichem Werdegang. Ein Hinweis auf die der Datenerhebung zugrunde liegende Rechtsnorm oder auch auf die Freiwilligkeit der Angaben i.S. des Art. 16 Abs. 2 BayDSG fehlte.

Die Erhebung der zuletzt genannten Daten überschreitet den Rahmen des Erforderlichen. Auch für die Zulässigkeit der Speicherung freiwilliger Angaben gilt, daß die Daten zur Erfüllung einer durch Rechtsnorm zugewiesenen Aufgabe erforderlich sein müssen. Nach § 1 der von der Handwerkskammer erlassenen „besonderen Rechtsvorschriften" für die Fortbildungsprüfung hat die Kammer festzustellen, ob „der Prüfling die notwendigen Kenntnisse, Fertigkeiten und Erfahrungen" für eine spätere praktische Tätigkeit im Prüfungsfach besitzt. Zur Prüfung zugelassen werden kann auch, wer „auf andere Weise glaubhaft macht, daß er Kenntnisse, Fertigkeiten und Erfahrungen erworben hat, die die Zulassung zur Prüfung rechtfertigen".

Die Kenntnis der Bankverbindung, des ausländischen Wohnsitzes, des Familienstandes, der Eltern, Geschwister, des Wehrdienstes und der Staatsangehörigkeit kann zum Nachweis dieser Zulassungsvoraussetzungen nicht beitragen. Bei den Fragen nach Lebenslauf, Schulbildung, Berufsausbildung und beruflichem Werdegang sind nur die Angaben erforderlich, die die Glaubhaftmachung einschlägigen Fachwissens ermöglichen. Deshalb muß auch genügen, wenn die Betroffenen auf den Erwerb des nötigen Fachwissens in einem von der Handwerkskammer selbst veranstalteten entsprechenden Ausbildungskurs hinweisen.

Ich habe die Datenerhebung beanstandet und die Handwerkskammer aufgefordert, für die Teilnahme an künftigen Prüfungen **keine überflüssigen und damit unzulässigen Angaben** zu verlangen. Außerdem habe ich die Kammer darauf hingewiesen, daß Prüflingen kein Nachteil entstehen darf, wenn sie nicht erforderliche Angaben verweigern.

Eine abschließende Äußerung der Handwerkskammer steht noch aus. Sie hat aber zwischenzeitlich beim Deutschen Handwerkskammertag eine bundesweite Änderung des Umfangs der Datenerhebung angeregt.

14. Landwirtschaft

Prüfung eines Amtes für Landwirtschaft

Bei einem Amt für Landwirtschaft mit Landwirtschaftsschule habe ich die Abwicklung der landwirtschaftlichen Förderungsprogramme und die landwirtschaftliche Schulverwaltung geprüft. Für diese Bereiche bietet das Staatsministerium für Ernährung, Landwirtschaft und Forsten den Ämtern über Bildschirm ADV-Verfahren im Rahmen des Systems BALIS an. Das Amt speichert als „Herr der Daten" jeweils die Angaben ein, die es zur Bearbeitung der bei ihm eingereichten Förderungsanträge oder zur Schulverwaltung benötigt.

Die Prüfung führte zu folgenden Feststellungen:

Inhalt der Dateien

Die stichprobenweise Überprüfung der vom Amt gespeicherten Daten für die dort genutzten 19 DV-unterstützten Förderungsprogramme hat keinen Anlaß zu Beanstandungen erbracht.

Regelmäßige Datenübermittlungen an das Landwirtschaftsministerium

Bei zahlreichen Förderungsprogrammen ist die regelmäßige Übermittlung personenbezogener Daten des Antragstellers vom Landwirtschaftsamt an das Ministerium vorgesehen. Sie dient teils der Erstellung von Geschäftsstatistiken für den Agrarbericht des Landwirtschaftsministeriums, teils der Erstattung von Förderungsaufwendungen durch den Bund oder die EG. Die Erforderlichkeit der Datenübermittlung wird im Rahmen einer generellen Datenschutzkontrolle des Landwirtschaftsministeriums geprüft werden.

Das Ministerium greift zu diesen Zwecken unmittelbar auf die vom Amt gespeicherten Daten zu. Über den Umfang der Datenübermittlung besaß dieses keine **Übersicht**, obwohl es speichernde Stelle ist. Wenn ein Betroffener Auskunft über regelmäßige Datenübermittlungen im automatisierten Verfahren begehrt, muß das Amt als speichernde Stelle die dem Ministerium zur Verfügung stehenden Daten kennen (Art. 8 Abs. 1 Satz 1 BayDSG).

Einkommensteuerbescheide

Bei der Einsichtnahme in Bearbeitungsunterlagen des Amtes wurden in mehreren Fällen vollständige Einkommensteuerbescheide der Antragsteller aufgefunden, obwohl die Daten des Steuerbescheides zur Sachbearbeitung nur teilweise erforderlich sind. Die Antragsteller müssen künftig darauf hingewiesen werden, welche Daten des Steuerbescheides **unkenntlich gemacht** werden dürfen, weil sie nicht gebraucht werden.

Datenübermittlung an die Hausbank

Zahlreiche Förderungsanträge sind dem Amt nach den Richtlinien des Ministeriums über die Hausbank vorzulegen. Sie erfährt auf diese Weise alle Daten des Antrags samt dessen Anlagen (z.B. Betriebsentwicklungsplan mit über 300 Einzelangaben, Buchführungsnachweis, Einkommen-, Lohn- und Vermögensteuerbescheide für Antragsteller und Ehegatten), ohne daß vorher geklärt würde, welche Angaben die Bank für ihre Kreditbereitschaftserklärung tatsächlich benötigt. **Nur die notwendigen Daten** braucht der Antragsteller der Bank mitzuteilen. Darüber hinausgehende Forderungen der Landwirtschaftsverwaltung sind unzulässig. Die Hausbank erhält andernfalls weit mehr Daten als nötig. Ich habe empfohlen, dem Antragsteller freizustellen, bei der Bank einen gesonderten, auf ihre Bedürfnisse abgestellten Kreditantrag zu stellen.

Übermittlung der Nutzflächen an den Bayerischen Bauernverband

Der Bayerische Bauernverband erhält vom Amt für bestimmte Betriebe Angaben über die Nutzflächen aus dem Gasölverbilligungs-Datenbestand. Der Verband berechnet daraus den Mitgliedsbeitrag. Diese Daten werden jedoch nur übermittelt, wenn der Betroffene vorher schriftlich **eingewilligt** hat.

Vor der Bekanntgabe der Daten an den Bauernverband überzeugt sich das Amt, ob eine Einwilligung in den Akten vorliegt. Für die Erteilung der Einwilligung wird ein Formblatt verwendet, nach dessen Formulierung der Betroffene jederzeit widerruflich das Einverständnis zu dieser Datenübermittlung erklärt. Die im Formblatt abgegebene Einwilligungserklärung bezieht sich allerdings auf das Landwirtschaftsministerium, nicht auf das Landwirtschaftsamt, obwohl dieses die Daten weitergibt.

Datenerhebung bei Dritten

Das Antragsformular für das bayerische Wohnbauprogramm enthält für das Landwirtschaftsamt die Ermächtigung, „zur Nachprüfung der Richtigkeit der im Antrag gemachten Angaben" Auskünfte auch von Dritten einzuholen. Gleichzeitig entbindet der Antragsteller formularmäßig Dritte und andere Stellen von der Schweigepflicht.

Im Hinblick auf den Grundsatz der Erforderlichkeit und Verhältnismäßigkeit muß der Betroffene klar erkennen können, wer als Dritter gemeint ist und welche Daten diesem zur Unterstützung der Auskunftserteilung übermittelt werden. An die Stelle der pauschalen Entbindung müssen daher **Einzelermächtigungen** treten. Ist zum Zeitpunkt der Antragstellung noch nicht bekannt, welche Stellen Auskunft erteilen sollen, dann sollte die bisherige pauschale Ermächtigung durch einen Hinweis ersetzt werden, daß weitere Einwilligungen und Schweigepflichtentbindungen für bestimmte Stellen eingeholt werden können

Datenspeicherung für die Schülerverwaltung

Für die Verwaltung der Schüler an Landwirtschaftsschulen wird auch die Nummer des Betriebes der Eltern des Landwirtschaftsschülers gespeichert.

Die Betriebsnummer könnte den Zugang zu weiteren Daten über den elterlichen Betrieb eröffnen, die dem Amt für andere Zwecke mitgeteilt wurden. Ich habe darauf hingewiesen, daß Voraussetzung für deren Nutzung die Zustimmung des Betriebsinhabers zur Verwendung für schulische Zwecke wäre.

15. Statistik

15.1 Volkszählung 1987

15.1.1 Vernichtung der Volkszählungsunterlagen

Inzwischen sind die Volkszählungsunterlagen aus ganz Bayern vernichtet worden, mit Ausnahme von fünf Gemeinden, deren Widersprüche gegen die Feststellung der amtlichen Einwohnerzahl noch nicht erledigt sind.

Am 20.3.1989 habe ich mich an Ort und Stelle von der ordnungsgemäßen Vernichtung einer Lastzugladung von Fragebögen überzeugt.

15.1.2 Maschinelle Aufbereitung

Bei der Auswertung der Volkszählungsunterlagen ist auch das Gebot der Verfremdung der laufenden Nummern und Ordnungsnummern zu beachten. Mit Hilfe dieser Angaben könnten die Volkszählungsdaten in einem extremen Ausnahmefall einer Person zugeordnet werden. Die Verfremdung dieser vor den einzelnen Datensätzen stehenden Angaben ist erforderlich, um einen Rückgriff auf die Hilfsmerkmale und Ordnungsnummern auszuschließen.

Ich habe das **Verfremdungsprogramm** des Landesamtes für Statistik und Datenverarbeitung geprüft. Ein Reanonymisierungsrisiko war nicht zu erkennen, zumal die Originalunterlagen vernichtet sind.

15.1.3 Blockseitenstatistik

Auch bei der Anfertigung der Blockseitenstatistik ist die Anonymität der Daten zu wahren. Ein Teil der Gemeinden hat beim Landesamt für Statistik und Datenverarbeitung aus dem Ergebnis der Volkszählung 1987 die Erstellung einer Gemeindestatistik nach Blockseiten beantragt. 68 Gemeinden haben im Rahmen der Volkszählung eine Untergliederung ihres Gebiets in Blöcke oder Blockseiten vorgenommen, um aussagekräftigere Statistiken zu erhalten.

Blockseite ist „innerhalb eines Gemeindegebiets die Seite mit gleicher Straßenbezeichnung von der durch Straßeneinmündungen oder vergleichbare Begrenzungen umfaßten Fläche". Die Blockseite ist die unterste Ebene der kleinräumigen Gliederung, die für eine statistische Verwendung vorgesehen werden darf (§ 15 Abs. 4 Satz 3 VZG 1987). Der Block ist die Zusammenfassung mehrerer Blockseiten, der in der Regel von Straßen und natürlichen oder baulichen Grenzen von allen Seiten umschlossen wird.

Die Blockseitenstatistik darf **nicht zu einer Reidentifizierung** der Bewohner führen.

Die Gefahr der Reidentifizierung besteht, wenn die Blockseitenstatistiken in den allgemeinen Verwaltungsvollzug gelangen. Zur Vermeidung des Reidentifizierungsrisikos verfährt das Landesamt für Statistik und Datenverarbeitung wie folgt:

Das Landesamt unterscheidet zwischen Gemeinden, die durch Satzung eine eigene **abgeschottete kommunale Statistikstelle** eingerichtet hat, und solchen, die das nicht getan haben. Eine eigene Statistikstelle haben z.B. die Landeshauptstadt München sowie die Städte Nürnberg und Augsburg. Eine kommunale Statistikstelle ist abgeschottet, wenn sie räumlich und personell vom allgemeinen Verwaltungsbetrieb abgetrennt ist: Beispielsweise darf in der kommunalen Statistikstelle kein Mitarbeiter aus dem allgemeinen Verwaltungsvollzug eingesetzt werden. Nur den abgeschotteten Statistikstellen darf das Landesamt die Blockseitenstatistiken liefern.

Kleinere Gemeinden können sich aus personellen und sachlichen Gründen kein eigenes abgeschottetes Statistikamt leisten. Das Landesamt hat bisher an keine dieser Gemeinden Ergebnisse der Blockseitenstatistik geliefert. Für diese Blockseitenstatistiken gebe es noch keine Regelungen für die statistische Geheimhaltung. Die erforderlichen Geheimhaltungsregelungen würden derzeit im Landesamt erarbeitet. Entscheidende Vorgabe sei, daß eine Reidentifizierung nicht möglich ist.

Ich habe das Landesamt für Statistik und Datenverarbeitung gebeten, mich bei der Ausgestaltung der Geheimhaltungsregelungen zu beteiligen.

15.2 Statistiksatzungen

Im Zusammenhang mit der Volkszählung 1987 sind auch die Statistiksatzungen zu sehen, die von einigen Städten (z.B. in der Landeshauptstadt München und den Städten Nürnberg und Augsburg) im Laufe dieses Jahres erlassen worden sind. In den Statistiksatzungen ist geregelt, unter welchen Voraussetzungen die **statistischen Ämter der Städte** Daten (nicht aus der Volkszählung) im eigenen oder im übertragenen Wirkungskreis sammeln, erheben, statistisch aufbereiten und anonymisiert den städtischen Dienststellen zur Verfügung stellen dürfen. Die Städte haben mir die Entwürfe ihrer Satzungen vor der Verabschiedung zur Begutachtung vorgelegt. Ich hatte dadurch Gelegenheit, Anregungen zur besseren datenschutzrechtlichen Ausgestaltung (z.B. hinsichtlich der Aufgabenstellung, Geheimhaltung u.a.) zu geben, denen weitgehend entsprochen worden ist.

15.3 Gebäude- und Wohnungsstichprobengesetz

Dieser Gesetzentwurf der Bundesregierung sieht alle 5 Jahre, beginnend 1990, eine Erhebung bei 1% der Privathaushalte vor. Die Erhebung soll die erforderlichen Informationen für die Absicherung einer ausgewogenen Wohnungs- und Mietenpolitik bringen. Erhebungseinheiten sind Gebäude, Wohnraum, bewohnte Unterkünfte und Wohnungen sowie die darin wohnenden Haushalte. Auskunftspflichtig sind je nach Erhebungsmerkmal die Gebäudeeigentümer oder -verwalter, Wohnungsinhaber und die einen eigenen Haushalt führenden Personen.

In meiner Stellungnahme gegenüber dem Staatsministerium des Innern habe ich folgende Punkte aufgegriffen und Änderungen vorgeschlagen:

- Als Erhebungsmerkmal ist neben dem Geburtsjahr auch der Geburtsmonat vorgesehen.

Der Geburtsmonat ist jedoch als Erhebungsmerkmal nicht erforderlich. Das **Geburtsjahr** allein ist ausreichend; jedenfalls genügt es für statistische Informationsbedürfnisse, lediglich den Geburtstag in einem näher zu bestimmenden Zeitraum zu erfragen (z.B. 1.1. bis 30.6. oder 1.7. bis 31.12.).

- Gefragt ist auch nach dem **monatlichen Nettoeinkommen** der Haushalte nach Einkommensklassen, wobei die Einkommensklassen nicht näher bestimmt sind.

Gegen die Frage nach dem Einkommen ist grundsätzlich nichts einzuwenden, weil andernfalls der Zweck der Erhebung verfehlt würde. Im Interesse der Bestimmtheit der gesetzlichen Regelung sollten jedoch die Einkommensklassen möglichst im Gesetz selbst festgelegt werden; zumindest sollten die Größenklassen durch Rechtsverordnung bestimmt werden.

- Der Gesetzentwurf enthält keine Aussagen über die **Ausgestaltung** der Erhebungsvordrucke und über das bei der Durchführung der Stichprobe zu beachtende Verfahren, insbesondere darüber, ob die Fragen nur mündlich gegenüber den Erhebungsbeauftragten oder auch schriftlich beantwortet werden können.

  Ich habe nachdrücklich gefordert, im Gesetz auch die Möglichkeit einer **schriftlichen Beantwortung** vorzusehen, damit der einzelne Bürger den Kreis der Personen, die über seine Verhältnisse Kenntnis erhalten, möglichst klein halten kann.

- In das Gesetz sollen Regelungen über die **Vernichtung** der Erhebungsunterlagen aufgenommen werden.

15.4 Viehzählungsstatistik

Durch eine Eingabe wurde mir folgender Fall bekannt:

Eine Gemeinde im ländlichen Raum hat für die Erstellung von Planungsunterlagen zum Bau einer Wasserversorgungsanlage zur Schätzung des Wasserverbrauches Viehzählungslisten der Viehzählung 1982 verwendet und die Planungsunterlagen einem Ingenieurbüro überlassen.

Bei der Viehzählung handelt es sich um eine gesetzlich angeordnete Bundesstatistik im Sinne des § 5 Bundesstatistikgesetz, für die Auskunftspflicht besteht (§ 4 Abs. 2 Viehzählungsgesetz). Die aufgrund des Viehzählungsgesetzes erhobenen Daten dienen zur Erfassung des vorhandenen Viehbestandes und werden von den Gemeinden an das Landesamt für Statistik und Datenverarbeitung weitergeleitet und dort ausgewertet. Dieses wiederum teilt den Gemeinden statistische Größen über die Viehzählung mit.

Nach § 16 Bundesstatistikgesetz sind Einzelangaben über persönliche und sachliche Verhältnisse, die für eine Bundesstatistik gemacht werden, von den Amtsträgern, die mit der Durchführung der Bundesstatistik betraut sind, geheimzuhalten. Sie dürfen auch nicht zur Erstellung von Planungsunterlagen verwendet werden.

Die Verwendung der alten Viehzählungsdaten bei der Erstellung der **Planungsunterlagen** und deren Weitergabe an das Ingenieurbüro war datenschutzrechtlich **unzulässig**. Ich habe gem. Art. 30 Abs. 1 BayDSG diese Verwendung der Viehzählungslisten beanstandet.

16. Schulwesen

Bereits in meinem letzten Tätigkeitsbericht habe ich positiv vermerkt, daß das Staatsministerium für Unterricht und Kultus auf die Verwendung einheitlicher Schulverwaltungsprogramme Wert gelegt hat, die zentral auf die Beachtung des geltenden Rechts überprüft sind.

Das Staatsministerium für Unterricht und Kultus hat zwischenzeitlich ausdrücklich angeordnet, daß ab 1. Juni 1989 an staatlichen Schulen landeseinheitlich grundsätzlich nur mehr die **bayerischen Schulverwaltungsprogramme** zur EDV-mäßigen Verwaltung von Schüler- und Lehrerdaten eingesetzt werden dürfen. Der Erwerb kommerzieller Programme ist ab diesem Zeitpunkt grundsätzlich nicht mehr zulässig. Diese Vereinheitlichung der Schulverwaltungsprogramme liegt im Interesse des Datenschutzes: Datenschutz und Datensicherheit sind am besten dann gewährleistet, wenn einheitliche Programme zum Einsatz kommen, die zentral entwickelt und gepflegt werden. Auf diese Weise können z. B. unzulässige Überschreitungen des Datenrahmens an einzelnen Schulen sicher ausgeschlossen und nachträgliche Veränderungen des Datensatzes aufgrund von Änderungen des Schulrechts gezielt und unter Beachtung der Datenschutzregelungen vorgenommen werden.

16.1 Neubekanntmachung „Erläuternde Hinweise zum Datenschutz"

Im März 1989 veröffentlichte das Staatsministerium für Unterricht und Kultus die Neufassung der Bekanntmachung „Erläuternde Hinweise für den Vollzug des Bayer. Datenschutzgesetzes", die die Bekanntmachung aus dem Jahr 1979 ablöste. Die Hinweise, an deren Ausarbeitung ich beteiligt war, sind nunmehr auf dem neuesten rechtlichen Stand und berücksichtigen auch die seither eingetretene technische Entwicklung sowie die erweiterte Einsatzmöglichkeit von Rechnern. Zum Beispiel ist dem Thema „Datenverarbeitung auf privaten Rechnern der Lehrer" ein eigenes Kapitel gewidmet. Das Ministerium legt die Grenzen der Datenverarbeitung auf privaten Rechnern fest. Beispielsweise dürfen nur die Daten derjenigen Schüler verarbeitet werden, die der Lehrer selbst als Fachlehrer unterrichtet. Es gibt Hinweise zur Datensicherheit und bestimmt schließlich, daß jeder Lehrer, der einen privaten Rechner für die Erledigung schulischer Aufgaben nutzen will, dies vorher seiner Schule mitteilen und eine Genehmigung einholen muß.

16.2 Vorschulische gesundheitliche Untersuchung

Die Mutter eines 5jährigen Kindes beschwerte sich bei mir über den Ablauf einer vorschulischen gesundheitlichen Untersuchung.

Die Untersuchung fand, da kein anderer Raum zur Verfügung stand, in der Turnhalle eines Kindergartens statt, wobei bei der Untersuchung andere Kinder mit ihren Eltern anwesend waren. Die Turnhalle war nicht in „Wartezimmer" und „Sprechzimmer" abgeteilt. Außerdem wurden gleichzeitig mehrere Kinder untersucht. Die Mutter beklagte, ihr Sohn habe die Anwesenheit der anderen Personen als unangenehm empfunden und sich infolgedessen gegen die Untersuchung gesträubt. Die untersuchende Ärztin habe laut und auch für andere vernehmbar an sie Fragen über den gesundheitlichen Zustand ihres Sohnes gestellt; andererseits habe sie auch mitbekommen, was die Ärztin bei den anderen Kindern festgestellt habe.

Das Staatsministerium des Innern hat eingeräumt, daß die Untersuchung unerfreulich verlaufen sei. Es sei vor allem versäumt worden, die Eltern darüber aufzuklären, daß die Untersuchung auf Wunsch auch in einem abgetrennten Raum durchgeführt werden könne. Das Ministerium hat die betroffene Gesundheitsbehörde gebeten, dafür Sorge zu tragen, daß künftig bei der Untersuchung von Kindern den

Belangen des Datenschutzes und der **ärztlichen Schweigepflicht** in vollem Umfang Rechnung getragen wird.

16.3 Datenübermittlungen im Schulbereich

- Ein Verein zur Förderung spastisch Gelähmter und anderer Körperbehinderter betreibt eine Schule für Körperbehinderte in der Rechtsform der staatlich genehmigten privaten Schule und gleichzeitig eine **heilpädagogische Tagesstätte**, in der die Schüler außerhalb der Schulzeit betreut werden. Der Verein wollte wissen, ob die Schule personenbezogene Schülerdaten an die heilpädagogische Tagesstätte herausgeben dürfe.

  Auf die Datenverarbeitung in staatlich genehmigten privaten Schulen ist das Bundesdatenschutzgesetz (BDSG) anzuwenden. Nach § 24 BDSG ist die Übermittlung personenbezogener Daten vor allem „im Rahmen der Zweckbestimmung eines Vertragsverhältnisses oder vertragsähnlichen Vertrauensverhältnisses" zulässig. Ob damit die Übermittlung von Schülerdaten an die heilpädagogische Tagesstätte gedeckt ist, ist nur an Hand der genauen Kenntnis der näheren Umstände zu klären. Dessenungeachtet habe ich dem Verein empfohlen, von den Eltern bzw. Erziehungsberechtigten der Schüler vertraglich die Zustimmung zur Übermittlung der gewünschten Daten an die heilpädagogische Einrichtung einzuholen, soweit sie nicht bereits vorliegt.

