Bayerischer Landtag
12. Wahlperiode

Drucksache **12/223**
13. 12. 90

Zwölfter Tätigkeitsbericht des Landesbeauftragten für den Datenschutz

Berichtszeitraum 1990

Der Landesbeauftragte für den Datenschutz
Nr. DSB/1 – 510 – 13

München, 13. Dezember 1990

An den
Herrn Präsidenten
des Bayerischen Landtags
München

Zwölfter 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 zwölften Bericht über die Tätigkeit des Landesbeauftragten für den Datenschutz.

Mit vorzüglicher Hochachtung

Sebastian Oberhauser

Inhaltsübersicht

1. Vorbemerkungen

1.1 Kontrolltätigkeit

Trotz intensiver Beschäftigung mit mehreren Gesetzesvorhaben lag auch im Berichtszeitraum 1990 der Schwerpunkt meiner Tätigkeit bei der Kontrolle bayerischer Behörden. Allgemeine Kontrollen habe ich durchgeführt: bei zwei Krankenhäusern, acht Betriebskrankenkassen, der Bayer. Versicherungskammer, einem Landwirtschaftsamt, einem Landratsamt, einer Regierung, fünf Kommunen, Stadtwerken, einer Staatsanwaltschaft, acht Polizeidirektionen, beim Grenzpolizeipräsidium, beim Landeskriminalamt und beim Landesamt für Verfassungsschutz.

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

Hinzu kommen technisch-organisatorische Kontrollen bei 17 Rechenzentren und Betreibern kleinerer Datenverarbeitungsanlagen.

1.2 Datenschutz in Bayern gewährleistet

Meine Kontrollen und die zahlreichen weiteren Kontakte mit den Behörden haben mir bestätigt, daß der Datenschutz in Bayern **grundsätzlich gewährleistet** ist. Soweit Mängel und Fehler festzustellen waren, waren die Behörden einsichtig und ohne lange Diskussionen zur Korrektur bereit. Auch das ist ein Zeichen für die Aufgeschlossenheit gegenüber dem Datenschutz.

1.3 Inhalt und Schwerpunkte des 12. Tätigkeitsberichts

Dieser Bericht kann wiederum nur eine **Auswahl** aus meiner Tätigkeit im Berichtszeitraum enthalten. Den Schwerpunkt bilden die Ergebnisse der durchgeführten **Datenschutzkontrollen**. Auf Anfragen von Behörden und Bürgern hatte ich wieder zahlreiche **Zweifelsfragen** über die Reichweite datenschutzrechtlicher Vorschriften zu klären. Zu einer Reihe von **Gesetzgebungsvorhaben** habe ich Stellungnahmen abgegeben und notwendige Datenschutzregelungen gefordert.

- Im Vordergrund der allgemeinen Datenschutzkontrollen stand die Datenverarbeitung im **Sicherheitsbereich**. Beim Landeskriminalamt habe ich wieder die Datei **APIS** (Arbeitsdatei innere Sicherheit) anhand von Stichproben überprüft. Bei den kontrollierten Polizeidirektionen galt mein besonderes Interesse neben dem **Kriminalaktennachweis** dem polizeilichen **Staatsschutz**. Beim Landesamt für Verfassungsschutz wurden wieder das **nachrichtendienstliche Informationssystem** (NADIS) und ausgewählte Dateien überprüft.

- Im **Gesundheitsbereich** wurde ich bei **Forschungsvorhaben** wie etwa zur Gewinnung von Aussagen über die Verbreitung und Entwicklung von Aids zur Prüfung der Anonymität von Testverfahren eingeschaltet. In die allgemeine Datenschutzkontrolle habe ich nunmehr auch die **Krankenhäuser** einbezogen. Dabei wurden nur wenige Mängel festgestellt.

- Von den **Sozialbehörden** habe ich mehrere **Betriebskrankenkassen** geprüft und als Ergebnis eine stärkere Abschottung zwischen Krankenkasse und Arbeitgeber gefordert. Außerdem waren wieder zahlreiche Einzelfragen über die **Reichweite des Sozialdatenschutzes** zu klären. Fest steht, daß bei Verdacht auf Kindsmißhandlungen durch die Eltern jedenfalls der Datenschutz der notwendigen Information der Jugendschutzbehörden nicht im Weg steht.

- Die Überprüfung der **Einwohnermeldeämter** habe ich durch allgemeine Kontrollen fortgesetzt. Überprüft wurden Städte und Gemeinden mit bisher noch nicht kontrollierten DV-Verfahren. Wie in früheren Jahren wiesen auch die im Berichtszeitraum kontrollierten Verfahren typische Fehler auf, in denen der vom Gesetzgeber minutiös geregelte Interessenausgleich nicht genau beachtet wurde.

- Im **Steuerbereich** hat das neue Bundesdatenschutzgesetz eine wesentliche Verbesserung des Datenschutzes gebracht. Nach seinem Inkrafttreten kann das Finanzamt dem Datenschutzbeauftragten das **Steuergeheimnis** nicht mehr entgegenhalten. Damit werden effektive Kontrollen in der bisher „verschonten" Steuerverwaltung möglich.

- Zunehmend treten Datenschutzfragen beim **Umweltschutz** auf. So war zu klären, ob eine Stadt einen **Altlastenkataster** und eine Karte mit Eintragungen aufgefüllter Kiesgruben veröffentlichen oder Einsicht in diese Unterlagen gewähren darf. Wegen der widerstreitenden Interessen der Eigentümer und der Betroffenen sowie wegen des allgemeinen Interesses an umfassenden Informationen über bestehende Umweltbelastungen und -risiken erscheint mir eine **bereichsspezifische Regelung** notwendig, wenn die allgemeinen Bestimmungen des Bayer. Datenschutzgesetzes keine angemessenen Konfliktlösungen bieten sollten.

- **Zeitgeschichtliche Forschung** und Datenschutz bleiben Spannungsgebiet. Das zeigte sich, als nach der letzten Kommunalwahl Forschungsergebnisse aus der Einsicht in NS-Akten veröffentlicht und über die Presse einem Bürgermeister mit inzwischen mehr als 60 Lebensjahren vorgehalten wurde, er habe vor fast 50 Jahren als damals knapp 14jähriger Hitlerjunge eine Frau bei der Gestapo denunziert. Dürfen Forscher der Zeitgeschichte Forschungsergebnisse, zu denen sie durch Einsichtnahme in staatlich verwahrte Unterlagen gekommen sind, zu dem Zweck verwenden, einem Mann von mehr als 60 Jahren seine **Sünden aus der Kindheit** vorzuhalten? Hier müssen **Zugang** zu archivierten Dokumenten der Zeitgeschichte und **Nutzung** der Forschungsergebnisse weit stärker, als das Beispiel zeigt, den Schutz der Persönlichkeit berücksichtigen.

- Beim Verfahren zur Aufstellung der **Denkmalliste** konnte Der Datenschutzbeauftragte erreichen, daß bei der Aufnahme beweglicher Gegenstände der Datenschutz gewährleistet ist. Da in die Denkmalliste jedermann — und damit leider auch Diebe — Einsicht nehmen können, darf ein Gegenstand wegen der damit verbundenen Gefährdung nur mit Zustimmung des Eigentümers in die Liste aufgenommen werden.

- Aus Gründen der **Datensicherheit** ist die Verwendung von privater Hard- und Software grundsätzlich zu untersagen. Auch in Arbeitsplatzcomputer bayerischer Behörden sind bereits Computerviren eingedrungen, weil die gebotenen Schutzvorkehrungen nicht beachtet wurden.

- Ein Fernsehbericht gab Anlaß, die datenschutzgerechte **Entsorgung von Datenträgern** zu kontrollieren. Manche Behörden gehen bei der Entsorgung von Altpapier und sonstigen Unterlagen mit personenbezogenen Daten nicht mit der gebotenen Sorgfalt und Umsicht vor. Häufig wird Altpapier sorglos in den Papierkorb geworfen und landet schließlich in der Mülltonne und auf der Deponie, wo es von Müllschnüfflern aufgestöbert werden kann. Diese gedankenlose Altpapierentsorgung entspricht **weder dem Datenschutz noch dem Umweltschutz**. Der Datenschutzbeauftragte hat deshalb die gesamte Verwaltung gebeten, für eine datenschutzgerechte Entsorgung von Altpapier einschließlich der ausgesonderten Akten Sorge zu tragen.

1.4 Fortschritte in der Gesetzgebung

Im Jahr vor der Landtagswahl hat der Bayerische Landtag einige wichtige **bereichsspezifische Datenschutzgesetze** beschlossen. Mit der Novellierung des **Polizeiaufgabengesetzes** wurde die Erhebung, Nutzung und Verwendung von personenbezogenen Daten durch die Polizei für die Aufgabe der Gefahrenabwehr und für sonstige nichtrepressive polizeiliche Aufgaben ausführlich und normenklar geregelt. Auch der Verfassungsschutz hat mit dem neuen **Bayerischen Verfassungsschutzgesetz** eine rechtsstaatlich einwandfreie Grundlage für die Informationsbeschaffung und -verarbeitung erhalten. In beiden Gesetzen wurden den Bürgern nach den jeweiligen Notwendigkeiten abgestufte **Auskunftsrechte** eingeräumt, ergänzt durch die Verpflichtung, bei einer Auskunftsverweigerung die Bürger an den Datenschutzbeauftragten zu verweisen. Das **Bayerische Statistikgesetz** sichert die Geheimhaltung der bei bayerischen Statistiken erhobenen Daten.

Auf Bundesebene konnten endlich das neue **Bundesdatenschutzgesetz**, das **Bundesverfassungsschutzgesetz**, das **BND-Gesetz** und das **MAD-Gesetz** verabschiedet werden. **Defizite** in der Bundesgesetzgebung zeigen sich allerdings vor allem im Justizbereich, wo kaum eines der angekündigten Gesetzesvorhaben mit datenschutzrechtlichem Schwerpunkt zum Abschluß gebracht werden konnte.

1.5 Datenschutz im vereinten Deutschland

Das **Einigungsvertragsgesetz** hat auch den Datenschutz in den neuen Bundesländern auf eine tragfähige Grundlage gestellt. Noch vor dem Beitritt der DDR hatte die Volkskammer ein am westdeutschen Niveau ausgerichtetes **Polizeigesetz** erlassen und somit die Voraussetzungen für den Datenaustausch zwischen den Polizeibehörden der alten und neuen Bundesländer geschaffen.

Eine wichtige Aufgabe der neuen Länder wird es sein, alsbald **eigene Datenschutzgesetze** zu erlassen und unabhängige **Datenschutzbeauftragte** einzurichten, um das Vertrauen der Bürger in die neue staatliche Ordnung zu stärken. Selbstverständlich bin ich im Rahmen meiner Möglichkeiten zur Hilfe bereit.

Der Beitritt der DDR zur Bundesrepublik muß auch Anlaß sein, die bisher als Folge der deutsch-deutschen Konfrontation gesammelten **Informationen beim polizeilichen Staatsschutz** und beim **Verfassungsschutz zu überprüfen**. Allerdings wird man auch weiterhin die zeitlos formulierten Aufgaben des polizeilichen Staatsschutzes und des Verfassungsschutzes im Auge behalten müssen, zumal es genug Anzeichen gibt, daß die Stasi-Organisation noch nicht zerschlagen ist.

1.6 Geschäftsstelle

Die Zunahme bereichsspezifischer detaillierter Regelungen des Datenschutzes und die notwendige Kontrolle der Einhaltung dieser Bestimmungen machen angesichts der Bedeutung unabhängiger Datenschutzbeauftragter für die Gewährleistung der Persönlichkeitsrechte der Bürger die angemessene Ausweitung meiner Geschäftsstelle unumgänglich. Künftig soll sich ein Referat ausschließlich mit der Kontrolle von Polizei und Verfassungsschutz befassen.

1.7 Ausblick

Nach der Verabschiedung des Bundesdatenschutzgesetzes ist nunmehr die Staatsregierung aufgefordert, ein **modernes Bayerisches Datenschutzgesetz** vorzulegen, das den Fortschritt im Datenschutz, die Rechtsprechung insbesondere der Verfassungsgerichte und die Erfahrungen der Praxis berücksichtigt. Im Jahr 1991 werde ich mein besonderes Augenmerk auf den **Sicherheitsbereich** richten. Die Richtlinien und Errichtungsanordnungen müssen an die neue Rechtslage angepaßt werden. Vor allem aber gilt es, die Einhaltung der neuen Gesetze durch Polizei und Verfassungsschutz zu kontrollieren.

2. Gesundheitswesen

2.1 Anonymer unverknüpfbarer HIV-Test (AUT)

Im Auftrag des Bayerischen Staatsministerium des Innern entwarf das MEDIS-Institut der Gesellschaft für Strahlen- und Umweltforschung (GSF) einen Studienplan für einen anonymen unverknüpfbaren HIV-Test (AUT). Mit dem AUT sollen Aussagen über die **Verbreitung und Entwicklung der HIV-Infektion** gewonnen werden. Es ist beabsichtigt, in ausgesuchten Krankenhäusern Restblut, das für diagnostische Zwecke nicht mehr benötigt wird, zu anonymisieren und im MEDIS-Institut auf HIV-Antikörper zu untersuchen. Eine Rückmeldung des Untersuchungsergebnisses der einzelnen Patienten an das Krankenhaus ist ausgeschlossen.

Den Studienplan zu AUT habe ich darauf überprüft, ob nach dem Verfahren die vom Innenministerium von vornherein geforderte **irreversible Anonymisierung** der Blutproben und die **Unverknüpfbarkeit des Testergebnisses** mit bestimmten Patienten sichergestellt sind. Gegen das Konzept haben sich keine Bedenken ergeben.

Die Gewinnung der nicht personenbezogenen Auswertungsdaten aus den in den Kliniklabors zunächst in personenbezogener Form vorliegenden Patientendaten ist nach Art. 26 Abs. 4 Satz 1 des Bayerischen Krankenhausgesetzes zulässig. Nach dieser Vorschrift dürfen Krankenhausärzte Patientendaten nutzen, soweit dies zu Forschungszwekken im Krankenhaus oder im Forschungsinteresse des Krankenhauses erforderlich ist. Das Projekt liegt auch im Forschungsinteresse des Krankenhauses, da die Ergebnisse dem Krankenhaus zur Feststellung der tatsächlichen Zahl der HIV-infizierten Patienten dienen.

Die für die Auswertung beim MEDIS Institut erforderlichen Daten geben nach der vorgelegten Konzeption dem MEDIS Institut **keine Möglichkeit zum Rückschluß** auf bestimmte

Patienten. Bei den Auswertungsdaten handelt es sich um Alterklasse, Geschlecht, Klinikbereich, ambulant/stationär, sowie die Angabe, ob der Patient aus dem näheren Einzugsbereich der Klinik kommt. Diese Daten werden, zusammen mit einer laufenden Nummer, die das Kliniklabor speziell für diesen Zweck vergibt, noch **in der Klinik** derart **verschlüsselt**, daß ein Rückgriff auf diese Daten und ihre Zuordnung zu bestimmten Patienten in der Klinik nicht mehr möglich ist. Das MEDIS-Institut erhält die verschlüsselten Daten von der Klinik erst, wenn jeweils mehrere Proben mit identischen Auswertungsdaten angesammelt wurden. Die genaue Zahl der Proben mit identischen Daten wird noch festgelegt. Auf diese Weise könnte auch eine — vereinbarungswidrige — Rückmeldung von Untersuchungsergebnissen an die Klinik dort nicht mehr bestimmten Patienten zugeordnet werden.

2.2 Bundeskrebsregister

Der Bundesminister für Jugend, Familie, Frauen und Gesundheit legte Thesen zu einem **Bundeskrebsregistergesetz** vor. Danach soll ein bundeseinheitliches Krebsregister geschaffen werden. Es soll möglichst alle Krebserkrankungen flächendeckend erfassen. Für die Ärzte ist keine Meldepflicht, sondern nur eine gesetzliche **Meldeberechtigung** vorgesehen. Die Krebspatienten sollen mit **vollem Namen** gemeldet werden. Die Befugnis zur Offenbarung soll sich im Regelfall aus der Einwilligung des Patienten ergeben. **Im Ausnahmefall soll jedoch auf die gesetzliche Meldeberechtigung zurückgegriffen werden.** Darüber hinaus sehen die Thesen auch eine **namentliche Weitergabe zu Forschungszwecken** und einen namentlichen **Abgleich** mit den gemeindlichen Melderegistern ohne Einwilligung des Krebspatienten vor.

Ich habe zu diesen Thesen die Auffassung vertreten, daß es bis heute an einem überzeugenden Nachweis dafür fehlt, daß ein so gravierender Eingriff wie die **namentliche Meldung Krebskranker an zentrale epidemiologische Register ohne Einwilligung** der Betroffenen zur Erreichung der Forschungs- und Therapieziele erforderlich ist. In mehreren Ländern, auch in Bayern, sind Krebsregistrierungsmodelle vorhanden bzw. im Aufbau, bei denen eine Meldung auf anonymer Basis erfolgt.

Die Datenschutzbeauftragten des Bundes und der Länder haben die Einrichtung eines Krebsregisters auf der Grundlage des Melderechtsmodells (also ohne Einwilligung des Patienten) abgelehnt.

2.3 Prüfung von Krankenhäusern

Im Berichtszeitraum habe ich, wie angekündigt, erstmals bei zwei Krankenhäusern eine datenschutzrechtliche Kontrolle durchgeführt. Überprüft wurden **Dateien** und **Karteien** sowie im Hinblick auf Art. 26 Abs. 4 und 5 BayKrG ausgewählte **Aktenunterlagen der Krankenhausverwaltung**. Nicht kontrolliert wurden Datenspeicherungen und -übermittlungen im medizinischen Bereich in und aus den Krankengeschichten. Bei den Kontrollen wurden **nur wenige Mängel** festgestellt. Sie betrafen im wesentlichen die Bereiche Patientenverwaltung und Archiv.

In folgenden Punkten bat ich um Änderung der bisherigen Verfahrensweisen:

- **Angaben zum Familienstand**
  Bei der Aufnahme eines Patienten werden auch Daten über seinen Familienstand erhoben. Dabei hat der Patient anzugeben, ob er **„ledig, verheiratet, geschieden, getrennt lebend oder verwitwet"** ist. Die Angaben sollten auf „verheiratet/nicht verheiratet" beschränkt werden, weil eine weitere Aufschlüsselung des Standes „nicht verheiratet" für Zwecke der Krankenhausverwaltung nicht erforderlich ist.

- **Religionszugehörigkeit**
  Verbesserungsbedürftig war auch die Datenerhebung über die Religionszugehörigkeit. Zwar wird der Patient schriftlich darauf hingewiesen, daß die Angabe der Religionszugehörigkeit freiwillig ist. Hingegen wird er nicht darüber informiert, daß bei Angabe der Religionszugehörigkeit **Pfarrern** und **kirchlichen Besuchsdiensten** anhand der Pfarrerlisten Name, Zimmernummer und Privatanschrift des Patienten mitgeteilt werden. Bei weitem nicht jedem Patienten, der seine Religion angibt, ist ein solcher Besuch erwünscht. Vor der Weitergabe dieser Daten an Pfarrer und kirchliche Besuchsdienste sollte das Einverständnis des Patienten eingeholt werden.

- **Pförtnerliste**
  Der Patient sollte auch vorher gefragt werden, ob der Pforte seine Aufnahme in das Krankenhaus zur Auskunft an Besucher mitgeteilt werden sollte. Entsprechende Einwilligungserklärungen sollten in den Krankenhausaufnahmeantrag aufgenommen werden.

- **Telefongesprächsdaten**
  Patienten und Bedienstete des Krankenhauses sollten darauf hingewiesen werden, welche Daten über Telefongespräche gespeichert und ausgedruckt werden. Bei privaten Telefongesprächen Bediensteter sollten die Zielnummern nur bei Meinungsverschiedenheiten über die Abrechnung ausgedruckt werden.

- **Datenübermittlung an Krankenkassen**
  Die Mitteilung des Krankenhauses an die Krankenkasse über die Aufnahme eines Patienten sollte keine Daten über Konfession des Patienten und Angehörige enthalten, weil sie zur Kostenabwicklung nicht erforderlich sind.

- **Polizeiliste**
  Für die Polizei sollten nur die nach dem Meldegesetz vorgeschriebenen Angaben (sog. Polizeiliste), nicht jedoch Daten über Angehörige vorgehalten werden.

- **Archiv**
  Bei hausinternen Anforderungen von Krankenblättern und Röntgenbildern ergab sich aus den Akten im nachhinein nicht, an wen und wann die Unterlagen übermittelt wurden. Folglich läßt sich nicht mehr feststellen, ob die Einsichtnahmen erforderlich und die Einsichtnehmenden befugt waren. Ich habe deshalb gefordert, für die Führung des **Krankenblattarchivs** ein Verfahren einzuführen, das jederzeit dokumentiert, welchen Stellen und Mitarbeitern des Krankenhauses zu welcher Zeit Patientenunterlagen zur Einsicht überlassen worden sind. Dies sollte auch bei Entnahmen an Wochenenden gelten.

3. Sozialbehörden

In der Gesetzgebung habe ich am Zustandekommen des **Kinder- und Jugendhilfegesetzes** mitgewirkt. Geprüft wurden die **Betriebskrankenkassen**. Auf Bitte des Landesverbandes der Betriebskrankenkassen hat ein Mitarbeiter meiner Geschäftsstelle mehrere **Fortbildungskurse** über Datenschutz bei Krankenkassen durchgeführt.

Zahlreiche Sozialbehörden und betroffene Bürger wandten sich wieder zur Klärung von Zweifelsfragen bei der Auslegung von Datenschutzvorschriften im Sozialrecht an meine Geschäftsstelle. Betroffene Bürger beklagten sich über Verletzungen des **Sozialgeheimnisses**. Die Anzahl der begründeten Beschwerden zeigt, daß manche Behörden bei der Beschaffung von Informationen über Bürger, beispielsweise über unterhaltspflichtige Kindsväter, nicht gerade zimperlich umgehen, über die Köpfe der Betroffenen hinweg Informationen beschaffen oder den Betroffenen einen Katalog von Fragen vorsetzen, zu deren Beantwortung sie nicht verpflichtet sind.

3.1 Kinder- und Jugendhilfegesetz (KJHG)

Der Entwurf eines Kinder- und Jugendhilfegesetzes hat mich mehrmals beschäftigt. Das Gesetz tritt zum 1. Januar 1991 in Kraft. Meine Vorstellungen zum Schutz personenbezogener Daten und zur **Trennung von Beratung und Eingriffsverwaltung** im Bereich der Jugendhilfe wurden im KJHG weitgehend berücksichtigt.

3.2 Prüfung bei Betriebskrankenkassen

Im Berichtsjahr habe ich acht Betriebskrankenkassen darauf überprüft, ob die gesetzlich vorgeschriebene **Abschottung** gegenüber dem Arbeitgeber eingehalten ist, die verhindern soll, daß dieser von der Krankenkasse Krankheitsdaten seiner Arbeitnehmer erfährt. Krankheitsdaten, die der Arbeitnehmer der Betriebskrankenkasse anvertrauen muß, sind allein für die Krankenkasse, keinesfalls für den Arbeitgeber bestimmt. Meine Feststellungen habe ich auch dem Landesverband der Betriebskrankenkassen mitgeteilt, der daraufhin durch Rundschreiben erneut alle angeschlossenen Kassen auf die gesetzlich vorgeschriebene Abschottung hinwies.

Im einzelnen waren folgende Feststellungen zu treffen:

3.2.1 Personalchef in Vorstand, Vertreterversammlung und Widerspruchsstelle

Ein Mitglied eines Selbstverwaltungsorgans darf bei der Beratung und Abstimmung **nicht anwesend** sein,

- wenn hierbei personenbezogene Daten eines Arbeitnehmers offengelegt werden, der ihm im Rahmen eines Dienst- oder Arbeitsverhältnisses untergeordnet ist, oder
- wenn das Mitglied des Selbstverwaltungsorgans Angehöriger der Personalverwaltung des Betriebes ist, dem der Arbeitnehmer angehört.

Das bestimmt § 63 Abs. 3 a SGB IV, der am 1. Januar 1989 in Kraft getreten ist. Die Regelung soll verhindern, daß Informationen über einen Arbeitnehmer aus der Betriebskrankenkasse an die für Personalentscheidungen zuständige Stelle des Arbeitgebers gelangen.

Bei sechs der acht im Berichtsjahr geprüften Betriebskrankenkassen habe ich festgestellt, daß entweder der Personalchef, sein Stellvertreter oder ein anderer leitender Angestellter mit Personalverantwortung als Arbeitgebervertreter in den **Vorstand** und die **Vertreterversammlung** der Betriebskrankenkasse entsandt waren. Da Vorstand und Vertreterversammlung in den geprüften Betriebskrankenkassen jedoch keinen Zugang zu Einzelfällen bei der Mitgliederführung oder Leistungsgewährung haben, war diese Besetzung nicht zu beanstanden.

Die genannten Arbeitgebervertreter waren allerdings auch als Mitglieder der **Widerspruchsstelle** benannt worden. Bei der Beratung und Entscheidung über einen Widerspruch gegen Entscheidungen der Betriebskrankenkasse erhalten sie auch Kenntnis von Einzelfällen. Dabei können Fragen über den Gesundheitszustand, die Arbeitsfähigkeit sowie die Familien- und Einkommensverhältnisse eine Rolle spielen.
Zwar waren bei den Widerspruchsfällen der letzten Jahre keine Beanstandungen auszusprechen, da sie entweder vor Inkrafttreten der Neuregelung abgewickelt oder schutzwürdige Belange der Betroffenen nicht erörtert worden waren. Eine **Neubesetzung der Widerspruchsstellen** unter Beachtung des § 63 Abs. 3a SGB IV halte ich dennoch für dringend erforderlich, damit das **Abschottungsgebot** sicher eingehalten wird.
Alle von mir geprüften Betriebskrankenkassen haben mittlerweile die Besetzung der Widerspruchsstellen in einer Weise geändert, daß der beschriebene Konflikt nicht mehr auftreten kann.

3.2.2 Personalkrankenkasse

Versicherungs- und Leistungsdaten der **Beschäftigten einer Krankenkasse** einschließlich der Daten ihrer mitversicherten Angehörigen dürfen nach § 284 Abs. 4 SGB V denjenigen Personen, die kasseninterne Personalentscheidungen treffen oder daran mitwirken können, weder zugänglich sein noch von Zugriffsberechtigten offenbart werden.
Diese Vorschrift war bei keiner der geprüften Betriebskrankenkassen eingehalten. Im Regelfall genehmigten die Geschäftsführer die Kassenleistungen für ihre Mitarbeiter.

Die genannte Regelung, die am 1. Januar 1989 in Kraft getreten ist, ist allerdings nicht nur bei Betriebskrankenkassen, sondern auch bei anderen kleinen Krankenkassen kaum vollziehbar, da die notwendige Voraussetzung hierfür, nämlich eine sinnvolle organisatorische Trennung der Zuständigkeiten, in kleinen Kassen nicht geschaffen werden kann. Um dem Sinn der Schutzvorschrift gerecht zu werden, empfiehlt es sich, die Führung der „Personalkrankenkasse" einem **Mitarbeiter unterhalb der Abteilungsleiterebene** zu übertragen, der das Vertrauen seiner Kollegen genießt.

Besteht die Krankenkasse jedoch nur aus sehr wenigen Mitarbeitern (eine der geprüften Betriebskrankenkassen hatte nur zwei Mitarbeiter), so muß eine andere Lösung gefunden werden. Zu denken wäre an eine **Auftragsvergabe an eine andere Krankenkasse** nach § 88 SGB X. Nach dieser Bestimmung kann eine Krankenkasse ihr obliegende Aufgaben durch eine andere Krankenkasse wahrnehmen lassen, wenn dies wegen des sachlichen Zusammenhangs, zur Durchführung der Aufgaben und im wohlverstandenen Interesse der Betroffenen zweckmäßig ist. Den betroffenen Mitarbeitern und ihren mitversicherten Angehörigen sollte jedoch die **Wahl** gelassen werden, ob sie bei der Abwicklung ihrer Leistungen eine andere Kasse beanspruchen wollen oder, nicht

zuletzt wegen der räumlichen und sachlichen Nähe, eine Abwicklung durch ihre eigene Betriebskrankenkasse wünschen.
Ich habe die geprüften Betriebskrankenkassen aufgefordert, die genannten organisatorischen Probleme umgehend in Absprache mit dem Landesverband der Betriebskrankenkassen und den Aufsichtsbehörden zu lösen. Die von mir geprüften Betriebskrankenkassen sind meiner Aufforderung gefolgt.

3.3 Datenverbund einer Landesversicherungsanstalt mit italienischen Sozialversicherungsträgern

Das Rentenreformgesetz 1992 erlaubt in § 148 Abs. 3 SGB VI auch den **Direktabruf** von Rentendaten bei deutschen Rentenversicherungsträgern **durch ausländische Rentenversicherungsträger**.

Inzwischen ist in meinem Zuständigkeitsbereich ein solcher Datenverbund eingerichtet worden. Es handelt sich um ein Direktzugriffsverfahren, mit dem der italienische Sozialversicherungsträger INPS und mehrere seiner Regionalstellen direkt auf **Rentendaten italienischer Staatsangehöriger**, die in der Bundesrepublik Rentenansprüche erworben haben, bei der dafür zuständigen deutschen Landesversicherungsanstalt zugreifen können. Als Grundlage dient ein Vertrag zwischen den beteiligten Stellen, der nähere Regelungen zum Verfahren, auch unter datenschutzrechtlichen Gesichtspunkten, enthält.

Die Landesversicherungsanstalt hat meine Vorschläge weitgehend berücksichtigt. Durch Einschränkung der **Zugriffsberechtigung**, des abzufragenden **Personenkreises** und der bereitzustellenden **Datenfelder** ist eine Regelung gefunden worden, welche die schutzwürdigen Belange der von der Online-Verbindung betroffenen Italiener ausreichend berücksichtigt.
Dabei waren auch Schwierigkeiten zu überwinden, die sich aus der kostengünstigeren Benutzung eines privaten Netzes ergeben.

- Sieht man in der Übermittlung eine **Datenfernübertragung über Vermittlungsstellen**, so ist deren Zulässigkeit nach § 81 Abs. 2 SGB X zu beurteilen. Die Übermittlung personenbezogener Daten durch einen Sozialleistungsträger im Wege der Datenfernübertragung über Vermittlungsstellen ist danach zulässig, wenn auf diese der 2. Abschnitt des Bundesdatenschutzgesetzes anzuwenden ist, d.h. wenn es sich um **öffentliche Stellen** handelt. Diese Voraussetzung ist für die Weiterleitung der Daten auf dem Privatnetz nicht gegeben. Anscheinend ist der Gesetzgeber davon ausgegangen, daß die Übertragung über öffentliche Stellen sicherer ist.

- Nach einer anderen Rechtsauffassung sind auf die vorliegenden Verhältnisse die Bestimmungen für die **Datenverarbeitung im Auftrag** nach § 80 SGB X anzuwenden. Dann müßten die Voraussetzungen für eine Vermittlungsstelle nach § 81 SGB X nicht erfüllt sein. Folgt man dieser Auffassung, so setzt eine Auftragserteilung nach § 80 Abs. 2 SGB X voraus, daß sich der Auftragnehmer, ein privater Netzbetreiber, schriftlich damit einverstanden erklärt hat, daß der Auftraggeber jederzeit berechtigt ist, **mit aufsichtsrechtlichen Mitteln** die Einhaltung der Vorschriften über den Datenschutz **zu überwachen**. Dies ist zumindest außerhalb der Bundesrepublik nicht mehr durchsetzbar.

Als Ausweg habe ich eine **Verschlüsselung** der Daten auf dem Leitungsnetz vorgeschlagen. Dadurch kann trotz der technisch jederzeit möglichen Aufzeichnung der Daten in den Knotenstellen des Leitungsnetzes ein Mißbrauch durch Unbefugte verhindert werden. Bei allen Sicherungsmaßnahmen ist allerdings zu berücksichtigen, daß es sich um nicht besonders sensible Daten von ehemaligen italienischen Gastarbeitern handelt, welche Dritte wenig interessieren dürften.

3.4 Hinweis der Krankenkasse an Arbeitgeber bei Schadensersatzanspruch

Ein Personalamt machte mich auf folgendes datenschutzrechtliche Problem aufmerksam:
Erleidet ein Arbeitnehmer einen Körperschaden durch Verschulden eines Dritten und wird dadurch arbeitsunfähig krank, so kann der Arbeitgeber das während der Ausfallzeit gezahlte Arbeitsentgelt von dem Dritten als Schadensersatz fordern. Den Arbeitnehmer trifft gegenüber dem Arbeitgeber eine **Meldepflicht** über Schadensereignisse, die einen Schadensersatzanspruch des Arbeitgebers auslösen (§ 4 Abs. 2 Lohnfortzahlungsgesetz). Diese Meldepflicht ist freilich manchen Arbeitnehmern nicht bekannt.

Verschiedene **Krankenkassen** sind dazu übergegangen, **den Arbeitgeber auf das Vorliegen eines Drittverschuldens** hinzuweisen. Sie erfahren es aus dem Fragebogen, den der Versicherte auszufüllen hat, oder entnehmen Hinweise auf einen Unfall — anders als der Arbeitgeber — der in der Arbeitsunfähigkeitsbescheinigung festgehaltenen Krankheitsdiagnose.

Besondere Bedeutung hat das genannte Problem im Bereich der Betriebskrankenkassen. Bei Prüfungen habe ich festgestellt, daß Vereinbarungen, die zum Teil **nur mündlich** abgeschlossen wurden, mit dem Arbeitgeber bestehen, wonach die Krankenkassen Schadensersatzansprüche der Arbeitgeber nach § 4 Lohnfortzahlungsgesetz bei den Haftpflichtversicherern der Schädiger geltend machen, einziehen und an den Arbeitgeber abführen. Der Bundesverband der Betriebskrankenkassen hat für seine Mitglieder und für die Arbeitgeber sogar Teilungsabkommen mit verschiedenen Haftpflichtversicherungen geschlossen.

Mit dem Staatsministerium für Arbeit und Sozialordnung habe ich gegen die genannte Verfahrensweise der Krankenkassen erhebliche datenschutzrechtliche Bedenken: Hilfe zur Verwirklichung zivilrechtlicher Schadensersatzansprüche des Arbeitgebers ist keine soziale Aufgabe der Krankenkasse. Daher fehlt es an einer Offenbarungsbefugnis nach § 69 SGB X. Auch eine konkludente Einwilligung des Arbeitnehmers kann nicht unterstellt werden. Besondere Umstände, weshalb von der grundsätzlich erforderlichen Schriftform für die Einwilligung des Arbeitnehmers in die Unterrichtung des Arbeitgebers über das Vorliegen eines Drittverschuldens abgesehen werden könnte, sind nicht ersichtlich. Vielmehr ist von der Nichteinwilligung auszugehen, wenn man bedenkt, daß durch die Mitteilung der Krankenkasse dem Arbeitgeber auch für den Arbeitnehmer nachteilige Ereignisse bekannt werden können (z.B. Beteiligung an einer Schlägerei oder an einem Verkehrsunfall in angetrunkenem Zustand). Zudem wird wohl jeder Arbeitnehmer erwarten, daß eine Krankenkasse, die auf eine Meldepflicht ihres Versicherten hinweisen möchte, ohne daß dies ihre Aufgabe wäre, diesen Hinweis ihm selbst, nicht aber dem Ar-

beitgeber gibt. Wegen **fehlender originärer Aufgaben** der Krankenkasse und **fehlender Zustimmung** der Arbeitnehmer ist der Hinweis auf das Vorliegen eines Drittverschuldens daher unzulässig.

Ich habe die Landesverbände der Krankenkassen über diese Rechtsauffassung in Kenntnis gesetzt und gebeten, die Mitgliedskassen entsprechend zu informieren. Eine Antwort der Verbände steht derzeit noch aus.

3.5 Krankenhausentlassungsberichte für Krankenkasse

Immer wieder treten Krankenhäuser mit der Frage an mich heran, ob sie nach dem Gesundheitsreformgesetz verpflichtet sind, Entlassungsberichte über Krankenhauspatienten an deren gesetzliche Krankenkasse zu übersenden. Die Krankenkassen fordern solche Unterlagen zur Klärung ihrer Kostenübernahmepflicht. Ich vertrete dazu folgende Rechtsauffassung:

Bayerische Krankenhäuser haben bei der Weitergabe von Patientendaten an Krankenkassen Art. 26 Abs. 5 des Bayerischen Krankenhausgesetzes (BayKrG) zu beachten. Danach darf das Krankenhaus Patientendaten weitergeben, wenn eine Rechtsvorschrift die Übermittlung erlaubt.

- Keine Rechtsgrundlage ist § 301 SGB V. Danach sind die Krankenhäuser befugt und verpflichtet, den Krankenkassen bei Krankenhausbehandlung genau bezeichnete Angaben, darunter die **Aufnahmediagnose** und die **Entlassungsdiagnose**, zu übermitteln. Der übrige, weit umfangreichere Inhalt eines Krankenhausentlassungsberichtes, welcher der Weiterbehandlung des Patienten durch den nachbehandelnden niedergelassenen Arzt dienen soll, ist in der Aufzählung **nicht** enthalten.

- Auch § 39 SGB V erlaubt die Übersendung des Krankenhausentlassungsberichts nicht. Nach § 39 SGB V wird Krankenhausbehandlung zeitlich unbegrenzt gewährt, wenn die Aufnahme in ein Krankenhaus erforderlich ist, weil das Behandlungsziel nicht durch ambulante Behandlung erreicht werden kann. In diesem Zusammenhang muß der gesetzlichen Krankenkasse als Kostenträger das Recht zugebilligt werden, sich von ihrer Leistungspflicht zu überzeugen. Insbesondere gewinnt dies Bedeutung bei der Abgrenzung zwischen dem Behandlungsfall und dem Pflegefall, für den die Krankenkasse nicht leistungspflichtig ist.
  Das Verfahren, das die Krankenkasse für die Überprüfung ihrer Leistungspflicht zu wählen hat, wurde im Gesundheitsreformgesetz genau festgelegt. Soweit nicht ein Prüfungsverzicht der Krankenkassen vorliegt, sind sie, wenn es nach Art, Schwere, Dauer oder Häufigkeit der Erkrankung oder nach dem Krankheitsverlauf erforderlich ist, nach § 275 Abs. 1 Nr. 1 SGB V verpflichtet, zur Prüfung von Voraussetzung, Art und Umfang der Krankenhausbehandlung eine gutachtliche Stellungnahme des Medizinischen Dienstes der Krankenversicherung einzuholen. Wenn es im Einzelfall erforderlich ist, sind die Ärzte des **Medizinischen Dienstes** befugt, die Räume der Krankenhäuser zu betreten, um dort die Krankenunterlagen einsehen und, soweit erforderlich, den Versicherten untersuchen zu können (§ 276 Abs. 4 SGB V).
  Ungeklärt ist in diesem Zusammenhang die Frage, ob an die Stelle der Einsichtnahme die **Übersendung von Auszügen** aus den Krankenunterlagen, etwa des Entlassungsberichts, **an den Medizinischen Dienst** (nicht an die Krankenkasse) treten kann. Ich halte eine solche Übersendung für zulässig, da der Medizinische Dienst in die gesamten Unterlagen Einsicht nehmen könnte.

Die Überlassung eines Krankenhausentlassungsberichtes an die Krankenkasse scheidet bei dieser Rechtslage nach meiner Auffassung aus, weil die Krankenkasse über andere, das Selbstbestimmungsrecht des Patienten weniger belastende Möglichkeiten verfügt, sich von ihrer Leistungspflicht zu überzeugen.

3.6 Datenerhebung des Amtsvormundes bei Unterhaltspflichtigen

Aufgrund einer Beschwerde war ich mit der Frage befaßt, welche Daten ein Amtsvormund als gesetzlicher Vertreter eines unterhaltsberechtigten nichtehelichen Kindes vom unterhaltspflichtigen Vater verlangen kann. Die Beschwerde des Vaters richtete sich gegen einen vom Jugendamt verwendeten „Ermittlungsbogen zur Überprüfung der wirtschaftlichen Verhältnisse", in dem u.a. die **Religionszugehörigkeit** des Beschwerdeführers, seine besonderen **finanziellen Belastungen** sowie Angaben zu seinen sonstigen unterhaltsberechtigten **Angehörigen** einschließlich deren Einkommensverhältnissen erfragt wurden.

Zusammen mit dem Staatsministerium für Arbeit und Sozialordnung bin ich der Auffassung, daß für den Auskunftsanspruch des Amtsvormundes nur der § 1605 BGB als Rechtsgrundlage in Betracht kommt. Die Auskunftspflicht nach dieser Bestimmung bezieht sich nur auf **Einkommen und Vermögen des Unterhaltsschuldners**, nicht hingegen auf das Einkommen von Ehepartnern oder Kindern des Unterhaltspflichtigen. Fragen zu den Einkommensverhältnissen dieses unterhaltsberechtigten Personenkreises dürfen nur dann gestellt werden, wenn sie mit einem **Hinweis auf die Freiwilligkeit** ihrer Beantwortung verbunden sind. Auch die Angaben über sonstige Belastungen dürfen nur auf freiwilliger Basis erhoben werden, denn sonstige Belastungen gewinnen erst an Bedeutung, wenn der Unterhaltsschuldner sich auf seine mangelnde Leistungsfähigkeit beruft, die er dann im nachhinein anhand konkreter Tatsachen näher darlegen und begründen muß. Für die Erhebung der Religionszugehörigkeit ist kein Rechtsgrund erkennbar.

Ich habe das Jugendamt aufgefordert, die Erhebungsbögen entsprechend abzuändern. Da ich jedoch annehme, daß andere Jugendämter ähnliche Fragebögen verwenden, habe ich den Bayerischen Landkreistag und den Bayerischen Städtetag gebeten, einen Musterentwurf für einen „Ermittlungsbogen zur Überprüfung der wirtschaftlichen Verhältnisse" zu erarbeiten und untereinander abzustimmen. Beide kommunale Spitzenorganisationen haben ein **Bedürfnis nach Abstimmung verneint**. Der Bayerische Landkreistag hat sich jedoch bereit erklärt, die Landkreise über eine mit mir abgestimmte Fassung des Vordruckes zu unterrichten.

Ein anderer Beschwerdeführer wendet sich dagegen, daß ein Amtspfleger sich unter **Umgehung des Unterhaltspflichtigen** unmittelbar an seinen Arbeitgeber gewandt und den Arbeitsverdienst erfragt hat. Für die Anfrage wurde eine „amtliche" Form gewählt, die den Arbeitgeber im Unklaren ließ, ob er zur Auskunftserteilung verpflichtet war oder — wie es der gegenwärtigen Rechtslage entspricht — die Anfrage nicht beantworten mußte. Außerdem fehlte jeder Hinweis auf die Freiwilligkeit der Angaben.

In Übereinstimmung mit dem Staatsministerium für Arbeit und Sozialordnung halte ich die Vorgehensweise des Amtspflegers für unzulässig. Der Amtspfleger darf sich Informationen über die wirtschaftlichen Verhältnisse eines unterhaltspflichtigen Vaters nicht unter **Vortäuschen von hoheitlichen Auskunftsrechten** vom Arbeitgeber beschaffen und diesen zu einem Verstoß gegen Schutzvorschriften gegenüber seinem Arbeitnehmer verleiten. Der Auskunftsanspruch nach § 1605 BGB richtet sich gegen den Unterhaltsschuldner, nicht gegen außenstehende Dritte. Dem legitimen Anspruch des Amtspflegers als gesetzlichen Vertreters des Kindes, ausreichende und nachprüfbare Informationen zu erhalten, ist in § 1605 Abs. 1 Satz 2 BGB bereits dadurch entsprochen, daß er bei Nichtselbständigen die Vorlage von Verdienstbescheinigungen und bei selbständig Tätigen die Einkommensteuererklärungen und -bescheide sowie Bilanzen verlangen und ggf. gerichtlich deren Herausgabe durchsetzen kann.

Ich habe das Jugendamt über diese Rechtsauffassung in Kenntnis gesetzt. Die neuen Bestimmungen des Kinder- und Jugendhilfegesetzes (KJHG) ändern diese Rechtslage nicht.

3.7 Auskunft eines Versorgungsamtes über Schwerbehinderung an Arbeitgeber

Ein Bürger hat in einer Beschwerde die Befürchtung geäußert, Informationen aus seinem Verfahren zur Anerkennung der Schwerbehinderteneigenschaft seien vom Versorgungsamt an seinen Arbeitgeber weitergegeben worden. Die Befürchtung hat sich nach meinen Ermittlungen bestätigt.

Der Betroffene führte einen Rechtsstreit vor dem Arbeitsgericht gegen seinen Arbeitgeber wegen der Kündigung seines Arbeitsverhältnisses. Für den Prozeß kam es darauf an, zu welchem Zeitpunkt dem Beschwerdeführer die Schwerbehinderteneigenschaft zuerkannt wurde. Meine Ermittlungen haben ergeben, daß sich der Arbeitgeber beim Sachbearbeiter im Versorgungsamt telefonisch nach dem Stand des Anerkennungsverfahrens erkundigt hat. Der Arbeitgeber erhielt ferner Auskunft, daß der Betroffene den bereits bescheidmäßig festgestellten Grad der Behinderung auch für die zurückliegende Zeit wünsche und deshalb gegen die Entscheidung des Versorgungsamtes Widerspruch eingelegt habe.

Für die Mitteilung dieser Informationen an den Arbeitgeber fehlte dem Versorgungsamt die Rechtsgrundlage. Eine Auskunft an den Arbeitgeber über den Stand des Anerkennungsverfahrens zählt nicht zu den gesetzlichen Aufgaben des Versorgungsamtes im Sinne des § 69 SGB X. Auch das Schwerbehindertengesetz enthält keine diesbezüglichen Befugnisse. Die genannte Bekanntgabe der Daten war daher ein Verstoß gegen das Sozialgeheimnis. Ich habe die Verhaltensweise des Versorgungsamtes beanstandet. Das Versorgungsamt hat mir eine eingehende Schulung seiner Mitarbeiter zugesichert.

3.8 Einsichtnahme der Polizei in Beherbergungsmeldescheine bei Obdachlosenheimen

Die Unterbringung von Obdachlosen in Heimen des Sozialamtes stellt eine Sozialhilfeleistung im Sinne der §§ 11 ff Bundessozialhilfegesetz (BSHG) dar mit der Folge, daß personenbezogene Daten dieser Bewohner aus der Sicht des Sozialamtes dem Sozialgeheimnis nach § 35 SGB I unterliegen. Zwischen einer Polizeidirektion und einer kreisfreien Stadt kam es zu Meinungsverschiedenheiten darüber, ob im Hinblick auf das Sozialgeheimnis die besonderen Meldescheine für Beherbergungsstätten nach Art. 27 Bayerisches Meldegesetz (MeldeG) von den Obdachlosenheimen zur Einsichtnahme für die Polizei bereitgehalten werden müssen. Nach Auffassung der kreisfreien Stadt enthält das Sozialgesetzbuch keine entsprechenden Offenbarungsbefugnisse.

Nach Abstimmung mit den Staatsministerien des Innern und für Arbeit und Sozialordnung habe ich der kreisfreien Stadt gegenüber die Auffassung vertreten, daß das Ausfüllen des Meldescheines eine melderechtliche Pflicht des Beherbergten, nicht des Beherbergungsbetriebes sei (Art. 26 Abs. 2, Art. 27 Abs. 1 MeldeG). Die Beherbergungsstätte bewahrt lediglich die Meldescheine für Polizei und Meldebehörde zur Einsichtnahme auf (Art. 27 Abs. 4 MeldeG). Es werden daher meiner Ansicht nach keine Sozialdaten erhoben, sondern die Meldedaten des Betroffenen nach dem Melderecht zur Einsichtnahme durch die Polizei vorgehalten. Auch ist die Pflicht der Beherbergungsstätte zur Aufbewahrung keine Aufgabe nach dem Sozialgesetzbuch, sondern nach dem Meldegesetz. Gegen die Einsichtnahme der Polizei in die Beherbergungsmeldescheine im Rahmen des Art. 27 Abs. 4 und Art. 29 MeldeG bestehen somit keine datenschutzrechtlichen Bedenken.

Selbst wenn die Beherbergungsstätte die Daten nach ihrer Erhebung für eigene Zwecke nutzt, werden die Daten in den Beherbergungsmeldescheinen gegenüber der Polizei dadurch noch nicht zu Sozialdaten. Die aus den Meldescheinen entnommenen Angaben werden aus der Sicht des Sozialamtes aber zu Sozialdaten, wenn sie für weitere Sozialleistungen herangezogen werden.

3.9 Unterrichtung des Jugendamts über Kindsmißhandlungen

Im Frühjahr 1990 berichtete eine Münchner Tageszeitung ausführlich über den tragischen Tod eines Kindes, das an den Folgen von Mißhandlungen durch die Eltern gestorben war. Das Kind war bereits ein Jahr zuvor schon einmal wegen schwerer Mißhandlungen in einer Kinderklinik behandelt worden. In diesem Zusammenhang wurde das Verhalten der zuständigen Behörden, insbesondere des Jugendamtes, kritisiert und für den Tod des Kindes mitverantwortlich gemacht. Ferner wurde im genannten Zeitungsartikel auf mögliche Hindernisse hingewiesen, die „der Datenschutz" für den notwendigen Datenaustausch zwischen der behandelnden Kinderklinik und dem Jugendamt bilden könne. Ich habe diese Vorwürfe zum Anlaß genommen, den tatsächlichen Informationsfluß zwischen den beteiligten Stellen zu überprüfen, da ich davon ausgehen mußte, daß Unsicherheiten über Befugnisse zur Offenbarung von personenbezogenen Daten bei Kindsmißhandlungen bestanden.

Das zuständige Jugendamt hat mir bestätigt, daß der Datenschutz im Falle des von seinen Eltern zu Tode mißhandelten Kindes zu keinem Zeitpunkt die Zusammenarbeit der beteiligten Stellen behindert hat. Die Kinder, bei denen die Klinik Verdacht auf Kindesmißhandlung hat, werden in aller Regel **mit Einwilligung der Eltern dem Jugendamt namentlich bekanntgegeben**. Das Jugendamt kann also seinen Betreuungspflichten nach der Entlassung des Kindes aus der Klinik nachkommen. An sogenannten „Fallkonferenzen" nehmen meist Mitarbeiter der Klinik und des Jugendamtes sowie der

betroffene Elternteil oder beide Eltern teil. Weigern sich die Eltern, so ist eine Durchbrechung der ärztlichen Schweigepflicht für die Ärzte des Krankenhauses im Rahmen des rechtfertigenden **Notstandes nach § 34 StGB** möglich.
Der Datenschutz steht somit dem Schutz der Kinder durch die zuständigen Stellen vor fortgesetzter Mißhandlung durch ihre Eltern nicht entgegen.

4. Polizei

4.1 Zur Lage des Datenschutzes

Mit dem Polizeiaufgabengesetz hat der Gesetzgeber der Forderung des Bundesverfassungsgerichtes und des Bayer. Verfassungsgerichtshofs entsprochen und für die Informationserhebung und -verarbeitung der Polizei eine tragfähige Grundlage geschaffen. Die Polizei erhielt allerdings auch zusätzliche Befugnisse, insbesondere zur nichtoffenen und verdeckten Informationsbeschaffung. So notwendig diese neuen Befugnisse, insbesondere zur Bekämpfung der organisierten Kriminalität sind, so eindeutig ist gleichzeitig die Herausforderung an den Datenschutz, die Datenerhebung und -verarbeitung der Polizei wirksam zu kontrollieren, damit das Vertrauen in die Rechtmäßigkeit polizeilichen Handelns erhalten bleibt.

Im Berichtsjahr hat die **Zahl der Datenverarbeitungsverfahren zugenommen**. Insbesondere im Bereich der Rauschgift- und der sonstigen organisierten Kriminalität bedingen neue Formen der Strafverfolgung auch zum Teil neue Formen der Datenverarbeitung. An der Erarbeitung solcher Projekte bin ich beteiligt, so daß auch in diesem Bereich der polizeilichen Straftatenbekämpfung datenschutzrechtliche Erfordernisse mitberücksichtigt werden.

Die Ausrüstung der Bayer. Polizei mit **Arbeitsplatzcomputern** (APC) ist im Berichtszeitraum fortgeführt worden. Das „moderne Büro" zieht auch bei der Polizei ein. Arbeitsplatzcomputer (APC) unterstützen die tägliche Arbeit. APC stellen aber die Datenschutzkontrolle vor neue Aufgaben.

Im zurückliegenden Jahr habe ich verstärkt Wert darauf gelegt, daß die Polizei über Speicherung und Dauer einer Speicherung im Kriminalaktennachweis, einer Verdächtigendatei, unter Ausnutzung aller vorliegenden Erkenntnisse entscheidet. Dazu gehört auch der **Ausgang des Justizverfahrens**, das für die Frage, ob ein Strafverdacht gegen jemand besteht, nicht gleichgültig sein kann. Deshalb werde ich weiterhin auf eine Verbesserung der Zusammenarbeit zwischen Staatsanwaltschaft und Polizei drängen.

Die Frage, ob sich aus einer Straftat Hinweise zur Verhütung und Aufklärung von weiteren Straftaten, die gegen die innere Sicherheit gerichtet sind, gewinnen lassen und deshalb eine Speicherung in der **Staatsschutzdatei APIS** gerechtfertigt ist, ist bei der Auswertung der Tatumstände des Einzelfalles oft nicht leicht zu beantworten. Das gilt insbesondere für die Frage, ob in einem bestimmten strafbaren Verhalten erste Anzeichen staatsfeindlicher krimineller Aktivitäten zu sehen sind. Deshalb wird es in der Frage, ob diese oder jene Speicherung in APIS gerechtfertigt ist, immer wieder Meinungsverschiedenheiten zwischen polizeilichem Staatsschutz und Datenschutz geben.

Die Polizei mißt dem Datenschutz bei der **Aus- und Fortbildung** der Beamten noch größeres Gewicht bei. Bei der Ausbildung von Polizeibeamten an der Bayer. Beamtenfachhochschule Fachbereich Polizei und am Fachinstitut der Bayer. Polizei wurden die Zahl der Unterrichtseinheiten zu Fragen des Datenschutzes und der Datensicherheit erhöht und das Angebot zur Weiterbildung ergänzt.

4.2 Schwerpunkte

Intensiv befaßt war ich mit der Novellierung des **Polizeiaufgabengesetzes**. Nach den Vorarbeiten zum Regierungsentwurf habe ich im Landtag und Senat zum Gesetzentwurf Stellung genommen und mich an den Beratungen beteiligt.

Ein weiterer Schwerpunkt meiner Tätigkeit im Polizeibereich lag wieder in der **Prüfung von Polizeidienststellen**.

Neben den Behördenprüfungen wurde ich zu einer Reihe neuer EDV-Vorhaben — zunehmend bereits in der Konzeptionsphase — zu Rate gezogen. Zu nennen ist hier die Einführung der sogenannten Protokolldatei beim Bayer. Landeskriminalamt, mit der seit November 1989 alle relevanten Dateiabfragen in landesweiten Dateien protokolliert werden. Das Verfahren dient dem Schutz der Bürger vor unberechtigten Abfragen, aber auch zum Schutz der Polizei vor ungerechtfertigten Vorwürfen.

4.3 Novellierung des Bayerischen Polizeiaufgabengesetzes

Mit dem 3. Gesetz zur Änderung des Polizeiaufgabengesetzes, das am 1. Oktober 1990 in Kraft getreten ist, hat der Bayerische Landtag eine tragfähige gesetzliche Grundlage für die polizeiliche Informationserhebung und -verarbeitung geschaffen.

