Bayerischer Landtag
11. Wahlperiode

Drucksache **11/9224**
12. 12. 88

Zehnter Tätigkeitsbericht des Landesbeauftragten für den Datenschutz

Berichtszeitraum 1987/1988

Der Landesbeauftragte für den Datenschutz
Nr. DSB/1 – 510 – 11

München, 12. Dezember 1988

An den
Herrn Präsidenten
des Bayerischen Landtags
München

Zehnter 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 zehnten Tätigkeitsbericht.

Mit vorzüglicher Hochachtung

Sebastian Oberhauser

Inhaltsübersicht

1. Vorbemerkung

1.1. Zehn Jahre Bayerisches Datenschutzgesetz

Über zehn Jahre ist es nun her, seit das Bayerische Datenschutzgesetz am 1. Mai 1978 in Kraft getreten ist. Das damals unbestritten fortschrittlichste Datenschutzgesetz in der Bundesrepublik hat sich in der stürmischen Entwicklung des Datenschutzes während der vergangenen Jahre hervorragend bewährt. Nur in wenigen Detailfragen hat sich heute die Notwendigkeit ergeben, dieses klare, übersichtliche und allgemein verständliche Gesetz an die gewandelten Anschauungen und an die technologische Entwicklung anzupassen. Da auch im Datenschutz ein gewisses Maß an Rechtseinheitlichkeit wünschenswert ist, sollte allerdings vor einer Änderung die Novellierung des Bundesdatenschutzgesetzes abgewartet werden.

1.2. Verstärkte Kontrollen

Wie im letzten Tätigkeitsbericht angekündigt, lag der Schwerpunkt meiner Tätigkeit im Berichtszeitraum 1988 in der verstärkten Datenschutzkontrolle bei den bayerischen Behörden. Zahlreiche, zum Teil mehrtägige Kontrollen der Rechtmäßigkeit der Datenverarbeitung wurden durchgeführt: bei fünf Gesundheitsämtern, einer Allgemeinen Ortskrankenkasse, einem Sozialamt, drei landwirtschaftlichen Sozialkassen, einer Staatsanwaltschaft, einer Justizvollzugsanstalt, beim Landeskriminalamt (zweimal), bei drei Polizeipräsidien, acht Polizeidirektionen, zwei Grenzpolizeibehörden, beim Landesamt für Verfassungsschutz (zweimal), beim Landesamt für Statistik und Datenverarbeitung, einer Regierung, einem Landratsamt, fünf Gemeinden und bei der Bayerischen Landeszentrale für Neue Medien. Ergänzt wurden die allgemeinen Kontrollen durch zahlreiche Überprüfungen von Behörden aufgrund von Eingaben und Beschwerden von Bürgern.

Hinzu kommen technisch-organisatorische Kontrollen bei drei Rechenzentren von Sozialversicherungsanstalten, beim Landesamt für Statistik und Datenverarbeitung, bei der Anstalt für Kommunale Datenverarbeitung in Bayern, einem Klinikum, einer Universität, drei Landratsämtern und vier Gemeinden.

Einen wenngleich nur vagen Eindruck über die Belastung der Geschäftsstelle vermitteln folgende Zahlen: Im Jahr 1988 habe ich fast 3800 Schreiben erhalten, über 3200 Schreiben haben meine Dienststelle verlassen; daneben konnten zahlreiche Vorgänge telephonisch erledigt werden.

1.3. Datenschutz in Bayern gewährleistet

Als wichtigstes Ergebnis meiner Kontrollen im Berichtszeitraum 1988 kann ich feststellen, daß der Datenschutz in Bayern gewährleistet ist. Im Verhältnis zum gewaltigen Umfang der täglichen Informationsverarbeitung gab es nur wenige Datenschutzverstöße. Sie liegen innerhalb der wohl unvermeidlichen Fehlerquote.

Bei allen bayerischen Behörden habe ich große Bereitschaft zur Zusammenarbeit und hohes Interesse an einem den gesetzlichen Vorschriften entsprechenden Datenschutz vorgefunden. Bei den Kontrollen wurden mir alle verlangten Unterlagen vorgelegt, jede Einsichtnahme gestattet. Selbst in Fällen, in denen meine Prüfkompetenz zweifelhaft sein konnte, wurde mir bereitwillig Auskunft und Einsicht gewährt. Diese gute Zusammenarbeit ist sicher nicht zuletzt darauf zurückzuführen, daß ich meine Aufgabe entgegen manchen Vorstellungen nicht darin sehe, in einer Art Opposition ein „Gegengewicht" gegen die Behörden zu bilden und den ordnungsgemäßen Vollzug der vom Parlament beschlossenen Gesetze zu hemmen und zu erschweren. Mein gesetzlicher Auftrag besteht vielmehr in der Kontrolle der Einhaltung der Datenschutzvorschriften.

1.4. Inhalt und Schwerpunkte des 10. Tätigkeitsberichts

Auch dieser Bericht kann aus Platzgründen nur eine Auswahl aus meiner Tätigkeit während des Berichtszeitraums 1988 umfassen. Aufgenommen wurden Beiträge, die über den Einzelfall hinaus von allgemeinem öffentlichen Interesse sind, sei es, daß es sich um neue Fragestellungen im Datenschutz handelt, sei es, daß typische Datenschutzprobleme des Alltags strittig oder daß Einzelfälle von den Medien aufgegriffen worden sind. In ihrer Gesamtheit sollen die Einzelbeiträge den aktuellen Stand des Datenschutzes in Bayern vermitteln.

- Den Schwerpunkt des Berichts bilden die Ergebnisse der im Berichtszeitraum durchgeführten **Datenschutzkontrollen**. Im Vordergrund steht wie in den vergangenen Jahren die Datenverarbeitung im Sicherheitsbereich (Polizei, Verfassungsschutz, Justiz). Nicht etwa weil hier ein Defizit an Datenschutz bestünde, sondern weil sich das Interesse der Öffentlichkeit im Blick auf die Freiheitsrechte der Bürger verständlicherweise auf diesen Bereich konzentriert.

- Von der Öffentlichkeit weniger beachtet, aber von zumindest gleicher Bedeutung für die Bürger sind die zahlreichen Datenschutzfragen, die bei den Städten, Gemeinden und Landratsämtern auftauchen. Mit diesen Behörden haben die meisten Bürger mehr zu tun als mit den Sicherheitsbehörden. Deshalb habe ich diesmal dem Datenschutz in der inneren Verwaltung, mit Schwerpunkt im Einwohnermeldewesen, breiteren Raum eingeräumt. Auch im Bereich der Gesundheitsämter habe ich einen Kontrollschwerpunkt gesetzt.

- Neu ist ein Kapitel über den Datenschutz im **Umweltbereich**. Immer deutlicher zeichnet sich ein Spannungsverhältnis zwischen Umweltschutz und Datenschutz ab. Einerseits benötigen die Umweltbehörden möglichst viele Daten über umweltgefährdende Betriebe und Tätigkeiten, um die Gefahren für die Umwelt beherrschen zu können. Die Öffentlichkeit ist an Informationen über bestehende Gefährdungen stark interessiert. Andererseits kollidiert dieses verständliche Informationsbedürfnis mit dem Anspruch der Betroffenen auf Geheimhaltung ihrer Umweltdaten (siehe unter 17).

- Neu ist auch ein Kapitel über Datenschutz bei der **Gentechnologie**, in dem in Anlehnung an die Erkenntnisse der „Enquete-Kommission Gentechnologie" des Bundestages datenschutzrechtliche Risiken aufgezeigt werden (siehe unter 20).

- Fortgeführt wird die Diskussion über den Datenschutz bei den **Medien** mit konkretisierten Vorschlägen zur Verbesserung des Persönlichkeitsschutzes in diesem Bereich (siehe unter 19.1).

- Während der Datenschutz im Vollzug der geltenden Gesetze gewährleistet ist, hat der Gesetzgeber in den kommenden Jahren einige dringliche Aufgaben zu

erledigen. Wieder erinnere ich an die Notwendigkeit, im Sicherheitsbereich endlich Konsequenzen aus dem Volkszählungsurteil des Bundesverfassungsgerichts von 1983 zu ziehen und eine tragfähige Grundlage für die Informationsbeschaffung und Datenverarbeitung der Polizei und der übrigen Sicherheitsbehörden zu schaffen.

Auf weiteren Regelungsbedarf im Datenschutz möchte ich besonders hinweisen, nämlich auf die „Datenschutzlücken" im Gemeinderat und im Finanzbereich.

Während der Datenschutz der Bürger in der Gemeindeverwaltung in der Regel beachtet wird, muß ich mehrfach feststellen, daß dieser Schutz nachläßt, sobald Angelegenheiten im **Gemeinderat** behandelt werden. Die derzeit möglichen Sanktionen bei Indiskretionen aus nichtöffentlichen Gemeinderatssitzungen sind in der Gemeindeordnung unzureichend ausgestaltet. Nur eine angemessene Strafvorschrift kann hier die Persönlichkeitsrechte der Bürger ausreichend schützen (Näheres unter 7.1).

Nicht zufriedenstellen kann der Datenschutz der Bürger im **Finanzbereich,** wie er derzeit gesetzlich geregelt ist und in der Novelle zum Bundesdatenschutzgesetz festgeschrieben werden soll. Außer Zweifel steht zwar, daß die Finanzbehörden das Steuergeheimnis strikt beachten. Doch dadurch allein wird der Datenschutz der Bürger im Finanzamt noch nicht gewährleistet. Allgemeinen rechtlichen Überprüfungen der Finanzämter durch die Landesbeauftragten für den Datenschutz steht nach herrschender Meinung derzeit das Steuergeheimnis entgegen. Die Einhaltung der Vorschriften über die Erhebung, Speicherung, Übermittlung und Löschung von steuerrelevanten Daten kann damit von den Datenschutzbeauftragten nicht effektiv kontrolliert werden (Näheres unter 9.1).

1.5. Ausblick

Meinem gesetzlichen Auftrag entsprechend wird auch im Berichtszeitraum 1989 der Schwerpunkt meiner Tätigkeit in der Kontrolle der bayerischen Behörden liegen.

Im Jahr vor den Wahlen zum Bundestag und Landtag ist erfahrungsgemäß mit reger Gesetzgebungstätigkeit zu rechnen. Diese Gesetzgebung werde ich genau beobachten und dabei, soweit notwendig, eigene Vorschläge zur angemessenen Berücksichtigung des Datenschutzes einbringen. In der Konferenz der Datenschutzbeauftragten, in der die Gesetzgebung ein vorrangiges Thema ist, werde ich mich weiterhin für einen Datenschutz nach Vernunft und Augenmaß einsetzen.