- Ein **Sozialer Beratungsdienst** einer Kirchengemeinde hat bei mir angefragt, ob er Adressen und Telefonnummern von Schulabgängern („aktuellen" und ehemaligen) einer Sonderberufsschule erhalten könne, damit er die Schulabgänger in den ersten Jahren ihres Berufslebens begleiten oder im Falle der Arbeitslosigkeit sozial unterstützen könne.

  Die Weitergabe von Daten und Unterlagen über Schüler ist in Art. 62 Abs. 2 des Bayerischen Gesetzes über das Erziehungsund Unterrichtswesen (BayEUG) geregelt. Danach ist die Weitergabe von Daten und Unterlagen (darunter fallen auch die Anschriften und Telefonnummern) an außerschulische Stellen untersagt, falls nicht ein **rechtlicher** Anspruch auf die Herausgabe der Daten nachgewiesen wird. Auch ehemalige Schüler sind durch diese Vorschrift geschützt. Einen „rechtlichen" Anspruch auf die Herausgabe der Daten kann der Soziale Beratungsdienst, bei aller Anerkennung seines sozialen Engagements, nicht geltend machen.

  Ich habe ihm deshalb folgenden Weg vorgeschlagen, den er auch akzeptiert hat:

  Der Dienst verfaßt Schreiben an die ehemaligen Schüler und steckt sie in unbeschriftete Briefumschläge. Die Umschläge läßt er durch die Sonderberufsschule mit den Adressen der ehemaligen Schüler versehen und dann versenden. Eine unzulässige Datenübermittlung durch die Schule findet auf diese Weise nicht statt; es bliebe den Adressaten überlassen, sich mit dem Sozialen Beratungsdienst in Verbindung zu setzen.

- Der Elternbeiratsvorsitzende eines Gymnasiums hat mich gefragt, ob die Schulverwaltung an den **Elternbeirat** die Anschriften der Eltern der **volljährigen** Schüler herausgeben darf. Der Elternbeirat möchte die Eltern der volljährigen Schüler anschreiben und um eine „Elternspende" für Aktivitäten (z.B. Zuschuß zu Klassenfahrten und Schulfesten) bitten.

  Art. 62 Abs. 2 BayEUG ist nicht einschlägig, da der Elternbeirat keine außerschulische Stelle im Sinne dieser Bestimmung ist. Ein „rechtlicher Anspruch" des Elternbeirats ist daher nicht erforderlich. Die Herausgabe der Adressen beurteilt sich nach Art. 17 Abs. 1 und 3 BayDSG.

  Danach ist die Übermittlung personenbezogener Daten an andere öffentliche Stellen zulässig, wenn sie zur rechtmäßigen Erfüllung der durch Rechtsnorm der übermittelnden Stelle oder dem Empfänger zugewiesenen Aufgaben erforderlich ist.

  Entscheidend ist hier, ob es Aufgabe des Elternbeirats ist, Spendenbriefe zu verfassen. Dies wird man dem Elternbeirat zubilligen können; die aufgabenzuweisende Rechtsvorschrift ist § 113 Abs. 1 Nr. 3 der Gymnasialschulordnung i.V.m. Art. 43 EUG. Wenn der Elternbeirat bei der Durchführung von Veranstaltungen, die der Pflege und Förderung der Gemeinschaftsarbeit von Schule und Elternhaus dienen, sowie bei Fragen der schulischen Freizeitgestaltung mitwirkt, kann man ihm auch das Recht einräumen, für diese Aktivitäten die erforderlichen Mittel zu besorgen. Dies gilt auch, wenn die Eltern volljähriger Schüler angeschrieben werden sollen. Der Aufgabenbereich des Elternbeirats ist bezüglich der volljährigen Schüler nicht eingeschränkt.

  Ich habe deshalb gegen die Datenübermittlung an den Elternbeirat keine datenschutzrechtlichen Bedenken geäußert.

- Der Schulleiter einer **Sprachheilschule** hat an mich die Frage gerichtet, ob und unter welchen Voraussetzungen er die Intelligenzquotienten von Schülern an das staatliche Schulamt weitergeben dürfe. Die Intelligenzquotienten wurden im Einvernehmen mit den Eltern aus unterrichtsmethodischen Gründen erhoben. Das Schulamt habe zur Vorlage der Intelligenzquotienten aufgefordert, um feststellen zu können, ob die betroffenen Kinder der ersten und zweiten Jahrgangsstufe begabungsmäßig zu Recht die Sprachheilschule besuchen.

  Im Einvernehmen mit dem Staatsministerium für Unterricht und Kultus vertrete ich dazu folgende Auffassung: Gem. Art. 15 Abs. 1 Schulpflichtgesetz besteht für die Sonderschulpflichtigen die Verpflichtung, eine geeignete Sonderschule zu besuchen. Daraus sind für die Schulaufsicht das Recht und die Pflicht abzuleiten, bei Bedarf korrigierend einzugreifen, z.B. für die Überweisung in die Sondervolksschulen zu sorgen. Wenn das Schulamt den Verdacht hat, daß Kinder zu Unrecht eine bestimmte Sondervolksschule besuchen, ist es berechtigt, als Grundlage für die nähere Überprüfung die IQ-Daten von Schülern vergleichbarer Schulen anzufordern. Für vergleichende Bewertungen über mehrere Schulen mit allen Schülern wird hierzu eine Übermittlung ohne Personenbezug in der Regel genügen.

- Ein Landratsamt hat an mich folgendes Problem herangetragen:

  Die **Beförderung von Schülern durch die Deutsche Bundesbahn** im Vollzug des Gesetzes über die Kostenfreiheit des Schulweges erfolgt bundeseinheitlich

auf der Grundlage von Tarifbestimmungen und einer Vereinbarung zwischen der Deutschen Bundesbahn und den einzelnen Kostenträgern. Hierbei gibt die Bahn an die beförderungsberechtigten Schüler über die Schulwegkostenträger Abonnementkarten aus und zieht die Kosten für die Karten von den Schulwegkostenträgern ein. Schulwegkostenträger sind in Bayern die Landkreise und kreisfreien Städte.

Bei einer mit Ausgehunfähigkeit verbundenen Krankheit eines Schülers besteht wegen der nicht voll ausgenutzten Schülerjahreskarten gegebenenfalls ein Erstattungsanspruch des Schulwegkostenträgers gegen die Deutsche Bundesbahn. Das Verfahren für die Erstattung läuft folgendermaßen ab:

Die Schulwegkostenträger erhalten die Krankmeldung der Schüler von den Schulen und leiten sie namentlich der Deutschen Bundesbahn weiter. Bei einer Krankheit von mehr als 14 Tagen ist ein ärztliches Attest oder eine Krankenhausbescheinigung vorzulegen.

Ich habe gegenüber dem für die Deutsche Bundesbahn zuständigen Bundesbeauftragten für den Datenschutz die Frage aufgeworfen, ob die Deutsche Bundesbahn die Namen der erkrankten Schüler benötigt, oder ob nicht die Übermittlung der Zahl der erkrankten Schüler und der Krankheitstage für Abrechnungszwecke genügt. Ferner habe ich Zweifel daran geäußert, daß die Deutsche Bundesbahn ärztliche Atteste benötigt. Meiner Ansicht nach reichen Bescheinigungen aus, die die Schule ausstellt. Begründet habe ich meine Auffassung damit, daß in der derzeitigen, die schutzwürdigen Belange der Schüler wenig berücksichtigenden Verfahrensweise ein unnötiges Mißtrauen gegen den Schulwegkostenträger liegt. Als Alternative habe ich vorgeschlagen, der Deutschen Bundesbahn Stichproben in den Schulen und hierbei Einsichtnahmen in die einzelnen ärztlichen Atteste zu gestatten.

Die Deutsche Bundesbahn erklärte, die Übermittlung der Namen der Schüler sei erforderlich, um u.a. festzustellen, zu welchem Preis die Schülerjahreskarte ausgegeben wurde. Auf der Vorlage einer ärztlichen Bescheinigung bei einer Krankheit von mehr als 14 Tagen besteht die Deutsche Bundesbahn jedoch nicht mehr. Insoweit wurde die Vereinbarung zwischen der Deutschen Bundesbahn und dem Schulwegkostenträger geändert. Es reicht der Deutschen Bundesbahn nunmehr aus, daß der Schulwegkostenträger in den Fahrpreiserstattungsanträgen bescheinigt, daß die ärztlichen Atteste bei ihm vorliegen. Die Deutsche Bundesbahn begnügt sich mit Stichproben. Damit wird meinem Anliegen zumindest für die sensiblen ärztlichen Atteste Rechnung getragen.

Dieser Fall gibt über die datenschutzrechtlichen Aspekte hinaus Anlaß zum Nachdenken über den mehr als beträchtlichen Verwaltungsaufwand, der bei Schulen, Schulwegkostenträgern und Bundesbahn zur Abwicklung eines Erstattungsverfahrens erforderlich ist und dessen finanzieller Ertrag für die Beteiligten gering sein dürfte. Wenn es schon nicht möglich sein sollte, auf die Erstattungsbeträge gegenüber der Bahn gänzlich zu verzichten, so sollte es doch wenigstens möglich sein, diese Beträge auf der Grundlage der Erfahrungen der letzten Jahre zu pauschalieren. Nicht zuletzt wäre damit auch dem Datenschutz gedient.

16.4 Prüfung von Schulen

Da auch an Schulen eine Vielzahl personenbezogener Daten verarbeitet wird, habe ich im Berichtszeitraum mehrere Gymnasien auf die Rechtmäßigkeit und Erforderlichkeit ihrer Datenverarbeitung überprüft.

Erfreulicherweise konnte ich feststellen, daß dem Datenschutz von seiten der Schulen großes Interesse entgegengebracht wird. Grobe Datenschutzverletzungen wurden nicht festgestellt. Insbesondere orientieren sich die in den automatisierten Schüler- und Kollegstufendateien gespeicherten Daten an den Vorgaben, die das Kultusministerium für die Schulverwaltungsprogramme im Rahmen seiner „Erläuternden Hinweise für die Schulen zum Vollzug des Bayerischen Datenschutzgesetzes" vorgegeben hat. Wiederholt habe ich allerdings die Speicherung des Merkmals **„Beruf des/der Erziehungsberechtigten"** festgestellt, obwohl dieses Merkmal nicht mehr vorgesehen ist.

Die Mehrzahl der festgestellten Mängel lag bei den manuellen Karteien, die bisher an den Schulen zu Verwaltungszwecken vorgehalten wurden und auch neben den automatisierten Schulverwaltungsprogrammen noch Verwendung finden. Hier fehlte des öfteren der Hinweis auf die Rechtsgrundlage für die Datenerhebung oder beispielsweise bei der Frage nach „gesundheitlichen Rücksichten wegen" die Freiwilligkeit der Angabe. Manche der teilweise von Verlagen angebotenen Karteikarten enthielten auch Fragen, deren Beantwortung für schulische Aufgaben nicht erforderlich und deren Speicherung damit unzulässig ist.

16.5 Einwilligungserklärung bei Forschungsvorhaben

Aufgrund einer Eingabe ist mir ein Forschungsvorhaben des Max-Planck-Instituts an Volksschulen bekannt geworden. Gegen das Forschungsvorhaben selbst war nichts einzuwenden, wohl aber gegen die dabei vorgesehene „Einwilligungserklärung" der Eltern bzw. Erziehungsberechtigten. Darin hieß es u.a.:

„Ich möchte nicht, daß mein Kind an der Studie teilnimmt."

Diese Erklärung (ein abtrennbarer Abschnitt auf einem Formblatt) mußten die Kinder beim Klassenlehrer abgeben.

Eine derartige „Einwilligungserklärung" ist faktisch eine Verweigerungserklärung. Auf die Eltern wird — jedenfalls indirekt Zwang ausgeübt, die Nichtteilnahme ihres Kindes an der Studie dem Lehrer und den Mitschülern ausdrücklich zu offenbaren. Möglicherweise werden manche Eltern unter diesen Umständen verzichten, diesen Abschnitt auszufüllen und ihrem Kind mitzugeben, obwohl sie mit der Teilnahme ihres Kindes — aus welchen Gründen auch immer — eigentlich nicht einverstanden sind. Ich habe deshalb folgende „neutrale" Fassung der elterlichen Erklärung für notwendig gehalten:

„Mit der Teilnahme meines Kindes an der Studie bin ich einverstanden — bitte ankreuzen:

O ja
O nein."

16.6 Automatisierte Lehrerdateien (DIAPERS)

Bereits in meinem letzten Tätigkeitsbericht habe ich mich zum Personalverwaltungsverfahren DIAPERS geäußert. Das elektronische Stellen- und Personalverwaltungssystem

DIAPERS erledigt bei den Regierungen Routinearbeiten und Planungsaufgaben und dient als aktuelle Informationsbasis. Dienstvereinbarungen über die Einführung des Verfahrens zur Verarbeitung von Lehrerdaten wurden von den Staatsministerien des Innern und für Unterricht und Kultus jeweils mit ihren Hauptpersonalräten abgeschlossen.

In DIAPERS werden nur Daten gespeichert, die für die Personalverwaltung **unbedingt notwendig** sind. Umfangreiche Datensicherungsmaßnahmen sorgen dafür, daß jeder Personalsachbearbeiter nur in seinem Zuständigkeitsbereich auf DIAPERS zugreifen kann. Wie im letzten Tätigkeitsbericht bereits erwähnt, ist die automatisierte Fertigung eines Persönlichkeits- oder Leistungsprofils nicht möglich, da hierfür weder die Daten noch die Programme vorhanden sind. Jeder Beschäftigte erhält alle vier Jahre einen Ausdruck aller über ihn gespeicherten Daten.

16.7 Erhebungen des Staatsinstituts für Schulpädagogik und Bildungsforschung

Das Staatsinstitut für Schulpädagogik und Bildungsforschung ist eine dem Staatsministerium für Unterricht und Kultus unmittelbar nachgeordnete Einrichtung, welche die Erkenntnisse der Forschung und die Erfahrungen aus der Praxis für die Schule nutzbar macht und das Kultusministerium bei der Weiterentwicklung des Schulwesens unterstützt. Zu diesem Zweck führt es regelmäßig Erhebungen zur Bildungssitutation der Schüler an Grund- und Hauptschulen durch. Erhebungen des Staatsinstituts für Schulpädagogik und Bildungsforschung sind stets vom Staatsministerium für Unterricht und Kultus zu genehmigen. Dieses macht die Genehmigung von einer Reihe von Voraussetzungen abhängig. So muß beispielsweise ein erhebliches pädagogisch-wissenschaftliches Interesse an der Erhebung bestehen. Die Belastung der Schule muß sich in zumutbarem Rahmen halten. Ferner muß gesichert sein, daß bei der Erhebung personenbezogener Daten die Datenschutzbestimmungen sorgfältig eingehalten werden. Durch die Genehmigungspflicht ist so bereits im Vorfeld eine rechtliche Überprüfung der einzelnen Erhebungen durch das Kultusministerium sichergestellt, was ich ausdrücklich begrüße.

Von entscheidender Bedeutung für mich ist die Gewißheit, daß aus Datenerhebungen für Forschungszwecke **keine Rückschlüsse** auf einzelne Personen gezogen werden können. Die Anonymität der betroffenen Schüler muß gewahrt bleiben. Diese Voraussetzung habe ich bei einer Befragungsaktion im Sommer 1989 nicht für gegeben erachtet. Von der Untersuchung waren ausländische Schüler und Schülerinnen an Gymnasien betroffen. In den Fragebögen, die von der Schule und nicht von den Schülern auszufüllen waren, sollten zwar nicht die Namen und Anschriften der Schüler, jedoch der Name der Schule und der Schulort eingetragen oder der Schulstempel verwendet werden. Damit war die Gefahr der Reidentifizierung der Schüler nicht vollständig ausgeschlossen. Um das Reidentifizierungsrisiko völlig auszuschließen, habe ich das Staatsministerium für Unterricht und Kultus gebeten, das Staatsinstitut zu veranlassen, bei der laufenden Erhebung den Namen und den Ort der Schule im Fragebogen nicht eintragen zu lassen. Soweit diese Angaben bereits eingetragen und die Fragebögen zurückgesandt waren, sollte das Institut dafür Sorge tragen, daß diese Daten umgehend vernichtet werden. Dieser Bitte hat das Kultusministerium im wesentlichen entsprochen. Das Ministerium hat ferner gegenüber dem Staatsinstitut schriftliche Anweisung erteilt, bei künftigen Umfragen, bei denen eine Reidentifizierung nicht ausgeschlossen werden könne, zumindest auf die Angabe der Schule auf dem Fragebogen zu verzichten.

Bei solchen Umfrageaktionen geht es mir auch darum, daß die für das Forschungsvorhaben notwendigen Daten möglichst den in den Schulen vorhandenen **Unterlagen** (Schülerakt bzw. -bogen und der Schülerbeobachtungsbogen) entnommen und die Daten nicht bei den Schülern selbst erhoben werden. Dieses Verfahren stellt sicher, daß nicht über den Schulbereich hinausgehende Daten erhoben werden. Auch ist die Gewähr für deren Richtigkeit eher gegeben. Zudem stellt sich nicht das Problem der Wirksamkeit etwa notwendiger Einwilligungen in solche Datenerhebungen. Schließlich würden die Schüler unnötig belastet, wenn sie vor der Klasse zu ihren sozialen Verhältnissen Auskunft geben müßten. Bei einer Befragung, die mir anläßlich einer Eingabe bekannt wurde, war dieses Verfahren nicht sichergestellt. Ich habe deshalb das Kultusministerium um Einhaltung dieses Verfahrens gebeten.

17. Hochschule

17.1 Abschluß der datenschutzrechtlichen Prüfung der Ludwig-Maximilians-Universität München

In meinem letzten Tätigkeitsbericht hatte ich erwähnt, daß die Aufbewahrung der statusrechtlichen Unterlagen der Studenten (z.B. Name und Adresse des Studenten, Angaben zum Studium und zu den abgelgeten Prüfungen) noch nicht geregelt ist. Inzwischen liegt die interne Dienstanweisung der Universität München vor. Sie regelt die Erfassung der statusrechtlichen Daten der Studenten sowie die Aussonderung und Archivierung der Daten.

17.2 Herausgabe von Studentendaten

Immer wieder erreichen mich Anfragen von Studenten, die den Verdacht äußern, die Universitätsverwaltung würde ihre Daten (Namen, Anschriften, Telefonnummern) an Versicherungen, Banken oder andere Stellen herausgeben. Folgende Fälle sind dafür beispielhaft:

- Eine Studentin im Prüfungssemester erhielt Post von einer Krankenversicherung.

  Es stellte sich heraus, daß die Studentin in einer Liste der Prüfungsteilnehmer aufgeführt war, die in einem Institut der Universität ausgehängt war. Die Liste der Prüfungsteilnehmer enthielt nur die Namen der Studenten, nicht jedoch Anschriften oder Telefonnummern. Ein Mitarbeiter der Krankenversicherung notierte sich den Namen der Studentin aus der Liste der Prüfungsteilnehmer. Die Anschrift der Studentin entnahm er anschließend dem örtlichen Stadtadreßbuch.

- Ein Student erhielt im Rahmen der AIDS-Aufklärung Informationsmaterial vom Bundesgesundheitsministerium. Er verdächtigte die Universitätsverwaltung, sie habe seinen Namen und seine Anschrift an das Bundesgesundheitsministerium übermittelt.

Der Verdacht war unbegründet. Vielmehr hatte das Bundesgesundheitsministerium die AIDS-Informationsschriften zunächst der Universitätsverwaltung zugeleitet. Die Universitätsverwaltung hat daraufhin das Schreiben an die Studenten adressiert und versandt.

In beiden geschilderten Fällen lagen also keine unzulässigen Datenübermittlungen aus dem Bereich der Universitätsverwaltungen vor.

17.3 Hochschulstatistik

Im Sommer dieses Jahres legte die Bundesregierung den Entwurf eines Gesetzes über die Statistik für das Hochschulwesen (Hochschulstatistikgesetz — HStatG) vor. In der Hochschulstatistik werden in anonymisierter Form Daten von Studenten und Hochschulbediensteten sowie über Hochschuleinrichtungen erhoben. Das geltende Hochschulstatistikgesetz stammt aus dem Jahr 1980 und wird den verfassungsrechtlichen Anforderungen des Volkszählungsurteils nicht gerecht. Die nach diesem Gesetz zu erhebenden Daten dienen neben statistischen Zwecken zugleich als Grundlage für die Arbeit der Hochschulverwaltung.

Der neue Gesetzentwurf berücksichtigt die vom Bundesverfassungsgericht aufgestellten verfassungsrechtlichen Grundsätze hinsichtlich des informationellen Selbstbestimmungsrechts (z.B. Zweckbindungsgebot für die Statistik, Trennung von Statistik und Verwaltungsvollzug). Des weiteren soll auf die personenbezogene Befragung der Prüfungsteilnehmer und auf die Verknüpfung von Einzeldaten der Studentenbestandsdateien mit der Prüfungsteilnehmerdatei sowie auf die Studienverlaufstatistik verzichtet werden. Datenschutzrechtliche Verbesserungen sind noch wünschenswert hinsichtlich einzelner Erhebungsmerkmale. So wird etwa noch nach dem Geburtsmonat des Studenten gefragt; hier müßte das Geburtsjahr als Erhebungsmerkmal ausreichen. Außerdem müßten in dem Gesetzentwurf noch Löschungsvorschriften aufgenommen werden.

18. Archivwesen und Forschung

18.1 Bayerisches Archivgesetz

Noch im letzten Tätigkeitsbericht (S. 46) konnte ich berichten, daß der am 3.5.1988 von der Staatsregierung beschlossene Entwurf meinen Vorstellungen weitgehend Rechnung trage.

Auf Vorschlag des Ausschusses für kulturpolitische Fragen hat der Bayerische Landtag das Archivgesetz in einer Fassung beschlossen, in welcher der Datenschutz abgeschwächt ist:

Nunmehr kann jedermann Archivgut benützen, soweit er nur ein **berechtigtes Interesse** an der Benutzung glaubhaft macht. Danach kann das Archiv von einer Vielzahl von Personen für eine Vielzahl von Zwecken benützt werden, **die über die derzeitige Nutzung** (u.a. für amtliche und wissenschaftliche Zwecke) hinausgehen kann. Während bisher z.B. heimatkundliche und familienkundliche Forschung einem gewissen wissenschaftlichen Anspruch genügen mußte, werden diese Anforderungen bei der beschlossenen Fassung nicht mehr gestellt. Dies bedeutet: Jeder Bürger, dessen Daten zwangsweise von einer Behörde erhoben werden, oder der sich an eine Behörde gewandt hat, muß grundsätzlich damit rechnen, daß nach Ablauf der Sperrfrist seine Unterlagen von einer Vielzahl von Personen eingesehen werden können.

Erfreulich ist immerhin, daß der Gesetzgeber weitergehenden Forderungen der zeitgeschichtlichen Forschung nicht nachgegeben und den Schutz der Persönlichkeit höher bewertet hat als den Drang nach Bewältigung und Aufarbeitung der Gegenwart, noch ehe sie Zeit-Geschichte geworden ist.