Im Gesetzgebungsverfahren konnte ich noch folgende wesentliche Verbesserungen des Datenschutzes erreichen:

- **Auskunftsrecht**

  Auskunftsrechte der Bürger gegenüber den Behörden zu den über sie gespeicherten Daten gehören zum Kern des informationellen Selbstbestimmungsrechts. Das Polizeiaufgabengesetz enthält in Art. 48 einen ausdrücklichen Auskunftsanspruch des Betroffenen über die zu seiner Person gespeicherten Daten. Die Auskunft darf nur in Ausnahmefällen verweigert werden (u. a. Gefährdung der öffentlichen Sicherheit oder der Aufgabenerfüllung der Polizei, oder wenn berechtigte Interessen eines Dritten entgegenstehen). Wird die Auskunft verweigert, so kann sich der Betroffene mit seinem Anliegen an den Datenschutzbeauftragten wenden. Ich prüfe dann in eigener Zuständigkeit, ob die Auskunftsverweigerung durch die Polizei gerechtfertigt war.

- **Offene Datenerhebung**

  Der Grundsatz des „offenen Visiers" wurde noch stärker verankert. Eine Datenerhebung, die nicht als polizeiliche Maßnahme erkennbar sein soll, ist nicht schon dann zulässig, wenn die Erfüllung polizeilicher Aufgaben auf andere Weise erschwert würde. Voraussetzung ist eine **erhebliche Erschwerung**.

- **Vernichtung übermittelter nicht benötigter Daten**

  Werden Daten, die an eine Polizeidienststelle übermittelt

werden, von dieser offensichtlich nicht mehr benötigt, dann sind sie zu vernichten.

Andere Vorschläge wurden nicht berücksichtigt. Es ist jedoch Sache des Gesetzgebers, wie er innerhalb der verfassungsmäßigen Schranken, insbesondere unter Beachtung der Grundsätze der Verhältnismäßigkeit und der Normenklarheit den teilweise entgegengesetzten Verfassungszielen Sicherheit der Bürger und Schutz der Privatsphäre des Einzelnen Rechnung tragen will.

- Die Belehrung eines Bürgers darüber, ob er bei Befragen durch einen Polizeibeamten zur Auskunft verpflichtet oder ob die Auskunft freiwillig ist, gehört zum Kern des informationellen Selbstbestimmungsrechts. Ein Bürger, der darüber im unklaren gelassen würde, ob er zur Auskunft verpflichtet ist, wäre nicht Herr seiner Daten. Jedenfalls dann, **wenn der Bürger hierüber Aufklärung verlangt, muß er bei Freiwilligkeit der Auskunft hierauf vorher hingewiesen werden**. Nur eine solche Auslegung der Bestimmung über die Hinweispflicht der Polizei erscheint mir verfassungskonform.

- Eines meiner Anliegen war es auch, eine **wirksame Datenschutzkontrolle insbesondere beim Einsatz besonderer Mittel** der Datenerhebung sicherzustellen, weil der Bürger hier besonders schutzwürdig ist. Da besondere Aufzeichnungspflichten zur Kontrolle dieser Einsätze durch den Datenschutzbeauftragten im Gesetz nicht vorgesehen wurden, kann der gebotene Datenschutz in diesem sensiblen Bereich nur durch zusätzliche allgemeine Kontrollen erreicht werden.

4.4 Allgemeine Prüfungen

Allgemeine Prüfungen habe ich im Berichtszeitraum bei folgenden Polizeibehörden vorgenommen:

- Landeskriminalamt
- Präsidium der Bayerischen Grenzpolizei mit der Grenzpolizeiinspektion und der Grenzpolizeistation München/Riem
- Polizeipräsidium Unterfranken mit den Polizeidirektionen Aschaffenburg, Schweinfurt und Würzburg
- Polizeipräsidium Oberbayern mit den Polizeidirektionen Fürstenfeldbruck und Weilheim
- Polizeipräsidium Niederbayern/Oberpfalz mit den Polizeidirektionen Amberg, Straubing und Weiden

Damit sind seit Einführung der Datenschutzkontrolle nunmehr alle Polizeipräsidien und -direktionen mindestens einmal überprüft worden. Die im Vorjahr getroffene Feststellung, daß die **Polizei im wesentlichen die Datenschutzbestimmungen beachtet und Datenschutzverstöße die Ausnahme sind**, kann ich auch für dieses Jahr wiederholen.

4.4.1 Kriminalaktennachweis (KAN)

Im KAN werden die Akten bayerischer Polizeivollzugsdienststellen nachgewiesen. Die Akten müssen folgende Zwecke erfüllen:

- Bei polizeilichen Ermittlungen die Aufklärung des Sachverhalts unterstützen und die Feststellung von Verdächtigen fördern,
- Hinweise zur Gefahrenabwehr, insbesondere zur vorbeugenden Verbrechensbekämpfung, geben,
- bei der Personenidentifizierung helfen,
- Hinweise für das taktische Vorgehen und die Eigensicherung der Polizei geben.

Im Regelfall enthalten die Kriminalakten Unterlagen über polizeiliche Ermittlungen bei Straftaten und Ordnungswidrigkeiten, wobei Ordnungswidrigkeiten nur in bestimmten Fällen und Verkehrsordnungswidrigkeiten überhaupt nicht in den KAN Eingang finden. Bei der Kontrolle der Zulässigkeit von Speicherungen prüfe ich neben der Zulässigkeit der Datenerhebung und der Richtigkeit der Daten und des zulässigen Inhalts der Speicherung auch, ob die in KAN und Akten gespeicherten Informationen einen der vorgenannten Zwekke erfüllen können.

Speicherungsebenen im KAN

Die Einrichtung des KAN erfolgte auf Beschluß der Konferenz der Innenminister des Bundes und der Länder vom 12. Juni 1981. Das bis heute gültige Konzept sieht vor, daß Speicherungen im KAN überregional, d.h. bundesweit, oder regional, d.h. landesweit abrufbar sind. Abweichend von diesen beiden Speicherungsebenen wurde allein in Bayern eine dritte Speicherungsebene auf der Ebene der Polizei**direktionen** eingerichtet (Regional-KAN). Er hielt bestimmte Daten nur für die Dienststellen der speichernden Polizeidirektionen vor, also nicht landesweit für alle bayerischen Polizeidienststellen. In den übrigen Bundesländern sind vergleichbare Daten hingegen landesweit abrufbar. Diese mit mir damals abgestimmte Speicherungsebene bei den Polizeidirektionen ging von der Annahme aus, daß die Speicherung bestimmter Daten nur für die Aufgabenerfüllung bestimmter Polizeidirektionen erforderlich ist. Die damalige Entscheidung ist nach den jahrelangen Erfahrungen aus fachlicher Sicht nicht mehr haltbar. Die Mobilität von Straftätern hat zugenommen; ein örtlicher Straftäter, der seinen Wohnbereich nicht verläßt, ist die Ausnahme. Auftretende Informationsdefizite — beispielsweise wußten zwei Polizeidirektionen nicht, daß bei beiden Stellen Erkenntnisse vorhanden waren — führten zu Doppelspeicherungen bei beiden Stellen oder zu zusätzlichen Belastungen des Betroffenen, z.B. zur wiederholten Überprüfung seiner Personalien.

Aus diesem Grunde habe ich keine datenschutzrechtlichen Bedenken gegen die Entscheidung des Innenministeriums erhoben, bei Beschuldigten und Tatverdächtigen künftig wie in den anderen Bundesländern zu verfahren. Auf der Ebene der Polizeipräsidien verbleibt künftig ein kleiner Teil von Speicherungen personenbezogener Daten im KAN, der weder Beschuldigte noch Tatverdächtige betrifft, also Fälle der sonstigen polizeilichen Gefahrenabwehr oder Vermißtenfälle. Auf die Speicherung von Fahrlässigkeitsdelikten im KAN, die zugleich Antragsdelikte sind, z.B. fahrlässige Körperverletzung, die nur auf Antrag verfolgt wird, und unter bestimmten Voraussetzungen auf die Erfassung von Privatklagedelikten wird künftig ganz verzichtet.

Ich werde dieses geänderte KAN-Konzept im Hinblick auf die Vorgaben der neuen Datenverarbeitungsregelungen im Polizeiaufgabengesetz im neuen Jahr prüfen.

Berücksichtigung des Verfahrensausgangs

Zur Bewertung der Frage, ob die Speicherung einer Straftat im KAN unter der gewählten **rechtlichen Bezeichnung** und

über die vorgesehene **Dauer** hin zulässig ist, muß die Polizei den **gesamten Akteninhalt** heranziehen. Dabei kann für Inhalt und Dauer der Speicherung nicht allein der Akteninhalt zum Zeitpunkt der Einspeicherung maßgeblich sein. Vielmehr müssen nachträglich gewonnene Erkenntnisse mitberücksichtigt werden und grundsätzlich zu einer Überprüfung der Speicherung führen. Nachträgliche Erkenntnismöglichkeiten, die eine sicherere Beurteilung des Tatverdachts erlauben, müssen genutzt werden. Insbesondere ist der **Verfahrensausgang bei Staatsanwaltschaft und Justiz** für die jeweilige Speicherung von Bedeutung. Die Polizei muß bei der Frage, ob die Speicherung beizubehalten ist, alle zumutbaren Erkenntnisquellen benutzen. Auch wenn sie an Verfahrenseinstellungen der Staatsanwaltschaft oder an einen Freispruch des Gerichts nicht unmittelbar gebunden ist und trotz solcher Justizentscheidungen weiterhin einen Verdacht annehmen kann, ist doch Voraussetzung für die Beibehaltung der Speicherung, daß die Polizei dabei die Entscheidung der Staatsanwaltschaft und des Gerichts in ihre Überlegungen einbezieht. Das ist schließlich auch der Sinn und Zweck des **Strafmitteilungsblattes**, in dem die Staatsanwaltschaft der Polizei den Ausgang des Verfahrens mitteilt.

- Wie in den Vorjahren mußte ich auch im Berichtszeitraum wiederholt feststellen, daß bei den überprüften Speicherungen vielfach der **Ausgang des Verfahrens der Polizei nicht bekannt** war, obwohl das Verfahren längst hätte abgeschlossen sein müssen. Wegen der Bedeutung des Verfahrensausgangs für den Inhalt und die Dauer der Speicherung ist es nicht hinnehmbar, wenn Staatsanwaltschaften die Rücksendung des Strafnachrichtenblattes an die Polizei unterlassen und auf diese Weise eine sachgerechte Entscheidung über die Beibehaltung der Speicherung im KAN verhindern. Staatsanwaltschaften, die ihrer Verpflichtung nicht nachkommen, werde ich künftig beanstanden.

- Eine andere Frage ist, ob die Polizei **von sich aus** nach Ablauf bestimmter Fristen oder bei bestimmten Anlässen, etwa einer Auskunft an eine Behörde, die Übersendung des Strafnachrichtenblattes bei der Staatsanwaltschaft **anmahnen** muß. Für ein Tätigwerden nach Ablauf bestimmter Fristen spricht, daß die Polizei die Speicherung einer Person im KAN, die schließlich eine erhebliche Belastung und Gefährdung für den Betroffenen bedeuten kann, in zumutbarer Weise **unter Kontrolle halten** muß. Andererseits darf aber auch durch Anmahnungen entstehender **Verwaltungsaufwand** nicht außer acht gelassen werden. Dieser könnte dadurch gering gehalten werden, daß der Ausgang des Verfahrens nur in den Fällen ermittelt wird, in denen der Vorgang bearbeitet wird, etwa aufgrund einer Anfrage, und nach den Erfahrungen der Praxis das Verfahren beendet sein müßte.

  Bis jetzt hat das Innenministerium zugesagt, daß die Polizei in folgenden Fällen den Verfahrensausgang durch **Rückfrage bei der Staatsanwaltschaft ermitteln wird**:

- Erneute polizeiliche Ermittlungen gegen die Person geben hierzu Anlaß
- Der Betroffene hat Antrag auf Vernichtung der polizeilichen Unterlagen gestellt
- Der Landesbeauftragte für den Datenschutz benötigt im Einzelfall anläßlich einer datenschutzrechtlichen Überprüfung die Kenntnis des Verfahrensausganges.

Diese vorläufige Regelung kann jedoch angesichts der Bedeutung des Verfahrensausgangs für die Frage der Beibehaltung einer Speicherung noch nicht befriedigen. Ich werde deshalb meine Bemühungen um eine sachgerechte Lösung fortsetzen.

- Mit dem Innenministerium habe ich die Frage erörtert, wie die Polizei auf Übersendung eines Strafnachrichtenblattes zu **reagieren** hat. Unproblematisch ist das Verfahren, wenn die mitgeteilte Entscheidung der Staatsanwaltschaft oder des Gerichts den Tatverdacht der Polizei bestätigt. Dann kann die Polizei die Speicherung ohne weitere Prüfungen unverändert beibehalten. Weicht die Justizentscheidung von der polizeilichen Anzeige ab (z. B. andere rechtliche Bewertung der Tat, Freispruch, Einstellung), dann stellt sich die Frage, ob die Polizei in jedem Fall die Speicherung vollständig zu überprüfen hat. Dabei ist zu bedenken, daß eine Einstellung des Verfahrens durch die Staatsanwaltschaft wegen zur Anklage nicht ausreichenden, aber doch noch weiterbestehenden Tatverdachts und ein Freispruch mangels Beweises kein Anlaß für aufwendige Nachprüfungen der Speicherung sein können, da in diesen Fällen auch bei der Justiz der Tatverdacht nicht ausgeräumt ist. Wird jedoch von Staatsanwaltschaft oder Gericht der **Tatverdacht verneint**, dann muß dies für die Polizei Anlaß sein, die Speicherung eingehend zu überprüfen. In diesem Fall ist die aufrechterhaltene Speicherung durch die Polizei zu begründen, die Gründe sind im Akt schriftlich festzuhalten. **Bei Einstellung des Verfahrens** durch die Staatsanwaltschaft oder bei einem **Freispruch** sollte deshalb die Polizei auch darüber **unterrichtet werden, ob der Tatverdacht verneint wird bzw. entfallen ist**.

Dauer der Aussonderungsprüffristen

Die **Aussonderungsprüffristen gespeicherter Daten** sind für Regelfälle vorgesehen. Sie sind bereits bei der Erfassung in der Datei KAN festzulegen. Kürzere Fristen gelten beispielsweise bei der Erfassung von Kindern, Jugendlichen und Personen über 70 Jahren, aber auch in Fällen von geringer Bedeutung (z.B. Privatklagedelikte) und in Fällen polizeilicher Gefahrenabwehr (z.B. Vermißtenfälle).

Eine Überschreitung der Regelfrist habe ich bei meinen Prüfungen nicht mehr festgestellt. Bei der Erfassung von Kindern, Jugendlichen oder 70jährigen bestanden noch **vereinzelt Flüchtigkeitsfehler** (z.B. bei der Erfassung einer länger zurückliegenden Straftat wurde übersehen, daß der Täter zur Tatzeit noch Jugendlicher war und deshalb nur eine kürzere Speicherungsdauer zulässig gewesen wäre). Im übrigen lag mein Augenmerk auf der **Bemessung kürzerer Fristen** in Fällen von geringer Bedeutung. Hier stelle ich doch bei meinen Prüfungen vereinzelt fest, daß die Polizei **bestehende Ermessensspielräume nicht nutzt** und nicht mehr erforderliche Daten bis zum Erreichen der Regelaussonderungsfrist vorhält.

Qualität des KAN

Die **Qualität der im KAN gespeicherten Daten** ist ansonsten aus datenschutzrechtlicher Sicht zwischenzeitlich zu-

friedenstellend. Die in früheren Tätigkeitsberichten herausgestellten Prüfansätze wie

- personengebundene Hinweise,
- Straftatenmerker,
- Erfassung von Verkehrsstraftaten,
- Erfassung von Ordnungswidrigkeiten,
- „sonstige polizeiliche Gefahrenabwehr", usw.,

bereiten den 1990 geprüften Dienststellen keine Schwierigkeiten mehr. Bestimmte Bereiche (z.B. Speicherungen unter dem Gesichtspunkt „sonstiger polizeilicher Gefahrenabwehr") sind bei verschiedenen Polizeidirektionen generell überprüft worden und haben zu einer teilweise erheblichen Reduzierung der Datenbestände geführt. Grundsätzlich kann gesagt werden, daß die Polizei die Erfahrungen, die sich aus dem Betrieb des KAN in den vergangenen Jahren ergeben haben, umgesetzt und somit eine erfreulich hohe Datenqualität erreicht hat.

Die Erfahrungen dieser Jahre hat das Staatsministerium des Innern in eine **Dienstanweisung zur Datei KAN** eingebracht. Die Dienstanweisung soll den Sachbearbeitern bei den erfassenden Stellen eine ergänzende Arbeitshilfe bieten. Die Erarbeitung der Dienstanweisung begrüße ich auch aus datenschutzrechtlicher Sicht.

4.4.2 Weitere Dateien/Karteien

Neben dem Kriminalaktennachweis habe ich einige **Rauschgift- und Prostituiertenkarteien** geprüft. Alle geprüften Karteien werden zumindest einmal pro Jahr auf Aussonderung von Karteikarten geprüft. Die **Aussonderungsprüffristen** betrugen nicht mehr als fünf Jahre, soweit es sich nicht auch hier um KAN-relevante Vorgänge, insbesondere Straftaten handelte. Zu kritischen Anmerkungen bestand kein Anlaß.

4.4.3 Polizeilicher Staatsschutz

Bei fünf geprüften Polizeidirektionen wurde jeweils auch der polizeiliche Staatsschutz kontrolliert. Bei einer Polizeidirektion habe ich diesen Bereich besonders unter die Lupe genommen. Dabei wurden geprüft

- die Kriminalakten über Staatsschutzdelikte im Kriminalaktennachweis (KAN),
- die Staatsschutzkartei mit den dazugehörenden Unterlagen,
- Informationssammlungen im Kommissariat Staatsschutz zu bestimmten Projekten.

Allgemein war festzustellen, daß die Informationsverarbeitung sehr unterschiedlich organisiert ist. Während bei der einen Polizeidirektion eine gesonderte Staatsschutzkartei nicht für erforderlich gehalten wird, und alle Unterlagen, soweit sie polizeiliche Ermittlungsverfahren betreffen, in der auch zentralen Aktensammlung verwahrt und im Kriminalaktennachweis nachgewiesen werden, führt das Staatsschutzkommissariat einer anderen Polizeidirektion eine gesonderte KS-Kartei, in der die Kriminalakten mit Staatsschutzbezug nachgewiesen werden.

Auch die Qualität der Datenverarbeitung ist von Direktion zu Direktion sehr unterschiedlich. Teilweise weisen Kriminalakten und Staatsschutzkartei nicht unerhebliche Mängel auf:

1. Fehlender Hinweis auf Verfahrensausgang

   Wie bei den übrigen Kriminalakten fehlten auch in den Akten des Staatsschutzkommissariats in Einzelfällen Strafnachrichtenblätter oder andere Hinweise auf den Verfahrensausgang. Eine Speicherung im KAN (bestehender Verdacht, Bezeichnung der Tat, Speicherungsdauer) kann jedoch erst dann abschließend bewertet werden, wenn der Verfahrensausgang in die Beurteilung einbezogen ist. Die Ausführungen zu 4.4.1 gelten auch hier.

2. Nicht begründete Speicherungsdauer nach Verfahrenseinstellung

   Insofern verweise ich auf Ziffer 4.4.1

3. Karteikarten

   Die in einem Kommissariat verwendeten Karteikarten für die Staatsschutzkartei entsprachen nicht den Vorgaben der Feststellungsanordnung. Teilweise enthielten sie Datenfelder, die nicht zulässig waren, andererseits fehlten notwendige Felder wie Aussonderungsprüffristen und betroffener Personenkreis.

4. Fehlender Staatsschutzbezug

   In zahlreichen Fällen ergab sich der Staatsschutzbezug, also der Grund für die Speicherung einer Straftat in der Staatsschutzkartei, weder aus der Karteikarte noch aus dem Kriminalakt, sondern entweder erst aus zusätzlichen mündlichen Angaben des Sachbearbeiters oder konnte gar nicht belegt werden.

5. Auffangkartei Staatsschutz

   In Einzelfällen habe ich festgestellt, daß Vorgänge, die zunächst eine Straftat begründeten, später aber nach Kenntnis des Verfahrensausgangs **aus den Kriminalakten gelöscht** wurden, als **„staatsschutzrelevanter Vorgang"** in der Kartei Staatsschutz verwahrt wurden. Diese Vorgehensweise entspricht nicht den rechtlichen Vorgaben: Wenn aus polizeilicher Sicht Restverdacht besteht, ist die KAN-Speicherung weiterhin grundsätzlich zulässig, ggf. mit verkürzter Aussonderungsprüffrist. Danach ist Platz in der Staatsschutzkartei nur, wenn Hinweise auf verfassungsfeindliche Handlungen vorliegen.

Die festgestellten Mängel habe ich beanstandet.

Zu den **Speicherungsfristen** in den KS-Karteien ist anzumerken, daß sie, soweit sie keine Staatsschutzdelikte betrafen, entsprechend den Richtlinien unter den Fristen im KAN lagen. In keinem Fall habe ich bei meinen Prüfungen längere als fünfjährige Fristen festgestellt. Davon ausgenommen sind die Staatsschutzdelikte. Sie werden nach den gleichen Vorgaben gespeichert wie andere Delikte.

4.5 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 und für die polizeiliche Datenverarbeitung und Datenübermittlung in Bayern sowie die **Fernmeldeleitstelle** für die polizeiliche Nachrichtenübermittlung. Wegen dieser zentralen Bedeutung für die polizeiliche Datenverarbeitung habe ich beim BLKA wieder eine mehrtägige allgemeine Prüfung verschiedener EDV-Vorhaben vorgenommen.

Prüfungsschwerpunkte waren:

- Arbeitsdatei PIOS innere Sicherheit (APIS)
- Kriminalaktennachweis (KAN)
- Datei Personenbeschreibung
- SPUDOK-Datei für Waffen- und Sprengstoffdelikte
- SPUDOK-Datei zur Bekämpfung der Glücksspielkriminalität

Arbeitsdatei PIOS innere Sicherheit (APIS)

Die Datei APIS soll als Hilfsmittel zur Verhütung oder Aufklärung von Straftaten mit staatsfeindlicher Zielsetzung dienen. Dabei handelt es sich nach den Richtlinien um Straftaten, die u.a. gegen die freiheitliche demokratische Grundordnung, den Bestand und die Sicherheit des Bundes oder eines Landes gerichtet sind oder die eine ungesetzliche Beeinträchtigung der Amtsführung von Mitgliedern verfassungsmäßiger Organe des Bundes oder eines Landes zum Ziele haben. Hierzu zählen sog. Katalogstraftaten, die im Regelfall erfaßt werden, beispielsweise Straftaten gegen Verfassungsorgane oder die Bildung einer terroristischen Vereinigung oder Gefährdung des demokratischen Rechtsstaats, aber auch andere Straftaten,

a) wegen des Motivs des Täters, wenn

   - über die aus dieser Straftat gewonnenen Erkenntnisse hinaus Anhaltspunkte dafür vorliegen, daß der oder die Täter staatsfeindliche Ziele verfolgen oder

   - Anhaltspunkte dafür vorliegen, daß der oder die Täter weitere Straftaten zum Erreichen staatsfeindlicher Ziele begehen werden,

b) wegen der Verbindung des Täters zu einer Organisation, die verdächtig ist, sich an Straftaten gegen die freiheitliche demokratische Grundordnung, den Bestand und die Sicherheit des Bundes oder eines Landes oder die Funktionsfähigkeit verfassungsmäßiger Organe verantwortlich zu beteiligen, wenn Anhaltspunkte dafür bestehen, daß mit der Tat Ziele der Organisation unterstützt werden sollen, oder

c) wegen des Objekts (Person, Institution oder Sache), gegen das sich die Straftat richtet, wenn sich hieraus der Verdacht begründet, daß staatsfeindliche Ziele verfolgt werden und keine Erkenntnisse vorliegen, die eine Erfassung wegen des Motivs des Täters ausschließen würden.

Nach der Errichtungsanordnung handelt es sich bei APIS also keineswegs um eine Terroristendatei, wie in Verkennung der Ziele von APIS immer wieder behauptet wird.

Diskutiert wird gelegentlich, ob der Erfassungstatbestand „andere Straftaten mit staatsfeindlicher Zielsetzung" eingeschränkt werden soll, weil dieser Tatbestand weit gefaßt ist und den größten Teil der Speicherungen in APIS stellt. Bis jetzt wurde jedoch keine brauchbare Alternative aufgezeigt, soll APIS nicht jede praktische Bedeutung als Arbeitsdatei zur Gewinnung von polizeilich nutzbaren Anhaltspunkten zur Verhütung und Aufklärung von politischen Straftaten verlieren.

Prüfungsansätze bei der Kontrolle von APIS waren insbesondere
- der **Staatsschutzbezug** des gespeicherten Vorgangs,
- die Speicherung des Vorgangs muß dazu dienen und geeignet sein, **Hinweise zur Verhütung oder Aufklärung** von Straftaten mit staatsfeindlicher Zielsetzung zu liefern. Besonderes Augenmerk habe ich darauf gerichtet, ob der Verdacht staatsfeindlicher Zielsetzung aus dem Motiv oder der Verbindung des Täters zu staatsfeindlichen Organisationen oder aus dem angegriffenen Objekt begründet ist.
- **Dokumentation** der Umstände, die den Staatsschutzbezug begründen
- **Nachvollziehbarkeit** der Bewertungen
- Speicherungsdauer
- Zulässigkeit der Datenübermittlung von anderen und an andere Dienststellen.

Die Kontrolle mußte sich wieder auf Stichproben beschränken, die wie folgt gezogen wurden:
- aus ausgewählten Erfassungsmonaten und Aussonderungsprüfmonaten
- nach ausgewählten Straftaten, z.B. Sachbeschädigungen, Nötigungen, Verwenden von Kennzeichen verfassungswidriger Organisationen
- nach bestimmten Berufen der in APIS erfaßten Personen
- nach ausgewählten Namen, wobei insbesondere Querschnittsauswertungen vorgenommen und Erkenntnisse aus Presseberichten und sonstige Hinweise verwertet wurden.

Ergebnis

Aus der Überprüfung wurde deutlich, daß sich das BLKA ernsthaft darum bemüht, nur Vorgänge mit Staatsschutzbezug zu speichern.

Das BLKA hat die **Dokumentation** der Umstände, aus denen es den Staatsschutzbezug, also die staatsfeindliche Zielsetzung der Straftat ableitet, verbessert. Nunmehr dokumentiert der einzelne Staatsschutzsachbearbeiter im Vorgang, welche der bezeichneten Straftaten vorliegt. Liegt eine der sogenannten „anderen Straftaten" vor, bei denen sich die Zielsetzung erst aus dem Motiv, der Einbindung in eine Organisation oder aus dem angegriffenen Objekt ergibt, muß der Sachbearbeiter die staatsfeindliche Zielsetzung im Vorgang kurz begründen. Diese Praxis begrüße ich, weil sie in der Tendenz zu einer restriktiven Speicherung führt.

Allerdings bestanden **in einigen Fällen Zweifel**, ob aus den angegebenen Umständen auf eine **staatsfeindliche Zielsetzung** geschlossen werden kann. In allen diesen Fällen fehlte der Verfahrensausgang, so daß mir eine abschließende Beurteilung zunächst nicht möglich war. Nach Eingang der Stellungnahme des BLKA besteht in der Bewertung der APIS-Relevanz der fraglichen Vorgänge mit dem BLKA Einvernehmen. Der überwiegende Teil der Vorgänge war zu Recht in APIS aufgenommen, der andere Teil ist inzwischen aus APIS gelöscht, überwiegend aufgrund des Verfahrensausgangs. Dieses Ergebnis zeigt einmal mehr, wie wichtig die Mitteilung des Verfahrensausgangs für die Fortdauer der Speicherung ist.

Popgruppen, in deren Namen ein S vorkommt, schreiben dieses S als **Sig-Rune**. Anhänger solcher Gruppen, die auf ihrer Jacke den Namen der Popgruppe mit der Sig-Rune tragen, werden wegen Verwendung eines Kennzeichens verfassungswidriger Organisationen angezeigt. Obwohl die Verfahren häufig eingestellt werden, halte ich im Hinblick auf die notwendige Beobachtung extremistischer Gruppen APIS-Eintragungen in solchen Fällen grundsätzlich für ge-

rechtfertigt, es sei denn daß bei diesen Gruppen extremistische Tendenzen ausgeschlossen werden können.

Die **Speicherungsdauer** der kontrollierten Eintragungen in APIS war korrekt. Positiv zu werten ist insbesondere, daß die Beschuldigten in minderschweren Fällen zunehmend mit teilweise erheblich verkürzten Aussonderungsprüffristen gespeichert waren. Auch bei Heranwachsenden, wird in geeigneten Fällen die Frist verkürzt. Dies begrüße ich, weil gerade bei dieser Altersgruppe eine schematische Vergabe von Aussonderungsprüffristen nicht gerechtfertigt ist.

Allerdings bin ich auch in APIS auf ältere Vorgänge gestoßen, bei denen der Ausgang des Strafverfahrens trotz länger zurückliegender Abgabe an die Staatsanwaltschaft nicht bekannt war. Gerade Verfahrenseinstellungen wegen fehlenden Tatverdachts oder wegen geringer Schuld können zu einer anderen als der ursprünglichen Bewertung der staatsfeindlichen Zielsetzung führen. Auch wenn das BLKA an die Auffassung der Justiz nicht starr gebunden ist, kann es für den Staatsschutz nicht ohne Bedeutung sein, wenn Staatsanwaltschaft oder Gericht eine staatsfeindliche Absicht verneinen.

Kriminalaktennachweis im Landeskriminalamt (LKAN)

Das BLKA ist neben seiner Zentralstellenfunktion auch für die Verfolgung bestimmter schwerer Straftaten und für die Verfolgung von Straftaten mit zumindest landesweiter Bedeutung zuständig. Die Daten, die im Rahmen dieser Ermittlungen anfallen, werden wie von den Polizeidirektionen im KAN erfaßt.

Aus den KAN-Speicherungen des BLKA habe ich nach folgenden Gesichtspunkten Stichproben gezogen:

- Ausgewählte Tatzeit,
- ausgewählte Straftaten mit ausgesuchten Aussonderungsprüfdaten,
- bestimmte Klassifizierungen von Straftaten z.B. Straftaten, bei denen gewerbsmäßiges Handeln oder internationale Tatbegehung vermerkt worden war (Vergabe sog. KAN-Merker),
- ausgewählte Namen.

Als Ergebnis der Prüfung war festzustellen, daß in jedem Fall der Verdacht der gespeicherten Straftat nachvollziehbar begründet war. Nur in wenigen Fällen mußten zur abschließenden datenschutzrechtlichen Bewertung fehlende Verfahrensausgänge bei den Staatsanwaltschaften nachgefragt werden.

Auf meine Anregung hin, wird das BLKA im KAN ein DV-Verfahren einführen, das Auswertungen (beispielsweise nach den oben genannten Gesichtspunkten) bei den jeweils speichernden Stellen (BLKA und — nach der künftigen KAN-Konzeption — die Polizeipräsidien) ermöglicht.

Datei Personenbeschreibung

Die Datei Personenbeschreibung enthält alle von bayerischen Polizeidienststellen gefertigten Personenbeschreibungen. Aufgenommen werden die **Beschreibungsdaten** von Beschuldigten, Verdächtigen, Betroffenen von Ordnungswidrigkeiten von schwerwiegender Bedeutung und von anderen Personen, bei denen aufgrund anderweitiger gesetzlicher Rechtsgrundlagen eine Personenbeschreibung vorgenommen wird. Ferner enthält die Datei **Hinweise**, wo Lichtbilder und Fingerabdrucke von Beschuldigten aufbewahrt werden.

Die Datei wird zur Zeit vom BLKA und bei den Polizeipräsidien Mittelfranken und München geführt. Eine Ausdehnung auf die anderen Polizeipräsidien ist vorgesehen.

Bei allen Stichproben waren die Voraussetzungen einer erkennungsdienstlichen Behandlung nach § 81 b Strafprozeßordnung gegeben.

SPUDOK-Datei für Waffen- und Sprengstoffdelikte

Zur Aufklärung von Waffen- und Sprengstoffdelikten hat das BLKA eine SPUDOK-Datei eingerichtet. Waffen- und Sprengstoffdelikte in Bayern sind von den sachbearbeitenden Polizeidienststellen dem BLKA **zu melden**. Dort werden sie in die SPUDOK-Datei aufgenommen und ausgewertet.

Wie ich festgestellt habe, werden in dieser Datei tatsächlich nur personenbezogene Daten von **Beschuldigten** eines strafrechtlichen Ermittlungsverfahrens sowie von Betroffenen in einem Bußgeldverfahren erfaßt. Ferner sind enthalten die Daten von **Verdächtigen**, also von Personen, die nicht Beschuldigte sind, bei denen aber Anhaltspunkte dafür vorliegen, daß sie Täter oder Teilnehmer einer Straftat sind.

Tatverdächtige Kinder oder Personen, die mit Waffen oder Sprengstoffen Selbstmord verübt haben, werden in der Datei nicht erfaßt. Meine Stichproben haben nach Einsicht in die dazugehörenden Unterlagen stets zulässige, insbesondere erforderliche Datenspeicherungen erbracht. Soweit Jugendliche gespeichert waren, waren kürzere Speicherungsfristen vergeben.

Allerdings waren einige Erfassungsfehler festzustellen: es fehlten teilweise die **Aussonderungsprüffristen**. Da die Dateien jedoch noch nicht lange geführt waren, waren noch keine Aussonderungsprüffristen versäumt. Die Mängel sind inzwischen behoben.

SPUDOK-Datei gegen Glücksspielkriminalität

Zur wirksamen Bekämpfung der Glücksspielkriminalität hat das BLKA eine SPUDOK-Datei eingerichtet, in der die **Meldungen** der sachbearbeitenden Polizeidienststellen aufgenommen und ausgewertet werden. Zweck dieser SPUDOK-Datei ist insbesondere, relevante Straftäter und Objekte zu erkennen und Zusammenhänge zwischen Straftaten, auch im Hinblick auf mögliche organisierte Kriminalität aufzuzeigen. Außerdem sollen mit Hilfe der Datei Erkenntnisse für das ermittlungstaktische Vorgehen gewonnen werden.

In der Datei werden personenbezogene Daten von **Beschuldigten** und **Verdächtigen** einschlägiger Straftaten erfaßt. Erfaßt werden ferner **Veranstalter** von Spielen mit Geldgewinn im Sinne der Gewerbeordnung, die in Spielclubs oder ähnlichen Einrichtungen betrieben werden. Dieser Personenkreis, der mit verkürzter Speicherungsfrist erfaßt wird, ist in der Datei **besonders gekennzeichnet**.

Der Inhalt der Datei war nicht zu beanstanden. Allerdings konnte eine dateimäßige Aussonderungsprüfung bisher nicht durchgeführt werden, weil ein entsprechendes Speicherungsfeld fehlte. Aber auch diese Datei war noch nicht so lange in Betrieb, daß regelmäßige Löschungen erforderlich gewesen wären. Schutzwürdige Belange der von der Dateispeicherung Betroffenen waren deshalb noch nicht verletzt. Inzwischen hat das BLKA sichergestellt, daß bei al-

len Dateispeicherungen die nach der Errichtungsanordnung vorgesehenen Aussonderungsprüffristen festgesetzt und damit auch eingehalten werden können.

4.6 Bayerische Grenzpolizei

Im Berichtszeitraum habe ich eine mehrtägige generelle Prüfung beim Präsidium der Bayerischen Grenzpolizei und der Grenzpolizeiinspektion München/Riem sowie der dazugehörenden Grenzpolizeistation vorgenommen.

Beim **Präsidium** der Bayerischen Grenzpolizei habe ich **alle Dateien und Karteien** mit Ausnahme der Personaldateien/-karteien geprüft. Neben dem grenzpolizeilichen Aktennachweis (GAN), in dem spezielle grenzpolizeiliche Vorgänge gespeichert werden, sind besonders die beiden **SPUDOK-Dateien** zur Bekämpfung organisierter Kriminalität im grenzüberschreitenden Verkehr und über „gefälschte Dokumente" zu nennen.

Ich habe beim Präsidium der Bayer. Grenzpolizei ein überdurchschnittliches Datenschutzbewußtsein festgestellt. Die wenigen festgestellten Fehler betrafen Einzelfälle. Seit meiner letzten generellen Prüfung ist ein Großteil der vorhandenen **Karteien** aufgelöst worden.

SPUDOK-Datei „Organisierte Kriminalität im grenzüberschreitenden Verkehr"

Stichproben aus dieser Datei gaben keinen Anlaß zu datenschutzrechtlichen Anmerkungen. Die Vorgänge werden zentral beim Grenzpolizeipräsidium erfaßt. Die hierzu von den Inspektionen oder Stationen übersandten Unterlagen werden zentral verwahrt. Löschungen sind grundsätzlich nach kürzeren Fristen als im KAN vorgesehen.

Da der **Bundesgrenzschutz** als Bundesbehörde an den außerbayerischen Landesgrenzen die gleichen grenzpolizeilichen Aufgaben zu erfüllen hat wie die Grenzpolizei in Bayern, hat das Staatsministerium des Innern dem Antrag des Bundesministers des Innern, der **Grenzschutzdirektion in Koblenz** im Rahmen ihrer gesetzlichen Aufgaben die **Mitbenutzung der Datei** zu genehmigen, zugestimmt. Dies bedeutet, daß die Grenzschutzdirektion ebenfalls Erfassungen, Abfragen, Veränderungen und Löschungen in der Datei vornehmen kann. Die Grenzschutzdirektion bleibt für die Richtigkeit der Daten im eigenen Bereich verantwortlich (Besitzerprinzip). Dies erfordert eine **eindeutige Trennung der beiden Dateibestände** durch geeignete Suchbegriffe. Nach der Prüfung hat das Präsidium der Grenzpolizei umgehend für eine entsprechende Trennungsmöglichkeit gesorgt. Datenschutzrechtliche Bedenken gegen die Mitbenützung der Datei durch die Grenzschutzdirektion bestehen nicht, weil die Grenzschutzdirektion die gespeicherten Daten für denselben Zweck nutzt.

SPUDOK-Datei „Gefälschte Dokumente"

Stichproben aus dieser Datei bestätigten den positiven Gesamteindruck der Prüfung. Die Datei besteht zu einem wesentlichen Teil aus einer polizeilichen **Ermittlungshilfe zum Erkennen von Dokumentenfälschungen**. Beschriebene Fälschungsmerkmale erleichtern dem kontrollierenden Grenzpolizeibeamten die Arbeit „am Schlagbaum". Personenbezogene Daten werden nur im Zusammenhang mit erkannten Urkundenfälschungen und bei Verdacht von Urkundenfälschungen erfaßt.

Stichproben aus dem GAN habe ich anhand von Vorgängen der Grenzpolizeiinspektion und der Grenzpolizeistation München-Riem vorgenommen. Grundlage meiner Prüfung waren u.a. Dateiauswertungen aus folgenden Bereichen:

- Datensätze mit personengebundenen Hinweisen,
- besondere Merker, wie beispielsweise „internationale Tatbegehung",
- Kinder und über 70jährige,
- bestimmte Aussonderungsprüffristen.

Trotz einer Vielzahl von Stichproben bestand kein Anlaß zu Beanstandungen. Sowohl bei der Vergabe der Merker, als auch bei der Vergabe personengebundener Hinweise legt die Grenzpolizei offensichtlich einen strengen Maßstab an. Zweifel an der Berechtigung der Vergabe der einzelnen Daten bestanden nicht. Gleiches gilt für die Erfassung von Kindern, Jugendlichen und über 70jährigen.

Wie bei Prüfungen des Kriminalaktennachweises habe ich allerdings auch beim GAN fehlende Verfahrensausgänge festgestellt. Meine Anmerkungen im Zusammenhang mit KAN-Prüfungen gelten auch beim GAN: Erst mit Kenntnis des Verfahrensausgangs kann die Grenzpolizei letztlich die berechtigte Speicherung des Vorganges im GAN feststellen.

4.7 Einsatz von Personalcomputern

Nach den Planungen des Innenministeriums sollen Personalcomputer verstärkt am **Arbeitsplatz** zur Entlastung der Polizei von Routine- und Verwaltungsarbeiten eingesetzt werden. Sie sollen die Beamten bei der Gewinnung und dem Austausch von Informationen unterstützen und somit die Effizienz der Bayerischen Polizei insgesamt erhöhen.

Die Planungen des Innenministeriums sehen den Einsatz von Arbeitsplatzcomputern (APC) bei allen Polizeidienststellen vor. Die APC ermöglichen neben der **Übertragung von Nachrichten** und Daten insbesondere die umfassende **Bearbeitung von Vorgängen**. Es kommen **Mehrplatz-APC mit einheitlicher Softwareausstattung** landesweit zum Einsatz. Nur zur Unterstützung von Aufgaben, die einer speziellen Lösung bedürfen, will das Ministerium der Beschaffung spezieller Hard- und Software zustimmen. Dieses Vorgehen halte ich aus Gründen der Datensicherheit für notwendig, weil der unkontrollierte Einsatz von Software (im Einzelfall auch von Hardware) ausgeschlossen sein muß.

Das Staatsministerium des Innern hat am 1.7.1990 „Rahmenrichtlinien für Beschaffung, Einführung und Einsatz sowie Datenschutz und die Datensicherung von dezentralen Rechenanlagen (APC) bei der Bayerischen Polizei" erlassen. Ich hatte Gelegenheit, diese Rahmenrichtlinien vor Erlaß zu prüfen. Die Anforderungen des Datenschutzes und der Datensicherheit waren erfüllt. Die Planungen sehen vor, daß im Lauf der nächsten Jahre alle Polizeidienststellen mit APC ausgerüstet und miteinander **vernetzt** werden.

Neben der generellen Unterstützung bei der polizeilichen „Vorgangsbearbeitung" kann der APC in folgenden Anwendungsfällen eingesetzt werden:

Konkrete Ermittlungsfälle

Es handelt sich hier um eine ähnliche Anwendung des APC wie bei SPUDOK-Verfahren. Der APC-Einsatz dürfte aus Gründen der Speicherkapazität der APC jedoch nur bei kleineren Ermittlungsverfahren in Frage kommen. Hierfür ist der

APC-Einsatz vom Innenministerium **generell freigegeben** worden. Der erstmalige Einsatz dieses Verfahrens muß von den Polizeipräsidien zum Datenschutzregister gemeldet werden.

Personaldatenverwaltung

Auf dem APC werden Personaldaten der Bediensteten der Polizei im örtlichen Bereich verarbeitet, in der Regel von der Polizeiinspektion. Auch für diese Anwendung liegt eine **generelle Freigabe** des Innenministeriums vor.

Polizeiliche Gefahrenabwehr und Verfolgung von Straftaten und Ordnungswidrigkeiten

Unabhängig vom APC-Einsatz im konkreten Ermittlungsfall können in diesen Dateien personenbezogene Daten insbesondere von Beschuldigten, Verdächtigen und Betroffenen in Ordnungswidrigkeitenverfahren aufgenommen werden, wenn und soweit dies **zur Abwehr von Gefahren** für die öffentliche Sicherheit oder Ordnung oder zur **Durchführung und Dokumentation von Straf- und Bußgeldverfahren** erforderlich ist. Eingabe- und abfrageberechtigte Benutzer dieser Dateien sind (wie generell im APC-Verfahren) nur die mit der Sachbearbeitung betrauten Beamten und Angestellten der jeweiligen Polizeidienststelle, beschränkt auf die ihnen zugewiesenen Anwendungen. Auch dieses Verfahren hat das Innenministerium freigegeben. Alle im Rahmen dieser Freigabe errichteten Dateien sind zum Zeitpunkt des Verfahrenseinsatzes durch die Polizeipräsidien oder das Landeskriminalamt zum Datenschutzregister zu melden. Somit ist gewährleistet, daß ich von allen Anwendungen Kenntnis erhalte.

Meine Bedenken gegen diese Anwendung sind noch nicht ausgeräumt, weil die Auswirkungen für den Datenschutz derzeit nicht überschaubar sind. Mit der allgemein gehaltenen Beschreibung des Dateizweckes kann eine **unüberschaubare** und damit letztlich **unkontrollierbare** Anzahl von Dateien entstehen, bei denen überdies nicht ersichtlich ist, ob die Dateien zu repressiven oder präventiven Zwecken einerseits oder zu Zwecken der Vorgangsverwaltung andererseits genutzt werden. Endgültige Aussagen zu diesen Verfahren können erst getroffen werden, wenn erste Anwendungsfälle auch aus datenschutzrechtlicher Sicht geprüft sind.

4.8 Informationssystem der Bayer. Polizei (IBP) — Benutzerkontrolle und Protokollierung

Im 11. Tätigkeitsbericht habe ich unter der Überschrift „Neue Sicherungsmaßnahmen" über einen verbesserten „Anmeldemodus für polizeiliche Informationssysteme" und eine eigene „Datei zur Protokollierung von Anfragen" der Polizeibeamten an verschiedene Dateien berichtet. Nach meinen wiederholten Forderungen, die **Protokollierung von Benutzeraktivitäten** der Polizei zu verbessern, hatte das Innenministerium eine **Protokolldatei** eingerichtet, die beim Landeskriminalamt geführt wird.

Protokolliert wird **jede personenbezogene Abfrage** von einem Datenendgerät, das an das Informationssystem der Bayer. Polizei angeschlossenen ist,
- in einer polizeilichen **bayerischen** Datei (IBP)
- in einer polizeilichen **bundesweiten** Datei (INPOL) sowie
- in den grundsätzlich erschließbaren **nichtpolizeilichen** Dateien (Einwohnermeldeamtsdateien, Ausländerzentralregister, zentrales Verkehrsinformationssystem — ZEVIS —).

Den personenbezogenen Abfragen sind Abfragen mit besonderen Ordnungsmerkmalen gleichgestellt, die einen Personenbezug ermöglichen (z.B. amtliches Kennzeichen). Inzwischen werden auch „negative Fahndungsabfragen", also Abfragen zu Personen, zu denen keine Speicherung vorhanden ist, protokolliert.

Ob der neue Anmeldemodus oder die Einrichtung der Protokolldatei Auswirkungen auf das Auskunftsverhalten der Polizeibeamten gegenüber Privatpersonen hat, ist mir nicht bekannt. Fest steht jedoch, daß sich seit meinem letzten Tätigkeitsbericht kein Bürger mehr mit einer vermuteten mißbräuchlichen **Nutzung** polizeilicher Informationssysteme durch Polizeibeamte an mich gewandt hat. Es ist beabsichtigt, die Protokolleinträge eines bestimmten Stichtages auszuwerten und die Rechtmäßigkeit der Abfrage zu überprüfen.

4.9 Bürgereingaben

Der Schwerpunkt der Bürgereingaben lag in diesem Jahr bei **vermuteten oder bekannten Speicherungen** im Kriminalaktennachweis (KAN). In den meisten Anfragen vermuten die Bürger, sie würden im KAN als „Straftäter" gespeichert, weil sie in irgendeiner Form von polizeilichen Ermittlungen betroffen waren. Diese Sorgen sind oft unbegründet und zeigen, daß über Zweck und Inhalt des polizeilichen KAN bei den Bürgern noch große Unklarheit besteht. Viele Bürger haben für eine Speicherung im KAN kein Verständnis, wenn ein Anzeigeverfahren nicht zu einer Verurteilung führt. Das beruht auf einem Mißverständnis über Sinn und Zweck des KAN.

Der KAN ist nichts weiter als eine in Dateiform geführte Aufstellung der bei der Polizei geführten Kriminalakten über eine Person. Voraussetzung für das Führen einer Kriminalakte und die Aufnahme in den KAN ist, daß eine Person Beschuldigter einer Straftat oder einer erheblichen Ordnungswidrigkeit ist oder war, oder daß von einer Person aus anderen Gründen (z.B. wegen einer Vermissung) **künftig eine Gefahr ausgehen kann.** Deshalb ist der KAN auch keine „Verurteiltendatei", sondern nur eine „Verdächtigendatei". Darin besteht der wesentliche Unterschied zum Bundeszentralregister in Berlin. Seine Rechtsgrundlage hat der KAN nunmehr in Art. 38 Abs. 1 und 2 Polizeiaufgabengesetz. Danach kann die Polizei personenbezogene Daten in Akten oder Dateien speichern, verändern und nutzen, soweit dies zur Erfüllung ihrer Aufgaben, erforderlich ist. Die Polizei kann insbesondere personenbezogene Daten, die sie im Rahmen strafrechtlicher Ermittlungsverfahren oder von Personen gewonnen hat, die verdächtig sind, eine Straftat begangen zu haben, speichern, verändern und nutzen, soweit dies zur Gefahrenabwehr, insbesondere zur vorbeugenden Bekämpfung von Straftaten erforderlich ist.

Keinesfalls enthält der KAN Opfer von Straftaten, Geschädigte, Anzeigeerstatter, Zeugen oder Hinweisgeber. Daten dieser Personen befinden sich in den Akten, in der Vorgangsverwaltung oder in SPUDOK-Dateien.

Da der KAN **nur Personen enthält, die nach kriminologischer Erfahrung mit einer gewissen Wahrscheinlichkeit**

wieder Anlaß zu polizeilichen Maßnahmen geben werden, führt die Einstellung eines Verfahrens (ja nicht einmal ein Freispruch) nicht **automatisch** zur Löschung im KAN. Nur wenn **für die Polizei** bei Straftaten oder Ordnungswidrigkeiten der Tatverdacht entfällt, sind Speicherungen im KAN zu löschen und die dazugehörenden polizeilichen Unterlagen zu vernichten (so jetzt Art. 38 Abs. 2 Satz 2 PAG). Verfahrenseinstellungen wegen Geringfügigkeit oder mangels hinreichenden Tatverdachts oder aus formalen Gründen haben allenfalls Auswirkungen auf die Speicherungsdauer, nicht aber auf die rechtliche Zulässigkeit einer weiteren Speicherung im KAN, wenn aus den der Polizei vorliegenden Unterlagen aus deren Sicht **nachvollziehbar Restverdacht** bestehen bleibt. In diesem Fall kann der Datenschutzbeauftragte weder die Löschung der Daten aus dem KAN noch die Vernichtung von Unterlagen fordern, weil die Speicherung dem Polizeiaufgabengesetz entspricht.

Die Bürgereingaben waren jedoch nicht stets erfolglos. In einer Reihe von Eingaben konnte ich erreichen, daß die speichernde Polizeibehörde Dateispeicherungen und Unterlagen unter Berücksichtigung des Verfahrensausgangs nochmals überprüfte mit dem Ergebnis, daß sie die KAN-Speicherung und die Kriminalakten zur Erfüllung der polizeilichen Aufgaben nicht mehr für erforderlich hielt und sie daraufhin löschte bzw. vernichtete.

Bei Bürgereingaben lassen sich folgende Schwerpunkte feststellen:

- Auskunft über Speicherung in Polizeicomputern
- Beschwerden wegen vermuteter Speicherungen in Polizeicomputern
- Beschwerden wegen bekannter Speicherungen bei Polizeibehörden
- Eingaben zu Speicherungen von erkennungsdienstlichen Daten wie Fingerabdrucke und Lichtbilder
- Nutzung polizeilicher Dateien für „private Zwecke"
- Eingaben zu grenzpolizeilichen Dateiabfragen im grenzüberschreitenden Verkehr.

Auskunft über Speicherungen in Polizeicomputern

Nach Art. 6 BayDSG kann sich jedermann — unbeschadet des allgemeinen Petitionsrechts oder anderer Rechte — an den Landesbeauftragten für den Datenschutz mit dem **Vorbringen** wenden, daß bei der Verarbeitung seiner personenbezogenen Daten durch öffentliche Stellen seine schutzwürdigen Belange beeinträchtigt werden. Dies ist in der Regel dann der Fall, wenn der Bürger aufgrund eines bestimmten Vorfalls vermutet, zu Unrecht gespeichert zu sein oder wenn ihm die speichernde Polizeidienststelle auf seinen Auskunftsantrag eine Auskunft verweigert oder nicht vollständig erteilt.

Der **Landesbeauftragte ist aber nicht die erste Anlaufstelle**, wenn der Bürger nur erfahren will, welche Informationen die Polizei über ihn speichert. Denn beim Landesbeauftragten sind die interessierenden Daten nicht gespeichert. Ein Antrag auf Auskunft ist in erster Linie an die **speichernde (Polizeidienst-)Stelle** zu richten. Bürger, die nur Auskunft über die gespeicherten Daten wünschen, verweise ich deshalb an ihre örtlich zuständige Polizeidirektion oder an das Bayer. Landeskriminalamt.

Beschwerden wegen vermuteter Speicherungen

Gelegentlich wenden sich Bürger an mich und vermuten allgemein eine Dateispeicherung bei Polizeibehörden (in diesen Fällen zumeist auch bei Verfassungsschutzbehörden), wobei die Anhaltspunkte, die für eine solche Speicherung sprechen, entweder sehr vage sind oder gänzlich fehlen.

Diese zumeist wohl etwas überängstlichen Menschen meinen aufgrund von Vorgängen, die sie sich nicht erklären können (z.B. Nebengeräuschen bei Telefonaten, Beobachtung durch andere Menschen), daß Sicherheitsbehörden über sie Daten sammeln oder sie überwachen. Auch wenn die Vermutung der Speicherung oder Überwachung noch so unwahrscheinlich klingen mag, prüfe ich jeden Einzelfall. Erbringen meine Prüfungen keinen Hinweis auf Speicherungen oder Maßnahmen von Sicherheitsbehörden, teile ich dies dem Bürger mit, um seine Befürchtungen zu zerstreuen.

Beschwerden wegen bekannter Speicherungen

Manche Bürger erhalten nach einem Antrag auf Auskunft über die zu ihrer Person gespeicherten Daten von der Polizei die Bestätigung, daß sie wegen eines Vorganges gespeichert sind oder erfahren aus anderen Anlässen (z.B. im Verlauf einer Vernehmung wegen einer Beschuldigung in anderer Sache) von einer Datenspeicherung. Wendet sich daraufhin der Betroffene an mich, so prüfe ich die **rechtliche Zulässigkeit der bestehenden Speicherung** einschließlich der Datenerhebung. Wie bei den generellen Prüfungen sind auch bei Beschwerden bei den speichernden Stellen kaum Fehler festzustellen. Allenfalls wenn der Verfahrensausgang in polizeilichen Unterlagen fehlt und von der Polizeibehörde bei der sachbearbeitenden Staatsanwaltschaft ermittelt wird, ergibt sich im Einzelfall die Notwendigkeit einer Löschung von Daten bzw. Vernichtung von Unterlagen oder die Löschung/Vernichtung von Daten/Unterlagen nach einer verkürzten Frist.

Eingaben zu Speicherungen von erkennungsdienstlichen Daten wie Fingerabdrucke, Lichtbilder

Wegen des schwereren Rechtseingriffs haben hier die Betroffenen zumeist bereits vorher rechtsanwaltschaftliche Hilfe bemüht und in manchen Fällen die Bestätigung erhalten, daß vorhandene erkennungsdienstliche Unterlagen vernichtet werden oder wurden. In diesen Fällen **überwache ich den Vollzug des erteilten Bescheides**. Im ablaufenden Berichtsjahr habe ich keine unzulässigen Speicherungen erkennungsdienstlicher Daten in der sogenannten „Erkennungsdienstdatei" im Informationssystem der Bayer. Polizei (IBP) festgestellt. Für einige Bürger konnte ich die vorzeitige Löschung der Daten und die Vernichtung der Unterlagen erreichen, weil die Polizei auch hier unter Berücksichtigung des Einzelfalls die weitere Aufbewahrung der Unterlagen nicht mehr für erforderlich gehalten hat. Dies zeigt, daß die Polizei bemüht ist, nur relevante Daten bereitzuhalten.

Nutzung polizeilicher Daten für „private Zwecke"

Gelegentlich werde ich gefragt, ob Polizeibeamte in bestimmten Fällen **privat Auskunft aus polizeilichen Dateien** erholen dürfen. Bei rein privaten Anlässen ist ein Polizeibeamter hinsichtlich der Nutzung vertraulicher Informationssysteme zu behandeln **wie jeder andere Bürger**. Er darf sich aus den Dateien zu persönlichen Zwecken nicht selbst bedienen. Beispielsweise verstößt ein Polizeibeamter gegen datenschutzrechtliche Bestimmungen, wenn er die „Dame seiner Wahl" oder einen künftigen Mieter ohne dienstlichen

Anlaß einer Dateiprüfung unterzieht. Zur Verhinderung unzulässiger Auskünfte wurde die Protokolldatei eingeführt.