2. Gesundheit

2.1. AIDS

Im 9. Tätigkeitsbericht habe ich zum Thema AIDS ausgeführt:

> „Wegen der besonderen Sensibilität der Daten in diesem Bereich muß es Aufgabe des Datenschutzbeauftragten sein darüber zu wachen, daß die Vorschriften des Datenschutzes strikt eingehalten werden. Erhobene Daten dürfen nur in dem zur Bekämpfung von AIDS notwendigen Umfang weitergegeben werden. Dieses Gebot dient nicht nur dem Schutz der Betroffenen vor Diskriminierung, sondern ist auch eine wesentliche Voraussetzung für ihre Bereitschaft, an der Bekämpfung von AIDS mitzuwirken."

An diesem Grundsatz habe ich im Berichtszeitraum die Datenschutzkontrolle in Bayern ausgerichtet. Dabei konnte ich feststellen, daß die bayerischen Behörden die Sensibilität des Datums „AIDS-infiziert" erkannt haben. Ich mußte im Zusammenhang mit AIDS nur einen Verstoß gegen Datenschutzvorschriften beanstanden (siehe unter 4.5.2).

AIDS hat auch im Jahr 1988 nichts von seinem Schrecken verloren. Die meist tödlich verlaufende Krankheit hat sich weiter ausgebreitet. Vorbeugender Impfschutz und wirksame medizinische Behandlung sind nicht in Sicht. Gefährdet sind nicht nur die Risikogruppen Fixer, Homosexuelle und Prostituierte. Selbst bei größter Sorgfalt kann eine AIDS-Infektion, beispielsweise durch Bluttransfusion, nicht völlig ausgeschlossen werden. Über das normale Maß hinaus gefährdet sind junge Menschen. Es muß auch zu denken geben und die Verantwortlichen zum Handeln veranlassen, daß die Ausbreitung von AIDS durch den intravenösen Rauschgiftkonsum begünstigt wird.

Aus diesen Gründen ist der Staat zum Schutz der Bevölkerung verpflichtet, im Kampf gegen AIDS seine Anstrengungen zu verstärken und alle geeigneten und wirksamen Mittel auszuschöpfen. Neben umfassender und intensiver Beratung und Aufklärung besteht der gesetzliche Auftrag, das seuchenrechtliche Instrumentarium voll anzuwenden. Wenn es dem freiheitlichen Rechtsstaat nicht gelingen sollte, der Ausbreitung der tödlichen Infektionskrankheit AIDS in der Bevölkerung Einhalt zu gebieten, wäre zumindest auf längere Sicht unsere Gesellschaftsordnung, die ein Höchstmaß an persönlicher Freiheit gewährleistet, ernsthaft bedroht.

Der Datenschutz steht geeigneten und wirksamen Maßnahmen, welche die Ausbreitung von AIDS verlangsamen und verhindern, nicht im Weg. Seine Aufgabe besteht vornehmlich darin, darüber zu wachen, daß bei allen Maßnahmen das Persönlichkeitsrecht der Betroffenen im verfassungsrechtlich und gesetzlich geschützten Rahmen gewahrt bleibt.

2.1.1. Sachbehandlung bei Gesundheitsämtern

Konkrete Angaben zum Ansteckungsverdacht

Bei der datenschutzrechtlichen Prüfung von Gesundheitsämtern habe ich zum Teil Unsicherheit darüber festgestellt, wie konkret polizeiliche Meldungen an das Gesundheitsamt den Ansteckungsverdacht beschreiben müssen, damit das Amt seuchenrechtliche Ermittlungen (Vorladung Ansteckungsverdächtiger) einleiten kann. Von Einzelfällen abgesehen haben die überprüften Gesundheitsämter erst dann einen HIV-Ansteckungsverdacht angenommen und Maßnahmen in die Wege geleitet, wenn der Sachverhalt ausreichend konkret beschrieben war, so daß der Verdacht für das Amt nachvollziehbar war. Die Polizei muß also in ihren Meldungen an das Gesundheitsamt die Umstände konkret bezeichnen, aus denen sie den Ansteckungsverdacht ableitet.

Niedrige Anforderungen an den Ansteckungsverdacht

Der Bayer. Verwaltungsgerichtshof hat in seiner Entscheidung vom 19. Mai 1988 (BayVBl. 1988 S. 463) festgestellt, die

Anforderungen an die Annahme des HIV-Ansteckungsverdachts nach § 31 Abs. 1 Bundesseuchengesetz seien im Hinblick auf die Schwere der AIDS-Erkrankung niedrig anzusetzen, um eine weitere Ausbreitung von AIDS zu verhindern. Im einzelnen führt er aus:

„Angesichts der Schwere der in der Regel tödlich verlaufenden AIDS-Erkrankung und ihrer Nichtheilbarkeit einerseits und der relativ leichten Verhinderung der Weiterverbreitung durch verantwortungsbewußtes Verhalten andererseits ist es sachgerecht und der gesetzlichen Zielsetzung entsprechend, die Ermittlungen nach §§ 31 ff Bundesseuchengesetz bereits bei einem sehr geringen Verdacht auf eine HIV-Infektion einzuleiten. Das Gebot der Verhältnismäßigkeit wird hierdurch nicht verletzt. Für diejenigen, die sich als nicht infiziert erweisen, ist der belastende Eingriff (Blutentnahme, Unsicherheit während des Wartens auf das Testergebnis) gering. Für die Infizierten allerdings wird die Konfrontation mit dem positiven Testergebnis in der Regel eine schwere persönliche Belastung mit im Einzelfall gravierenden Folgen (Suizidgefahr, Depressionen, psychosomatische Störungen) bedeuten...

Gleichwohl ist das Verhältnismäßigkeitsprinzip nicht verletzt. Denn je größer und folgenschwerer der möglicherweise eintretende Schaden ist, desto belastender kann die zur Schadensabwendung getroffene Maßnahme sein. Angesichts der in der Regel tödlich verlaufenden, nicht heilbaren AIDS-Erkrankung ist es nicht unverhältnismäßig, den Infizierten um der Verhinderung der weiteren Verbreitung der Krankheit willen mit der Kenntnis seiner Infizierung zu belasten...

Die Volksgesundheit und der Schutz der Bürger vor einer tödlich verlaufenden, ansteckenden, übertragbaren Krankheit sind überragende Gemeinschaftsgüter, die auch unter Umständen schwerwiegende Eingriffe in die Rechte Einzelner rechtfertigen."

Anonyme AIDS-Beratung

Die Sorgfalt, mit der bei den kontrollierten Ämtern die AIDS-Beratung anonym durchgeführt wird, ist besonders hervorzuheben. Ich konnte mich davon überzeugen, daß die über die einzelnen Beratungen geführten Vermerke keine namentliche Bestimmung der beratenen Personen ermöglichen. In einem Tagebuch wird nur festgehalten, was zur Zuordnung des Untersuchungsergebnisses zu einem, vom Betroffenen angegebenen Codewort erforderlich ist. Unter diesem Codewort kann dieser das Testergebnis dann erfragen. Den Bediensteten ist strengstens auferlegt, Auskunft nur gegen Nennung des vereinbarten Codeworts zu erteilen.

Soweit es die räumlichen Verhältnisse des einzelnen Gesundheitsamtes zulassen, findet die anonyme AIDS-Beratung in Zonen statt, die vom allgemeinen Besuchsverkehr abliegen. Außerdem sind besonders beauftragte – meist ärztliche – Mitarbeiter eingesetzt. Ein überprüftes Gesundheitsamt betreibt die anonyme AIDS-Beratung sogar in Räumen außerhalb des Dienstgebäudes. Das ist aus der Sicht des Datenschutzes positiv zu bewerten, da die Besucher von Bediensteten des übrigen Gesundheitsamtes nicht wahrgenommen werden.

Angesichts dieser ernsthaften Bemühungen der Ämter, die Anonymität der AIDS-Beratung zu gewährleisten und so zum AIDS-Test zu ermuntern, sind vereinzelte Presseberichte über angebliche Verletzungen der Anonymität der AIDS-Beratung umso unverantwortlicher. Selbst wenn im Einzelfall einmal Zweifel an der Anonymität geäußert werden, wäre es besser, sinnvoller und der AIDS-Bekämpfung dienlicher, den Datenschutzbeauftragten einzuschalten, anstatt kurzsichtig mit Schlagzeilen gegenüber einer notwendigen und bewährten Institution Mißtrauen zu wecken.

2.1.2. Weitergabe des positiven HIV-Testergebnisses durch Blutspendedienst

Der anwaltliche Vertreter einer AIDS-infizierten Studentin bat mich um datenschutzrechtliche Bewertung eines Vorfalls, der in Teilen der Massenmedien starkes Interesse fand. Aufgrund meiner Ermittlungen beim Gesundheitsamt stellt sich der Vorfall, der inzwischen auch von der Staatsanwaltschaft untersucht wird, jedoch so dar, daß die Weitergabe der Information über die AIDS-Infektion vom Blutspendedienst an die Nervenärztin und an die Kreisverwaltungsbehörde als Unterbringungsbehörde ebensowenig zu beanstanden war wie die Unterrichtung der Polizeibeamten über die näheren Umstände der Unterbringungsgründe.

Von Einzelheiten möchte ich mit Rücksicht auf die Betroffene absehen.

2.1.3. Weitergabe von Erkenntnissen an Versammlungsbehörden

Im Zusammenhang mit dem 2. Europäischen Treffen HIV-positiver Menschen an Pfingsten 1988 in München wurde in der Presse berichtet, ein im Staatsministerium des Innern gelagertes Dossier habe dazu geführt, daß das Kreisverwaltungsreferat der Landeshauptstadt München die als stellvertretende Versammlungsleiterin eines Solidaritätszugs vorgesehene Person abgelehnt habe. Die Betroffene wandte sich an mich mit der Bitte um Überprüfung der Angelegenheit.

Meine Ermittlungen haben ergeben, daß ein solches Dossier nicht existiert. Es stellte sich vielmehr heraus: Das Staatsministerium des Innern richtete im Zusammenhang mit der von der Münchner AIDS-Hilfe durchgeführten Veranstaltung Anfragen an Polizei und Sicherheitsbehörden. Die ermittelten Tatsachen teilte das Staatsministerium des Innern der Landeshauptstadt München – Kreisverwaltungsreferat – mit.

Diese Handlungsweise ist aus datenschutzrechtlicher Sicht nicht zu beanstanden. Das Staatsministerium des Innern ist das für das Versammlungsrecht zuständige Ministerium in Bayern. Ihm obliegt die Aufsicht über den Vollzug des Versammlungsrechts; das Versammlungsrecht wird von der Landeshauptstadt München als staatliche Aufgabe im übertragenen Wirkungskreis vollzogen (Art. 83 Abs. 4 Bayer. Verfassung i.V.m. Art. 8, 9, 108 ff der Gemeindeordnung).