Durch diese Erweiterung der Benutzungszwecke wird allerdings nur die vorderste Schutzschranke gegen mißbräuchliche Archivnutzung zurückgenommen. Die weiteren Schranken, nämlich die Beachtung von Schutzfristen und die Pflicht der Archivbehörden, die Einsicht bei zu befürchtender Verletzung des Persönlichkeitsrechts zu versagen, bleiben bestehen, so daß insgesamt noch ein ausreichender Datenschutz gewährleistet bleibt.

Die nunmehr beschlossene Fassung des Gesetzes, die den zur Einsicht berechtigten Personenkreis erweitert, stellt an die Archivbehörden bei der Prüfung der Einsichtsbegehren weit höhere Anforderungen als der Regierungsentwurf. Um den notwendigen Persönlichkeitsschutz zu gewährleisten, wird die Archivbehörde bei Zweifeln, ob das Persönlichkeitsrecht des Betroffenen verletzt ist, vor der Gewährung von Einsicht in Archivgut um eine **Anhörung etwaiger Betroffener** nicht herumkommen.

18.2 Datenschutz und zeitgeschichtliche Forschung

Die zeitgeschichtliche Forschung beschäftigt sich zeitnah mit Informationen aus Politik und Verwaltung. In der Regel arbeitet sie nicht mit bereits archiviertem und deshalb nach allgemeinen Zugangsregelungen den Wissenschaftlern eröffnetem Material, wie sie inzwischen für die Verwendung von archivierten Daten durch das Bayer. Archivgesetz geschaffen worden sind.

Die Wissenschaftler beklagen zunehmend, daß der Datenschutz ein Hindernis für die notwendige umfassende und effiziente Forschung darstelle. Manche Probleme, welche die zeitgeschichtliche Forschung sieht, liegen weniger im Bereich des Datenschutzes als vielmehr in der Entwicklung der Informationstechnologien. Der Trend zur „flüchtigen" Speicherung auf Bändern, Disketten und Platten unter dem Diktat der Wirtschaftlichkeit und Effizienz der Verwaltung wird sich kaum aufhalten lassen. Vorgänge sind dadurch aber nicht mehr vollständig durch schriftliche Unterlagen nachgewiesen. So können Entwicklungszusammenhänge verloren gehen.

Neben technischen Sachzwängen kann aber auch der Datenschutz der Grund dafür sein, daß Daten den zeitgeschichtlichen Forschern nicht zur Verfügung stehen. Datenschutzvorschriften grenzen Datenübermittlungen ein, zwangsläufig auch solche an Forscher. Sie legen die Pflicht fest, Daten zu sperren oder zu löschen. Damit können Datenschutzvorschriften auch zeitgeschichtlichen Forschern den Zugang zu personenbezogenen Daten verwehren.

Das Recht auf Wissenschaftsfreiheit ist, wie ich schon in meinem 8. Tätigkeitsbericht (S. 52) ausgeführt habe, verfassungsrechtlich durch Art. 5 Abs. 3 Satz 1 Grundgesetz (GG) gewährleistet. Die Norm beruht auf der

Schlüsselfunktion, die einer freien Wissenschaft für die Selbstverwirklichung des einzelnen wie auch für die gesamtgesellschaftliche Entwicklung zukommt. Begrenzungen der Wissenschaftsfreiheit durch Gesetz sind ausgeschlossen, doch kann die Wissenschaftsfreiheit nicht grenzenlos sein. Auch ein Forscher darf sich bei seiner wissenschaftlichen Tätigkeit nicht über die verfassungsrechtlich verbürgten Rechte seiner Mitbürger hinwegsetzen. Weil die Wissenschaftsfreiheit aber nicht durch Gesetze eingeschränkt werden kann, können etwaige Einschränkungen nur aus der Verfassung selbst hergeleitet werden. Auch das allgemeine Persönlichkeitsrecht, aus dem das Recht auf informationelle Selbstbestimmung und damit auch der Datenschutzgedanke abgeleitet worden ist, durch Art. 2 Abs. 1 i.V. mit Art. 1 Abs. 1 GG garantiert. Art. 1 Abs. 1 GG sichert die Würde des Menschen, die auch in der freien Entfaltung seiner Persönlichkeit besteht. Art. 2 Abs. 1 GG schließt Wertschutzlücken in Bereichen, welche die im Grundgesetz einzeln aufgeführten Freiheitsrechte inhaltlich nicht erfassen. Das Grundgesetz gewährt also dem einzelnen Bürger einen unantastbaren Bereich privater Lebensgestaltung. Eingriffe in das Persönlichkeitsrecht und hier speziell das Recht auf informationelle Selbstbestimmung sind nur aufgrund normenklarer, den Verhältnismäßigkeitsgrundsatz beachtender gesetzlicher Regelungen zulässig.

Auch die Wissenschaftsfreiheit ist der in Art. 1 Abs. 1 GG garantierten Würde des Menschen zugeordnet, die als oberster Wert das ganze grundrechtliche Wertsystem beherrscht. Diese Verpflichtung endet auch nicht mit dem Tode, was etwa für die Archivverwaltung bedeutsam ist. Zwar ist es zunächst Aufgabe des Gesetzgebers, einen Ausgleich zwischen diesen teilweise im Konflikt zueinander stehenden Grundrechtspositionen des Persönlichkeitsschutzes und der Wissenschaftsfreiheit zu finden. Solange derartige Entscheidungen des Gesetzgebers fehlen, kann die mit Rücksicht auf kollidierende Verfassungswerte notwendige Grenzziehung nur im Einzelfall durch eine entsprechende Güterabwägung vorgenommen werden. Dies ist von den Stellen zu beachten, die den Forschern Daten zur Verfügung stellen, aber auch von den Forschern selbst.

Als Ergebnis läßt sich daher feststellen, daß auch die zeitgeschichtliche Forschung die **Rechte und Interessen der Bürger** zu wahren hat. Dies kann durch **Anonymisierung**, durch **Auswahl** des Forschungspersonals oder durch Erholung der **Einwilligung** der durch die Datenverarbeitung Betroffenen erreicht werden. Nur ausnahmsweise kann eine Datenübermittlung ohne Einwilligung, dann allerdings auf gesetzlicher Grundlage akzeptiert werden, wobei aber auch die Bedeutung des Forschungsvorhabens in bezug zum beabsichtigten Eingriff in das informationelle Selbstbestimmungsrecht gesetzt werden muß. Keinesfalls kann hingenommen werden, daß zeitgeschichtliche Forschung schrankenlos auf personenbezogene Daten jeder Art und zu jeder Zeit zugreifen darf.

18.3 Einzelfragen

18.3.1 Aufarbeitung alter gemeindlicher Beschlußbücher

Eine Gemeinde hat angefragt, ob ein Privatmann die gemeindlichen Beschlußbücher von der alten deutschen in die lateinische Schrift übertragen darf. Außerdem solle er maßgebliche Beschlüsse für das Gemeindearchiv aufbereiten. Der Bürger bediene sich dabei eines Computers mit Dateiverwaltungsprogramm. Hierdurch sei er in der Lage, Daten von Personen in bezug auf ihr Amt und ihre Tätigkeit auszuwerten und historisch wertvolle Begebenheiten von ehemaligen Gemeindebürgern für das Archiv festzuhalten oder in einer Gemeindechronik zu veröffentlichen.

Hinsichtlich der **Veröffentlichung** personenbezogener Daten aus gemeindlichen Beschlußbüchern in einer Ortschronik bin ich mit dem Staatsministerium des Innern der Auffassung, daß Vorkommnisse, die mehr als 100 Jahre zurückliegen, auch Verschuldungen, Prozesse und sonstige persönliche Angaben, regelmäßig veröffentlicht werden dürfen, da die Betroffenen inzwischen verstorben sind und eine Beeinträchtigung der Rechte von Nachkommen nicht mehr zu erwarten ist. Das Bundesverfassungericht hat zwar im sog. „Mephisto-Urteil" festgestellt, daß das Persönlichkeitsrecht auch über den Tod einer Person hinaus weitergilt. Es hat allerdings betont, daß der Schutzbereich dieses Rechts mit zunehmender zeitlicher Entfernung des Todes abnimmt. Diese Erwägungen gelten auch für Geburts- und Heiratsdaten verstorbener Personen sowie deren Todesdaten.

Bezüglich der **Aufarbeitung** der Unterlagen für das Gemeindearchiv einschließlich der EDV-mäßigen Erschließung habe ich in Abstimmung mit dem Staatsministerium des Innern angeregt, die Regelungen des Bayerischen Archivgesetzes entsprechend heranzuziehen. Es hat zum Inhalt, daß schutzwürdige Belange Betroffener oder Dritter und überwiegende Interessen des Gemeinwohls auch nach der Archivierung angemessen zu berücksichtigen sind. Schließlich müssen die Archive die ordnungs- und sachgemäße dauernde Aufbewahrung und Benützbarkeit des Archivguts und seinen Schutz vor unbefugter Benützung oder Vernichtung durch geeignete technische, personelle und organisatorische Maßnahmen sicherstellen. Konkret bedeutet das im vorliegenden Fall, daß die hier tätige Person die erforderliche Zuverlässigkeit und Gewissenhaftigkeit besitzen muß. Außerdem muß Vorsorge getroffen werden, daß kein Unbefugter Zugang zum Computer hat, z.B. durch Abschließen der Datenträger und der Geräte sowie Aufstellen der Geräte in nicht allgemein zugänglichen und abschließbaren Räumen. Die Verknüpfung verschiedener personenbezogener Daten miteinander durch das Archiv ist nur zulässig, wenn schutzwürdige Belange Betroffener oder Dritter nicht beeinträchtigt werden.

18.3.2 Forschungsprojekt „Strukturelle und inhaltliche Bedingungen der Frühförderung" in Bayern

Bereits in meinem letzten Tätigkeitsbericht bin ich Stimmen entgegengetreten, die davon sprachen, daß sozialwissenschaftliche und medizinische Untersuchungen aufgrund der strengen Datenschutzbestimmungen nicht mehr durchzuführen seien.

Daß Datenschutz und Forschung miteinander vereinbar sind, zeigt folgendes Beispiel: Der Leiter eines sozialwissenschaftlichen Institutes einer Universität ist mit der Bitte an mich herangetreten, einen im Rahmen eines Forschungsprojektes entwickelten Fragebogen datenschutzrechtlich zu überprüfen.

Der umfangreiche Fragebogen enthält eine Vielzahl zum Teil sehr persönlicher Fragen, die an in der Frühförderung

Beschäftigte gerichtet sind und Aussagen über ihr persönliches Befinden, die Streßbelastung sowie die Ursachen hierfür zulassen. Ziel der Fragebogenaktion, die anonym erfolgen und statistisch ausgewertet werden soll, ist eine Verbesserung der Ausbildung und Weiterbildung des vorgenannten Personenkreises beispielsweise durch Entwicklung von Streßtrainingsprogrammen.

Da der Projektleiter sowohl die große Anzahl als auch den Inhalt der Fragen als unverzichtbar für die Aussagequalität der Untersuchung erklärte, wurden gemeinsam mit meiner Geschäftsstelle Bedingungen ausgearbeitet, wie die **Anonymität** der Befragung und die **Einhaltung des Datenschutzes** bei der Auswertung am besten gewährleistet sind.

Folgende Hauptforderungen habe ich gestellt:

- Aufnahme eines deutlichen Hinweises auf die Freiwilligkeit der Teilnahme sowie der Beantwortung der Fragen im Begleitschreiben zu der Umfrage

  Da eine Rechtsvorschrift für die Datenerhebung nicht existiert, kommt dem Hinweis auf die Freiwilligkeit besondere Bedeutung zu.

- Beschäftigung eines möglichst kleinen Personenkreises mit der Auswertung der Fragebögen

  Insbesondere darf keine Person mit Zusatzwissen, z.B. der Arbeitgeber der einzelnen Bediensteten, Einblick in die Fragebögen erhalten. Hierdurch soll eine Reidentifizierung unmöglich werden.

- Verwendung eines Freikuverts zum Rückversand, so daß ein Rückschluß auf den Wohnort aufgrund des Poststempels verhindert wird;

- sorgfältige Auswahl des mit der Auswertung befaßten Personals und Verpflichtung auf das Datengeheimnis;

- Vernichtung der Fragebögen zum frühestmöglichen Zeitpunkt;

- Zugriffssicherung durch Verwendung von Benutzerkennung und Paßwörtern;

- Auswertung der Fragen nach Altersgruppen und Zeiträumen sowie Verwendung von Größenordnungen (von — bis), anstelle genauer Jahres- oder Einwohnerzahlen;

- Verzicht auf Veröffentlichung von Aussagen zu Kleingruppen (bis zu 40 Personen) oder Einzelpersonen;

- Vorbehalt einer Kontrolle durch meine Geschäftsstelle während der gesamten Dauer des Forschungsprojekts.

Durch die rechtzeitige Beteiligung des Datenschutzbeauftragten konnte eine Regelung getroffen werden, die sowohl den Anliegen des Datenschutzes als auch den wissenschaftlichen Anforderungen gerecht wird.

Eine frühzeitige Einschaltung meiner Geschäftsstelle ist auch deshalb wünschenswert, um von Anfang an bloße Unachtsamkeiten oder datenschutzrechtlich bedenkliche Verfahrensweisen zu vermeiden, die sonst zu einem späteren Zeitpunkt in Form von Anfragen oder Beschwerden und oftmals unter breiter Beteiligung der Öffentlichkeit wieder an mich herangetragen werden.

19. Umweltfragen

19.1 Einführung

Der Schutz der natürlichen Lebensgrundlage ist der besonderen Fürsorge der staatlichen Gemeinschaft anvertraut. Es gehört zu den vorrangigen Aufgaben des Staates, Boden, Wasser und Luft als natürliche Lebensgrundlagen zu schützen und eingetretene Schäden möglichst zu beheben oder auszugleichen.

Zur Erfüllung dieser Verfassungsaufgaben (Art. 141 Bayer. Verfassung) benötigt der Staat umfassende Informationen über den Zustand und die Veränderungen der Umwelt. Der automatisierten Datenverarbeitung kommt dabei große Bedeutung zu. Nur mit ihrer Hilfe ist es möglich, eine Vielzahl von Umweltdaten zu speichern, auszuwerten und mit anderen Daten zusammenzuführen, um aktuelle Informationsgrundlagen für die Umweltpolitik zu erhalten.

Das Staatsministerium für Landesentwicklung und Umweltfragen arbeitet derzeit am Aufbau eines umfassenden Umweltinformationssystems, das bereits bestehende Datenbanken, Meßnetze und Fachinformationssysteme koordinieren soll. Die Zugriffe zu den Daten sollen diejenigen Stellen erhalten, die sie zur Erfüllung ihrer Aufgaben benötigen.

Daneben bestehen im Geschäftsbereich des Ministeriums, insbesondere beim Landesamt für Umweltschutz, eine Vielzahl an automatisierten Dateien, wie beispielsweise Deponiedatendatei, Sickerwasserdatei, Artenschutzkartierung, Bioindikatoren und Daten der Wasserforschung.

Soweit bei den zu verarbeitenden Daten ein Personenbezug herstellbar ist, werden datenschutzrechtliche Gesichtspunkte und Aspekte des technisch-organisatorischen Datenschutzes zu berücksichtigen sein.

Mit folgenden Datenbanken war meine Geschäftsstelle im Berichtsjahr befaßt:

19.2 Umweltdatenbanken

19.2.1 Bodeninformationssystem (BIS)

Auf das in Bayern einzurichtende Bodeninformationssystem bin ich in meinem letzten Tätigkeitsbericht ausführlich eingegangen. Zwischenzeitlich wurde von einer von der Umweltministerkonferenz eingerichteten Sonderarbeitsgruppe ein „Vorschlag für die Einrichtung eines länderübergreifenden Bodeninformationssystems" ausgearbeitet, den die Länder beim Aufbau von Bodeninformationssystemen zugrundelegen sollen. Die Ausarbeitung baut auf dem Konzept des BIS auf. Ziel ist es, Ergebnisse von Auswertungen und Risikovorhersagen in den verschiedenen Bundesländern vergleichbar zu machen. Ausgehend von einem Rahmenkonzept werden den Ländern konkrete Arbeitsschritte vorgeschlagen, die notwendigen Anforderungen an Methoden und Modelle definiert und der Forschungsbedarf dargelegt.

Da sich das Bodeninformationssystem aus zentralen Systemen und selbständigen dezentralen Fachinformationssystemen zusammensetzen soll, stehen derzeit Fragen der Kompatibilität, nämlich der technischen Zusammenführbarkeit verschiedener Fachdatenbanken, im Mittelpunkt der Planungen.

Im Anschluß daran sollen die konkreten Inhalte der einzelnen Dateien sowie Fragen der Zugriffsberechtigung erörtert werden. Durch Teilnahme an den Sitzungen der Arbeitsgruppe werde ich Gelegenheit haben, Aspekte des rechtlichen sowie des technisch-organisatorischen Datenschutzes einfließen zu lassen.

19.2.2 Altlasten-Datenbank

Von früheren Abfallablagerungen und von stillgelegten oder noch betriebenen Anlagen wie Fabriken oder Lagerstätten können erhebliche Gefahren für die Allgemeinheit ausgehen, wenn dort mit umweltgefährdenden Stoffen gearbeitet wurde oder wird. Ziel einer demnächst vom Staatsministerium für Landesentwicklung und Umweltfragen herausgegebenen Broschüre „Leitfaden für die Altlastenermittlung" ist es, in Zusammenarbeit mit den zuständigen Behörden sowie den verantwortlichen jetzigen oder ehemaligen Betreibern altlastverdächtige Flächen festzustellen sowie deren Gefährdungspotential, insbesondere im Hinblick auf eine mögliche Grundwasserbeeinträchtigung, abzuschätzen. Daran anschließen soll sich die Sanierung der Altlasten in der Reihenfolge ihrer Dringlichkeit.

Die „Altlasten-Datenbank", die beim Landesamt für Umweltschutz eingerichtet ist, soll die Auswertung und den Überblick über die einzelnen Altlastenflächen erleichtern.

Zunächst wird die sog. Altlastenerhebung mittels zweier verschiedener Fragebögen durchgeführt, je nach dem, ob es sich um eine gefahrenverdächtige Ablagerung oder um stillgelegte oder aufgelassene gefahrenverdächtige Standorte von Gewerbe- und Industriebetrieben handelt. Beide Fragebögen enthalten Fragen zu über 60 Einzelangaben. Als personenbezogene Daten werden Name und Anschrift des jetzigen und auch des früheren Betreibers gespeichert.

Die bestehenden Gesetze und Verordnungen zum Abfall-, Wasser- und Immissionsschutzrecht sehen umfangreiche Auskunfts- und Mitwirkungspflichten für die Betreiber einer Anlage vor. Sie stellen zum jetzigen Zeitpunkt — vorbehaltlich einer späteren bereichsspezifischen Regelung — eine ausreichende Rechtsgrundlage für die Verarbeitung auch der personenbezogenen Daten dar. Zur Kooperation zwischen Behörden und Betreibern bei der Durchführung der Altlastensanierung sowie zur Durchsetzung des Verursacherprinzips bei der Sanierung sind die erhobenen Daten erforderlich.

19.2.3 Gefahrstoffdatenbank

Auf Bitten des Staatsministeriums für Arbeit und Sozialordnung habe ich zur Speicherung personenbezogener Daten in einer Gefahrstoffdatenbank in seinem Geschäftsbereich Stellung genommen. Der Anfrage lag folgender Sachverhalt zugrunde:

Die Gewerbeaufsichtsämter der Länder vollziehen zum Schutz der Arbeitnehmer die auf das Chemikaliengesetz gestützte Gefahrstoffverordnung. Zur Überwachung gefährlicher Stoffe und zur Abwendung hiervon ausgehender Gefahren sind bestimmte Produktdaten mit Angaben über Hersteller und Verwender notwendig. Die obersten Arbeitsschutzbehörden der Länder beabsichtigen deshalb, Gefahrstoffdatenbanken einzurichten, bei denen die Gewerbeaufsichtsämter für ihre Prüftätigkeit Daten abfragen können. Die Daten sollen zwischen den Ländergefahrstoffdatenbanken ausgetauscht werden.

Ich habe die Auffassung vertreten, daß nach den Vorschriften des Bayerischen Datenschutzgesetzes und des Chemikaliengesetzes eine **Erhebung und Speicherung der bei den Gewerbeaufsichtsämtern** anfallenden Gefahrstoffdaten sowie deren Übermittlung an andere Gewerbeaufsichtsämter, soweit es für deren Kontrollzwecke erforderlich ist, zulässig ist. Da die Gewerbeaufsichtsämter für den Vollzug des Chemikaliengesetzes zuständig sind, dürfen sie die von ihnen erhobenen Daten selbst speichern. Im Fall einer Verarbeitung der Daten durch eine andere (öffentliche) Stelle blieben die Gewerbeaufsichtsämter als Auftraggeber für die Einhaltung der Vorschriften des BayDSG verantwortlich.

Soweit Art und Zusammensetzung eines Stoffes ein Betriebs- oder Geschäftsgeheimnis darstellen können, an dessen Geheimhaltung der Betriebsinhaber ein wirtschaftliches Interesse hat, habe ich jedoch Vorsorgemaßnahmen zur Sicherstellung einer vertraulichen Behandlung für erforderlich gehalten.

19.2.4 Integriertes Meß- und Informationssystem zur Überwachung der Umweltradioaktivität (IMIS)

Das im Dezember 1986 in Kraft getretene Strahlenschutzvorsorgegesetz (StrVG) sieht die jährliche Berichterstattung durch den Bundesminister für Umwelt, Naturschutz und Reaktorsicherheit an den Bundestag und den Bundesrat über die Entwicklung der Radioaktivität in der Umwelt vor.

Mit Hilfe eines bundesweiten integrierten Meß- und Informationssystems zur Überwachung der Umweltradioaktivität, das derzeit von Bund und Ländern gemeinsam erarbeitet wird, sollen aktuelle Daten und Meßzahlen schneller abrufbar und verfügbar sein.

Folgendes Konzept liegt den geplanten Datenübermittlungen zugrunde:

Die Meßstellen der einzelnen Bundesländer (in Bayern u.a. die Landesuntersuchungsämter) ermitteln mit einem Erfassungsbogen Radioaktivitätswerte in Lebensmitteln, Futtermitteln, Trinkwasser, Grundwasser, Abwässern, Düngemitteln usw. In die Erfassungsbögen werden personenbezogene Daten wie Hersteller, Lieferant, Betrieb, Standort nicht eingetragen. Da freilich die Probenahmestellen anhand eines Koordinatensystems im Raster von ca. 1 Kilometer erfaßt werden, kann in Einzelfällen ein Personenbezug hergestellt werden, wenn es sich um einen Privateigentümer großer Grundstücke handelt. Bei der Mehrheit der von den Bodennahmen betroffenen Eigentümer handelt es sich jedoch um juristische Personen des öffentlichen Rechts oder Privatrechts, auf die die Datenschutzgesetze keine Anwendung finden.

Daneben erfordert die Vergleichbarkeit der Entwicklung der radioaktiven Kontamination in Einzelfällen auch die Benennung der verarbeitenden Betriebe (z.B. Molkereien) in den Meßprogrammen.

Die gemessenen Radioaktivitätswerte werden über die zuständige Landesdatenzentrale an die Zentralstelle des Bundes (ZdB) weitergegeben.