4.10 Einzelfälle

4.10.1 Kopieren von Ausweisen von Besuchern des Bayerischen Landtages

Aufgrund eines Hinweises im Juni 1990 habe ich festgestellt, daß im Bayer. Landtag bei einer Besuchergruppe die abgegebenen Personalausweise oder Pässe abgelichtet worden sind.

Bereits im November 1988 hatte mir das Landtagsamt, das im Bayerischen Landtag das Hausrecht ausübt, auf meine Anfrage mitgeteilt, daß über Besucher des Bayerischen Landtags Daten, insbesondere Personalien, weder erhoben noch gespeichert würden. Die Pförtner des Landtagsamts seien angewiesen, bei Einzelbesuchen eine Identitätsprüfung anhand eines amtlichen Ausweises vorzunehmen. Dieser würde an der Pforte während der Verweildauer des Besuchers im Maximilianeum hinterlegt. Schriftliche Aufzeichnungen würden nicht angefertigt. Das Landtagsamt teilte mir damals weiter mit, daß bei **angemeldeten** Besuchergruppen auf eine Identitätsprüfung verzichtet würde. Der jeweilige Gruppenleiter würde eine Sichtkontrolle vornehmen, damit nur die Mitglieder der Gruppe das Haus betreten. Gegen diese Regelung hatte ich keine datenschutzrechtlichen Bedenken erhoben, da schutzwürdige Belange der Landtagsbesucher nicht beeinträchtigt werden.

Am 23. Januar 1990 trafen Besucher für den Wackersdorf-Untersuchungsausschuß des Bayer. Landtages an der Westpforte ein. Alle Besucher mußten, da sie nicht zuvor als Gruppe angemeldet waren, wie Einzelpersonen ihre Personalpapiere an der Westpforte hinterlegen, wie es die Sicherungsmaßnahmen des Bayer. Landtags vorsehen. Die Personalpapiere wurden danach von einem Mitarbeiter des Landtagsamtes abgelichtet und später einem Polizeibeamten der für den Bayer. Landtag zuständigen Polizeiinspektion ausgehändigt. Nach Erklärung des Polizeibeamten hat dieser die Kopien der Personalausweispapiere zur Polizeidienststelle mitgenommen und dort im Reißwolf vernichtet, ohne vorher irgendwelche Stellen zu informieren.

Dieser Sachverhalt steht fest durch Befragen von Mitarbeitern des Landtagsamtes und der Polizei.

Meine Befragungen konnten jedoch nicht eindeutig Klarheit schaffen, wer letztlich die Verantwortung für die Ablichtung der Personalausweise trägt. Nach Darstellung des leitenden Polizeibeamten hat dieser einem Mitarbeiter des Landtagsamtes lediglich anheimgestellt, Kopien der Ausweise für den Fall zu fertigen, daß das Landtagsamt der Ansicht sei, diese im Rahmen der Ausübung des Hausrechts für eigene Zwekke zu benötigen. Nach Darstellung der Vertreter des Landtagsamtes seien die Ablichtungen der Ausweise auf Bitten eines der vor dem Sitzungssaal des Untersuchungsausschusses anwesenden Polizeibeamten gefertigt worden.

Nicht geklärt werden konnte die Frage, unter welchen Umständen die Kopien der Personalausweise letztlich in den Besitz der Polizei gelangt sind.

Wer auch immer die Ablichtung der Ausweispapiere und die spätere Aushändigung an die Polizei veranlaßt hat: Aus datenschutzrechtlicher Sicht steht fest, daß weder die Ablichtung der Personalausweispapiere der Besucher des Bayer. Landtages noch die Übergabe dieser Kopien an einen Polizeibeamten für die gesetzlich zugewiesene Aufgabenerfüllung des Landtagsamtes oder der Polizei erforderlich waren. Die Verarbeitung dieser personenbezogenen Daten habe ich sowohl gegenüber dem Landtagsamt als auch gegenüber dem Staatsministerium des Innern als unzulässig bezeichnet.

Zu klären war ferner, ob die personenbezogenen Daten der Landtagsbesucher vor ihrer Vernichtung im Reißwolf an andere Stellen übermittelt worden waren. Meine umfangreichen Prüfungen beim Landesamt für Verfassungsschutz (Registratursystem und nachrichtendienstliches Informationssystem NADIS), dem Landeskriminalamt (Staatsschutzabteilung — Datei APIS) und dem Polizeipräsidium München (Vorgangsverwaltung, Kriminalaktennachweis, Staatsschutzkartei im Staatsschutzdezernat) haben keine Anhaltspunkte für eine Übermittlung der abgelichteten Ausweisdaten an diese Behörden oder für eine Speicherung bei ihnen erbracht.

4.10.2 Verdeckte Datenerhebung durch einen Polizeibeamten bei der Gründungsversammlung einer Aktionsgemeinschaft gegen die Autobahn A 6

Am 14.02.1989 fand in einer Gaststätte eine öffentliche Versammlung der „Aktionsgemeinschaft zum Schutz der Oberpfälzer Heimat vor der A 6" statt. Unter den 180 Teilnehmern befand sich auch ein Beamter der Zivilen Einsatzgruppe (ZEG) der Polizei. Der Beamte, der sich dem Versammlungsleiter nicht zu erkennen gab, notierte sich im Laufe der Versammlung die Redner, die bei der Veranstaltung auftraten, und zwar den Familiennamen sowie die Funktion der Redner in den einzelnen Verbänden.

Der Bericht des ZEG-Beamten wurde in der Polizeidirektion in der Akte „Einsatz" als Bestandteil der polizeilichen Aktenverwaltung abgelegt. Außerdem übersandte die Polizeidirektion den Bericht einer Polizeiinspektion zur Kenntnisnahme. Der Bericht wurde dort in einem Ordner abgelegt, in dem sich bis zu diesem Zeitpunkt lediglich Pressemeldungen über den geplanten Bau der A 6 befanden.

Das Staatsministerium des Innern hat zu diesem Vorgang festgestellt, daß sich die Polizei in dieser Angelegenheit nicht richtig verhalten habe. Diese Auffassung teile ich. Für eine verdeckte Beobachtung der Versammlung bestand kein Anlaß, weil der Polizei **keine tatsächlichen Anhaltspunkte für die Annahme vorlagen, daß von der Versammlung erhebliche Gefahren für die öffentliche Sicherheit oder Ordnung ausgehen könnten**. Deshalb waren die verdeckte Beobachtung der Veranstaltung, das Notieren der Namen, der Funktionen und Äußerungen von Teilnehmern, die Aufnahme der Daten in Berichte, die Weitergabe dieser Berichte an andere Dienststellen sowie die Aufbewahrung dieser Berichte nicht zulässig. Ich habe deshalb das Unkenntlichmachen der personenbezogenen Daten in den Berichten oder die Entfernung der Berichte aus den operativen Arbeitsunterlagen der Polizei gefordert. Dies ist inzwischen nach Mitteilung des Innenministeriums geschehen.

Nach Auffassung des Staatsministeriums des Innern stellt dieser Vorgang eine Ausnahme dar. Ich werde bei künftigen Kontrollen von Polizeidienststellen mein besonderes Augenmerk auf polizeiliche Unterlagen im Zusammenhang mit ähnlichen Projekten richten und die Einhaltung der Vorschriften

über die Datenerhebung und -verarbeitung nach dem Versammlungsgesetz überwachen.

5. Verfassungsschutz

Am 1. November 1990 ist das neue Bayerische Verfassungsschutzgesetz in Kraft getreten. Der Bundesgesetzgeber hat endlich nach wiederholtem Anlauf das Bundesverfassungsschutzgesetz, das Gesetz über den Bundesnachrichtendienst und das Gesetz über den militärischen Abschirmdienst verabschiedet. Damit sind die **Informationsbeschaffung und die Datenverarbeitung der Nachrichtendienste in Bayern und im Bund auf eine verfassungsgemäße gesetzliche Grundlage** gestellt.

Am Gesetzgebungsverfahren zum Bayerischen Verfassungsschutzgesetz habe ich mich mit schriftlichen und mündlichen Stellungnahmen in Landtag und Senat beteiligt.

Ein weiterer Schwerpunkt des Datenschutzes im Bereich Verfassungsschutz war wie in den Vorjahren eine **mehrtägige allgemeine Prüfung** beim Landesamt für Verfassungsschutz. Außerdem hatte ich die Datenverarbeitung des Landesamts aufgrund einiger **Eingaben** zu kontrollieren.

5.1 Bayerisches Verfassungsschutzgesetz

Mit dem neuen Bayerischen Verfassungsschutzgesetz hat der Gesetzgeber noch rechtzeitig vor Ablauf der Übergangsfrist eine neue **tragfähige Grundlage** für die Datenerhebung und -verarbeitung des Landesamts für Verfassungsschutz geschaffen.

Im Gesetzgebungsverfahren konnte der Datenschutz noch weiter verbessert werden:

- Besonders hervorzuheben ist das **Auskunftsrecht** des Bürgers gegenüber dem Landesamt für Verfassungsschutz. In Art. 11 Abs. 2 wurde für Personen, die einer Sicherheitsüberprüfung unterzogen werden oder zu denen das Landesamt amtliche Auskünfte erteilt hat, ein Anspruch auf Auskunft über die übermittelten Daten eingeräumt. Hat in den übrigen Fällen eine Person ein besonderes Interesse an einer Auskunft über ihre gespeicherten Daten, so entscheidet das Landesamt nach **pflichtgemäßem Ermessen** über das Auskunftsbegehren. Jedem Bürger steht ein Recht auf fehlerfreie Ermessensentscheidung zu. Wird die Auskunftserteilung abgelehnt, so ist der Bürger darauf hinzuweisen, daß er sich an den Landesbeauftragten für den Datenschutz wenden kann, dem Auskunft zu erteilen ist. Mit dem auf diese Weise ausgestalteten Auskunftsrecht des Bürgers ist den Anforderungen der Verfassung entsprochen worden.
- Für den **verdeckten Einsatz** besonderer technischer Mittel zur Informationsgewinnung **in Wohnungen** gelten die gleichen Vorkehrungen wie bei Abhörmaßnahmen nach dem Gesetz zu Art. 10 Grundgesetz.
- Meiner Forderung, daß durch nachrichtendienstliche Mittel **unzulässigerweise erhobene Daten** 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, sowie der Forderung nach einer Regelung über **Zufallsfunde** ist mit der Ergänzung der Begründung wenigstens teilweise entsprochen worden.

Tiefgreifende Eingriffe des Staates in Bürgerrechte erfordern eine **effektive Kontrolle**. Durch das neue Gesetz sind die Befugnisse des Landesamts zur Erfüllung seiner Aufgaben präziser und teilweise restriktiver geregelt worden. Insbesondere die **Anwendung nachrichtendienstlicher Mittel** kann zu tiefen Eingriffen in die Persönlichkeitsrechte führen, deren Zulässigkeit der Betroffene naturgemäß kaum selbst nachprüfen und gegen die er sich deshalb nur schwer zur Wehr setzen kann. Um so notwendiger ist deshalb eine wirksame Kontrolle der Informationserhebung und -verarbeitung. Die G-10-Kommission und die neu eingerichtete parlamentarische Kontrollkommission sowie die Gerichte können die Kontrolle des Einsatzes nachrichtendienstlicher Mittel nicht in vollem Umfang gewährleisten, so daß der Landesbeauftragte für den Datenschutz in diesem sensiblen Bereich ergänzend tätig werden muß.

Zur Erleichterung meiner Kontrolltätigkeit hatte ich im Gesetzgebungsverfahren vorgeschlagen, daß das Landesamt den Einsatz nachrichtendienstlicher Mittel, zumindest den Einsatz geheimer Mitarbeiter und besonderer technischer Mittel bei nicht nur geringfügigen Eingriffen in die Privatsphäre **aktenkundig** macht und die **Aufzeichnungen zur Kontrolle** durch den Landesbeauftragten vorhält. Leider wurde mein Vorschlag nicht aufgegriffen, so daß die unverzichtbare Kontrolle nur durch **mehr Kontrollaufwand** erreicht werden kann.

Das neue Bayerische Verfassungsschutzgesetz macht die grundlegende **Überarbeitung der behördeninternen Richtlinien und Arbeitsanweisungen** erforderlich. Ferner müssen die vorhandenen Datei- und Karteispeicherungen einschließlich der dazugehörenden Personen- und Sachakten nach und nach im Rahmen der laufenden Sachbehandlung auf ihre Vereinbarkeit mit dem neuen Recht überprüft werden.

5.2 Reaktion auf den Prüfbericht 1989

Auf meinen letztjährigen Prüfungsbericht hat das Landesamt erfreulich positiv reagiert: Beim Landesamt werde das Erkenntnisdatum, nach dem sich die Aussonderungsfrist berechnet, künftig einheitlich an das Datum des letzten relevanten Ereignisses anknüpfen. NADIS-Speicherung und Vorgangsverwaltung würden strikt getrennt. Alle Anregungen zur Durchführung des Datenschutzes bei Sicherheitsüberprüfungen wurden übernommen. Arbeitsanweisungen für die Führung von Karteien sollen, soweit noch nicht vorhanden, erstellt werden. Alle Extremistenkarteien würden bereinigt.

5.3 Generelle Prüfung 1990

Im Berichtszeitraum habe ich beim Landesamt wieder über zwei Tage die dort geführten Dateien und Karteien stichprobenweise überprüft. Anhand einer vorab übersandten Liste mit über 70 Namen wurden die Speicherungen in der **Registraturdatei** und im **Nachrichtendienstlichen Informationssystem** (NADIS) geprüft. Zu den gespeicherten Namen waren die dazugehörenden Personen- und/oder Sachakten beigezogen worden. Ferner wurden anhand der Registratureintragungen weitere Prüfungen von NADIS-Speicherungen und der dazugehörenden Personen- und Sachakten vorgenommen.

Außerdem habe ich eine Anzahl von **Karteien** aus der vom Landesamt übersandten Zusammenstellung mit dem

Schwerpunkt „Extremismus links" und „Extremismus rechts" kontrolliert. Mit der Überprüfung von **Übersiedlervorgängen** wurde die diesjährige Kontrolle abgeschlossen. Während der Prüfung erhielt ich umfassende Auskünfte auf alle gestellten Fragen und Einsicht in alle erforderlichen Unterlagen und Belege.

5.3.1 NADIS

Die umfangreiche Prüfung von NADIS-Speicherungen hat zu **keinen Beanstandungen** Anlaß gegeben. Noch geklärt werden muß die Frage, ob das Landesamt bei einer Sicherheitsüberprüfung noch weitere Ermittlungen anstellen darf, wenn sich aufgrund einer NADIS-Speicherung bereits Sicherheitsbedenken ergeben haben. Noch konsequenter beachtet werden müssen die Vorschriften über den **Beginn der Aussonderungsprüffristen**. Erfreulicherweise konnten Verwaltungsvorgänge in NADIS nicht mehr festgestellt werden. Auf ein Versehen dürfte zurückzuführen sein, daß in einem Fall die Akte zu einer NADIS-Speicherung vernichtet, die NADIS-Speicherung selbst aber nicht gelöscht war.

In NADIS gespeichert wegen des Verdachts geheimdienstlicher Agententätigkeit war ein Bürger, weil ein anonymer Hinweis vorlag, er habe bei einer Feier unter Alkoholeinfluß geäußert, daß er von der DDR angeworben worden sei. Obwohl das Verfahren vom Bayerischen Obersten Landesgericht eingestellt worden war, war hier eine 15jährige Speicherung wegen des verbliebenen Restverdachts vorgesehen. Im Hinblick auf die deutsche Einheit und wegen des sehr zweifelhaften Tatverdachts habe ich eine Löschung der Speicherung empfohlen.

In NADIS war ferner ein Übersiedler aus der DDR gespeichert, der erst wenige Monate vor Öffnung der Grenzen im Herbst 1989 in die Bundesrepublik eingereist war. Der Aufgabenbereich des Amtes war eröffnet. Wenn auch im konkreten Fall die Speicherung vertretbar, und auch der Verweis auf die frühere Datei ADOS auf dem Erfassungsblatt im Personenakt nicht zu beanstanden waren, so habe ich doch wegen dieses Vorgangs das Landesamt gebeten, **im Hinblick auf die deutsche Einheit alle NADIS-Speicherungen von Übersiedlern aus der DDR baldmöglichst auf ihre weitere Erforderlichkeit** zu **überprüfen**. Diese Empfehlung gilt für alle Speicherungen in Dateien und Karteien sowie für die Führung von Akten, soweit sie auf Grund des Umbruchs im Osten nicht mehr benötigt werden. Man muß sich allerdings auch darüber im klaren sein, daß man hier **nicht überstürzt** Informationen vernichten darf, sondern wie auch sonst die **Aufgaben des Landesamts im Auge zu behalten** hat, zumal es genug Anzeichen gibt, daß der Staatssicherheitsdienst der ehemaligen DDR noch nicht zerschlagen ist.

5.3.2 Karteien

Einen breiten Raum der diesjährigen Prüfung nahm die Kontrolle von Karteien ein. Das Landesamt hat mir hierzu ein vollständiges Verzeichnis der von ihm geführten Dateien und Karteien vorgelegt. Geprüft habe ich insbesondere Karteien in den Bereichen **Linksextremismus** und **Rechtsextremismus**.

Entsprechend meiner Forderung im 11. Tätigkeitsbericht hat das Landesamt die Karteien überarbeitet. Obwohl die behördeninternen Aussonderungsprüfungen noch nicht abgeschlossen waren, war der Bestand einiger Karteien seit der Einsichtnahme im Jahr 1989 schon erheblich reduziert worden.

Die Prüfung der Karteien hat allerdings auch diesmal die Notwendigkeit bestätigt, daß den Sachbearbeitern **klare Arbeitsanweisungen** zur Hand gegeben werden müssen, damit eine einheitliche, ermessensfehlerfreie, am Grundsatz der Erforderlichkeit ausgerichtete Informationsverarbeitung erreicht wird.

Die nachhaltigen Anstrengungen des Landesamts, die Datenbestände zu aktualisieren und auf das für die Aufgabenerfüllung erforderliche Maß zu beschränken, waren bei der Datenschutzkontrolle unverkennbar. Die Erfahrungen aus behördeninternen Karteiprüfungen und aus früheren Datenschutzkontrollen sollten bei der geplanten Umstellung von Karteien auf Dateien genutzt werden.

Vereinzelt wurde festgestellt, daß in den Karteien Daten der Vorgangsverwaltung eingetragen waren. Teilweise waren die Speicherungen wegen möglicher Namensverwechslungen, fehlender Mitteilungen über den Ausgang von strafrechtlichen Verfahren oder nicht ausreichend belegten Restverdachts nach Verfahrenseinstellung oder wegen fehlender Karteirelevanz nicht nachvollziehbar. Der Überprüfung bedarf ferner die bei der Führung mancher Kartei geübte Praxis, nach Ablauf der festgesetzten Aussonderungsprüffristen die Speicherung ohne weitere aktuelle Erkenntnisse automatisch zu verlängern. Eine solche automatische Verlängerung widerspricht dem Sinn von Aussonderungsprüffristen. Eine Verlängerung kann nur in konkret begründeten Einzelfällen oder ausnahmsweise bei bestimmten Fallgruppen in Frage kommen.

In einer Anzahl von Fällen sind **Kfz-Halter** in der Kartei gespeichert, obwohl trotz Indizien nicht eindeutig feststand, daß die betroffene Person selbst beispielsweise zu einer einschlägigen Veranstaltung gefahren ist und/oder der Fahrer daran teilgenommen oder nur in der Nähe der Veranstaltung geparkt hat. Da hier in Einzelfällen nicht auszuschließen ist, daß bei der Halterspeicherung völlig unbeteiligte Personen verdächtigt werden, ist in solchen Fällen eine **genauere Prüfung der Person vor der Speicherung** notwendig. Soweit eine Prüfung nicht möglich ist, kann nur eine wesentlich verkürzte Speicherungsfrist in Betracht kommen.

5.3.3 Sonderprüfungen

Nach der Ablichtung der Personalausweise und Pässe einer Gruppe von Besuchern des Bayerischen Landtags im Januar 1989 war der Verdacht geäußert worden, die Ablichtungen seien dem Landesamt zugeleitet worden. Eine Überprüfung der Registraturdatei und von NADIS hat jedoch ergeben, daß im Zusammenhang mit diesem Besuch beim Landesamt keine personenbezogenen Daten gespeichert worden sind.

Ferner habe ich geprüft, ob das Landesamt im Zusammenhang mit dem Volksbegehren „das bessere Müllkonzept" personenbezogene Daten gespeichert hat. Auch hier konnten keinerlei Anhaltspunkte festgestellt werden, daß Personen gespeichert oder Listen mit Unterschriften für das Volksbegehren registriert seien.

5.4 Konsequenzen aus der Wiedervereinigung

Das Landesamt für Verfassungsschutz hat bereits vor dem 3. Oktober Überlegungen angestellt, welche Auswirkungen die Wiedervereinigung auf die Arbeit des Landesamts für Verfassungsschutz und damit auch auf die Dateispeicherung haben kann. Zu den Überlegungen gehörte auch die Überprüfung der einschlägigen Dateien/Karteien auf ihre

weitere Erforderlichkeit im Hinblick auf die deutsche Einheit. Wie jedoch die Erfahrungen bis in den Herbst 1990 belegen, wäre es falsch, unter dem Gesichtspunkt der Erforderlichkeit überstürzt und voreilig Informationen zu vernichten. Vielmehr wird man, wie auch sonst bei der Frage nach der weiteren Speicherung von Informationen, die Aufgaben des Verfassungsschutzes stets im Auge behalten müssen.

5.5 Auflösung der Datei „Adressen- und Objektedatei Ost" (ADOS)

Angesichts der politischen Entwicklung in der vormaligen DDR und in Osteuropa hatte der Bundesminister des Innern im März 1990 festgestellt, daß die Datei ADOS für das Bundesamt für Verfassungsschutz nicht mehr notwendig sei. Er hat daraufhin beschlossen, die gespeicherten Daten zu löschen und die dazu noch vorhandenen Unterlagen zu vernichten. In der Datei waren personenbezogene Daten von Aus- und Übersiedlern aus der vormaligen DDR und aus Osteuropa gespeichert.

Das Landesamt hatte zu keiner Zeit über einen eigenen Datenbestand in ADOS verfügt, sondern lediglich Daten in der Datei des Bundes erfaßt. Nach der Entscheidung des Bundesministers des Innern wurden auf Weisung des Staatsministeriums des Innern auch die vom Landesamt erfaßten Daten gelöscht. Nach Mitteilung des Amtes sind auch alle ausgefüllten bayerischen ADOS-Erfassungsvordrucke vernichtet. Hinweise in den Akten auf frühere Erfassungen in der Datei ADOS werden vom Landesamt für Verfassungsschutz im Zuge routinemäßiger Sachbearbeitung vernichtet, soweit sie nicht im Rahmen der gesetzlichen Aufgaben des Amtes auch weiterhin benötigt werden.

5.6 Bürgereingaben

Die Mehrzahl der Eingaben betraf wiederum Fälle, bei denen die **Vermutungen der Bürger**, beim Landesamt gespeichert zu sein, unbegründet waren. Manche Eingabenführer wollten sich anscheinend zur eigenen Beruhigung nur vergewissern, daß sie beim Landesamt nicht gespeichert sind. Andere glaubten, aus ihnen nicht erklärbaren Umständen oder aus einem konkreten Anlaß auf eine Speicherung schließen zu müssen. Die im Einzelfall erteilte Auskunft, daß der Verfassungsschutz von ihnen keine Notiz genommen habe, hat sicherlich zur Beruhigung und Vertrauensbildung beigetragen.

In einigen Fällen allerdings waren über die Eingabenführer Speicherungen vorhanden. Meine Überprüfungen anhand der Akten und der Stellungnahmen des Landesamts führten zum Ergebnis, daß die Speicherungen nicht zu beanstanden waren, weil der gesetzliche Aufgabenbereich des Landesamts eröffnet war, eine gesetzliche Befugnis für Datenerhebung und -speicherung gegeben und die weitere Speicherung notwendig war. Davon abgesehen nimmt das Landesamt regelmäßig Eingaben zum Anlaß für interne Relevanzprüfungen. Diese führten in einigen Fällen zu dem Ergebnis, daß eine Speicherung nicht mehr benötigt wurde und so vorzeitig gelöscht und die dazugehörenden Unterlagen vernichtet werden konnten.

Einige Eingabenführer wollten über mich erfahren, **welche Gründe** bei der ihnen bekannten Sicherheitsüberprüfung zur Äußerung von Sicherheitsbedenken durch das Landesamt gegenüber dem Arbeitgeber maßgebend waren und ob diese Sicherheitsbedenken gerechtfertigt waren. Hier prüfe ich, **ob die Äußerung des Landesamts im Rahmen seines Beurteilungsspielraums rechtlich nachvollziehbar** ist. Bei den überprüften Vorgängen waren die Sicherheitsbedenken durch mehrere Straftaten begründet, die auch den Eingabeführern bekannt waren.

Manche Eingabenführer vermuteten eine Sicherheitsüberprüfung mit für sie nachteiligem Ausgang, weil sie bei Bewerbungen aus ihnen nicht erklärlichen Gründen immer wieder abgelehnt worden sind. Solche Eingaben sind jedoch rückläufig, weil sich offensichtlich die auf die Anordnung des Staatsministeriums des Innern beruhende Praxis bereits herumgesprochen hat, daß Sicherheitsüberprüfungen nur nach vorheriger Einwilligung durchgeführt werden.

Ein Eingabeführer beklagte sich darüber, das Landesamt habe ihn gegenüber seinem Arbeitgeber zu unrecht der Mitgliedschaft in der marxistischen Gruppe bezichtigt. Meine Einsichtnahme in die Unterlagen beim Landesamt bestätigte jedoch die Verbindung des Eingabeführers zur marxistischen Gruppe. Auch wenn die nachgewiesenen Kontakte schon längere Zeit zurücklagen, war die Speicherung im Hinblick auf die konspirative Vorgehensweise der marxistischen Gruppe, die im bayerischen Verfassungsschutzbericht als verfassungsfeindliche Gruppierung aufgeführt ist, nicht zu beanstanden. Auch die Unterrichtung des Arbeitgebers war gerechtfertigt, weil sie aus der Aufgabenstellung des Landesamts nach Art. 2 Abs. 1 Nr. 1 des Gesetzes über die Errichtung eines Landesamts für Verfassungsschutz geboten erschien.

Andere Bürger wandten sich an mich, weil sie nach dem Abheben des Telefonhörers Knacksgeräusche zu hören glaubten und daraus auf Aktivitäten von Geheimdiensten schlossen. Zur Überprüfung von Abhörmaßnahmen des Landesamts ist jedoch nicht der Landesbeauftragte für den Datenschutz, sondern die Kommission zu Art. 10 Grundgesetz, die im Bayerischen Landtag besteht, zuständig. Soweit der Bundesverfassungsschutz oder eine andere Bundesstelle vermutet wird, wäre eine Anfrage an die G-10-Kommission des Bundestags oder an den Bundesbeauftragten für den Datenschutz zu richten.

6. Justiz

6.1 Gesetzgebung

Obwohl der Berichtszeitraum das Jahr vor der Bundestagswahl umfaßt, in dem erfahrungsgemäß die angekündigten Gesetzgebungsvorhaben verwirklicht werden, gibt es über erlassene Justizgesetze wenig zu berichten.

6.1.1 Strafverfahrensänderungsgesetz (StVÄG) 1989

Wie ich bereits im 11. Tätigkeitsbericht dargelegt habe, erfordert die neuere Rechtsprechung des Bundesverfassungsgerichts zum Grundrecht auf informationelle Selbstbestimmung **gesetzliche Grundlagen für neuartige strafprozessuale Ermittlungsmethoden**. Regelungsbedürftig sind auch einige hergebrachte Methoden, die Verarbeitung und Nutzung polizeilicher Informationen im Strafverfahren, das Akteneinsichtsrecht sowie die Verwendung von polizeilichen Informationen aus Strafverfahren für die Gefahrenabwehr.

Leider hat die Bundesregierung auch im Berichtsjahr — sieben Jahre nach dem Volkszählungsurteil — noch keinen Gesetzentwurf ins Gesetzgebungsverfahren eingebracht. Angesichts der teilweise tiefen Eingriffe strafprozessualer Ermittlungsmethoden in das Persönlichkeitsrecht ist diese Zögerlichkeit für die Bürger nicht länger hinnehmbar. Für einen Teil der Datenerhebungen im Ermittlungsverfahren fehlt es an einer dem Gesetzesvorbehalt entsprechenden normenklaren Rechtsgrundlage. Es gibt keine „vorkonstitutionellen" Befugnisse der Strafverfolgungsorgane. Seit dem Volkszählungsurteil des Bundesverfassungsgerichts von 1983 ist klar, daß der Gesetzgeber Teile der Datenerhebung in Verfahren von Polizei und Justiz auf eine gesetzliche Grundlage stellen muß. Die Übergangsfrist, welche dem Gesetzgeber zur Behebung eines als verfassungswidrig erkannten Zustandes eingeräumt ist, dürfte in Kürze ablaufen. Wünschenswert wäre es, wenn das Bundesverfassungsgericht alsbald Gelegenheit bekäme, die Verfassungsrechtslage verbindlich zu klären.

6.1.2 Entwurf eines Gesetzes zur Bekämpfung des illegalen Rauschgifthandels und anderer Erscheinungsformen der Organisierten Kriminalität (OrgKG)

Zur wirksameren Bekämpfung der Rauschgiftkriminalität und anderer Erscheinungsformen des organisierten Verbrechens ist neben anderen Maßnahmen die Verbesserung des rechtlichen Instrumentariums der Strafverfolgungsbehörden unerläßlich. Mit diesem Ziel hat der **Bundesrat** am 11. Mai 1990 **ohne Gegenstimme** bei nur zwei Enthaltungen den Entwurf eines Gesetzes zur Bekämpfung des illegalen Rauschgifthandels und anderer Erscheinungsformen der Organisierten Kriminalität beschlossen und ins Gesetzgebungsverfahren gebracht.
Neben der Einführung einer Vermögensstrafe, erweiterter Möglichkeiten zur Einziehung von Vermögensgegenständen, der Einführung eines Straftatbestandes der „Geldwäsche" und verschiedener Strafverschärfungen enthält der Entwurf eine Reihe **strafverfahrensrechtlicher Eingriffe**, die im Hinblick auf den Schutz der Bürger von Bedeutung sind.

Der Gesetzentwurf regelt unter anderem:

- den Einsatz Verdeckter Ermittler (Polizeibeamte unter einer Legende).
- den verdeckten Einsatz technischer Mittel (Lichtbilder, Bildaufzeichnungen, besondere Sichthilfen und akustische Überwachungsgeräte).
- die Rasterfahndung, den Datenabgleich und die Ausschreibung zur polizeilichen Beobachtung.
- die Erweiterung der Telefonüberwachung auf Bandenkriminalität und zur Abwehr einer gegenwärtigen Gefahr für Leib, Leben und Freiheit einer Person.

6.1.3 Justizmitteilungsgesetz (JuMiG)

Der Bundesminister der Justiz hat einen weiteren Referentenentwurf für ein Gesetz über Mitteilungen der Justiz von Amts wegen in Zivil- und Strafsachen vorgelegt. Damit setzt er die Bemühungen fort, die Übermittlung der sensiblen personenbezogenen Daten im Justizbereich, die bisher noch aufgrund von Verwaltungsvorschriften (MiStra und MiZi) stattfindet, auf die gebotene gesetzliche Grundlage zu stellen.

Der Entwurf soll die gesetzliche Grundlage schaffen für die von Amts wegen vorzunehmende Übermittlung personenbezogener Daten für diejenigen Fälle, in denen bereichsspezifische Datenübermittlungsregelungen fehlen. Dabei schafft der Entwurf lediglich **Zulässigkeitsvoraussetzungen für die Datenübermittlungen**.

In meiner Stellungnahme gegenüber dem Staatsministerium der Justiz habe ich auf folgende datenschutzrechtliche Anforderungen aufmerksam gemacht:

- Die Verwendung von **Generalklauseln**, die erst durch Verwaltungsvorschriften konkretisiert werden sollen, sollte eingeschränkt werden, damit bereits aus dem Gesetz selbst entnommen werden kann, wann eine Datenübermittlung statthaft ist.
- Die Anordnung der Mitteilung sollte — jedenfalls in besonders sensiblen Bereichen wie vor Klageerhebung, vor Rechtskraft einer Entscheidung, in Jugendsachen — dem Staatsanwalt oder dem Richter vorbehalten bleiben.
- Die Dauer der Aufbewahrung und der Zeitraum, innerhalb dessen die Mitteilung verwendet werden darf, müssen festgelegt werden, damit das Verwertungsverbot des Bundeszentralregistergesetzes nicht umgangen werden kann.
- Der Schutz Dritter, deren Daten sich in den Mitteilungen befinden, ist zu verbessern.
- Die Betroffenen sollten von der Übermittlung so rechtzeitig unterrichtet werden, daß sie noch effektiven Rechtsschutz erlangen können.

6.1.4 Strafverfolgungsstatistikgesetz

Die Strafverfolgungsstatistik ist die wichtigste Quelle für Erkenntnisse über die Anwendung des materiellen Strafrechts in der strafgerichtlichen Praxis. Durch die Erfassung von Ergebnissen der Strafverfahren vermittelt sie Erkenntnisse über den Umfang und die Struktur der Kriminalität, sowie über strafrechtliche Sanktionen bei den einzelnen Straftaten und erlaubt eine genaue Einschätzung der Strafzumessungspraxis der Gerichte. Diese Statistik wird bisher als Länderstatistik, außerhalb Bayerns nur auf der Grundlage von Verwaltungsvorschriften, geführt. Nunmehr soll mit dem Strafverfolgungsstatistikgesetz die erforderliche gesetzliche **Grundlage für eine Bundesstatistik** geschaffen werden.

In dem vom Bundesminister der Justiz vorgelegten Arbeitsentwurf werden eine Reihe datenschutzrechtlicher Forderungen, die zum Vorentwurf erhoben worden waren, berücksichtigt. Der Vorentwurf ging noch davon aus, daß die meisten Daten für die Strafverfolgungsstatistik über das **Bundeszentralregister** geleitet werden sollten. Damit waren zwei wesensverschiedene Aufgaben — Führung des Bundeszentralregisters und Statistik — eng miteinander verknüpft. Die Registerbehörde hätte dabei mehr Daten erhalten, als dies für die Wahrnehmung ihrer Aufgabe erforderlich gewesen wäre. Der neue Arbeitsentwurf hat dieser Kritik Rechnung getragen und verzichtet auf eine Beteiligung des Bundeszentralregisters an der künftigen Strafverfolgungsstatistik.

Doch auch der Arbeitsentwurf sollte aus datenschutzrechtlicher Sicht noch verbessert werden:

- Auf die Erhebung des **genauen Geburtsdatums** einer verfolgten Person kann und sollte verzichtet werden. Für Zwecke der Statistik reicht die Angabe des Geburtsmonats, wahrscheinlich sogar des Geburtsjahres gegenüber dem Statistikamt grundsätzlich aus.

- Gegen die vorgesehene umfassende Erhebung der **Täter-Opfer-Beziehung** bei Gewaltdelikten bestehen Bedenken. Da nicht hinreichend klar ist, welche Delikte darunter zu verstehen sind, müßte der Begriff „Gewaltdelikte" im Gesetz präzisiert werden. Im übrigen dürfte eine begrenzte Erhebung wie in der bisherigen Statistik, ob und wieviele Kinder Opfer der Straftat waren, für die Zwecke der Strafverfolgungsstatistik ausreichen.

- Hingegen dürfen an eine Geschäftsstatistik, die aus den bei Behörden vorhandenen Unterlagen erstellt wird, nicht die gleichen Anforderungen gestellt werden, wie etwa an die Volkszählungsstatistik, bei welcher der Bürger unmittelbar seine Daten der Statistik preisgibt. Deshalb bestehen gegen die Erhebung der Geschäftsnummer des Gerichts oder der Staatsanwaltschaft als Hilfsmerkmal keine Bedenken, auch wenn dadurch ein Rückgriff auf die Strafverfahrensakte möglich ist.

- Nicht vernünftig begründbar sind auch Bedenken gegen die Speicherung der Daten in einer gesonderten **Statistikdatei bei den auskunftspflichtigen Stellen**. Der Einwand einer unnötigen Doppelspeicherung geht schon deshalb fehl, weil zum einen eine Statistik auf Bundes- und auf Behördenebene **keine Doppelspeicherung** ist und weil es zum anderen der auskunftspflichtigen Stelle, also der die Statistikdaten liefernden Behörde nicht verwehrt sein kann, einen **Überblick über Stand und Entwicklung in ihrem eigenen Bereich** zu haben.

6.1.5 Gesetz zur Änderung von Vorschriften über das Schuldnerverzeichnis

Nach langjähriger Diskussion hat die Bundesregierung einen überarbeiteten Entwurf eines Gesetzes zur Änderung von Vorschriften über das Schuldnerverzeichnis vorgelegt. Wesentliche datenschutzrechtliche Änderungen und Verbesserungen gegenüber dem Vorentwurf aus dem Jahre 1989, zu dem ich mich in meinem letzten Tätigkeitsbericht geäußert habe, sind nicht erkennbar.

Der Gesetzentwurf wurde vom Bundestag nicht verabschiedet.

6.2 Kontrolle einer Staatsanwaltschaft

Die Prüfung der Datenverarbeitung bei einer Staatsanwaltschaft brachte ein erfreuliches Ergebnis. Es war ein ausgeprägtes Datenschutzbewußtsein festzustellen. Die datenschutzrechtlichen Bestimmungen waren sorgfältig beachtet.

6.2.1 Zentrales Namensregister

Den Schwerpunkt der Prüfung bildete das zentrale Namensregister, das dort seit Anfang 1987 automatisiert geführt wird. Dieses Namensverzeichnis ist ein Hilfsmittel zur Führung der Akten, mit dessen Hilfe der Name eines Beschuldigten einem bestimmten Verfahren zugeordnet werden kann. Die Datei enthält darüber hinaus noch weitere Datenfelder zur näheren Identifizierung des Betroffenen, zum Tatvorwurf und zur Erledigung des Verfahrens.

Name und Beschuldigung

Erfreulich war, daß das zentrale Namensverzeichnis nur die Namen von Beschuldigten enthielt. Namen von Anzeigenerstattern und Geschädigten waren nicht gespeichert. Zur Identifizierung der dem Ermittlungsverfahren zugrundeliegenden Straftat bedient man sich, soweit ein Beschuldigter fehlt, anderer Umstände, wie etwa Tatzeit, Tatort, Pkw-Kennzeichen oder polizeilicher Tagebuchnummer.

Eindeutiger Erledigungsvermerk

Die Art der Erledigung eines Ermittlungsverfahrens wird zwar grundsätzlich erfaßt. Allerdings werden Verfahren, die mangels hinreichenden Tatverdachts nach § 170 Abs. 2 Strafprozeßordnung eingestellt werden, nicht gekennzeichnet. Dies hat zur Folge, daß man bei den Verfahren, bei denen kein Erledigungsvermerk angebracht ist, dem zentralen Namensverzeichnis nicht entnehmen kann, ob eine Kennzeichnung versehentlich unterblieben ist, ob das Verfahren noch unerledigt ist, oder ob es eingestellt wurde. Bei dem in der Erprobung stehenden Verfahren „SIJUS-Strafsachen" ist die Kennzeichnung vorgesehen.

Kinder

Bei der Erfassung von Kindern im zentralen Namensverzeichnis ergab sich kein Grund zur Beanstandung. In allen überprüften Fällen war die Einstellung des Verfahrens wegen Strafunmündigkeit zutreffend erfaßt. Auch die Speicherungsdauer, die höchstens zwei Jahre betragen sollte, falls keine weiteren Ermittlungsverfahren hinzukommen, war eingehalten.

Änderung der Bewertung

Ändert sich im Lauf des Verfahrens die Bewertung der dem Verfahren zugrundeliegenden Straftat, so schlägt sich diese Änderung nicht in jedem Fall in einer **Berichtigung des Namensverzeichnisses** beim Abschluß der Ermittlungen nieder. Eine solche Berichtigung ist jedoch nach der justizinternen Verwaltungsvorschrift des § 47 Abs. 1 Satz 6 Aktenordnung vorgeschrieben. Danach hat die Staatsanwaltschaft vor Übersendung der Akten an das Gericht die Straftat, die der öffentlichen Klage zugrunde liegt, auf dem Aktenumschlag zu korrigieren, wenn sie die öffentliche Klage wegen einer anderen als der auf dem Aktenumschlag angegebenen Straftat erhebt. Da Dateien einen richtigen Inhalt haben müssen, muß das Namensverzeichnis bei einer Änderung der rechtlichen Bewertung einer Tat — eine ursprünglich als Raub bewertete Tat wird nur als Diebstahl angeklagt — ebenfalls geändert werden.

SIJUS-Strafsachen

Mit der Einführung des automatisierten Verfahrens „SIJUS-Strafsachen", das derzeit noch bei der Staatsanwaltschaft bei dem Landgericht Landshut erprobt wird, werden die automatisierten Dateien der Staatsanwaltschaften, insbesondere das zentrale Namensverzeichnis, weiter verbessert werden.

Datensicherheit

Die Datensicherheit war bei der geprüften Staatsanwaltschaft beachtet. Die Vergabe von Zugriffsberechtigungen an Mitarbeiter und die Auskunftserteilung an behördenfremde Personen entsprechen den datenschutzrechtlichen Bestimmungen. Ausdrucke aus dem Namensverzeichnis werden

ordnungsgemäß aufbewahrt oder vernichtet. Zur Vermeidung von Zugriffen nichtberechtigter Personen auf die Datei werden die Aufbewahrungsräume sorgfältig verschlossen.

6.2.2 Manuelle Dateien

In die manuellen Dateien der Staatsanwaltschaft habe ich stichprobenweise Einsicht genommen. In der manuellen zentralen Namenskartei und im manuellen Register für unbekannte Täter wurden die Verfahren vor Einführung der EDV registriert. Diese Karteien werden **zugriffssicher** aufbewahrt. Bei der inhaltlichen Überprüfung hat sich allerdings gezeigt, daß Karteikarten entgegen den Vorschriften über die Aufbewahrungsfrist für das Schriftgut der ordentlichen Gerichte, der Staatsanwaltschaften und der Justizvollzugsbehörden (Aufbewahrungsbestimmungen) zu lange aufbewahrt wurden. Diese Karteikarten wurden inzwischen entfernt.

6.2.3 Geldstrafendatei

Schließlich habe ich die Datei „Gesamtbestand der Vollstreckungsschuldner im Anwendungsbereich des Verfahrens EDV-Geldstrafenvollstreckung" überprüft. Mit Hilfe dieser Datei erledigt und überwacht die Staatsanwaltschaft die Geldstrafenvollstreckung. Die Vollstreckungsdaten werden an das Landesamt für Statistik und Datenverarbeitung übermittelt, das die Vollstreckung durch Datenverarbeitung im Auftrag abwickelt. Falls die Vollstreckung nicht ordnungsgemäß verläuft oder wenn sie beendet ist, wird die Staatsanwaltschaft davon unterrichtet. Die „EDV-Geldstrafen-Datei" entspricht datenschutzrechtlichen Bestimmungen.

6.3 Datenschutz im Zivilverfahren

Eine Eingabe machte deutlich, daß der Datenschutz im Zivilprozeß noch nicht ausreichend geregelt ist:

In einer Mietstreitigkeit mit geringem Streitwert bestanden Zweifel, ob die 75 Jahre alte Klägerin in der Lage sei, ihre Angelegenheit selbst zu besorgen, oder ob wegen Prozeßunfähigkeit ein Pfleger bestellt werden müsse. Mit Einverständnis der Betroffenen, jedoch ohne sie darauf hingewiesen zu haben, daß das Ergebnis der Begutachtung aktenkundig zu machen war und damit auch dem Prozeßgegner zur Verfügung stehen würde, führte der Landgerichtsarzt eine psychiatrische Begutachtung durch. Dabei wurden in dem Gutachten u.a. Feststellungen niedergelegt, von denen ich nicht nachvollziehen kann, was sie mit der Prozeßfähigkeit der Klägerin zu tun haben können. Bis weit in die Kindheit hinein wurden die persönlichen Verhältnisse, Krankheiten, persönliche Schicksalsschläge und Verhaltensweisen dargestellt, welche die Betroffene der Lächerlichkeit preisgeben könnten, falls diese Kenntnisse in die Öffentlichkeit gelangen und zum Spott benutzt würden. Dazu war das Gutachten in einer Sprache abgefaßt, die meines Erachtens an Beleidigung grenzt. Der Landgerichtsarzt reichte das Gutachten bei Gericht ein. Das Gericht nahm es zu den Akten und übersandte es dem gegnerischen Anwalt zur Kenntnisnahme und ggf. Stellungnahme. Auf diese Weise erlangte auch der Prozeßgegner eine Abschrift des Gutachtens. Dieser hatte nach dem Vorbringen der Petentin nichts besseres zu tun, als das Gutachten in seinem Freundeskreis herumzureichen und aus ihm zur Belustigung auf Partys zu zitieren. Die Betroffene, die seitdem auf der Straße verspottet wird, mußte schließlich dem gegnerischen Anwalt auch noch die Kosten ersetzen, die dieser für die Kopien, die er seinem Mandanten ausgehändigt hatte, aufgewendet hatte.

Nach meiner Auffassung stellt die Erhebung von intimen personenbezogenen Daten und deren Niederlegung in einem Gutachten einen **unzulässigen Eingriff** in das informationelle Selbstbestimmungsrecht des Betroffenen dar, wenn diese Daten zur Beurteilung der zu begutachtenden Fragestellung nicht notwendig sind. Das Einverständnis des Betroffenen mit der Begutachtung umfaßt nur die Preisgabe solcher Daten, die **notwendig** sind. Eine darüber hinausgehende Datenerhebung verstößt gegen den verfassungsrechtlichen Grundsatz der Erforderlichkeit. Dasselbe gilt für die Datenübermittlungen vom Gutachter an das Gericht und vom Gericht an den Prozeßgegner. Die Darstellung von personenbezogenen Daten in einer Form, die geeignet ist, den Betroffenen lächerlich zu machen, verletzt darüber hinaus das **allgemeine Persönlichkeitsrecht**. Der Landgerichtsarzt als staatliche Institution hätte die Grundrechte der von ihm begutachteten Klägerin schützen müssen. Dasselbe gilt für das Gericht, welches das Gutachten zu den Akten genommen und dem Prozeßgegner zugänglich gemacht hat. Es kann nicht hingenommen werden, daß in **formaler Anwendung von Prozeßvorschriften** — nämlich Gewährung des rechtlichen Gehörs für den Prozeßgegner — die Verletzung des Persönlichkeitsrechts eines Prozeßbeteiligten durch Zugänglichmachung der Unterlagen an den Prozeßgegner ermöglicht und der Betroffene anschließend auf mögliche Unterlassungs- und Schadensersatzansprüche verwiesen wird. Neben dem Grundsatz des rechtlichen Gehörs ist gerade die Würde des Menschen an hervorragender Stelle im Grundgesetz garantiert. Hätte der Gutachter in der mündlichen Hauptverhandlung entwürdigende oder nicht zur Sache gehörende Fragen gestellt, so hätte das Gericht nach der Prozeßordnung das Recht und die Pflicht gehabt, diese Fragen zurückzuweisen. Für die Verletzung des Persönlichkeitsrechts in einem Gutachten kann im Ergebnis nichts anderes gelten.

Nach meiner Auffassung hätte das Gericht das Gutachten vorab auf Persönlichkeitsrechtsverletzungen hin prüfen müssen und Feststellungen, die nicht notwendig oder in verletzender Form gehalten waren, zurückweisen und die Erstellung eines korrekten Gutachtens verlangen müssen. Als Alternative wäre daran zu denken, das erstellte Gutachten zwar zu akzeptieren, es jedoch nicht oder nicht in vollem Umfang zu den Akten zu nehmen und dem Prozeßgegner nur solche Ausführungen zur Kenntnis zu bringen, die für die Entscheidung über die Prozeßfähigkeit von Bedeutung sind. Wenn eine Akteneinsicht zu einer Grundrechtsverletzung führen würde, muß § 299 Zivilprozeßordnung verfassungskonform angewendet werden. Schließlich bleibt noch die Frage, ob der gegnerische Prozeßvertreter als Organ der Rechtspflege nicht verpflichtet gewesen wäre, ein derartiges Gutachten seinem Mandanten zumindest nicht in Ablichtung auszuhändigen.

Die verschiedenen Lösungsmöglichkeiten sollten für den Gesetzgeber Anlaß zu einer gesetzlichen Regelung sein.

6.4 Einzelfälle

6.4.1 Schuldnerlisten an Kreditvermittler

Die Gefährdungen, die sich aus dem Schuldnerverzeichnis, der Erteilung der Abschriften aus dem Schuldnerverzeichnis an die Industrie- und Handelskammer sowie aus der Weiter-

gabe von Schuldnerlisten an weitere Interessenten für die Betroffenen ergeben können, habe ich in nahezu jedem vorangegangenen Tätigkeitsbericht dargestellt.

Auch im Berichtszeitraum haben mich wieder mehrere Eingaben von Bürgern erreicht, denen nach Eintragung in das Schuldnerverzeichnis von Kreditvermittlungsfirmen aus dem gesamten Bundesgebiet Angebote auf Abschluß von Kreditverträgen zugesandt worden sind. Die Aufklärung, aus welcher Quelle die Kreditvermittler die Namen der eingetragenen Personen erlangt haben, ist mir kaum möglich, da diese privaten Firmen mir gegenüber nicht auskunftspflichtig sind und verschiedene Möglichkeiten bestehen, an die Namen der in das Schuldnerverzeichnis eingetragenen Personen herankommen. So können die Kreditvermittler die Informationen aus den sich im Umlauf befindlichen Schuldnerlisten beziehen. Ebenso denkbar ist, daß die Informationen aus einem inzwischen eingerichteten privaten Schuldnerverzeichnis stammen oder durch einen Adressentausch der Firmen untereinander in die Hände von Kredithaien gelangt sind.

In einem einzigen Fall konnte ich in Erfahrung bringen, daß die betreffende Firma Bezieherin der vertraulichen Mitteilungen aus dem Schuldnerverzeichnis war. Dieser Firma war der Bezug bewilligt worden, da sie gleichzeitig einen Warenhandel betreibt und in diesem Zusammenhang auf die Kenntnis der Zahlungsfähigkeit ihrer Kunden angewiesen ist. Der Industrie- und Handelskammer war die gleichzeitig betriebene Kreditvermittlung verschwiegen worden. Die Möglichkeit einer Einstellung der Belieferung mit den vertraulichen Mitteilungen aus dem Schuldnerverzeichnis wird derzeit geprüft.

Die erkannten Gefährdungen des Datenschutzes durch die mögliche zweckfremde Verwendung der Abschriften aus dem Schuldnerverzeichnis und der Schuldnerlisten haben dazu geführt, daß die Anträge privater Kreditvermittlungsfirmen auf fortlaufende Erteilung von Abschriften aus den Schuldnerverzeichnissen bei den Präsidenten der Landgerichte abgelehnt werden.

Es ist bedauerlich, daß der Gesetzentwurf der Bundesregierung zur Änderung von Vorschriften über das Schuldnerverzeichnis vom Bundestag nicht verabschiedet wurde.

6.4.2 Beauftragung von Gutachtern durch Gerichte

Der Datenschutzbeauftragte einer Forschungsgesellschaft hat sich darüber beklagt, daß Gerichte vielfach bei der **Versendung von Verfahrensakten** zur Erstellung von Abstammungsgutachten das Persönlichkeitsrecht des Betroffenen zu wenig beachten. Dem Institut würden vollständige Gerichtsakten zugesandt. Der zuständige Wissenschaftler werde in der Anschrift nicht namentlich genannt. Die Posteinlaufstelle sei daher gezwungen, die gesamten Akten, die auch eine Vielzahl vertraulicher Angaben aus dem Gerichtsverfahren enthielten, nach dem Beweisbeschluß durchzusehen, in dem der Gutachter benannt sei. Außerdem enthielten die übersandten Akten eine Fülle äußerst sensiblen Materials, das für die Erstellung des Gutachtens nicht benötigt werde und in diesem Zusammenhang irrelevant sei.

Die geschilderte Problematik dürfte nach meiner Einschätzung nicht nur bei erbbiologischen Gutachten, sondern generell in gerichtlichen Verfahren bedeutsam sein. Das informationelle Selbstbestimmungsrecht der Verfahrensbeteiligten darf auch in Gerichtsverfahren nur im sachlich erforderlichen Umfang eingeschränkt werden.

Die zuständigen Ministerien haben mir darin beigepflichtet, daß der jeweils beauftragte **Sachverständige in der Anschrift namentlich** benannt werden sollte, damit der sensible Akteninhalt nur den unmittelbar mit der Begutachtung befaßten Personen zur Kenntnis gelangt. Hinsichtlich des Umfangs der Aktenübersendung vertraten die Ministerien die Auffassung, daß hier die richterliche Unabhängigkeit im Rahmen der gerichtlichen Beweiserhebung zu beachten sei. Auch könne eine Aussonderung von Aktenbestandteilen im Einzelfall Schwierigkeiten bereiten, da nicht immer eindeutig erkennbar sei, welche Aktenbestandteile der Sachverständige für die Erstellung des Gutachtens benötige. In Strafsachen lege die Verteidigung darüber hinaus erfahrungsgemäß großen Wert darauf, daß dem Sachverständigen der gesamte Akteninhalt zur Verfügung stehe. Das Gericht dürfe sich nicht dem Vorwurf aussetzen, sich spezielle Sachkunde anzumaßen. Die Ministerien werden die Beachtung des Datenschutzes zum Thema von Dienstbesprechungen machen.

Diesen Ausführungen stimme ich grundsätzlich zu. Für mich besteht kein Zweifel, daß die Gerichte im Verfahren neben dem Grundsatz des rechtlichen Gehörs und dem Gebot der Sachaufklärung auch das Persönlichkeitsrecht der Betroffenen zu beachten haben. Das Persönlichkeitsrecht, letztlich die Würde des Menschen, setzt der richterlichen Wahrheitsfindung Schranken. Wenn der Versand der Gerichtsakten unter keinem Gesichtspunkt plausibel begründet werden kann, liegt ein Verstoß gegen das Persönlichkeitsrecht des Betroffenen vor, gegen den er sich mit den gegebenen Rechtsbehelfen wehren kann.

6.4.3 Zeugenanschriften im Strafbefehl

Im Zusammenhang mit einer Verbesserung des Zeugenschutzes im Strafverfahren wird zur Zeit zwischen der Justiz und den Datenschutzbeauftragten die Frage erörtert, ob es nach der geltenden Rechtslage zulässig und geboten ist, in Strafbefehlen die vollständigen Wohnanschriften von Zeugen wegzulassen und nur noch deren Namen, Vornamen und evtl. den Wohnort anzugeben.

Nach § 409 Abs. 1 Nr. 5 Strafprozeßordnung enthält der Strafbefehl die Beweismittel. Diese Vorschrift entspricht § 200 Abs. 1 Satz 2 Strafprozeßordnung, wonach in der Anklageschrift **die Beweismittel anzugeben** sind. Nach der weiteren Bestimmung des § 222 Abs. 1 Satz 1 Strafprozeßordnung sind dem Angeklagten die vom Gericht geladenen Zeugen in der Ladungsmitteilung zur mündlichen Hauptverhandlung namhaft zu machen und Wohn- oder Aufenthaltsort anzugeben. Sinn dieser Vorschriften ist es, dem Angeklagten die Möglichkeit einzuräumen, Erkundigungen über die benannten Zeugen einzuholen und sich ein Bild über die Beweislage zu verschaffen. Im Gegensatz zur Anklage, auf die zwingend die Ladung zur mündlichen Hauptverhandlung folgt, wird ein Großteil der Strafbefehle ohne Einspruch und Verhandlung rechtskräftig, weshalb die genaue Angabe der Anschrift von Zeugen entbehrlich sein könnte.