Zulässig war insbesondere die Übermittlung der Erkenntnisse von den Sicherheits- und Polizeibehörden an das Staatsministerium des Innern sowie die Weitergabe dieser Kenntnisse an die Landeshauptstadt München zur Erfüllung der dem Staatsministerium des Innern gesetzlich zugewiesenen Aufsichtsaufgaben nach dem Versammlungsrecht (§ 15 Versammlungsgesetz, Art. 7 des Gesetzes zur

Ausführung des Versammlungsgesetzes, Art. 110 Satz 4 der Gemeindeordnung). Nach Art. 17 Abs. 1 BayDSG ist die Übermittlung personenbezogener Daten an andere öffentliche Stellen zulässig, wenn sie zur rechtmäßigen Erfüllung der durch Rechtsnorm der übermittelnden Stelle oder dem Empfänger zugewiesenen Aufgaben erforderlich ist. Diese Erforderlichkeit war vorliegend zu bejahen. Von der Darstellung weiterer Einzelheiten möchte ich mit Rücksicht auf die Betroffene absehen.

2.2. Datenschutz im Krankenhaus

2.2.1. Übermittlung von Patientendaten an Sozialämter

Auch im Berichtszeitraum sind Beschwerden über die Weitergabe von Patientendaten durch Krankenhäuser an Sozialämter eingegangen (s. a. 8. Tätigkeitsbericht, Nr. 2.11, S. 10). Abrechnungsstellen von Krankenhäusern meldeten wiederum vorsorglich dem Sozialamt selbst dann die Namen stationär behandelter Patienten, wenn diese durch Vorlage einer Bestätigung des Dienstherrn einen Beihilfeanspruch nachgewiesen hatten. Ich habe diese unzulässige Patientendatenübermittlung beanstandet.

Nicht zu rügen ist grundsätzlich, wenn das Krankenhaus zur Sicherung seiner Kostenerstattungsansprüche die Sozialhilfeverwaltung eines Hilfeempfängers als Kostenträger (§§ 37, 121 Bundessozialhilfegesetz – BSHG) ermittelt und verständigt. Das gehört zu den Aufgaben eines Krankenhauses (Art. 26 Abs. 2 Bayer. Krankenhausgesetz). Zu diesem Zweck darf es, wenn die Kostenerstattung nicht durch eine Krankenkasse gesichert ist, einen Patienten bei der Aufnahme fragen, ob er Sozialhilfeempfänger ist oder aus anderen Gründen eine Kostenerstattung durch die Sozialhilfe beantragen werde. Bejaht der Patient die Frage oder verweigert er die Angabe oder bestehen sonstige Anhaltspunkte für eine Kostenerstattungspflicht der Sozialhilfe, kann das Krankenhaus die Sozialhilfeverwaltung verständigen.

Unzulässig ist aber die vorsorgliche Übermittlung von Namen und Anschriften aller aufgenommenen Patienten an die Sozialhilfeverwaltung, weil diese Maßnahme wegen der nur in Ausnahmefällen begründeten Kostenübernahme durch das Sozialamt unverhältnismäßig und auch nicht erforderlich ist.

Für den Kreis der Beihilfeberechtigten hat das Staatsministerium der Finanzen klargestellt, daß die Krankenhäuser künftig unmittelbar bei den Festsetzungsstellen Abschläge auf die Beihilfe anfordern können. Die Bayerische Krankenhausgesellschaft ist zur Umsetzung dieser Regelung bei den ihr angeschlossenen Krankenhausträgern unterrichtet worden.

2.2.2. Mitteilung von Patientendaten zur Feststellung der Vaterschaft

Der Datenschutzbeauftragte eines Krankenhausträgers bat um Prüfung der Frage, ob Name und Anschrift eines früheren Patienten zum Zweck der Vaterschaftsfeststellung an das anfragende Jugendamt übermittelt werden dürfen. Das Jugendamt hatte als Amtspfleger um Mitteilung dieser Daten eines Patienten gebeten, der nach den Angaben der Mutter der mutmaßliche Vater ihres unehelich geborenen Kindes sei. Name und Anschrift des fraglichen Vaters konnten vom Krankenhaus aufgrund von Hinweisen der Kindsmutter zum Vornamen, zu seinem Äußeren (Schnauzbart), zum Zeitpunkt seines Krankenhausaufenthaltes, zum Behandlungszweck und zu seinem Arbeitgeber ermittelt werden.

Das Staatsministerium für Arbeit und Sozialordnung wies darauf hin, daß im vorliegenden Fall die datenschutzrechtliche Sondervorschrift des Bayer. Krankenhausgesetzes (BayKrG) anzuwenden und die erbetene Übermittlung von Namen und Anschrift des mutmaßlichen Vaters nur zulässig sei, wenn die Voraussetzungen des Art. 26 Abs. 5 BayKrG erfüllt seien. Evtl. vorhandene Offenbarungsbefugnisse des § 203 Strafgesetzbuch (StGB) würden die Datenübermittlung nicht automatisch auch nach dem BayKrG zulassen.

Wegen der strengen datenschutzrechtlichen Sondervorschrift des Art. 26 Abs. 5 BayKrG habe ich die Übermittlung von Name und Anschrift des mutmaßlichen Vaters durch das Krankenhaus an das Jugendamt zum Zwecke der Vaterschaftsfeststellung nicht für zulässig gehalten. Zu den geschützten Daten eines Patienten zählen auch dessen Name und Anschrift. Diese Angaben dürfen an das Jugendamt nur im Rahmen des Behandlungsvertrages weitergegeben werden oder wenn eine Rechtsvorschrift dies erlaubt oder der Betroffene eingewilligt hat. Eine Weitergabe aufgrund des Behandlungsvertrags oder der Einwilligung des Betroffenen schied aus. Es kam also darauf an, ob eine sonstige Rechtsvorschrift die Weitergabe erlaubte.

§ 203 Strafgesetzbuch scheidet als Rechtfertigungs- bzw. Befugnisnorm für eine Datenweitergabe aus. Denn diese Vorschrift ist eine Strafnorm, keine Befugnisnorm. Nicht jede Offenbarung, die nicht unter Strafe verboten ist, ist deshalb erlaubt.

Übergesetzlicher Notstand (§ 34 StGB) scheidet als Rechtfertigungsgrund aus, weil durch die Nichtweitergabe von Name und Anschrift des mutmaßlichen Vaters Leib und Leben des Kindes oder ein ähnlich hohes Rechtsgut nicht gefährdet werden.

Zwar ist das Interesse des Kindes und der Mutter an der Feststellung der Vaterschaft höher einzustufen als das Interesse des früheren Patienten und mutmaßlichen Vaters, nicht in einen Vaterschaftsprozeß verwickelt und zu Unterhaltszahlungen herangezogen zu werden. Für eine solche Interessenabwägung ist jedoch bei Art. 26 Abs. 5 BayKrG kein Platz. Da es sich um eine Sondervorschrift für den Datenschutz der Krankenhauspatienten handelt, können auch die Rechtsgrundsätze der Art. 17 und 18 des Bayer. Datenschutzgesetzes nicht herangezogen werden. Es ist davon auszugehen, daß das Bayer. Krankenhausgesetz die im Krankenhaus behandelten Patienten unter einen besonderen, über § 203 StGB und die allgemeinen Datenschutzvorschriften hinausgehenden Schutz stellen wollte.

Dieses Ergebnis mag im vorliegenden Fall im Hinblick auf die Interessen des unehelichen Kindes und der Mutter unbefriedigend sein. Ein anderes Ergebnis ist jedoch nur nach einer Änderung des Art. 26 Abs. 5 BayKrG zu erreichen, die allerdings einer eingehenden Erörterung bedürfte.

2.2.3. Weitergabe von Patientendaten an einen Landtagsabgeordneten

Durch mehrere Telefonanrufe von Bürgern habe ich erfahren, daß Bedienstete eines Krankenhauses sensible Patientendaten (Name und Krankheit von Patientinnen, angebliche ärztliche Kunstfehler) an einen Stadtrat und Landtagsabgeordneten übermittelt haben.

Mitarbeiter meiner Geschäftsstelle suchten daraufhin das Krankenhaus auf, um die Datenschutzverstöße an Ort und Stelle zu untersuchen. Die Krankenhausverwaltung legte mehrere Schreiben des Stadtrats und Landtagsabgeordneten an den Vorsitzenden des Krankenhauszweckverbandes vor. Zur Untermauerung seines Vorwurfs, ein Chefarzt habe zahlreiche Kunstfehler begangen, waren in dem Schreiben Namen von Patientinnen, ihre Krankheiten und die angeblichen ärztlichen Kunstfehler genannt. Der Abgeordnete bezog sich dabei auf nicht näher bezeichnete Informanten.

Ich habe die Mitteilung der Namen der Patientinnen, ihrer Erkrankungen und der ärztlichen Behandlung durch Bedienstete an einen Stadtrat und Abgeordneten als Verletzung der ärztlichen Schweigepflicht gerügt und deswegen den Krankenhauszweckverband beanstandet.

Die Herausgabe von Patientendaten an Dritte ist nach Art. 26 Abs. 5 Bayer. Krankenhausgesetz zu beurteilen. Es ist keine Rechtsvorschrift ersichtlich, welche die Information eines Dritten über ärztliche Kunstfehler unter Nennung der Patientennamen rechtfertigen könnte. Wenn die Informanten es schon für erforderlich gehalten haben, einen Stadtrat und Landtagsabgeordneten zu unterrichten, so wäre das zur Erreichung ihres legitimen Ziels, Mißstände anzuprangern und für Abhilfe zu sorgen, auch ohne Nennung der Patientennamen möglich gewesen. Auch in diesem Fall wäre eine Untersuchung der Vorwürfe ohne Verletzung der ärztlichen Schweigepflicht möglich gewesen. Die ärztliche Schweigepflicht ist auch bei der Information von Stadträten oder Abgeordneten über angebliche Mißstände im Krankenhaus zu beachten.

Die Aufklärung des Falls ist dadurch erschwert und der Bruch der ärztlichen Schweigepflicht möglicherweise erleichtert worden, daß das Krankenblattarchiv nicht ordnungsgemäß geführt wurde. Wegen fehlender Eintragungen konnte bei dem Kontrollbesuch nicht festgestellt werden, an wen die Akten über die Patientinnen, deren Daten preisgegeben wurden, ausgehändigt wurden. Ich habe deshalb das Krankenhaus aufgefordert, für die Führung des Krankenblattarchivs ein Verfahren einzuführen, das jederzeit dokumentiert, zu welcher Zeit von wem welchen Stellen und Mitarbeitern des Krankenhauses Patientenunterlagen zur Einsicht überlassen worden sind.

2.3. Gesundheitsamt

2.3.1. Prüfung von Gesundheitsämtern

Im Berichtszeitraum wurden 5 Gesundheitsämter überprüft. Dabei wurden 17 verschiedene Karteiarten festgestellt.