Die hierbei anfallende Datenverarbeitung ist datenschutzrechtlich zulässig. Nach § 3 Abs. 1 StrVG sind die Länder verpflichtet, die Radioaktivität in den dort aufgezählten Medien an die Zentralstelle zu übermitteln. § 12 StrVG

berechtigt die zuständigen Behörden, Grundstücke und Betriebs- sowie Geschäftsräume während der Betriebs- und Arbeitszeit zu betreten, die Radioaktivität zu ermitteln und Proben zu nehmen. In Erfüllung der Aufgabe, zum Schutz der Bevölkerung vor ionisierender Strahlung die Umweltradioaktivität zu überwachen, ist es erforderlich, im begrenzten Umfang auch — aufgrund von Koordinaten bestimmbare — personenbezogene Daten zu speichern und zur Plausibilitätskontrolle an die Landesdatenzentrale sowie an die Zentralstelle zu übermitteln.

Entgegen den Befürchtungen mehrerer Datenschutzbeauftragter der Länder ist ein „Online-Zugriff" durch die Zentralstelle auf die Datensammlungen der Länder nicht vorgesehen. Die Zentralstelle kann nur nicht rechtzeitig übermittelte Daten anmahnen.

Wie das Staatsministerium für Landesentwicklung und Umweltfragen mitgeteilt hat, veröffentlicht es Meßdaten grundsätzlich nur unter Nennung des Landkreises als Ortsbezug. Somit ist ein Rückschluß auf natürliche Personen ausgeschlossen.

Gegen das geplante Verfahren IMIS bestehen keine datenschutzrechtlichen Bedenken.

19.2.5 Einzelfragen

Als Hilfsmittel zur Beschleunigung von Verwaltungsverfahren und damit für eine bürgerfreundlichere Verwaltung werden im Umweltbereich zunehmend automatisierte Verfahren eingesetzt:

- Eine bei einer Regierung eingerichtete Datei „PLADIS" dient zur Durchführung von Planfeststellungsverfahren. Sie speichert unter anderem die Namen der Einwendungsführer, ihrer Vertreter, die Art der Einwendung, den Einwirkungsort sowie den Namen des Sachbearbeiters und erleichtert so einen ersten Überblick über die oft große Zahl von Verfahrensgegnern bei abfallrechtlichen, wasserrechtlichen und sonstigen Planfeststellungsverfahren. Rechtsgrundlage für die Speicherung sind Art. 73, 74 Bayerisches Verwaltungsverfahrensgesetz in Verbindung mit den jeweiligen Spezialnormen.

  Gegen die Datenspeicherung bestehen keine Bedenken. Da der Inhalt der Einwendungen den Datensatz sprengen würde, muß für die Sachbearbeitung ohnehin der jeweilige Akt herangezogen werden. Die Datei ist nach Erledigung des Planfeststellungsverfahrens zu löschen.

- Zur Steigerung des Umweltbewußtseins seiner Bürger veranstaltete ein Landkreis ein **Umweltpreisausschreiben** mit Fragen zum Umweltverhalten, die anschließend automatisiert ausgewertet werden sollten. Vorher wurde das Adressenfeld vom Fragebogen abgetrennt und nach der Ermittlung der Gewinner ordnungsgemäß vernichtet. Eine Weiterverwendung der Adressen zur Anforderung von zusätzlichem Informationsmaterial, wie sie ein zum gleichen Zeitpunkt von einer Verbrauchergemeinschaft bundesweit veranstaltetes Preisrätsel vorsah, war hier von Anfang an nicht beabsichtigt.

19.3 Abfall- und Wertstoffkataster beim Landratsamt Ebersberg

Wachsende Mengen an Müll stellen die Landkreise, die nach dem Abfallgesetz zur Beseitigung der in ihrem Gebiet angefallenen Abfälle verpflichtet sind, vor zunehmende Probleme. Gleichzeitig ist nach den Vorschriften des Abfallgesetzes vor der Beseitigung zu prüfen, ob und inwieweit Abfälle wiederverwertet werden können. Da insbesondere der ständig steigende Gewerbemüll ein erhebliches Recyclingpotential darstellt, hat der Landkreis Ebersberg ein automatisiertes Abfall- und Wertstoffkataster eingerichtet. Hierzu wurde ein rechnergestütztes Abfallwirtschaftskonzept erarbeitet, das derzeit als Pilotprojekt durchgeführt wird. Inzwischen waren Mitarbeiter meiner Geschäftsstelle vor Ort beratend tätig.

Zur Datenerhebung wurden Fragebögen an im Landkreis ansässige Gewerbebetriebe versandt. Damit sollte der Istzustand hinsichtlich Abfallarten, -mengen, -vorkommensorte, Transportwege und bisheriger Wiederverwertungs- und Entsorgungsarten ermittelt werden. Derzeit werden die Daten nach Abfallbranchen getrennt erfaßt. Für einen Teilbereich wurde bereits eine vorläufige Auswertung vorgenommen. Eine spätere überregionale Koordinierung ist ins Auge gefaßt.

Die der Datenerfassung zugrunde liegenden Fragebögen enthalten folgende personenbezogenen Angaben: Firmenname oder Familienname, Adresse, Branche/Betriebsart, Ansprechpartner, Telefon, Zahl der Beschäftigten im Betrieb.

Da für die Datenerhebung keine spezielle Rechtsnorm besteht, wurde die Erhebung auf freiwilliger Basis durchgeführt. Die Begleitschreiben zu der Umfrage enthielten Hinweise auf die Freiwilligkeit. Die vorgenannten Daten ermöglichen eine rasche Zuordnung des Abfallaufkommens. Die „Zahl der Beschäftigten im Betrieb" dient als Hilfsmerkmal für die mengenmäßige Abschätzung.

Der Einhaltung des Datenschutzes wird von seiten des Landkreises auch deshalb große Bedeutung beigemessen, weil aus Abfallstoffen unter Umständen auf die hergestellten Produkte rückgeschlossen werden kann. Diese fallen häufig unter das Betriebs- oder Geschäftsgeheimnis. Im Interesse der Schaffung eines Vertrauensverhältnisses sollen die Daten auch innerhalb des Landratsamtes nicht in personenbezogener Form weitergegeben werden. Inwieweit überhaupt Datenübermittlungen stattfinden sollen, wird derzeit erörtert.

20. Straßenverkehr

20.1 Zentrales Informationssystem (ZEVIS)

Das novellierte Straßenverkehrsgesetz (vgl. näher Seite 53 des 9.Tätigkeitsberichts) hat die Rechtsgrundlage für die Einrichtung eines zentralen Fahrzeugregisters geschaffen. Da neben den Kraftfahrzeugzulassungsstellen noch weitere Behörden, z.B. die Polizei, zur Nutzung des Systems befugt sind, hat das Straßenverkehrsgesetz die Protokollierung von Anfragen aus dem Zentralen Fahrzeugregister angeordnet, um die Kontrolle der Rechtmäßigkeit der Anfragen zu ermöglichen. So wird durchschnittlich bei jeder 50. Anfrage einer Polizeidienststelle an den Datenbestand des Zentralen Fahrzeugregisters beim Kraftfahrtbundesamt (KBA) in Flensburg der Anfragende automatisch aufgefordert, über die sonst üblichen Anfragedaten hinaus zusätzliche Angaben zu machen, und zwar Angaben zur Identität des Anfragenden und zum Grund der Anfrage. Erst bei Erfüllung dieser Vorgaben wird die erfragte Auskunft erteilt. Diese

Protokolldaten zeichnet in Bayern das Landeskriminalamt auf.

Als Ergebnis einer ersten ZEVIS-Prüfung im letzten Jahr hatte ich festgestellt, daß die Qualität der von den Polizeidienststellen angelieferten Protokolldaten noch verbesserungsbedürftig ist. Trotz der daraufhin vom Staatsministerium des Innern angeordneten weiteren organisatorischen Maßnahmen hat auch meine diesjährige Prüfung erhebliche **Mängel bei den protokollierten Daten** ergeben. So war wieder ein hoher Anteil an Negativprotokollierungen festzustellen, das sind Protokollierungen von abgebrochenen Anfragen: der Anfragende hat auf Anforderung seine Identität und den Anfragegrund nicht innerhalb einer vorgegebenen Zeit eingegeben. Durch die angeordneten zusätzlichen manuellen Aufzeichnungen über Abbrüche bei den Dienststellen konnten in diesem Jahr allerdings die Ursachen der Fehler festgestellt werden. Im wesentlichen waren dies **Schwierigkeiten mit dem Eingabeverfahren**. Auch der vom System vorgegebene Abbruch des Dialogs mit dem Rechner nach einem bestimmten Zeitablauf (der anfragende Polizeibeamte konnte innerhalb der zur Verfügung stehenden Zeit die vom System gestellten Anforderungen nicht erfüllen) wurde als Fehlerursache erkannt. Ferner ergaben sich auch technische Fehler, die es dem Polizeibeamten unmöglich machten, eine ordnungsgemäße „Auswahlprotokollierung" durchzuführen. Damit sind es wohl hauptsächlich Unsicherheiten der Anwender und technische Unwägbarkeiten, die zu Fehlern und unvollständigen Protokollierungen geführt haben.

Das Staatsministerium des Innern hat hieraus Konsequenzen gezogen und angeordnet, daß künftig **jede** ZEVIS-Anfrage eines Polizeibeamten beim Bayerischen Landeskriminalamt protokolliert wird und der anfragende Beamte von **vornherein** die Gründe für seine Abfrage in das System einzugeben hat. Dies ist ein sehr begrüßenswerter Schritt. Damit kann stärker noch als bisher die Rechtmäßigkeit des polizeilichen Abfrageverhaltens in ZEVIS geprüft werden.

Meine Überprüfung der ZEVIS-Auswahlprotokolldatensätze eines ganzen Kalendermonats im Jahr 1989 hat im übrigen gezeigt, daß in den ganz überwiegenden Fällen Anfragen wegen der „Überwachung des Straßenverkehrs" und der „Verfolgung von Straftaten oder Ordnungswidrigkeiten" gestellt worden sind. Die gesetzlich ebenfalls zugelassenen Anfragen in Fällen „von sonstigen Anlässen" betreffen nur etwa 5% aller Anfragen. Dies ist aus datenschutzrechtlicher Sicht deshalb bedeutsam, weil sich unter diesem sehr allgemeinen Abfragegrund eher ungerechtfertigte Anfragen verbergen könnten. Deshalb ist in diesen Fällen auch eine zusätzliche Erläuterung des Anfragegrundes vorgesehen. Grundsätzlich erachte ich einen Anteil von 5% der Abfragen wegen „sonstiger Anlässe" noch akzeptabel.

20.2 Zulassung/Umschreibung von Kraftfahrzeugen

Ende 1988 führte das Staatsministerium für Wirtschaft und Verkehr bei den Kfz-Zulassungsstellen einen **neuen Vordrucksatz** für die Zulassung und Umschreibung von Kraftfahrzeugen ein. Veranlaßt war die Neueinführung durch die 1987 neu geschaffenen Vorschriften über die Erfassung, Speicherung und Weitergabe von Halter- und Fahrzeugdaten im Straßenverkehrsgesetz. Bei der Ausarbeitung des neuen Vordrucksatzes war ich beteiligt.

Ich habe darauf hingewirkt, daß vom Antragsteller nur noch die notwendigen Daten erhoben und gespeichert werden (z.B. Namen, Anschriften, „Kfz-schadstoffarm"). Bei einigen Daten besteht keine gesetzliche Verpflichtung zur Angabe. Sie sind mit einem „Stern" gekennzeichnet und mit dem Hinweis versehen, daß die Angaben freiwillig sind (z.B. Vorbesitzerdaten, Nummern des bisherigen Fahrzeugbriefs, Telefonnummer des Antragstellers). Neu ist auch, daß die Kfz-Zulassungsstellen mit Einführung des neuen Vordrucksatzes keine Daten mehr an Dritte für Zwecke der Werbung oder Meinungsforschung herausgeben dürfen.

20.3 Unterrichtung über Fahrverbot

Der Datenschutzbeauftragte eines anderen Bundeslandes hat die Frage aufgeworfen, ob bei Verhängung eines Fahrverbotes gemäß § 25 StVG die für die Verfolgung von Verkehrsordnungswidrigkeiten zuständige Behörde (Bußgeldstelle)

- die Führerscheinstelle und
- die Wohnortpolizei von der Verhängung des Fahrverbotes unterrichten dürfe.

Mit dem Staatsministerium des Innern bin ich der Auffassung, daß die **Verständigung** der für den Wohnort des Betroffenen zuständigen **Polizeidienststelle** zulässig ist. Diese hat in Bayern die Aufgabe, die Führerscheine amtlich zu verwahren, deren Inhaber mit dem Fahrverbot belegt sind. Zur Erfüllung dieser Aufgaben ist die Verständigung der Polizeidienststelle über das verhängte Fahrverbot erforderlich.

Die Verständigung der Führerscheinstelle jedoch ist auch nach Auffassung des Staatsministeriums des Innern nicht erforderlich. Die Führerscheinstelle wird somit in Bayern vom Fahrverbot nicht informiert.

20.4 Telefonische Auskünfte an kommunale Verkehrsüberwachung

Ein Landratsamt fragte an, ob es zulässig sei, an die kommunale Verkehrsüberwachung einer Stadt telefonische Auskünfte zu geben. Der Verkehrsüberwachungsdienst hat die Aufgabe, Ordnungswidrigkeiten im ruhenden Verkehr (z.B. Parkverstöße) zu verfolgen.

Mit dem Staatsministerium des Innern halte ich die telefonische Datenübermittlung aus dem Datenbestand der Zulassungsstelle des Landratsamtes an den Verkehrsüberwachungsdienst im Hinblick auf § 35 Abs. 1 Nr. 3 StVG rechtlich für zulässig. Um zu verhindern, daß Fahrzeug- und Halterdaten Unberechtigten, die sich als Bedienstete eines kommunalen Verkehrsüberwachungsdienstes ausgeben, mitgeteilt werden, habe ich die Verwendung eines Kennwortes empfohlen, das in kürzeren Zeitabständen zu erneuern ist.

21. Medien

21.1 Presse und Datenschutz

In den letzten beiden Tätigkeitsberichten habe ich auf Lücken im Persönlichkeitsschutz gegenüber Rundfunk und Presse hingewiesen. Der nunmehr vorliegende Gesetzentwurf zur Fortentwicklung der Datenverarbeitung und des Datenschutzes (EBDSG) ist ein wichtiger Schritt zu

verbessertem Medienschutz in einem Teilbereich, nämlich dem Rundfunk des Bundes. Da der Entwurf aber nach wie vor den übrigen Rundfunk, den öffentlichen wie privaten, und die gesamte Presse ausnimmt, bleibt er hinter den verfassungsrechtlichen Notwendigkeiten zurück, die Persönlichkeit der Bürger vor Beeinträchtigungen durch unrichtige Datenverarbeitung (Speicherung und Nutzung) vorbeugend zu schützen.

Anläßlich eines Fachgesprächs in Bonn zur Novellierung des Bundesdatenschutzgesetzes habe ich konkrete Vorschläge für eine Regelung der Datenverarbeitung bei den Medien zur Einführung eines Datenschutzbeauftragten für die Presse vorgelegt (vgl. Anlage 2). Hierbei habe ich gefordert:

- Den Betroffenen sollte nicht nur gegenüber Rundfunkanstalten des Bundesrechts und nicht erst, wenn eine Beeinträchtigung des Persönlichkeitsrechts bereits vorliegt (so § 37 Abs. 3 EBDSG) ein **Auskunftsanspruch** über die zu ihrer Person in Dateien der Presse oder des Rundfunks gespeicherten Daten eingeräumt werden. Allerdings darf dadurch die Pressefreiheit nicht in ihrem Kernbereich berührt werden, wozu insbesondere der gesamte Bereich publizistischer Vorbereitungstätigkeit, also die Beschaffung von Informationen und das Redaktionsgeheimnis zählen. Deshalb habe ich eine Erweiterung des bereits im Gesetzentwurf enthaltenen Auskunftsverweigerungsrechts auf diejenigen Fälle vorgeschlagen, in denen die Erfüllung der publizistischen Aufgabe das Interesse des Betroffenen an der Auskunftserteilung überwiegt.

- Da sich der Schutz der Pressefreiheit auf die **wahrheitsgemäße** Berichterstattung beschränkt, hat die Presse keinen Anspruch darauf, nachweisbar unrichtige Daten zu speichern. Unrichtige Daten sind zu berichtigen. Können richtige Daten nicht ermittelt werden, so muß der Betroffene die Löschung der gespeicherten Daten verlangen können.

- Wegen der für den Bürger bestehenden Undurchsichtigkeit der Speicherung und Verwendung von Daten in Pressedatenbanken und auch im Interesse eines vorgezogenen Rechtsschutzes ist die Tätigkeit eines **unabhängigen Kontrollorgans** von entscheidender Bedeutung für einen effektiven Schutz des Rechts auf informationelle Selbstbestimmung gegenüber der Presse. Ein solches unabhängiges Kontrollorgan könnte auch in den Fällen, in denen die Wahrung des Redaktionsgeheimnisses, der Quellenschutz oder gerade laufende Presseermittlungen eine unmittelbare Auskunft an den Bürger verbieten, anstelle des Bürgers und für diesen die Rechtmäßigkeit und Richtigkeit der durch die Presse vorgenommenen Verarbeitung personenbezogener Daten der Bürger und die Berechtigung einer Auskunftsverweigerung überprüfen. Zur Sicherung der notwendigen Staatsfreiheit könnte dieses Kontrollorgan vom Presserat vorgeschlagen und vom Bundespräsidenten ernannt werden. Zumindest wäre ein verlagsinterner Datenschutzbeauftragter mit garantierter Kontrollunabhängigkeit unverzichtbar.

21.2 Bayerische Landeszentrale für Neue Medien

Die Fortsetzung der im letzten Tätigkeitsbericht beschriebenen Prüfung (S. 50) habe ich zunächst zurückgestellt. Die Bayerische Landeszentrale für Neue Medien (BLM) teilte mir zwischenzeitlich mit, daß sie ihre EDV inhaltlich völlig umgestalten werde. Sie hat nunmehr ein EDV-Grobkonzept vorgelegt, zu dem ich bei einem ausführlichen Gespräch Hinweise, insbesondere zu Datensicherungsmaßnahmen gegeben habe. Ich werde den EDV-Neuaufbau weiterhin beratend begleiten.

21.3 Prüfung einer Kabelgesellschaft

Eine erste datenschutzrechtliche Prüfung einer bayerischen Kabelgesellschaft ergab folgende Feststellungen:

Die Kabelgesellschaft nutzt für ihre Datenverarbeitung einen städtischen PC. Auf dem PC, bei dem bisher keine Sicherungsmaßnahmen vorgesehen sind, finden sich nebeneinander Dateien der Stadt sowie Dateien und Textkonserven der Kabelgesellschaft. Ich habe gefordert:

- Die Datenverarbeitung ist zu trennen; Mitarbeiter der Stadt dürfen nur Zugriff auf städtische, Mitarbeiter der Kabelgesellschaft nur Zugriff auf ihre Dateien haben.

- Ein datenschutzrechtlicher Mindeststandard ist einzuhalten:

  Soweit dies vom System her möglich ist, ist ein Start- und Tastaturkennwort vorzusehen. Zumindest ist der PC bei Dienstschluß mechanisch abzusperren.

  Eine Benutzerkennung und persönliche Paßworte sind einzuführen. Außerdem ist sicherzustellen, daß die Benutzung der Dateien geprüft werden kann.

  Die Datenbestände sind regelmäßig zu sichern. Die Sicherungsdatenträger sind zugriffssicher zu lagern.

In einem eigenen Geschäftsraum verarbeitet die Kabelgesellschaft von der Deutschen Bundespost übermittelte Aufträge für Kabelanschlüsse.

- Diese Datenübermittlung ist unbedenklich, soweit Neuteilnehmer gemeldet werden, die neben einem fernmelderechtlichen Vertrag mit der Post zugleich mit dieser im Namen der Kabelgesellschaft rundfunkrechtliche Teilnehmerverträge abschließen (Art. 23 Abs. 3 Satz 3 MEG). Die Datenübermittlung dient insoweit der Sicherstellung des Gebührenaufkommens.

- Die Deutsche Bundespost übermittelt Namen und Anschrift von Hauseigentümern auch dann an die Kabelgesellschaft, wenn nur Übergabepunkte zu diesen Häusern gelegt werden, die jeweiligen Bewohner diese jedoch nicht nutzen. Die Kabelgesellschaft möchte mit den Daten dieser Personen künftig Akquisition betreiben. Eine generelle Übermittlung der Namen und Anschriften der Bewohner von Häusern, zu denen nur Übergabepunkte gelegt sind, die jedoch die Kabelanschlüsse nicht nutzen, ist zur Aufgabenerfüllung der Kabelgesellschaften nicht erforderlich. Die vollständige Speicherung dieser Daten ist somit unzulässig.

- Abmeldungen von Kabelteilnehmern werden bisher nur in Ordnern der jeweiligen Anmeldung beigeheftet. Eine Vernichtung ist nicht vorgesehen. Dies kann nur noch für eine kurze Übergangszeit bis zur bevorstehenden Änderung der Gebührenabrechnung hingenommen werden.

In ihrem Geschäftsraum bewahrt die Kabelgesellschaft Geschäftsunterlagen und Ordner mit Teilnehmerdaten in offenen Regalen auf. Dies genügt nicht den datenschutzrechtlichen Mindestanforderungen (Art. 15 BayDSG). Ich habe die Kabelgesellschaft aufgefordert, die Geschäftsunterlagen und Ordner in verschließbaren Schränken aufzubewahren.

21.4 Private Satellitenempfangsanlagen in Bayern

Im letzten Tätigkeitsbericht hatte ich mitgeteilt, daß die Bayerische Landeszentrale für Neue Medien nach Art. 35 Medienerprobungs- und -entwicklungsgesetz (MEG) Genehmigungsbehörde von solchen Satellitenempfangsanlagen ist, die Rundfunkprogramme an mindestens 100 angeschlossene Wohneinheiten weiterverbreiten. Insoweit muß die Landeszentrale von der Deutschen Bundespost die Daten der Anlagebetreiber erhalten.

Vertretbar erscheint die Rechtsauffassung, daß die BLM bei einer Weiterverbreitung an weniger als 100, d.h. an 2 — 99 Wohneinheiten, zwar keine Genehmigung, aber eine Unbedenklichkeitsbescheinigung erteilen kann. Bei einer Individual-Satelliten-Empfangsanlage jedenfalls findet eine **Weiter**verbreitung unzweifelhaft nicht statt. Die Speicherung der Betreiber dieser Anlagen habe ich deshalb bei der BLM als nicht erforderlich beanstandet.

Die BLM hat zwischenzeitlich mitgeteilt, daß die entsprechenden 1327 Datensätze gelöscht sind. Die Deutsche Bundespost übermittelt die Daten der Nutzer von Satellitenempfangsantennen, an die niemand weiterer angeschlossen ist, nicht mehr an die BLM.

21.5 ISDN

Der Bundespostminister hat im März dieses Jahres das „dienste-integrierende digitale" Fernmeldenetz ISDN in Betrieb genommen und damit begonnen, die Fernmeldedienste in einem einheitlichen Netz anzubieten. Diese Entwicklung führt sowohl bei den Netzbetreibern als auch bei den Diensteanbietern zur Verarbeitung von erheblich mehr personenbezogenen Daten, als dies bei den bisherigen Fernmeldenetzen der Fall war.