Nach herrschender Auffassung in Literatur und Rechtsprechung umfaßt die im Gesetz geforderte Angabe des Beweismittels „Zeuge" auch dessen Anschrift. Damit kann sicherlich eine gewisse Gefährdung des Zeugen im Einzelfall verbunden sein. Andererseits ist aber nicht zu übersehen, daß der Beschuldigte in den meisten Fällen den ihn belastenden Zeugen kennt oder sich zumindest seine genaue Anschrift beschaffen könnte. Nach § 68 Strafprozeßordnung besteht

zwar die Möglichkeit, daß der Vorsitzende in der Hauptverhandlung dem Zeugen gestatten kann, seinen Wohnort nicht anzugeben, wenn die Besorgnis besteht, daß er oder eine andere Person gefährdet würde. Nach übereinstimmender Auffassung soll diese 1979 geschaffene Regelung aber den Zeugen nur in der Hauptverhandlung, nicht jedoch vor späteren Nachstellungen durch den Angeklagten schützen.

Deshalb ist wohl der herrschenden Auffassung zuzustimmen, daß nach geltender Rechtslage dem Beschuldigten **auch im Strafbefehlsverfahren die Möglichkeit** einzuräumen ist, sich über die ihn belastenden Zeugen und deren Identität ein genaues Bild zu verschaffen und Erkundigungen über sie einzuziehen. Es genügt nicht, den Beschuldigten auf die Möglichkeit einer anwaltlichen Akteneinsicht oder eines Einspruchs mit der Folge einer Hauptverhandlung zu verweisen, wenn er die Anschrift eines Zeugen in Erfahrung bringen will.

Eine andere Frage ist, ob die geltende Strafprozeßordnung das auch einem Zeugen zustehende Recht auf informationelle Selbstbestimmung ausreichend berücksichtigt. Diese Frage muß im Hinblick auf die dem Angeklagten eingeräumten umfangreichen Verteidigungsmöglichkeiten sehr sorgfältig bedacht und bei der anstehenden Änderung der Strafprozeßordnung entschieden werden.

6.4.4 Schweigerecht von Bewährungshelfern

Bei Fortbildungsveranstaltungen von Bewährungshelfern wird immer wieder die Frage angesprochen, ob der Bewährungshelfer berechtigt oder gar verpflichtet sein kann, die von Probanden erhaltenen Informationen dem Gericht und seinem Dienstherrn nur in beschränktem Umfang weiterzugeben. Immerhin hat der Bewährungshelfer als Sozialarbeiter und Amtsträger die nach § 203 Abs. 1 Nr. 5, Abs. 2 Strafgesetzbuch im Verhältnis zu außenstehenden Dritten bestehende Schweigepflicht zu beachten.

Nach der Auffassung des Staatsministeriums der Justiz kann bei Bewährungshelfern eine sogenannte „innerbehördliche Schweigepflicht" nicht anerkannt werden. Zwar sei der staatlich anerkannte Sozialarbeiter ein Geheimnisträger im Sinne der vorgenannten Vorschrift. Dies genüge jedoch keinesfalls für die Annahme einer innerbehördlichen Schweigepflicht. Der Bewährungshelfer begegne seinen Klienten nicht nur als Vertrauensperson, sondern auch als Helfer des Gerichts und als Angehöriger einer Behörde, in deren Organisation er eingebunden sei. Deswegen bestehe auch gegen die Telefondatenerfassung von Bewährungshelfern, mit deren Hilfe sich Erkenntnisse darüber gewinnen lassen, mit wem der Bewährungshelfer wann und wie lange gesprochen hat, keine Bedenken.

Diese Auffassung des Justizministeriums teile ich. Allerdings sollten sowohl die Bewährungshelfer als auch die von ihnen betreuten Probanden über die geltende Rechtslage **unterrichtet** werden.

6.4.5 Informationen an die Meldebehörde

Nach Nr. 12 a der Anordnung über Mitteilungen in Strafsachen (MiStra) teilt die Staatsanwaltschaft der Gemeinde den Tenor des Urteils mit, durch das

- wegen eines Verbrechens auf eine Freiheitsstrafe von mindestens einem Jahr erkannt worden ist,
- einem Verurteilten die Fähigkeit aberkannt worden ist, öffentliche Ämter zu bekleiden oder Rechte aus öffentlichen Wahlen zu erlangen,
- einem Verurteilten das Recht aberkannt worden ist, in öffentlichen Angelegenheiten zu wählen oder zu stimmen.

Ferner wird die Urteilsformel mitgeteilt, wenn ein Verurteilter in einer psychiatrischen Anstalt untergebracht wird.

Bei der Prüfung einer Gemeinde habe ich festgestellt, daß manche Staatsanwaltschaften teilweise die **vollständigen Strafurteile** einschließlich der Begründungen an die Meldebehörden übermitteln. Andere übersenden im Einklang mit der MiStra nur den Urteilstenor, der sich jedoch häufig gegen **mehrere Angeklagte** richtet. Damit werden an die Meldebehörden wesentlich mehr Informationen geliefert, als zur Erfüllung von deren Aufgaben erforderlich ist, oder es werden Daten von Mitverurteilten übermittelt, bei denen die jeweilige Meldebehörde örtlich gar nicht zuständig ist oder bei denen die Voraussetzungen für Nr. 12 a MiStra nicht vorliegen. Diese Praxis ist nicht zulässig. In diesen Fällen muß es genügen, wenn die Staatsanwaltschaft der Meldebehörde mitteilt, daß gegen einen bestimmten Verurteilten ein zu benennendes Erkenntnis ausgesprochen wurde, das die Voraussetzungen von Nr. 12 a MiStra erfüllt. Das Justizministerium teilt meine Auffassung. In einer Dienstbesprechung hat es die Behördenleiter der Staatsanwaltschaften von meiner Auffassung unterrichtet und sie gebeten, künftig entsprechend zu verfahren.

6.4.6 Unterrichtung des Dienstherrn über Strafbefehl oder Anklage

Nach Nr. 15 MiStra ist u.a. der Antrag auf Erlaß eines Strafbefehls oder die Erhebung der öffentlichen Klage gegen einen Angehörigen des öffentlichen Dienstes dem Dienstherrn mitzuteilen. Die Mitteilungen sind an den unmittelbaren Dienstvorgesetzten zu richten, teilweise zusätzlich an den Leiter der Aufsichtsbehörde, in anderen Fällen an den Leiter der Beschäftigungsstelle. Sie sind an den Behördenleiter oder dessen Vertreter im Amt zu adressieren und als „vertrauliche Personalsache" zu kennzeichnen.

Ich habe festgestellt, daß Staatsanwaltschaften gelegentlich die Mitteilungen ohne diesen Hinweis versenden mit der Folge, daß die Briefe als üblicher Posteinlauf geöffnet und von Nichtberechtigten zur Kenntnis genommen werden. Auch ist der Behördenleiter nicht immer nach der Geschäftsverteilung für Personalangelegenheiten der zuständige Ansprechpartner. Soweit der Staatsanwaltschaft bekannt gegeben worden ist, daß für die Entgegennahme eine andere Stelle zuständig ist, muß die Mitteilung unmittelbar an diese gerichtet werden.

6.5 Datenschutz im Notariat

Im Bereich des Notariatswesens ist Kernpunkt einer seit längerer Zeit bundesweit geführten Diskussion die Frage nach der Anwendbarkeit der Bestimmungen des jeweils maßgebenden Landesdatenschutzgesetzes auf die Tätigkeit der Notare. Im einzelnen geht es insbesondere um die Meldepflicht der Notare zum Datenschutzregister, aber auch um die Kontrollzuständigkeit des Landesbeauftragten für den Datenschutz.

Ich habe mich schon vor Jahren zu diesen Fragen in einer Stellungnahme gegenüber dem Staatsministerium der Justiz

und der Landesnotarkammer Bayern geäußert. Dabei habe ich die Auffassung vertreten, daß die bayerischen Notare als Träger eines öffentlichen Amtes grundsätzlich als **öffentliche Stellen** im Sinne des Bayerischen Datenschutzgesetzes angesehen werden müssen und deshalb den Bestimmungen dieses Gesetzes unterliegen, soweit sie personenbezogene Daten in Dateien verarbeiten. Die Bundesnotarordnung als maßgebendes Berufsrecht der Notare steht dem nicht entgegen, da das Bayerische Datenschutzgesetz keine weitergehenden spezifisch berufsrechtlichen Regelungen enthält, sondern sich mit einer Querschnittsmaterie eigener Art befaßt. Bereichsspezifische Vorschriften über den Datenschutz im Notariat gehen selbstverständlich den Bestimmungen des Bayerischen Datenschutzgesetzes im Einzelfall vor, berühren die Geltung des Gesetzes aber im übrigen nicht. Es besteht daher keine Veranlassung, die bayerischen Notare aus der umfassenden Kontrollbefugnis des Datenschutzbeauftragten zu entlassen oder von einer Registrierung etwaiger anmeldepflichtiger Dateien im Datenschutzregister abzusehen, auch wenn mir bisher aktuelle Fälle einer mißbräuchlichen Datenverarbeitung in bayerischen Notariaten nicht bekanntgeworden sind.

Meine Rechtsauffassung wurde im Ergebnis von allen anderen Datenschutzbeauftragten, auch vom Bundesminister der Justiz, geteilt. Demgegenüber vertrat die Landesnotarkammer Bayern die Auffassung, daß das Bayerische Datenschutzgesetz auf die Tätigkeit der bayerischen Notare keine Anwendung finde. Der Landesgesetzgeber sei nicht zuständig, datenschutzrechtliche Regelungen mit Wirkung für den Bereich des Notariats zu erlassen.

Durch Beschluß des Bundesgerichtshofs vom 30. Juli 1990 ist dieser Rechtsstreit nun entschieden worden. Der Bundesgerichtshof hat — allerdings für die Rechtslage in Nordrhein-Westfalen — festgestellt, daß das Nordrhein-Westfälische Datenschutzgesetz auf die Notare anwendbar sei und diese verpflichtet seien, ihre automatisierten Dateien beim Landesbeauftragten für den Datenschutz anzumelden. Der Bundesgerichtshof hat die **Notare als sonstige öffentlichen Stellen** des Landes angesehen, da sie Träger eines öffentlichen Amtes seien, die durch Hoheitsakt bestellt würden und der Dienstaufsicht der Landesjustizverwaltung unterlägen. Daß die Notare Aufgaben der Rechtspflege erfüllten, befreie sie nicht von der gesetzlichen Anmeldeverpflichtung gegenüber dem Landesbeauftragten für den Datenschutz. Weiter führt der BGH aus, die bundesrechtlichen Regelungen des Berufsrechts der Notare in der Bundesnotarordnung stünden einer allgemeinen datenschutzrechtlichen Regelung im Landesdatenschutzgesetz, die auch für die Notare zutreffe, nicht entgegen.

Aufgrund der Rechtsprechung des Bundesgerichtshofs werde ich auf die Einhaltung der Vorschriften des Bayerischen Datenschutzgesetzes durch die Notare drängen.

7. Regierungen, Landkreise, Städte und Gemeinden

7.1 Veröffentlichung eines Untersuchungsberichts

Im 10. Tätigkeitsbericht habe ich von „Datenschutzlücken im Gemeinderat" berichtet. Ich habe darauf hingewiesen, daß wiederholt der Datenschutz der Bürger bei der Behandlung sensibler Angelegenheiten in nichtöffentlichen Sitzungen verletzt wurde. Bürger hatten sich darüber beklagt, daß aus dem Gemeinderat heraus persönliche Angaben über sie öffentlich bekannt würden, beispielsweise ihr Einkommen, ihre wirtschaftlichen Belastungen, Geschäftsbeziehungen, Eigentumsverhältnisse und ähnliches.

Ein neuerlicher Fall, der mir wiederum durch eine Eingabe bekannt geworden ist, veranlaßt mich, dieses Thema nochmals aufzugreifen. Folgendes war geschehen:

Einem leitenden Beamten einer kreisfreien Stadt war zum Vorwurf gemacht worden, er habe seine berufliche Stellung dazu genutzt, ein denkmalgeschütztes Haus günstig zu erwerben. Zur Überprüfung dieser Vorwürfe hat der Stadtrat eine Untersuchungskommission bestellt. Der Abschlußbericht der Kommission wurde in einer nichtöffentlichen Sitzung erörtert. Kurze Zeit später wurde der gesamte Untersuchungsbericht sehr ausführlich in der örtlichen Presse wiedergegeben. Aufgrund der gesamten Umstände ist davon auszugehen, daß ein Mitglied dieses Untersuchungsausschusses den Bericht der örtlichen Presse zugespielt hat. Wer dies war, konnte nicht festgestellt werden.

Den Fall habe ich zum Anlaß genommen, den Oberbürgermeister auf die erforderlichen Maßnahmen zur Sicherung der Persönlichkeitsrechte der Bürger bei Behandlung ihrer Angelegenheiten im Stadtrat hinzuweisen. Folgende Maßnahmen habe ich konkret vorgeschlagen:

- Bei der Herausgabe von Sitzungsunterlagen sollte äußerst zurückhaltend verfahren werden. Nur die wirklich notwendigen Unterlagen sollten an die Stadtratsmitglieder verteilt werden. Besonders sensible Unterlagen sollten vorher numeriert werden. Die Mitnahme oder der Versand solcher Unterlagen an die Privatwohnung der Stadtratsmitglieder sollte untersagt werden.

- Sensible Sitzungsunterlagen dürfen nicht abgelichtet und aus dem Sitzungssaal entfernt werden.

- Die Sitzungsunterlagen müssen nach der Sitzung wieder vollständig eingesammelt werden.

- Die Stadtratsmitglieder sollten immer wieder auf ihre Verschwiegenheitspflicht nach Art. 20 Gemeindeordnung, auf ihre besondere Verantwortung gegenüber den Bürgern gerade im Blick auf deren Persönlichkeitsrechte, aber auch auf die strafrechtlichen Bestimmungen hingewiesen werden.

Ich bin mir durchaus darüber im klaren, daß es in der Praxis immer wieder besondere Schwierigkeiten bereiten kann, bei der Unterrichtung des Stadtrats über kommunale Vorgänge sowohl den Persönlichkeitsrechten der Bürger als auch der Verantwortlichkeit und dem Informationsrecht des Stadtrats gerecht zu werden. Eine stärkere Respektierung der Persönlichkeitsrechte der Bürger im Stadtrat wird nur dann zu erreichen sein, wenn das Datenschutzbewußtsein im Stadtrat gestärkt wird, und die Preisgabe von Bürgergeheimnissen an Unbefugte nicht mehr als Kavaliersdelikt oder unvermeidbare und deshalb hinnehmbare Nebenfolge politischer Auseinandersetzungen verniedlicht, sondern als schwerer Verstoß gegen die Pflichten eines Stadtrats und als Zeichen fehlender politischer Kultur von der Öffentlichkeit verurteilt wird.

7.2 Prüfung von Regierungen

Bei der Prüfung einer weiteren Regierung war folgendes festzustellen:

- Anlaß zur Beanstandung gab einmal mehr die Handhabung der **Beihilfe**. Mein vorangegangener Bericht war offensichtlich in den Wind geschrieben. Bei dieser Regierung wurden die Beihilfeanträge in der allgemeinen Poststelle geöffnet, registriert und in ein offenes Postaustauschfach gelegt. Von dort aus wurden sie in die Beihilfestelle, die in einer Außenstelle der Regierung untergebracht ist, transportiert. Ich habe die Regierung darauf hingewiesen, daß dies nicht den vom Staatsministerium des Innern erlassenen Richtlinien entspricht. Danach dürfen die mit der Anschrift „Beihilfe" gekennzeichneten Umschläge nur von den Beihilfestellen geöffnet werden. Die auf dem Umschlag an die Beihilfestelle adressierten Anträge sind ungeöffnet von der Poststelle an die Beihilfestelle weiterzuleiten. Außerdem habe ich festgestellt, daß aus der Beihilfestelle aus Kapazitätsgründen gelegentlich Schreibarbeiten in die allgemeine Schreibkanzlei gegeben werden. Ich habe die Regierung gebeten, Beihilfeangelegenheiten ausschließlich in der Beihilfestelle selbst schreiben zu lassen.

- In der Personalabteilung bin ich auf eine Kartei **„Personal der Staatlichen Gesundheitsverwaltung"** gestoßen. Diese Kartei enthielt Personalkarten über Ärzte, die längst aus der staatlichen Gesundheitsverwaltung ausgeschieden waren. Zum Teil waren Karteikarten aus der unmittelbaren Nachkriegszeit enthalten. Diese Karteikarten vermerkten so sensible Angaben wie Spruchkammerbescheide ("Mitläufer") oder Angaben zur NSDAP-Mitgliedschaft. Ich habe gefordert, diese Karteikarten auszusortieren und datenschutzgerecht zu vernichten, nachdem mir die Regierung versichert hatte, daß diese Daten nicht mehr benötigt werden. Die Regierung hat dies zwischenzeitlich getan.

- Im übrigen habe ich auch bei dieser Prüfung wieder zahlreiche **Personalkarteien** vorgefunden, die, während einer Übergangsphase noch gebraucht, nach Einführung des Personalverwaltungssystems DIAPERS aber nicht mehr benötigt werden. Ich habe gefordert, diese Personalkarteien nach Ablauf der Probezeit von DIAPERS datenschutzgerecht zu vernichten.

- Weitere Punkte waren die nicht immer datenschutzgerechte **Aufbewahrung von Karteien und Akten** in nicht verschließbaren Behältnissen. Auch insoweit habe ich Abhilfe durch Bereitstellung entsprechend sicherer Schränke oder ähnliche Vorkehrungen gefordert.

Nach Mitteilung der Regierung sind die beanstandeten Mängel inzwischen behoben.

7.3 Prüfung von Landratsämtern

Bei der Prüfung eines Landratsamtes mußte ich wiederum feststellen, daß die **Organisation der Beihilfesachbearbeitung** nicht den Anforderungen entspricht, die das Staatsministerium des Innern zum Persönlichkeitsschutz bei Beihilfedaten aufgestellt hat. Zwar ist bei diesem Landratsamt diesmal kein Personalsachbearbeiter gleichzeitig für die Beihilfesachbearbeitung zuständig, wie bei anderen von mir bisher geprüften Landratsämtern; es ist jedoch auch bei diesem Amt das **Gebot der sachlichen und organisatorischen Trennung** von Personal- und Beihilfeverwaltung auf **Sachgebietsleiterebene** nicht eingehalten, weil die Beihilfesachbearbeitung innerhalb des Personalreferats angesiedelt ist. Der vom Staatsministerium des Innern erarbeitete Mustergeschäftsverteilungsplan enthält diese Trennung auf Sachgebietsebene.

Auf der **Urlaubs- und Krankenkartei** speichert das Landratsamt neben Namen, Geburtsdatum, Anschrift, Sachgebiet, Bedienstetengruppe, Beschäftigungs- und Dienstzeit auch das **Bekenntnis**. Nach Auffassung des Landratsamtes ist die Speicherung des Bekenntnisses erforderlich wegen des katholischen Feiertags „Mariä Himmelfahrt". In der überwiegend evangelischen Kreisstadt ist Mariä Himmelfahrt kein gesetzlicher Feiertag (Art. 1 Abs. 1 Nr. 2 Feiertagsgesetz). Die katholischen Bediensteten dürfen an diesem Tag jedoch auf Antrag dem Dienst fernbleiben; der Dienst muß „vorher oder nachher" eingearbeitet werden. Aus der Urlaubskartei müsse deshalb, so das Landratsamt, die Dienstbefreiung ersichtlich sein. Nach meiner Auffassung reicht es aber aus, wenn hier lediglich bei den katholischen Bediensteten das Bekenntnis „katholisch" gespeichert wird. Die Speicherung der anderen Bekenntnisse ist nicht erforderlich.

Das Landratsamt führt eine sogenannte **Rauschgiftkartei**. In dieser Kartei sind die wegen Rauschgiftdelikten vorbestraften Personen aufgeführt. Die Rauschgiftkartei enthält Namen, Beruf, Geburtsdatum/-ort, Staatsangehörigkeit, Anschrift sowie die Verurteilung der Betroffenen. Das Landratsamt benötigt die Kartei zur Prüfung der Frage, ob den Verurteilten Erlaubnisse, die von der persönlichen Zuverlässigkeit der Inhaber abhängen (z.B. Waffenschein, Jagdschein und Sprengstofferlaubnisse) belassen werden können oder ob und in welchen Abständen eine Wiedererteilung von entzogenen Erlaubnissen in Betracht kommen kann.

Für diese Zwecke habe ich gegen die Führung einer solchen Kartei keine Einwände. Über Personen, die nicht Inhaber von Erlaubnissen sind, darf eine solche Kartei jedoch nicht geführt werden. Das Staatsministerium des Innern teilt diese Ansicht.

Auch bei der Prüfung dieses Landratsamtes mußte ich feststellen, daß eine Reihe von **Akten und Karteien in nicht abschließbaren Schränken und Schubladen** untergebracht sind. So sind z.B. die laufenden Personalakten in einem nicht abschließbaren Stahlschrank untergebracht. Zwar steht dieser Stahlschrank in einem abschließbaren Abstellraum. Da jedoch außer dem Sachbearbeiter für das Personalwesen noch der Beihilfesachbearbeiter Zutritt zu dieser Abstellkammer hat, halte ich den Verschluß des Stahlschrankes selbst für notwendig. Positiv aufgefallen ist mir bei diesem Landratsamt die vorbildliche Papier- und Aktenvernichtung. Das Landratsamt verfügt über mehrere Papiervernichtungsmaschinen mit verschiedenen Sicherheitsstufen (u.a. auch für VS-Sachen); ferner werden die ausgesonderten Akten des Landratsamtes unter Aufsicht von Mitarbeitern des Landratsamtes in einer nahegelegenen Papierfabrik zu Altpapier verarbeitet.

7.4 Prüfung von Stadtwerken

Bei der Prüfung der Stadtwerke habe ich folgende Feststellungen getroffen:

- Die Verkehrsbetriebe legen für jeden Mitarbeiter einen Umschlag mit Arbeitsunfähigkeitsbescheinigungen an. Auf der Außenseite befindet sich neben den Angaben zu Namen, Dienstbezeichnung, Geburtsdatum, Dienststelle und Zeitraum der Erkrankung eine Spalte mit „Bemerkungen", in der sich zum Teil handschriftliche Vermerke über die **Art der Erkrankung** befinden.

  Ich habe dagegen Bedenken geäußert, da für Bedienstete keine Pflicht besteht, dem Arbeitgeber die Art ihrer Erkrankung mitzuteilen.

  Mit den Stadtwerken habe ich mich auf folgende Regelung verständigt:
  Es wird nicht mehr die Art der Erkrankung angegeben, sondern es werden nur noch folgende Vermerke angebracht: Arbeitsunfall, Privatunfall, Aussprache, Niederschrift.

  Erforderlich sind diese Angaben aus folgenden Gründen:

  Bei einem Arbeitsunfall sind bestimmte Mitteilungen an die Berufsgenossensohaft nötig. Bei einem Privatunfall stellt sich für die Stadtwerke die Frage der Geltendmachung von Schadensersatzansprüchen nach dem Lohnfortzahlungsgesetz. Die Bemerkungen „Aussprache oder Niederschrift" werden nur dann angebracht, wenn aufgrund auffällig häufiger oder langanhaltender Erkrankungen sich entweder Zweifel an der Arbeitsunfähigkeit aufdrängen oder im Rahmen der Fürsorgepflicht die gesundheitliche Eignung des Einsatzes des Mitarbeiters am konkreten Arbeitsplatz einer Überprüfung bedarf.

- Bei den Stadtwerken werden **Karteien über ausgeschiedene Mitarbeiter** geführt. Diese Karteien dürfen trotz der sich öfter ergebenden Rückfragen nur vorgehalten werden, solange sie zur Aufgabenerfüllung gebraucht werden. Das ist in der Regel nur sechs Jahre nach dem Ausscheiden der Mitarbeiter der Fall. Außerdem darf nur ein Grunddatensatz (Name, Vorname, Geburtsdatum, -ort und Beschäftigungsverhältnis) geführt werden. Ich habe die Stadtwerke aufgefordert, mir ihre Vorstellungen über eine Aussonderung oder Vernichtung dieser Karteien mitzuteilen.

- Ferner habe ich bei den Verkehrsbetrieben die Speicherung minderjähriger Jugendlicher in der **„Schwarzfahrerdatei"** überprüft. Beanstandungen haben sich dabei nicht ergeben:

  Kinder bis zum vollendeten 7. Lebensjahr werden von den Kontrolleuren der Verkehrsbetriebe nicht beanstandet und infolgedessen auch nicht in der Schwarzfahrerdatei gespeichert.

  Kinder vom 8. bis zum vollendeten 14. Lebensjahr werden bis zur Bezahlung des erhöhten Beförderungsentgelts durch die Erziehungsberechtigten in der Schwarzfahrerdatei geführt. Anschließend werden die Daten mittels eines vierteljährlichen Pflegelaufs gelöscht. Verweigern die Erziehungsberechtigten die Bezahlung, wird ein Mahnverfahren eingeleitet. Spätestens nach Beendigung des Mahnverfahrens werden die Daten wiederum mittels des vierteljährlichen Pflegelaufs gelöscht.

  Die Daten der Jugendlichen ab dem 14. Lebensjahr werden — wie bei Erwachsenen — in der Regel zwei Jahre gespeichert. Die Speicherung ist erforderlich für eine eventuelle strafrechtliche Verfolgung (Beförderungserschleichung) von Mehrfachtätern. Personen, die während dieser zwei Jahre keine weiteren Verstöße gegen die Tarifbestimmungen begangen haben, werden aus der Datei gelöscht.

  Zur Schwarzfahrerdatei vgl. auch 18.5.

7.5 Datenübermittlung an Jagdgenossenschaften

Mehrere Gemeinden haben angefragt, ob sie Grundstücksangaben (Daten über Verkäufer, Käufer, Flurnummer und Flurstücksgröße) an Jagdgenossenschaften weitergeben dürfen. Die Jagdgenossenschaften sind öffentlich-rechtliche Körperschaften; Mitglieder sind die Eigentümer jagdbarer Flächen des gemeinschaftlichen Jagdbezirks. Die Gemeinden erhalten diese Grundstücksangaben von den Notaren zur Prüfung der Frage, ob sie das Vorkaufsrecht ausüben wollen.

In Übereinstimmung mit den Staatsministerien des Innern und für Ernährung, Landwirtschaft und Forsten halte ich die Weitergabe von Daten, welche die Gemeinde im Rahmen der Prüfung der Ausübung des Vorkaufsrechts von den Notaren erhalten hat, an die Jagdgenossenschaften für unzulässig. Dies wäre eine **zweckwidrige Verwendung** der Angaben.

7.6 Übermittlung von Anschriften leerstehender Wohnungen von den Stadtwerken an das Amt für Wohnungswesen

Das Amt für Wohnungswesen einer kreisfreien Stadt hat die Stadtwerke gebeten, ihm den EDV-Ausdruck einer Liste zu überlassen, aus der ersichtlich sein sollte, in welchen Gebäuden zur Zeit kein oder ein Minimalverbrauch an elektrischem Strom festgestellt werden kann. Das Amt für Wohnungswesen möchte auf diese Weise leerstehende Wohnungen erfassen.

Die Stadtwerke haben gegenüber diesem Verlangen, das einer Rasterfahndung ähnlich ist, datenschutzrechtliche Bedenken geäußert. Diese Bedenken teile ich.

Die Stadtwerke sind ein Wettbewerbsunternehmen. Auf sie finden insoweit nicht die materiellen Vorschriften des Bayerischen Datenschutzgesetzes Anwendung, sondern die des Bundesdatenschutzgesetzes (Art. 22 BayDSG). Für die Übermittlung von Kundendaten der Stadtwerke ist § 24 BDSG anwendbar; in dieser Vorschrift sind die Voraussetzungen festgelegt, unter denen Daten über einzelne Kunden übermittelt werden dürfen. Bezogen auf diesen Fall bedeutet dies:

Als Zulässigkeitstatbestand für die Datenübermittlung an das Wohnungsamt kommt nur § 24 Abs. 1 Satz 1 3. Alternative BDSG in Betracht, da die Übermittlung von den Stadtwerken an das Amt für Wohnungswesen **anderen** als den Zwecken aus dem Vertrag der Stadtwerke mit einzelnen Kunden dient. Danach ist die Übermittlung personenbezogener Daten an das Amt für Wohnungswesen dann zulässig, wenn es zur Wahrung berechtigter Interessen der übermittelnden Stelle (= Stadtwerke) oder eines Dritten oder der Allgemeinheit erforderlich ist und dadurch schutzwürdige Belange des Betroffenen (= Kunden der Stadtwerke) nicht beeinträchtigt werden. Das BDSG spricht sich damit für eine Interessenabwägung aus.

Es mag sein, daß die Übermittlung des EDV-Ausdrucks von den Stadtwerken an das Amt für Wohnungswesen im Interesse der Allgemeinheit erforderlich ist, um leerstehenden Wohnraum zu erfassen. Die Zulässigkeit der Übermittlung scheitert jedoch daran, daß dadurch die schutzwürdigen Belange der betroffenen Kunden der Stadtwerke beeinträchtigt werden.

Schutzwürdige Belange sind grundsätzlich bereits dann beeinträchtigt, wenn der Betroffene seine Daten der speichernden Stelle zu ganz bestimmten Zwecken überläßt, der Informationsempfänger (hier: das Amt für Wohnungswesen) die Angaben aber für völlig andere Ziele nutzen will. Die Zweckbindung umschreibt die aus der Sicht des Betroffenen zulässige Verarbeitung seiner Daten. Der Kunde der Stadtwerke vertraut aufgrund der vertraglichen Zweckbindung darauf, daß seine Daten nur für die Zwecke verwendet werden, für die sie erhoben und gespeichert wurden. Die Übermittlung einzelner Daten an das Amt für Wohnungswesen wäre aber mit einer Zweckänderung verbunden. In diesem Zusammenhang ist noch zu bedenken, daß dem einzelnen Kunden die Stadtwerke bei der Strom- und Wasserversorgung als sog. Monopolbetrieb gegenüber stehen. Die Kundendaten werden also zwangsläufig bei den Stadtwerken gespeichert. Würde man diese Daten bei Verdacht auf Leerstehenlassen einer Wohnung dem Amt für Wohnungswesen übermitteln, so würde man eine Überwachungsmöglichkeit eröffnen, der sich der einzelne Kunde nicht entziehen könnte.

7.7 Weitergabe der Adressen von Aussiedlern an Beratungsdienste

Bereits im 11. Tätigkeitsbericht habe ich darauf hingewiesen, daß es nicht zulässig ist, Meldedaten von Aussiedlern ohne deren Einwilligung weiterzugeben. Die Meldedaten der Aussiedler werden oftmals angefordert, um die Aussiedler — sicher in bester Absicht — beim Start in ein neues Leben beraten zu können.

Ich halte es für besser, wenn die Aussiedler (z.B. beim Meldeamt) durch Informationsbroschüren auf diese Beratungsmöglichkeiten ausdrücklich aufmerksam gemacht werden. Es liegt dann am einzelnen Aussiedler, ob er von diesem Beratungsangebot Gebrauch macht. Nicht jeder Aussiedler möchte sich — aus welchen Gründen auch immer — automatisch und ohne seine vorherige Initiative von anderen Personen oder Institutionen beraten lassen. Eine Weitergabe der Aussiedlerdaten ohne deren vorherige Einwilligung wäre ein Eingriff in das informationelle Selbstbestimmungsrecht dieses Personenkreises.

7.8 Weitergabe einer Unterschriftenliste an die Feuerwehr

Eine Bürgerinitiative hat sich mit einer Eingabe an mich gewandt. Folgendes war passiert:

Der 1. Bürgermeister einer Gemeinde hat Unterschriftenlisten, die ihm eine Bürgerinitiative ausgehändigt hatte, an den Vorsitzenden des örtlichen Feuerwehrvereins und an den Kommandanten der Freiwilligen Feuerwehr weitergegeben. Die Unterschriftenlisten enthielten ca. 1.000 Namen, Adressen und Unterschriften von Gemeindebürgern, die sich gegen die geplante Erweiterung des Feuerwehrgerätehauses wandten.

Datenschutzrechtlich ist zu unterscheiden zwischen der Weitergabe der Unterschriftensammlung an den Kommandanten der Freiwilligen Feuerwehr und an den Vorsitzenden des Feuerwehrvereins:

- Die Weitergabe der Unterschriftensammlung an den Kommandanten der Freiwilligen Feuerwehr

  Die Freiwillige Feuerwehr ist eine Einrichtung, die gem. Art. 57 Abs. 1 Gemeindeordnung, Art. 1 Abs. 1 Bayer. Feuerwehrgesetz Pflichtaufgaben der Gemeinde wahrnimmt. Die Feuerwehr ist damit als **öffentliche Stelle** anzusehen.

  Die Datenübermittlung an öffentliche Stellen richtet sich nach Art. 17 BayDSG: Danach ist bei entsprechender Anwendung dieser Vorschrift 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 die Weitergabe der Unterschriftensammlung an den Kommandanten der Freiwilligen Feuerwehr zur rechtmäßigen Erfüllung der der Freiwilligen Feuerwehr zugewiesenen Aufgaben **erforderlich** war.

  Ich habe diese Frage verneint. Auch in Anbetracht der Aufgaben, welche die Freiwillige Feuerwehr für die Gemeinde zu erfüllen hat, ist es nicht erforderlich, daß der Feuerwehrkommandant Namen und Anschriften der sich gegen die Erweiterung des Feuerwehrgerätehauses wendenden Bürger erhält. Es reicht vollkommen aus, wenn der Feuerwehrkommandant über die **Tatsachen** dieses Widerstandes und über die **Anzahl** der Bürger, die sich gegen das Projekt wenden, informiert ist. Aus der Anzahl der Unterzeichner kann der Feuerwehrkommandant ersehen, wie gewichtig der Widerstand in der Gemeinde ist.

- Weitergabe an den Vorsitzenden des örtlichen Feuerwehrvereins

  Der Feuerwehrverein ist keine gemeindliche Einrichtung, sondern ein privater Verein; gegenüber der gemeindlichen Einrichtung Freiwillige Feuerwehr ist er selbständig.

  Die Weiterleitung der Unterschriftensammlung an den Vorsitzenden des Feuerwehrvereins ist datenschutzrechtlich als Übermittlung personenbezogener Daten **an Stellen außerhalb des öffentlichen Bereichs** anzusehen. Die Übermittlung personenbezogener Daten an Personen und an Stellen außerhalb des öffentlichen Bereichs ist gem. Art. 18 BayDSG (bei entsprechender Anwendung) zulässig, wenn sie zur rechtmäßigen Erfüllung der durch Rechtsnorm der übermittelnden Stelle zugewiesenen Aufgabe erforderlich ist oder soweit der Empfänger ein berechtigtes Interesse an der Kenntnis der zu übermittelnden Daten glaubhaft macht und dadurch schutzwürdige Belange des Betroffenen nicht beeinträchtigt werden.

  Entscheidend ist hier, daß ein **berechtigtes** Interesse des privaten Feuerwehrvereins an der Kenntnis der Namen der Unterzeichner nicht angenommen werden kann und im übrigen auch nicht glaubhaft gemacht wurde. Durch die Diskussion über den Standort des Feuerwehrgerätehauses wurden allenfalls mittelbar die Interessen des Vereins berührt. Außerdem wurden schutzwürdige Belange

der Unterzeichner durch die Weiterleitung der Unterschriftenliste an den Verein beeinträchtigt, weil durch das Bekanntwerden der Namen Spannungen zwischen Befürwortern und Gegnern des Vorhabens entstehen könnten, in die einzelne Unterzeichner möglicherweise nicht einbezogen werden wollen.

Ich habe meine Auffassung dem 1. Bürgermeister der Gemeinde mitgeteilt.

7.9 Zweckfremde Verwendung eines Kaufvertrages durch eine Gemeinde

Ein Bürger hat sich bei mir darüber beschwert, eine Marktgemeinde habe einen Grundstückskaufvertrag aus dem Jahr 1986 mit dem Voreigentümer seines Grundstückes gegen ihn im Rahmen von Kaufpreisverhandlungen im Jahre 1990 verwendet. Der Kaufvertrag war der Marktgemeinde seinerzeit zur Prüfung der Frage, ob das Vorkaufsrecht ausgeübt werden soll, vom Notar zugeleitet worden. Einen Teil des Grundstücks benötigte die Marktgemeinde nunmehr für Straßenbaumaßnahmen; zu diesem Zweck hat sie mit dem Bürger Verhandlungen aufgenommen. Dabei hat sie den Bürger darauf hingewiesen, er habe 1986 das Grundstück wesentlich billiger erworben; seine jetzigen Preisvorstellungen lägen beträchtlich darüber. Der Bürger hielt die Verwendung des Kaufvertrages aus dem Jahr 1986 in diesem Zusammenhang für unzulässig.

Nach meiner Auffassung liegt in der Heranziehung des Kaufvertrages im Rahmen der jetzigen Kaufpreisverhandlungen in der Tat eine datenschutzrechtlich unzulässige Zweckentfremdung des Kaufvertrages, den der Bürger vor Jahren mit dem Voreigentümer abgeschlossen hatte. Dieser Kaufvertrag ist der Marktgemeinde seinerzeit **zweckgebunden** zur Prüfung der Frage, ob das Vorkaufsrecht ausgeübt werden soll, zugeleitet worden. Im Rahmen der jetzigen Kaufpreisverhandlungen mit dem Bürger hätte er keine Verwendung finden dürfen.

Ich habe die Verwendung des Kaufvertrages gegen den Bürger im Rahmen dieser Kaufpreisverhandlungen durch die Marktgemeinde gerügt. Dieser Fall belegt einmal mehr die Forderung, daß die Notare den Gemeinden zur Prüfung der Frage, ob ein Vorkaufsrecht besteht, nicht den gesamten Kaufvertrag übersenden, sondern ihnen zunächst lediglich die Tatsache des Verkaufs mitteilen sollten.

7.10 Datenschutz bei Wahlen und Volksbegehren

Im Wahljahr 1990 (3 Wahlen, 1 Volksbegehren) hatte ich mich zu einer ganzen Reihe von datenschutzrechtlichen Fragen und Problemen zu äußern, die mir entweder durch die Wahlbehörden oder aus dem Kreis der betroffenen Personen und Unternehmen vorgetragen wurden.

7.10.1 Datenschutz für Unterstützungslisten bei Kommunalwahlen

Einem 3. Bürgermeister, der gleichzeitig Ortsvorsitzender einer politischen Partei ist, wurde vom Wahlleiter Einsicht in die vollständige Unterstützungsliste einer konkurrierenden Wählergemeinschaft gewährt, obwohl er weder dem Wahlausschuß angehörte noch sich selbst eintragen wollte. In der Unterstützungsliste fand er auch einige Namen seiner Parteigenossen. Seine Erkenntnisse benutzte er dazu, die Betroffenen durch massive Pressionen (bis hin zum Parteiausschluß) zur Rücknahme der Unterschrift zu veranlassen. Abgesehen davon, daß die Einsichtnahme in die Unterstützungsliste durch einen Unberechtigten unzulässig war, macht der Vorfall auch eine empfindliche datenschutzrechtliche Lücke im kommunalen Wahlrecht augenfällig.

Nach Art. 19 a Abs. 1 Satz 2 Gemeindewahlgesetz (GWG) haben sich die Wahlberechtigten, die einen Wahlvorschlag einer bisher noch nicht im Gemeinderat vertretenen Partei oder Wählergruppe unterstützen wollen, persönlich in eine vom Gemeindewahlleiter aufgelegte Liste einzutragen. Diese Liste steht allen Wahlberechtigten, die den Vorschlag durch ihre Unterschrift unterstützen wollen, in dem sich daraus notwendig ergebenden Umfang zur Einsicht offen. Bei der Unterschriftsleistung auf einer Liste werden die Unterzeichner zwangsläufig Kenntnis von Namen, Anschrift und Unterschrift der auf der gleichen Seite bereits stehenden Unterzeichner nehmen.

Die Wahlfreiheit der Bürger wird dann über Gebühr eingeschränkt, wenn sie damit rechnen müssen, daß ihre Unterschrift unter eine Unterstützungsliste zu Pressionen mißbraucht wird. Ich habe deshalb dem Staatsministerium des Innern eine Änderung des Gemeindewahlgesetzes dahingehend empfohlen, daß eine Beeinträchtigung schutzwürdiger Belange der Unterstützer von Wahlvorschlägen ausgeschlossen wird.

Das Ministerium hält zwar eine Änderung des Wahlgesetzes nicht für geboten, wird aber in den für die Wahlbehörden vorgesehenen Wahlbekanntmachungen deutlich darauf hinweisen, daß die Unterstützungslisten ausschließlich im Zusammenhang mit einer Unterschriftsleistung, jedoch **nicht von Dritten aus sonstigen Gründen** eingesehen werden darf.

7.10.2 Bekanntgabe von Wahlvorschlagsdaten zu Werbezwecken

Erneut haben ein nordrhein-westfälischer Verlag sowie einige Verbände die bayerischen Gemeinden um Übersendung der Wahlvorschläge der letzten Kommunalwahl gebeten.

Dem Verlag sowie den sonstigen an den Wahlvorschlägen Interessierten habe ich mitgeteilt, daß ich trotz des zeitlichen Zusammenhangs mit der Wahl 1990 die gewünschte Datenübermittlung für unzulässig halte, da die zu erwartende Speicherung sämtlicher Wahlbewerber und die kommerzielle Nutzung der Daten geeignet sein kann, schutzwürdige Belange einzelner Betroffener zu beeinträchtigen: Durch Vergleich mit den neuen Mandatsträgern sind Rückschlüsse auf Erfolg oder Mißerfolg der Wahlbewerber möglich. Außerdem könnten die Wahlbewerber von Produktwerbung belästigt werden.

Zwar waren die Wahlvorschläge seinerzeit aus **wahlrechtlichen** Gründen (örtlich begrenzt) der Öffentlichkeit zugänglich. Es wäre daher auch nicht zu verhindern gewesen, wenn sich die an den Daten Interessierten die veröffentlichten Wahlvorschläge durch beauftragte Privatpersonen hätten besorgen lassen, wie es z.B. von Versicherungen und Banken bei standesamtlichen Veröffentlichungen, insbesondere bei Aufgeboten praktiziert wird. Für unzulässig und mit dem Volkszählungsurteil 1983 nicht für vereinbar halte ich es aber, wenn bayerische Gemeinden durch die Übermittlung **wahlrechtlicher** Daten an einen Verlag oder andere private Interessenten für kommerzielle oder sonstige Zwecke an einer **Zweckentfremdung** der Wahlbewerberdaten mitwirken würden.

Das Staatsministerium des Innern, das diese Auffassung teilt, hat auf meine Bitte sämtliche bayerischen Gemeinden von der Unzulässigkeit der Datenübermittlung unterrichtet.

7.10.3 Volksbegehren „Das bessere Müllkonzept" — Schutz der Eintragungslisten

Zur Unterstützung des Volksbegehrens wurden bei den Gemeinden Eintragungslisten ausgelegt, in die sich die Unterstützer gemäß § 78 Abs. 1 der Landeswahlordnung mit Familienname, Vornamen, Geburtsdatum und Unterschrift einzutragen hatten. Ein Petent machte datenschutzrechtliche Bedenken mit der Begründung geltend, daß jeder Nachfolgende Kenntnis von den bereits eingetragenen Daten, insbesondere vom Geburtsdatum, nehmen könne. Zur Diskussion stand die Forderung, für jeden Eintragenden ein eigenes Unterschriftsblatt zur Verfügung zu stellen.

Diesen Vorschlag hielt ich im Hinblick auf die zu erwartende Vielzahl von Unterschriften und der damit verbundenen Gefahr des Verlusts für unverhältnismäßig. Der Persönlichkeitsschutz ist durch § 80 Abs. 5 der Landeswahlordnung ausreichend gewährleistet, wonach aus den Eintragungslisten keine Auskünfte erteilt und keine Aufzeichnungen zugelassen werden dürfen. Außerdem darf dem Eintragungsberechtigten nur die **laufende** Liste vorgelegt werden.

Diese Bestimmung wurde vom Staatsministerium des Innern in einer Vollzugsbekanntmachung zum Volksbegehren über den Entwurf eines Bayerischen Abfallwirtschaftsgesetzes wie folgt konkretisiert, so daß eine Beeinträchtigung schutzwürdiger Belange der Eintragenden unwahrscheinlich war:

„Die Eintragung in die Listen für das Volksbegehren geschieht zwar öffentlich. Bei den Eintragungslisten handelt es sich aber um amtliche Unterlagen, aus denen keine Auskünfte erteilt werden dürfen. Sie dürfen daher auch niemandem zur Einsicht vorgelegt werden. Nach Feststellung der Eintragungsberechtigung darf dem Betreffenden nur die laufende Liste des Volksbegehrens vorgelegt werden. Dabei muß er von dem Text und der Begründung des Volksbegehrens Kenntnis nehmen können. Nicht zu verhindern ist, daß er dabei die Namen der Personen erfährt, die sich in diese Liste bereits eingetragen haben. Er darf aber keine Aufzeichnungen machen. Die Listen liegen lediglich zur Eintragung und nicht zur Einsichtnahme auf."

8. Einwohnermeldewesen

8.1 Rechtliche Entwicklung

Im Berichtszeitraum hat sich in gesetzgeberischer Hinsicht wenig bewegt. So wurde der im 11. Tätigkeitsbericht erwähnte Änderungsentwurf zum Melderechtsrahmengesetz (MRRG) u.a. wegen Meinungsverschiedenheiten innerhalb der Bonner Regierungskoalition über die Hotel- und Krankenhausmeldepflicht nicht verabschiedet. Auch die Konferenz der Datenschutzbeauftragten des Bundes und der Länder befaßte sich mit dieser Problematik.

Ich teile nicht die verfassungsrechtlichen Bedenken gegen die geltende, im Melderechtsrahmengesetz des Bundes seit langem festgelegte Hotel- und Krankenhausmeldepflicht. Die Forderung nach Abschaffung dieser Meldepflicht im Zusammenhang mit der Novellierung des Gesetzes läßt sich keinesfalls auf verfassungsrechtliche Argumente stützen. Unzutreffend ist der Ansatz, die Hotel- und Krankenhausmeldepflicht diene ausschließlich polizeilichen Zwecken und sei deshalb materiell Polizeirecht. Vielmehr handelt es sich um Melderecht. So sind beispielsweise die Meldescheine von der Beherbergungsstätte ein Jahr zur Einsicht für die Polizei und die Meldebehörde bereitzuhalten und auf Verlangen auszuhändigen. Außerdem dienen die Hotelmeldescheine in Fremdenverkehrsorten der Berechnung der Kur- und Fremdenverkehrsabgabe. Die Auffassung der Mehrheit der Datenschutzbeauftragten bedeutet deshalb einen verfassungsrechtlichen Rückschritt in die Zeit vor Inkrafttreten des Grundgesetzes.

Es kann auch keine Rede davon sein, daß die bestehende Hotel- und Krankenhausmeldepflicht unverhältnismäßig tief in das informationelle Selbstbestimmungsrecht eingreife, wie die Mehrheit der Datenschutzbeauftragten behauptet. Diese Meldepflicht hat erhebliche Bedeutung für die Aufklärung von Vermißtenfällen und für die polizeiliche Fahndung. So konnten beispielsweise beim Polizeipräsidium München allein in der Zeit von 1985 bis 1990 durch Auswertung der Hotelmeldungen 447 Rechtsbrecher gefaßt werden. Die Mehrheit der Datenschutzbeauftragten verkennt, daß sich der allgemeine Sicherheitszustand bei Abschaffung der Hotelmeldepflicht nicht unerheblich verschlechtern würde. Ihre Abschaffung kann deshalb nicht mit verfassungs- und datenschutzrechtlichen Argumenten betrieben werden. Ähnliches gilt für eine Krankenhausmeldepflicht. Sie ist beispielsweise zur Aufklärung von Vermißtenfällen notwendig. Ferner sollte kein Anreiz für Straftäter geschaffen werden, im Krankenhaus unterzutauchen.

8.2 Prüfungen

Meine verstärkte Prüfungstätigkeit bei den Gemeinden im Einwohnermeldewesen habe ich im Berichtszeitraum fortgesetzt. Dabei habe ich in erster Linie die Rechtmäßigkeit, insbesondere die Erforderlichkeit weiterer von den verschiedenen Softwarehäusern angebotener und bei den Gemeinden eingesetzter Verfahren überprüft. Aber auch bei größeren Städten **selbst** entwickelte Verfahren wurden einer Überprüfung unterzogen.

Allgemein ist festzustellen, daß die hauptsächlichen Mängel, die ich bereits in früheren Tätigkeitsberichten ausführlich dargestellt habe, auch in den im Berichtszeitraum geprüften Verfahren in unterschiedlichem Umfang enthalten waren. Dies ist bedauerlich, zeigt es doch, daß Softwarehersteller meine in den Tätigkeitsberichten veröffentlichten Mängelbeschreibungen nicht ausreichend in ihre Programmorganisation (präventiv) einbeziehen. Auch meine Erwartung, daß die Städte und Gemeinden von sich aus aufgrund der Hinweise in den Tätigkeitsberichten Folgerungen für das eigene Einwohnerverfahren ziehen, hat sich bisher nicht erfüllt. Erst meine Beanstandung der jeweils geprüften Meldebehörden bewirkt, daß die Verfahrensmängel bereinigt werden.

Neben den bereits in früheren Tätigkeitsberichten dargestellten Mängeln, bin ich bei meinen Verfahrensprüfungen auf nachstehende Mängel und Probleme aufmerksam geworden:

8.2.1 Wehrüberwachung/Wehrerfassung bei Aus- und Übersiedlern, Eingebürgerten und aus dem Ausland und dem Land Berlin wieder Zuziehenden

Während die früher immer wieder beanstandete fehlerhafte Kennzeichnung der der Wehrüberwachung unterliegenden

Personen inzwischen weitgehend fehlerfrei erfolgt, wurde dem durch § 41 WPflG betroffenen Personenkreis bisher verfahrenstechnisch wenig Aufmerksamkeit zuteil.

Aus- und Übersiedler, Eingebürgerte, aus dem Ausland und dem Land Berlin wieder Zuziehende werden erst nach Ablauf von **zwei Jahren** wehrpflichtig; sie sind demnach nicht, wie vielfach geschehen, bereits mit dem Zuzug, sondern erst nach Ablauf der Zweijahresfrist als Wehrpflichtige zu **erfassen**.

Da eine Kennzeichnung im Melderegister als Aus- oder Übersiedler oder als Eingebürgerter melderechtlich unzulässig ist, habe ich den geprüften Meldebehörden folgende Verfahrensweise vorgeschlagen:

a) Eine Speicherung darf im Zusammenhang mit Art. 3 Abs. 2 Nr. 4 MeldeG nur als sog. Hinweisdatum, und zwar in allgemeiner Form (z.B. als Datumsfeld „Erfassung erst am ...") vorgenommen werden. Dadurch ist im Einzelfall nicht erkennbar, ob der Betroffene Aussiedler, Übersiedler, Eingebürgerter, aus dem Ausland oder aus Berlin wieder Zuziehender ist.

b) Der Hinweis darf nur bei den durch § 41 WPflG Betroffenen, das sind **männliche Deutsche zwischen 16 und 32 Jahren**, gespeichert werden.

c) Es ist zu gewährleisten, daß der Hinweis unmittelbar nach der Wehrerfassung **gelöscht** wird. Bis zu diesem Zeitpunkt dürfen die Daten keinem unbefugten Dritten zur Kenntnis gebracht, insbesondere dürfen keine Auswertungen für andere als Wehrerfassungszwecke gefertigt werden. Eine Übermittlung der Daten des betroffenen Personenkreises an das Kreiswehrersatzamt (§ 2 2. BMeldDÜV) hat während der beiden Jahre zu unterbleiben.

8.2.2 Melderegisterauskünfte über JVA-Insassen und über Patienten in Bezirkskrankenhäusern

Bei meinen datenschutzrechtlichen Überprüfungen habe ich festgestellt, daß dem Persönlichkeitsrecht von Strafgefangenen und von Patienten in Bezirkskrankenhäusern nicht immer in ausreichendem Maße Rechnung getragen wird.

So fand ich unter der — zumindest regional allgemein bekannten — Anschrift einer Justizvollzugsanstalt sowie eines Bezirkskrankenhauses im Adreßbuch die Namen von JVA-Insassen und von Patienten.

Das Meldegesetz erlaubt Auskünfte (hier an den Adreßbuchverlag) nur dann, wenn die Meldebehörde durch Prüfung im Einzelfall festgestellt hat, daß schutzwürdige Belange des Betroffenen nicht beeinträchtigt werden. Vor Melderegisterauskünften ist der Betroffene (JVA-Insasse oder Patient des Bezirkskrankenhauses) zu hören (Art. 25 Abs. 4 MeldeG).

Ich habe den beanstandeten Meldebehörden nahegelegt, bei dem betroffenen Personenkreis von Amts wegen eine Auskunftssperre nach Art. 35 Abs. 3 MeldeG (keine Melderegisterauskunft an Adreßbuchverlage) zu speichern.

8.3 Hinweis zum Melderegister

Löschung der Seriennummern des Passes oder Personalausweises im Melderegister

Im Datensatz für das Meldewesen dürfen gegenwärtig noch die Paß- und Personalausweis-Seriennummern gespeichert werden. Diese Speicherung ist allerdings ab **1. September 1991** gemäß § 3 Abs. 4 PAuswG, § 16 Abs. 4 PaßG nicht mehr zulässig. Ich habe den überprüften Behörden empfohlen, schon jetzt an die Schaffung einer entsprechenden Routine für Sperrung oder Löschung zu denken.

8.4 Übermittlungen und Auskünfte aus dem Melderegister

8.4.1 Begrenzung des Online-Zugriffs auf Melderegisterdaten

Nach Art. 31 Abs. 7 und 1 MeldeG darf die Meldebehörde anderen kommunalen Dienststellen innerhalb der Gemeinde bzw. Verwaltungsgemeinschaft Melderegisterdaten übermitteln, soweit diese Daten zur rechtmäßigen Erfüllung der Aufgaben des Datenempfängers **erforderlich** sind. Diese Übermittlung ist auch im Online-Zugriff der Empfängerbehörde zulässig.

Der Grundsatz der **Erforderlichkeit** bleibt meinen Erfahrungen zufolge jedoch häufig unbeachtet, insbesondere weil manche Software-Anbieter den Gemeinden keine variablen, auf die jeweilige Aufgabenerfüllung abgestellten Bildschirmmaskeninhalte zur Verfügung stellen. So erhält beispielsweise ein Standesbeamter mit der sog. Universalauskunft auch die Wahlausschluß-, Paß- und Personalausweisdaten sowie Wehrüberwachungs- und lohnsteuerrelevante Daten, die für seine Tätigkeit nicht erforderlich und daher unzulässig sind.

Die Anstalt für Kommunale Datenverarbeitung in Bayern (AKDB) bietet ihren Anwendern verschiedene Verfahren im Einwohnerwesen an. Ein (dezentrales) Verfahren verfügt über variable Bildschirmmasken, so daß dem Grundsatz der Erforderlichkeit Rechnung getragen werden kann. Die beiden teildezentralen Verfahren haben ein Standardpaket mit festen Abfragemasken für die wichtigsten Dienststellen; die AKDB arbeitet an einem Projekt, das bis Herbst 1991 auch im teildezentralen Verfahren variable Bildschirmmasken vorsieht.

8.4.2 Regelmäßige Weitergabe von Meldeamtslisten über alle Zu-, Um- und Wegzüge an andere gemeindliche Dienststellen

Zahlreiche gemeindliche Fachabteilungen (z.B. Steueramt) sind zur Fortführung und Bereinigung ihres eigenen Adreßbestandes an regelmäßigen Informationen über Zu-, Um- und Wegziehende durch die Meldebehörde interessiert. Sie werden häufig durch Weitergabe von Listen über die Meldebewegungen unterrichtet.