Bei keinem der kontrollierten Gesundheitsämter habe ich eine AIDS-Datei festgestellt. Eine AIDS-Infektion ist allenfalls in anderen manuell geführten Karteien mitvermerkt.

Bei den vorgefundenen Karteien handelt es sich teilweise um „interne" Karteien, deren Daten nicht zur Übermittlung an Dritte bestimmt sind, so daß von den Vorschriften des Bayer. Datenschutzgesetzes nur die Regelungen über die Datensicherung anzuwenden sind (Art. 1 Abs. 2 Satz 2 BayDSG). Auf interne nicht automatisiert geführte Karteien anwendbar sind außerdem die Vorschriften des Gesetzes über den öffentlichen Gesundheitsdienst (GDG) sowie die Regeln der ärztlichen Schweigepflicht. Die vorgefundenen Datenspeicherungen sowie die Verarbeitung der Daten begegnen in den meisten Fällen keinen Bedenken.

Die nachfolgenden Punkte waren zu klären:

- Zentralkartei:

  Die Zentralkartei als Suchkartei enthält Hinweise auf Vorgänge aus der Begutachtung, der freiwilligen Beratung sowie aus der hoheitlichen Tätigkeit. Bei dieser Verfahrensweise muß besonders darauf geachtet werden, daß keine Informationen aus der freiwilligen Beratung an andere Tätigkeitsbereiche des Amtes gelangen, die dort nach der Geheimhaltungsvorschrift des Art. 6 GDG nicht verwendet werden dürfen. Diese Vorschrift bestimmt nämlich, daß Geheimnisse, die im Rahmen freiwilliger Beratung, Untersuchung oder Begutachtung gesammelt wurden, bei der Erfüllung anderer Aufgaben nicht verwertet werden dürfen. Eine Ausnahme sieht das Gesetz nur vor zur Abwehr von Gefahren für Leben oder Gesundheit Dritter.

  Die Abschottung der Daten, die bei der freiwilligen Inanspruchnahme gewonnen werden, etwa gegenüber hoheitlicher Tätigkeit des Gesundheitsamtes, muß durch organisatorische und personelle Maßnahmen gewährleistet werden.

  Ebenso problematisch wäre es, wenn Daten aus einer Nebentätigkeit eines Amtsarztes (z.B. vertrauensärztliche Untersuchungen für einen Sozialversicherungsträger) in der Zentralkartei festgehalten würden. Auch solche Daten unterliegen dem Verbot anderweitiger Verwertung nach Art. 6 GDG. Das Innenministerium hat meine Auffassung hierzu bestätigt und mitgeteilt, daß Nachweise und Erkenntnisse, die über Nebentätigkeiten erlangt wurden, nicht in der Zentralkartei erfaßt werden dürfen (siehe auch 2.3.2).

  Ein Hinweis auf bestimmte Erkrankungen etwa auf AIDS, darf sich aus der Zentraldatei nicht ergeben.

- Schwangerschaftkonfliktberatung

  Im Bereich der Gesundheitshilfe führen die Gesundheitsämter auch die nach dem Schwangeren-Beratungsgesetz (SchwBerG) vorgeschriebenen Beratungen durch. Zu deren Nachweis wird nach Art. 10 SchwBerG den Schwangeren eine Bestätigung ausgestellt. Die Durchschriften der Bestätigungen werden im Amt als Kartei gesammelt. In Art. 10 Abs. 2 SchwBerG ist der Inhalt der Bestätigung im einzelnen festgelegt. Danach darf nur der Tag der Beratung, Name, Geburtsdatum und Anschrift der Betroffenen sowie Name und Anschrift des Ausstellers festgehalten werden. Hier hat sich die Frage ergeben, ob weitere Angaben, etwa über die sozialen Verhältnisse der Betroffenen, auf der Durchschrift oder auf besonderen Unterlagen festgehalten werden dürfen. Nach Auffassung des Innenministeriums sind zusätzliche Angaben für eine ordnungsgemäße Dokumentation der Beratung nicht erforderlich.

Ich halte die Regelung, wonach die Bestätigung der Beratung und der Beleg für die Erteilung der Bestätigung sorgfältig aufzubewahren und nach fünf Jahren zu vernichten sind, für abschließend und eine Speicherung weiterer Informationen aus der Beratung für unzulässig.

- Datensicherung

  Nach Art. 15 Abs. 1 BayDSG sind auch manuell geführte Karteien mit den notwendigen und vertretbaren Maßnahmen gegen den Zugriff Unbefugter zu schützen. Die Kontrolle ergab hier noch umfangreiche Verbesserungsmöglichkeiten. Ich habe die betroffenen Ämter zur umgehenden Behebung der festgestellten Mängel aufgefordert und das Innenministerium gebeten, bei allen Gesundheitsämtern die notwendigen Datensicherungsmaßnahmen sicherzustellen. Das Innenministerium hat seine Unterstützung zugesagt.

- Löschung von Daten

  Die Kontrolle hat wiederholt Unsicherheit über den Zeitpunkt der Löschung von Speicherungen und der Vernichtung aussortierter Unterlagen ergeben. Ich habe das Innenministerium gebeten, den Gesundheitsämtern hierzu klare Hinweise zu geben.

2.3.2. Organisatorischer Datenschutz im Gesundheitsamt

Verschiedene Vorkommnisse in der Vergangenheit haben zu Überlegungen Anlaß gegeben, inwieweit aus datenschutzrechtlichen Gründen der hoheitliche Tätigkeitsbereich des Gesundheitsamtes von den sonstigen Aufgabenbereichen des Amtes in organisatorischer und personeller Hinsicht abzutrennen ist.

Nach Art. 6 Abs. 1 Gesundheitsdienstgesetz (GDG) dürfen die Gesundheitsbehörden personenbezogene Daten, die sie aufgrund freiwilliger Mitwirkung des Betroffenen erfahren, nicht für andere Aufgaben des Gesundheitsamtes verwerten.

Anhand des Organisationsschemas eines Städtischen Gesundheitsamts stellte ich allerdings fest, daß einzelne Abteilungen sowohl Aufgaben des Beratungsdienstes nach Art. 11 GDG als auch hoheitliche Aufgaben wahrnehmen. Ich habe deshalb gegenüber dem Gesundheitsamt angeregt, die einzelnen Arbeitsbereiche, deren Daten nach Art. 6 Abs. 1 GDG untereinander nicht verwendet werden dürfen, organisatorisch und personell deutlicher voneinander abzusetzen, als dies bisher der Fall ist.

Nach Mitteilung des Städtischen Gesundheitsamtes ist jedoch aus Gründen des Verwaltungsablaufes und der personellen, technischen und räumlichen Gegebenheiten eine stärkere Trennung der Beratungs- und Vorsorgebereiche von den hoheitlichen Aufgaben nicht möglich. Es seien lediglich folgende Einheiten ausschließlich dem einen oder anderen Bereich zuzuordnen:

- Informationszentrum,
- Kreisverwaltungsaufgaben,
- Anonyme AIDS-Beratungsstelle,
- Humangenetische Beratungsstelle,
- Sozialpsychiatrischer Dienst,
- Indikationsstelle zu § 218 StGB,
- Blutspendedienst.

Die restlichen Einheiten würden dagegen sowohl Beratungs- und Vorsorgeaufgaben als auch Ordnungsaufgaben wahrnehmen. Durch eine stärkere Trennung wäre die umfassende medizinische Betreuung der Bürger durch möglichst nur eine Anlaufstelle nicht mehr in jedem Fall gewährleistet. Eine doppelte Darstellung und Erhebung des Krankheitsverlaufes und seiner Hintergründe mit allen daraus resultierenden Nachteilen für den Bürger wären zwangsläufig die Folge. Eine stärkere Trennung von Beratungs- und Vorsorgeaufgaben einerseits und hoheitlichen Aufgaben andererseits könnte daher nicht als sinnvoll angesehen werden. Ich werde die Angelegenheit weiterverfolgen.

3. Sozialbehörden

3.1. Gesundheitsreformgesetz

Der Entwurf des umfangreichen Gesetzeswerks wurde mehrmals geändert. In den fortentwickelten Entwürfen war zu erkennen, daß gegenüber den Vorentwürfen eine Reihe von Forderungen des Datenschutzes verwirklicht wurden. Die verbliebenen Bedenken und Forderungen habe ich mit dem Staatsministerium für Arbeit und Sozialordnung erörtert. Das Ministerium hat sich gegenüber meinen Einwendungen und Vorschlägen sehr aufgeschlossen gezeigt: Die Gespräche führten zu Änderungsanträgen des Freistaates Bayern im Bundesrat, die dort auch übernommen wurden.

Der Arbeitskreis „Sozialwesen" der Datenschutzbeauftragten hat sich unter meiner Federführung zweimal mit dem Gesetzentwurf befaßt. Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat am 6. Juni 1988 den Gesetzentwurf beraten und hierzu einen Beschluß gefaßt.

Der Ausschuß für Arbeit und Sozialordnung des Deutschen Bundestags hat die Vorschriften über den Schutz der Gesundheitsdaten gegenüber dem Regierungsentwurf in wichtigen Punkten geändert. Nach Auffassung des Bundesbeauftragten für den Datenschutz sind damit alle datenschutzrechtlichen Mängel der Gesundheitsreform beseitigt. Der Datenschutz der Patienten ist auch künftig gewährleistet.

3.2. Sozialversicherungsausweisgesetz

Der Gesetzentwurf zur Einführung eines Sozialversicherungsausweises wurde im Herbst 1988 im Bundestag eingebracht. Vorher hatten die Datenschutzbeauftragten von Bund und Ländern wiederholt über eine gemeinsame Stellungnahme zur Erhebung und Verarbeitung personenbezogener Daten im Zusammenhang mit der Einführung eines Sozialversicherungsausweises beraten. Sie sind jedoch zu keiner gemeinsamen Wertung gelangt. Die Meinungen reichten von vollständiger Ablehnung bis zu der Auffassung, der Gesetzentwurf sei im Grundsatz akzeptabel und nur in einzelnen Punkten verbesserungsbedürftig.

Die Einführung eines Sozialversicherungsausweises ist nach meiner Überzeugung ein geeignetes und grundsätzlich auch verhältnismäßiges Mittel, die Schwarzarbeit wirksamer zu bekämpfen, die Erschleichung von Sozialleistungen zu unterbinden und den Mißbrauch der Sozialversicherungsfreiheit bei geringfügiger Beschäftigung (450 DM-Grenze) zu erschweren. Eingeschlossen in diese positive Bewertung ist

die Verwendung der Rentenversicherungsnummer zur Erleichterung der Mißbrauchskontrolle. Die Rentenversicherungsnummer als Sozialversicherungsnummer ist in der Vergangenheit völlig zu Unrecht zum sozialpolitischen Tabu erklärt worden. Es gibt keine verfassungsrechtlichen Gründe gegen ihre Verwendung im Sozialversicherungsausweis.