Aus Datenschutzgründen und auch zur Akzeptanz der neuen Telekommunikationstechnologien sollten bei offenen Netzen folgende Datenschutzmaßnahmen angestrebt werden:

- Für einige Telekommunikationsdienste (Telefon, Datenübermittlungsdienste) sollten Zahleinrichtungen geschaffen werden, bei denen die Anonymität des Nutzers gewahrt bleibt, insbesondere keine Nutzerdaten anfallen.
- Jedermann sollte das Recht erhalten, in unentgeltlichen Teilnehmerverzeichnissen nicht zu erscheinen.
- Jedes ISDN-Telefongespräch wird registriert: Zeitpunkt und Dauer der Verbindung sowie die Rufnummern von Anrufendem und Angerufenem werden ca. vier Monate aufbewahrt. Diese wie auch sonstige **Abrechnungsdaten** für Telekommunikationsdienste dürfen nur für Abrechnungszwecke verwendet und nur solange gespeichert werden, wie dies zur Abrechnung erforderlich ist.
- Daten, die für die Vermittlung von Telekommunikationsdiensten erforderlich sind, sind nach Beendigung einer Verbindung unverzüglich zu löschen.

Datenschutzforderungen sind darüber hinaus auch bei speziellen Merkmalen einzelner Dienste zu stellen:

- ISDN-Anschlüsse sind im Telefonbuch besonders zu kennzeichnen: Weil an einen ISDN-Anschluß nicht nur ein Telefon, sondern weitere, beispielsweise aufzeichnende Endgeräte angeschlossen sein können, kann sich der Anrufer über diese Kennzeichnung darauf einstellen.
- Die **Anzeige** des anrufenden Teilnehmers am Display (Sichtfenster des Telefonapparates) sollte sowohl vom Anrufer als auch vom Angerufenen fallweise unterdrückt werden können. Bei Telefonanschlüssen, über die besonders sensible Gespräche geführt werden, z.B. die Telefonseelsorge, oder bei AIDS-Beratungsstellen, muß generell auf die Rufnummernanzeige verzichtet werden. Bei der Umleitung oder der Weiterschaltung von Telefongesprächen muß die Rufnummernanzeige verzögert erscheinen, damit der Anrufer noch rechtzeitig abbrechen kann.

Zu diesen Fragen habe ich mich in ähnlicher Weise auch auf verschiedenen öffentlichen Veranstaltungen geäußert.

Die Datenschutzbeauftragten haben auf der 11. Internationalen Konferenz im August 1989 in Berlin einen umfangreichen Forderungskatalog verabschiedet und weiterhin erklärt, daß sie die diesen Fragenbereich betreffende Arbeit des Sachverständigenausschusses des Europarates zu Datenschutzfragen unterstützen wollen.

Obwohl ISDN erst vor einigen Monaten in Betrieb genommen wurde, hat sich in der Praxis bereits ein Problem ergeben: Wenn derzeit in der öffentlichen Verwaltung abzurechnende private Telefongespräche von Bediensteten geführt werden, darf nur ein verkürzter Teil der Zielnummer ausgedruckt werden. Eine Identifizierung des Angerufenen durch andere Behördenangehörige ist somit nicht möglich.

Im ISDN wurde nun die schon bisher in einem begrenzten Rahmen vorgesehene Möglichkeit, einen Nachweis über die einzelnen von einem Apparat/einer Vermittlung geführten Gespräche der Fernsprechrechnung **(Einzelgebührennachweis)** zu beantragen, ab 1.7.1989 erweitert. Ein solcher Nachweis enthält u. a. Datum, Uhrzeit, Zielnummer und Gebühreneinheiten. Damit ist erkennbar, wann von einem Anschluß oder einer Vermittlung Verbindungen zu anderen Anschlüssen hergestellt worden sind. So besteht die Gefahr, daß über den Einzelgebührennachweis, der alle von einer Behörde geführten Gespräche einschließlich der vollständigen Zielnummer wiedergibt, der mit der Verkürzung der Zielnummern erreichte Schutz für das Persönlichkeitsrecht verloren geht.

Das Staatsministerium der Finanzen hat auf meine Anfrage mitgeteilt, daß im staatlichen Bereich bisher kaum Vermittlungen an ISDN-fähige digitale Vermittlungsstellen angeschlossen sind. Die Möglichkeit, gebührenpflichtige Einzelgebührennachweise zu beantragen, sei derzeit noch ohne praktische Bedeutung. Trotz zunehmender Technisierung werde man in den oben angeführten Bereichen auf den Einzelgebührennachweis verzichten müssen. Die für Bayern geltenden Dienstanschlußvorschriften würden Anträge auf Einzelgebührennachweise nicht vorsehen. Auch bei deren Überarbeitung sei dies nicht zu erwarten.

21.6 Änderungen des Gesetzes zu Art. 10 GG und der Strafprozeßordnung im Rahmen der Poststrukturreform

Der Deutsche Bundestag hat das Fernmeldewesen teilweise privatisiert. In den letzten Beratungen vor der Verabschiedung des Gesetzes zur Poststrukturreform wurde eine Änderung des Gesetzes zu Art. 10 GG (Gesetz zur Beschränkung des Brief-, Post- und Fernmeldegeheimnisses) beschlossen. Danach dürfen die Verfassungsschutzbehörden des Bundes und der Länder, der Militärische Abschirmdienst und der Bundesnachrichtendienst künftig den gesamten Fernmeldeverkehr nach Genehmigung des G-10-Ausschusses überwachen und aufzeichnen. Auch die Überwachungsvorschriften der Strafprozeßordnung (§§ 100 a, 100 b) wurden entsprechend geändert.

Während in der Vergangenheit neben dem Briefverkehr nur Telefongespräche und Fernschreiben kontrolliert und ausgewertet werden durften, ist dies nunmehr auch für alle neuen Fernmeldedienste (z. B. Bildschirmtext, Temex, Telefax, Mailbox, Datel-Dienste, ISDN) zulässig. Dies kann bedeuten, daß nun auch Abrechnungs-, Verbindungs- und Nutzungsdaten, die bei den Fernmeldediensten anfallen, sowie im Rahmen elektronischer Dienste gespeicherte Inhaltsdaten (z. B. bei Mailboxen, Btx usw.) kontrolliert werden dürfen.

Die Datenschutzbeauftragten des Bundes und der Länder sowie die Datenschutz-Kommission Rheinland-Pfalz hatten auf ihrer Konferenz vom 5./6.4.1989 in einer Entschließung (Anlage 2) darauf hingewiesen, daß eine solche Erweiterung der Eingriffe in Grundrechte einer gründlichen Überprüfung durch alle Beteiligten bedürfte. Sie hatten vorgeschlagen, im Rahmen der vom Bundestag als dringlich angesehenen Poststrukturreform das Gesetz zu Art. 10 GG und die Strafprozeßordnung nur insoweit zu ändern, als dies in einem unmittelbaren Zusammenhang zu den geplanten ordnungspolitischen Änderungen der Telekommunikation steht.

Bundestag und Bundesrat haben die Erweiterung der Überwachungsbefugnisse gleichwohl beschlossen.

22. Bayerische Versicherungskammer

Prüfung bei der Bayerischen Rechtsanwaltsversorgung

Die Bayerische Rechtsanwaltsversorgung ist eine rechtsfähige Pflichtversorgungsanstalt des öffentlichen Rechts. Sie wird mit den ebenfalls rechtlich selbständigen Versorgungsanstalten für Apotheker und Architekten im gleichen Geschäftsbereich der Bayerischen Versicherungskammer verwaltet. Einzelne Aufgaben (z.B. Personaleinsatz, EDV-Unterstützung) werden für alle Anstalten von den Zentralbereichen der Kammer wahrgenommen.

Die Prüfung der Rechtsanwaltsversorgung führte zu folgenden Ergebnissen:

Lesezugriff auf gespeicherte Mitgliederdaten

Die drei Verwaltungsbereiche der Rechtsanwaltsversorgung (Beitrag, Leistungen, Buchhaltung) hatten jeder für sich einen unbeschränkten Lesezugriff auf die gesamten gespeicherten Daten der Rechtsanwaltsversorgung sowie der Versorgungsanstalten für Apotheker und Architekten. Die gleiche unbeschränkte Zugriffsmöglichkeit wurde auch beim gemeinsamen Schreibdienst und bei der gemeinsamen Poststelle der drei genannten Versorgungsanstalten festgestellt.

Diesen Umfang des Datenzugriffs habe ich zur Aufgabenerfüllung für nicht erforderlich gehalten und eine Beschränkung des Zugriffs auf den jeweiligen Zuständigkeitsbereich gefordert.

Die Bayerische Versicherungskammer teilte mir inzwischen die Aufhebung des Lesezugriffs der in der Rechtsanwaltsversorgung Beschäftigten auf Daten der beiden anderen Anstalten mit. Der Zugriff auf Daten der jeweils anderen Versorgungsanstalten wurde auf wenige für die richtige Zuordnung von Vorgängen nötige Angaben beschränkt. Zum Umfang der Zugriffsberechtigung der Verwaltungsbereiche innerhalb der Rechtsanwaltsversorgung hat die Kammer mitgeteilt, daß der Datenzugriff der Buchhaltung auf Daten des Beitragssachgebiets neu festgelegt und auf das erforderliche Maß beschränkt wird. Post- und Schreibdienst sollen im wesentlichen nur noch auf Adressen zugreifen können. Ferner wurden die Richtlinien für den Zentralbereich Elektronische Datenverarbeitung neu gefaßt. Nun ist stets ein schriftlicher Auftrag des verantwortlichen Sachbereichs für die Entwicklung und Änderung automatisierter Verfahren erforderlich.

Anstaltsübergreifende Sachbearbeitung

Die Mitarbeiter in den Verwaltungsbereichen Buchhaltung und Leistungen bearbeiten die Angelegenheiten der Mitglieder aller drei Versorgungsanstalten. Daten von Mitgliedern einer Anstalt stehen mithin theoretisch auch bei der Sachbearbeitung für die anderen Anstalten zur Verfügung, für die sie nicht bestimmt sind. Für eine solche Nutzung besteht in der Regel kein Anlaß. Ich habe deshalb angeregt, die Sachbearbeitung der drei Anstalten möglichst zu trennen.

Hierzu teilte die Versicherungskammer mit, die Sachbearbeitung in den Verwaltungsbereichen Leistung und Buchhaltung werde künftig organisatorisch verselbständigt und jeweils bestimmten Mitarbeitern zugeordnet werden, die ausschließlich für eine Anstalt zuständig sind. Derzeit würde jedoch die anfallende Arbeitsmenge eine sinnvolle Trennung der Anstalten noch nicht zulassen.

Einkommensteuerbescheide

Zur Festsetzung der Beiträge der Versicherten erhebt die Rechtsanwaltsversorgung Angaben zum Einkommen. Als Nachweis haben die Betroffenen Einkommensteuerbescheide vorzulegen.

Die Steuerbescheide können jedoch Angaben enthalten, die für das Versicherungsverhältnis in der Rechtsanwaltsversorgung unerheblich sind. Dies trifft etwa bei Zusammenveranlagung von Ehegatten hinsichtlich der Angaben zum Einkommen des anderen Ehegatten zu. Die Anstalt erhält in diesen Fällen Kenntnis über Daten, die sie zu ihrer Aufgabenerfüllung nicht benötigt.

Die Versicherungskammer sagte zu, daß künftig bei der Anforderung von Steuerbescheiden oder entsprechenden Unterlagen die notwendigen Daten ausdrücklich benannt werden. Gleichzeitig werde den Betroffenen mitgeteilt, daß alle übrigen Daten unkenntlich gemacht werden könnten. Damit ist meiner Forderung Rechnung getragen.

Lesezugriff des Zentralbereichs Mathematik

Der Zentralbereich Mathematik der Versicherungskammer, der für alle Bereiche der Kammer Leistungen erbringt, hat die Möglichkeit des unbeschränkten Lesezugriffs auf alle von der Rechtsanwaltsversorgung gespeicherten Mitgliederdaten. Auch auf die vollständigen Akten kann zur Auswertung zurückgegriffen werden. Die Prüfung ergab, daß ein so umfassender Datenzugriff nicht erforderlich ist.

Die Versicherungskammer teilte dazu mit, daß sie die für den mathematischen Bereich erforderlichen Daten neu festlegen und den Lesezugriff entsprechend einschränken werde.

Kenntnisnahme von ärztlichen Gutachten

Ärztliche Gutachten werden bei der Rechtsanwaltsversorgung nur eingeholt, wenn über das Vorliegen von Berufsunfähigkeit oder über deren Beginn oder Dauer zu entscheiden ist. Das ärztliche Zeugnis ist bisher jeweils Bestandteil der Akte.

Zum besseren Schutz der sensiblen medizinischen Daten vor Kenntnisnahme durch Unbefugte habe ich angeregt, die ärztlichen Zeugnisse vom sonstigen Inhalt der Akten zu trennen.

Die Versicherungskammer hat der Anregung entsprochen.

23. Technischer und organisatorischer Bereich

23.1 Grundsatzfragen

23.1.1 Datensicherheit beim Einsatz von Arbeitsplatzcomputern

In der öffentlichen Verwaltung gewinnen Arbeitsplatzcomputer (APC) zusehends an Gewicht. Obwohl ich in früheren Tätigkeitsberichten bereits über dieses Thema berichtet habe, gebe ich wegen der großen Bedeutung dieser Rechner für die Abwicklung von Verwaltungsaufgaben an dieser Stelle eine Zusammenfassung über Datensicherheitsmaßnahmen beim Einsatz von APC.

Moderne Arbeitsplatzcomputer haben inzwischen die Leistungsfähigkeit der Rechner erreicht, die noch vor 15 Jahren als sogenannte Großrechner in den meisten Rechenzentren der öffentlichen Verwaltung standen.

Beeindruckt von dieser Technologie mit ihren vielfältigen Einsatzmöglichkeiten der DV-Systeme vergessen die Benutzer nur allzu häufig die damit verbundene Eigenverantwortlichkeit für die ordnungsgemäße Durchführung aller Sicherungsaufgaben. Unsachgemäßer und allzu sorgloser Umgang können eine große Gefahr für die Datensicherheit bedeuten. Durch Fehlbedienung, mangelndes Sicherheitsbewußtsein oder auch falsche Sparsamkeit können Daten, Programme und sonstige wichtige Informationen zerstört werden, die — wenn überhaupt — nur mit unverhältnismäßig hohem Aufwande wiederherstellbar sind. Häufig übersteigen dabei die Wiederherstellungskosten um ein Vielfaches die Mittel, die für die Sicherheit aufzuwenden gewesen wären. Deshalb sind frühzeitig geeignete Maßnahmen zu ergreifen, welche die Sicherheit der Datenverarbeitung APC gewährleisten.

APC-Betriebssysteme und Sicherheitssoftware

In der Vergangenheit verfügten APC unter dem Betriebssystem DOS (DISK OPERATING SYSTEM) über keine Zugangsschutzeinrichtungen. Außerdem bestand keine Möglichkeit, Ablaufinformationen aufzuzeichnen. Dies hat sich inzwischen insoweit geändert, als Zugangsschutzeinrichtungen wie Start- und Tastaturkennwort vorhanden sind und Zusatzprodukte angeboten werden, die diese Mängel beseitigen.

Damit werden erstmals ausreichende Sicherheitsvorkehrungen für den APC-Einsatz geschaffen, die auch eine revisionsfähige Protokollierung aller abgelaufenen Aktivitäten in einem Logbuch gestatten. Ferner greifen neben den bislang organisatorischen Maßnahmen wie Arbeits- und Benutzeranweisungen sowie Verpflichtung auf das Datengeheimnis nunmehr auch hard- und softwaretechnische Sicherheitseinrichtungen, die eine Absicherung gegen unbefugte Dritte weitgehend ermöglichen. Schließlich gibt es auch für den APC-Einsatz Werkzeuge, welche die Einhaltung einer verbindlichen Verarbeitungslogik sicherstellen, und somit eine weisungswidrige Datenverarbeitung erschweren.

Voraussetzungen für den APC-Einsatz

Ein geplantes Vorgehen erfordert eine umfassende Analyse, Bewertung und Dokumentation aller Aspekte der Datensicherheit und des Datenschutzes beim APC-Einsatz. Dabei sind insbesondere zu beachten:

- Allgemeine softwaretechnische Sicherheitsmaßnahmen
- Maßnahmen zur Ausfallsicherheit
- Sicherheitsüberlegungen bei unterschiedlichen Einsatzformen
  - Stand alone-Gerät (Single/Multi User-Betrieb)
  - APC-Netz (lokales Netz)
  - APC mit Terminaleigenschaften
  - Anschluß an einen Zentralrechner (Groß-EDV)
  - Anschluß an ein beliebiges System (z.B. Btx).

Zu den wesentlichsten Punkten, die vor dem APC-Einsatz individuell geregelt sein müssen, zählen:

- Einrichtung eines Benutzerservice, der den Endbenutzer berät und unterstützt.
- Hard- und Software müssen miteinander abgestimmt sein
- Schaffung einer einheitlichen Bedienoberfläche und Integration der Anwendung
- Festlegung der Datensicherungsmaßnahmen
- Klärung der Datensicherung
- Definition und Beschreibung aller Maßnahmen, die zur Gewährleistung der Datensicherheit und des Datenschutzes erforderlich sind.

Benutzerservice

Anwender, die einen reibungslosen Einsatz und eine koordinierte und datenschutzgerechte Nutzung von APC anstreben, richten einen Benutzerservice ein. Die Größe dieser Stabstelle hängt von der Anzahl der zu betreuenden Benutzer ab. Aufgabe dieses Benutzerservice ist die Förderung, Unterstützung und zentrale Steuerung der Individuellen Datenverarbeitung (IDV). Hard- und Software werden zentral und koordiniert beschafft. So kann Wildwuchs vermieden werden. Eine zentral getestete und freigegebene Hard- und Software unterstützt die Vorgabe allgemein gültiger Richtlinien und Arbeitsanweisungen.

Aufgaben und Pflichten des Benutzerservices sind genau festzulegen sowie zusammen mit den Schnittstellen und Kommunikationsbeziehungen aller beteiligten Abteilungen in der Verwaltung zu beschreiben. Als zentrales „Information Center" führt der Benutzerservice die erforderlichen Informationen wie das Hard- und Softwarekataster, trägt die Verantwortung für die Sicherheit und den Datenschutz sowie für die Organisation der Benutzer- und Zugriffsrechte. Letztgenannte Funktion wird in großen Institutionen an dezentrale Administrationseinrichtungen delegiert. Schließlich plant und organisiert der Benutzerservice den Einsatz von APC-Netzen und den Host-Anschluß.

Verfahrensentwicklung, -pflege und -dokumentation

Weiterhin hat der Benutzerservice sicherzustellen, daß die Verfahrensentwicklung mit Test und Freigabe zentral überwacht, koordiniert und kontrolliert wird.

Auch die Programmpflege und -wartung sowie die Erstellung der aktuellen Dokumentation aller Verfahren sollte durch den Benutzerservice erledigt werden.

Wichtig ist ferner, bereits bei der Verfahrensentwicklung eine Zuordnung von Programmen und Daten zu bestimmten Schutzklassen entsprechend dem Sicherheitsbedürfnis sowie der Sensitivität vorzunehmen und die daraus abzuleitenden Sicherheitsmaßnahmen zu ergreifen.

Benutzeranweisung APC

Um den ordnungsgemäßen Einsatz von APC zu gewährleisten, sollte der Benutzerservice allen Anwendern eine Benutzeranweisung zur Verfügung stellen und die Anwendungen laufend betreuen. Neben den Bedienungsanleitungen für den laufenden Betrieb benötigt der Anwender Applikationshandbücher mit detaillierten Handlungsanweisungen.

Verwendung von privater Hard- und Software

Eine Verwendung privater Hard- und Software für dienstliche Belange ist grundsätzlich zu verbieten und nur in begründeten Einzelfällen (z.B. bei Lehrern, siehe 16.1) zu gestatten, sofern hierdurch der Datenschutz nicht gefährdet wird.

Verpflichtungserklärung des APC-Benutzers

Jeder APC-Benutzer hat eine Verpflichtungserklärung zu unterschreiben, in der die beim APC-Einsatz zu beachtenden Gebote und Verbote enthalten sind. Dies sind insbesondere:

Gebote:
- Ausschließlicher Einsatz freigegebener Hard- und Software
- Einhaltung der vorgegebenen Datensicherheitsmaßnahmen
- Meldung der personenbezogenen Dateien zum behördeninternen Datenregister
- Verantwortung für die Datensicherung

Im einzelnen handelt es sich dabei um folgende Maßnahmen:
- Jeder APC-Anwender ist für die Sicherung seiner Dateien selbst verantwortlich.
- Personenbezogene Daten müssen bei Festplattenbetrieb auf externe Sicherungsmedien (Disketten/Streamer) gesichert werden.
- Die Sicherungsbestände müssen zugriffssicher aufbewahrt werden.
- Mindestens einmal im Jahr ist eine Datenträgerinventur vorzunehmen, deren Ergebnis revisionsfähig zu dokumentieren ist.

- Verpflichtung zu besonderen Datensicherheitsmaßnahmen Wenn im Multi User-Betrieb Programm- und Datenbereiche der einzelnen Benutzer gegeneinander abzuschotten sind, müssen benutzerbezogene Programm- und Dateibereiche eingerichtet werden.

Verbote:
- Einsatz nicht lizenzierter Software (private Programme, Raubkopien etc.)
- Verfälschung von Programmen und Daten
- Weitergabe von Programmen und Daten an Dritte ohne Erlaubnis
- Verwendung von Programmen und Daten zu anderen Zwecken als zur rechtmäßigen Aufgabenerfüllung

Durch die Verpflichtung des APC-Benutzers zur Beachtung obenstehender Gebote und Verbote wird die grundsätzliche Verantwortung der Dienstvorgesetzten für den APC-Einsatz nicht geschmälert.

Aufgaben des behördeninternen Datenschutzbeauftragten bei APC-Einsatz

Zu den Aufgaben des internen Datenschutzbeauftragten (vgl. Nr. 26.1 VollzBek BayDSG) zählt im Rahmen der Eigenkontrolle auch die Überprüfung des APC-Einsatzes. Dabei gilt es festzustellen, ob nur die zugelassenen Programme verarbeitet werden, eine Anforderung, die — wird sie nur manuell/visuell durchgeführt — bei umfangreichem APC-Einsatz nicht in der gebotenen Weise zu erfüllen ist.

Folgende Vorgehensweise bietet sich an:
In einem ersten Schritt sollte die Behörde die zugelassene und freigegebene Sollkonfiguration des APC festschreiben und dokumentieren. Dazu werden mit Hilfe eines Programmes über alle Programme und Directories nach einem bestimmten Verfahren sog. Checksummen gebildet. Diese Checksummen werden als Prüfergebnis auf einem externen Speichermedium, etwa der Diskette, aufgezeichnet und beim Datenschutzbeauftragten verwahrt. Bei einer späteren Überprüfung kann anhand der vorhergehenden Checksummenbildung festgestellt werden, ob Veränderungen stattgefunden haben. Ist dies der Fall, wird das betreffende Objekt unter Angabe von Datum und Uhrzeit der Veränderung angezeigt. Der interne Datenschutzbeauftragte kann dann im Einzelfall prüfen, ob es sich hier um eine legale Änderung handelt oder ein Mißbrauch zu vermuten und somit weitere Recherchen veranlaßt sind. Das bei der erneuten Überprüfung erhaltene Ergebnis dient wiederum als Basis für die nächste Prüfung. Die Revisionsfähigkeit wird durch eine umfassende Protokollierung des Prüfungsvorganges unterstützt.