Nach Art. 31 Abs. 1 und 7 MeldeG darf die Meldebehörde Meldedaten an andere gemeindliche Dienststellen weitergeben, sofern dies zur rechtmäßigen Aufgabenerfüllung des Datenempfängers **erforderlich** ist.

Da nicht jeder Zu-, Um- oder Wegziehende zu der datenempfangenden Dienststelle in Beziehung steht (z.B. ist nicht jeder Umziehende, dessen Daten an das gemeindliche Steueramt übermittelt werden, auch Abgabepflichtiger), werden mit der Listenübersendung zwangsläufig mehr Daten als erforderlich übermittelt. Andererseits verbietet das Melderecht eine Kennzeichnung der Betroffenen z.B. als Abgabepflichtige, Sozialhilfe- oder Wohngeldempfänger, so daß eine Selektierung des für den einzelnen Datenempfänger relevanten Personenkreises durch die Meldebehörde unmöglich ist.

Um hier einen Ausgleich zwischen dem Informationsbedarf der gemeindlichen Dienststellen zur Aktualisierung des eigenen Adressenbestandes und den schutzwürdigen Belangen der betroffenen Bürger zu schaffen, hat der Beirat beim Landesbeauftragten für den Datenschutz meinem Vorschlag zugestimmt, daß die regelmäßige Weitergabe von Meldeamtslisten an andere gemeindliche Dienststellen dann als zulässig anzusehen ist, wenn **die nicht erforderlichen Daten** nach der Auswertung durch die Datenempfänger zuverlässig gelöscht werden. Das Staatsministerium des Innern hat diese Haltung begrüßt.

8.4.3 Übermittlung von Jubiläumsdaten an das Bayerische Rote Kreuz

Ein BRK-Kreisverband beabsichtigt, älteren Gemeindebürgern zum Geburtstag zu gratulieren und die Jubilare mit einer kleinen Aufmerksamkeit zu beschenken.

Die Meldebehörde, die um Übermittlung der Jubiläumsdaten ersucht wurde, hat dies aus Gründen des Datenschutzes abgelehnt.

Diese Haltung ist nicht zu beanstanden. Da das BRK eine Körperschaft des öffentlichen Rechts ist, sind Datenübermittlungen aus dem Melderegister an Art. 31 Abs. 1 MeldeG zu messen. Danach **darf** die Meldebehörde Meldedaten an eine andere öffentliche Stelle — ohne Einwilligung der Betroffenen — nur übermitteln, wenn es zur rechtmäßigen Aufgabenerfüllung (hier des BRK) **erforderlich** ist. Geburtstagsgrüße an alle älteren Mitbürger gehören nicht hierher.

Da die Bekanntgabe der Jubiläumsdaten darüber hinaus **regelmäßig** gewünscht wird, müßte die Datenübermittlung außerdem in einer Rechtsverordnung im Sinne von Art. 31 Abs. 5 MeldeG vorgesehen sein.

Sollte die Meldebehörde allerdings im Rahmen des Art. 35 Abs. 2 MeldeG Jubiläumsdaten unter Beachtung des für die Bürger bestehenden Widerspruchrechts öffentlich bekanntmachen (z.B. im gemeindlichen Mitteilungsblatt), hätte ich keine Bedenken, wenn das BRK diese Veröffentlichungen für Gratulationszwecke auswerten oder diese Jubiläumsdaten unmittelbar vom Einwohnermeldeamt erhalten würde.

8.4.4 Meldedatenübermittlung zum Zwecke der Kindergarten- und Kinderhortbedarfsplanung

Wiederholt habe ich mich mit der Frage befaßt, ob den kommunalen oder kirchlichen Kindergarten- und Kinderhortträgern zur Bedarfsplanung folgende Daten der in Frage kommenden Kinder mitgeteilt werden dürfen:
- Name, Vornamen
- Geburtsdatum
- Wohnanschrift.

Eine solche Mitteilung personenbezogener Daten liefe dem in Art. 31 Abs. 1 MeldeG, Art. 17 Abs. 1 BayDSG normierten Erforderlichkeitsgrundsatz zuwider. Es ist kein vernünftiger Grund ersichtlich, weshalb die gewünschten personenbezogenen Daten für die Kindergarten- und Kinderhortplanung von Bedeutung sein sollten.

Nach meinem Dafürhalten würde es für Planungszwecke genügen, die **Zahl der pro Geburtsjahrgang** im Planungsgebiet in Frage kommenden Kinder mitzuteilen.

Ein Kindergartenträger wollte außer der personenbezogenen Auskunft über die Kinder wissen, ob für beide Elternteile (als Indiz dafür, daß beide berufstätig sind) eine Lohnsteuerkarte ausgestellt wurde. Abgesehen davon, daß solche Informationen gegen das Steuergeheimnis (§ 30 AO) verstoßen würden, halte ich sie auch für wenig aussagekräftig, weil einerseits nicht jeder Lohnsteuerkarteninhaber berufstätig ist, andererseits Selbständige keine Lohnsteuerkarte benötigen.

Den Meldebehörden habe ich deshalb von solchen Datenübermittlungen abgeraten.

8.4.5 Melderegisterauskünfte an Kreditauskunfteien u.ä.

Im 10. Tätigkeitsbericht habe ich bereits das Geschäftsgebaren einer Kreditauskunftei behandelt. Auch im Berichtszeitraum haben sich besorgte Bürger und Gemeinden über die Zulässigkeit von Melderegisterauskünften an solche Unternehmen erkundigt.

Z.B. wurde eine Petentin von ihrem Einwohneramt verständigt, daß über sie eine sog. erweiterte Melderegisterauskunft an eine Kreditauskunftei erteilt worden sei, weil dem Auskunftsersuchen ein „berechtigtes Interesse", das mit „Kreditentscheidung" begründet wurde, zugrundegelegen hätte.

Da die Petentin keinerlei Kredite beantragt hatte, stellte sie begreiflicherweise die Rechtmäßigkeit des Auskunftsersuchens und der erteilten Melderegisterauskunft in Frage.

Die mir vorgetragenen Bedenken sind Anlaß, mich etwas ausführlicher mit dem Thema zu befassen. Zunächst einige allgemeine Bemerkungen zur „erweiterten" Melderegisterauskunft:

Neben der sogenannten einfachen Melderegisterauskunft (Name, Anschrift, akademischer Grad), die der Gesetzgeber von keinen besonderen Voraussetzungen abhängig gemacht hat (Art. 34 Abs. 1 MeldeG), darf die Meldebehörde nach Art. 34 Abs. 2 MeldeG bei Glaubhaftmachung eines „berechtigten Interesses" eine erweiterte Melderegisterauskunft über nachstehende Daten eines Einwohners erteilen:
- Tag und Ort der Geburt,
- frühere Vor- und Familiennamen,
- Familienstand, beschränkt auf die Angabe, ob verheiratet oder nicht,
- Staatsangehörigkeit,
- frühere Anschriften,
- Tag des Ein- und Auszugs,
- gesetzlicher Vertreter sowie
- Sterbetag und -ort.

Zum Ausgleich für die Herausgabe dieser zusätzlichen persönlichen Daten hat die Meldebehörde den Betroffenen über die Erteilung einer erweiterten Melderegisterauskunft unter Angabe des Datenempfängers unverzüglich zu unterrichten, es sei denn, daß der Anfrage ein „rechtliches Interesse" (z.B. ein vollstreckbarer Titel) zugrunde gelegen hat.

Kreditauskunfteien, Inkassobüros, Rechtsanwälte usw. haben in der Regel ein „berechtigtes Interesse" an einer erweiterten Auskunft, deren Hintergrund Geschäftsanbahnungen, Kreditentscheidungen, aber auch die Ermittlung eines Schuldners usw. sind. Das damit begründete „berechtigte Interesse" hat der Auskunftsuchende für jedes einzelne Datum glaubhaft zu machen. Veranlaßt kann das Auskunftsbegehren sein durch einen Geschäftsmann, Kreditunternehmer oder Gläubiger, der die Kreditauskunftei beauftragt hat,

über eine bestimmte Person Informationen einzuholen und mitzuteilen. Die Kreditauskunftei wird zur Erfüllung ihres Geschäftszwecks (Auskunftserteilung bei künftigen Anfragen) die eingeholten Informationen speichern (was nach dem vierten Abschnitt des Bundesdatenschutzgesetzes grundsätzlich zulässig ist). Hingegen kann die Auskunftei nach meiner Auffassung allein aus ihrem allgemeinen Geschäftszweck, Daten zu sammeln und zu speichern, in der Regel kein berechtigtes Interesse an einer erweiterten Auskunft ableiten.

Zu dem bei der erweiterten Melderegisterauskunft glaubhaft zu machenden berechtigten Interesse zählt **jedes von der Rechtsordnung erlaubte, insbesondere auch ein wirtschaftliches** Interesse.

Dieses berechtigte Interesse muß in der Regel bei demjenigen liegen, der die Kreditauskunftei mit der Auskunftseinholung beauftragt. Die Auftraggeber, z.B. Banken, Sparkassen, Geschäfte sind meist nicht in der Lage, vor Bonitätsprüfungen zu angemessenen wirtschaftlichen Bedingungen die notwendigen Informationen in Eigenregie zu beschaffen. Es ist üblich, sich solche Informationen von darauf spezialisierten Betrieben besorgen zu lassen.

Die Frage, ob hinter der Auskunftei ein Auftraggeber steht und wer das ist, kann für die Glaubhaftmachung des berechtigten Interesses an der erweiterten Auskunft von Bedeutung sein. Man könnte sich daher mit einer Eingabe an die Meldebehörde wenden und vorbringen, daß die Meldebehörde der Auskunftei keine erweiterte Auskunft hätte geben dürfen. Dann wird die Meldebehörde das berechtigte Interesse an der erweiterten Auskunft über die betroffene Person unter Berücksichtigung dessen Vorbringens nochmals überprüfen müssen. Sollte die Auskunftei das berechtigte Interesse zu Unrecht geltend gemacht haben, werden hieraus Konsequenzen zu ziehen sein. Beispielsweise kann nach Art. 39 Nr. 1 des Meldegesetzes mit Geldbuße bis zu 50.000,-- Deutsche Mark belegt werden, wer unrichtige oder unvollständige Angaben macht oder benutzt, um für sich oder einen anderen die Erteilung einer erweiterten Melderegisterauskunft zu erwirken.

Außerdem kann sich der Bürger, über den eine Meldebehörde eine erweiterte Auskunft an eine Auskunftei erteilt hat, mit einer Beschwerde über die Auskunftei an die zuständige Aufsichtsbehörde für den Datenschutz im nichtöffentlichen Bereich (in Bayern die Regierungen) wenden. Die Aufsichtsbehörde für den Datenschutz wird dann den Sachverhalt aufklären und prüfen, ob die Auskunftei gegen das Bundesdatenschutzgesetz verstoßen hat.

8.5 Adressen für politische Parteien und Wählergruppen zur Wahlwerbung

Ein oft behandeltes Thema in den Tätigkeitsberichten ist die Weitergabe von Wähleranschriften an politische Parteien und Wählergruppen gemäß Art. 35 Abs. 1 Bayer. Meldegesetz (MeldeG). Danach darf die Meldebehörde den Parteien und Wählergruppen im Zusammenhang mit allgemeinen Wahlen und Abstimmungen in den sechs der Stimmabgabe vorangehenden Monaten Auskunft aus dem Melderegister über Vor- und Familiennamen, akad. Grad und Wohnanschrift **von Gruppen von Wahlberechtigten erteilen, für deren Zusammensetzung das Lebensalter der Betroffenen bestimmend ist.**

Jeder betroffene Wahlberechtigte hat das Recht, ohne Nennung von Gründen, der Weitergabe seiner Daten zu widersprechen. Der Widerspruch ist gegenüber der Meldebehörde zu erklären.

Auch im Wahljahr 1990 hatte ich zahlreiche Bürger- und Behördenanfragen zu beantworten. Folgende Themen sind von allgemeinem Interesse:

8.5.1 Ist eine Auswahl der „Gruppe von Wahlberechtigten" außer nach dem Lebensalter auch nach dem Geschlecht und/oder ortsteilbezogen zulässig?

Dem Staatsministerium des Innern habe ich zu dieser Frage folgende Auffassung mitgeteilt:

„In der Tat spricht aus datenschutzrechtlicher Sicht einiges dafür, eine geschlechts- bzw. ortsteilbezogene Auswahl zuzulassen, weil es ohnehin für die Empfänger (insbesondere bei Übermittlung der Wähleranschriften auf automatisierten Datenträgern) unproblematisch wäre, aus den Vornamen und Straßenbezeichnungen die gewünschten Informationen zu selektieren. Eine geschlechts- bzw. ortsteilbezogene Übermittlung der Wähleranschriften würde **verhindern**, daß die Parteien und Wählergruppen **mehr** Daten als gewünscht erhielten. Der Grundsatz der Erforderlichkeit wäre gewahrt; eine mögliche (mißbräuchliche) Nutzung der nicht gewünschten Daten entfiele."

Wegen der nicht ganz eindeutigen Formulierungen in Art. 35 Abs. 1 MeldeG halte ich nachstehende Auffassung des Staatsministeriums des Innern für einen vertretbaren Kompromiß:

„Nach Auffassung der Innenminister/-senatoren der Länder darf die Auswahl der Gruppen von Wahlberechtigten **nicht** nach dem **Geschlecht** vorgenommen werden. Die Meldegesetze lassen eine Differenzierung nur nach dem Lebensalter zu.

Dagegen bestehen nach unserer Auffassung gegen eine **ortsteilbezogene** Datenweitergabe an Parteien und Wählergruppen keine rechtlichen Bedenken. Dem Datenempfänger wird in diesen Fällen nur ein Teil der nach Art. 35 Abs. 1 MeldeG zulässigen Wähleranschriften mitgeteilt. Diese Verfahrensweise ist bei Meldebehörden größerer Städte unerläßlich."

8.5.2 Darf die Meldebehörde der Jugendorganisation einer politischen Partei Wähleranschriften übermitteln?

Art. 35 Abs. 1 MeldeG bestimmt eindeutig, daß Empfänger von Wähleranschriften ausschließlich Parteien (im Sinne des Parteiengesetzes) und Wählergruppen sein dürfen. Jugendorganisationen politischer Parteien kommen als Datenempfänger schon deshalb nicht in Betracht, weil nur die **berechtigte** Partei oder Wählergruppe dem Löschungsgebot (Löschung der übermittelten Adressen spätestens einen Monat nach der Wahl) entsprechen muß und dem Zweckbindungsgrundsatz sowie evtl. behördlichen Auflagen und Bedingungen unterliegt.

8.6 Ausstellung einer Lebensbescheinigung für Kinder geschiedener Eltern trotz Auskunftssperre im Melderegister

Ein geschiedener Vater beantragte von einer Meldebehörde Lebensbescheinigungen seiner Kinder zur Vorlage beim Finanzamt. In den Meldedatensätzen der Kinder waren Aus-

kunftssperren nach Art. 34 Abs. 5 MeldeG (Gefahr für Leben, Gesundheit, persönliche Freiheit oder ähnliche schutzwürdige Belange) gespeichert. Die Frage, ob dem Vater trotz der eingetragenen Auskunftssperren die Lebensbescheinigungen ausgestellt werden dürfen, mußte ich im Einvernehmen mit dem Staatsministerium des Innern verneinen, damit die Kinder nicht gefährdet werden.

Ich habe folgende Lösungswege angeboten:

- Die geschiedene Frau erteilt der Meldebehörde ihre Einwilligung, daß die Lebensbescheinigungen an den Vater der Kinder geschickt werden. Dabei wird auf die Angabe der genauen Wohnanschrift verzichtet,

  oder

- die Meldebehörde setzt sich mit dem zuständigen Finanzamt in Verbindung und sendet ggf. die Lebensbescheinigungen unmittelbar dorthin. Dabei weist die Meldebehörde ausdrücklich auf das Bestehen einer Auskunftssperre nach Art. 34 Abs. 5 MeldeG hin, um zu verhindern, daß dem Vater im Wege der Akteneinsicht in seine Steuerunterlagen die Wohnanschrift der Kinder zur Kenntnis gelangt.

8.7 Gästemeldescheine in Fremdenverkehrsorten

Das Beherbergungsgewerbe hat besondere Meldescheine für die Gäste bereitzuhalten. In Fremdenverkehrsorten dient der Durchschlag des Meldescheins der Gemeinde zur Berechnung des Kurbeitrages bzw. der Kurtaxe. Das Original verbleibt beim Leiter der Beherbergungsstätte, der den Meldeschein gem. Art. 27 Abs. 4 MeldeG vor unbefugter Einsichtnahme zu sichern hat. Verstöße gegen die Aufbewahrungspflicht können als Ordnungswidrigkeit mit einer Geldbuße bis zu 1.000,-- DM belegt werden.

Es ist üblich, daß die Fremdenverkehrsgemeinden den örtlichen Beherbergungsbetrieben die Gästemeldescheine in **Blockform** zur Verfügung stellen. Aus einer Eingabe erfuhr ich, daß der für den Beherbergungsbetrieb vorgesehene Meldeschein entgegen Art. 27 Abs. 4 MeldeG im Block verbleibt und dadurch die Daten der bereits gemeldeten Personen einem nachfolgenden Gast zur Kenntnis gelangen können. Diese Praxis verstößt gegen den Datenschutz.

Die von den Gemeinden zur Verfügung gestellten Meldeblöcke sind bei dieser Verfahrensweise geeignet, das informationelle Selbstbestimmungsrecht des Gastes zu verletzen. Außerdem werden die Beherbergungsbetriebe durch die Blockform dazu verleitet, sich ordnungswidrig zu verhalten, weil ihnen vielfach die Pflicht zur Sicherung der Meldedaten vor unbefugter Einsichtnahme nicht ausreichend bekannt ist.

Ich habe deshalb die Staatsministerien des Innern und für Wirtschaft und Verkehr sowie den Landesfremdenverkehrsverband und den Bayerischen Gemeindetag auf diese Problematik aufmerksam gemacht und gebeten, die Fremdenverkehrsgemeinden aufzufordern, entweder keine Meldescheinblöcke mehr an die Beherbergungsbetriebe auszugeben oder dafür zu sorgen, daß die Beherbergungsbetriebe bei jeder Ausgabe eines Meldescheinblockes deutlich auf die melderechtlichen Sicherungspflichten und die Bußgeldbestimmung (z.B. durch ein entsprechendes Deckblatt auf jedem Block) hingewiesen werden.

9. Steuerverwaltung

9.1 Datenschutzvorschriften in der Steuerverwaltung

Im 11. Tätigkeitsbericht habe ich deutlich gemacht, daß das Steuergeheimnis eine wirksame Datenschutzkontrolle verhindert, solange es von der Finanzverwaltung auch den Datenschutzbeauftragten entgegen gehalten werden kann. Dieses Kontrollhindernis soll nunmehr durch das neue Bundesdatenschutzgesetz aus dem Weg geräumt werden: Nach § 24 Abs. 2 erstreckt sich die Kontrolle durch die Datenschutzbeauftragten des Bundes auch auf personenbezogene Daten, die dem Steuergeheimnis nach § 30 der Abgabenordnung unterliegen.

Da § 24 Abs. 6 des neuen Bundesdatenschutzgesetzes die Kontrollbefugnis des Abs. 2 hinsichtlich der dem Steuergeheimnis unterliegenden Daten auch für die Landesdatenschutzbeauftragten für entsprechend anwendbar erklärt, werden die in meinem 11. Tätigkeitsbericht geschilderten Schwierigkeiten bei der Kontrolle der staatlichen Steuerverwaltung, die sich aus dem Steuergeheimnis ergaben, mit dem Inkrafttreten des neuen Bundesdatenschutzgesetzes der Vergangenheit angehören.

9.2 Übergangsbonus für Kontrollmitteilungen abgelaufen

Zur Sicherung der Besteuerung hat die Bundesregierung seit Inkrafttreten des § 93 a Abgabenordnung (Steuerbereinigungsgesetz 1986 vom 19. Dezember 1985) die Möglichkeit, durch Rechtsverordnung Behörden zu verpflichten, allgemeine Kontrollmitteilungen über Zahlungen z.B. aus Werk- oder Dienstverträgen an die Finanzämter zu schicken. Bis zum Erlaß dieser Rechtsverordnung, der Kontrollmitteilungsverordnung, die von der Finanzverwaltung immer wieder angekündigt worden war, hatte ich in der Übergangszeit gegen die eingeschränkte Fortführung der bisherigen Kontrollmitteilungspraxis unter dem Gesichtspunkt des sogenannten Übergangsbonus keine Einwendungen erhoben. In der Übergangszeit sollten in den Kontrollmitteilungen nur noch die identifizierenden Daten des Leistungsempfängers, Art und Zeitpunkt der Leistung, nicht hingegen die Höhe des gezahlten Betrags dem für die Besteuerung zuständigen Finanzamt mitgeteilt werden. Die Betragshöhe erklärt der Leistungsempfänger bei Abgabe seiner Einkommensteuererklärung.

Als schließlich auch zu Beginn des Berichtszeitraums der Erlaß der Kontrollmitteilungsverordnung noch nicht absehbar war, habe ich dem Finanzministerium mitgeteilt, daß ich mit dem 1. Juli 1990 die Übergangszeit als abgelaufen betrachten werde, da es für ein weiteres Hinauszögern der Verordnung keine sachlichen Gründe gebe. Mit Rundschreiben vom 21. Juni 1990 hat daraufhin das Finanzministerium allen Ministerien folgendes mitgeteilt: „Solange die Rechtsverordnung zur Ausführung des § 93 a AO nicht ergangen ist, besteht keine ausreichende Rechtsgrundlage für die allgemeine Übermittlung von Kontrollmitteilungen an die Finanzämter. Nachdem mit dem Ergehen der Verordnung zu § 93 a AO (Mitteilungsverordnung) in absehbarer Zeit nicht zu rechnen ist, bitte ich, von der bisherigen Praxis allgemeiner Kontrollmitteilungen Abstand zu nehmen und die jeweils nachgeordneten Dienstbehörden entsprechend zu unterrichten."

Ich begrüße diese Entscheidung des Finanzministeriums,

weil sie dem Recht auf informationelle Selbstbestimmung auch in der Steuerverwaltung Geltung verschafft.

Das Finanzministerium vertritt allerdings die Auffassung, Kontrollmitteilungen, die weiterhin entgegen dieser Entscheidung bei den Finanzämtern eingehen, unterlägen keinem Verwertungsverbot, dürften also von der Steuerbehörde verwendet werden. Diese Auffassung widerspricht jedoch dem Grundsatz, daß der Staat Rechtsverletzungen zu unterlassen, geschehene Rechtsverletzungen unter dem Gesichtspunkt des Folgenbeseitigungsanspruchs rückgängig zu machen hat. Allgemeine Kontrollmitteilungen, die nach dem 1. Juli 1990 den Finanzämtern zugehen, dürfen deshalb nach meiner Auffassung nicht ausgewertet und aufbewahrt werden, sondern sind zu vernichten.

9.3 Lohnsteuerkarten für Gefangene

Wenn ein entlassener Strafgefangener sich um einen Arbeitsplatz bewirbt und dabei dem Arbeitgeber die Lohnsteuerkarte vorlegt, in der als Meldeadresse die Anschrift der früheren Haftanstalt eingetragen ist, muß er dem Arbeitgeber konkludent mitteilen, daß er soeben aus der Haft entlassen worden ist. Diese Information ist weder vom Melderecht beabsichtigt, noch dient sie der Resozialisierung des Entlassenen. Er muß sich zwangsläufig, ohne daß der Arbeitgeber danach fragt, diesem gegenüber bloßstellen. Die unbeabsichtigte Zusatzinformation greift unnötig in sein Persönlichkeitsrecht ein. Seit längerem versuche ich deshalb, mit den Staatsministerien der Finanzen und der Justiz eine Regelung zu finden, bei der die Anschrift der Haftanstalt nicht mehr auf der Lohnsteuerkarte erscheint.

Eine Verbesserung des Persönlichkeitsschutzes hat die Anordnung des Finanzministeriums vom 20. Juli 1989 gebracht: Danach sind die Gefangenen, die unter der Anschrift der Justizvollzugsanstalt gemeldet sind, darauf hinzuweisen, daß sie während ihrer Haft auf die Ausstellung einer Lohnsteuerkarte verzichten können. Die nachträgliche Ausstellung kann dann nach der Haftentlassung beantragt werden. Für die Ausstellung ist zwar nach wie vor die Gemeinde örtlich zuständig, in deren Bezirk sich die Anstalt befindet. Die Ausstellung ist aber mit der Abmeldung und der Anmeldung bei der ersten Wohnsitzgemeinde nach der Haftentlassung in der Weise zu verbinden, daß die zuständige Gemeinde zwar die Lohnsteuerkarte ausstellt, als Wohnanschrift aber die neue Meldeadresse einträgt.

Dem Justizministerium genügt diese Regelung nicht, weil sie den Belangen der Wiedereingliederung der Gefangenen nicht ausreichend Rechnung trage. Dem Gefangenen sollten bei seiner Entlassung in die Freiheit sämtliche notwendigen Papiere ausgehändigt werden können.

Nach meiner Auffassung nimmt die Anordnung des Finanzministeriums (Ausstellung der Lohnsteuerkarte nach der Haftentlassung mit der neuen Meldeadresse) nicht nur ausreichend Rücksicht auf das Persönlichkeitsrecht des ehemaligen Häftlings, sondern nützt auch der Wiedereingliederung mehr als eine Lohnsteuerkarte, die ihn für den kundigen Personalchef sofort als Strafentlassenen ausweist. Den Vorschlag des Justizministeriums könnte ich deshalb nur unterstützen, wenn dem Gefangenen bei seiner Entlassung eine Lohnsteuerkarte mit der neuen Meldeadresse ausgehändigt wird.

9.4 Gewerbesteuermeßbescheide an Gemeinden

Der Bund der Steuerzahler in Bayern bat mich um Unterstützung seiner Forderung, daß die Finanzämter den gemeindlichen Steuerbehörden nur den notwendigen Inhalt des Gewerbesteuermeßbescheides übermitteln. Ich habe dieses Anliegen gerne erneut aufgegriffen.

Das Steuerbereinigungsgesetz 1986 schuf in § 184 Abs. 3 der Abgabenordnung die Rechtsgrundlage zur Übermittlung des „Inhalts des Steuermeßbescheides" an die kommunalen Steuerämter. Diese Regelung fand nicht die Zustimmung der Datenschutzbeauftragten. Denn mit den Gewerbesteuermeßbescheiden erhalten die kommunalen Steuerbehörden Kenntnis über interne Geschäftsdaten, wie Gewinn, Einheitswert des Gewerbebetriebs, Dauerschulden und Dauerschuldzinsen, obwohl zur Berechnung der Gewerbesteuer der vom Finanzamt festgestellte Gewerbesteuermeßbetrag genügt. Nur in wenigen Ausnahmefällen, z.B. bei Zerlegung, könnte für Rechtsbehelfsverfahren der Gemeinden die Kenntnis von betrieblichen Einzeldaten erforderlich werden. Diese Ausnahmefälle rechtfertigen es aber nicht, alle Gewerbesteuermeßbescheide vollinhaltlich den gemeindlichen Steuerbehörden zuzusenden. Bei dieser Vorgehensweise ist eine unnötige Gefährdung des Steuergeheimnisses, insbesondere in kleinen Gemeinden, nicht auszuschließen.

Ich habe deshalb den Bundesbeauftragten für den Datenschutz gebeten, beim Bundesfinanzminister auf eine datenschutzfreundliche Änderung des § 184 der Abgabenordnung zu drängen.

Der Bayerische Staatsminister der Finanzen, dem ich meine Auffassung ebenfalls mitgeteilt habe, stimmt in seiner Stellungnahme der geforderten Reduzierung der zu übermittelnden Daten aus dem Gewerbesteuermeßbescheid grundsätzlich zu, sieht derzeit allerdings nur geringe Chancen zu einer Änderung, weil § 184 Abs. 3 der Abgabenordnung erst im Steuerbereinigungsgesetz 1986 novelliert worden sei.

Bei einer Reduzierung der übermittelten Gewerbesteuerdaten befürchtet er ferner eine Zunahme von Akteneinsichtnahmen der Gemeinden bei den Finanzämtern, was mit erheblichem Verwaltungsaufwand verbunden sei.

Diese Argumente müssen bei einer sachgerechten Lösung sicherlich berücksichtigt werden, können aber die unveränderte Beibehaltung der bisherigen Regelung nicht stützen. Der Gesetzgeber darf die mögliche Ausnahme, daß die Gemeinden ergänzende Informationen benötigen, nicht zur Regel machen. Wenn in den wenigen Streit- oder Zweifelsfällen der gesamte Gewerbesteuermeßbescheid den Gemeinden nachgereicht wird, dürfte sich der Verwaltungsaufwand hierfür in verantwortbaren Grenzen halten.

10. Personalwesen

10.1 Löschung von Zeiterfassungsdaten

Aufgrund einer Eingabe hatte ich zur Dauer der Aufbewahrung von Zeiterfassungsdaten Stellung zu nehmen. Das Staatsministerium der Finanzen hat dazu die Auffassung vertreten, daß das im Zusammenhang mit der Zeiterfassung anfallende Datenmaterial längstens zwei Jahre aufzubewahren ist. Der genannte Zeitraum orientiert sich an entsprechenden Fristen für Geschäftsprüfungen sowie an der Ver-

folgungsverjährung für geringere Dienstvergehen. Auch bei längerer Erkrankung oder Inanspruchnahme von Erziehungsurlaub ist die genannte Aufbewahrungsfrist von Bedeutung.

Der genannten Rechtsauffassung des Staatsministeriums der Finanzen bin ich gefolgt. Ich habe jedoch darauf hingewiesen, daß der einzelne Betroffene nach Art. 11 Nr. 2 BayDSG verlangen kann, daß zu seiner Person gespeicherte Daten gelöscht werden, wenn ihre Kenntnis für die speichernde Stelle zur rechtmäßigen Erfüllung der ihr durch Rechtsnorm zugewiesenen Aufgaben nicht mehr erforderlich ist. Auf Verlangen wäre daher im Einzelfall zu prüfen, ob die Zeiterfassungsdaten vor Ablauf der 2-Jahresfrist gelöscht werden können.

Meine Vorstellungen wurden vom Staatsministerium der Finanzen in einer Bekanntmachung zur Änderung der Rahmenbestimmungen für die gleitende Arbeitszeit berücksichtigt.

10.2 Trennung von Beihilfebearbeitung und Versorgungsfestsetzung

In einer Beschwerde wurde bemängelt, daß bei einer Bezirksfinanzdirektion Beihilfebearbeitung und Versorgungsfestsetzung von ein und derselben Stelle abgewickelt würden, da in beiden Fällen Bescheide mit derselben Unterschrift ergangen sind. Der Verdacht mangelnder Abschottung der Beihilfestelle war jedoch nicht begründet.

Die datenschutzrechtliche Überprüfung ergab, daß bei der Bezirksfinanzdirektion für Versorgung und Beihilfe selbständige Arbeitsgebiete mit Sachbearbeitern und Arbeitsgebietsleitern innerhalb eines Referates eingerichtet sind. Der gemeinsame Referent hat jedoch keine Möglichkeit, Kenntnisse aus den Beihilfedaten im Rahmen seiner weiteren Zuständigkeit für Versorgung zu verwenden, da bei Versorgungsempfängern keine Personalentscheidungen zu treffen sind, die durch Informationen aus Beihilfeunterlagen beeinflußt werden könnten. Dies gilt auch bei einer erneuten Berufung in das Beamtenverhältnis nach Wiederherstellung der Dienstfähigkeit. In diesem Fall entscheidet ausschließlich die Ernennungsbehörde über die Reaktivierung des Ruhestandsbeamten. Die Pensionsbehörde ist mit der Angelegenheit nicht befaßt. Sie wird erst im Falle der erneuten Berufung des Ruhestandsbeamten in das Beamtenverhältnis wegen der erforderlichen Einstellung der Versorgungsbezüge unterrichtet. Eine Beeinflussung der Personalentscheidung durch Beihilfedaten ist somit nicht möglich, da die Beihilfeunterlagen bei der Pensionsbehörde und nicht bei der Ernennungsbehörde geführt werden.

10.3 Offenbarung der Schwerbehinderteneigenschaft gegenüber dem Dienstherrn

Mit dem Staatsministerium für Arbeit und Sozialordnung habe ich die Frage erörtert, ob und wann ein Arbeitnehmer oder Beamter seinen Arbeitgeber oder Dienstherrn von der Anerkennung als Schwerbehinderter unterrichten muß. In Übereinstimmung mit dem Ministerium vertrete ich folgende Auffassung:

- Bei der **Einstellung** hat der **Dienstherr das Recht**, den Bewerber **zu fragen**, ob er Schwerbehinderter ist oder einen Antrag auf Anerkennung als Schwerbehinderter gestellt hat oder vom Arbeitsamt einem Schwerbehinderten gleichgestellt wurde. Der Bewerber ist zur wahrheitsgemäßen Beantwortung dieser Frage verpflichtet. Eine unrichtige Angabe gegenüber dem Dienstherrn bzw. Amtsarzt auf die Frage nach Beschwerden und schweren Krankheiten kann den Tatbestand der arglistigen Täuschung erfüllen und zur Rücknahme der Ernennung führen.
- Bei der **Einstellung** muß der Bewerber ohne entsprechende Frage des Arbeitgebers/Dienstherrn **von sich aus** nur dann auf eine Schwerbehinderteneigenschaft oder seine Gleichstellung mit einem Schwerbehinderten hinweisen, wenn er erkennen muß, daß er wegen der Behinderung, die der Schwerbehinderteneigenschaft oder der Gleichstellung zugrunde liegt, die vorgesehene Arbeit nicht zu leisten vermag oder die Minderung der Leistung und Fähigkeiten für den in Betracht kommenden Arbeitsplatz von ausschlaggebender Bedeutung ist.
- Wird jemand **während eines bestehenden Arbeits- oder Dienstverhältnisses** als schwerbehindert anerkannt, so braucht der Arbeitnehmer oder Beamte die Tatsache der Anerkennung dem Arbeitgeber oder Dienstherrn nicht zu offenbaren, soweit mögliche Vergünstigungen nicht in Anspruch genommen werden. So brauchen Arbeitnehmer/Beamte, die zwar die Steuerermäßigung beantragen, jedoch auf den Zusatzurlaub verzichten, den Arbeitgeber/Dienstherrn nicht zu unterrichten. Dies gilt entsprechend für Personen, die trotz Vorliegens der Voraussetzungen keinen Antrag auf Feststellung der Behinderung stellen. Hiervon unberührt bleibt eine etwaige Pflicht zum Hinweis auf gesundheitliche Beeinträchtigungen, die von ausschlaggebender Bedeutung für die Arbeit sind.

10.4 Personaldatenverarbeitung auf privaten PC

Ein Behördenleiter fragte an, ob er auf seinem privaten PC Personaldaten öffentlicher Bediensteter speichern dürfe. Beabsichtigt sei, zur Gedächtnisstütze Informationen aus Gesprächen mit den Mitarbeitern zu speichern, z. B. deren Versetzungswünsche.

In Übereinstimmung mit dem Staatsministerium der Finanzen habe ich die Auffassung vertreten, daß die Verarbeitung und Nutzung personenbezogener Daten von Bediensteten mit Hilfe privater PC grundsätzlichen datenschutzrechtlichen und dienstrechtlichen Bedenken begegnet. Dem Einsatz privater PC im Bereich der Personalverwaltung stehen die Grundsätze des Personalaktenrechts entgegen. Ungeachtet der jeweils gewählten Speicherungsform entstünde nämlich eine Nebenpersonalakte, ohne daß der Dienstherr hierüber die erforderliche Verfügungsgewalt erhielte. Die Einhaltung der Schutzbestimmungen des Personalvertretungs-, Beamten- und Datenschutzrechts sowie die Durchführung der vorgeschriebenen Genehmigungs- und Freigabeverfahren könnte daher durch die zuständigen Behörden nicht gewährleistet werden.

11. Gewerbe und Handwerk

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

Im 11. Tätigkeitsbericht habe ich bereits auf die noch ausstehende Anpassung des Gewerbe- und Wirtschaftsverwal-

tungsrechts an die Vorgaben des Bundesverfassungsgerichts hingewiesen. Gleichzeitig hatte ich über den damaligen Stand der Arbeiten zur Änderung der diesen Bereich betreffenden datenschutzrechtlichen Vorschriften berichtet. Bisher sind diese Arbeiten jedoch über die Vorlage eines weiteren vom Bund-Länder-Ausschuß „Gewerberecht" erarbeiteten Referentenentwurfs nicht hinausgekommen. Dieser Entwurf sieht, wie schon der vorausgegangene, in erster Linie die Ergänzung der Gewerbeordnung mit datenschutzrechtlichen Regelungen vor. Nach wie vor fehlen Vorschläge für andere bereichsspezifische Regelungen (z.B. im Gaststättengesetz und in den Zulassungsordnungen für freie Berufe). Die weitere Entwicklung ist deshalb abzuwarten.

11.2 Datenspeicherung der Handwerkskammern bei der Führung des Verzeichnisses der Berufsausbildungsverhältnisse

Nach §§ 73, 74 Berufsbildungsgesetz (BBiG) i.V.m. § 28 ff, 91 Abs. 1 Nr. 4 Handwerksordnung (HwO) haben die Handwerkskammern ein Verzeichnis der Berufsausbildungsverhältnisse (Lehrlingsrolle) zu führen. Darin ist der wesentliche Inhalt jedes in ihrem Zuständigkeitsbereich abgeschlossenen Berufsausbildungsvertrages einzutragen. Die Verträge sind bei der Handwerkskammer mit dem Antrag auf Eintragung vom Ausbilder vorzulegen. Alle Handwerkskammern führen dieses Verzeichnis inzwischen automatisiert. Es dient insbesondere auch der Überwachung der Berufsausbildung im Einzelfall (§ 41 a HwO). Demnach dürfen dort nur Daten gespeichert werden, soweit sie zur Erfüllung dieser Überwachungsaufgabe der Handwerkskammer erforderlich sind.

In diesem Zusammenhang habe ich Bedenken erhoben gegen die häufig festgestellte Speicherung der Tatsache der Behinderung eines Auszubildenden — und vor allem auch der Art der Behinderung (körperlich, geistig oder körperlich und geistig). Die Angabe der Behinderung durch den Auszubildenden führt bei der Handwerkskammer zunächst lediglich zur Überprüfung des Ausbildungsvertrages, ob die mitgeteilte Ausbildung in einem Beruf für Behinderte i.S. des § 42 b HwO erfolgt. Ein weiterer unmittelbarer Handlungsbedarf entsteht für die Handwerkskammer dadurch nicht.

Ob der Auszubildende allerdings tatsächlich die Behinderteneigenschaft und die sich aus ihr ergebenden rechtlichen Folgen (z.B. Ausbildungsberuf für Behinderte oder Gewährung von Sonderurlaub) wahrnehmen will, steht in seinem Belieben. Nur er kann beurteilen, ob er sich den üblichen Ausbildungsanforderungen gewachsen fühlt. Aus diesem Grund können seine entsprechenden Angaben nur freiwillig sein.

Ich habe deshalb die Handwerkskammern aufgefordert, bei der Datenerhebung auf die Freiwilligkeit der Angabe der Behinderung hinzuweisen. Nur unter dieser Voraussetzung ist die Speicherung der Tatsache der Behinderung in der Form ja/nein/unbekannt als zulässig anzusehen. Dagegen ist die Erhebung und Speicherung von weitergehenden Angaben über die Art der Behinderung nicht erforderlich. Aus ihrer Kenntnis lassen sich keine rechtlichen Folgen ableiten, weshalb ihre Speicherung für die Aufgabenerfüllung der Handwerkskammer nicht zulässig ist (Art. 16 Abs. 1 BayDSG).

Die Handwerkskammern haben sich meiner Auffassung bereits weitgehend angeschlossen und überwiegend ihre Erhebungsbögen in den Berufsausbildungsverträgen entsprechend abgeändert. Insbesondere wird nunmehr regelmäßig auch auf die Freiwilligkeit der Angabe der Behinderung hingewiesen.

11.3 Datenerhebung der Handwerkskammer für die Eintragung in die Handwerksrolle

Ein Handwerksmeister, der mehrere Betriebe führt, kann sich nach § 45 GewO dort jeweils durch einen technischen Betriebsleiter vertreten lassen. Will der Handwerksmeister für die einzelnen Betriebe seiner Eintragungspflicht in die Handwerksrolle nachkommen, muß auch der Betriebsleiter die für die Führung eines Handwerksbetriebs vorgeschriebenen Erfordernisse erfüllen. Zur Beurteilung dieser Eintragungsvoraussetzung hat der Handwerksmeister nach § 17 HwO der Handwerkskammer die erforderlichen Auskünfte zu erteilen.

In einer Eingabe beklagte sich ein Handwerksmeister darüber, daß die Handwerkskammer die Eintragung in die Handwerksrolle von der Beantwortung von Fragen zum Betriebsleiter abhängig mache, die weit über das übliche Maß hinausgingen. Hierzu ist festzustellen, daß die Handwerkskammer nur die für ihre Aufgabenerfüllung erforderlichen Auskünfte verlangen darf. Aus ihnen muß sich ergeben, daß der Betriebsleiter in der Lage ist, den Betrieb jederzeit führen zu können. Dies setzt seine fachliche und gesundheitliche Eignung sowie die Möglichkeit der ständigen Anwesenheit im Betrieb voraus. Letztere wird vor allem in Gesundheitsberufen — einen solchen betraf die Eingabe — als notwendig angesehen.

In Übereinstimmung mit dem Staatsministerium für Wirtschaft und Verkehr und mit dem Bayerischen Handwerkstag darf deshalb z.B. die Vorlage des mit dem Betriebsleiter abgeschlossenen Arbeitsvertrages oder auch dessen Lohnsteuerkarte gefordert werden. Aus diesen Unterlagen können sich Anhaltspunkte dafür ergeben, ob die mitgeteilte Betriebsleitung ernst gemeint ist. Dies gilt auch für die Krankenkassenanmeldung des angestellten Meisters, weil das durch sie nachgewiesene gesetzliche Sozialversicherungsverhältnis ebenfalls die wirkliche Bestellung des Versicherten zum technischen Betriebsleiter belegt.

Das zusätzliche Verlangen auf Erteilung einer schriftlichen Vollmacht, nach der die zuständigen Sozialversicherungsträger der Handwerkskammer jederzeit Auskunft geben müssen, geht dagegen über das erforderliche Maß hinaus. Eine so weitgehende Vollmacht ist zur Beurteilung der Betriebsleitereigenschaft nicht erforderlich. Von Interesse könnte hier die Bestätigung der vom Betroffenen mitgeteilten Entgelthöhe durch den Sozialversicherungsträger sein.

Nicht zu beanstanden sind Fragen nach früheren, evtl. selbständigen Tätigkeiten des Betriebsleiters, nach seinen Befugnissen bei der Angebotserstellung, nach Haupt- und Nebenwohnsitzen, Dienstwohnung sowie weiteren Niederlassungen des Unternehmens. Die Angaben hierzu können auf eine nicht zulässige doppelte oder gar nicht wahrgenommene Betriebsführung hinweisen. Die Folge wäre die Versagung der begehrten Eintragung in die Handwerksrolle. Zulässig ist auch die Frage nach einer gegen den Betriebsleiter bereits ausgesprochenen Gewerbeuntersagung (§ 35 GewO), weil diese durch die Bestellung zum technischen Betriebsleiter umgangen würde. Ferner darf nach Rentenbezug und nach der gesundheitlichen Eignung für die technische Betriebsleitung gefragt werden. Ohne diese Voraus-

setzungen müßte die Eintragung in die Handwerksrolle versagt werden.

11.4 Datenerhebung für Prüfungszulassung

Im 11. Tätigkeitsbericht habe ich erwähnt, daß eine Handwerkskammer zur Teilnahme an einer Prüfung zum „Computerschein A" zu viele Daten erhebt. Die betroffene Handwerkskammer ist meinen Hinweisen weitgehend gefolgt. Sie hat zwischenzeitlich den Umfang der verlangten Angaben wesentlich eingeschränkt und den Formularinhalt neu gefaßt.

Noch immer aber fordert die Handwerkskammer von den Prüfungsteilnehmern einen **Lebenslauf**. Sie verwies dazu als Begründung lediglich auf § 10 Abs. 2 a ihrer „Prüfungsordnung für die Durchführung von Fortbildungsprüfungen für nichthandwerkliche Berufe" vom 29.5.1974. Danach ist der Anmeldung zu einer Prüfung ein Lebenslauf (tabellarisch) beizufügen. Eine Erklärung, wofür dieser hier bei der Aufgabenerfüllung der Handwerkskammer erforderlich wäre, unterblieb jedoch bisher.

Da die Handwerkskammer „besondere Rechtsvorschriften für die Fortbildungsprüfungen für die Computerscheine A, B und C" erlassen hat, die in § 2 unter den Zulassungsvoraussetzungen den Lebenslauf nicht nennen, bestehen auch insoweit Bedenken gegen seine Anforderung.

Ich habe deshalb bei der Handwerkskammer und dem Staatsministerium für Wirtschaft und Verkehr angeregt, die pauschale Regelung des § 10 Abs. 2 a Fortbildungsprüfungsordnung zu überdenken und hier auf die Vorlage des Lebenslaufs zu verzichten.

11.5 Datennutzung durch die Handwerksinnung

Als Aufgabe einer Handwerksinnung wird auch die Führung gerichtlicher Prozesse angesehen, die auf die Unterlassung wettbewerbsverletzender Handlungen nach dem Gesetz gegen unlauteren Wettbewerb (UWG) gerichtet sind. Zur Einleitung eines solchen gerichtlichen Verfahrens hatte eine Innung in ihrer Klageschrift u.a. auf Daten des Prozeßgegners zurückgegriffen, die dieser kurz zuvor in einem Antrag auf Erteilung einer Ausnahmebewilligung nach § 8 des Gesetzes zur Ordnung des Handwerks (HwO) angegeben hatte. Diese Daten hatte sie zur Anhörung als zuständige Berufsvereinigung von der Handwerkskammer erhalten. Eine Anhörung ist im Rahmen der Entscheidung über einen Ausnahmebewilligungsantrag in § 8 Abs. 3 HwO vorgesehen und hat den Zweck, der Innung eine Stellungnahme zu den für die Ausnahmebewilligung notwendigen Kenntnissen und Fertigkeiten des Antragstellers zu ermöglichen. Die der Innung übermittelten Daten unterliegen insoweit einer datenschutzrechtlichen Zweckbindung.

Die Verwendung dieser zweckgebundenen Daten in einem gerichtlichen Verfahren, das mit dem Antrag auf Ausnahmebewilligung in keinem Zusammenhang steht, halte ich für unzulässig.

Die Verwendung solcher Daten für die Einleitung des gerichtlichen Verfahrens wegen unlauteren Wettbewerbs stellt eine wesentliche Nutzungsänderung dar und ist als ein unverhältnismäßiger Eingriff in das informationelle Selbstbestimmungsrecht des Betroffenen aufzufassen. Dieser beabsichtigt nämlich gerade mit Hilfe seines Antrags die Beseitigung eines bisher möglicherweise gesetzwidrigen Zustandes, wofür in § 8 Abs. 1 HwO die Erteilung einer Ausnahmebewilligung ausdrücklich vorgesehen ist. Solange über den Ausnahmebewilligungsantrag nicht entschieden ist, muß die gleichzeitige Verwendung der Antragsdaten in einem gerichtlichen Verfahren als unverhältnismäßig angesehen werden. Das gilt vor allem auch gegenüber der Forderung auf Unterlassung von Handlungen, deren erlaubte Ausübung durch den Antrag angestrebt wird. Es kann nicht Sinn der Anhörung der Innung sein, daß der Antragsteller postwendend auf Grund seiner Angaben im Antrag auf Ausnahmegenehmigung von der Innung mit einem Gerichtsverfahren überzogen wird.

Die zuständige Handwerkskammer und das Staatsministerium für Wirtschaft und Verkehr haben hier ebenfalls datenschutzrechtliche Bedenken gegen die Verwendung der Daten durch die Innung geäußert. Ich habe die betroffene Innung auf die Unzulässigkeit einer solchen Datennutzung hingewiesen und die zweckfremde Verwendung der Antragsdaten gerügt.

12. Landwirtschaft

12.1 Prüfung der Landwirtschaftsverwaltung

Die im Jahr 1989 begonnene Prüfung in der Landwirtschaftsverwaltung habe ich bei zwei weiteren Ämtern für Landwirtschaft fortgesetzt.

Folgende Feststellungen waren u.a. zu treffen:

Freigabeerklärungen und Meldungen zum Datenschutzregister

In verschiedenen Fällen (z. B. Förderungsprogramm „Soziostruktureller Einkommensausgleich") waren automatisierte BALIS-Verfahren im Einsatz, die von der obersten Dienstbehörde noch nicht freigegeben waren. Auch fehlte häufig die Meldung zum Datenschutzregister.

Dies habe ich beanstandet. Das Staatsministerium für Ernährung, Landwirtschaft und Forsten hat die Freigabeerklärungen inzwischen nachgeholt. Die erforderlichen Meldungen zum Datenschutzregister erfolgten ebenfalls.

Verwendung von Daten für mehrere Förderungsprogramme

Wenn Anträge für verschiedene Förderungsmaßnahmen gestellt werden, stellt sich für die Landwirtschaftsverwaltung die Frage, ob Daten, die in einem bestimmten Förderungsantrag angegeben werden, auch für die Beurteilung eines anderen Antrags genutzt werden dürfen. Ob dies zulässig ist, ist jedoch umstritten.

Im Hinblick auf die Freiwilligkeit der Datenangabe bei Förderungsanträgen ist hier zunächst von einem besonderen Vertrauensschutz der Antragsteller auszugehen. Auch ist die möglicherweise vorhandene unterschiedliche Zielrichtung der einzelnen landwirtschaftlichen Förderungsmaßnahmen zu berücksichtigen. Deshalb könnte beispielsweise fraglich sein, ob die in der Gasölverbilligungsdatei gespeicherten Daten zur Bearbeitung eines Antrags auf Gewährung einer Startbeihilfe für Junglandwirte herangezogen werden dürfen, wenn der Betroffene in die Verwendung seiner Angaben zur Gasölverbilligung für den Antrag auf Startbeihilfe nicht

eingewilligt hat, diese Datennutzung auch nicht durch eine Rechtsnorm erlaubt wird.

Die stichprobenartigen Überprüfungen der Unterlagen haben ergeben, daß die Ämter für Landwirtschaft regelmäßig die **Einwilligung der Betroffenen zur anderweitigen Nutzung** ihrer Daten einholen, und zwar bereits im Antragsformular. Dies geschieht inzwischen in der Weise, daß der Antragsteller z.B. im Förderungsantrag auf Startbeihilfe zur Hofübernahme erklärt, die näheren Angaben über Betriebsgröße, Flächen, Viehbestand und Bankverbindung sollten dem letzten „4fach-Antrag" entnommen werden. In diesem Förderungsantrag kann der Antragsteller außerdem auf seine Angaben in einem evtl. gleichzeitig gestellten Antrag auf Förderung von Investitionen verweisen. Damit **willigt er in die anderweitige Verwendung** der betreffenden Daten, etwa aus der Gasölverbilligungsdatei, ein. Insoweit bestehen daher keine datenschutzrechtlichen Bedenken gegen die Datennutzung.

Lesezugriff auf Daten eines anderen Amtes

Ein Landwirtschaftsamt hatte bis zur Ausstattung eines Tierzuchtamts mit BALIS-Datenendgeräten in dessen Auftrag die Dateneingabe für die dort bearbeiteten Förderungsprogramme vorgenommen. Obwohl bereits ab etwa 1988 diese Auftragsdatenverarbeitung nicht mehr erforderlich war — das betreffende Tierzuchtamt hatte inzwischen den Anschluß zum System BALIS erhalten — und auch nicht mehr vorgenommen wurde, bestand weiterhin ein Lesezugriff des Landwirtschaftsamtes auf die seinerzeit im Auftrag gespeicherten Daten.

Ein solcher Lesezugriff auf Daten einer anderen speichernden Stelle ist mangels einer entsprechenden Rechtsgrundlage unzulässig. Das Staatsministerium für Ernährung, Landwirtschaft und Forsten hat die Zugriffsmöglichkeit des geprüften Landwirtschaftsamtes auf die Daten des betreffenden Tierzuchtamts gelöscht.

13. Statistik

13.1 Bayerisches Statistikgesetz

Am 10.8.1990 hat der Bayerische Landtag das neue Bayerische Statistikgesetz (BayStatG) beschlossen, das am 1.9.1990 in Kraft getreten ist. Das Statistikrecht in Bayern entspricht nunmehr den Anforderungen, die das Bundesverfassungsgericht im Volkszählungsurteil für Erhebungen zu statistischen Zwecken aufgestellt hat. Es enthält jetzt die zum Schutz des Persönlichkeitsrechts erforderlichen Verfahrensbestimmungen in gesetzlicher Form.

Datenschutzrechtlich von besonderer Bedeutung sind folgende Regelungen:

- Trennung und Löschung von Hilfsmerkmalen (Art. 15):
  Hilfsmerkmale sind von den Erhebungsmerkmalen zum frühestmöglichen Zeitpunkt zu trennen und gesondert aufzubewahren. Sie sind zu löschen, sobald die Überprüfung der Erhebungs- und Hilfsmerkmale auf Schlüssigkeit und Vollständigkeit abgeschlossen ist. Erhebungsmerkmale sind zur Erstellung einer Statistik bestimmte Angaben über persönliche oder sachliche Verhältnisse. Hilfsmerkmale sind Angaben, die der technischen Durchführung von Statistiken dienen (z.B. Name und Adresse des Betroffenen).

- Geheimhaltung (Art. 17):
  Einzelangaben sind u.a. von den mit der Statistik betrauten Stellen und Personen geheimzuhalten. Ausgenommen davon sind Einzelangaben, in deren Übermittlung oder Veröffentlichung die Auskunftgebenden schriftlich eingewilligt haben, und Einzelangaben aus allgemein zugänglichen Quellen. Die Verletzung des Statistikgeheimnisses ist unter Strafe gestellt.

- Zweckbindungsgrundsatz (Art. 18):
  Einzelangaben dürfen ausschließlich für statistische Zwecke verarbeitet oder genutzt werden, es sei denn, sie beruhen auf allgemein zugänglichen Quellen oder eine Rechtsvorschrift läßt eine andere Verwendung zu.

- Hinweispflicht (Art. 19):
  Die zu Befragenden sind grundsätzlich schriftlich auf Zweck, Art und Umfang der Erhebung, die Geheimhaltung, die Auskunftspflicht oder die Freiwilligkeit der Auskunft, die Rechte und Pflichten der Erhebungsbeauftragten u.a. hinzuweisen.

- Abschottung der Statistikstellen (Art. 24):
  Statistikstellen sind räumlich und organisatorisch von anderen Verwaltungsstellen zu trennen. Die in Statistikstellen tätigen Personen dürfen statistische Einzelangaben und bei ihrer Tätigkeit gewonnene Erkenntnisse grundsätzlich auch nach Beendigung ihrer Tätigkeit nicht in anderen Verfahren oder für andere Zwecke verarbeiten. Soweit und solange sie Einzelangaben bearbeiten, dürfen sie nicht andere Aufgaben des Verwaltungsvollzugs wahrnehmen. Im Anschluß an eine Tätigkeit in der Statistikstelle sollen sie nicht für Aufgaben eingesetzt werden, bei denen eine Nutzung der in den Statistikstellen gewonnenen Erkenntnisse möglich ist, soweit das die organisatorischen und personellen Verhältnisse zulassen.

- Reidentifizierungsverbot (Art. 26):
  Die Zusammenführung von Einzelangaben aus Statistiken öffentlicher Stellen oder von Einzelangaben aus Statistiken öffentlicher Stellen mit anderen Angaben zum Zwekke der Herstellung eines Personen-, Unternehmens-, Betriebs- oder Arbeitsstättenbezugs ist untersagt, es sei denn, die Aufgabenstellung des Statistikgesetzes oder einer anderen Rechtsvorschrift oder ein sonstiger eine Statistik einer öffentlichen Stelle anordnender Rechtsakt lassen das zu.