Ich habe allerdings nach wie vor Zweifel, ob die Einrichtung einer Zentraldatei geringfügig beschäftigter Personen für die ganze Bundesrepublik notwendig ist. Nach dem Gesetzentwurf sollen geringfügig beschäftigte Personen bei der Datenstelle der Rentenversicherungsträger mit Anschrift und Angaben über Arbeitgeber, Beschäftigungsdauer und Beschäftigungsart gespeichert werden. Vielfach handelt es sich dabei um Schüler, Ferienjobber, Werkstudenten und Hausfrauen mit Nebenbeschäftigungen.

Bis jetzt konnte ich mich nicht davon überzeugen, daß das vom Gesetzentwurf angestrebte Ziel, die mißbräuchliche Ausnutzung der Sozialversicherungsfreiheit zu verhindern oder zu erschweren, nicht auf weniger aufwendige und bürokratische Weise, mit geringerem Eingriff in die Persönlichkeitsrechte der Betroffenen und ohne bundeszentrale Erfassung erreicht werden kann. Mißbrauchsfälle können in den meisten Fällen durch die einzelnen Krankenkassen, denen die geringfügig beschäftigten Personen von den Arbeitgebern zu melden sein werden, aufgedeckt werden. Allenfalls könnte an einen regional beschränkten Datenabgleich gedacht werden. Eine bundesweite Zentraldatei einzurichten, um die verbleibenden wenigen Fälle durch Abgleich zu erkennen, erscheint daher als hoher Aufwand. Ob der damit verbundene Eingriff in das informationelle Selbstbestimmungsrecht der Betroffenen noch verhältnismäßig ist, bedarf weiterer Prüfung.

Für nicht nötig und daher auch aus datenschutzrechtlicher Sicht für bedenklich halte ich hingegen die Einbeziehung von Personen unter 18 Jahren in die automatisierte Kontrolle geringfügig Beschäftigter. Bei Personen unter 18 Jahren dürfte ein Mißbrauch der Geringfügigkeitsgrenze nur eine sehr untergeordnete Rolle spielen. Im übrigen dürfte die Einbeziehung der geringfügig beschäftigten Jugendlichen in die Meldepflicht bei der Bevölkerung kaum auf Verständnis stoßen. Das gilt vor allem für kurzfristige Beschäftigungen wie etwa Ballholen beim Tennis oder Golf und ähnliche völlig untergeordnete Tätigkeiten. In den seltensten Fällen werden sich die „Arbeitgeber" ihrer Meldepflicht bewußt werden.

3.3. Prüfung bei einem Sozialamt

Bei der Prüfung eines Sozialamtes konnte ich mich davon überzeugen, daß die Vorschriften zum Schutz der Sozialdaten (SGB X) und die daneben geltenden Bestimmungen des Bundesdatenschutzgesetzes in erfreulicher Weise beachtet werden.

Ich habe mein Hauptaugenmerk auf die maschinell geführten Dateien der Sozialhilfeempfänger und Empfänger von Kriegsopferfürsorge gerichtet. Auch eine Reihe manuell geführter Karteien (DDR-Besucher, Asylanten, Tbc-Hilfe u. a.) wurden überprüft. Anhaltspunkte für eine unzulässige Datenspeicherung haben sich dabei nicht ergeben.

Ein weiterer Prüfungsschwerpunkt betraf die Verknüpfung der Sozialhilfedaten mit anderen Leistungen (z. B. Wohngeld, Ausbildungsförderung, Jugendhilfe) sowie die Übermittlung von Sozialhilfedaten an andere Stellen (z. B. Wohnungsvermieter, Sozialdienste, Ausländeramt u. ä.). Zu rügen war lediglich, daß bei mehreren vom Sozialamt selbst entwickelten Erhebungsbögen der Hinweis auf die Rechtsgrundlage oder die Freiwilligkeit der Angaben gemäß § 9 Abs. 2 BDSG fehlte. Das Sozialamt hat eine Ergänzung der Formulare zugesagt.

3.4. Wahrung des Sozialgeheimnisses durch kreisangehörige Gemeinden

Immer wieder taucht in der Praxis die Frage auf, ob kreisangehörige Gemeinden die Vorschriften über den Schutz der Sozialdaten zu beachten haben, wenn sie – ohne selbst Sozialleistungsträger zu sein – bei der Gewährung von Sozialleistungen mitwirken. Das Sozialgesetzbuch, die Reichsversicherungsordnung, das Bundessozialhilfegesetz und andere Sozialgesetze sehen diese Mitwirkung z. B. bei der Antragstellung vor. Andererseits enthält § 35 SGB I eine abschließende Aufzählung der Stellen, die das Sozialgeheimnis zu wahren haben. In dieser Aufzählung sind die kreisangehörigen Gemeinden nicht enthalten. Anfragen bei den Gemeinden sind besonders ergiebig, weil die bei ihnen gesammelten Unterlagen aus dem Bereich der gesetzlichen Sozialversicherung in manchen Fällen viele Jahrzehnte zurückreichen. Vergleichbare Unterlagen bei den Sozialleistungsträgern sind oft durch Kriegseinwirkung verlorengegangen. Als Interessenten für die genannten Daten treten daher die Sozialleistungsträger, Sozialforscher und zeitgeschichtliche Forscher, aber auch Organisationen wie der Internationale Suchdienst des Roten Kreuzes (zur Feststellung ausländischer Zwangsarbeiter während des „Dritten Reiches") an die Gemeinden heran.

Ich vertrete die Auffassung, daß die Gemeinden die Vorschriften über den Schutz der Sozialdaten zu beachten haben. Mit dem Staatsministerium für Arbeit und Sozialordnung bin ich der Ansicht, daß die Gemeinden, bei denen Anträge auf Sozialleistungen eingereicht werden (§ 16 Abs. 1 Satz 2 SGB I), kraft Gesetzes Aufgaben des jeweiligen Leistungsträgers erfüllen. Sie werden somit als verlängerter Arm des jeweiligen Leistungsträgers, nicht aber als eigenständige Behörde tätig. Die Gemeinden unterliegen folglich als „Erfüllungsgehilfen" eines Leistungsträgers der Pflicht, das Sozialgeheimnis zu wahren (§ 35 Abs. 1 Satz 1 SGB I). Das Sozialgeheimnis erfaßt auch Listen, die vor dem Inkrafttreten des SGB erstellt worden sind. Auch im Ausland lebende Versicherte haben einen Anspruch auf Wahrung ihrer Geheimnisse. Das Gebot der Geheimhaltung dauert über den Tod des Versicherten hinaus an.

3.5. Angabe des Arbeitgebers auf Krankenscheinen und Rezepten

In meinem 7. Tätigkeitsbericht habe ich unter Punkt 4.10 geschildert, daß auf den bisher verwendeten Vordrucken der gesetzlichen Krankenversicherung (Krankenscheine, Überweisungsscheine, Rezepte) die Angabe des Arbeitgebers des Versicherten vorgesehen war. Auf diesem Weg wurde allerdings auch die Arbeitslosigkeit des Versicherten einer Reihe von Stellen (Arzt, Apotheker, Masseur, Taxifahrer usw.) bekannt.

Die Bemühungen des Bundesbeauftragten und aller Landesbeauftragten für den Datenschutz um Änderung der genannten Vordrucke hatten Erfolg. Seit dem 1. Januar 1988

wird auf den Vordrucken anstelle des Arbeitgebers die Mitgliedsnummer des Versicherten eingetragen.

Damit erfahren Dritte künftig über Krankenscheine, Überweisungsscheine und Rezepte weder den Arbeitgeber noch die Tatsache der Arbeitslosigkeit.

3.6. Unzulässige Werbung mit Sozialdaten durch Privatfirma

Ein Krankenkassenverband machte mich auf den Mißbrauch von Sozialdaten durch eine Privatfirma aufmerksam: In einem Schreiben an eine Krankenkasse hatte ein Hersteller seine medizinischen Produkte vorgestellt. Als Argumentationshilfe hatte er dabei ein Verzeichnis der Krankenkassen beigelegt, mit denen er bereits in Geschäftsverbindung stand. Dieses Verzeichnis wies neben den Krankenkassen auch die Namen von Personen aus, welche die Produkte des Herstellers offenbar von der Kasse ersetzt erhalten hatten. Aus der Beschreibung der Produkte des Herstellers konnten außerdem Schlüsse auf die Art der Erkrankung dieser Personen gezogen werden.

Da der Hersteller als privates Unternehmen nicht unter die Kontrollzuständigkeit des Bayer. Datenschutzbeauftragten fällt, habe ich die für seinen Sitz zuständige Bezirksregierung eingeschaltet. Diese rügte den Hersteller, daß die Weitergabe der Namen der Kassenpatienten an andere Kassen unzulässig war. Um künftig derartige Verstöße zu verhindern, unterrichtete ich die Arbeitsgemeinschaft der bayerischen Krankenkassenverbände über den Vorfall und regte an, bei der Genehmigung von Heil- und Hilfsmitteln die künftige Verhaltensweise der Firma zu überprüfen und gegebenenfalls geeignete Maßnahmen zur Verhinderung weiterer datenschutzrechtlicher Verstöße zu ergreifen. Die Herstellerfirma hat mir inzwischen versichert, bei ihrer Werbung künftig den Datenschutz zu beachten.

3.7. Verwendung der Rentenversicherungsnummer beim Zeitschriftenversand durch eine gesetzliche Krankenkasse

Die Mitglieder gesetzlicher Krankenkassen erhalten regelmäßig Informationsschriften. Diese werden mit einem Adreßaufkleber versehen und durch die Post zugesandt. Ist die Zustellung wegen einer Wohnungsänderung des Versicherten nicht möglich, so vermerkt der Postbote dies oder die neue Adresse auf dem Aufkleber und sendet diesen an die Krankenkasse zurück. Die Krankenkasse benutzt die übersandten Aufkleber zur Bereinigung ihres Adreßbestandes. Damit die Kasse die Person des Versicherten dabei leichter feststellen kann, wird auf den Adreßaufklebern neben der Zustelladresse des Versicherten auch ein numerischer Ordnungsbegriff aufgedruckt. Ein Bürger hat sich darüber beschwert, daß die Krankenkasse hierzu seine Rentenversicherungsnummer verwendet habe, aus der sein Geburtsdatum entnommen werden könne.

Ich habe gegenüber der Krankenkasse die Auffassung vertreten, daß es zur Erleichterung der Identifikation des angeschriebenen Versicherten nicht erforderlich ist, als Ordnungsbegriff die Rentenversicherungsnummer zu verwenden (§ 18 f SGB IV). Die Krankenkasse hat das eingesehen und verwendet nunmehr eine neutrale Ordnungsnummer, die keine weiteren personenbezogenen Rückschlüsse auf den Adressaten zuläßt.