Installationsanforderungen

Die Basis für einen nach Maßgabe des Datenschutzes und der Datensicherheit geforderten ordnungsgemäßen Einsatz von APC wird bereits im Vorfeld einer Installation, beginnend

bei der Raumauswahl und aller damit zusammenhängenden Sicherheitsfragen, gelegt. Neben der Auswahl des geeigneten Aufstellungsortes sind weitere Aspekte wie Intrusionsschutz, Zutrittsicherung, Vernetzung einzubeziehen. Grundlage hierzu bildet eine Sicherheitsanalyse, die meist anhand von herstellerbezogenen Checklisten durchgeführt wird.

Betrieb der Arbeitsplatzrechner

Die Inbetriebnahme eines APC ist in der Regel sehr einfach, da die meisten Systeme bereits nach dem Einschalten der Stromzufuhr automatisch hochfahren, das Betriebssystem sowie die zum Betrieb erforderliche systemnahe Software laden und den Aufruf der Anwendung erwarten. Teilweise werden die Systeme sogar so vorkonfiguriert, daß das Anwenderverfahren ohne einen zusätzlichen Aufruf bereitgestellt wird. Das mag zwar für den berechtigten Nutzer eine durchaus arbeitserleichternde Vorgehensweise sein, eröffnet jedoch dann Risiken, wenn ein Unbefugter Zugang zum APC erlangt.

Deshalb müssen Zugangssicherungsmaßnahmen ergriffen und Benutzerrechte definiert werden!

Systemverwaltung

Analog zur Groß-EDV ist auch beim APC-Einsatz ein verantwortlicher Benutzer zu bestimmen, der die Aufgaben des Systemverwalters wahrnimmt. Zur Systemverwaltung zählen insbesondere:
- Einrichten von Benutzern und Zuteilen von Rechten
- Zuordnung der benötigten Betriebsmittel
- Definition und Dokumentation aller Maßnahmen zur Gewährleistung der Datensicherheit und des Datenschutzes sowie der Sanktionen bei Verletzung von Sicherheitsmaßnahmen
- Festlegung von Art und Umfang der Protokollierung zum Nachweis der ordnungsgemäß durchgeführten Datenverarbeitung, wobei nachvollziebar sein muß:
  WER HAT
  WANN
  MIT WELCHEN MITTELN
  WAS VERANLASST
  UND WORAUF ZUGEGRIFFEN?
- Auswertung der Ablaufdaten
- Organisation und Durchführung der Datensicherung und Archivierung.

Die Verwaltung der Benutzerrechte ist revisionsfähig auszugestalten und muß eine Antwort auf die Frage
WER HAT(TE)
ZU WELCHER ZEIT
WELCHE BENUTZER- UND ZUGRIFFSRECHTE
ermöglichen.

Zugriffssicherung

Bei einem Multi User-Betrieb (mehrere Benutzer teilen sich einen APC) oder bei vernetztem Einsatz besteht die unverzichtbare Notwendigkeit, Daten und Betriebsmittel gegenseitig vor unberechtigtem Zugriff zu schützen.

Wesentliche Grundfunktionen des Zugriffsschutzes, insbesondere bei der Verarbeitung sensitiver Daten, sind dabei:
- Benutzeranmeldung nur über
  - Benutzeridentifikation
  - Paßwort
  - Chipkarte
- Sperren des APC nach „n" Fehlversuchen (n = 3)
- Sperren des APC außerhalb der Arbeitszeit
- Lückenlose Menüsteuerung
- Sperren der Betriebssystemebene
- Sperren von Laufwerken
- Verstecken von Dateien, Schutz vor Überschreiben und Ändern, Verschlüsseln und Sperren von Dateien (Programmen) und von gesamten Verzeichnissen
- Führen einer Protokolldatei (Revision)
- Sperren und Dunkelschaltung des Bildschirms in Arbeitspausen
- Sperren der Tastatur (Tastaturverriegelung)
- Überschreiben von gelöschten Dateien.

Auf den Zwang zur Paßwortnutzung und die Regeln für eine sichere Paßwortverwendung weise ich erneut hin.

Betriebszustand „Wartung"

Neben allgemeinen Sicherheitsmaßnahmen bei der Wartung von APC ist besondere Vorsicht geboten, wenn ein Rechner zur Reparatur außer Haus gegeben werden muß und die auf der Festplatte gespeicherten Daten nicht mehr gelöscht werden können. Das gleiche gilt bei Fehlern der Festplatte, die eine Reparatur beim Hersteller oder der Wartungsfirma erforderlich macht. Es muß sichergestellt sein, daß mit den gespeicherten Daten kein Mißbrauch betrieben wird. Bei einer Wartung von Festplattenspeichern außer Haus sind demzufolge vorsorglich zumindest vertragliche Zusatzvereinbarungen zu treffen, die einen Mißbrauch ausschließen sollen.

Entsorgung von Datenträgern

Berichte, daß Datenträger, die nicht ordnungsgemäß entsorgt wurden, Unbefugten in die Hände fielen und von diesen dann mißbräuchlich verwendet wurden, sind immer wieder in der Tagespresse zu lesen. Sachgerecht zu entsorgen sind Disketten, Streamer Tapes, Festplatten und natürlich auch Papierausdrucke. Derartige Datenträger dürfen nicht in den Papierkorb geworfen werden. Auch wenn Dritte mit der Durchführung der Entsorgung von Datenträgern mit sensitiven Daten beauftragt werden, bleiben die APC-Benutzer für die Sicherheit des gewählten Verfahrens letztlich verantwortlich. Demzufolge ist auf ein lückenloses Entsorgungskonzept zu achten, nach dessen Durchführung ein Entsorgungsgut vorliegen muß, das den Empfehlungen der deutschen Sicherheitsnorm über das Vernichten von Informationsträgern (DIN 32757, Teil I und Teil II) entspricht. Es gibt eine Reihe geeigneter Geräte und Lösungen, die dieser Norm entsprechen.

Als erste Entsorgungsmaßnahme ist in jedem Fall zu empfehlen, maschinenlesbare Datenträger, die vernichtet werden sollen, unverzüglich mit einem starken Magneten oder einem speziellen Entmagnetisierungsgerät zu behandeln.

Datensicherung und Datenträgerverwaltung

Die Datensicherung ist für die meisten APC-Benutzer eine lästige und zudem zeitaufwendige Tätigkeit, die häufig nur unregelmäßig und teilweise unzureichend ausgeführt wird. Um den Zeitbedarf für die Durchführung der Datensicherung

möglichst gering zu halten, ist eine strenge Organisation vorzugeben. Damit die Durchführung einer ordnungsgemäßen und revisionsfähigen Datensicherung nicht vergessen wird, empfiehlt es sich, Mechanismen einzubauen, die zur Erinnerung dienen. Einige integrierte Sicherheitsprodukte für den APC-Einsatz bieten die Möglichkeit, daß der Anwender beim Abmelden durch den automatischen Aufruf eines Programms zur Datensicherung gezwungen wird.

Zur ordnungsgemäßen Datensicherung gehört auch die sachgemäße Aufbewahrung der Datenträger. Zumindest sollte ein Doppel aller Programme und Dateien (Gesamtsicherung) an einem Ort ausgelagert werden, der räumlich vom APC-Platz getrennt ist. Die Aufbewahrung soll diebstahl-, feuer-, wasser- und staubsicher sein. Am besten ist es deshalb, Datenträger in geeigneten Data Safes zugriffssicher aufzubewahren.

APC im Netz

Zur Gewährleistung des ordnungsgemäßen Einsatzes von APC im Netz gilt es zu klären:
- Wie wird gewährleistet, daß bei vernetzten APC über ein lokales Netzwerk (LAN) die Zugriffs- und Verarbeitungssicherheit eingehalten wird?
- Erkennt das Netzwerkbetriebssystem den Versuch, einen nicht zugelassenen Arbeitsplatzrechner anzuschließen?
- Wird das Netzwerk ausreichend dokumentiert (Konfiguration und User Management)?
- Existieren revisionsfähige Ablaufdaten?
- Ist eine Verschlüsselung der Daten im Netz erforderlich? Beim Einsatz von Verschlüsselungstechniken ist hier besonders darauf zu achten, daß die Ver- und Entschlüsselung im Arbeitsspeicher geschieht, so daß immer nur verschlüsselte Daten über das Netz laufen.
- Welche Maßnahmen sind zur Erhöhung der Netzwerksicherheit, etwa nach Ausfall eines Endgerätes, angebracht?

Anschluß an einen Host

Bei einem Anschluß an ein Hostsystem (zentraler Rechner) gilt als oberster Grundsatz, daß die Zugriffssicherung des zentralen Rechners durch den APC nicht außer Kraft gesetzt oder gemindert werden darf.

Die Zugriffsberechtigung ist unter folgenden Gesichtspunkten zu bestimmen:
- Die Zugriffsberechtigung ist verfahrensbezogen festzulegen.
- Unberechtigte Anmelde- und Zugriffsversuche sind revisionsfähig zu protokollieren und Sanktionen (z.B. Sperren des Terminals oder der Benutzerkennung) müssen weitere Mißbrauchsversuche ausschließen.
- Es ist festzulegen, welcher Benutzer auf welche Daten zugreifen darf.
- Benutzerrechte sind revisionsfähig zuzuteilen und zu verwalten. Für den Fall, daß das Betriebssystem dazu keine geeignete Unterstützung bietet, sind zumindest manuelle Aufzeichnungen zu führen.

Für die Funktionen eines File Transfer Systems ist die Zugangsberechtigung beim File Transfer entscheidend. Von der Zugangsberechtigung werden die Benutzerrechte abgeleitet, die wiederum festlegen, ob und wenn ja wie der Zugriff auf bestimmte Ressourcen, d.h. Betriebsmittel einschließlich der Datenbestände, gestattet ist.

Ein File Transfer sollte nur unter folgenden Voraussetzungen gestattet werden:
- Bei der Zulassung eines File Transfer ist darauf zu achten, daß zwei voneinander unabhängige Zugangsberechtigungen (lokales System und fernes System) eingerichtet werden.
- Für den File Transfer sind bestimmte Zugangsrechte zu vergeben, die wiederum festlegen, ob und wie der Zugriff auf bestimmte Ressourcen, etwa Datenbestände, erlaubt ist.
- Bei der Festlegung der Benutzerrechte sind die Art des Partnersystems und die Anwendungsumgebung zu berücksichtigen.
- Übertragungsrechte sind — so weit erforderlich — auf Senden oder Empfangen auszurichten.
- Der Zugriff ist auf bestimmte Dateien einzugrenzen. **Grundsatz:** Der APC soll nur die zentral gespeicherten Daten erhalten, die der Benutzer zur Aufgabenerfüllung benötigt.
- Von der Notwendigkeit, die Folgeverarbeitungsmöglichkeiten einzuschränken (Sperren bestimmter Kommandos), muß bei Bedarf Gebrauch gemacht werden.
- Die mit File Transfer auf den APC übertragenen Daten sind gegen unberechtigtes Kopieren besonders zu schützen.
- Gehen Daten vom APC in den zentralen Rechner, so sind diese Daten dort genauestens zu überprüfen, damit Zerstörung, Sabotage und ähnliches weitgehend ausgeschlossen sind.
- Eine direkte Änderung von Daten im zentralen Rechner ist nicht zuzulassen.
- Es ist zu verhindern, daß eine unbefugte Steuerung des zentralen Rechners über eine Netzwerkverbindung ausgeführt wird.
- Der netzwerkfähige APC ist vor unbefugter Inbetriebnahme durch ein APC-Schloß zu sichern. Die Schlüsselverwaltung ist entsprechend revisionsfähig zu organisieren.

Notfall- und Katastrophenvorsorge

Die Abhängigkeit von der stets funktionsfähigen Datenverarbeitung wird mit zunehmender Dezentralisierung auch in der Individuellen Datenverarbeitung immer größer. Deshalb sind geeignete Vorsorgemaßnahmen zu treffen, um in Not- und Katastrophenfällen die Verfügbarkeit der Rechnerleistung und vor allem der Programme und Daten ohne große zeitliche Unterbrechung zu gewährleisten.

So ist auf der Grundlage einer Risiko- und Schwachstellenanalyse ein Notfallhandbuch zu erstellen, das die Beschreibung aller Maßnahmen für die Sicherstellung eines schnellen Wiederanlaufs enthält. Es ist sicherzustellen, daß alle Betriebsmittel, wie Hard- und Software, Datenbestände und Dokumentationen ohne große zeitliche Verzögerung zur Verfügung stehen.

23.1.2 Benutzerverwaltung

Zu den wichtigsten Sicherungsmaßnahmen in der automatisierten Datenverarbeitung zählen die Zugriffsschutzmaßnahmen. Jedes Großrechnerbetriebssystem enthält deshalb eine Benutzerverwaltung, in der die Zugriffsberechtigungen eines jeden Benutzers festgelegt werden können. Weil man jedoch auf Anwendungsebene detailliertere Zugriffsschutzmechanismen benötigt, verfügen moderne Dialogverfahren über eine zusätzliche Benutzerverwaltung, in der geregelt ist, auf welche Verfahrensschritte (Dialogschritte, Transak-

tionen) und Datensätze ein Benutzer Zugriff hat. Darüber hinaus muß die Benutzerverwaltung für Revisionszwecke auch Angaben darüber machen können, wer zu welcher Zeit welche Zugriffsrechte hatte. Für eine Revision der Benutzerverwaltung genügt es nicht, nur den aktuellen Stand wiederzugeben. Um die Lückenlosigkeit der Zugriffsberechtigungen belegen zu können, empfiehlt es sich, bei jeder Änderung ein eindeutiges Identifizierungsmerkmal, etwa eine Versionsnummer mit Datum und Uhrzeit, zu speichern. Jeder Änderung in den Benutzerrechten eines Teilnehmers an einem Dialogverfahren muß außerdem ein Änderungsauftrag zugrundeliegen, für den eine dafür privilegierte Stelle verantwortlich zeichnet. Bei Dialogverfahren mit vielen Teilnehmern ist es üblich, daß die Benutzerrechte durch einen eigenen Administrator verwaltet werden, der der Systemverwaltung angegliedert ist und meist selbst keine Zugriffsberechtigung auf die Echtdaten hat.

Bei Prüfungen habe ich gut durchdachte Benutzerverwaltungssysteme angetroffen, die meinen Vorstellungen von einer ordnungsgemäßen Datenverarbeitung entsprechen. Man geht vielfach sogar soweit, daß bei längerer Abwesenheit eines Benutzers, etwa bei Krankheit oder Urlaub, die Zugriffsberechtigungen gesperrt werden. Bei Urlaub- oder Krankheitsvertretungen werden andererseits die Zugriffsrechte der Betroffenen erweitert. Auch im neuentwickelten APC-Verfahren (Arbeitsplatzcomputer) der bayerischen Polizei sind meine Vorstellungen von einer revisionsfähigen Benutzerverwaltung verwirklicht worden. Diese Entwicklung begrüße ich.

Die Verwaltung der Zugriffsrechte erfordert Zeit und Sorgfalt, sie ist jedoch für eine ordnungsgemäße Datenverarbeitung unerläßlich.

23.1.3 Datenbanksysteme

Datenbanken sind große Datenbestände, die von einem eigenen Datenverwaltungssystem, auch Datenbanksystem genannt, verwaltet werden. Aufgabe eines Datenbanksystems ist die Speicherung und Wiedergewinnung von Daten nach bestimmten vom Benutzer vorgegebenen Kriterien. Moderne Datenbanksysteme enthalten vielfach eine Abfragesprache (Query-Komponente), mit deren Hilfe ad-hoc Auswertungen der Datenbestände erstellt werden können. Verfügt ein Benutzer über die Berechtigung zur Benutzung der Abfragesprache, dann stehen ihm bei der Auswertung alle verfügbaren Mittel und Wege offen. Während der Datenbankzugriff von einem Dialogprogramm aus genau festgelegt und stets überprüfbar ist, kann über die Abfragesprache jedes Datenfeld angesprochen und mit jedem anderen verknüpft werden. Abfragesprachen sind also leistungsfähige Instrumente, von deren Anwendung man nur in Ausnahmefällen Gebrauch machen sollte, sofern die Auswertung personenbezogene Ergebnisse liefert. Die Verantwortlichen für den Betrieb von Datenbanken müssen sich der Bedeutung und der Risiken dieser Komponente bewußt werden. Überall dort, wo DV-Systeme mit frei formulierbaren Auswertungen im Einsatz sind, sind deshalb folgende Regeln zu beachten:

- Die Berechtigung für die Anwendung von Query-Komponenten ist nur einigen wenigen privilegierten Personen zu gestatten.
- Über die Art einer Auswertung ist ein Protokoll zu führen, in dem das Datum, der Auftraggeber und der Zweck der Auswertung sowie der Benutzer festgehalten wird.
- Soweit vertretbar, sollte das 4-Augen-Prinzip eingehalten werden, d.h. die Auftragserstellung ist von der Auftragsbearbeitung zu trennen und unterschiedlichen Personen zuzuordnen, damit eine gewisse gegenseitige Kontrolle gewährleistet ist.
- Die Möglichkeiten der Anwendung von Query-Komponenten sollten bei der datenschutzrechtlichen Freigabe nach Art. 26 Abs. 2 BayDSG gewürdigt werden.

23.2 Prüfungstätigkeit

23.2.1 Kontrolle und Beratung

Im Berichtszeitraum haben meine Mitarbeiter bei folgenden Stellen die Einhaltung der technischen und organisatorischen Maßnahmen zur Datensicherung überprüft:
- Rechenstelle in der Obersten Baubehörde
- Rechenzentrum des Landesverbands der Betriebskrankenkassen in Bayern
- Rechenzentrum des Polizeipräsidiums München
- Zentrale Datenverarbeitung der Bayerischen Versicherungskammer
- Rechenzentrum des Gemeindeunfallversicherungsverbandes
- Rechenstelle des Bezirks Oberbayern (Sozialhilfeverwaltung)
- Rechenzentrum der Regierung von Oberbayern
- Maschinelle Datenverarbeitung im Finanzamt München II
- Maschinelle Datenverarbeitung der AOK Berchtesgadener Land — Traunstein
- Landratsamt Landshut
- Stadtverwaltung Fürth
- Stadtverwaltung Neuburg a.d.Donau
- Stadtverwaltung Wolfratshausen
- Gemeindeverwaltung Germering (Landkreis Fürstenfeldbruck)
- Maschinelle Datenverarbeitung bei zwei Gymnasien und einer Berufsschule

Informationsbesuche fanden wiederum bei einer Reihe von Privatfirmen statt, die für öffentliche Stellen im Auftrag personenbezogene Daten verarbeiten. Bei den Privatfirmen handelte es sich um Mikroverfilmungsbetriebe, Datenträgerentsorgungsunternehmen und Datenerfassungsbüros.

Die Beratungen verfolgen das Ziel, Verstößen gegen die Datenschutzgesetze vorzubeugen und die Sicherheit der maschinellen Datenverarbeitung zu erhöhen. Sicherheitsberatungen wurden bei sechs Landratsämtern, drei Gemeinden, zwei Allgemeinen Ortskrankenkassen, mehreren Kliniken und bei fünf Fachrechenzentren durchgeführt.

Die Kontakte zu den Herstellern von Hard- und Software sind für die Beurteilung neuer DV-Techniken und für die Entwicklung von geeigneten Vorschlägen für Sicherheitsmaßnahmen außerordentlich wichtig. Wie im vergangenen Jahr wurden auch im Berichtszeitraum die Kontakte zu Hard- und Softwareherstellern gepflegt. Sichtbare Ergebnisse dieses Dialogs sind beispielsweise die Orientierungshilfen für Datensicherheitsmaßnahmen beim Einsatz mittlerer DV-Systeme. Zu den bereits 1988 verfügbaren Orientierungshilfen für die DV-Anlagen des Typs Hewlett Packard 3000, Mannesmann-Kienzle 9000, NCR ITX 10.000 und

Nixdorf 8870 (siehe 10. Tätigkeitsbericht, S. 58) kamen 1989 ähnlich aufgebaute Papiere für Wang VS 100 und Siemens MX 300/MX 500 hinzu. Die Reihe soll für moderne Unix-Systeme anderer Hersteller fortgesetzt werden.

Die Orientierungshilfen können bei meiner Geschäftsstelle angefordert werden.

23.2.2 Ergebnisse der Kontrolltätigkeit

Auch im Berichtszeitraum 1989 konnte bei den Kontrollen festgestellt werden, daß der Stand der technischen und organisatorischen Maßnahmen zur Datensicherung recht unterschiedlich ist. Zum Teil wurden wiederum Datensicherungsmaßnahmen von hoher Qualität angetroffen. Aber ich mußte auch immer noch teilweise erhebliche Mängel im Datensicherungskonzept feststellen.

Typisch sind folgende Mängel:
- Unregelmäßigkeiten bei der Vergabe der Benutzerrechte
- Fehlen einer revisionsfähigen Dokumentation der Benutzerrechte
- Fehlen von geeigneten Reaktionen bei Verletzungen von Sicherheitsmaßnahmen
- hohe Brandlasten im Rechnerraum
- Fehlen von Feuchtigkeitsmeldern im Rechnerraum
- mangelhafte Sicherung der Frischluftansaugstutzen für die Klimaanlage, die den Rechnerbereich versorgen
- mangelhafte Aufbewahrungsbehältnisse für die Sicherungsdatenträger
- Mängel bei der ordnungsgemäßen Verwaltung der Datenträger
- mangelhafte Kontrollmaßnahmen gegenüber Betriebsfremden (z.B. Reinigungskräften im Rechnerbereich)
- mangelhafte Dokumentation von DV-Verfahren, insbesondere bei Programmänderungen
- fehlender Überblick über die eingesetze Hard- und Software, insbesondere im PC-Bereich
- mangelhafte Kontrolle vorgegebener Datensicherungsmaßnahmen, insbesondere bei der Entsorgung von Datenträgern

Wegen ihrer generellen Bedeutung wird auf einige Mängel ausführlicher eingegangen.

Vergabe von Zugriffsrechten

Bei Kontrollen habe ich festgestellt, daß die tatsächlich **vergebenen** und wirksamen Zugriffsrechte mit den bei der Fachabteilung **dokumentierten** nicht übereinstimmen. Diese Diskrepanz ist häufig darauf zurückzuführen, daß die Fachabteilung die Zugriffsrechte nicht schriftlich beantragt hat oder kein formalisiertes Verfahren für die Vergabe dieser Zugriffsrechte vorliegt. Keinesfalls dürfen Zugriffsrechte etwa auf einen telefonischen Hinweis hin eingerichtet werden.

Fehlen eines Notfallkonzepts

Die Abhängigkeit von der Funktionsfähigkeit der automatisierten Datenverarbeitung wächst ständig. Viele Behörden wickeln ihre Tagesgeschäfte fast ausschließlich im Dialog mit der DV-Anlage ab. Die maschinell gespeicherten und verwalteten Datenbestände haben weitgehend die herkömmlichen Karteien abgelöst. Um so dringlicher ist es, daß man sich Gedanken macht, wie man einen längeren Ausfall der DV-Anlage verkraften und durch geeignete Maßnahmen überbrücken kann. Nur vereinzelt sind Ansätze für Notfallkonzepte vorzufinden. Manchmal gibt es überhaupt keine Vorstellungen darüber, welche Aufgaben nach welcher Zeit und unter welchen Bedingungen wieder anlaufen müssen.