13.2 Volkszählung 1987

In meinem letzten Tätigkeitsbericht habe ich auf die datenschutzrechtlichen Probleme bei der Erstellung einer Gemeindestatistik nach Blockseiten ("Blockseitenstatistik") hingewiesen. Blockseite ist „innerhalb eines Gemeindegebiets die Seite mit gleicher Straßenbezeichnung von der durch Straßeneinmündungen oder vergleichbare Begrenzungen umschlossenen Fläche". Die Blockseite ist die unterste Ebene der kleinräumigen Gliederung, die für eine statistische Verwendung vorgesehen werden darf. Eine Reihe von Gemeinden hat beim Landesamt für Statistik und Datenverarbeitung aus dem Ergebnis der Volkszählung 1987 die Erstellung einer Gemeindestatistik nach Blockseiten beantragt.

Ich habe im letzten Tätigkeitsbericht dargelegt, daß für die Blockseitenstatistik, die für **Gemeinden ohne abgeschottete Statistikstellen** bestimmt sind, noch keine Regelungen hinsichtlich der statistischen Geheimhaltung gefunden worden sind, die eine Identifizierung der Blockseitenbewohner ausschließen. Die Gefahr der Reidentifizierung besteht insbesondere dann, wenn die Blockseitenstatistiken in den allgemeinen Verwaltungsvollzug gelangen.

Mittlerweile ist bundesweit ein solches Blockseitenprogramm entwickelt worden. Es wird seit Sommer 1990 auch in Bayern eingesetzt. Seine Methodik schließt die Identifizierung aus, so daß das Statistikgeheimnis gewahrt bleibt.

14. Schulwesen

14.1 Ausdruck von Datenblättern aus der Lehrerdatei

Beim Staatsministerium für Unterricht und Kultus besteht seit 20 Jahren eine Lehrerdatei, in der Daten über alle hauptamtlichen und hauptberuflichen staatlichen Lehrkräfte in Bayern gespeichert sind. Im Berichtszeitraum hat mir das Ministerium mitgeteilt, es werde den an staatlichen Volks- und Sonderschulen unterrichtenden Lehrern ihr Datenblatt, in dem alle in der Lehrerdatei zu einer Person gespeicherten Daten enthalten sind, zusenden.

Das Datenblatt wurde in verschlossenen Kuverts an die Schulämter versandt, die es anschließend an die Schulen weiterleiteten. Zusammen mit dem Datenblatt ging allen Lehrkräften außerdem ein Schreiben zu, in dem sie u.a. gebeten wurden, tatsächliche oder vermeintliche Fehleinträge auf dem Dienstweg der personalaktenführenden Stelle mitzuteilen. Damit sollte die Richtigkeit und Aktualität der gespeicherten Daten verbessert und dem Bedürfnis der Lehrkräfte nach Informationen über die gespeicherten Daten Genüge getan werden.

Die durch diese Aktion erzeugte Nachvollziehbarkeit der Speicherungen begrüße ich ausdrücklich. Daneben scheint die automatisierte Personalverwaltung auch sehr sorgfältig mit Daten umzugehen. Nach Angaben des Staatsministeriums für Unterricht und Kultus wurden bereits im letzten Jahr auf Anforderung über 1000 Datenblätter versandt. Zu ihnen gingen insgesamt nur 15 Rückfragen ein.

14.2 Zugriff von Lehrern auf Schülernoten

Von seiten mehrerer Schüler wurde folgendes Problem an mich herangetragen:

Die „Schülerdatei" enthält neben persönlichen Daten der Schüler und ihrer Erziehungsberechtigten auch Fach- und Leistungsdaten, insbesondere Noten. Nach ihrer Kenntnis könne jeder Lehrer die Einzelnoten von allen Schülern einer Schule aus dem schuleigenen Personal Computer erfahren.

Nach Rücksprache mit dem Staatsministerium für Unterricht und Kultus stellt sich die Situation wie folgt dar:

An jeder Schule existiert für jede Klasse ein Notenbogen. In diesen trägt jeder Fachlehrer die Noten seiner Schüler in dem Fach, das er unterrichtet, ein. Alle Lehrer, die in der Klasse unterrichten, sind berechtigt, in diesen Notenbogen Einsicht zu nehmen.

Die Daten des Notenbogens werden von der damit beauftragten Person in den PC eingegeben. Die Lehrer haben das Recht zur Einsicht in die gespeicherten Daten im gleichen Umfang, wie sie in den Notenbogen Einblick nehmen dürfen. Um Einsicht zu nehmen, müssen sie sich allerdings an die Person wenden, die in der Schule das Paßwort verwaltet, das den Zugang zu den gespeicherten Daten sichert. Selbst unmittelbar Daten am Bildschirm aufrufen können die Lehrer nicht. Das Paßwort kennen in der Regel nur die Schulsekretärin und der Systemverwalter.

Eine solche Regelung ist datenschutzrechtlich nicht zu beanstanden.

14.3 Datenübermittlungen im Schulbereich

Folgende Fragen wurden an mich herangetragen:

1. Verteilung einer Lehrerliste an das Lehrerkollegium

   Ein Lehrer berichtete, zum Schuljahresbeginn habe der Schulleiter eine Liste der an der Schule unterrichtenden Lehrkräfte **an das Kollegium** verteilt. Die Liste enthielt neben Name, Anschrift und Telefonnummer auch das Geburtsdatum.

   In Abstimmung mit dem Staatsministerium für Unterricht und Kultus habe ich hierzu folgende Auffassung vertreten:

   Gegen die Verteilung einer Liste, die nur die Namen der einzelnen Lehrkräfte und/oder Daten zu ihrer dienstlichen Tätigkeit (Aufgaben, Funktionen, unterrichtete Fächer usw.) enthält, bestehen keine datenschutzrechtlichen Bedenken. Enthält die Liste jedoch weitere persönliche Angaben wie Anschrift, Telefonnummer und Geburtsdatum, dann darf sie nur mit Einwilligung der betroffenen Lehrer weitergegeben werden. Diese Angaben können zwar die Abstimmung und Zusammenarbeit zwischen den Lehrkräften erleichtern, sie sind jedoch für die dienstliche Zusammenarbeit nicht unbedingt erforderlich.

2. Weitergabe von Namen und Adressen der Elternvertreter an Elternverbände

   Ein Schulleiter wandte sich mit folgender Frage an mich: Ein Elternverband habe um Übermittlung von Namen und Adressen derjenigen Eltern gebeten, die als Elternvertreter dem Berufsschulbeirat angehören. Als Grund hierfür nannte der Verband, er müsse sich um die Situation der Schüler in der Berufsausbildung kümmern. Hierzu sei ein direkter Erfahrungsaustausch geplant.

   Ich habe dem Schulleiter geantwortet:

   Die Erhebung und Verarbeitung von Daten an Schulen ist in Art. 62 des Bayer. Gesetzes über das Erziehungs- und Unterrichtswesen (BayEUG) geregelt. Die Weitergabe von Elternadresssen an Elternverbände gehört nicht zu den den Schulen durch Rechtsvorschriften zugewiesenen Aufgaben (Art. 62 Abs. 1 BayEUG). Nach Art. 62 Abs. 2 BayEUG ist die Weitergabe an außerschulische Stellen untersagt, falls nicht ein rechtlicher Anspruch auf die Herausgabe der Daten nachgewiesen wird. Einen „rechtlichen" Anspruch auf die Herausgabe der Elternadressen kann der Elternverband nicht geltend machen. Deshalb habe ich dem Schulleiter empfohlen, die betreffenden Elternvertreter anzuschreiben und um ihr ausdrückliches Einverständnis zur Datenweitergabe an den

Elternverband zu bitten. Die Schule kann dann die Adressen derjenigen Elternvertreter, die ihr Einverständnis erklärt haben, an den Verband weiterleiten.

3. Namen und Klasse von Schülern an Schulbusunternehmen

   Die Datenschutzregistermeldung einer Schule sah die jährliche Übermittlung folgender Daten aus der Schülerdatei an das zur Schülerbeförderung beauftragte Omnibusunternehmen in Listenform vor: Name, Vornamen, Klasse, Buslinie und Zusteigehaltestelle aller Fahrschüler, die im Laufe des Schuljahres von dem Omnibusunternehmen von und zur Schule befördert werden.

   Das Unternehmen sollte aufgrund dieser Liste eine Übersicht erhalten, mit wie vielen Fahrschülern an den jeweiligen Haltestellen pro Schuljahr zu rechnen ist.

   Ich halte diese Datenübermittlung, die in den vom Staatsministerium für Unterricht und Kultus freigegebenen Schulverwaltungsprogrammen nicht vorgesehen ist, für unzulässig. Nach meiner Auffassung reicht für die Planung des Omnibusbetriebes die Übermittlung des Buchstabens der benutzten Buslinie, der Einsteigehaltestelle sowie der jeweiligen **Zahl** der Schüler aus. Die Übermittlung von Familienname, Vorname und Klasse ist dafür nicht erforderlich.

   Der Schulleiter hat mir daraufhin mitgeteilt, daß er aufgrund meines Schreibens von der bisher noch nicht praktizierten Datenübermittlung, die als „Serviceleistung" gegenüber der Firma gedacht und „vorsorglich" zum DSR-Register gemeldet worden war, Abstand nehmen werde.

14.4 Programm für ein Soziogramm über Schüler

Ein Lehrer bat mich um Beurteilung eines Programms, mit dem Aussagen zur „Interaktionshäufigkeit" von Schülern gemacht werden können. Das Programm sollte festhalten, wie häufig ein Schüler mit einer anderen Person spreche und wie häufig er sich über andere Schüler ärgere. Damit sind detaillierte Angaben zum Verhalten und Werdegang eines Schülers möglich (sog. Soziogramm).

Der Datensatz besteht aus Name und Vorname des jeweiligen Schülers. Die Aussagen (Sprechen, Ärgern) werden in einer Datei in numerischer Form festgehalten. Beispiel: „243142" aus einer Skala von 1 — 5, wobei „1" gleichbedeutend ist mit „keinerlei Äußerungen" und „5" mit „ständigem Sprechen, Ärgern". Die Ziffern „2" bis „4" stehen für dazwischenliegende Aktionshäufigkeiten. Da das Programm kompiliert ist, können die Namen zwar nicht unmittelbar den einzelnen Ziffern zugeordnet werden. Aus den Rohdaten werden aber verschiedene statistische Werte berechnet und in einem eigenen Feld abgespeichert. Die sich daraus ergebenden Aussagen zur „Interaktionshäufigkeit" werden dann dem einzelnen Schülernamen zugeordnet und ausgedruckt.

Das Staatsministerium für Unterricht und Kultus sah die Tatsache, daß im Datensatz des Programms sowohl der Name des Schülers als auch sein soziometrisches Profil erscheint, als datenschutzrechtlich bedenklich an. Soweit nicht ganz auf Soziogramme verzichtet werden könne, schlug es vor, anstatt der Merkmale „Name, Vorname des Schülers" eine laufende Nummer zu verwenden. Die sensiblen Aussagen zum Verhalten der Schüler können vom Lehrer anhand der vergebenen Nummern dem jeweiligen Schüler manuell zugeordnet werden. Dies hat gegenüber der Verwendung von Namen und Vornamen den Vorteil, daß die Daten der betroffenen Schüler anonymisiert sind und diese jedenfalls nicht ohne zusätzliche Bemühungen reanonymisiert werden können.

Der Haltung des Staatsministerium für Unterricht und Kultus schließe ich mich an. Da ein Soziogramm wohl auch „negative" Auffälligkeiten berücksichtigt und nennt, habe ich den Lehrer um nochmalige Überprüfung gebeten, ob auf die Verwendung solcher Programme nicht ganz verzichtet werden kann.

15. Hochschule

15.1 Novellierung des Hochschulstatistikgesetzes

Im Berichtszeitraum hat der Bundesgesetzgeber das Gesetz über die Statistik für das Hochschulwesen (Hochschulstatistikgesetz — HStatG) verabschiedet. Es tritt zum 1. Juni 1992 in Kraft. Während bisher die primär für statistische Zwecke vom Studenten erhobenen Daten in vollem Umfang auch der Verwaltung zur Verfügung standen, wird die Statistik künftig von dem Datensatz ausgehen, den die Hochschulverwaltung für ihre administrativen Zwecke erhebt. Auf der Basis dieser Verwaltungsunterlagen wird die Studentenstatistik als Sekundärstatistik durchgeführt werden. Ab 1. Juni 1992 wird der Weitergabe von Studentendaten, die von den Hochschulen erhoben wurden, nicht mehr die Geheimhaltungspflicht nach § 15 HStatG entgegenstehen. Entfallen ist die Studienverlaufsstatistik.

Wichtigste Forderung des Bundesrates war die Wiedereinführung der „Abiturientenbefragung", die ein wichtiges Hilfsmittel für Planungen im Hochschulbereich, insbesondere für die Aktualität von Vorausschätzungen der Studienanfänger, ist. Dieser Forderung hat der Bundestag zugestimmt. Die Teilnahme an der Abiturientenbefragung ist freiwillig. Folgende Datenschutzmaßnahmen wurden bei der Abiturientenbefragung vorgesehen:

- Ausgefüllte Erhebungsbögen werden in verschlossenen Umschlägen abgegeben.
- Die Bediensteten der Schulen sind zur Öffnung dieser Umschläge nicht befugt, sondern haben sie verschlossen an die statistischen Ämter weiterzuleiten.

Insgesamt gesehen kann man das beschlossene Gesetz als datenschutzgerecht bezeichnen. Von seiten der statistischen Ämter wurde allerdings am Gesetz Kritik geübt, weil es die Aussagefähigkeit der Hochschulstatistik verschlechtere und die Möglichkeiten der Hochschulstatistik beschneide, insbesondere durch den Verzicht auf die Studienverlaufsstatistik.

15.2 Einzelfälle

15.2.1 Herausgabe von Studentendaten an öffentliche und private Stellen

Häufig wenden sich öffentliche oder private Stellen an die Hochschulverwaltung mit der Bitte um Auskunft über die an der Hochschule immatrikulierten Studenten:

- Eltern fragen an, ob ihre Kinder an der Hochschule immatrikuliert sind, weil sie die Immatrikulationsbescheinigun-

gen für den Bezug von Kindergeld benötigen und diese von ihren Kindern nicht erhalten.

- Öffentliche Arbeitgeber oder Dienstherren der Eltern fragen im Zusammenhang mit der Berechnung der Vergütung und Besoldung sowie der Gewährung von Kindergeld an.
- Auch private Gläubiger wenden sich an die Universitäten mit der Bitte um Auskunft über den aktuellen Wohnort ihrer Schuldner.

Eine Hochschule bat mich um Stellungnahme zur Zulässigkeit solcher Auskünfte.

Die Rechtslage stellt sich nach Auffassung des Staatsministeriums für Wissenschaft und Kunst, die ich teile, wie folgt dar:

Nach der derzeitigen Rechtlage ist eine Herausgabe der Studentendaten an private und öffentliche Stellen unzulässig. Die Daten der Studenten werden primär zu Statistikzwecken erhoben und dienen gleichzeitig internen Verwaltungszwecken. Sie sind nach § 16 Bundesstatistikgesetz i.V.m. § 15 Hochschulstatistikgesetz geheimzuhalten. Nach § 15 Abs. 3 Satz 2 Hochschulstatistikgesetz dürfen im Fall des Hochschulwechsels Einzelangaben mit Namen und Anschrift der Studenten an die neue Hochschule für deren verwaltungsinterne Zwecke weitergeleitet werden. Andere Datenübermittlungen sieht das Gesetz nicht vor. Auch eine Berufung auf die Verpflichtung zur Amtshilfe gegenüber anderen öffentlichen Stellen ist insoweit ausgeschlossen.

Das Staatsministerium für Wissenschaft und Kunst hat zwar bestätigt, daß zumindest ein Teil der Hochschulen bereits zum jetzigen Zeitpunkt schon getrennte Erhebungen für die Hochschulstatistik einerseits und für verwaltungsinterne Zwecke der Hochschule andererseits durchführt. Dennoch dürfen die erhobenen Studentendaten insgesamt nur unter den strengen Voraussetzungen des derzeit noch geltenden Hochschulstatistikgesetzes weitergegeben werden.

Eine Änderung dieser Praxis ist allerdings in Aussicht, wenn das mittlerweile novellierte Hochschulstatistikgesetz in Kraft tritt und gleichzeitig im bayerischen Landesrecht eine ausdrückliche Rechtsgrundlage für die Erhebung der Daten für verwaltungsinterne Zwecke der Hochschulen geschaffen wird. Bei der letzten Novellierung des Bayer. Hochschulgesetzes 1988 hatte das Staatsministerium für Wissenschaft und Kunst die Aufnahme einer solchen Rechtsgrundlage abgelehnt, da zunächst die neuzuschaffenden Regelungen in den Querschnittsgesetzen abgewartet werden sollten.

Meine Forderungen zur Novellierung des Bayer. Hochschulgesetzes, die ich bereits in früheren Tätigkeitsberichten dargelegt habe, sind daher weiterhin aktuell. Ich werde sie zu gegebener Zeit in die Diskussion einbringen.

15.2.2 Aushang von Klausurnoten

Ein Student beschwerte sich über die Praxis des Diplomvorprüfungsamtes einer Universität, Klausurnoten zusammen mit Vornamen, Namen und Datum des Studienbeginns am öffentlich zugänglichen „Schwarzen Brett" auszuhängen. Er hielt diese Praxis im Zeitalter des Datenschutzes für nicht angemessen. Zu Recht.

Ich habe mich bereits in meinem 7. Tätigkeitsbericht ausführlich mit der Problematik auseinandergesetzt und dabei im Ergebnis festgestellt, daß ein Notenaushang dann schutzwürdige Belange beeinträchtigt, wenn die Daten einer bestimmten Person zugeordnet werden können und ein größerer Personenkreis von dem Aushang Kenntnis nehmen kann. Beide Voraussetzungen waren in dem mir geschilderten Fall eindeutig gegeben.

Meine Auffassung habe ich der Universität mitgeteilt. Sie will künftig die Klausurteilnehmer mit ihrer Matrikelnummer oder einer speziellen Prüfkennzahl bezeichnen. Alternativ will sie die schriftliche Einwilligung der Klausurteilnehmer zu einer namentlichen Auflistung einholen. Gegen diese Lösungsmöglichkeiten bestehen keine datenschutzrechtlichen Bedenken.

15.2.3 Einkommen der Eltern in BAföG-Bewilligungsbescheid

Ein Vater wandte sich hilfesuchend mit folgendem Problem an mich: Seine Tochter, die bei seiner geschiedenen Frau wohne, erhalte Leistungen nach dem Bundesausbildungsförderungsgesetz (BAföG). Da der Bescheid über die Gewährung von BAföG Angaben zur Höhe seines Einkommens enthalte, werde dieses automatisch auch seiner geschiedenen Frau sowie dem Freund seiner Tochter bekannt, was keinesfalls in seinem Interesse liege.

Meine Antwort wird den Vater kaum befriedigt haben:

Die Entscheidung über die Gewährung von BAföG-Leistungen ist dem Antragsteller (Tochter) nach § 50 Abs. 1 BAföG in einem Bescheid schriftlich mitzuteilen. Im Bescheid ist dabei notwendigerweise auch die Höhe seines Einkommens sowie des Einkommens seiner Eltern und seines Ehegatten anzugeben, soweit nicht die Ausnahme des § 50 Abs. 2 Satz 3 BAföG zur Anwendung kommt: Danach können auf Verlangen eines Elternteils oder des Ehegatten die Angaben über deren Einkommen auf den Betrag des angerechneten Einkommens beschränkt werden, es sei denn, der Auszubildende hat im Zusammenhang mit der Geltendmachung seines Anspruches „ein besonderes berechtigtes Interesse" an der Kenntnis der Einkommenshöhe. Mit diesem Ergebnis hat der Gesetzgeber den Interessenkonflikt zwischen einem Antragsteller auf BAföG-Leistungen und seinen Eltern entschieden — eine zwar komplizierte, aber angemessene Lösung.

Aus der Sicht des Datenschutzes besonders erfreulich ist, daß in den amtlichen Antragsformularen ausdrücklich auf die Möglichkeit des § 50 Abs. 2 Satz 3 BAföG hingewiesen wird. Dies begrüße ich ausdrücklich.

16. Archiv und Forschung

16.1 Einsichtnahme in NS-Akten

Im 11. Tätigkeitsbericht hatte ich darauf hingewiesen, daß das vom Landtag beschlossene Archivgesetz an die Archivbehörden bei der Prüfung der Anträge auf Einsichtnahme weit höhere Anforderungen stellt als der Regierungsentwurf, wenn die Persönlichkeitsrechte der Betroffenen geschützt werden sollen. Meine Besorgnis hat sich bereits im Berichtsjahr bestätigt, wie nachfolgender Fall zeigt:

Der Presse habe ich entnommen, daß eine Faschismusforscherin einem über 60 Jahre alten Bürgermeister vorgehalten hat, er habe 1943 als Hitlerjunge im Alter von 14 Jahren eine Hausfrau denunziert, die daraufhin von einem Sonder-

gericht verurteilt worden sei. Diese Informationen habe sie aus den Akten des Bayerische Staatsarchivs entnommen.

Die Akten über den zugrundeliegenden Vorgang werden tatsächlich im Staatsarchiv verwahrt. Der dem Bürgermeister vorgehaltene Sachverhalt stimmte auch weitgehend mit dem Akteninhalt überein. Meine Ermittlungen haben ergeben, daß die genannte Forscherin in den Jahren 1983/1984 mehrmals im Rahmen einer wissenschaftlichen Arbeit über den Nationalsozialismus Einsicht in die Materialien des Archivs genommen hat. Rechtsgrundlage war damals noch die Benützungsordnung für die staatlichen Archive Bayerns vom 31.5.1955. Die Forscherin war auf die Verpflichtung zur Wahrung der Persönlichkeitsrechte hingewiesen worden und hatte sich **in einer Erklärung verpflichtet, die schutzwürdigen Belange Dritter zu beachten**. Eine Überprüfung durch das Staatsarchiv hat jedoch ergeben, daß sie gerade die betreffenden Sondergerichtsakten nicht eingesehen hatte, sondern ihre Detailkenntnisse aus anderen Quellen bezogen haben mußte. Es stellte sich heraus, daß ein weiterer Forscher kurz vor der Veröffentlichung in der Presse die Sonderakten des Archivs eingesehen hatte, wobei sein Wunsch, ihm eine Ablichtung des Urteils auszuhändigen, aus Gründen des Persönlichkeitsschutzes abgelehnt worden war.

Diese Archivbenützung erfolgte auf der Grundlage des inzwischen in Kraft getretenen Bayer. Archivgesetzes, das die Archivbenützung regelt. Dennoch erscheinen die Voraussetzungen für eine Archivbenützung und die Anforderungen an die Wahrung der Persönlichkeitsrechte noch nicht vollständig geklärt. Nach Art. 10 des Bayer. Archivgesetzes kann das in staatlichen Archiven verwahrte Archivgut benützt werden, **soweit ein berechtigtes Interesse an der Benützung glaubhaft gemacht wird und nicht Schutzfristen entgegen stehen**. Die Zulassung zur Benützung ist u.a. dann zu versagen oder von Auflagen abhängig zu machen, wenn und soweit Grund zu der Annahme besteht, daß schutzwürdige Belange Betroffener oder Dritter entgegenstehen. Die **Schutzfrist bei personenbezogenem Archivgut beträgt grundsätzlich zehn Jahre nach dem Tod des Betroffenen**.

Wie mir das Staatsarchiv mitgeteilt hat, wurde dem Forscher die Einsicht in die Unterlagen gewährt, da die denunzierte Frau seit mehr als zehn Jahren verstorben war und der Forscher ein berechtigtes wissenschaftliches Interesse glaubhaft machte. Nach meiner Ansicht wurde hierbei nicht beachtet, daß es sich **bei dem noch lebenden Bürgermeister ebenfalls um einen Betroffenen handelte**, da umfangreiche personenbezogene Daten auch über ihn den Akten entnommen werden konnten. Die **Schutzfrist hätte somit auch zum Schutz des Bürgermeisters beachtet werden müssen**. Zumindest hätten seine schutzwürdigen Belange bei der Zulassung zur Benützung stärker beachtet werden müssen.

Wie mir die Generaldirektion der staatlichen Archive Bayerns mitteilt, ist eine Erweiterung der zitierten Verpflichtungserklärung in Vorbereitung. Danach müßten sich Benützer von Archivmaterial, das nach 1900 entstanden sei, künftig verpflichten, sich bei der Benützung und Auswertung der Archivalien auf den angegebenen Forschungszweck zu beschränken, aus den Archivalien gefertigte Abschriften nicht an Dritte weiterzugeben und Namen noch lebender Personen, deren Nennung für den Forschungszweck nicht dringend erforderlich ist, bei der Veröffentlichung so zu anonymisieren, daß eine Identifizierung ausgeschlossen ist. Leider wird eine solche Verpflichtungserklärung ohne praktische Bedeutung sein, da wirksame Sanktionen, insbesondere **Strafvorschriften fehlen**.

16.2 Inventarisation von Kunst- und Geschichtsdenkmälern

Als Land mit einer alten Tradition und einer bedeutenden historischen Vergangenheit besitzt Bayern reiches Kulturgut, das auch für die kommenden Generationen erhalten werden soll. Das 1973 in Kraft getretene Denkmalschutzgesetz trifft hierzu nähere Regelungen. Es definiert Denkmäler als „von Menschen geschaffene Sachen oder die Teile davon aus vergangener Zeit, deren Erhaltung wegen ihrer geschichtlichen, künstlerischen, städtebaulichen, wissenschaftlichen oder volkskundlichen Bedeutung im Interesse der Allgemeinheit liegt. Dem Landesamt für Denkmalpflege kommt dabei eine zentrale Rolle zu. Ihm obliegt unter anderem die Erstellung und Fortführung der Inventare und der Denkmalliste, in die Baudenkmäler einschließlich ihrer historischen Ausstattungsstücke sowie Bodendenkmäler aufgenommen werden sollen. Auf Antrag des Berechtigten und in besonders wichtigen Fällen können bewegliche Denkmäler, die nicht bereits "historische Ausstattungsstücke" sind, ebenfalls Gegenstand der Inventarisation sein.

Ein Mitglied des Landesdenkmalrats hat mich auf folgende Problematik aufmerksam gemacht:

Mit der demnächst geplanten Inventarisation von Kunst- und Geschichtsdenkmälern ist eine erhebliche Gefahr für die Eigentümer verbunden. Neben einer genauen wissenschaftlichen Beschreibung, die insbesondere Rückschlüsse auf den Wert des Denkmals zuläßt, wird auch seine Lage genau beschrieben. Damit ist zumindest in Verbindung mit anderen Unterlagen wie Stadtadreßbuch, Liegenschaftskataster und Grundbuch in zahlreichen Fällen ein Rückschluß auf die Eigentümer der Kunstdenkmäler möglich. Da die Inventare veröffentlicht und somit der Allgemeinheit zugänglich gemacht werden sollen, besteht eine erhebliche Gefahr, daß sie Kunsträubern als „Nachschlagewerk" dienen könnten. Insbesondere die Veröffentlichung des Standorts beweglicher Denkmäler erhöht die Gefahr, daß sie von Dieben entwendet werden.

Ich habe hierzu in Gesprächen mit dem Staatsministerium für Wissenschaft und Kunst und dem Landesamt für Denkmalpflege folgende Auffassung vertreten:

Die Inventare enthalten personenbezogene Daten. In ihrer Bereitstellung zur Einsichtnahme ist eine Datenübermittlung zu sehen. Das Inventar stellt zwar keine Datei im Sinne des Bayer. Datenschutzgesetzes dar. Dessen Grundsätze können jedoch für die Beurteilung der Frage, ob die Bereitstellung der Inventare für allgemeine Einsichtnahme zulässig ist, entsprechend herangezogen werden. Das Denkmalschutzgesetz weist zwar dem Landesamt für Denkmalpflege die Aufgabe zu, das Inventar und die Denkmalliste zu erstellen und fortzuführen. Anders als zur Denkmalliste enthält es jedoch — beabsichtigt oder nicht — keine Regelungen zur Veröffentlichung von Inventaren. Nach Art. 18 Abs. 1 Satz 1 2. Alternative BayDSG ist daher für eine Einsichtnahme erforderlich, daß ein „berechtigtes Interesse" an der Kenntnis der Daten nachgewiesen wird — dies ist beispielsweise der Fall bei wissenschaftlichem oder Forschungsinteresse — **und** daß durch derartige Einsichtnahmen „schutzwürdige Belange" nicht beeinträchtigt werden. Solche schutzwürdi-

ge Belange können bei beweglichen Denkmälern oder Gegenständen in Denkmälern dadurch beeinträchtigt werden, daß ein erhöhtes Diebstahlrisiko geschaffen wird.

Deshalb ist in solchen Fällen eine Veröffentlichung durch Aufnahme in die Inventare nur mit Einwilligung der betroffenen Eigentümer zulässig. Zu demselben Ergebnis gelangt man, wenn man die Vorschriften über die Eintragung in die Denkmalliste „auf Antrag des Berechtigten" und in besonders wichtigen Fällen (Art. 2 Abs. 2 DSchG) auf Inventare analog anwendet. Dann bestehen allenfalls keine grundsätzlichen Bedenken dagegen, jedermann Einsicht in das Inventar zu gewähren.

Meine Hinweise hat das Staatsministerium für Wissenschaft und Kunst in die kürzlich erlassenen „Grundsätze für die Inventarisation der Kunst- und Geschichtsdenkmäler Bayerns" aufgenommen:

Unter Ziff. 10 „Datenschutz" wird darauf hingewiesen, daß „bewegliche historische Ausstattungsstücke" im Sinne von Art. 1 Abs. 2 Denkmalschutzgesetz und bewegliche Gegenstände, die nicht „historische Ausstattungsstücke" sind, **nur mit Einwilligung** des Eigentümers oder des sonstigen Berechtigten in das Inventar aufgenommen werden dürfen. Eine Einwilligung ist nur dann nicht erforderlich, wenn in besonders wichtigen Fällen ein berechtigtes öffentliches Interesse an der Inventarisation des betreffenden Gegenstandes besteht und dadurch schutzwürdige Belange des Eigentümers oder des sonstigen Berechtigten nicht beeinträchtigt werden. Die Einwilligung bedarf der Schriftform, soweit nicht wegen besonderer Umstände eine andere Form angemessen ist. Außerdem ist der Betroffene in geeigneter Weise über die Bedeutung der Einwilligung aufzuklären.

Damit wird sichergestellt, daß auch bei Offenlegung der Inventare die berechtigten Interessen der Eigentümer beweglicher Denkmäler angemessen Berücksichtigung finden. Das Ministerium hat außerdem zugesagt, bei einer Novellierung des Denkmalschutzgesetzes präzise Regelungen zur Inventarisation in das Gesetz aufzunehmen.

17. Umweltfragen

17.1 Gesetzgebung

Im Berichtszeitraum wurden auf Landes-, Bundes- sowie EG-Ebene mehrere Gesetzesinitiativen eingebracht und zum Teil verabschiedet. Allen gemeinsam ist, daß sie ein **erweitertes Auskunftsrecht der Bürger** über Umweltdaten anstreben und so zu **mehr Transparenz** für Behörden und Betroffene bei Entscheidungen über umweltrelevante Vorhaben führen sollen.

Im einzelnen handelte es sich um folgende Gesetzgebungsverfahren:

1. Auf Landesebene

1.1 Bayerisches Abfallwirtschafts- und Altlastengesetz (BayAbfAlG)

Zwischenzeitlich hat der Landtag das am 1.7.1990 in Kraft getretene Gesetz zur Vermeidung, Verwertung und sonstigen Entsorgung von Abfällen (Bayer. Abfallwirtschaftsgesetz) um Vorschriften über Altlasten erweitert. Art. 27 sieht die Erstellung und Fortführung eines Altlastenkatasters beim Landesamt für Umweltschutz vor und enthält Regelungen zur Datenübermittlung an nachgeordnete Behörden. Ein Auskunftsrecht für Bürger ist nicht enthalten. Das Gesetz wird dem Volk gemeinsam mit dem Volksbegehren „Das bessere Müllkonzept" zur Abstimmung vorgelegt.

1.2 Volksbegehren über den Entwurf eines Bayer. Abfallwirtschaftsgesetzes

Der Gesetzentwurf enthält in Art. 21 Regelungen zum „Altablagerungskataster". Das Kataster soll **der Öffentlichkeit zugänglich gemacht** werden.

1.3 Gesetz zum Auskunftsrecht über Umweltdaten — Umweltdatenauskunftsgesetz (UAG)

Dieser Gesetzentwurf der SPD sah einen **gesetzlich verankerten Anspruch der Bürger** gegenüber der Umweltverwaltung vor, **Auskunft über bestimmte Umweltdaten** zu erhalten. Außerdem sollte der Verwaltung das Recht eingeräumt werden, diese Daten von sich aus zu **veröffentlichen**.

Der Gesetzentwurf wurde im Landtag und im Senat wegen verfassungsrechtlicher Bedenken — ein Anspruch auf Auskunft über Umweltdaten durch „Jedermann" gefährde das Grundrecht auf informationelle Selbstbestimmung — sowie im Hinblick auf den bevorstehenden Erlaß einer ähnlich lautenden EG-Richtlinie abgelehnt.

2. Auf Bundesebene

2.1 Gesetz über die Umweltverträglichkeitsprüfung (UVP-Gesetz)

Am 1.8.1990 traten wesentliche Teile dieses Gesetzes in Kraft. Es führt die gemeinschaftsrechtlich vorgeschriebene Umweltverträglichkeitsprüfung umweltrelevanter Großvorhaben in das deutsche Recht ein. Umweltverträglichkeitsprüfung bedeutet die Ermittlung, Beschreibung und Bewertung der Auswirkungen eines Vorhabens auf die einzelnen Umweltmedien einschließlich der jeweiligen Wechselwirkungen **unter Einbeziehung der Öffentlichkeit**.

Als Kernstück enthält das UVP-Gesetz die Beteiligung der Öffentlichkeit bei der Zulassung aller umweltrelevanten Großvorhaben (§ 2 Abs. 1 i.V.m. § 9 UVPG). Die zuständige Behörde hat die **Öffentlichkeit** zu den Umweltauswirkungen des Vorhabens auf der Grundlage der ausgelegten Unterlagen **anzuhören**. Das Anhörungsverfahren muß den Anforderungen des § 73 Abs. 3 bis 7 des Verwaltungsverfahrensgesetzes für Planfeststellungsverfahren entsprechen. § 10 UVPG bestimmt, daß die Rechtsvorschriften über **Geheimhaltung** und **Datenschutz** unberührt bleiben.

2.2 Drittes Gesetz zur Änderung des Bundesimmissionsschutzgesetzes

§ 27 BImSchG, der nähere Regelungen zur **Emissionserklärung** enthält, sieht in Absatz 3 Satz 1 vor, daß „Einzelangaben der Emissionserklärung **nicht veröffentlicht** werden dürfen, wenn aus diesen **Rückschlüsse auf Betriebs- oder Geschäftsgeheimnisse** gezogen werden können". Bisher war der Betreiber vor der Veröffentlichung zu deren Art und Umfang zu hören (Satz 2). Nunmehr wurde Satz 2 dahingehend geändert, daß der Be-

treiber „bei Abgabe der Emissionserklärung der zuständigen Behörde **mitzuteilen** und **zu begründen** hat, **welche Einzelangaben** der Emissionserklärung **Rückschlüsse** auf **Betriebs- oder Geschäftsgeheimnisse** erlauben." Während bisher die einzelne Behörde bei Auskunftserteilung aus Emissionserklärungen zu prüfen hatte, ob dadurch keine Betriebs- oder Geschäftsgeheimnisse unzulässigerweise offenbart werden, obliegt nun dem Betreiber einer Anlage die vorgezogene **Darlegungslast**, welche Einzelangaben seiner Emissionserklärung Rückschlüsse auf Betriebs- oder Geschäftsgeheimnisse erlauben. Die Novellierung des § 27 BImSchG macht Änderungen der 5., 6. und 11. Verordnung zum BImSchG erforderlich, die noch erfolgen werden.

2.3 Umwelthaftungsgesetz (UmweltHG)

Das Gesetz, das am 1.1.1991 in Kraft tritt, unterwirft bestimmte gefährliche Anlagen — unabhängig von einem Verschulden — der Gefährdungshaftung. Ansprüche entstehen, wenn bei einem Schaden ein einzelner Verursacher ermittelt werden kann.

Das Gesetz sieht **Auskunftsansprüche** des Geschädigten gegenüber dem Inhaber einer Anlage sowie gegenüber den Behörden, die die Anlage genehmigt haben oder überwachen, vor, soweit dies zur Feststellung eines Anspruches auf Schadensersatz nach dem Gesetz erforderlich ist.

Als Grenzen für die Auskunftserteilung sieht das Gesetz u.a. das Vorliegen eines überwiegenden Interesses des Inhabers der Anlage oder berechtigter Interessen Dritter an der Geheimhaltung an.

3. Auf EG-Ebene

3.1 Vorschlag für eine Richtlinie des Rates über den freien Zugang zu Informationen über die Umwelt

Die EG-Kommission beschloß am 19.10.1988 den Vorschlag einer Richtlinie, die einen **weitgehenden Auskunftsanspruch** des Bürgers über Umweltdaten vorsieht. Danach sollen die Behörden verpflichtet werden, allen natürlichen oder juristischen Personen auf Antrag **ohne Nachweis eines Interesses Informationen über die Umwelt** zur Verfügung zu stellen. Die Mitgliedsstaaten legen die praktischen Regeln fest, nach denen die Informationen zugänglich gemacht werden. So kann für die Übermittlung der Informationen eine Gebühr in angemessener Höhe erhoben werden. Auch besteht die Möglichkeit, einen Antrag auf Zugang zu Informationen abzulehnen, wenn er sich auf die Übermittlung noch nicht abgeschlossener Schriftstücke oder noch nicht aufbereiteter Daten oder interner Mitteilungen bezieht oder der Antrag offensichtlich mißbräuchlich oder zu allgemein formuliert ist.

Die Richtlinie läßt auch eine **Einschränkung des Auskunftsanspruchs** unter anderem zum Schutz von **Geschäfts- und Betriebsgeheimnissen** sowie personenbezogenen Daten in größerem Umfang zu, wenn dadurch beispielsweise Geschäfts- und Betriebsgeheimnisse einschließlich des geistigen Eigentums, die Vertraulichkeit personenbezogener Daten und/oder Akten oder Unterlagen, die von einem Dritten übermittelt worden sind, der dazu nicht gesetzlich verpflichtet war, berührt werden.

Die Behörde soll dem Antragsteller sobald wie möglich, spätestens jedoch innerhalb von zwei Monaten eine Antwort erteilen, wobei die Ablehnung des Antrags auf Information zu begründen ist. Ist jemand der Ansicht, daß sein Informationsersuchen zu Unrecht abgelehnt oder nicht beachtet worden ist, oder hat er eine unzulängliche Antwort erhalten, so steht ihm gegen den Bescheid der Gerichts- oder Verwaltungsrechtsweg der jeweiligen Mitgliedsstaaten offen.

Weiterhin sieht die Richtlinie vor, der **Öffentlichkeit allgemeine Informationen** über den Zustand der Umwelt, z.B. durch die **regelmäßige Veröffentlichung** von Zustandsberichten, zur Verfügung zu stellen.

Der Bundesrat sah mit Beschluß vom 21.4.1989 in dem Richtlinienvorschlag eine geeignete Grundlage für die Schaffung der Informationsfreiheit im Bereich des Umweltschutzes in den Mitgliedsstaaten der Europäischen Gemeinschaft und auch gegenüber den Gemeinschaftsorganen der EG. Im Juni 1990 wurde die Richtlinie vom Rat der Europäischen Gemeinschaften in Brüssel **beschlossen.** Nach seiner Auffassung wird der Zugang zu umweltbezogenen Informationen im Besitz der Behörden den Umweltschutz verbessern.

Um der Richtlinie bis spätestens am 31.12.1992 nachzukommen, müssen die Mitgliedsstaaten entsprechende Rechts- und Verwaltungsvorschriften erlassen und in Kraft setzen.

Der vorliegende Vorschlag der Richtlinie stützt sich auf Art. 130 s des EWG-Vertrages (EWGV). Richtlinien nach dieser Vorschrift stellen gemäß Art. 130 t EWGV ausnahmslos Mindestregelungen dar. Der nationale Gesetzgeber kann über sie zugunsten des Umweltschutzes hinausgehen, allerdings nur insoweit, als die strengeren nationalen Regelungen mit den sonstigen Normen des EWG-Vertrags vereinbar sind. Schranken setzen insoweit vor allem die Grundfreiheiten.

17.2 Offenlegung von Altlastenkatastern

In den Umweltschutzreferaten mehrerer bayerischer Städte werden sogenannte Altlastenkataster erstellt. Sie enthalten Aussagen zu Grundstücken, bei denen der Verdacht einer Bodenverunreinigung durch umweltgefährdende Stoffe besteht (sogenannte Altlasten). Dabei wird nach Altstandorten und Altablagerungen unterschieden. Während es sich bei den „Altstandorten" um Betriebe handelt, in denen möglicherweise umweltgefährdende Stoffe verwendet, verarbeitet oder gelagert wurden, kennzeichnet der Begriff „Altablagerungen" frühere Abgrabungen (z.B. Kiesgruben), die mit einem bisher noch unbekannten Material verfüllt wurden, das Risiken für die Umwelt und somit auch für den Menschen darstellen kann.

Für beide Arten von Altlasten gilt, daß — soweit nicht im Einzelfall bereits Untersuchungen vorgenommen oder Maßnahmen aufgrund einer konkreten Gefahr getroffen wurden — für alle in das Kataster aufgenommenen Flächen nur der noch nicht verifizierte Verdacht einer Kontamination besteht. Das Thema „Altlasten" wird in der Öffentlichkeit lebhaft diskutiert. Verschiedene Gruppen fordern immer wieder eine generelle oder teilweise Offenlegung des Katasters.

Im Berichtszeitraum habe ich mich mit der Zulässigkeit der Veröffentlichung und der Einsichtnahme durch Mieter, Pächter, Nachbarn und Kaufinteressenten in das Altlastenkataster befaßt.

1. Gegenstand der Einsichtnahme

   Gegenstand der Einsichtnahme können nur Daten sein, die zur Feststellung einer eventuellen Bodenverunreinigung erforderlich sind. Bei Altstandorten kommen beispielsweise Daten zum Grundstück, seiner Beschaffenheit sowie seiner Nutzung in der Vergangenheit in Frage. Oft finden sich jedoch auch Angaben zur gegenwärtigen Nutzung des Grundstücks sowie seiner Umgebung und Hinweise darauf, welche Schadstoffe möglicherweise verwendet oder verarbeitet wurden. Katasterblätter zu Altablagerungen enthalten häufig folgende Daten: Bezeichnung der Grube, Lage, Abgrabegenehmigung, Fassungsvermögen, Tiefe, Jahr der Einfüllung, Hinweise auf das Verfüllmaterial, Name des Eigentümers/Pächters.

   Soweit darüber hinausgehende Informationen enthalten sind, beispielweise über die geplante oder künftige Nutzung (Bauantrag/Bauvoranfrage, geplante Nutzungsänderung), welche zur Feststellung einer evtl. Kontamination des Grundstücks nicht erforderlich sind, ist eine Einsichtnahme in diese Daten nicht erforderlich und daher unzulässig.

2. Rechtsgrundlagen für eine Einsichtnahme

2.1 Solange eine bereichsspezifische Regelung fehlt, kommt als Rechtsgrundlage für die Einsichtnahme in das Altlastenkataster **Art. 18 Abs. 1 Satz 1 2. Alternative BayDSG** in entsprechender Anwendung in Betracht. Danach ist eine Datenübermittlung, wie sie die Einsichtnahme darstellt, nur zulässig, wenn der Empfänger ein berechtigtes Interesse an der Kenntnis der zu übermittelnden Daten glaubhaft macht und dadurch schutzwürdige Belange des Betroffenen nicht beeinträchtigt werden.

   Zu den „berechtigten Interessen" gehört jedes von der Rechtsordnung als schutzwürdig anerkannte ideelle oder vermögenswerte Interesse. Es kann sich dabei um wirtschaftliche, soziale, kulturelle oder ideelle Belange handeln. Bei Mietern, Pächtern und Grundstücksnachbarn kann ein berechtigtes Interesse in der Sorge um ihre Gesundheit gesehen werden. Auch ihre wirtschaftlichen Interessen können betroffen sein, wenn sich der Verdacht auf eine Gesundheitsgefährdung durch eine — nachgewiesene — Bodenbelastung bestätigen sollte und sich damit eine Beschränkung oder ein Verbot der bisherigen Nutzung, der gemieteten/gepachteten Sache oder des Nachbargrundstückes ergibt.

   „Schutzwürdige Belange" der Grundstückseigentümer können beeinträchtigt werden, wenn durch eine Einsichtnahme der Eindruck erweckt wird, daß von dem Grundstück ein Umweltrisiko ausgeht und damit der Wert des Grundstücks gemindert wird, obwohl diese Frage zum Zeitpunkt der Einsichtnahme nicht zutreffend beantwortet werden kann.

   Art. 18 Abs. 1 BayDSG verlangt eine Abwägung: Je schwerwiegender das „berechtigte Interesse" des Auskunftssuchenden ist, desto höherwertiger müssen die „schutzwürdigen Belange" des Eigentümers sein, wenn ihre Beeinträchtigung eine Datenübermittlung verhindern soll.

   Im vorliegenden Fall spricht für eine Bekanntgabe die relativ geringe Sensibilität der Daten. Mit Ausnahme der Angaben zu geplanten Bauvorhaben und Nutzungsänderungen — hierfür ist kein „berechtigtes Interesse" erkennbar — besagt das Kataster nur, daß der Betrieb möglicherweise umweltgefährdende Stoffe verwendet oder verarbeitet hat, nicht jedoch, wie der Betrieb mit den Stoffen umgegangen ist und welches Risiko er für das Grundstück tatsächlich erzeugt hat. Genauso besagt die Tatsache, daß eine Abgrabung vorliegt, noch nichts darüber aus, ob sie tatsächlich mit umweltgefährdendem Material verfüllt wurde. Allerdings schlägt sich der allgemeine Erfahrungswert, daß zu mehr als 75% umweltriskantes Material verfüllt wurde, als Verdacht auf das betreffende Grundstück nieder. Als weiteres Motiv für eine Einsichtnahme sind gesundheitliche Interessen der Mieter, Pächter und Grundstücksnachbarn zu nennen. Erst wenn man von einer potentiellen Gefahr Kenntnis hat, kann man weitere Schritte unternehmen, um den Verdacht auszuräumen oder zu erhärten. Dies liegt gleichzeitig im öffentlichen Interesse, da somit bereits zu einem früheren Zeitpunkt festgestellt werden kann, ob eine konkrete Gefahr für Leib und Leben vorliegt und entsprechende Maßnahmen ergriffen werden können.

   Demgegenüber sind die möglicherweise für die Betroffenen (Grundstückseigentümer) zu erwartenden Wertminderungen als rein ökonomische Interessen geringer zu bewerten. Sie müssen hinter den „berechtigten Interessen" der Mieter, Pächter und Nachbarn zurücktreten.

   Aus den vorgenannten Gründen halte ich die **Einsichtnahme von Mietern, Pächtern und Nachbarn in das Altlastenkataster** unter der Voraussetzung **für zulässig**, daß das berechtigte Interesse und insbesondere die es begründenden Tatsachen durch Vorlage des Miet- bzw. Pachtvertrags oder eines Adreßnachweises glaubhaft gemacht werden.

   Eine Einsichtnahme von Miet-, Pacht- und Kauf**interessenten** sollte dagegen **nur mit Zustimmung des Eigentümers** gewährt werden. Ansonsten könnten auch Personen Einsicht erhalten, welche die im Kataster enthaltenen Informationen für andere Zwecke verwenden. Ihnen gegenüber scheint mir das Interesse des Eigentümers an der Geheimhaltung zu überwiegen und deshalb schutzwürdig. Die Einsichtnahme wäre durch Art. 18 BayDSG nicht gedeckt.

   Außerdem hat die Behörde sicherzustellen, daß bei einer Einsichtnahme durch den berechtigten Personenkreis ausdrücklich auf die eingeschränkte Aussagekraft des Katasters hingewiesen wird, nämlich darauf, daß das Kataster nur einen nicht näher verifizierten Verdacht der Kontamination der aufgeführten Grundstücke begründet.

   Aus den vorstehenden Überlegungen ergibt sich gleichzeitig, daß eine Einsichtnahme der Allgemeinheit in das Kataster oder eine Veröffentlichung des Katasters nicht zulässig ist.

Auch im folgenden Fall geht es um die Problematik der Veröffentlichung von Altlastendaten:

17.3 Veröffentlichung einer Karte mit Eintragungen ehemaliger Kiesgruben

Eine Behörde wandte sich mit folgendem Problem an mich:

In ihrem Umweltschutzreferat sei eine **Karte über Abgrabungen im Stadtgebiet** angelegt worden. Ehemalige und noch in Betrieb befindliche Kiesgruben sowie aufgefüllte Abgrabungen seien farblich hervorgehoben. Die aufgefüllten Abgrabungen seien von besonderer Bedeutung, weil sie früher häufig mit bisher unbekanntem Schutt und Abfällen angefüllt worden seien und heute potentielle Altlasten darstellten, die sowohl für das Grundwasser wie auch für die Nachfolgenutzung erhebliche Probleme aufwerfen könnten. Die Karte sei anhand alter Unterlagen über Baugenehmigungen und wasserrechtliche Erlaubnisse sowie Luftbildauswertungen erstellt worden. Sie enthalte außerdem, ähnlich wie ein Stadtplan, Straßenzüge sowie Gewässer und andere markante Punkte, so daß ein ortskundiger Betrachter jederzeit die Lage seines Hauses oder seines Grundstücks rekonstruieren und somit in Erfahrung bringen könne, ob es sich auf einer farblich markierten und somit problematischen Fläche befinde. Da die Behörde eine Veröffentlichung der Karte plante, bat sie mich um datenschutzrechtliche Stellungnahme.

Ich habe hierzu folgende Auffassung vertreten:

Bei der **Veröffentlichung** der Karte handelt es sich um eine **Datenübermittlung an einen nicht näher bestimmbaren Personenkreis**. Da aufgrund der Struktur der Karte die potentiellen Altlasten einem Grundstück oder zumindest einer Siedlungseinheit zugeordnet werden können, handelt es sich — zumindest soweit sich die Grundstücke in der Hand von Privateigentümern befinden — um Angaben über sachliche Verhältnisse des Eigentümers und damit um personenbezogene Daten. Solange keine bereichsspezifische Regelung vorliegt, beurteilt sich die Übermittlung der Daten **nach den Grundsätzen des Art. 18 Abs. 1 BayDSG.** Danach wäre eine Veröffentlichung der Karte zulässig, **soweit die Empfänger ein berechtigtes Interesse an der Kenntnis der Daten glaubhaft machen und dadurch schutzwürdige Belange der Betroffenen nicht beeinträchtigt werden.**

Wie bereits oben (vgl. 17.2) ausführlich dargelegt wurde, ist zwar ein „berechtigtes Interesse" bestimmter Personengruppen, nicht jedoch der Öffentlichkeit als Ganzes erkennbar. Dem gegenüber stehen „schutzwürdige Belange" der Eigentümer in der Form, daß sie vor einer unbegründeten Wertminderung ihres Grundstücks geschützt sein sollen. Durch die im Vergleich zu einem parzellenscharfen Kataster ungenauen Flächenmarkierungen besteht zudem die Gefahr, daß unbelastete Flächen als altlastenverdächtig angesehen werden und damit automatisch einer Wertminderung unterliegen.

Da andere Möglichkeiten bestehen, den Personenkreis, der ein „berechtigtes Interesse" nachweisen kann, über mögliche Altlasten auf einem Grundstück zu informieren — beispielsweise durch Einsichtgewährung in das vorgenannte Altlastenkataster- habe ich **von einer Veröffentlichung der vorbeschriebenen Karte in der vorgesehenen Form abgeraten.** Soll eine Karte mit Erkenntnissen über Altablagerungen der Öffentlichkeit zugänglich gemacht werden, darf sie keine Angaben enthalten, die einen Bezug auf eine bestimmte oder bestimmbare natürliche Person zulassen, es sei denn, solche Angaben sind offenkundig oder ihre Bekanntgabe ist zur Abwehr von Gefahren oder aus anderen überwiegenden Gründen des Gemeinwohls erforderlich. Eine Veröffentlichung würde zudem zu einer im Einzelfall unbegründeten Verunsicherung der Bevölkerung führen, womit letztendlich niemandem gedient wäre. Anders zu bewerten wäre eine Veröffentlichung von Teilgebieten für den Fall, daß sich eine konkrete Gefahr aufgrund vorgenommener Untersuchungen oder anderer Erkenntnisse ergibt.

18. Verkehrswesen

18.1 Verständigung der Führerscheinstelle bei Anordnung von Pflegschaften durch Amtsgerichte (Vormundschaftsgerichte)

Ein Bürger fragte nach, ob es zulässig sei, daß die Amtsgerichte (Vormundschaftsgerichte) die Führerscheinstellen der Kreisverwaltungsbehörden über Anordnungen von Pflegschaften unterrichten.

Rechtsgrundlage für die Bekanntgabe der Pflegschaftsanordnung an die Kreisverwaltungsbehörden sind derzeit noch die „Mitteilungen in Zivilsachen" (Mizi). Die Mitteilungen in Zivilsachen werden als Rechtsgrundlage abgelöst durch das bereits vom Bundestag verabschiedete Betreuungsgesetz, das am 1.1.1992 in Kraft treten wird: In § 69 k des Gesetzes über die Freiwillige Gerichtsbarkeit ist die Mitteilungspflicht der Vormundschaftsgerichte künftig gesetzlich festgelegt.

Innerhalb der Kreisverwaltungsbehörde erhalten auch die Führerscheinstellen die Mitteilung über die Anordnung der Pflegschaft. Die Führerscheinstelle hat dann nach § 15 b Abs. 2 der Straßenverkehrszulassungsordnung (StVZO) zu prüfen, ob Anlaß zur Annahme besteht, daß der Inhaber einer Erlaubnis zum Führen eines Kraftfahrzeugs ungeeignet oder nur noch bedingt geeignet ist.

18.2 Befragung einer Marktgemeinde zur Einführung von Tempo-30-Zonen

Eine Marktgemeinde führte eine Befragung zur Einführung von Tempo-30-Zonen in ihrem Gemeindebereich durch. Die Befragung lief folgendermaßen ab: Die Marktgemeinde verschickte Antwort-Postkarten an die Bürger, auf denen Namen und Anschrift der Bürger bereits eingetragen waren. Folgender Text war u.a. auf der Postkarte aufgedruckt:

„Einführung von Tempo-30-Zonen
Zur Ausweisung von Tempo-30-Zonen stimme ich folgendermaßen:
Ja, ich bin für Tempo-30-Zonen.
Nein, ich bin gegen Tempo-30-Zonen.
Zutreffendes bitte ankreuzen."

Auf der Rückseite der Postkarte stand u.a. der Satz:

„Für Ihre Bemühungen und die Teilnahme an dieser Aktion bedanken wir uns bereits im voraus recht herzlich.

gez. ... 1. Bürgermeister"

Ein Bürger aus dieser Gemeinde hat mich um datenschutzrechtliche Beurteilung dieser Befragung gebeten.

Zunächst ist anzumerken, daß ein **Hinweis auf die Freiwilligkeit** der Beteiligung an der Befragung fehlte (Hinweis gem. Art. 16 Abs. 2 BayDSG). Der Satz „Für Ihre Bemühungen und die Teilnahme an dieser Aktion bedanken wir uns bereits im voraus recht herzlich" ist kein solcher Hinweis. Auch wenn die meisten Bürger des Marktes es wahrscheinlich als selbstverständlich ansehen, daß die Teilnahme freiwillig ist, wird man doch nicht ausschließen können, daß einzelne Bürger durch den fehlenden Hinweis irritiert sind und glauben, sie seien zur Beantwortung der Frage gesetzlich verpflichtet.