4. Polizei

4.1. Zur Lage des Datenschutzes

Die Polizei sieht sich einer wachsenden Kriminalität gegenüber. Gleichzeitig steht sie unter dem Druck, die Aufklärungsquote zu verbessern. Die Mittel zur Erhöhung der Polizeistärke sind begrenzt. In dieser Situation dürfen der Polizei unter Berufung auf den Datenschutz durch die Gesetzgebung und die Kontrollpraxis keine vom Persönlichkeitsschutz nicht geforderten Beschränkungen auferlegt werden. Allerdings muß die Informationstätigkeit der Polizei plausibel und für den Datenschutzbeauftragten rechtlich nachvollziehbar sein.

Als Ergebnis meiner umfangreichen und intensivierten Kontrollen der polizeilichen Informationstätigkeit kann ich feststellen, daß die Zahl der zu beanstandenden Datenschutz-Fehler deutlich abgenommen hat. Die Polizei verdient beim Datenschutz das Vertrauen der Bürger.

Um die Berechtigung dieses Vertrauens noch stärker nach außen zu dokumentieren und eventuelle Datenschutzverstöße aufdecken zu können, dränge ich jedoch darauf – übrigens nicht nur bei der Polizei – das Abfragen aus Dateien zu protokollieren. Soweit dies heute schon geschieht, hat sich die Protokollierung aus meiner Sicht bewährt. Sie ist neben einer Erleichterung der datenschutzrechtlichen Kontrolle geeignet, die Versuchung zum Mißbrauch zu verringern und Fehlentwicklungen schon im Ansatz zu erkennen.

Dies gilt auch im Hinblick auf den sich bei der Polizei abzeichnenden umfangreichen Einsatz von Personal-Computern. Dieser wird zum Teil völlig neue Überlegungen zur Gewährleistung des Datenschutzes erfordern. Hier sind Polizeibehörden und Datenschutzbeauftragter gleichermaßen gefordert (siehe auch 21.1.3.).

4.2. Schwerpunkte meiner Tätigkeit

Mehr noch als in den vergangenen Jahren habe ich den Schwerpunkt meiner Tätigkeit im polizeilichen Bereich auf Prüfungen von Polizeibehörden gelegt. Neben allgemeinen Querschnittsprüfungen habe ich der besonderen Aktualität wegen die im Zusammenhang mit der Volkszählung und der WAW stehenden Datenspeicherungen kontrolliert. Daneben gaben wieder zahlreiche Eingaben von Bürgern Anlaß zur Prüfung polizeilicher Datenverarbeitung.

Ein weiterer Schwerpunkt meiner Arbeit liegt auf der Beratung. So habe ich ständig Kontakt mit der polizeilichen Praxis, beantworte Fragen zum polizeilichen Alltagsbetrieb und äußere mich außerdem auf Anforderung des Staatsministeriums des Innern zu Automationsvorhaben sowie zu neuen Rechts- und Verwaltungsvorschriften im Sicherheitsbereich. Ich meine, gerade mit dieser Beratungstätigkeit ist es mir gelungen, das Spannungsverhältnis zwischen Polizei und Datenschutz weitgehend abzubauen und stattdessen vertrauensvolle, konstruktive Zusammenarbeit zu erreichen.

4.3. Novellierung des Polizeiaufgabengesetzes (PAG)

Die Novellierung des Polizeiaufgabengesetzes (PAG) noch in dieser Legislaturperiode ist dringend, weil andernfalls der Polizei die für die Erfüllung ihrer Aufgaben notwendigen Informationen entzogen werden könnten.

Notwendigkeit der Novellierung

Der Bayer. Verfassungsgerichtshof hat in seiner Entscheidung vom 9.7.1985 ausdrücklich festgestellt, daß es derzeit für die Führung von personenbezogenen kriminalpolizeilichen Sammlungen an der gebotenen gesetzlichen Rechtsgrundlage fehle. Unter Hinweis auf seine bisherige Rechtsprechung weist der Verfassungsgerichtshof allerdings darauf hin, daß bestehende Regelungslücken für eine gewisse Übergangszeit hingenommen werden könnten, damit der Gesetzgeber ausreichend Zeit für die Beratung und den Erlaß der erforderlichen Vorschriften zur Verfügung hat. Derzeit dürfte diese Übergangszeit trotz anderslautender Entscheidungen mehrerer Verwaltungsgerichte noch nicht abgelaufen sein. Derartige verwaltungsgerichtliche Entscheidungen machen aber den dringenden Handlungsbedarf in der Gesetzgebung deutlich.

Dabei verkenne ich nicht, daß eine Abstimmung der Regelungen im Polizeiaufgabengesetz mit dem Gesetz zum Bundeskriminalamt (BKA) und für den Bundesgrenzschutz und insbesondere mit den neu zu schaffenden Vorschriften in der Strafprozeßordnung wünschenswert wäre. Dies darf jedoch nicht zu einer ungebührlichen Verzögerung der Novellierung des bayerischen Polizeirechts führen. Zwar liegt aus dem Bundesjustizministerium ein erster Entwurf zu einer Ergänzung der Strafprozeßordnung um Vorschriften zur strafprozessualen Datenverarbeitung vor. Auch gibt es inzwischen einen Entwurf zur Novellierung des BKA-Gesetzes. Doch bestehen insbesondere im Hinblick auf die Komplexität der Materie bei der Strafprozeßordnung nachhaltige Zweifel, ob deren Novellierung im Hinblick auf die notwendige Änderung des Polizeiaufgabengesetzes zeitgerecht abgeschlossen werden kann. Deshalb kann mit der Novellierung des Polizeiaufgabengesetzes nicht bis zur Verabschiedung der Novelle zur Strafprozeßordnung gewartet werden.

Auf die möglichen Folgen eines Ausbleibens der Novellierung habe ich die Staatskanzlei und das Innenministerium hingewiesen. Die Staatsregierung hat gegenüber dem Landtag erklärt, sie beabsichtige die Novelle zum Polizeiaufgabengesetz dem Landtag so rechtzeitig zuzuleiten, daß die parlamentarischen Beratungen noch vor der Sommerpause 1989 aufgenommen werden können.

4.4. Prüfungen

Neben den aufgrund von Eingaben notwendigen Kontrollen habe ich insbesondere bei folgenden Behörden zum Teil mehrfach Prüfungen vor Ort vorgenommen:

Landeskriminalamt
Polizeipräsidium Mittelfranken
mit Polizeidirektionen Ansbach, Erlangen, Fürth und Nürnberg
Polizeipräsidium Oberfranken
mit Polizeidirektionen Bamberg, Bayreuth, Coburg und Hof
Polizeipräsidium Niederbayern/Oberpfalz
mit Polizeidirektionen Landshut und Amberg
Polizeipräsidium München
Grenzpolizeiinspektion Freilassing

Bei diesen Prüfungen mache ich mir die Prüferfahrungen der vergangenen Jahre zunutze und greife ganz bewußt fehlerträchtige Bereiche heraus. Dennoch bleiben die Prüfungen letztlich auf Stichproben beschränkt.

Insgesamt lassen diese generellen Prüfungen in Verbindung mit den aufgrund von Bürgereingaben veranlaßten Kontrollen von Einzelfällen doch einen guten Überblick über die polizeiliche Datenverarbeitung zu. Deshalb kommt auch meiner Feststellung, daß die Polizei im wesentlichen die Datenschutzbestimmungen sorgfältig beachtet und Datenschutzverstöße die Ausnahme sind, Allgemeingültigkeit zu.

4.4.1. Kriminalaktennachweis (KAN)

Der in Dateiform geführte KAN dient dem Nachweis von Kriminalakten auf der Ebene der Polizeidirektionen und besonderer Ballungsräume (Ballungsraum-KAN), auf Landes- und Bundesebene.

Prüfungen des KAN führe ich nun bereits seit mehreren Jahren durch. Inzwischen hat die Zahl der Fehler bei dieser polizeilichen Datenverarbeitung deutlich abgenommen. Nur bei einer einzigen Polizeidirektion habe ich in Teilbereichen noch überdurchschnittlich viele Fehler festgestellt, die aber nach Eingang meines Prüfberichts bereinigt worden sind.

Einer der Gründe für den erfreulichen Rückgang der Fehler liegt wohl darin begründet, daß inzwischen einzelne Polizeipräsidien polizeiinterne Datenschutzprüfungen teilweise regelmäßig, teilweise von Fall zu Fall durchführen. Hierbei werden offensichtlich die Feststellungen meiner früheren Prüfungen berücksichtigt. Diese Selbstkontrolle empfehle ich allen Polizeibehörden.

Wenn ich im folgenden über einzelne Fehlertypen berichte, dann darf dies nicht zu dem falschen Schluß führen, diese Fehler träten massenhaft auf. Trotzdem sollte die Polizei auch bei der künftigen Sachbearbeitung auf diese Bereiche achten. Ich habe diese Bereiche des KAN deshalb intensiver geprüft, weil sie sich in der Vergangenheit als besonders fehlerträchtig erwiesen haben.

Kinder, alte Menschen und Ordnungswidrigkeiten

Kinder werden nur noch in ganz wenigen Ausnahmefällen im KAN gespeichert. Ist eine derartige Speicherung im Einzelfall erforderlich, lege ich Wert darauf, daß sich aus dem Akt eindeutig ergibt, weshalb trotz der Strafunmündigkeit des Kindes eine Speicherung erforderlich war. Diese Begründung habe ich im Regelfall vorgefunden. Zu beachten ist jedoch, daß für den Fall der Straffälligkeit mehrerer Kinder geprüft werden muß, ob die besonderen Speicherungsvoraussetzungen (beispielsweise besondere kriminelle Energie) nur bei einem Kind oder tatsächlich bei allen Kindern vorgelegen haben. Zulässig ist die Aufnahme nur derjenigen Kinder, bei denen die besonderen Speicherungsvoraussetzungen vorliegen.

Die Zahl der über 70 Jahre alten Senioren im Kriminalaktennachweis war deutlich geringer als bei früheren Prüfungen. Die Stichproben haben gezeigt, daß die Speicherungen im wesentlichen sachlich gerechtfertigt waren. Soweit im Einzelfall die Speicherung zur Aufgabenerfüllung der Polizei nicht mehr erforderlich war, hat die geprüfte Behörde meist bereits während der Prüfung die Daten gelöscht. Die verkürzte Aussonderungsfrist (fünf Jahre) wurde bei diesem Personenkreis in aller Regel beachtet.