Fehlender Zugriffsschutz und Dokumentation

Bei den Kontrollen z.B. im Schulbereich hat sich gezeigt, daß die Verwaltung überwiegend Personal Computer einsetzt, die vom System her keine Sicherungsmaßnahmen bieten. Steht ein solcher Rechner in einem vielen Personen zugänglichen Raum, dann sind Zugriffsschutzmaßnahmen unerläßlich. Gerade im MS-DOS-Bereich gibt es heute eine Vielzahl von Produkten, welche die Datensicherheit und den Zugriffsschutz ausreichend unterstützen.

Außerdem zeigten die Kontrollen, daß die Dokumentation der Schulverwaltungsprogramme weitgehend fehlt. Die Dokumentation eines DV-Verfahrens muß aber so beschaffen sein, daß sich ein sachverständiger Dritter in einer angemessenen Zeit darin zurechtfindet.

Schließlich ist immer wieder festzustellen, daß in der manuellen Datenverarbeitung personenbezogene Unterlagen teilweise hoch sensiblen Inhalts nicht zugriffssicher aufbewahrt werden.

Trotz der aufgeführten Mängel ist festzuhalten, daß sich die meisten Behörden bemühen, den Anforderungen an eine ordnungsgemäße Datensicherung gerecht zu werden. Als Beispiel für eine überdurchschnittliche Sicherungsmaßnahme sei die revisionsfähige Abwicklung der Datenverarbeitungsaufgaben in einem Fachrechenzentrum herausgestellt. Da das Betriebssystem viele Sicherheitskomponenten nicht ausreichend unterstützt, wurden im Rechenzentrum in Eigenregie eine automatisierte Datenträgerverwaltung und Terminplanung erstellt, welche die unter Ziffer 21.4 auf S. 57 im 10. Tätigkeitsbericht geforderten Eigenschaften weitgehend erfüllen.

23.2.3 Erledigung von Prüfungsfeststellungen

Den nach Art. 15 BayDSG kontrollierten öffentlichen Stellen wird unter angemessener Fristsetzung die Beseitigung der festgestellten Mängel auferlegt. In der Regel werden — von baulichen Maßnahmen abgesehen — die Mängel in der vorgegebenen Zeit auch tatsächlich behoben. Bei baulichen Sicherheitsmaßnahmen größeren Umfangs läßt sich eine zeitliche Verzögerung nicht ausschließen, da die Haushaltsmittel vielfach erst im nächsten Doppelhaushalt beantragt werden müssen.

In der letzten Zeit waren aber in Stellungnahmen von geprüften Dienststellen wiederholt nur Absichtserklärungen als Erledigungsvermerke zu Prüfungsfeststellungen enthalten. Bemerkungen wie, „man werde die aufgezeigten Mängel beheben" oder „die Beschaffungsmaßnahme werde in die Wege geleitet", sind als Erledigung unzureichend, zumal dann, wenn keine Terminangaben gemacht werden. Ich muß erwarten, daß die festgelegten, häufig mit den geprüften Dienststellen abgesprochenen Erledigungstermine eingehalten werden, wobei Fristverlängerungen im begründeten Einzelfall selbstverständlich möglich sind.

Ein konkreter Anlaß zwingt mich desweiteren darauf hinzuweisen, daß es zu den dienstlichen Aufsichtspflichten eines Behördenleiters gehört, sich davon zu überzeugen, daß Maßnahmen, die als Erledigung von Prüfungsbemerkun-

gen beschrieben werden, auch tatsächlich getroffen worden sind. Bei einer Nachprüfung stellte sich jedoch heraus, daß die gerügten Mängel keineswegs behoben waren. Aus dieser Erfahrung heraus werde ich künftig vermehrt Nachkontrollen im Rahmen des Art. 15 BayDSG vornehmen.

23.3 Technische Einzelprobleme

23.3.1 Verschlüsselung

Mit wachsendem Sicherheitsbedürfnis gewinnt in Wirtschaft, Forschung und Verwaltung die Verschlüsselungstechnik an Bedeutung. Die Hersteller von Betriebssystemen bieten heute beispielsweise standardmäßig die sog. Einwegverschlüsselung für Paßworte an. Einwegverschlüsselung bedeutet, daß es keinen Algorithmus gibt, mit dessen Hilfe aus dem verschlüsselten Text (Chiffrat) der Ursprungstext zu ermitteln ist. Die Einwegverschlüsselung verwendet man deshalb nur für die Verschlüsselung von Code-Wörtern (z.B. Paßwörter) oder zur Erzeugung sog. Prüfsummen für Programme und Daten. Die Gültigkeit eines Code-Wortes oder einer Prüfsumme ist über den Vergleich des aktuell gebildeten Chiffrats mit dem gespeicherten Chiffrat des Code-Wortes oder der Prüfsumme festzustellen. Sind die Schlüsseltexte identisch, so ist das eingegebene Code-Wort gültig bzw. sind das Programm oder die Daten, die die Prüfsumme ergaben, in unverändertem Zustand. Prüfsummenverfahren werden z.B. zum Erkennen eines Virenbefalls eines Programms eingesetzt.

Bei Prüfungen habe ich festgestellt, daß gewählte Verschlüsselungsverfahren keine echten Verschlüsselungen darstellen, weil es sich bei diesen Verfahren lediglich um Code-Umsetzungen handelte. Code-Umsetzungen bieten jedoch gegenüber Experten nur einen geringen Schutz, da sie durch die Auswertung des Chiffrats (Häufigkeitsauszählungen) und unter Hinzuziehung von öffentlich zugänglichem Zusatzwissen (z.B. Telefonbuch, Adreßbuch) meist schon geknackt werden können. Sie sind als Verschlüsselungstechnik heute nicht mehr geeignet.

Für die Verschlüsselung von Nachrichten, Daten und Programmen werden andere sicherere Verfahren benötigt, beispielsweise symmetrische oder asymmetrische Verschlüsselungsverfahren. Bei einem symmetrischen Verschlüsselungsverfahren wird für die Ver- und Entschlüsselung derselbe Schlüssel verwendet. Die Entschlüsselung geschieht durch nochmalige Verschlüsselung des Chiffrats mit dem gleichen Schlüssel. Bei einem asymmetrischen Verschlüsselungsverfahren verwendet man ein Schlüsselpaar, einen sog. öffentlichen und einen geheimen Schlüssel. Bei dieser Methode wird mit dem sog. öffentlichen Schlüssel verschlüsselt und mit dem geheimen Schlüssel entschlüsselt. Wegen des größeren Durchsatzes werden heute überwiegend symmetrische Verschlüsselungsverfahren eingesetzt.

Bei meiner Dienststelle fragen auch wissenschaftliche Forschungseinrichtungen und Klinikverwaltungen an, ob die für Forschungsvorhaben entwickelten Verschlüsselungsverfahren die Anonymität der gespeicherten Personen gewährleisten. Für die Verschlüsselung von identifizierenden Merkmalen dieser Personen sind höherwertige Verschlüsselungstechniken, etwa symmetrische Verschlüsselungsverfahren zu verwenden.

23.3.2 Zugriffssicherheit bei Wählleitungen

Auch im Berichtszeitraum ist kein Fall bekannt geworden, daß Unberechtigte über Wählleitungen (= Telefonverbindungen) in Computersysteme der öffentlichen bayerischen Verwaltung eingedrungen seien. Dennoch weise ich wegen der besonderen Bedeutung, die der Zugriffssicherheit bei Wählleitungen zukommt, noch einmal kurz auf folgendes hin.

Hacker können einen Verbindungsaufbau nur erfolgreich durchführen, wenn ihnen die Anschlußnummern der Wählleitung, eine zugelassene Benutzerkennung und das vereinbarte Kennwort bekannt sind.

Daraus sind folgende Sicherungsmaßnahmen abzuleiten:

Fehlversuche, hinter denen sich auch das Eindringen eines Hackers verbergen kann, müssen systemseitig erkannt und automatisch abgewiesen werden. Nach einer bestimmten Anzahl von Fehlversuchen, in der Regel nach drei Versuchen, ist die Leitung zu sperren oder die betreffende Benutzerkennung stillzulegen. Die Fehlversuche sind mit den Anmeldeparametern revisionsfähig zu protokollieren, damit solchen mißbräuchlichen Zugriffsversuchen nachgegangen werden kann. Erfolgt der Verbindungsaufbau durch einen automatischen Wählvorgang beim Anmeldenden, ist die zulässige Anzahl von Fehlversuchen — sofern die Zentrale Kenntnis über die Art des Anmeldevorganges hat (z.B. bei der Fernwartung) — auf eine einzige zu begrenzen, da in diesem Fall unbeabsichtigte Fehleingaben auszuschließen sind. Protokollinformationen sind nach unberechtigten Anmeldeversuchen täglich auszuwerten. Hierüber ist ein Sicherheitsbericht anzufertigen.

Die Zugriffssicherheit bei Wählanschlüssen kann jedoch DV-gestützt nur gewährleistet werden, wenn eine geeignete Sicherheitssoftware, etwa RACF (Resource Access Control Facility) bei IBM-Anwendern, vorhanden ist. Steht eine solche automatisierte Unterstützung nicht zur Verfügung, sind andere geeignete technische und organisatorische Maßnahmen zu ergreifen.

So wird in einem mir bekannten Fall ein manuelles Rückrufverfahren praktiziert. Der Anrufer, der einen Verbindungsaufbau anstrebt, wird anhand seiner Kennung identifiziert. Erst nach erfolgreicher Überprüfung durch einen Rückruf (Authentifikation) wird die Verbindung hergestellt.

23.3.3 Auftragsdatenverarbeitung

In der automatisierten Datenverarbeitung muß die öffentliche Verwaltung häufig auf Expertenwissen von Privaten zurückgreifen, wenn komplizierte technische Programme zu entwickeln sind. Ist für eine solche Verfahrensentwicklung die Kenntnis von Echtdaten erforderlich, ist besondere Vorsicht geboten. Eine Panne bei der Abwicklung eines Programmentwicklungsauftrages durch eine Privatfirma nehme ich zum Anlaß, an die Einhaltung folgender Datensicherheitsmaßnahmen zu erinnern, insbesondere dann, wenn sensitive personenbezogene Daten verwendet werden:

- Bei der Vergabe von Aufträgen an Externe ist darauf zu achten, daß nur solche Firmen DV-Aufträge erhalten, die in der Lage sind, die Aufgaben ohne Einschaltung von Subunternehmen durch eigenes zuverlässiges Personal

zu erledigen. Die Sicherheit muß hier Vorrang vor dem billigeren Angebot haben.

- Bei den Aufträgen, die mit Privatfirmen abgeschlossen werden, sind für den Fall der Verletzung von Datenschutzvorschriften Vertragsstrafen vorzusehen.

- Um den Echtbetrieb simulieren zu können, ist für den Testbetrieb ein wirklichkeitsgetreuer Datenbestand aufzubauen, der aber keine Originaldaten enthalten darf. Ein Test mit Originaldaten ist privaten Auftragnehmern grundsätzlich nicht zu erlauben.

- Ist in Ausnahmefällen die Verwendung von Echtdaten unvermeidbar, so ist durch organisatorische Maßnahmen, etwa durch eine Vier-Augen-Kontrolle, sicherzustellen, daß Originaldaten nicht zweckentfremdet verwendet und keinesfalls aus dem Bereich der speichernden Stelle entfernt werden.

- Verlassen Datenträger den geschützten Bereich, ist deren Inhalt genauestens zu überprüfen (Abgangskontrolle). Durch eine solche Kontrollmaßnahme läßt sich feststellen, ob die Datenträger noch versehentlich kopierte Daten enthalten. Außerdem ist zu protokollieren, wer wann welche Datenträger mit welchem Inhalt erhalten hat.

23.3.4 Entsorgung von Datenträgern

Im Berichtszeitraum wurde ich wiederum mit einer Reihe von Fällen befaßt, bei denen durch ein mangelhaftes Datenträgerentsorgungskonzept Unbefugte Kenntnis von personenbezogenen Daten erhielten. Meistens handelte es sich um Papierunterlagen.

Besonders peinlich war für eine Behörde zu erfahren, daß ein Altarchiv bei einem Umzug in ein neues Dienstgebäude offenbar „vergessen" wurde. Einige, mittlerweile schon vernichtete Unterlagen mit sensiblen Sozialdaten gelangten durch Zufall an die Öffentlichkeit. Solche Pannen sind vermeidbar, wenn die Aussonderungsvorschriften strikt eingehalten werden. Das nützt nicht nur dem Datenschutz, sondern schafft obendrein freien Registraturraum.

Noch immer gibt es Behörden, die Unterlagen mit personenbezogenen Daten, seien es nur Name, Geburtsdatum und Anschriften eines Petenten, mit dem Hausmüll entsorgen. Diese Entsorgungsart ist nicht datenschutzgerecht, da dabei Bürgerdaten in falsche Hände gelangen können.

Ferner erhielt ich unsachgemäß entsorgte Unterlagen mit schutzwürdigen Daten zugesandt, die als Füllmaterial in Verpackungsbehältnissen verwendet wurden. Zwar waren aus den Papierschnitzel, die manchmal eine Breite von mehreren Zentimetern aufwiesen, die Dokumente nicht mehr vollständig rekonstruierbar. Das kann aber daran gelegen haben, daß mir nur ein Bruchteil des mangelhaft entsorgten Gutes zugänglich gemacht wurde.

Diese Beispiele zeigen, daß bei der Entsorgung von Datenträgern vielfach noch zu gedankenlos verfahren wird. Deshalb weise ich an dieser Stelle nochmals auf die Notwendigkeit hin, für eine sichere Entsorgung nach DIN 32757 zu sorgen.

23.3.5 Sicherer Transport von Datenträgern

Beim Versand einer Datei mit personenbezogenen Daten ist die Einhaltung der erforderlichen Sicherheitsmaßnahmen zu beachten. Im normalen Postversand ist auf eine ordentliche und stabile Verpackung Wert zu legen. Pakete können während des Transports aufgerissen werden. Außerdem können Unbefugte solche Pakete absichtlich anreißen, ohne daß sich hierfür ein Nachweis erbringen läßt. Gefährdete Stellen sind deshalb besonders zu verkleben. Wegen des Risikos einer Falschzustellung oder eines Verlustes ist beim Versand von besonders sensiblen personenbezogenen Unterlagen eine höherwertige Versandart zu wählen oder ein Kurierdienst einzuschalten. Zu solchen sensiblen personenbezogenen Daten können im Einzelfall auch Einwohnermeldedaten zählen, wenn „ein Mißbrauch dieser Daten die gesellschaftliche Stellung oder die wirtschaftlichen Verhältnisse des Betroffenen erheblich beeinträchtigen kann" (Datenklassifikation im Datensicherungskatalog des Koordinierungsausschusses Datenverarbeitung in Bayern vom 30.7.1980). Jede Gemeinde hat deshalb beim Versand einer Datei mit Meldedaten zu prüfen, welche Versandart angesichts der Empfindlichkeit der transportierten Daten notwendig ist.

Häufig lassen Gemeinden die neuen, von der DV-Anlage ausgedruckten Lohnsteuerkarten durch eigene Bedienstete oder Hilfskräfte zustellen. Hierbei ist darauf zu achten, daß sich die Lohnsteuerkarte in einem verschlossenen Umschlag befindet und in den Briefkasten des Empfängers geworfen wird. Keinesfalls dürfen die Briefe mit den Lohnsteuerkarten im Hausflur abgelegt werden, wie es ein Austräger getan hätte, um sich dadurch seine Arbeit zu erleichtern. Die Zusteller sind in geeigneter Weise zu schulen und auf die Sicherungsmaßnahmen bei der Zustellung aufmerksam zu machen.

24. Datenschutzregister

Nach § 8 der Verordnung über das Datenschutzregister (DSRegV) vom 23. November 1978 veröffentlicht der Landesbeauftragte für den Datenschutz jährlich eine Übersicht über den Inhalt des Datenschutzregisters. Diese Übersicht kann auch auf Nachträge zu bereits veröffentlichten Übersichten beschränkt werden.

Wegen des Umfanges der Veröffentlichungen der vergangenen Jahre und des geringen Nutzens für den Bürger wurde 1984 letztmals eine Übersicht des Gesamtinhalts des Datenschutzregisters veröffentlicht. Diese Veröffentlichung bestand aus zwei Teilen. Seit 1985 wurde von der Möglichkeit Gebrauch gemacht, lediglich Nachträge zu veröffentlichen. Der Umfang dieser Nachträge hat sich von Jahr zu Jahr ausgeweitet und beträgt inzwischen weit über 100 Druckseiten. Der 5. Nachtrag, der am 22. Dezember 1989 als Beilage zum Bayerischen Staatsanzeiger erscheinen wird, berücksichtigt die Meldungen automatisierter Dateien von speichernden Stellen, die vom 7. November 1988 bis 3. November 1989 in meiner Geschäftsstelle eingegangen sind.

Am Stichtag für den Vierten Nachtrag (7.11.1988) umfaßte das gesamte Datenschutzregister 17.871 meldepflichtige Dateien von insgesamt 5.124 speichernden Stellen. Ein Jahr später waren zum Datenschutzregister 18.858 Dateien von

5.313 speichernden Stellen gemeldet. Die Zunahme ist wiederum auch auf das Anwachsen der Schülerdateien in Realschulen, Grund- und Hauptschulen zurückzuführen. Gerade im Schulbereich sind wegen der Unvollständigkeit der Meldungen besonders viele Rückfragen erforderlich, so daß eine Reihe von Meldungen noch nicht in die Übersicht aufgenommen werden konnten. Auch die Verarbeitung von meldepflichtigen Adreßdateien und sonstigen personenbezogenen Dateien in Personal Computern und Textsystemen trägt zum jährlichen Anstieg merklich bei.

Die Pflege des Datenschutzregisters umfaßte im Berichtszeitraum folgende Arbeiten:

Neueintragen einer speichernden Stelle	209
Neueintragen einer Datei bei einer speichernden Stelle	1.221
Änderungen bei der Bezeichnung einer speichernden Stelle	819
Dateibezogene Änderungen	11
Löschen einer speichernden Stelle	20
Löschen einer Datei	234

Die relativ hohe Zahl gelöschter Dateien ist dadurch zu erklären, daß speichernde Stellen alte DV-Verfahren durch neue, dem Stand der Technik angepaßte ersetzen, so daß eine Neumeldung erforderlich ist.

25. Datenschutz beim Bayerischen Rundfunk

Bericht des Rundfunkbeauftragten

Nach Art. 21 Abs. 3 BayDSG wird die Einhaltung des Datenschutzes im Bayerischen Rundfunk (BR) vom dortigen Datenschutzbeauftragten überwacht, der jährlich über seine Tätigkeit einen Bericht erstattet. Diesen Bericht hat er auch dem Landesbeauftragten für den Datenschutz zu übermitteln (Art. 21 Abs. 3 Satz 6 BayDSG). Hieraus leite ich, wie schon in den Jahren zuvor, für mich die Aufgabe ab, kurz über den Datenschutz beim Bayerischen Rundfunk zu berichten.

Bei der Überwachung der Datenverarbeitung des BR im Zeitraum vom 01.01. — 31.12.1988 hat der Datenschutzbeauftragte — wie auch in den Vorjahren — keine datenschutzrechtliche Beanstandung ausgesprochen.

Der Gesetzentwurf der Bundesregierung zur Fortentwicklung der Datenverarbeitung und des Datenschutzes enthält einen rundfunkspezifischen Teil. Hierzu hat sich der Datenschutzbeauftragte des BR wie folgt geäußert: Der von der Berichterstattung durch die öffentlich-rechtlichen Rundfunkanstalten des Bundesrechts Betroffene soll künftig Auskunft über die der Berichterstattung zugrunde liegenden, zu seiner Person gespeicherten Daten verlangen können. Diese Regelung würde zu einer Stärkung des Persönlichkeitsrechts der Betroffenen führen. Allerdings bleibe unklar, warum der Bundesgesetzgeber diese Stärkung des Persönlichkeitsrechts nur im Rundfunk-, nicht aber im Pressebereich vornehme. Auch dort sei er jedenfalls für die Rahmengesetzgebung zuständig.

Im Berichtszeitraum hat sich der Datenschutzbeauftragte u.a. mit Problemen im Bereich der dezentralen DV-Anlagen beschäftigt. In einem Gespräch mit dem Personalrat hatte dieser die Auffassung vertreten, die Verarbeitung personenbezogener Daten auf Personalcomputern (PC) sei aus Datenschutzgründen abzulehnen. Dadurch würde auch nach Meinung des Datenschutzbeauftragten dem Datenschutz am besten Rechnung getragen. Nach den Datenschutzgesetzen sei die Verarbeitung personenbezogener Daten auf PC jedoch nur dann unzulässig, wenn die technischen und organisatorischen Maßnahmen der Datensicherheit (vgl. Art. 15 BayDSG) nicht hinreichend realisiert werden könnten. Datensicherungsmaßnahmen müßten hierbei in einem angemessenen Verhältnis zu dem angestrebten Schutzzweck stehen. Deshalb könne man nur bei besonders sensiblen personenbezogenen Daten zu dem Ergebnis kommen, daß deren Sicherheit bei einer Verarbeitung auf einem PC nicht hinreichend gewährleistet wäre. Die auf dezentralen Anlagen verarbeiteten Mitarbeiterdaten (für Bereitschaftsdienste, Vertretungen, Akkreditierungen usw.) seien nicht als sehr sensibel einzustufen.

Bis Ende Mai 1988 hat der Datenschutzbeauftragte eine Erhebung sämtlicher dezentraler DV-Anlagen im BR durchgeführt. Hierbei wurden ihm eine Reihe bis dahin nicht bekannter Anlagen gemeldet. Er geht davon aus, daß er künftig alle notwendigen Informationen vom neu eingerichteten Arbeitsbereich Büroorganisation und Kommunikationstechnik bereits im Planungsstadium erhält.

Der Datenschutzbeauftragte hat den Organisationsreferenten um Erarbeitung von Datenschutzrichtlinien für dezentrale DV-Anlagen gebeten.

Der Datenschutzbeauftragte will in nächster Zeit eine Reihe von Datenschutzfragen aufgreifen:

- Die Rundfunkanstalten werden über die Gebühreneinzugszentrale (GEZ) vernetzt. Daraus ergeben sich insbesondere Gefahren für die Datensicherheit. Außerdem wird zu klären sein, welche Daten zu welchem Zweck und auf welche Weise übermittelt werden dürfen. Die Datenschutzbeauftragten der Rundfunkanstalten haben von diesem Vorhaben erst spät erfahren. Der Datenschutzbeauftragte des BR wird diesen Problemen nachgehen.

- Kontrollmitteilungen über die Empfänger von Honorarzahlungen der Rundfunkanstalten werden im Vorgriff auf eine zu erwartende Rechtsverordnung zu § 93 AO bereits jetzt an die Finanzämter geschickt. Diese Sachbehandlung beruht auf einer Empfehlung des Datenschutzbeauftragten des BR, die mit mir abgesprochen ist.