Dem Datenschutz hätte es auch eher entsprochen, wenn die Fragebogenaktion **anonymisiert** durchgeführt worden wäre. Es ist kein vernünftiger Grund ersichtlich, warum Namen und Anschrift des Befragten auf der Postkarte eingetragen waren. Der Marktgemeinde kam es erkennbar darauf an, einen Überblick zu erhalten, wie die Stimmungslage in der Bevölkerung hinsichtlich der Einführung von Tempo-30-Zonen ist. Dazu hätte das Stimmenverhältnis (ja oder nein) ausgereicht. Der mehrfachen Stimmabgabe durch eine Person hätte man durch andere Maßnahmen vorbeugen können.

Technisch hätte dies so ausgesehen, daß auf einem Fragebogenblatt oder einer Rücklaufpostkarte ein abtrennbarer Abschnitt mit dem Anschriftenfeld angebracht wird. Beim Rücklauf des Bogens wird dann dieses Anschriftenfeld abgetrennt und mit einer zur Rücklaufkontrolle angelegten Liste der Bürger des Marktes verglichen. Rücklaufkontrolliste und Anschriftenfeld werden anschließend vernichtet. Ausgewertet werden nur noch die anonymisierten Angaben mit den Antworten ja oder nein zu Tempo-30-Zonen.

Ich habe meine Auffassung dem 1. Bürgermeister der Marktgemeinde mitgeteilt.

18.3 Auskünfte der Kfz-Zulassungsstelle gegenüber Beauftragten der Rundfunkanstalten

Ein Beschwerdeführer fragte an, ob die Beauftragten der Rundfunkanstalten von den Kraftfahrzeugzulassungsstellen Auskünfte darüber erhalten dürfen, wer Halter eines bestimmten Kraftfahrzeuges ist. Ich habe einen Auskunftsanspruch verneint.

Die Beauftragten der Rundfunkanstalten benötigen Name und Anschrift von Fahrzeughaltern, um feststellen zu können, ob eine Rundfunkgebührenpflicht des Halters besteht. Das ist zum Beispiel dann der Fall, wenn das Kraftfahrzeug zu gewerblichen Zwecken oder zu einer anderen selbständigen Erwerbstätigkeit genutzt wird. Die Rundfunkbeauftragten haben dann zu überprüfen, ob das Autoradio angemeldet ist. Das Bereithalten von Rundfunkgeräten ohne Anmeldung nach Art. 9 Rundfunkgebührenstaatsvertrag stellt eine Ordnungswidrigkeit dar.

Als Rechtsgrundlage für solche Auskunftsbegehren der Rundfunkbeauftragten kommt § 35 Abs. 1 Satz 1 Nr. 3 Straßenverkehrsgesetz (StVG) in Frage. Diese Bestimmung gewährt einen Auskunftsanspruch, wenn die Halterdaten **für die Verfolgung von Ordnungswidrigkeiten** benötigt werden. Das Problem besteht darin, daß die Rundfunkanstalten für die **Verfolgung der Ordnungswidrigkeit** nicht zuständig sind; dies sind vielmehr die Kreisverwaltungsbehörden. Die Rundfunkanstalten können lediglich den **Antrag** auf Verfolgung dieser Ordnungswidrigkeit **stellen**; sie werden im Vorfeld ihrer Entscheidung, ob ein Antrag auf Verfolgung zu stellen ist, Ermittlungen vornehmen. Diesen Ermittlungen kommt jedoch nicht der Charakter einer Verfolgung von Ordnungswidrigkeiten zu. Vielmehr dienen sie der Klärung der Frage, ob überhaupt der Verdacht einer Ordnungswidrigkeit besteht. § 35 Abs. 1 Satz 1 Nr. 3 StVG scheidet demnach als Rechtsgrundlage aus.

Als weitere Rechtsgrundlage für eine Auskunftserteilung an die Beauftragten der Rundfunkanstalten kommt § 39 Abs. 1 StVG in Betracht. Danach können die Halterdaten durch die Zulassungsstelle übermittelt werden, wenn der Empfänger unter Angabe des betreffenden Kennzeichens darlegt, daß er die Daten zur Geltendmachung, Sicherung oder Vollstrekkung oder zur Befriedigung oder Abwehr von Rechtsansprüchen **im Zusammenhang mit der Teilnahme am Straßenverkehr** oder zur Erhebung einer Privatklage **wegen im Straßenverkehr begangener Verstöße** benötigt. Diese Voraussetzungen liegen nicht vor. Das Bereithalten eines Autoradios erfüllt insoweit nicht den straßenverkehrsrechtlichen Tatbestand der „Teilnahme am Straßenverkehr". Die Ausnahmevorschrift des § 39 Abs. 1 StVG kann nach allgemeinen Rechtsgrundsätzen nur eng ausgelegt werden.

Die Kfz-Zulassungsstellen dürfen also dem Rundfunkbeauftragten die Halter von Kraftfahrzeugen nicht mitteilen.

18.4 Zentrales Verkehrsinformationssystem (ZEVIS)

Das Straßenverkehrsgesetz enthält die Rechtsgrundlage für die Einrichtung eines zentralen Fahrzeugregisters und bestimmt auch die Stellen, die neben den Fahrzeugzulassungsstellen befugt sind, das Register zu nutzen (z.B. Polizeibehörden). Wie ich bereits im 11. Tätigkeitsbericht angekündigt habe, werden nunmehr auf Anordnung des Staatsministeriums des Innern **alle** ZEVIS-Anfragen durch bayerische Polizeidienststellen in einer Protokolldatei beim Bayer. Landeskriminalamt aufgezeichnet. Der anfragende Polizeibeamte muß sich **vor der Anfrage** „identifizieren" und **vor der Ausgabe** der Auskunft den Grund der Anfrage — hierzu bestehen Katalogbegriffe — eingeben.

Das Abrufverfahren der Polizei aus ZEVIS und den Protokollierungsmodus habe ich geprüft. Beide entsprechen den datenschutzrechtlichen Anforderungen und stellen wegen der eindeutigen **Identifizierung der Abfragenden** und der **Protokollierung des Anlasses** datenschutzfreundliche Lösungen dar. Schwierigkeiten mit dem Abrufverfahren oder dem Protokollierungsmodus sind mir nicht bekannt geworden. Anfängliche technische Fehler und menschliche Unzulänglichkeiten bei der Handhabung des Verfahrens dürften ausgeräumt sein.

Da beispielsweise hinsichtlich Abrufberechtigungen und Protokollierungen von Abfragen in den Ländern verschiedene Lösungswege beschritten worden sind, haben der Bundesbeauftragte für den Datenschutz und die Landesbeauftragten ein sogenanntes „Fahrzeugregister-Informationskonzept" geplant, das der Verbesserung des Informationsstandes zwischen Aufsichtsbehörden und Datenschutzinstanzen dienen soll. Einem solchen Informationskonzept stehe ich mit Skepsis gegenüber, weil eine vollständige Umsetzung letztlich auch bundesweite und bundeseinheitliche Prüfungen erfordern würde. Eine Einbindung in gemeinsame Prüfungen lehne ich jedoch aus grundsätzlichen Erwägungen ab. Das geplante Konzept erscheint mir in Teilbereichen darüber hinaus zu aufwendig, weil es zur Wiederholung bereits durchgeführter Kontrollen führen würde.

18.5 Speicherung eines Unschuldigen in der Schwarzfahrerkartei der Bundesbahn oder der Verkehrsbetriebe

In der Münchner Presse ist der Fall eines 17jährigen Schülers geschildert worden, der in der Schwarzfahrerkartei der Deutschen Bundesbahn gespeichert war. Folgendes war geschehen:

Ein unbekannter Schwarzfahrer hatte in der S-Bahn bei einer Kontrolle Namen und Adresse dieses 17jährigen Schülers angegeben. Der Kontrolleur glaubte seiner Namensangabe. Der 17jährige war jedoch zum Zeitpunkt dieses Vorfalls in der Schule, konnte also der Schwarzfahrer nicht gewesen sein, wie der Kontrolleur später nach einem Anruf bei der Mutter des 17jährigen feststellen mußte. Dennoch nahm die Bundesbahn den Schüler nicht sofort aus der Schwarzfahrerkartei heraus. Er blieb noch über Monate gespeichert.

Da die Deutsche Bundesbahn nicht meiner Kontrollkompetenz unterliegt, habe ich den hierfür zuständigen Bundesbeauftragten für den Datenschutz gebeten, der Sache nachzugehen.

Dessen ungeachtet habe ich den Vorfall zum Anlaß genommen, mich bei den Stadtwerken München nach der dortigen Praxis in Fällen des Namensmißbrauchs zu erkundigen. Die Stadtwerke München haben mir mitgeteilt:

Der Name des Opfers, den der unbekannte Schwarzfahrer mißbraucht hat, wird zwar gespeichert, allerdings mit dem ausdrücklichen Hinweis, daß der Betroffene nicht selbst schwarzgefahren ist, sondern das Opfer einer falschen Personalienangabe ist (Namensmißbrauch). Nach einem Vierteljahr wird der Name automatisch unkenntlich gemacht. Auf Wunsch des Betroffenen wird der Name auch sofort manuell in der Datei unkenntlich gemacht.

Die dreimonatige Speicherung des Namensmißbrauchs ist nach Auffassung der Stadtwerke erforderlich, um die Fälle des wiederholten Mißbrauchs ein und desselben Namens erkennen zu können.

Ich halte diese Praxis für unbefriedigend und mit dem Datenschutz nicht vereinbar. Nicht hinzunehmen ist, daß man als unschuldiger Bürger allein aufgrund der falschen Namensangabe eines tatsächlichen Schwarzfahrers sofort in der Schwarzfahrerdatei gespeichert wird. In diese Datei, die ja keine „Empfehlungsliste" darstellt, darf nur der aufgenommen werden, dessen Identität feststeht. In den Fällen, in denen sich der Fahrgast ohne Fahrkarte auch noch zusätzlich nicht ausreichend ausweisen kann, halte ich die Eintragung in die Schwarzfahrerdatei erst dann für gerechtfertigt, wenn die Identität feststeht. Dieser für Polizeidateien selbstverständliche Grundsatz muß auch für eine Schwarzfahrerdatei gelten. Es ist Sache des Kontrolleurs, sich von der Identität des Schwarzfahrers zu überzeugen, sei es durch Anruf bei Verwandten oder Arbeitskollegen oder mit Hilfe der Polizei. Keinesfalls darf das Opfer einer falschen Namensangabe in der Schwarzfahrerdatei weiter gespeichert bleiben — auch nicht mit Zusätzen — mit der Begründung, auf diese Weise Fälle des wiederholten Mißbrauchs des gleichen Namens erkennen zu können. Das Problem muß durch eine umgehende Klärung der Personalien des Schwarzfahrers gelöst werden, keinesfalls darf es auf dem Rücken des Opfers ausgetragen werden.

18.6 „Schwarze Liste" über MVV-Störenfriede bei der U-Bahnwache

In der Münchner Presse erschienen Berichte über „Schwarze Listen" der U-Bahnwache in München. Eine Zeitung druckte sogar einen Auszug aus der Liste ab.

Die U-Bahnwache ist für die Überwachung der Sicherheit bei der Münchner U-Bahn zuständig. Sie beschäftigt ca. 40 Mitarbeiter im Streifendienst, die im Schichtdienst „rund um die Uhr" die U-Bahnhöfe bewachen.

In der Presse wurde bekannt, daß die U-Bahnwache in ihrer Dienststelle in einem Rechner ca. 200 Personen speichert und regelmäßig Listen mit diesen Personen an die Mitarbeiter im Streifendienst sowie an die Einsatzleitung verteilt. Die Personen in dieser Liste sind in der U-Bahn unangenehm als „Störenfriede" aufgefallen (z.B. wegen Trunkenheit, Sachbeschädigungen, Beleidigung anderer Fahrgäste u.ä.).

Von den gespeicherten Personen sind Name, Vorname, Geburtsdatum sowie die gegen sie verhängten Maßnahmen (z.B. das Hausverbot) vermerkt. Bei einigen sind zusätzlich Buchstaben wie „S", „A" oder „R" eingetragen. „S" steht für „Störer", „A" für „aggressiv" und „R" für „Randalierer". Bei einzelnen Personen steht „§ 20"; das bedeutet „schuldunfähig". Nach Angaben der Einsatzleitung der U-Bahnwache soll die Liste die im Streifendienst eingesetzten Mitarbeiter in die Lage versetzen, beim Zusammentreffen mit diesen Person die gebotenen Maßnahmen zu ergreifen, insbesondere zum Eigenschutz.

Grundsätzlich halte ich eine solche Liste für erforderlich. Die Bediensteten der U-Bahnwache müssen bei ihrem gewiß nicht einfachen Dienst wissen, mit welchen Personen sie es im Zweifelsfall zu tun haben, wenn sie wegen grober Verstöße gegen die Ordnung einschreiten müssen.

Anlaß zu Kritik gab mir jedoch die Anzahl der ausgedruckten Exemplare der Liste sowie die Buchstabenabkürzungen auf den Listen. Wie der Abdruck eines Auszugs aus der Liste in einer Zeitung zeigt, werden die Listen mißbraucht. Ich habe zunächst erreicht, daß statt der bislang verwendeten 40 Exemplare nur noch insgesamt 7 Listen (5 für die Doppelstreifen, je eine für eine Sonderstreife und die Einsatzleitung) ausgedruckt werden. Das Risiko, daß eine solche Liste in falsche Hände gerät, ist damit schon erheblich reduziert. Ferner ist es mir gelungen, die U-Bahnwache dazu zu bewegen, statt der Buchstabenkombinationen unverfängliche Ziffern zu verwenden. Statt der Buchstaben „A", „S" oder „R" sowie „§ 20" werden nunmehr Ziffern verwendet. Jede Ziffer hat eine andere Bedeutung; der „Klartext" ist nur den Bediensteten der U-Bahnwache bekannt. Für den Fall, daß eine solche Liste trotz aller Sicherheitsmaßnahmen unzulässigerweise weitergegeben wird, ist es für den Empfänger nicht mehr ohne weiteres erkennbar, welche Charakterisierung sich z.B. hinter der Ziffer „3" verbirgt. Dies ist ein wesentlicher Fortschritt.

Darüber hinaus habe ich die U-Bahnwache aufgefordert, die Aufzeichnungen über die Vorfälle (sogenannte „Protokolle") längstens drei Jahre aufzubewahren und dann anschließend zu vernichten. Auch habe ich die U-Bahnwache eindringlich darauf hingewiesen, daß die Personen, die bei ihr gespeichert und in der Liste verzeichnet sind, vorher eindeutig (am besten natürlich anhand amtlicher Personaldokumente) identifiziert werden müssen. Eine Speicherung einer Person,

deren Name lediglich von einer anderen Person mißbraucht worden ist, hielte ich gerade bei dieser Liste für einen schweren Verstoß gegen das Persönlichkeitsrecht. Nach Angaben der U-Bahnwache ist dies bislang noch nicht vorgekommen.

19. Datenschutz in Europa

Im 11. Tätigkeitsbericht hatte ich mit Blick auf den EG-Binnenmarkt 1992 die Notwendigkeit eines europäischen Datenschutzes unterstrichen. Im Berichtsjahr haben sich die Aussichten dafür, daß wir in absehbarer Zeit innerhalb der Europäischen Gemeinschaft Datenschutzregelungen von hohem Schutzniveau erhalten werden, beträchtlich verbessert. Im Herbst 1990 hat die EG-Kommission ein Datenschutz-Paket vorgelegt, das aus folgenden Teilen besteht:

- Vorschlag für eine **Richtlinie** des Rates zum Schutz von Personen bei der Verarbeitung personenbezogener Daten
- Entwurf einer **Entschließung** der im Rat vereinigten Vertreter der Regierungen der Mitgliedsstaaten der Europäischen Gemeinschaften
- **Erklärung der Kommission** betreffend die Anwendung der Grundsätze der Richtlinie zum Schutz von Personen bei der Verarbeitung personenbezogener Daten auf die Organe und Einrichtungen der Europäischen Gemeinschaften
- Vorschlag für eine Richtlinie des Rates zum Schutz personenbezogener Daten und der Privatsphäre in öffentlichen digitalen **Telekommunikationsnetzen**, insbesondere im diensteintegrierenden digitalen Telekommunikationsnetz (ISDN) und in öffentlichen digitalen Mobilfunknetzen
- Empfehlung für einen Beschluß des Rates zur Aufnahme von Verhandlungen über den **Beitritt** der Europäischen Gemeinschaft zum **Übereinkommen des Europarats** zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten
- Vorschlag für einen Beschluß des Rates auf dem Gebiet der **Informationssicherheit**

Mit den vorgeschlagenen Maßnahmen soll ein EG-weites Schutzsystem errichtet werden, um die Grundrechte der Bürger, insbesondere das Recht auf Privatsphäre und informationelle Selbstbestimmung auf einem hohen Schutzniveau zu gewährleisten und Hemmnisse für die Errichtung des Binnenmarkts abzubauen.

Der Vorschlag für eine **allgemeine Richtlinie** verfolgt das Ziel, in allen Mitgliedsstaaten der Gemeinschaft ein gleichwertiges hohes Datenschutzniveau einzuführen. Bislang bestehen nicht in allen Mitgliedsstaaten Datenschutzvorschriften. In den anderen Mitgliedsstaaten ist der Datenschutz unterschiedlich geregelt. Die Richtlinie, die eine Mischung aus den bestehenden nationalen Datenschutzgesetzen in den EG-Mitgliedsländern darstellt, verpflichtet die Mitgliedsstaaten, nationale Datenschutzregelungen entsprechend den in der Richtlinie genannten Grundsätzen zu erlassen. Die Richtlinie legt jedoch kein abschließendes Höchstniveau des Datenschutzes fest. Sie überläßt vielmehr den nationalen Gesetzgebern in vielen Fragen einen angemessenen Regelungsspielraum, so daß die einzelnen Länder an einer stärkeren Ausgestaltung ihres Datenschutzes nicht gehindert sind.

Die Richtlinie gilt für alle **Dateien**, deren Verantwortliche dem privaten Bereich oder dem öffentlichen Bereich zuzuordnen sind. Nicht erfaßt sind jedoch die Dateien des öffentlichen Bereichs, wenn die Tätigkeit dieser Organe nicht in den Anwendungsbereich des Gemeinschaftsrechts fällt, wie z.B. das Recht der Polizei oder des Verfassungsschutzes. Die Grundsätze, deren Beachtung die Richtlinie den nationalen Gesetzgebern auferlegt, beziehen sich insbesondere auf die Bedingungen, unter denen eine Verarbeitung personenbezogener Daten rechtmäßig ist, die Rechte der betroffenen Personen auf Unterrichtung, Auskunft, Recht auf Berichtigung, Einspruchsrecht, u.a. Die nötige Qualität der Daten wird festgelegt — sie müssen richtig nach Treu und Glauben und für bestimmte rechtmäßige Zwecke gespeichert sein. Für die Kontrolle der Einhaltung der Bestimmungen sind verschiedene Organe vorgesehen. Die Mitgliedsstaaten haben unabhängige mit Untersuchungs- und Eingriffsmöglichkeiten ausgestattete **Kontrollbehörden** zu errichten. Auf europäischer Ebene ist eine unabhängige „Gruppe für den Schutz personenbezogener Daten" vorgesehen, die aus Vertretern der nationalen Aufsichtsbehörden besteht und die EG-Kommission **beratend** unterstützt. Ein weiteres Organ stellt der **„beratende Ausschuß"** dar, der sich aus Vertretern der Mitgliedsstaaten zusammensetzt und die EG-Kommission bei den Maßnahmen zur Durchführung der Richtlinie unterstützt.

Den Entwurf der EG-Richtlinie halte ich für eine **geeignete Grundlage des Datenschutzes in der EG**. Auch wenn die Regelungen in manchen Bereichen hinter dem neuen Bundesdatenschutzgesetz zurückbleiben, ist es begrüßenswert, daß damit europaweite Datenschutzregelungen und Kontrollmöglichkeiten geschaffen werden und den nationalen Gesetzgebern **Spielraum bleibt, ihr eigenes nationales Datenschutzrecht noch zu verbessern**. In verschiedenen Punkten wird im Zuge der weiteren Diskussion der Richtlinie auch noch eine Verbesserung zu erreichen sein. Hierüber ist die Meinungsbildung innerhalb der Datenschutzbeauftragten im Gange.

Der **Entschließungsentwurf** der im Rat vereinigten Vertreter der Mitgliedsstaaten der Europäischen Gemeinschaft verfolgt das Ziel, die Geltung der Grundsätze der EG-Richtlinie auf diejenigen Dateien des öffentlichen Bereichs auszudehnen, für die die Richtlinie nicht gilt. Um den Grundsätzen Geltung zu verschaffen, müßten sich die Mitgliedsstaaten verpflichten, die erforderlichen Gesetzgebungsverfahren auf einzelstaatlicher Ebene einzuleiten. Aus der Sicht des Datenschutzes begrüße ich diese Zielsetzung des Entschließungsentwurfs, da für alle Dateien öffentlicher Verwaltungen, auch wenn sie nicht unter die allgemeine Richtlinie fallen, Datenschutzregelungen gelten müssen.

Die **Erklärung der Kommission** betreffend die Anwendung der Bestimmungen der allgemeinen Richtlinie auf die **Organe und Einrichtungen der Gemeinschaft** bringt den Wunsch zum Ausdruck, daß die Grundsätze der Richtlinie auch für die Organe und Einrichtungen der Gemeinschaft gelten sollen. Hierzu ist vorgesehen, daß die Kommission die erforderlichen Maßnahmen trifft und vorschlägt. In der Zwischenzeit wird die Richtlinie auf ihre eigenen Dateien angewendet.

Der Vorschlag für eine Richtlinie des Rates zum Schutz personenbezogener Daten und der Privatssphäre in öffentlichen digitalen **Telekommunikationsnetzen**, insbesondere im diensteintegrierenden digitalen Telekommunikationsnetz (ISDN) und in öffentlichen digitalen Mobilfunknetzen soll die allgemeine Richtlinie mit der Anwendung der allgemeinen Grundsätze des Datenschutzes auf den spezifischen Bedarf der neuen Telekommunikationsnetze ergänzen. Ziel dieser Richtlinie ist es, den Benützern der Telekommunikationseinrichtungen in allen Mitgliedsstaaten einen Datenschutz durch Maßnahmen zu garantieren, die in die von den neuen Netzen gebotenen Dienste zu integrieren sind. Auch diese Richtlinie halte ich für notwendig, damit die Gefährdungen durch die neue Telekommunikationstechnik europaweit begrenzt werden können.

Die Empfehlung für einen Beschluß des Rates betreffend den **Beitritt** der Europäischen Gemeinschaft zum Übereinkommen des Europarats zum Schutze des Menschen bei der automatischen Verarbeitung personenbezogener Daten wird in den Beziehungen zwischen der Gemeinschaft und den Drittländern, die Vertragspartner sind, den Schutz der betroffenen Personen und des grenzüberschreitenden Verkehrs personenbezogener Daten gewährleisten.

Der Vorschlag für eine Entscheidung des Rates über die Annahme eines **Zwei-Jahres-Aktionsprogramms** im Bereich der Sicherheit der Informationssysteme soll die Instrumente ergänzen, mit denen die Rechte der Personen bei der Verarbeitung personenbezogener Daten verstärkt werden sollen. Die Sicherheit der in elektronischer Form gespeicherten, verarbeiteten und übermittelten Daten vor zufälligen oder beabsichtigten Gefährdungen ist für die tatsächliche Wahrnehmung der Rechte der Personen bei der Verarbeitung personenbezogener Daten von wesentlicher Bedeutung. Die fortschreitende technische Entwicklung macht eine Zusammenarbeit auf dem Gebiet der Forschung und Entwicklung notwendig.

20. Medien

20.1 Medien und Datenschutz

In den letzten Tätigkeitsberichten habe ich auf Lücken im Persönlichkeitsschutz gegenüber Rundfunk, Presse und Film hingewiesen. Im Verfahren zum Gesetzentwurf zur Fortentwicklung der Datenverarbeitung und des Datenschutzes habe ich konkrete Vorschläge zur Verbesserung des Datenschutzes unterbreitet.

Zwischenzeitlich ist das neue Bundesdatenschutzgesetz verabschiedet. Es bringt eine Verbesserung des Mediendatenschutzes leider nur in einem Teilbereich, nämlich gegenüber dem Rundfunk des Bundes. Von den wesentlichen datenschutzrechtlichen Regelungen ausgenommen bleiben nach wie vor der übrige öffentliche Rundfunk sowie der private Rundfunk, die Presse und der Film.

§ 41 Abs. 1 des neuen Bundesdatenschutzgesetzes schreibt für die Presse, den Film und den Rundfunk im **journalistisch-redaktionellen Bereich** lediglich die Beachtung des **Datengeheimnisses** und technisch-organisatorischer Maßnahmen zur Gewährleistung der **Datensicherheit** vor. § 41 Abs. 2 macht den Rundfunkanstalten des Bundesrechts die Veröffentlichung von **Gegendarstellungen** der Betroffenen zur Pflicht sowie deren Speicherung für denselben Zeitraum wie die umstrittenen Daten selbst.

§ 41 Abs. 3 gewährt gegenüber den Rundfunkanstalten des Bundes einen **Auskunftsanspruch**, wenn jemand durch eine Berichterstattung in seinem Persönlichkeitsrecht beeinträchtigt worden ist. Ich hatte diesen Auskunftsanspruch bereits zu einem früheren Zeitpunkt, nämlich schon **vor einer Beeinträchtigung** des Persönlichkeitsrechts gefordert. Weiter sieht § 41 Abs. 3 einen **Berichtigungsanspruch** unrichtiger Daten vor. Ich hatte darüber hinaus einen **Löschungsanspruch** gefordert, wenn richtige Daten nicht ermittelt werden können. § 41 Abs. 4 i.V.m. § 42 sieht die Bestellung eines **Beauftragten für den Datenschutz** im Bereich der Rundfunkanstalten des Bundesrechts vor. Er kontrolliert die Einhaltung der datenschutzrechtlichen Vorschriften und ist in Ausübung dieses Amtes unabhängig und nur dem Gesetz unterworfen. Jedermann kann sich an ihn wenden.

Mit der Teilregelung des Datenschutzes in § 41 Bundesdatenschutzgesetz ist die **Diskussion um die Verbesserung des Datenschutzes im Medienbereich nicht abgeschlossen**.

Zum einen bleibt der Bundesgesetzgeber nach wie vor aufgefordert, der verfassungsrechtlichen Verpflichtung zur Gewährleistung eines ausreichenden Persönlichkeitsschutzes des einzelnen Bürgers gegenüber den Medien in einem **Presserechtsrahmengesetz** nachzukommen. Zum anderen wird es Aufgabe des bayer. Gesetzgebers sein, bei der Beratung des neuen **Bayer. Datenschutzgesetzes** im Rahmen seiner Zuständigkeit den Persönlichkeitsschutz gegenüber den Medien angemessen zu berücksichtigen.

Schließlich bezieht die von der EG-Kommission vorbereitete Richtlinie des Rates zum Schutz von Personen bei der Verarbeitung personenbezogener Daten den Medienbereich ein. Ausnahmen können nur vorgesehen werden, „sofern diese darauf abzielen, das Recht auf die Privatsphäre mit dem Recht auf Information und dem Recht, Informationen zu empfangen oder zu übermitteln, zu vereinbaren, das insbesondere in Art. 10 der Konvention zum Schutz der Menschenrechte und Grundfreiheiten garantiert ist". Damit wird das sog. Medienprivileg auf seinen Kern zurückgeführt.

20.2 Bayerische Landeszentrale für Neue Medien

In meinem vorletzten Tätigkeitsbericht hatte ich über die datenschutzrechtliche Prüfung bei der Bayerischen Landeszentrale für Neue Medien (BLM) berichtet. Wegen einer inhaltlichen Umstellung der EDV konnte damals die Prüfung nicht abgeschlossen werden. Diese Umstellung ist zwischenzeitlich weitgehend durchgeführt, aber noch nicht abgeschlossen. Einige automatisierte Verfahren befinden sich noch in der Entwicklungsphase. Ich habe deshalb davon abgesehen, im Berichtszeitraum die datenschutzrechtliche Überprüfung fortzusetzen. Kontrolliert habe ich hingegen die Einhaltung der Bestimmungen über die Datensicherheit. Hierzu verweise ich auf Ziff. 22.

20.3 ISDN

Zu den datenschutzrechtlichen Fragen, die das „dienste-integrierende digitale" Fernmeldenetz (ISDN) der Deutschen Bundespost mit sich bringt, habe ich mehrfach Stellung genommen. Damit das durch Art. 10 Grundgesetz garantierte

Grundrecht auf Wahrung des Fernmeldegeheimnisses, also das Grundrecht auf unkontrollierte und unbeobachtete Kommunikation nicht gefährdet wird, darf eine Speicherung und Verarbeitung von **Verbindungsdaten** von Telefonaten nur **aus wichtigen Gründen** und nur im hierzu notwendigen **Umfang** und für die erforderliche **Dauer** vorgenommen werden. Die in meinem letzten Tätigkeitsbericht dargelegten Forderungen zur Gewährleistung des Datenschutzes gelten nach wie vor.

Die Einführung öffentlicher digitaler Telekommunikationsnetze ist nunmehr auch in der **Europäischen Gemeinschaft** voll angelaufen. Dies erfordert ein gemeinschaftsweites gemeinsames Konzept für den Schutz der Privatsphäre und der personenbezogenen Daten sowie für die Datensicherheit. Zur Gewährleistung dieses Schutzes hat die EG-Kommission einen Vorschlag für eine **Richtlinie des Rates zum Schutz personenbezogener Daten und der Privatsphäre in öffentlichen digitalen Telekommunikationsnetzen**, insbesondere im diensteintegrierenden digitalen Telekommunikationsnetz (ISDN) und in öffentlichen digitalen Mobilfunknetzen vorgelegt. Ziel der Richtlinie ist es, gemeinschaftsweit ein datenschutzrechtliches Mindestniveau für den europäischen Bürger zu gewährleisten. Zum einen soll das Mißbrauchsrisiko minimiert werden. Hierzu sollen die bei öffentlichen Telekommunikationsdiensten verarbeiteten und gespeicherten Daten auf das strikte Minimum begrenzt werden, das zur Gewährleistung eines ordnungsgemäßen Betriebs sowie einer angemessenen Qualität der Dienste und der Teilnehmereinrichtungen notwendig ist. Zum anderen soll das Recht des Teilnehmers auf informationelle Selbstbestimmung gewährleistet werden, sowohl gegenüber der Telekommunikationsorganisation als auch gegenüber dem zweiten Teilnehmer einer Verbindung wie auch gegenüber Dritten, die Zugang zu den über ein öffentliches Kommunikationsnetz übertragenen oder bereitgestellten Daten haben wollen.

Die im Richtlinienentwurf vorgesehenen Anforderungen bringen eine Verbesserung des Persönlichkeitsschutzes in der europaweiten Telekommunikation. Sie entsprechen allerdings noch nicht dem Stand der Datenschutzdiskussion in der Bundesrepublik.

21. Bayerische Versicherungskammer

21.1 Prüfung bei der Bayer. Ärzteversorgung

Die Bayerische Ärzteversorgung ist die berufsständische Pflichtversorgungsanstalt des öffentlichen Rechts für Ärzte, Zahnärzte und Tierärzte in Bayern und in einigen anderen Bundesländern. Die Anstalt wird von der Bayerischen Versicherungskammer verwaltet und vertreten.

Die Prüfung dieser Einrichtung führte u.a. zu folgenden Feststellungen:

Speicherung der Ursache der Berufsunfähigkeit

Im Leistungsbereich der Versorgungsanstalt wird unter Verwendung des WHO-Schlüssels für Krankheitsursachen mit Hilfe einer Kennziffer die Ursache der Berufsunfähigkeit eines Leistungsempfängers personenbezogen gespeichert. Von der Versorgungsanstalt werden derartige Daten zu statistischen Zwecken benötigt. Aus ihnen ergeben sich Hinweise auf Maßnahmen, die zur dauerhaften Erfüllung des gesetzlichen Versorgungsauftrags notwendig und geeignet sind. Weil aber die **personenbezogene Speicherung der Ursachen** der Berufsunfähigkeit zu statistischen Zwecken nicht erforderlich ist, habe ich die anonymisierte Speicherung dieser Daten empfohlen. Die Bayer. Ärzteversorgung ist dieser Anregung gefolgt.

Kenntnisnahme ärztlicher Gutachten

Die Ärzteversorgung führt ihre Bearbeitungsunterlagen chronologisch fortlaufend ab Beginn der Mitgliedschaft des Versicherten. Dies gilt auch für die zur Feststellung der Leistungsvoraussetzung bei Berufsunfähigkeit erforderlichen ärztlichen Gutachten. Sie werden zusammen mit den übrigen Unterlagen in der Versichertenakte aufbewahrt und sind dann bei deren weiterer Bearbeitung jederzeit einsehbar. Obwohl medizinische Unterlagen regelmäßig nur zur Feststellung der Leistungsvoraussetzung bei einem Mitglied erforderlich sind, können auf diese Weise auch Arbeitsbereiche der Versorgungsanstalt Einblick in diese besonders sensiblen Unterlagen nehmen, die sie zu ihrer Aufgabenerfüllung (z.B. Beitragsberechnung) nicht benötigen.

Ich habe — wie schon bei der Bayerischen Rechtsanwaltsversorgung — angeregt, künftig die medizinischen Unterlagen vom übrigen Akteninhalt getrennt zu führen. Sie könnten dann beim Leistungsbereich der Versorgungsanstalt verbleiben, während sich die Akte z.B. in deren Beitragsbereich zur Bearbeitung befindet. Dadurch würde sichergestellt, daß nur die jeweils unmittelbar fachlich zuständigen Mitarbeiter Einblick in die ärztlichen Unterlagen nehmen können. Dies würde einer unbefugten Kenntnisnahme oder auch Offenbarung medizinischer Daten vorbeugen.

Die Ärzteversorgung ist inzwischen auch dieser Anregung gefolgt. Sie wird die medizinischen Unterlagen des Versicherten künftig getrennt vom Beitragsteil der Akte führen, der das Versicherungsverhältnis allein betrifft.

Datenspeicherung in der Mitglieder-Bestandskartei

Die Bayer. Ärzteversorgung unterhält seit ihrer Gründung im Jahre 1923 als Suchkartei eine manuelle Kartei mit Angaben zu allen früheren und jetzigen Mitgliedern und auch zu den Personen, deren Mitgliedschaft nicht zustande kam. Seit 1986 besteht neben dieser manuellen Mitgliederkartei eine automatisierte Suchdatei mit Angaben zum gleichen Personenkreis. Diese doppelte Dateiführung erscheint künftig nicht mehr erforderlich.

Aufgrund meiner Bedenken wird die Ärzteversorgung die manuelle Mitgliederkartei künftig nicht mehr fortführen. Es sollen lediglich noch die Karteiblätter mit Daten bis 1960 aufbewahrt werden. Die später erstellten Karteikarten werden nach Übertragung ihres Inhaltes in die automatisierte Datei vernichtet. Die früheren Karteiblätter werden noch zur Beantwortung in die Vergangenheit zurückreichender Versichertenanfragen benötigt.

Lesezugriff auf gespeicherte Mitgliederdaten

Die Erfassungsfunktionen (z.B. Änderungsberechtigung) des für die Bearbeitung der Mitgliederangelegenheiten eingesetzten Datenverarbeitungsverfahrens können nur von den dazu fachlich zuständigen Mitarbeitern genutzt werden. Dagegen haben die mit der Ärzteversorgung befaßten Mitarbeiter, denen ein Bildschirm zur Verfügung steht, teilweise die Möglichkeit eines **Lesezugriffs auf mehr Mitgliederda-**

ten als sie für die Aufgabenerfüllung benötigen. Die Ärzteversorgung hat bereits unmittelbar nach dieser Feststellung den Lesezugriff der Mitarbeiter an deren jeweilige fachliche Aufgabenstellung geknüpft und den Dateizugriff entsprechend technisch eingeschränkt.

21.2 Datenübermittlung an andere Versicherungsunternehmen durch den Bayerischen Versicherungsverband

Aufgrund einer Eingabe hatte ich mich mit der Frage zu befassen, inwieweit der Bayerische Versicherungsverband Daten von Schadensfällen aus einem früher bei ihm bestehenden Versicherungsverhältnis an ein anderes Versicherungsunternehmen auf dessen Wunsch übermitteln darf, wenn der Versicherungsnehmer dort ein neues Vertragsverhältnis begründen will. Der Bayerische Versicherungsverband ist eine von der Bayerischen Versicherungskammer verwaltete und vertretene öffentlich-rechtliche Anstalt. Er hat die Aufgabe die Schadens- und Unfallversicherung im Wettbewerb mit privaten Versicherungsunternehmen zu betreiben.

Die Mitteilung etwa der Art von Schäden, der Höhe der Aufwendungen für diese und des Zeitpunkts der Beendigung des Vorversicherungsverhältnisses an einen möglichen Nachversicherer ist zulässig, wenn der Versicherungsnehmer eingewilligt hat und der Umfang der Datenübermittlung den erforderlichen Rahmen nicht überschreitet.

Die Einwilligung des Betroffenen wird von den Versicherungsunternehmen, so auch vom Bayer. Versicherungsverband, regelmäßig gleichzeitig mit der Begründung eines Versicherungsverhältnisses eingeholt. Dies erfolgt unter Verwendung von Datenschutzklauseln im Formular, mit welchem der Abschluß eines Versicherungsvertrages begehrt wird. Die Datenschutzklausel hat dabei einen Hinweis auf den Zweck der Datenübermittlungen, z.B. Beurteilung des Risikos durch den anderen Versicherer, zu enthalten. Die im zu überprüfenden Fall vom Bayer. Versicherungsverband erfolgte Datenübermittlung entsprach der vom Betroffenen formularmäßig erteilten Einwilligung zur Datenübermittlung und war deshalb nicht zu beanstanden.

22. Technischer und organisatorischer Bereich

22.1 Grundsatzfragen

22.1.1 Verwendung von privater Hard- und Software

Die Datensicherheit beim Einsatz von Arbeitsplatzcomputern habe ich im 11. Tätigkeitsbericht ausführlich behandelt. Die dort geforderten Sicherheitsstandards finden allmählich Eingang in die Praxis. Probleme ergeben sich jedoch, wenn für dienstliche Zwecke private Hard- und Software eingesetzt werden soll.

In vielen Haushalten stehen heute Personal Computer (PC). Bereits für relativ wenig Geld gibt es dazu leistungsfähige Anwendungssoftware. Eine spezielle Sicherheitssoftware ist im privaten Bereich allerdings kaum anzutreffen, so daß beim Einsatz privater PC der Datenschutz sowie die Einhaltung der Grundsätze ordnungsgemäßer Datenverarbeitung, wie sie für dienstliche Belange erforderlich sind, nicht gewährleistet sind. Aber nicht nur wegen der **fehlenden Sicherheitskomponenten** ist von der Verwendung privater Hard- und Software für dienstliche Zwecke abzuraten, sondern auch wegen der dadurch entstehenden **Abhängigkeiten** von Arbeitsmitteln, über die der Dienstherr keine Verfügungsgewalt hat. Besonders bedenklich ist es, wenn der Arbeitsplatzcomputer alternierend betrieben wird, also sich einmal im Büro und das andere Mal in der häuslichen Umgebung befindet. Schließlich sind die Kontinuität der DV-Ausstattung und die Einhaltung einer vorgegebenen Programmlogik beim Einsatz privater Arbeitsplatzcomputer nicht gegeben. Auch die regelmäßige Datensicherung ist oft nicht gewährleistet, so daß bei Schadensfällen Daten verloren gehen können. Wegen der fehlenden softwaretechnischen Zugriffsschutzmaßnahmen ist eine **Datenmanipulation** durch Unbefugte leicht durchführbar, für den Befugten aber schwer, unter Umständen sogar überhaupt nicht erkennbar.

Der Einsatz privater Arbeitsplatzcomputer ist nur in besonders begründeten Einzelfällen zu gestatten. Beispielsweise dort, wo der Arbeitsplatzcomputer nur eine untergeordnete Stelle im Arbeitsablauf spielt, und keine Abhängigkeiten von der Verfügbarkeit dieses Mediums geschaffen werden.

Die Verwendung privater Software auf dienstlichen Geräten ist dem Dienstherrn häufig nicht bekannt. Mitunter handelt es sich bei dieser Software in vielen Fällen um sog. **Raubkopien** und nicht um Original-Software, der ein Lizenzvertrag zugrundeliegt. Bei der Verwendung von Raubkopien ist die Gefahr der Einschleusung von **Programmviren** nicht zu unterschätzen. Bei der Verwendung privater Software sind noch strengere Maßstäbe als beim Einsatz privater Hardware zu setzen. Der Einsatz privater Software ist generell zu verbieten. Er darf erst dann zugelassen werden, wenn dafür eine Freigabe durch einen qualifizierten Revisor oder durch den Benutzerservice vorliegt. Manche Dienstherren haben deshalb die Verwendung privater Hard- und Software für dienstliche Zwecke verboten.

So ist beispielsweise der Einsatz privater Hard- und Software bei der Verarbeitung von Daten, die dem Steuergeheimnis unterliegen, in der Finanzverwaltung untersagt, wenn die Verarbeitung mit einem „amtlich automatisierten" Verfahren vorgesehen ist. Der Einsatz privater automatischer Einrichtungen ist nicht bekannt.

Das Innenministerium hat in einem Rundschreiben an die nachgeordneten staatlichen Behörden festgestellt, daß die Verarbeitung personenbezogener dienstlicher Daten mit privater Hardware und der Einsatz privater Software zur Erledigung dienstlicher Aufgaben mit personenbezogenen Daten grundsätzlich nicht zulässig ist. Ausnahmen von diesem Verbot seien nur in wenigen Ausnahmefällen (z.B. bei Lehrern und Richtern) denkbar. Für den Bereich der Polizei galt schon bisher ein Verbot der dienstlichen Verwendung von privater Hard- und Software.

22.1.2 Computerviren

Im Berichtszeitraum wurden mir einige Fälle bekannt, in denen Computerviren in Arbeitsplatzcomputern bayerischer Behörden festgestellt wurden. Ursache der Infizierung waren meist das Einspielen raubkopierter Software, insbesondere von Spielprogrammen, und die Verwendung von frei zugänglicher Software, sogenannter PUBLIC-DOMAIN-Software.

Als Computervirus wird ein nicht eigenständiges Programm bezeichnet, das sich selbst vervielfältigen und in sogenannte Wirtsprogramme einnisten kann, um danach eine definierte, meist Schaden verursachende Funktion auszuführen.

Computerviren können die Sicherheit von Rechnern und Computernetzen erheblich gefährden und den ordnungsgemäßen Einsatz der Datenverarbeitung behindern, ja sogar lahmlegen. Zur Zeit sind ca. 250 Virusarten bekannt. PC-Viren sind zwar auf dem Großrechner wirkungslos, weil ein PC-Virus dort nicht ablauffähig ist. Das bedeutet jedoch nicht, daß es keine Viren gibt, die Großrechner befallen könnten. UNIX-Viren sind bisher nicht bekannt geworden.

Ein Computervirus besteht meist aus vier Programmblöcken mit unterschiedlichen Aufgaben: einem Vorspann mit Prüfroutine, einem Vervielfältigungsteil, einer Kennungsroutine und der schadensverursachenden Routine. Die wichtigsten Virustypen sind überschreibende, nicht überschreibende und speicherresistente Viren.

Woran erkennt man eine Infektion?

Wenn ein Arbeitsplatzcomputer plötzlich längere Lade- oder Verarbeitungszeiten benötigt oder nicht erklärbare Plattenzugriffe durchführt, wenn häufig Programmabstürze auftreten oder gar zu wenig Speicher für die Ausführung eines Programmes angezeigt wird, ist besondere Vorsicht geboten. Solche Anomalitäten können Anzeichen für einen Virenbefall sein. Ebenso kritisch sind der plötzlich und rapide abnehmende Speicherplatz auf der Festplatte sowie nicht mehr einwandfrei ablaufende Anwendungen und völlig neue und unbekannte Fehlermeldungen.

In diesen Fällen ist es geboten, unverzüglich selbst eine Virusanalyse durchzuführen oder einen Fachmann zu Rate zu ziehen. Tritt eine unbekannte Virusart auf, muß diese, damit sie wirksam bekämpft werden kann, zuerst analysiert werden. Dann ist ein Antivirus zu entwickeln.

Computerviren können beispielsweise durch folgende Sicherheitsmaßnahmen verhindert werden:

- kein Einsatz fremder, nicht geprüfter Software
- kein Einsatz von DEMO-Disketten und -Programmen
- kein Einsatz von Raubkopien jeglicher Art, insbesondere von Spielprogrammen
- keine Verwendung privater Hard- und Software
- kein Einsatz von PUBLIC-DOMAIN-Software
- Prüfung unbekannter Software oder Disketten auf einem speziellen Testgerät
- kein Programmaustausch über MAIL-Boxen ohne Einsatz geeigneter Überprüfungsmechanismen
- Anlegen von Sicherheitskopien für Programme und Daten
- regelmäßige Überprüfung aller Sicherungskopien auf Virenbefall
- Einsatz eines Virensuchprogrammes bei der Überprüfung von Disketten sowie von Programmen und Dateien, die über Modem und Netzwerk geladen werden
- keine Speicherung der Programme im Quellcode
- keine Installation von Compilern, soweit das im Produktionsbetrieb möglich ist
- Umbenennung ausführbarer Programme (COM, EXE, BAT), damit ein Virus diese nicht auffinden und infizieren kann
- regelmäßige Schulung der Anwender und Einrichtung eines Benutzerservice

Einige Software-Hersteller bieten heute Schutz- und Analyseprogramme an, die vor Virenbefall schützen und die Ausbreitung des Virus im System verhindern sollen, d.h. gegen Virenbefall vor und nach einem Virenbefall nachsorgen. Ein Virenschutzprogramm muß

- die gängigsten Viren an ihrer Signatur erkennen,
- vor der Installation den Speicher des Rechners einschließlich Boot-Sektor nach Virensignaturen überprüfen,
- als resistentes Programm den Speicher überwachen,
- alle Programme, die über Diskette, Modem und Netzwerk geladen werden, überprüfen sowie
- bei der Prüfung ein manipulationssicheres Verfahren wählen.

Schließlich sollte ein Virusschutzprogramm lernfähig sein und neue Viren erkennen, sei es durch Mutation bereits bekannter Viren oder durch Editieren neuer Virusstämme.

Wenn bemerkt wird, daß ein Computer von einem Virus befallen ist, sind unverzüglich folgende Maßnahmen einzuleiten:

- Gerät unverzüglich ausschalten und alle Kommunikationsmöglichkeiten unterbrechen
- Bei Arbeitsplatzcomputern, die mit einer Batteriepufferung arbeiten, sind die Batterien abzuklemmen und der Computer solange außer Betrieb zu setzen, bis von einer vollständigen Löschung aller Informationen ausgegangen werden kann. Meist genügen dazu zwei Tage
- Arbeitsplatzcomputer mit einer schreibgeschützten, unverseuchten Diskette mit dem Originalbetriebssystem neu starten
- Neuformatierung der Festplatte bzw. aller betroffenen Datenträger
- Neuinstallation der Anwendersoftware aus dem Backup
- Die Datendateien sind aus den Sicherungen zu überspielen. Da Virusprogramme nur ausführbare Programme infizieren, können Datendateien von bereits verseuchten Datenträgern übernommen werden. Deshalb sind auch die Datendateien von einem Virus-Suchprogramm auf Virenbefall zu untersuchen
- Die als infiziert erkannten Programme sind zur Beweissicherung zu sichern und keinesfalls zu vernichten
- Nach der Wiederinbetriebnahme ist erhöhte Wachsamkeit geboten.

22.1.3 Entsorgung von Datenträgern

Früher wurde vielfach die Meinung vertreten, daß mit zunehmender Automatisierung der Datenträger „Papier" an Bedeutung verlieren würde. Bisher ist eher das Gegenteil der Fall. Das papierlose Büro scheint noch in weiter Ferne zu liegen. Oft ist Papier auch nur ein kurzlebiger, temporärer Datenträger. Da jeder diesen Datenträger ohne Zuhilfenahme technischer Geräte verstehen kann, ist bei der Entsorgung nicht mehr benötigter Papierunterlagen, die personenbezogene Daten enthalten, besonders darauf zu achten, daß die Anforderungen nach Art. 15 Bayer. Datenschutzgesetz beachtet werden.

Im Berichtszeitraum mußte ich immer wieder feststellen, daß manche Behörden bei der Entsorgung von Altpapier und sonstigen Unterlagen, die personenbezogene Daten enthalten, nicht mit der gebotenen Sorgfalt und Umsicht vorgehen. Aus diesem Grunde habe ich die obersten Dienstbehörden gebeten, in ihrem Zuständigkeitsbereich die Art und Weise der gegenwärtigen Entsorgung zu überprüfen. Dabei sollte beispielsweise der Weg des Entsorgungsmaterials vom Papierkorb bis zur endgültigen Vernichtung in einer Papier-

mühle lückenlos untersucht werden. Es genügt nicht, den Weg nur bis zum Altpapierhändler zu verfolgen.

Neben dem Datenschutz sollte im Hinblick auf das neue Abfallwirtschaftsgesetz auch Wert auf den Umweltschutz gelegt werden. Beide hochrangigen Anliegen lassen sich miteinander in Einklang bringen.

Bei der Entsorgung von Altpapier, dazu gehört täglich anfallendes Papier ebenso wie ausgesondertes Aktengut, sind insbesondere folgende Grundsätze zu beachten, auf die ich die Verwaltung hingewiesen habe:

- Soweit kein geeigneter Reißwolf vorhanden ist, sollte Altpapier grundsätzlich Spezialentsorgungsunternehmen überlassen werden, die eine datenschutzgerechte Entsorgung „vom Papierkorb bis zur Papiermühle" gewährleisten. Dazu gehört auch, daß Unbefugte auf diesem Weg keinen Zugriff erlangen. In einem solchen Fall kann von maschineller Zerkleinerung und Unkenntlichmachen im allgemeinen abgesehen werden.

  Durch regelmäßige Stichproben sollte kontrolliert werden, ob sich das beauftragte Unternehmen an die Auflagen hält.

- Bei der Abgabe an Altpapierhändler ist besonders sorgfältig zu prüfen, ob diese die Gewähr dafür bieten, daß Unbefugte keinen Zugriff auf die abgelieferten Materialien erhalten. In der Regel ist das Entsorgungsgut vor der Abgabe an den Händler mit Hilfe eines Reißwolfs zu zerkleinern oder sonst unleserlich zu machen.

- Soweit Altpapier nur über Müllbehälter entsorgt werden kann, ist es zum Schutz vor unbefugtem Zugriff vorher zu zerkleinern oder sonst unleserlich zu machen.

- Im übrigen ist bei der Beschaffung von Reißwölfen die DIN 32757 zu beachten.

22.1.4 Zusammenarbeit mit anderen Kontrollorganen

Der Bundesrechnungshof hat in der Bundestagsdrucksache 11/7691 vom 28.8.1990 über die Sicherheit der Informationsverarbeitung in Rechenzentren der Bundesverwaltung berichtet.

Er stellt dabei grundsätzlich fest: „Der Sicherheit der Informationsverarbeitung, insbesondere in kassenwirksamen, sicherheitsempfindlichen und sonstigen sensiblen Bereichen, kommt eine herausragende Bedeutung zu. Die Datenverarbeitungsanlagen müssen technisch verfügbar und gegen Ausfall gesichert, die Vertraulichkeit der Daten sowie die Richtigkeit und Unversehrtheit der Daten und Programme müssen gewährleistet sein. Sicherheitsmaßnahmen kosten im allgemeinen Geld. Nicht ausreichende Sicherheitsmaßnahmen können aber zu Schäden führen, deren finanzielle und sonstige Auswirkungen den Sicherheitsaufwand bei weitem übersteigen."

Diese Forderungen sind aus der Sicht des Datenschutzes und der Datensicherheit nachhaltig zu unterstreichen. Für die Prüfung der Sicherheit von Rechenzentren hat meine Geschäftsstelle in den letzten Jahren einen umfangreichen Erhebungskatalog entwickelt. Zur Gesamtbeurteilung der Sicherheit der automatisierten Datenverarbeitung werden sowohl die Organisation des Rechenzentrums, die Programmierung, die Verfahrensdokumentation und das Dateisicherungskonzept als auch bauliche Maßnahmen und Brandschutzmaßnahmen in Rechenzentren sowie Maßnahmen zur Katastrophenvorsorge und Notfallmaßnahmen in die Prüfung mit einbezogen. Das Fehlen geeigneter Sicherheitsmaßnahmen in diesen Bereichen hatte der Bundesrechnungshof in dem oben erwähnten Bericht bemängelt.

Auch im Interesse der Betreiber von Rechenzentren halte ich es für unerläßlich, daß die Kontrollorgane bei ihren Forderungen in diesen originären Sicherheitsfragen am gleichen Strang ziehen. Die Unabhängigkeit der Kontrollorgane sehe ich dadurch nicht beeinträchtigt. Mit dem Bayerischen Landesprüfungsamt für Sozialversicherung pflege ich in dieser Beziehung seit Jahren einen Erfahrungsaustausch. Daß ich mit meinen Forderungen an die Datensicherheit auch mit der Aufsichtsbehörde für den nichtöffentlichen Bereich in Bayern übereinstimme, zeigt die Bemerkung des TÜV Bayern, der für die Aufsichtsbehörde im technischen Bereich tätig wird, über die festgestellten Sicherheitsmaßnahmen anläßlich einer Prüfung in Nürnberg. „Das vorgefundene Sicherungssystem ist dadurch gekennzeichnet, daß bei ..... der Schutz und die Sicherung der zu verarbeitenden personenbezogenen Daten eine besondere Bedeutung und einen hervorragenden Stellenwert besitzen."

Auf meine Anfrage zu einer verstärkten Zusammenarbeit zwischen Rechnungsprüfung und Datenschutz wurde mir vom Bayer. Obersten Rechnungshof mitgeteilt, daß eine generelle Abstimmung der Tätigkeiten und eine Arbeitsteilung rechtlich zwar nicht möglich sein dürfte, ein Gedanken- und Erfahrungsaustausch zum Thema „Datensicherheit in Rechenzentren, beim Einsatz von Personal Computern und bei Dialogverarbeitung" auf Referentenebene aber durchaus zu begrüßen ist.

22.1.5 Risiken und Maßnahmen bei Inanspruchnahme von DV-Dienstleistungen

Die Bedeutung der DV-Dienstleistung in Form der Auftragsdatenverarbeitung außer Haus hat zwar mit zunehmender Dezentralisierung der Datenverarbeitung abgenommen, dennoch nehmen immer wieder datenverarbeitende Stellen Service-Leistungen von privaten Dritten in Anspruch. Eine DV-Dienstleistung kann eine Auftragsdatenverarbeitung sein, kann aber auch Hardware-Leasing und Software-Miete bedeuten. In allen Fällen aber gerät der Auftraggeber in ein Abhängigkeitsverhältnis, das er durch geeignete Maßnahmen absichern sollte.

Große Schwierigkeiten können beispielsweise dann auftreten, wenn das Service-Unternehmen in Konkurs geht und Hard- und Software in die Konkursmasse einfließen. Auf diese Weise können Kundendaten, die sich auf den Datenträgern befinden, in unbefugte Hände geraten. In einem derartigen Fall, der bei einer Reihe von speichernden Stellen in einem anderen Bundesland aufgetreten ist, wurden Eigentumsansprüche Dritter an gemieteter Hardware geltend gemacht, weil der Vermieter selbst nicht Eigentümer der Hardware und seinen Verpflichtungen gegenüber seinen Schuldnern nicht nachgekommen war. Werden die Daten auf den Festplatten nicht gelöscht, gelangen sie ebenfalls in unbefugte Hände. Der Arbeitskreis „Technische und organisatorische Datenschutzfragen" der Datenschutzbeauftragten des Bundes und der Länder hat sich mit dieser Problematik beschäftigt und eine Orientierungshilfe zusammengestellt. Die Orientierungshilfe beschreibt ausführlich Notfälle, in die eine speichernde Stelle geraten kann, und schlägt Maßnahmen zum Schutze gegen solche Ereignisse vor. Die Orientie-

rungshilfe kann bei meiner Geschäftsstelle angefordert werden.