Bei den Ordnungswidrigkeiten hat die Polizei erkannt, daß eine Speicherung nur in besonders begründeten Fällen erforderlich und zulässig ist. Soweit bei einzelnen

Polizeidirektionen die Zahl der gespeicherten Ordnungswidrigkeiten über dem Landesdurchschnitt lag, war dies in lokalen Besonderheiten (z. B. Ausländerunterkunft) begründet. Erfreulich ist auch meine Feststellung, daß bei Ordnungswidrigkeiten im Regelfall eine deutlich, zum Teil auf drei Jahre verkürzte Aussonderungsprüffrist vergeben worden ist. Nur in wenigen Fällen habe ich sachlich nicht gerechtfertigte 10-jährige Aussonderungsfristen bei Ordnungswidrigkeiten vorgefunden.

Speicherungsebenen im KAN

Die Vergabe der sog. „KAN-Merker", die zur bundesweiten Abrufbarkeit der KAN-Daten führen, entspricht nun weitgehend den Richtlinien. Nach wie vor ist hier jedoch Sorgfalt geboten.

- So wird manchmal der Begriff „gewohnheitsmäßig" zu Unrecht mit Wiederholungstätern gleichgesetzt. Wenn ich bei den Stichprobenkontrollen solche Fehler festgestellt habe, habe ich von der geprüften Behörde eine vollständige Prüfung der Vergabe dieses Merkers verlangt.
- Teilweise werden noch „Bagatelldelikte" wie Ladendiebstahl durch die Vergabe von KAN-Merkern im Bundes-KAN gespeichert. Darin liegt eine unverhältnismäßige Beeinträchtigung schutzwürdiger Belange der Betroffenen. Außerdem werden die polizeilichen Informationssysteme mit wenig bedeutsamen Daten belastet.
- Für die Vergabe des KAN-Merkers „planmäßig und überörtlich" reicht eine „nichtdeutsche Staatsangehörigkeit" ebenso wenig aus wie eine einmalige Straftat in einem anderen polizeilichen Zuständigkeitsbereich. Liegen nur zwei Ladendiebstähle vor und weichen Wohnsitz und Tatort voneinander ab, so kann noch nicht von planmäßigem überörtlichem Handeln gesprochen werden.

Weitere Schulung und interne polizeiliche Datenschutzkontrolle können dazu beitragen, solche und ähnliche Fehler auszumerzen.

Sonstige polizeiliche Gefahrenabwehr

Unter dem Schlüssel „sonstige polizeiliche Gefahrenabwehr" kann die Polizei Daten solcher Personen speichern, von denen sie in Erfüllung ihrer nach dem Polizeiaufgabengesetz zugewiesenen Aufgabe der Gefahrenabwehr annehmen kann, daß sie erneut „polizeilich" in Erscheinung treten werden. In der Regel speichern die einzelnen Polizeidirektionen unter diesem Schlüssel nur einige wenige Personen. Bei einer Polizeidirektion habe ich allerdings zahlreiche Speicherungen festgestellt, die sich bei Stichproben überwiegend als unrichtig erwiesen haben. Sie wurden inzwischen nach einer vollständigen Überprüfung deutlich verringert.

Generell gilt: Es ist unzulässig, Daten, die nach den polizeilichen Richtlinien zu löschen sind, unter diesem Schlüssel erneut einzuspeichern. Nicht hierher gehören Speicherungen über Freisprüche oder Hinweise auf alte Vorstrafen und Urteile, über die keine Unterlagen mehr bei der Polizeibehörde vorhanden waren. Teilweise werden unter diesem Schlüssel fälschlicherweise reine Tätigkeitsnachweise gespeichert wie die Erledigung von Ersuchen anderer Dienststellen, ein Hafturlaub oder der Vollzug eines Haftbefehls. Solche Vorgänge gehören in die Vorgangsverwaltung, aber nicht in den KAN. Alte Strafurteile dürfen nicht unter diesem Schlüssel gesammelt werden. Zu beachten ist bei diesem Schlüssel auch die richtige Vergabe des Aussonderungsdatums; eine 10-jährige Frist ist hier in den meisten Fällen nicht angemessen.

Zusammenfassend weise ich darauf hin, daß der Schlüssel „sonstige polizeiliche Gefahrenabwehr" nicht zum Auffangbecken für alle die Vorgänge werden darf, für deren Speicherung die Richtlinien keinen Raum lassen.

Aussonderungsprüffristen

Eine unbemerkte Überschreitung der Aussonderungsprüffrist und damit eine unzulässige Speicherungsdauer können durch den Einsatz der elektronischen Datenverarbeitung vermieden werden. Die Nichtbeachtung dieser Frist, die sich bei herkömmlicher Karteiführung zumeist als Mengenproblem oder organisatorisches Problem darstellte und in der Vergangenheit wiederholt von mir beanstandet wurde, ist durch automatische Überwachung ausgeschlossen. Alle Kriminalakten, die in einem bestimmten Kalendermonat zur Aussonderungsprüfung heranstehen, werden aufgezeigt und können durch unmittelbare Beiziehung der Akte überprüft werden. Voraussetzung ist allerdings, daß diese Fristen richtig vergeben werden.

Tatsächlich haben auch bei der Vergabe der Aussonderungsprüffristen meine steten Hinweise Früchte getragen. Beanstandungen sind hier nun die Ausnahme. Bei der Fristenvergabe lege ich Wert darauf, daß der polizeiliche Sachbearbeiter, der den Vorgang bearbeitet hat und deshalb am besten eine Täterprognose abgeben kann, die Entscheidung über die Dauer der notwendigen Speicherung trifft.

Die Polizeidirektion Ansbach hat ein besonders empfehlenswertes Aussonderungsprüfverfahren entwickelt. Die einzelnen Polizeiinspektionen im Direktionsbereich erhalten kurz vor Ablauf der Aussonderungsfrist einen schriftlichen Hinweis. Sollte eine Polizeidienststelle im Einzelfall die weitere Speicherung der Daten für erforderlich halten, hat sie dies auf dem Hinweisblatt kurz zu begründen.

Ballungsraum-KAN

In den Großräumen München und Nürnberg sind in den Jahren 1987 und 1988 die sogenannten Ballungsraum-KAN-Verfahren eingeführt worden. Weil in diesen Großräumen eine Abschottung der Datenverarbeitung auf einzelne Direktionen wegen der Mobilität der Täter nicht sachgerecht erschienen ist, werden hierbei die ansonsten jeweils bei den einzelnen Polizeidirektionen getrennt geführten Daten zu einer einzigen Datei zusammengefaßt. Im Großraum Nürnberg betrifft dies die KAN-Daten der Polizeidirektionen Nürnberg, Fürth und Erlangen, in München die KAN-Daten der zum Polizeipräsidium München gehörenden 4 Polizeidirektionen.

Bei meinen Prüfungen habe ich neben den sonstigen Prüfpunkten beim KAN darauf geachtet, ob durch die Zusammenführung mehrerer Direktionsbereiche die schutzwürdigen Belange der Bürger über Gebühr tangiert werden. Eine Änderung für den Betroffenen bringt zweifelsohne die Tatsache, daß die Aktenaussonderungen nun nicht mehr im einzelnen Direktionsbereich, sondern für die zusammengefaßten Direktionen einheitlich vorgenommen werden. Das kann im Einzelfall dazu führen, daß Daten und die

dazugehörigen Akten weitergeführt werden, obwohl deren Aussonderungsprüffristen bei einer Direktion abgelaufen sind.

Das Ballungsraum-KAN-Verfahren bietet außerdem einige neue Auswertungsmöglichkeiten. Einem eventuellen Mißbrauch wird durch die Vergabe von Zugriffsberechtigungen begegnet, die auf einige wenige Personen mit hervorgehobenen Funktionen beschränkt sind. Auch diesem Gebiet werde ich weiterhin meine Aufmerksamkeit schenken.

Datenschutzverstöße, die etwa durch die Besonderheiten des Ballungsraum-KAN bedingt waren, habe ich nicht festgestellt.

4.4.2. Polizeipräsidium München

Das Ergebnis meiner letzten datenschutzrechtlichen Prüfung beim Polizeipräsidium München im Jahr 1986 hatte ich zurückhaltend mit den Worten kommentiert, daß es mich „recht nachdenklich stimmt". Ich hatte allerdings auch festgestellt, daß die Versäumnisse in der Vergangenheit liegen. Als Resümee meiner diesjährigen Prüfung kann ich nun eindeutig feststellen, daß sich die Situation des Datenschutzes beim Polizeipräsidium München nachhaltig gebessert hat.

Das Polizeipräsidium München hat die Zahl seiner Dateien verringert und hierbei insbesondere auf solche Sammlungen verzichtet, die nahezu parallel ohne Abstimmung bei verschiedenen Dienststellen geführt worden sind. Inzwischen liegt auch eine aktuelle und vollständige Übersicht über sämtliche bei dieser Behörde geführten Dateien vor. Außerdem bestehen nun, wie für alle kartei- und dateiführenden Stellen erforderlich, für alle Karteien Feststellungsanordnungen und für alle automatisierten Dateien Errichtungsanordnungen, die Zweck und Inhalt der Dateien festlegen. Dies ist eine wichtige Voraussetzung dafür, daß auch behördenintern die Rechtmäßigkeit der Datenverarbeitung überprüft werden kann. Die einzige Kartei, die sich erübrigt hatte, wurde noch während meiner Prüfung vernichtet.

Schlagwortartig kann zu einigen früher beanstandeten Karteien folgendes festgestellt werden:

- Die Kartei der erkennungsdienstlichen Behandlungen, in der bei der letzten Prüfung noch ca. 76.500 Personen erfaßt waren, ist nahezu aufgelöst. Ihre Aufgabe wird von einer Datengruppe im Informationssystem INPOL übernommen.
- Die Kartei über Stadtstreicher und Bettler trägt nun keinen diskriminierenden Titel mehr. Der Umfang dieser Kartei ist im übrigen sehr klein; keine Information liegt länger als ein Jahr zurück. Es handelt sich somit um aktuelle Informationen. Eine gesonderte Kennzeichnung für Alkoholkranke besteht nicht mehr.
- Transvestiten werden wegen dieser Eigenschaft überhaupt nicht mehr in einer gesonderten Kartei geführt.
- In der Kartei „strafbare Homosexualität und männliche Prostitution" ist der Datenbestand ebenfalls drastisch verringert worden und enthält nur noch solche Personen, die Beschuldigte oder Betroffene eines einschlägigen Straf- oder Ordnungswidrigkeiten-Verfahrens waren.