- Im Fernseharchiv-Dokumentationssystem FEFAD sind auch Mitarbeiterdaten enthalten, die grundsätzlich dem Medienprivileg unterliegen. Die Daten lassen eine Verhaltens- und Leistungskontrolle zu. Außerdem enthält das System auch einige administrative Daten. Daher unterliegt die Datei insgesamt den Datenschutzvorschriften. Der Datenschutzbeauftragte des BR wird prüfen, ob die Datenverarbeitung hinsichtlich aller Daten datenschutzrechtlich zulässig ist und dem BR dann die notwendigen Empfehlungen geben.

26. Der Beirat

Die Mitglieder des Beirats werden nach Art. 29 Abs. 2 BayDSG für vier Jahre, die Mitglieder des Landtags für die Wahldauer des Landtags bestellt. Im Berichtszeitraum gehörten dem Beirat an:

Ordentliche Mitglieder	Vertreter
Die Landtagsabgeordneten	
Franz Brosch	Willi Baumann
Adolf Dinglreiter	Franz Xaver Werkstetter
Dieter Heckel	Anneliese Fischer
Peter Welnhofer	Adolf Beck
Klaus Warnecke	Armin Nentwig
Carmen König	Hedda Jungfer
Die Senatoren	
Wolfgang Burnhauser	Hartwig Reimann
Für die Staatsregierung	
Dr. Klaus Geiger Ministerialdirigent im Bayer. Staatsministerium der Finanzen	Joachim Schweinoch Ministerialdirigent im Bayer. Staatsministerium des Innern Nach dessen Ableben wurde Ministerialdirigent Alfons Metzger zum Nachfolger bestellt.
Für die Kommunalen Spitzenverbände	
Dr. Georg Wilhelm Geschäftsleitender Direktor der Anstalt für kommunale Datenver- arbeitung in Bayern und nach dessen Aus- scheiden aus dem öffent- lichen Dienst ab 01.05.1989 sein Nachfolger Klaus Eichhorn	Klaus Eichhorn Direktor der Anstalt für kommunale Datenver- arbeitung in Bayern und nach dessen Berufung zum ordentlichen Mitglied Hanns Herlitz Direktor bei der Anstalt für kommunale Datenverarbei- tung in Bayern
Für die Sozialversicherungsträger	
Franz Martin Fehn Erster Direktor der Landesversicherungs- anstalt Oberfranken und Mittelfranken	Herbert Schmaus Verwaltungsdirektor beim AOK-Landesverband Bayern
Für den Verband der Freien Berufe in Bayern e.V.	
Dr. med. Hans Braun Präsident des Verbandes der Freien Berufe in Bayern e.V.	Winfried Wachter Präsidiumsmitglied des Verbandes der Freien Berufe in Bayern e.V.

Den Vorsitz im Beirat führt MdL Franz Brosch, sein Stellvertreter ist MdL Klaus Warnecke.

Der Beirat befaßte sich in seinen vier Sitzungen am 08.12.1988, 07.03.1989, 11.07.1989 und 24.10.1989 insbesondere mit folgenden Themen:

- Beratung des 10. Tätigkeitsberichts
- Bericht über Prüfungen und Beanstandungen
- Stand und wesentliche Inhalte der Novellierung der Strafprozeßordnung
- Entwurf eines Gesetzes zur Fortentwicklung der Datenverarbeitung und des Datenschutzes
- Entwurf eines Gesetzes zur Einführung eines Sozialversicherungsausweises
- Entwurf für ein Rentenreformgesetz
- Übermittlung von Meldedaten an politische Parteien
- Ausübung des gemeindlichen Vorkaufsrechts nach den Vorschriften des Baugesetzbuches
- Aktivitäten von Auskunfteien
- Computerhacking und Computerkriminalität

27. Konferenz der Datenschutzbeauftragten

Die Datenschutzbeauftragten der Länder und des Bundes und die Datenschutzkommission Rheinland-Pfalz trafen sich 1989 zu drei Konferenzen. Schwerpunkte der Erörterungen waren:

- Entwurf eines Rentenreform-Gesetzes 1992
- Strafverfahrensänderungsgesetz 1988
- Änderung des G 10-Gesetzes und der StPO im Rahmen der Poststrukturreform
- Gesetzentwürfe für ein Bundesverfassungsschutzgesetz, ein MAD-Gesetz und ein BND-Gesetz
- Genomanalyse
- Datenschutzrechtliche Forderungen zum Schengener Zusatzübereinkommen über Ausgleichsmaßnahmen zum Grenzabbau
- Datenschutz in der Europäischen Gemeinschaft
- EG-Statistikrecht

28. Vorträge und Seminare über Datenschutz

Die Nachfrage nach Referenten für Vorträge zum Datenschutz und zur Datensicherung hat sich weiter erhöht. Soweit nicht die Arbeitsbelastung durch vorrangige Datenschutzkontrollen die Übernahme von Vorträgen und Seminaren verhinderte, konnte den Anfragen entsprochen werden.

Beim Landesamt für Statistik und Datenverarbeitung und bei der Bayerischen Verwaltungsschule waren zahlreiche Vorträge oder auch mehrtägige Seminare zu halten. Neben einer allgemeinen Einführung in Datenschutz und Datensicherung befaßten sich die Veranstaltungen mit speziellen Themen wie „Datenschutz im Krankenhaus", „Datenschutz im Sozialamt", „Datenschutz im Melderecht", „Datenschutz im Sicherheits- und Ordnungsrecht". Außerdem war ich an der Aus- und Weiterbildung behördlicher Datenschutzbeauftragter beteiligt. Da die Aufnahme des Informatik-Unterrichts an den Schulen fortschreitet, bestand unverändert Bedarf an entsprechender Weiterbildung von Lehrkräften an der Lehrerakademie Dillingen. An der Fort- und Ausbildung der bayerischen Polizei wirkten meine Mitarbeiter mit

zahlreichen Vorträgen mit. Die Ausbildung der Rechtsreferendare konnte ich fortführen.

Neben diesen regelmäßig laufenden Fortbildungsmaßnahmen waren Vorträge zu halten vor juristischen Staatsbeamten eines Regierungsbezirks, in Zusammenarbeit mit dem Staatsministerium der Justiz vor Bewährungshelfern sowie vor Richtern und Staatsanwälten, vor Referendaren des Vermessungsdienstes sowie im Fachhochschulbereich.

Zu erwähnen ist ferner, daß eine Gruppe von Studenten der Rechtswissenschaft der „University of Warwick" in Coventry (Großbritannien) einen Besuch in München zum Anlaß nahm, sich in meiner Geschäftsstelle über die Grundzüge des deutschen Datenschutzrechts unterrichten zu lassen. Der Erfolg dieses Besuchs wird daran deutlich, daß das Thema Datenschutz nunmehr auch im Lehrplan der University of Warwick berücksichtigt wird. Auch ist der Besuch weiterer Studentengruppen in meiner Dienststelle bereits angekündigt.

Anhang 1: Genomanalyse und Datenschutz

Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder sowie der Datenschutzkommission Rheinland-Pfalz vom 26./27.10.1989 über Genomanalyse und informationelle Selbstbestimmung

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder sowie der Datenschutzkommission Rheinland-Pfalz hat den Abschlußbericht der Enquete-Kommission des Deutschen Bundestages „Chancen und Risiken der Gentechnologie" (Drucksache 10/6775) zum Anlaß genommen, die Risiken für die informationelle Selbstbestimmung jedes Betroffenen abzuwägen gegenüber den Chancen, die die Genomanalyse bringt. Durch die Offenlegung genetischer Daten eines Menschen kann dieser in seinem Persönlichkeitsrecht und sonstigen schutzwürdigen Belangen nachhaltig beeinträchtigt werden. Informationen aus dem Kernbereich der Privatsphäre, die dem Betroffenen selbst bisher unbekannt waren, können ihn zu einem an sich ungewollten Verhalten in seiner Lebens- oder Berufsgestaltung veranlassen; ihre Kenntnis kann zu einer psychischen und sozialen Zwangslage für den Betroffenen führen. Wegen der genetischen Bedingtheit solcher Informationen können sich daher auch entsprechende Auswirkungen auf dritte Personen, insbesondere die Familie, ergeben. Das Bekanntwerden solcher Informationen kann den Betroffenen in seinem sozialen Umfeld diskriminieren mit der möglichen Folge gesellschaftlicher Ausgrenzung.

Um den besonderen Risiken bei der Anwendung der Genomanalyse zu begegnen, bedarf es der gesetzlichen Absicherung folgender Grundsätze:

1. Die Genomanalyse darf grundsätzlich nur auf freiwilliger Basis nach umfassender Aufklärung der Betroffenen vorgenommen werden; ausgenommen sind Straf- und Abstammungsverfahren.

2. Die jederzeit widerrufliche Einwilligung muß sich auch auf die weitere Verwendung der genetischen Informationen erstrecken. Im Falle eines Widerrufs sind die gewonnenen Informationen zu löschen oder an den Betroffenen herauszugeben.

3. Jede Genomanalyse muß zweckorientiert vorgenommen werden. Es ist diejenige genomanalytische Methode zu wählen, die keine oder die geringste Menge an Überschußinformationen bringt. Überschußinformationen sind unverzüglich zu vernichten.

4. Es ist zu prüfen, inwieweit genomanalytische Untersuchungsmethoden einer staatlichen Zulassung bedürfen. Für DNA-Sonden ist dies jedenfalls zu bejahen.

5. Die Genomanalyse im gerichtlichen Verfahren muß auf die reine Identitätsfeststellung beschränkt werden; es dürfen keine genomanalytischen Methoden angewandt werden, die Überschußinformationen zur Person liefern. Die Nutzung der Genomanalyse im Strafverfahren setzt eine normenklare gesetzliche Ermächtigung voraus. Präzise Regelungen müssen u.a. sicherstellen, daß genomanalytische Befunde einer strengen Zweckbindung unterworfen werden.

6. Im Arbeitsverhältnis sind die Anordnung von Genomanalysen oder die Verwendung ihrer Ergebnisse grundsätzlich zu verbieten. Ausnahmen bedürfen der gesetzlichen Regelung. Eine bloße Einwilligung des Arbeitnehmers ist wegen der faktischen Zwangssituation, der er im Arbeitsleben häufig unterliegt, nicht ausreichend.

7. Genomanalysen im Versicherungswesen sind grundsätzlich nicht erforderlich und mit dem Prinzip der Versicherungen, Risiken abzudecken und nicht auszuschließen, unvereinbar. Dies sollte durch eine Klarstellung im Versicherungsvertragsgesetz deutlich gemacht werden.

8. Im Rahmen der pränatalen Diagnostik dürfen nur Informationen über das Vorhandensein oder Fehlen von Erbanlagen erhoben werden, bei denen eine Schädigung heilbar ist oder die zu einer so schwerwiegenden Gesundheitsschädigung des Kindes führen würden, daß ein Schwangerschaftsabbruch straffrei bliebe.

   Reihenuntersuchungen an Neugeborenen dürfen sich nur auf solche Erbkrankheiten erstrecken, die bei frühzeitiger Erkennung eines genetischen Defekts geheilt oder zumindest spürbar therapeutisch begleitet werden können.

   Die Eltern müssen nach umfassender fachkundiger Beratung in voller Freiheit über die Anwendung genomanalytischer Methoden entscheiden können. Jegliche Beeinflussung, insbesondere jeder individuelle und gesellschaftliche Druck, muß vermieden werden.

   Die informationelle Selbstbestimmung Dritter, zu der auch das Recht auf Nichtwissen gehört, muß berücksichtigt werden.

Die Konferenz versteht ihre Stellungnahme als Beitrag zur Diskussion mit allen Institutionen, die an den Fragen der Genomanalyse arbeiten. Sie legt Wert darauf, den Dialog mit der Wissenschaft fortzusetzen und dabei neue wissenschaftliche Erkenntnisse einzubeziehen.

Anlage 2: Vorschlag zur Ergänzung des Bundesdatenschutzgesetzes, betreffend die Medien

§ 37
Verarbeitung und Nutzung personenbezogener Daten durch die Medien

(1) [1]Soweit personenbezogene Daten von Unternehmen oder Hilfsunternehmen der Presse oder des Films oder von Hilfsunternehmen des Rundfunks ausschließlich zu eigenen journalistisch-redaktionellen Zwecken verarbeitet oder genutzt werden, gelten die Vorschriften des Ersten Abschnittes mit Ausnahme des § 4. [2]Soweit Verlage personenbezogene Daten zur Herausgabe von Adressen-, Telefon-, Branchen- oder vergleichbaren Verzeichnissen verarbeiten oder nutzen, gelten Satz 1 und § 38 a nur, wenn mit der Herausgabe zugleich eine meinungsbildende journalistisch-redaktionelle Tätigkeit verbunden ist.

(2) Führt die journalistisch-redaktionelle Verarbeitung oder Nutzung personenbezogener Daten durch Unternehmen oder Hilfsunternehmen der Presse oder des Films oder die Rundfunkanstalten des Bundesrechts zur Veröffentlichung von Gegendarstellungen der Betroffenen, so sind diese Gegendarstellungen zu den gespeicherten Daten zu nehmen und für dieselbe Zeitdauer aufzubewahren wie die Daten selbst.

(3) [1]Dem Betroffenen ist auf Antrag über die zu seiner Person gespeicherten Daten Auskunft zu erteilen. [2]Die Auskunft kann verweigert werden, soweit aus den Daten auf die Person des Verfassers, Einsenders oder Gewährsmannes von Beiträgen, Unterlagen und Mitteilungen für den redaktionellen Teil geschlossen werden kann oder die Erfüllung der publizistischen Aufgabe das Interesse des Betroffenen an der Auskunftserteilung überwiegt. [3]Der Betroffene kann die Berichtigung unrichtiger Daten verlangen. [4]Steht die Unrichtigkeit von Daten fest und können richtige Daten nicht ermittelt werden, so kann der Betroffene die Löschung verlangen.

(4) Im übrigen gelten für die Rundfunkanstalten des Bundesrechts die Vorschriften des Ersten Abschnittes mit Ausnahme des § 4. Anstelle der §§ 22 bis 24 gilt § 38, auch soweit es sich um Verwaltungsangelegenheiten handelt.

(5) Für die Unternehmen oder Hilfsunternehmen der Presse gilt im übrigen § 38 a.

§ 38 a
Beauftragter für den Datenschutz bei Presse

(1) [1]Es ist ein Beauftragter für den Datenschutz der Presse zu bestellen. [2]Der Beauftragte für den Datenschutz wird auf Vorschlag des Presserates vom Bundespräsidenten auf die Dauer von vier Jahren ernannt, wobei Wiederbestellungen zulässig sind. [3]Das Amt eines Beauftragten für den Datenschutz kann neben anderen Aufgaben innerhalb eines Unternehmens der Presse wahrgenommen werden.

(2) § 38 Abs. 2 Satz 2 und Abs. 3 gelten entsprechend.

(3) Der Beauftragte für den Datenschutz erstattet dem Presserat alle zwei Jahre, erstmals zum 1. Januar ..., einen Bericht.

(4) Der Beauftragte für den Datenschutz kontrolliert die Einhaltung der Vorschriften dieses Gesetzes sowie anderer Vorschriften über den Datenschutz bei Unternehmen und Hilfsunternehmen der Presse, soweit sich ein Betroffener an ihn wendet und ihm hinreichende Anhaltspunkte dafür darlegt, daß er in seinen Rechten verletzt worden ist, oder dem Beauftragten für den Datenschutz hinreichende Anhaltspunkte für eine derartige Verletzung vorliegen; die Kontrolle ist auf den Einzelfall beschränkt.

(5) § 53 Abs. 1 Nr. 5 StPO sowie § 21 Abs. 4 und § 34 Abs. 3 und 4 gelten entsprechend.

Begründung zu § 37

Der Geltungsbereich von § 37 wird über den Rundfunk hinaus auf Unternehmen und Hilfsunternehmen der Presse und des Films ausgedehnt.

Die Pressefreiheit ist nicht schrankenlos gewährleistet; sie findet ihre Grenzen u.a. in den Vorschriften der allgemeinen Gesetze (Art. 5 Abs. 2 GG). Die Pressefreiheit findet auch dort eine Grenze, wo sie auf andere gewichtige Interessen des freiheitlichen demokratischen Staates trifft und die Erfüllung der publizistischen Aufgabe nicht den Vorrang der Pressefreiheit erfordert (BVerfGE 25, 296/305 ff). Zu diesen gewichtigen Interessen zählen die Achtung der Menschenwürde und die freie Entfaltung der Persönlichkeit. Pressefreiheit und der durch Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG garantierte Schutz der Persönlichkeit stehen in einem Spannungsverhältnis (BVerfGE 35, 202/219). Diesen möglichen Konflikt zwischen der Pressefreiheit und dem Schutz der Persönlichkeit der einzelnen Bürger hat die Verfassung durch Verweisung auf die allgemeine Rechtsordnung geregelt (BVerfGE 35, 202/223).

Damit können auch Datenschutzgesetze Schranken für die Presse enthalten. Allerdings darf die Pressefreiheit durch das Datenschutzrecht nicht in ihrem Kernbereich angegriffen werden, wozu insbesondere der gesamte Bereich publizistischer Vorbereitungstätigkeit, also die Beschaffung von Informationen und das Redaktionsgeheimnis, zählen.

Absatz 1:
Abgesehen von § 4 gelten sämtliche Vorschriften des Ersten Abschnitts des BDSG für die Medien statt, wie bisher vorgesehen, nur §§ 5 und 8. Damit sind anwendbar der Geltungsbereich des BDSG (§ 1), die Begriffsbestimmungen (§ 3), die Tatsache der Unabdingbarkeit der Rechte des Betroffenen (§ 6) und der Schadenersatz (§ 7).

Absatz 2:
Absatz 2 ist § 37 Abs. 2 des Entwurfs nachgebildet. Es besteht kein Anlaß, Gegendarstellungen von Betroffenen im Bereich der Presse oder des Films anders als im Rundfunkbereich zu behandeln. Der Schutz der Pressefreiheit beschränkt sich auf die wahrheitsgemäße Berichterstattung. Deshalb ist die Presse um ihrer Aufgaben bei der öffentlichen Meinungsbildung willen gehalten, Behauptungen, die sie weitergibt, auf ihren Wahrheitsgehalt zu prüfen (BVerfGE 12, 130). Eine leichtfertige Weitergabe unwahrer Nachrichten, erst recht die bewußte Entstellung der Wahrheit, auch durch das Weglassen wesentlicher Sachverhalte, wird durch Art. 5 GG nicht gedeckt.

Die Regelungen für private Rundfunkanstalten fallen in die Kompetenz der Landesgesetzgeber.

Absatz 3:
Dem Betroffenen ist über § 37 Abs. 3 des Entwurfs hinaus nicht nur gegenüber Rundfunkanstalten und nicht erst dann, wenn eine Beeinträchtigung des Persönlichkeitsrechts vorliegt, ein Auskunftsanspruch einzuräumen. Der Kernbereich der Pressefreiheit wird durch eine eigenständige Regelung zur Auskunftsverweigerung geschützt, die über § 37 Abs. 3 Satz 2 des Entwurfs hinausgeht.

Im Falle der Beeinträchtigung von Rechten Betroffener (bisher war dies eine Voraussetzung für die Auskunft) wird das Maß der erfolgten Beeinträchtigung ein wesentliches Abwägungskriterium zwischen dem Interesse des Betroffenen und der Erfüllung publizistischer Aufgaben sein. Damit eine auf Satz 2 gestützte Auskunftsverweigerung überprüft werden kann, ist ein Datenschutzbeauftragter (§§ 38 und 38 a) erforderlich, der im Streitfall Nachprüfungen vornehmen kann.

Dem Betroffenen wird ein Löschungsanspruch eingeräumt, wenn zwar die Unrichtigkeit seiner Daten feststeht, aber richtige Daten sich nicht ermitteln lassen. Absatz 3 Satz 4 ist Art. 9 Abs. 2 BayDSG nachgebildet.

Absatz 4:
Auch für die Rundfunkanstalten des Bundesrechts können die gesamten Vorschriften des Ersten Abschnitts mit Ausnahme des § 4 Anwendung finden (Absatz 4).

Absatz 5:
Die Verweisung in Absatz 5 ist erforderlich, da für den Bereich der Presse ein eigenständiger Beauftragter für den Datenschutz vorgesehen ist (vgl. § 38 a).

Begründung zu § 38 a

Wegen der für den Bürger bestehenden Undurchsichtigkeit der Speicherung und Verwendung von Daten und auch im Interesse eines vorgezogenen Rechtsschutzes ist die Tätigkeit eines unabhängigen Kontrollorgans von erheblicher Bedeutung für einen effektiven Schutz des Rechts auf informationelle Selbstbestimmung auch gegenüber der Presse. Die Einrichtung nur eines Datenschutzbeauftragten für die Rundfunkanstalten genügt nicht.

Ein solches unabhängiges Kontrollorgan könnte auch in den Fällen, in denen die Wahrung des Redaktionsgeheimnisses, der Quellenschutz oder gerade laufende Presseermittlungen eine unmittelbare Auskunft an den Bürger verbieten würden, anstelle des Bürgers und für diesen die Rechtmäßigkeit und Richtigkeit der durch die Presse vorgenommenen Verarbeitung personenbezogener Daten der Bürger überprüfen.

Vorbild für § 38 a sind die Vorschriften für den Bundesbeauftragten für den Datenschutz und für die Rundfunkdatenschutzbeauftragten bei gleichzeitig deutlicher Vereinfachung der Normen.

Absatz 1:
Zur Sicherung der notwendigen Staatsfreiheit wird der Datenschutzbeauftragte vom Presserat vorgeschlagen. Die Ernennung durch den Bundespräsidenten unterstreicht die Bedeutung dieses Amtes.

Der Datenschutzbeauftragte wird nicht in ein öffentliches Amtsverhältnis berufen, um die vom Grundgesetz geforderte Unabhängigkeit der Medien zu gewährleisten. Aus der Zulässigkeit der Wahrnehmung anderer Aufgaben innerhalb eines Medienunternehmens ergibt sich, daß in der Regel nur an eine Aufwandsentschädigung gedacht ist.

Absatz 2:
Absatz 2 verweist auf § 38 Abs. 2 Satz 2 und Abs. 3 des Entwurfs. § 38 Abs. 2 Satz 3 des Entwurfs wird aus systematischen Gründen nicht übernommen. Im Hinblick darauf, daß die Presse nicht öffentlich-rechtlich strukturiert ist, bestehen hiergegen auch keine verfassungsrechtlichen Bedenken.

Absatz 3:
Absatz 3 hat § 38 Abs. 4 des Entwurfs zum Vorbild.

Absatz 4:
Absatz 4 ist § 22 des Entwurfs nachgebildet.

Absatz 5:
Die entsprechende Geltung von § 21 Abs. 4 dieses Gesetzes und von § 53 Abs. 1 Nr. 5 StPO soll sicherstellen, daß der Beauftragte für den Datenschutz berechtigt ist, das Zeugnis zu verweigern, unabhängig davon, ob ihm in seiner Eigenschaft „Tatsachen anvertraut" worden sind oder ob er in sonstiger Weise, etwa bei Prüfungen im Medienbereich, Kenntnisse erlangt hat.

Die gegenüber der Aufsichtsbehörde geltende Auskunftspflicht (§ 34 Abs. 3) und das Betretungsrecht (§ 34 Abs. 4) gelten auch für den Medienbeauftragten.

Inwieweit ein Bedürfnis für einen Datenschutzbeauftragten im Filmbereich besteht, müßte noch geprüft werden.