22.1.6 Sicherheit in der Informationstechnik

Die Erhöhung der Sicherheit in der Informationstechnik beschäftigt seit Jahren viele einschlägige Fachgremien. Der Deutsche Bundestag hat am 24.10.1990 ein Gesetz über die Errichtung des Bundesamtes für die Sicherheit in der Informationstechnik (BSIG) verabschiedet. Damit wurde den seit Jahren bestehenden Forderungen, eine zentrale Stelle zu schaffen, die Sicherheitsstandards definiert und vor allem Systeme (Hard- und Software) bewertet, Rechnung getragen. Die Zentralstelle für die Sicherheit in der Informationstechnik (ZSI) wird deshalb am 1.1.1991 in das neue Bundesamt für Sicherheit in der Informationstechnik (BSI) übergehen.

Die Aufgaben dieses Amtes sind gesetzlich vorgeschrieben. Für den Bereich der Computersicherheit sind dies u.a.:

- Erstellen und Aktualisieren spezifischer Bedrohungsmodelle, Aufdecken von Schwächen in IT-Systemen, Untersuchung von Angriffsmethoden, Analyse konkreter Manipulationsfälle
- Definition der Kriterien bzw. Standards für die vergleichende Bewertung der Sicherheitseigenschaften von Systemen
- Forschung und Entwicklung im Bereich „sichere IT-Systeme und -Komponenten" in Zusammenarbeit mit Hochschulen und Industrie
- Prüfen und Bewerten von Systemen und Produkten (Hard- und Software) im Hinblick auf deren Sicherheitseigenschaften (Evaluierung und Zertifizierung), Aufbau der Evaluierungsmethodik und -werkzeuge.

Bereits 1990 wurden von der ZSI nach den nationalen IT-Sicherheitskriterien das Mehrplatz-Betriebssystem SINIX-S Version 5.22 der Siemens AG und das PC-Sicherheitswerkzeug Safe guard professional Version 3.1.Z der utimaco Software geprüft und bewertet. In den folgenden Jahren sollen weitere DV-Systeme geprüft werden. Auf lange Sicht ist also mit einer spürbaren Verbesserung der Sicherheit in der Informationstechnik zu rechnen.

22.2 Prüfungstätigkeit

22.2.1 Kontrolle und Beratung

Im Berichtszeitraum habe ich bei folgenden Stellen die Einhaltung der technischen und organisatorischen Maßnahmen zur Datensicherung überprüft:

- Rechenzentrum für Planung und Umwelt
- Rechenzentrum der Bayer. Ärzteversorgung in der Bayer. Versicherungskammer
- Rechenstelle des Bezirks Oberbayern (Bezirkskrankenhaus Haar)
- Rechenstelle der Betriebskrankenkasse der Bayer. Staatsbauverwaltung
- Stadtverwaltung Rosenheim
- Landratsamt Neustadt an der Aisch
- Polizeiinspektion Nabburg
- Betriebskrankenkasse Krones
- Datenverarbeitung im Finanzamt München I
- Kreiskrankenhaus Starnberg
- Maschinelle Datenverarbeitung beim Landgericht Kempten
- Datenverarbeitung der Bayer. Landeszentrale für Neue Medien
- Maschinelle Datenverarbeitung im Forstamt München
- Maschinelle Datenverarbeitung bei zwei Gymnasien und einer Hauptschule

Darüber hinaus wurde die Datenträgerentsorgung bei insgesamt 14 speichernden Stellen im Großraum München geprüft. Im Universitätsbereich wurde das Zeiterfassungssystem für die Bediensteten der Friedrich-Alexander-Universität Erlangen-Nürnberg untersucht. Um die Sicherheit der maschinellen und manuellen Datenverarbeitung zu erhöhen, habe ich auch im Berichtszeitraum wieder eine Reihe von bayerischen Behörden beraten. So wurden Sicherheitsberatungen bei Landratsämtern, Städten und Gemeinden, Allgemeinen Ortskrankenkassen, im Justiz- und Klinikbereich sowie bei fünf Fachrechenzentren durchgeführt.

Regelmäßige Kontakte zu den Herstellern von Hard- und Software im Großrechner- wie im PC-Bereich sind für die Entwicklung von geeigneten Vorschlägen für Sicherheitsmaßnahmen wichtig. Die Kontakte zu diesen Stellen wurden weiter ausgebaut. Die Reihe der Orientierungshilfen für Datensicherungsmaßnahmen beim Einsatz mittlerer DV-Systeme wurde um eine Anleitung für die IBM AS/400 fortgesetzt. Den UNIX-Systemen werden bei den zukünftigen Abteilungsrechnern die größten Chancen eingeräumt. Aus diesem Grunde wird in den nächsten Jahren diesem Anlagentyp noch stärkeres Augenmerk gewidmet.

Auf Anfrage stelle ich Orientierungshilfen für Datensicherungsmaßnahmen beim Einsatz von Anlagen des Typs Hewlett Packard 3000, Mannesmann-Kienzle 9000, NCR ITX 10.000, Wang VS 100, Siemens MX300/MX500 und IBM AS/400 kostenlos zur Verfügung.

22.2.2 Ergebnisse der Kontrolltätigkeit

Auch bei den Kontrollen im Berichtszeitraum war festzustellen, daß die vorgefundenen Maßnahmen zur Datensicherung unterschiedliche Qualität erkennen ließen. Erfreulich ist, daß bei vielen Stellen der Datenschutz und die Datensicherheit ernst genommen werden und einen hohen Stellenwert besitzen, so daß keine oder nur geringfügige Lücken im Sicherheitssystem festzustellen waren. Infolge der zunehmenden Komplexität der Datenverarbeitung — neben Großrechnern gibt es eine Vielzahl von kleineren und mittleren DV-Anlagen, die auch noch untereinander vernetzt werden können — werden auch die Anforderungen an die Datensicherheit vielfältiger. Oft tritt der Fall ein, daß einzelne Maßnahmen einfach vergessen werden oder durch die Lücken im Sicherheitssystem nicht voll zur Geltung kommen.

Dazu einige Beispiele:

- Ein ausgefeiltes Zugriffssicherungssystem verliert an Wirkung, wenn nicht belegbar ist, seit wann und durch wen veranlaßt ein Benutzer Zugriff auf welche Verfahren und Datenbestände hat.
- Die Zugangssicherung mit Panzerglasscheiben im Rechenzentrum verfehlt ihre hervorragende Schutzwirkung, wenn die Fenster zu öffnen und keine Kontrollmaßnah-

men vorgesehen sind, die ein offenstehendes Fenster anzeigen.

- Ein Zugangssicherungssystem ist wirkungslos, wenn beim unberechtigten Zugang der entstehende Alarm an eine Stelle weitergeleitet wird, die nicht besetzt ist.

- Brandschutzmaßnahmen in Form einer Sprinkleranlage im Rechenzentrum können bei einem lokalen Brand durch austretendes Wasser einen größeren Schaden verursachen als das Primärereignis.

Die Abhängigkeit von der Funktionsfähigkeit der automatisierten Datenverarbeitung wird immer größer. Um so dringlicher ist es, daß man sich Gedanken darüber macht, welche Arbeiten nach einem Katastrophenfall nach welcher Zeit, unter welchen Bedingungen und vor allem an welchem Ort wieder anlaufen können. Erfreuliche Ansätze für Notfallmaßnahmen sind im staatlichen Bereich festzustellen. Es gibt Rechenzentren, welche die Auslagerung der Datenverarbeitung in ein anderes Rechenzentrum regelmäßig üben und ein Notfallrechenzentrum unterhalten. Ein Schreibtischtest allein genügt nicht. Zuverlässige Erkenntnisse über die Wirksamkeit der Maßnahmen sind nur im Echteinsatz zu erfahren.

Ein Universitätsrechenzentrum hat beispielsweise die vorbereitenden Maßnahmen für ein Backup-Konzept in Form der Erstellung eines Katastrophenverzeichnisses beispielhaft gelöst. Das Katastrophenhandbuch befaßt sich mit folgenden Problemkreisen:
- Beschreibung der Datensicherung
- Forderungen für ein Ausweichrechenzentrum (Software, Peripherie, Datenfernverarbeitung)
- Beschreibung der Anwendungssysteme
- Datenrestauration bei Ausfall einzelner Platten (mit Hinweisen auf die Anwendungssysteme)
- Übernahme der Verarbeitung in ein Ausweichrechenzentrum.

Diese Arbeiten sind die Grundvoraussetzung für einen späteren einwandfrei funktionierenden Wiederanlauf. Außerdem ist festzulegen, welche Ausfallzeiten die einzelnen Anwendungssysteme verkraften können und nach welcher Zeit welche Verfahren in welcher Ausbaustufe verfügbar sein müssen. Die Frage eines geeigneten Ausweichrechenzentrums ist in dem oben geschilderten Falle allerdings aus finanziellen Gründen noch ungeklärt, so daß man für den Ernstfall derzeit trotzdem nicht gerüstet ist.

Bei der Kontrolle der **Datenträgerentsorgung**, insbesondere von Papierunterlagen wurden in Einzelfällen erhebliche Mängel festgestellt. Leider entsorgen manche Behörden ihre Papierabfälle immer noch über den Hausmüll. Sind die Mülltonnen für jedermann von der Straße zugänglich, so ist es nur eine Frage der Zeit, daß sensible Unterlagen Unbefugten in die Hände fallen. Auf die Grundsätze unter 22.1.3 nehme ich Bezug.

Hilflos scheinen manche Behörden bei Archivaussonderungen zu sein. Keinesfalls darf das Papiergut unzerkleinert an einen Altpapierhändler abgegeben werden. Je nach Sensibilität der Daten ist die erforderliche Vernichtungsstufe nach DIN 32757 einzuhalten. Es gibt jedoch, wenn auch nicht zum Nulltarif, eine Reihe von datenschutzgerechten Entsorgungsmethoden, um auch dieses Problem zukünftig in den Griff zu bekommen. So hat das Staatsministerium der Finanzen in der Neufassung der Aufbewahrungsbestimmungen für Schriftgut der Finanzämter Hinweise für eine datenschutzgerechte Entsorgung von auszusondernden Unterlagen aufgenommen.

Schließlich ist mir bei der Prüfung von DV-Verfahren, insbesondere wenn sie auf DV-Anlagen mittlerer Größe oder auf Arbeitsplatzrechnern zum Einsatz kommen, aufgefallen, daß die für eine ordnungsgemäße Durchführung der Datenverarbeitung erforderliche Dokumentation fehlte. Es genügt nicht, wenn lediglich Programmlisten vorhanden sind. Die Dokumentation muß zumindest eine kurze Programmbeschreibung, Angaben über den aktuellen Versionsstand, die Programmhistorie, einen Datenflußplan und eine Bedienungsanleitung umfassen.

Beim Einsatz von Arbeitsplatzcomputern wird außerdem zu wenig darauf geachtet, daß Programme und Daten zusammen mit der Hardware durch ein- und dasselbe Schadensereignis zerstört werden können. Wichtig ist deshalb, daß Daten und Programme regelmäßig gesichert und Sicherungsbestände in einem Tresor, der sich in einem anderen Raum befindet, aufbewahrt werden. In einem Fall, bei dem ein Personal Computer gestohlen wurde, war seit Monaten keine Datensicherung mehr durchgeführt worden. Die Wiederherstellung von Daten und Programmen kann dann sehr kosten- und zeitaufwendig sein. Personenbezogene Dateien befanden sich aber nicht auf dem PC.

22.3 Technische Einzelprobleme

22.3.1 Sicherheit von Paßworten

Sowohl in der Groß-EDV als auch beim Einsatz von Arbeitsplatzcomputern ist die Verwendung von persönlichen Kennwörtern (Paßworten) eine unverzichtbare Zugriffsschutzmaßnahme. Die Prüfungen vor Ort haben gezeigt, daß in nahezu allen Fällen zwar Paßworte verwendet wurden, aber nicht überall die gebotene Sorgfalt bei der Sicherheit der Paßworte beachtet wurde. Noch immer gibt es Verfahren und DV-Installationen, bei denen der Systemverwalter selbst das Paßwort eines Benutzers verwalten muß; der Benutzer besitzt also keine Möglichkeit, sein persönliches Kennwort selbst zu vergeben. Ein solches Verfahren entspricht nicht dem Stand der Technik. Da das Paßwort nur dem Benutzer selbst bekannt sein sollte, darf es der Systemverwalter auch nicht aus dem Speicher auslesen können. Aus diesem Grunde speichern moderne Systeme Paßworte einwegverschlüsselt ab.

Es ist ferner darauf zu achten, daß nach der Installation die standardmäßig eingerichteten Kennungen durch individuelle Paßworte geschützt werden. Häufig habe ich bei Prüfungen noch die vom Hersteller vergebenen Installationspaßworte vorgefunden. Solche allgemein bekannten Paßworte bieten keinen Schutz.

Bei der Verwendung von Paßworten sind folgende Sicherheitsgrundsätze zu beachten:

- Alle Benutzerkennungen sind mit einem Paßwort zu schützen.

- Es ist sicherzustellen, daß die Paßworte nur dem Benutzer bzw. einem begrenzten Personenkreis bekannt sind und bleiben.

- Bei der Vergabe der Paßworte ist die maximale Länge und der gesamte verfügbare Zeichenvorrat auszuschöpfen. Als Mindestlänge werden 6 Stellen empfohlen.
- Paßworte sind so zu wählen, daß kein Bezug auf den Paßwortinhaber oder seine Umgebung sowie zu echten Benutzern entsteht. Trivialpaßworte sind systemseitig abzufangen.
- Paßworte dürfen nicht auf programmierbare Tasten gelegt werden.
- Paßworte sind häufig und in unregelmäßigen Abständen zu ändern. Das System muß erkennen, ob sich das neue Paßwort vom alten unterscheidet.

Häufig ist die Ansicht verbreitet, würde man einwegverschlüsselte Paßworte vergessen, so bedeutete dies den Verlust von Daten und Programmen, die mit diesem Paßwort geschützt werden. Diese Meinung ist selbstverständlich falsch. Der Systemverantwortliche kann nämlich dem Benutzer den Zugang zu Programmen und Daten wieder eröffnen, indem er das alte Paßwort löscht und ein neues vergibt, mit dem der Benutzer wieder auf seine Programme und Daten zugreifen kann. Sofern es das Paßwortsystem zuläßt, sollte das vom Systemverwalter vorgegebene Paßwort allerdings nur zum einmaligen Gebrauch zugelassen sein und danach seine Gültigkeit verlieren. Beim ersten Anmeldevorgang hat der Benutzer deshalb unverzüglich das vorgegebene Paßwort zu ändern und sein eigenes persönliches Kennwort einzugeben, von dem kein anderer Kenntnis hat.

Bei Paßwortverstößen sind folgende Sicherheitsmaßnahmen vorzusehen:

- Nach einer bestimmten Anzahl von Fehleingaben, in der Regel nach drei aufeinander folgenden Versuchen, sind der Dialog abzubrechen und die Benutzerkennung, die Leitung oder das Datenendgerät zu sperren.
- Fehlversuche sind in den Ablaufinformationen so aufzuzeichnen, daß auch die ungültigen Eingabewerte gespeichert werden, um auf diese Weise den Täter entlarven zu können. Dazu ist eine regelmäßige Auswertung der Protokollaufzeichnungen erforderlich. Sie sollte von den Herstellern durch die Bereitstellung von entsprechenden AUDIT-Programmen unterstützt werden.
- Um die Einhaltung der vorgegebenen Paßwortregeln zu überprüfen, sind geeignete organisatorische oder technische Maßnahmen zu ergreifen.

22.3.2 Versand

Im Berichtszeitraum haben einige Petenten darüber geklagt, daß Behörden Unterlagen mit sensiblem Inhalt (Sozialdaten, medizinische Daten) in einem offenen Umschlag versenden. Oft handelte es sich um vertrauliche Mitteilungen, die, werden sie anderen offenbart, schutzwürdige Belange des Betroffenen beeinträchtigen können.

Die Behörden wurden in allen Fällen auf die Einhaltung der gebotenen Sicherheitsmaßnahmen hingewiesen: der Versand von personenbezogenen Unterlagen in einem offenen Umschlag ist zu unterlassen. Sofern die Voraussetzungen auf Seiten der Post erfüllt sind, können diese Schreiben allerdings als **Briefdrucksache** bzw. als Drucksache (ab 100 Sendungen) in einem verschlossenen Umschlag versendet werden. Bei der Einlieferung muß der Absender ein Inhaltsmuster vorlegen. Anhand von Stichproben prüft der Schalterbeamte, der die Poststücke entgegennimmt, ob der Inhalt mit dem Muster übereinstimmt. Die Prüfung erfolgt bei der Einlieferung und im Beisein des Einlieferers, der die gegebenenfalls geöffneten Sendungen zur Neukuvertierung wieder mitnimmt. Andere bei der Beförderung beteiligte Postbeamte öffnen eine Briefdrucksache nicht mehr. Da die überprüften und geöffneten Poststücke stets an den Absender zur Neukuvertierung zurückgehen, findet der Empfänger bei dieser Versandart immer eine verschlossene Sendung vor, die sich äußerlich nicht vom Brief unterscheidet.

Unter diesen Bedingungen kann dem Versand von Unterlagen mit sensiblem Inhalt auch als Briefdrucksache oder Drucksache zugestimmt werden, wenn die Schreiben in jedem Fall in einem verschlossenen Umschlag befördert und zugestellt werden.

22.3.3 Betrieb von Kommunikationsanlagen

Moderne Telekommunikationsanlagen (TK-Anlagen) sind hinsichtlich ihrer Leistungsfähigkeit und Komplexität nicht mehr mit den Nebenstellenanlagen früherer Zeiten vergleichbar. Zwar ist die Sprachkommunikation immer noch die wichtigste Komponente, die Nutzungsmöglichkeiten solcher Anlagen sind jedoch vielfältiger geworden. Die TK-Anlagen besitzen einen Speicher, in dem personenbezogene Daten, meist für Abrechnungszwecke, gesammelt werden können. Außerdem ist es möglich, den einzelnen Nebenstellen und infolgedessen den Benutzern unterschiedliche Rechte einzuräumen. Für die Verwaltung der Benutzerrechte sind ebenfalls DV-Komponenten erforderlich.

Da der Betrieb von TK-Anlagen meist bei der Abteilung „Allgemeine Verwaltung" angesiedelt ist, fehlt es häufig an geeignetem Personal mit EDV-Wissen. DV-Kenntnisse sind aber notwendig, wenn man eine TK-Anlage einrichten und verwalten will. Nicht selten kommt es vor, daß auf Betreiberseite Unkenntnis darüber herrscht, welche Nebenstelle einer ISDN-fähigen TK-Anlage über welche Leistungsmerkmale verfügt, weil der Betreiber die Einrichtung und die laufende Verwaltung dem Hersteller überläßt. Auf diese Weise können auch Abrechnungsdaten in die Hände von Amtsfremden gelangen.

Dieses Risiko ist zu vermeiden, wenn der Anwender selbst einen Systemverwalter ausbildet, der die TK-Anlage betreuen kann. Dazu sollte jede größere Behörde imstande sein. Für die Einrichtung der Benutzerrechte muß eine Aufstellung als Dokumentation vorhanden sein, aus der hervorgeht, welche Nebenstellen für welche Leistungsmerkmale berechtigt sind. Das Verwalten und Bearbeiten der Nutzungsdaten gehört ebenfalls zum Aufgabenbereich des Systemverwalters.

Wie jede andere DV-Anlage muß auch die TK-Anlage von Zeit zu Zeit gewartet werden. Die Wartung kann sowohl vom Anwender als auch vom Hersteller durchgeführt werden. Ein Zugriff auf Abrechnungsdaten ist dafür nicht notwendig. Die Wartungsprivilegien können vom Betreiber so eingerichtet werden, daß der Wartungstechniker ausschließlich auf die für die Wartung relevanten Statusinformationen (Diagnosedateien) zugreifen kann. Die Abrechnungsdaten sind durch ein spezielles Paßwort zu schützen. Für die Wartung einer TK-Anlage ist die Systemverwalterberechtigung nicht erforderlich. Selbstverständlich muß der Systemverwalter die Sy-

stemverwalterberechtigung ebenfalls mit einem Paßwort schützen.

Die Hersteller haben für Wartungszwecke meist Fernwartungszentren eingerichtet, die über Telefonleitung die TK-Anlage ihrer Kunden betreuen. Die Leitung, über welche die TK-Anlage angewählt wird, ist meist eine Wählleitung, die jedoch durch vielfältige Maßnahmen zu schützen ist, so daß ein Zugriff Unbefugter weitgehend ausgeschlossen werden kann.

- Die Verwendung von unterschiedlichen Paßworten für den Systembetreuer und den Wartungstechniker ist zwingend erforderlich. Außerdem ist die Benutzerkennung zu sperren, wenn mehrmals aufeinanderfolgend falsche Paßworte festgestellt werden.
- Stellt die TK-Anlage ein gültiges Paßwort fest, muß eine spezielle Verständigungsprozedur ablaufen, die nur dem Berechtigten bekannt ist.
- Stellt die TK-Anlage die Identität und die Berechtigung des Anrufenden fest, unterbricht sie die Verbindung und wählt die Wartungszentrale von sich aus automatisch an (Rückruf).

Die Wartung selbst hat nur Zugriff auf Diagnosedateien. Eine Veränderung von Software ist in der Regel ausgeschlossen, weil die Fernwartung nur über eine Leseberechtigung verfügt. Änderungen in der Betriebssoftware werden vor Ort ausschließlich unter der Kontrolle des Betreibers durchgeführt.

Bei Beachtung dieser Sicherheitsmaßnahmen ist ein ordnungsgemäßer Betrieb in einer ISDN-fähigen TK-Anlage durch den Betreiber sichergestellt.

22.3.4 Datensicherheit bei der Datenübertragung

Mit der Abhöranfälligkeit von Datenleitungen und der Verwertbarkeit der kompromittierenden Abstrahlung von Bildschirmen, Leitungen und sonstigen DV-Komponenten, bei denen elektrische Ladung bewegt wird, beschäftigen sich die einschlägigen Fachgremien immer wieder von Neuem. Oft wird durch übertriebene Schwarzmalerei der technische Laie verunsichert. Auch auf diesem Gebiet ist zwischen dem technisch Möglichen und der Wirklichkeit wie in vielen anderen Lebensbereichen ein großer Unterschied. In den Vereinigten Staaten von Amerika hat das National Center of Computer Crime Data (NCCCD) Mitte 1990 eine Statistik über die Ursachen von Datenverlusten und -manipulationen veröffentlicht. Mit einem Anteil von lediglich 4% liegen die Ursachen Hacking, Abhören und Computerviren unverändert am Ende der Skala, genauso wie nach einer Untersuchung aus dem Jahre 1985.

Das bedeutet aber nicht, daß man diese Gefahren vermeidlichen oder ganz außer acht lassen sollte. Die Virenproblematik ist, wie oben gezeigt wurde, durch technische und organisatorische Maßnahmen in den Griff zu bekommen. Das Eindringen in Computersysteme durch sogenanntes Hakking läßt sich durch eine Vielzahl von Sicherheitsmaßnahmen weitgehend unterbinden. In früheren Tätigkeitsberichten habe ich darüber ausführlich berichtet.

An der Verminderung der kompromittierenden Abstrahlung wird ständig gearbeitet. Es gibt heute bereits Bildschirme, die so wenig abstrahlen, daß die noch auftretende kompromittierende Abstrahlung mit den derzeit bekannten Methoden nicht mehr verwertbar ist.

Was bleibt, ist vor allem das Risiko, daß die Datenübertragungsstrecken abgehört werden. Große Verunsicherung herrschte, als im Jahr 1990 in der Öffentlichkeit bekannt wurde, daß fremde Geheimdienste regelmäßig und in manchen Gebieten vollständig den Fernsprechverkehr abgehört haben. Neben meist erdgebundenen Kabeln (Kupferkabel oder Lichtwellenleiter) werden für die Datenübertragung auch Richtfunkstrecken verwendet. Auf diese Weise erhöht sich das Abhörrisiko um ein Vielfaches. Selbst, wenn der Benutzer eine sogenannte stehende Leitung (HfD) gemietet hat, ist nicht ausgeschlossen, daß die Datenübertragung in manchen Fällen über eine Richtfunkstrecke erfolgt. Bei Verwendung von Datex-P treten dieselben Risiken auf. Der Anwender hat grundsätzlich keinen Einfluß über die Art des Transportweges.

Der Anwender kann sich nur insoweit gegen das Abhören schützen, als er die auf die Leitung geschickten Daten verschlüsselt. Die sogenannte **Leitungsverschlüsselung** gewinnt in der automatisierten Datenverarbeitung zunehmend an Bedeutung. Mit einem Transaktionssicherungssystem (TSS) bietet ein großer DV-Hersteller seit 1990 ein System an, das mit modernsten Sicherheits- und Verschlüsselungsmethoden arbeitet. Unerläßlich ist allerdings, daß alle über eine Leitung geschickten Daten, einschließlich Benutzerkennung und Paßwort, verschlüsselt werden. Damit die übertragenen Daten beim Empfänger auch verstanden werden können, muß erkennbar sein, von wem die Daten kommen, um sie in den Klartext entschlüsseln zu können. Ein solches Verfahren setzt deshalb eine sorgfältige Schlüsselverteilung und -organisation voraus. Verschlüsselungstechniken gibt es auch beim Telefax (siehe 22.3.6).

Solange im Fernsprechverkehr die Analogtechnik angewendet wird, ist eine Verschlüsselung der übertragenen Signale nicht (im Bereich des Netzbetreibers) bzw. nur mit unverhältnismäßig großem Aufwand (beim Endgerät) möglich und für die Praxis deshalb bedeutungslos. Mit Einführung der digitalen Übertragungstechnik (ISDN) eröffnen sich aber für die Verschlüsselung neue Wege.

22.3.5 Datensicherheit beim Telefax

Der Telefax-Dienst hat in den letzten Jahren eine sehr starke Verbreitung gefunden. Die meisten Behörden verfügen heute über einen Telefax-Anschluß. Probleme beim Versand können aber dort auftreten, wo bestimmte **Berufsgeheimnisse** zu beachten sind.

Beim Versand von sensiblen Unterlagen mit Telefax sind bestimmte zusätzliche Anforderungen an die Datensicherheit zu beachten:

- Vor dem Absenden eines Telefax hat der Absender zu prüfen, ob die **richtige Zielnummer** gewählt wurde. Die gewählte Zielnummer erscheint vor dem Absenden im Display des eigenen Gerätes. Dadurch läßt sich ein Versand an einen anderen Adressaten weitgehend vermeiden. Im übrigen ist die Wahrscheinlichkeit, bei einer Falschwahl eine gültige Telefax-Nummer zu erreichen, äußerst gering, da Telefax und Fernsprechverkehr im gleichen Netz abgewickelt werden und die Zahl der Telefonanschlüsse sehr viel höher ist als die der Fax-Anschlüsse. Handelt es sich bei der angewählten Nummer um einen

Fernsprechanschluß, erscheint eine Fehlermeldung; das Telefax wird nicht übertragen.

- Da es sich beim Telefax um eine **offene Zustellung** handelt, ist außerdem zu prüfen, ob die Sendung den Empfänger direkt oder über Dritte, etwa eine zentrale Poststelle, erreicht. Beim Versand von Arztberichten an den niedergelassenen Arzt kann man davon ausgehen, daß auch die Mitarbeiter, die das Telefax empfangen, als ärztliche Gehilfen der Schweigepflicht nach § 203 Abs. 3 StGB unterliegen. Hingegen ist beim Versand von Arztberichten an Krankenkassen und andere Sozialversicherungsträger nicht sichergestellt, daß ausschließlich solche Personen diese Unterlagen erhalten, die auch der ärztlichen Schweigepflicht unterliegen. In diesen Fällen empfiehlt es sich, Arztberichte in konventioneller Weise in einem verschlossenen Brief zu versenden, sofern nicht sicherzustellen ist, daß das Telefax vom Gerät weg unmittelbar in die Hände des Empfängers gelangt. Verfügt der ärztliche Dienst dieser Dienststellen über ein eigenes Telefax-Gerät, ist gegen den Versand von Unterlagen, die der ärztlichen Schweigepflicht unterliegen, als Telefax nichts einzuwenden.

- Für den Bereich der Deutschen Bundespost gilt beim Telefax-Dienst das Fernmeldegeheimnis. Der Inhalt des Telefax wird bei der Deutschen Bundespost nicht gespeichert. Zur Sicherheit gegen ein Abhören auf dem Übertragungsweg gibt es Zusatzgeräte, welche die Daten vor der Übertragung verschlüsseln und beim Empfänger vor dem Ausdrucken wieder in die Ursprungsform zurückverwandeln. Der Einsatz solcher Verschlüsselungsgeräte scheitert heute allerdings noch meist daran, daß nur wenige Kommunikationspartner über derartige Ver- und Entschlüsselungsgeräte verfügen.

22.3.6 Reparatur von Festplattenspeichern beim Hersteller

Beim Betrieb von dezentralen Systemen kann es in selten auftretenden Fällen vorkommen, daß an den Festplatten Schäden auftreten, die einen Ausbau und einen Transport zum Hersteller erforderlich machen. Ein Löschen der auf der Festplatte vorhandenen Daten ist in solchen Fällen wegen des aufgetretenen Defekts meist nicht mehr möglich, so daß die auf der Festplatte gespeicherten Daten außer Haus gegeben werden müssen. Eine physikalische Löschung der gesamten Platte mit einem Magneten ist zwar technisch möglich, erschwert jedoch die Fehlersuche und wird vom Hersteller meist nicht gerne gesehen.

Da es sich bei den gespeicherten Daten auch um schutzwürdige personenbezogene Daten handeln kann, wird empfohlen, im Wartungsvertrag folgende Klausel mitaufzunehmen:

„Der Auftragnehmer versichert, die für ihn und den Auftraggeber geltenden Anforderungen des Datenschutzrechts zu beachten und die ihm anvertrauten personenbezogenen Daten nur entsprechend den Weisungen des Auftraggebers zu benutzen. Der Auftragnehmer versichert weiter, daß er die Personen, denen diese Daten zugänglich sind, gemäß § 5 Abs. 2 BDSG bzw. Art. 14 Abs. 2 BayDSG auf die Einhaltung des Datengeheimnisses verpflichtet hat."

23. Datenschutzregister

Nach § 8 der Verordnung über das Datenschutzregister (DSRegV) vom 23.11.1978 veröffentlicht der Landesbeauftragte für den Datenschutz jährlich eine Übersicht über den Inhalt des Datenschutzregisters. Diese Übersicht kann auf Nachträge zu bereits veröffentlichten Übersichten beschränkt werden.

Wegen der Vielzahl der inzwischen angemeldeten Dateien und des begrenzten Nutzens der Übersicht für den Bürger wurde 1984 letztmalig eine Übersicht des Gesamtinhalts des Datenschutzregisters veröffentlicht. Seit 1985 wurden nur noch Nachträge veröffentlicht. Der Umfang dieser Nachträge hat sich wegen der Ausweitung der automatisierten Datenverarbeitung von Jahr zu Jahr vergrößert und füllt inzwischen ebenfalls weit über 100 DIN A 4-Druckseiten pro Jahr.

Der 6. Nachtrag vom 7. und 14. Dezember 1990 (Beilage zum Bayer. Staatsanzeiger Nr. 49/50) enthält die Meldungen automatisierter Dateien von speichernden Stellen, die vom 6. November 1989 bis 9. November 1990 in meiner Geschäftsstelle eingegangen sind, sowie eine vollständige Aufstellung aller automatisierten personenbezogenen Dateien im Schulbereich.

Am 3.11.1989 umfaßte das gesamte Datenschutzregister 18858 meldepflichtige Dateien von insgesamt 5313 speichernden Stellen. Zum Stichtag des 6. Nachtrags waren zum Datenschutzregister 20758 Dateien von 6073 speichernden Stelle gemeldet. Die Zunahme ist vor allem auf den vermehrten Einsatz von Arbeitsplatzcomputern zurückzuführen.

Etwa 60 Bürger wenden sich jährlich an mich, um zu erfahren, in welchen Dateien Daten über sie gespeichert sein können. Dazu leistet das Datenschutzregister wertvolle Dienste. Bezogen auf seinen Wohnort erhält der Auskunftssuchende einen **Auszug aus dem Datenschutzregister über alle Stellen, deren Zuständigkeitsbereich sich auf seinen Wohnort erstreckt**. Nicht in dieser Aufstellung enthalten sind allerdings solche Behörden, zu denen der Auskunftssuchende ebenfalls Beziehungen haben kann, etwa wegen eines Zweitwohnsitzes oder wegen des Besitzes eines Grundstückes in einem anderen Landkreis. Der Auszug enthält neben dem Namen und der Anschrift der Behörde die Art der Datei in einer Form, die ihm die Feststellung ermöglicht, ob er in dieser Datei gespeichert sein kann.

Die Pflege des Datenschutzregisters umfaßte im Berichtszeitraum folgende Arbeiten:

Neueintragen einer Stelle	799
Neueintragen einer Datei bei einer speichernden Stelle	2030
Änderungen bei der Bezeichnung einer speichernden Stelle	980
Dateibezogene Änderungen	13
Löschen einer speichernden Stelle	39
Löschen einer Datei	130

Die relativ hohe Zahl gelöschter Dateien ist wiederum dadurch zu erklären, daß speichernde Stellen alte Programme durch moderne, dem Stand der Technik angepaßte und um wesentliche Funktionen erweiterte Verfahren ersetzen, so daß eine Neuanmeldung erforderlich ist. Häufig erweitert sich auch der Dateiinhalt.

Die Führung eines Datenschutzregisters beim Landesbeauftragten für den Datenschutz hat sich bewährt. Das Register

gewährleistet für den Datenschutzbeauftragten den Überblick über die automatisiert betriebenen Dateien und für die Bürger die erforderliche Transparenz. Die Bürger können sich mit Hilfe des Registers Kenntnis darüber verschaffen, wer wo welche Daten automatisiert verarbeitet.

Bei der Novellierung des Bayerischen Datenschutzgesetzes ist jedoch zu überlegen, ob die jährliche Veröffentlichung einer Übersicht über den Inhalt des Datenschutzregisters angesichts des beträchtlichen Umfangs des Registers sinnvoll ist. Desgleichen ist der praktische Wert eines Auszugs aus dem vollständigen Datenschutzregister, den der Bürger nach Art. 7 Abs. 4 BayDSG verlangen kann, sehr gering. Dem Interesse der Bürger eher entsprechen würde es, die derzeitige Praxis (siehe oben) im Gesetz festzuschreiben.

24. Datenschutz beim Bayer. Rundfunk

Bericht des Rundfunkbeauftragten

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

Bei der Überwachung der Datenverarbeitung des BR im Zeitraum vom 1.1. bis 31.12.1989 hat der Datenschutzbeauftragte **keine Beanstandung** ausgesprochen.

Der Datenschutzbeauftragte schildert die Entwicklung des Datenschutzrechts im Bereich der Medien anhand des Entwurfs zum Bundesdatenschutzgesetz, des Hamburgischen sowie des Berliner Datenschutzgesetzes. Bei der Behandlung des Hamburgischen Datenschutzgesetzes berichtet er, daß die Staatskanzlei Schleswig-Holstein Vorschläge unterbreitet habe, wonach Gegendarstellungen, Unterlassungserklärungen und Widerrufe zu den gespeicherten redaktionellen Daten zu nehmen seien und einem von der Berichterstattung Betroffenen ein Auskunftsanspruch zu gewähren sei. Der NDR habe sich aus systematischen Erwägungen dagegen ausgesprochen, derartige Regelungen nur für den öffentlich-rechtlichen Rundfunk im Hamburgischen Datenschutzgesetz zu schaffen. Der NDR habe vielmehr für eine bereichsspezifische Regelung im NDR-Staatsvertrag und für gleiche Regelungen für den Bereich der privaten Medien plädiert.

In seinem letzten Tätigkeitsbericht hatte der Datenschutzbeauftragte des BR angekündigt, daß für den Betrieb dezentraler DV-Anlagen wegen der besonderen Probleme bei Datenschutz und Datensicherheit im BR Richtlinien erlassen werden sollten. Der Datenschutzbeauftragte erläutert, daß dieses Vorhaben im Berichtszeitraum vom Organisationsreferat noch nicht verwirklicht worden sei. Der Grund hierfür sei, daß die Gespräche mit dem Personalrat über eine Dienstanweisung hinsichtlich der dezentralen elektronischen Personaldatenverarbeitung noch nicht hätten abgeschlossen werden können. In diesem Zusammenhang verweist der Datenschutzbeauftragte auf das Problem der Datenverarbeitung auf mitarbeitereigenen PC's, mit denen diese an ihrem Arbeitsplatz betriebliche Daten verarbeiten. Die hierdurch entstehenden datenschutzrechtlichen, arbeitsmedizinischen und unternehmenspolitischen Fragen müßten in den zu erlassenden Richtlinien (Dienstanweisung) ebenfalls gelöst werden.

Datenschutzrechtliche Probleme, die sich beim Direktzugriff der Internen Revision auf die EDV-Daten stellen, werden anhand des Bayer. Datenschutzgesetzes erörtert. Die Interne Revision hatte zur Erfüllung ihrer Aufgaben beantragt, auf die gespeicherten Daten anderer Abteilungen direkt zugreifen zu können. Nach Art. 17 Abs. 1 BayDSG sei eine Übermittlung von Daten an die Interne Revision nur zulässig, wenn und soweit dies zur rechtmäßigen Erfüllung der der übermittelnden Stelle oder der dem Empfänger zugewiesenen Aufgaben erforderlich sei. Im Ergebnis rät der Datenschutzbeauftragte dringend davon ab, die Interne Revision mit einem PC direkt an die Zentral-EDV anzuschließen.

Im Zusammenhang mit der Einführung des ISDN-Netzes der Deutschen Bundespost (siehe hierzu 20.3) weist der Datenschutzbeauftragte auf einen weiteren Problemkreis hin, der sich besonders für Presse und Rundfunk ergibt. Bei Unternehmen, die wie der BR eine Telefonkostenkontrolle durchführten, werde die regelmäßig mit den Mitarbeitervertretungen vereinbarte Anonymisierung der Zielnummern aufgehoben, wenn infolge des ISDN-Anschlusses von der Deutschen Bundespost Rechnungen übersandt würden, aus denen sich die vollständigen Verbindungsdaten von der Nebenstelle bis zur Zielnummer herstellen ließen. Von besonderer Problematik erweise sich im Medienbereich die vollständige Gesprächsdatenerfassung im Zusammenhang mit dem Informantenschutz. Ein Redakteur einer Rundfunkanstalt, der von einem Informanten telefonisch geheime Informationen erhalte, habe zwar in einem strafrechtlichen Ermittlungsverfahren ein Auskunftsverweigerungsrecht nach § 53 Abs. 1 Nr. 5 StPO, trotzdem könne nicht ausgeschlossen werden, daß die Strafverfolgungsbehörden stattdessen bei der Rundfunkanstalt und der Deutschen Bundespost Datenträger beschlagnahmen, aus denen sich die Verbindungsdaten und damit die beiden Gesprächspartner ergeben. Diese und ähnliche Probleme müßten vor der Einführung von ISDN gelöst werden.

Auch die Probleme des Datenschutzes im Zusammenhang mit dem Medienprivileg werden erörtert (vgl. insoweit 20.1). Hierbei hält der Datenschutzbeauftragte nicht nur eine Einschränkung des bisherigen Medienprivilegs zugunsten des Persönlichkeitsschutzes, sondern auch eine Erweiterung des Medienprivilegs für geboten. Das Medienprivileg sei in sachlicher Hinsicht auf journalistisch-redaktionelle Zwecke zu beschränken. Andererseits müsse das Privileg in personeller Hinsicht auf den Kundenservice (Leserservice, Manuskriptdienst und ähnliches) oder auf die kollegiale Hilfe von Medienarchiven und Redaktionen untereinander ausgeweitet werden. Einen Auskunftsanspruch des Betroffenen gegenüber Presse und Rundfunk halte er für besonders problematisch, da hierdurch eine künftige Berichterstattung ausgeforscht oder verhindert werden könnte. Ein Auskunftsanspruch dürfe daher jedenfalls erst **nach** der Veröffentlichung oder Ausstrahlung der der Berichterstattung zugrundeliegenden Information geltend gemacht werden. Die bereits früher erhobenen Bedenken zur Speicherung von Gegendarstellungen halte er aufrecht, da damit eine Verpflichtung zur Speicherung von möglicherweise objektiv falschen Daten geschaffen würde. Allerdings räume er ein, daß zu einer ordnungsgemäßen journalistischen Arbeit auch die

Kenntnis über etwaige Gegendarstellungen zu früheren Veröffentlichungen gehöre.

25. Der Beirat

Die Mitglieder des Beirats werden nach Art. 29 Abs. 2 BayDSG für vier Jahre, die Mitglieder des Landtags für die Wahldauer bestellt. Nach der Landtagswahl im Oktober 1990 wurden die dem Beirat angehörenden Mitglieder des Landtags neu bestellt.

Im Berichtszeitraum gehörten als Vertreter des Landtags bis zur Landtagswahl im Oktober 1990 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

In der neuen Legislaturperiode gehören dem Beirat an:

die Landtagsabgeordneten	
Franz Brosch	Dr. Hans Gerhard Stockinger
Alois Braun	Dr. Helmut Müller
Franz Meyer	Wilhelm Wenning
Markus Sackmann	Georg Grabner
Dr. Klaus Hahnzog	Armin Nentwig
Carmen König	Joachim Wahnschaffe
die Senatoren	
Wolfgang Burnhauser	Hartwig Reimann
für die Staatsregierung	
Alfons Metzger Ministerialdirigent im Bayer. Staatsministerium Innern	Dr. Klaus Geiger Ministerialdirigent im Bayer. Staatsministerium des der Finanzen
für die Kommunalen Spitzenverbände	
Klaus Eichhorn Geschäftsführender Direktor der Anstalt für Kommunale Datenverarbeitung in Bayern	Hanns Herlitz Direktor bei der Anstalt für Kommunale Datenverarbeitung in Bayern
für die Sozialversicherungsträger	
Franz Martin Fehn Erster Direktor der Landesversicherungsanstalt Oberfranken und Mittelfranken nach dessen Ausscheiden ab 26.10.1990 Dr. Ludwig Bergner Erster Direktor der Landesversicherungsanstalt Oberbayern	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 führte bis zum Ende der Legislaturperiode MdL Franz Brosch, sein Stellvertreter war MdL Klaus Warnecke. Auch jetzt übt den Vorsitz MdL Franz Brosch aus, seine Stellvertreterin ist MdL Carmen König.

Der Beirat befaßte sich in seinen drei Sitzungen am 12.12.1989, 8.5.1990 und 10.7.1990 insbesondere mit folgenden Themen:

- Beratung des 11. Tätigkeitsberichts;
- Bericht über Prüfungen und Beanstandungen;
- Bericht zum Stand der Datenschutzgesetzgebung im Bund und in Bayern;
- Datenschutz im Zusammenhang mit Wahlen und Volksbegehren;
- regelmäßige Weitergabe der Daten aller Zu-, Weg- und Umzüge von der Meldebehörde an die gemeindliche Finanzverwaltung;
- Konsequenzen aus der Prüfung des Polizeipräsidiums München;
- anonymer unverknüpfter HIV-Test;
- Datenschutz in der ehemaligen DDR.

26. Konferenz der Datenschutzbeauftragten

26.1 Konferenz der Datenschutzbeauftragten des Bundes und der Länder

Die Datenschutzbeauftragten des Bundes und der Länder sowie die Datenschutzkommission Rheinland-Pfalz trafen sich 1990 zu drei Konferenzen.

Schwerpunkte der Erörterungen waren:

- Auswirkungen der Entwicklung in der früheren DDR und im Ostblock auf die Datenverarbeitung der Sicherheitsbehörden,
- Personaldatenverarbeitung im öffentlichen Bereich,
- Einrichtung eines Arbeitskreises „Datenschutz in der EG",
- Krankenhaus- und Hotelmeldepflicht im Melderechtsrahmengesetz,
- Gesetzentwurf des Bundesrats zur Bekämpfung des illegalen Rauschgifthandels und anderer Erscheinungsformen der organisierten Kriminalität,
- Technik zur Überwachung des Fernmeldeverkehrs und des nichtöffentlich gesprochenen Wortes,
- Stärkung des Schutzes des Brief-, Post- und Fernmeldegeheimnisses sowie des nichtöffentlich gesprochenen Wortes,
- Bundeskrebsregister.

Datenschutz in der DDR

Der Fall der Berliner Mauer und die geöffneten Schlagbäume zwischen Ost- und Westdeutschland machten eine verstärkte Zusammenarbeit der Behörden beiderseits der Grenze notwendig. Der damit einhergehende verstärkte Datenfluß, insbesondere zwischen den Sicherheitsbehörden, weckte die Sorge der Datenschutzbeauftragten um den Datenschutz der Bürger in der Bundesrepublik, wohl in der Annahme, daß die damalige DDR und der Stasi-durchsetzte Si-

cherheitsapparat noch über Jahre weiter existieren würden. Diese Sorgen wurden jedoch durch die rasche Entwicklung bis zur Wiedervereinigung überholt. Es ist Aufgabe der staatlichen Organe in den neuen Bundesländern, den Datenschutz aller Bürger zu gewährleisten und möglichst bald unabhängige Datenschutzbeauftragte einzurichten. Nach wie vor Gültigkeit hat jedoch die Mahnung, aus der Entwicklung in Mittel- und Osteuropa für die praktische Tätigkeit der Sicherheitsbehörden Konsequenzen zu ziehen.

Arbeitskreis EG

Mit der Einrichtung des Arbeitskreises Europa trugen die Datenschutzbeauftragten dem Umstand Rechnung, daß sich die EG mit Blick auf Europa 1992 verstärkt des Datenschutzes annimmt und deshalb aus Brüssel wesentliche Anstöße für die Entwicklung des Datenschutzes in Europa zu erwarten sind.

Gesetzentwurf des Bundesrats zur Bekämpfung der organisierten Kriminalität

Der Gesetzentwurf des Bundesrates zur Bekämpfung des illegalen Rauschgifthandels und anderer Erscheinungsformen der organisierten Kriminalität wurde in einer Sonderkonferenz beraten. Die Mehrheit übte an dem Gesetzentwurf, den der Bundesrat ohne Gegenstimme (!) über die Parteigrenzen hinweg beschlossen hat, heftige Kritik, weil er das Recht auf informationelle Selbstbestimmung nicht ausreichend gewährleiste. Einschnitte in das Privatleben auch des unbeteiligten Bürgers würden auf der Grundlage zu weit und häufig schwammig formulierter Tatbestände zugelassen werden. Die Mehrheit lehnte zwar intensive Fahndungsmethoden zur Bekämpfung der organisierten Kriminalität nicht grundsätzlich ab. Voraussetzungen seien aber eine Begrenzung auf diese Bereiche und wirksame flankierende datenschutzrechtliche Maßnahmen.

Die total ablehnende Kritik der Mehrheit wird jedoch dem Gesetzentwurf in keiner Weise gerecht. In ihrer fundamentalistischen Kritik am Entwurf unterschätzt die Mehrheit die zunehmende Gefahr mafia- und camorra-ähnlicher Zustände durch das Anwachsen der organisierten Kriminalität in der Bundesrepublik. Man macht sich offensichtlich über die konspirative Vorgehensweise bestens organisierter Krimineller und über die dadurch bedingten Notwendigkeiten auf polizeilicher Seite völlig falsche Vorstellungen. Ferner darf dem Rechtsstaat zur Verteidigung der Freiheits- und Sicherheitsrechte der Bürger die Nutzung der automatisierten Datenverarbeitung und anderer moderner Aufklärungsmittel nicht unverhältnismäßig und unter Kautelen, die bis zu deren Unwirksamkeit führen, erschwert werden. Der Entwurf wies zwar einige Mängel auf. Diese wären aber im laufenden Gesetzgebungsverfahren zu beheben gewesen.

Krankenhaus- und Hotelmeldepflicht

Kein Beschluß kam über die Krankenhaus- und Hotelmeldepflicht im Melderechtsrahmengesetz zustande. Während die Mehrheit die Auffassung vertrat, daß es sich bei dieser Meldepflicht um materielles Polizeirecht handle und der Bund nicht zuständig sei, geht der Bundesgesetzgeber seit Jahren zu Recht davon aus, daß es sich bei der Krankenhaus- und Hotelmeldepflicht um eine Materie des Melderechts handelt. Eine Abschaffung dieser Verpflichtung kann jedenfalls nicht mit verfassungsrechtlichen Argumenten begründet werden.

Fernmeldegeheimnis

Keine Einigung konnte auch erzielt werden zu der Frage, ob zum Schutz des Brief-, Post- und Fernmeldegeheimnisses die gesetzlichen Vorschriften enger und präziser gefaßt werden müßten.

Soweit die technische Entwicklung, insbesondere die Einführung von ISDN durch die Deutsche Bundespost, die Speicherung von Milliarden zusätzlicher Telefondaten gestattet, die auch der Justiz und den Sicherheitsbehörden zur Verfügung stehen, bin ich durchaus der Auffassung, daß sich der Gesetzgeber mit der Frage befassen muß, ob diese Daten in vollem Umfang für Zwecke der Justiz und der Sicherheit genutzt werden dürfen.

Entgegen der Auffassung der Mehrheit meine ich aber, daß für eine grundsätzliche Einschränkung der Abhörmöglichkeiten, weil Sicherheitsbehörden und Justiz davon angeblich im Übermaß Gebrauch machten, kein Anlaß besteht. Von einem generellen Mißbrauch der Abhörmöglichkeiten kann keine Rede sein. Im übrigen steht die Anwendung der Abhörbefugnisse unter der Kontrolle unabhängiger Richter und des Parlaments. Dafür, daß diese Instanzen einen Mißbrauch oder eine übermäßige Nutzung der Abhörbefugnisse zulassen, gibt es keinerlei Belege.

Bundeskrebsregister

Einvernehmen bestand hingegen in der Ablehnung von Überlegungen der Bundesregierung, bei der Einführung eines Bundeskrebsregisters, Patienten auch ohne ihre Einwilligung mit vollem Namen an das Register zu melden, sie ohne ihr Einverständnis im Bundeskrebsregister zu speichern und die Einwohnermeldeämter in den Datenfluß einzubeziehen.

26.2 Internationale Datenschutzkonferenz in Paris

Die Konferenz befaßte sich schwerpunktmäßig mit dem Schutz medizinischer Daten, mit den Möglichkeiten eines anonymisierten Krebsregisters sowie mit der Genomanalyse Strafverfahren. Ein weiterer Schwerpunkt waren die Entwicklung des Datenschutzes in einzelnen Ländern und Probleme in der praktischen Kontrolltätigkeit. Eingehend befaßte sich die Konferenz mit Grundsätzen für die künftige Telekommunikation in Europa. Positiv gewürdigt wurden die Initiativen der EG-Kommission zur Verankerung des Datenschutzes auf dem Gebiet der Europäischen Gemeinschaft.

Die französische Regierung widmete der Internationalen Datenschutzkonferenz große Aufmerksamkeit.

26.3 Besuch des Luxemburgischen Datenschutzbeauftragten

Mit dem Luxemburgischen Datenschutzbeauftragten habe ich bei einem Arbeitsbesuch Fragen der Datenschutzgesetzgebung in Bayern und in Luxemburg sowie die Entwicklung des Datenschutzes in Europa erörtert. Ferner haben wir Erfahrungen bei Datenschutzkontrollen ausgetauscht. Besichtigungen des Landeskriminalamtes und des Einwohnermeldeamtes der Landeshauptstadt München vermittelten dem Gast einen Einblick in die Datenverarbeitung in Bayern.

27. Vorträge und Seminare über Datenschutz

Der unverändert anhaltenden Nachfrage nach Referenten für einzelne Vorträge oder Seminare zum Datenschutz und zur Datensicherung habe ich auch im vergangenen Berichtszeitraum entsprochen, soweit es die Arbeitsbelastung der Mitarbeiter meiner Geschäftsstelle jeweils zuließ.

Zu den schon im 11. Tätigkeitsbericht genannten Einrichtungen, an deren Fortbildungsprogrammen ich mich regelmäßig beteilige, ist nunmehr auch die Anstalt für Kommunale Datenverarbeitung in Bayern (AKDB) hinzugekommen. Die Ausbildung der Rechtsreferendare findet inzwischen mit einer Ausnahme in allen Regierungsbezirken statt. Sie erfolgt jetzt regelmäßig bereits in den auf das zweite juristische Staatsexamen hinführenden Arbeitsgemeinschaften.

28. Geschäftsstelle beim Landesbeauftragten

In meiner Geschäftsstelle sind derzeit 20 Mitarbeiter tätig. Es handelt sich um 3 Referenten, 10 Prüfbeamte und 7 Mitarbeiter für den inneren Dienstbetrieb (Schreibdienst, Registratur, Führung des Datenschutzregisters u.a.). Dieser Personalstand ist seit dem Jahre 1987 unverändert.

Das Bundesverfassungsgericht hat in den letzten Jahren die Bedeutung der Kontrolltätigkeit der Datenschutzbeauftragten für die Gewährleistung des informationellen Selbstbestimmungsrechts der Bürger wiederholt bestätigt und die Einrichtung unabhängiger Datenschutzkontroll-Instanzen für unverzichtbar erklärt. Die automatisierte Datenverarbeitung hat in den letzten Jahren sprunghaft zugenommen. Die Bürger sind, wenn es um ihre Persönlichkeitsrechte geht, stark sensibilisiert. Andererseits wird es für sie immer schwieriger, sich einen Überblick darüber zu verschaffen, wer welche Daten wo über sie gespeichert hat und wer welche Daten an wen weitergibt. Der Datenschutzbeauftragte muß durch seine Kontrolltätigkeit dieses wachsende Defizit ausgleichen. Hinzu kommt, daß die Forderung des Bundesverfassungsgerichtes nach bereichsspezifischen differenzierten gesetzlichen Vorschriften für Eingriffe in das informationelle Selbstbestimmungsrecht zu einer Fülle von Detailregelungen führt, deren Einhaltung kontrolliert werden muß. Gleichzeitig steigt der Schulungsbedarf.

Schließlich kommen auch neue Aufgaben auf den Datenschutzbeauftragten zu:

Durch die Novellierung des Bundesdatenschutzgesetzes werden die Erhebung personenbezogener Daten sowie teilweise auch die Speicherung und Verarbeitung personenbezogener Daten in Akten der Kontrolle des Datenschutzbeauftragten unterworfen. Diese Änderungen wirken sich bereits heute auf den Umfang der Kontrolltätigkeit aus.

Das neue Bayerische Verfassungsschutzgesetz erfordert dichtere Kontrollen des Einsatzes nachrichtendienstlicher Mittel durch das Landesamt für Verfassungsschutz sowie bei der Überprüfung der gespeicherten Daten für den Bürger.

Das novellierte Polizeiaufgabengesetz läßt die Informationsbeschaffung und -verarbeitung nur unter detailliert geregelten Voraussetzungen zu. Der Einsatz besonderer technischer Mittel und verdeckter Ermittler stellt einen besonders tiefen Eingriff in das informationelle Selbstbestimmungsrecht dar. Diese Eingriffe müssen durch verstärkte Datenschutzkontrollen flankiert werden, weil der Bürger sich gerade in diesem sensiblen Bereich nicht selbst schützen kann.

Die wachsenden Aufgaben sind mit dem bisherigen Personal nicht zufriedenstellend zu bewältigen. Eine angemessene Erweiterung der Geschäftsstelle ist daher unumgänglich. Trotz der durch die deutsche Einheit gebotenen Sparmaßnahmen mußte ich deshalb für den Haushalt 1991/1992 zusätzliche Planstellen beantragen.