Bei den Dateien über bekannte und unbekannte Täter sind weitere Datensicherungsmaßnahmen getroffen worden, die den Zugriff Unbefugter ausschließen. Auch stimmt nun die Verfahrensbeschreibung der Datei „Bekannte Täter" mit dem tatsächlich eingesetzten Verfahren überein. Stichprobenartige Überprüfungen nach verschiedenen Merkmalen, z.B. „Taubstumme", „Skinhead", „Schlitzaugen", „Transvestiten", „Polit" haben nur noch wenige Fehler erbracht. Gelegentlich gab es Schwierigkeiten bei der richtigen Bewertung von „Fußballrandalierern", die ausweislich des Akteninhalts manchmal zu Unrecht als „Skinheads" bezeichnet oder mit dem Merker „Polit" versehen worden sind.

Soweit bei der Prüfung der verschiedenen Dateien Kriminalakten herangezogen worden sind, haben sich allerdings die bei früheren Prüfungen festgestellten Schwachpunkte der Aktenführung erneut bestätigt. Nachhaltige Besserung ist hier wohl erst zu erwarten, wenn der gesamte Aktenbestand in der Datei „Kriminalaktennachweis" erfaßt und hierbei bereinigt sein wird.

Wie bereits oben kurz erwähnt, wird seit Januar 1988 auch vom Polizeipräsidium München das Verfahren „Ballungsraum-KAN" in vollem Umfang betrieben. Bislang sind 63.000 Kriminalakten erfaßt. Meine nach etwa 20 verschiedenen Prüfansätzen durchgeführten Querschnittsprüfungen erbrachten folgendes Ergebnis:

Die bisherige Erfassung im Kriminalaktennachweis über wenige Monate zeigt, daß das Polizeipräsidium München bemüht ist, seinen Aktenbestand in möglichst kurzer Zeit im KAN nachzuweisen.

Die umfangreichen Stichproben machen allerdings deutlich, daß dieser neue automatisierte Nachweis von Kriminalakten dringend einer qualitativen Verbesserung bedarf. Diese habe ich in einem umfangreichen Prüfbericht angemahnt. Bei den festgestellten Fehlern ist zu berücksichtigen, daß bei einem neuen Verfahren üblicherweise Probleme auftreten. Ich gehe davon aus, daß durch gezielte Schulungsmaßnahmen und polizeiinterne Kontrollen die Qualität dieses neu angelegten und automatisiert geführten Datenbestandes deutlich verbessert wird.

Bei der Staatsschutzkartei (näheres siehe unter 4.10) sind keine besonderen Datenschutzverstöße festgestellt worden.

4.5. HIV-Infektionen und polizeiliche Datenverarbeitung

4.5.1. Speicherung in polizeilichen Informationssystemen

Gegen die Speicherung des personengebundenen Hinweises „ANST" (Ansteckungsgefahr) mit dem Zusatz „Vorsicht Blutkontakte" habe ich – wie bereits im 9. Tätigkeitsbericht dargelegt – keine datenschutzrechtlichen Bedenken, wenn folgende Voraussetzungen erfüllt sind:

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

Im Berichtszeitraum habe ich mehrfach die auf Veranlassung bayerischer Polizeibehörden vorgenommenen Speicherungen dieses Hinweises überprüft. Zunächst ist festzustellen, daß in Bayern, abgesehen von den Ballungsräumen München und Nürnberg, nur das Landeskriminalamt technisch in der Lage ist, derartige Speicherungen im „Personendatensatz" des Betroffenen vorzunehmen. Somit ist eine weitgehend einheitliche Sachbehandlung gewährleistet. In den Ballungsräumen sollte dafür Sorge getragen werden, daß dort nur jeweils eine Stelle zu derartigen Speicherungen befugt ist. Die Speicherung an zentralen Stellen erleichtert auch die datenschutzrechtlichen Kontrollen. Diese haben ergeben, daß die von mir aufgestellten Bedingungen für eine Speicherung des PHW „ANST – Vorsicht Blutkontakte" eingehalten worden sind. Daß Bayern sehr zurückhaltend mit der Speicherung dieses Hinweises ist, belegt im übrigen die Zahl von derzeit nur 108 Personen (Stand: 31.10.1988), bei denen dieser Hinweis hinzugefügt worden ist.

Durch eine beim Landeskriminalamt geführte manuelle Dokumentation der Unterlagen für diese Speicherungen ist deren Richtigkeit einfach nachzuprüfen (siehe auch 4.12.2).

4.5.2. Fehler im Einzelfall

Unter Überschriften wie „Angst vor Aids: Polizist vernahm Zeugen nur am Telefon" oder „Polizist lehnte Vernehmung von aids-verdächtigen Zeugen ab", berichteten die Medien über folgenden Vorfall:

Im Herbst 1986 ersuchte eine auswärtige Kriminalpolizeiinspektion das Polizeipräsidium München, zwei in München wohnhafte Zeugen in einer Brandsache zu vernehmen. Der Sachbearbeiter des Polizeipräsidiums München stellte bei der Vorbereitung dieser Zeugeneinvernahmen fest, daß zu einem der beiden Zeugen eine polizeiliche Personenakte vorlag. In dieser fand sich ein ärztlicher Untersuchungsbericht, der anläßlich einer polizeilich veranlaßten Blutentnahme wegen Verdachts einer Trunkenheitsfahrt erstellt worden war und der den Vermerk „AIDS" trug. Zur Person des zweiten zu vernehmenden Zeugen lagen keine Erkenntnisse vor. Daraufhin telefonierte der polizeiliche Sachbearbeiter mit der auswärtigen Kriminalpolizeiinspektion und fragte an, ob er beide Zeugen auch telefonisch vernehmen könne, weil er sich wegen deren AIDS-Erkrankung keiner Ansteckungsgefahr aussetzen wolle und im Hinblick auf die relativ geringe Bedeutung der Angelegenheit eine Vernehmung in Form der fernmündlichen Befragung der Zeugen ausreichend sei. Dem stimmte die auswärtige Kriminalpolizeiinspektion zu. Diese fernmündliche Anfrage wurde nun in dem Ermittlungsvorgang wegen der Brandsache vermerkt unter ausdrücklicher Nennung der beiden Zeugen und mit dem Hinweis auf deren Aids-Erkrankung. Damit bestand für die beiden Zeugen das Risiko, daß bei einer Akteneinsicht Dritte, auch Sachbearbeiter der Brandversicherung, von dieser behaupteten Aids-Erkrankung Kenntnis erlangen könnten.

Ich habe den Vorgang beanstandet: Wenn wegen relativ geringer Bedeutung des zugrundeliegenden Sachverhalts eine fernmündliche Vernehmung der beiden Zeugen ausreichend war, genügte es, diese Tatsache als Grund für die beabsichtigte fernmündliche Befragung anzugeben. Die telefonische Übermittlung der angeblichen AIDS-Erkrankung der beiden Zeugen an die auswärtige Kriminalpolizeiinspektion war deshalb nicht erforderlich und demnach unzulässig (Art. 17 Abs. 1 BayDSG). Für die Mitteilung der AIDS-Erkrankung des zweiten Zeugen lagen zudem keine ausreichenden Beweise zur Richtigkeit dieser Behauptung vor. Weil der Hinweis auf eine AIDS-Erkrankung für den Betroffenen auch erhebliche gesellschaftliche Nachteile mit sich bringen kann, muß bei Speicherung oder Übermittlung eines entsprechenden Hinweises mit besonderer Sorgfalt auf Richtigkeit und Erforderlichkeit geachtet werden.

4.6. Personengebundene Hinweise (PHW)

Zur Beschreibung bestimmter Eigenschaften der in polizeilichen Informationssystemen aufgenommenen Personen speichert die Polizei sog. personengebundene Hinweise. Dies können, wie bereits früher berichtet, Hinweise auf Prostitutionsausübung, Geisteskrankheit, Rauschgiftkonsum oder Bewaffnung sein, um nur einige dieser katalogmäßig aufgelisteten personengebundenen Hinweise zu nennen. Die Hinweise sollen der Polizei eine erste Einschätzung der gespeicherten Personen erlauben, um ggf. Vorkehrungen zur Eigensicherung des einschreitenden Beamten zu treffen oder Maßnahmen zum Schutz des Betroffenen vorzunehmen.

An der grundsätzlichen Notwendigkeit der Verwendung personengebundener Hinweise in polizeilichen Informationssystemen habe ich nie Zweifel gelassen. Allerdings waren mir hierbei zwei Gesichtspunkte wesentlich:

Die einzelnen personengebundenen Hinweise müssen für die polizeiliche Aufgabenerfüllung geeignet und dienlich sein und dürfen nicht außer Verhältnis zum angestrebten polizeilichen Zweck stehen. Außerdem muß bei der Aufnahme und weiteren Speicherung personengebundener Hinweise sichergestellt sein, daß Richtigkeit und Aktualität dieser Daten gewährleistet sind.

Aufgrund der verschiedenen Aktivitäten der Datenschutzbeauftragten haben die zuständigen Polizeigremien die Notwendigkeit der einzelnen personengebundenen Hinweise erneut geprüft und beschlossen, zwei weitere personengebundene Hinweise „Land-/ Stadtstreicher" und „häufig wechselnder Aufenthaltsort" entfallen zu lassen. Außerdem wird die Nutzung personengebundener Hinweise in der Haftdatei, die Hinweise über den Aufenthalt in Justizvollzugsanstalten enthält, eingestellt. Auch wurden die Laufzeiten für die einzelnen personengebundenen Hinweise exakt festgelegt und zum Teil verringert. Diese Reduzierung der Speicherung personengebundener Hinweise auf das für die polizeiliche Aufgabenerfüllung erforderliche Maß begrüße ich.

4.7. Beanstandungsfälle

Wie ich bereits eingangs ausgeführt habe, ist die Zahl der Beanstandungen gegenüber Polizeibehörden aufgrund der Eingaben von Bürgern sehr gering. Einen Einblick, unter welchen Voraussetzungen Beanstandungen auszusprechen sind, sollen die folgenden zwei Fälle geben:

1. Ein Polizeibeamter hat sich an mich mit der Beschwerde gewandt, daß die Tatsache, daß er mit seinem Privatwagen einige Parkverstöße begangen habe, von der für die Verfolgung von Ordnungswidrigkeiten zuständigen Polizeidienststelle an seine vorgesetzte Dienststelle übermittelt worden sei, mit der Folge der Einleitung eines dienstaufsichtsrechtlichen Verfahrens gegen ihn.

Diese Datenübermittlung von der Polizeistelle, die Ordnungswidrigkeiten bearbeitet, zur personalverwaltenden Stelle habe ich beanstandet. Auch wenn die Daten des betroffenen Beamten bei dieser Übermittlung innerhalb des Polizeibereichs verblieben sind, ist dieser Vorgang datenschutzrechtlich als Übermittlung zu bewerten. Für diese Übermittlung gibt es derzeit keine Rechtsgrundlage. Eine solche Unterrichtung des Dienstvorgesetzten von Angehörigen des öffentlichen Dienstes wird von der Rechtsprechung lediglich dann für nötig gehalten, wenn der Angehörige des öffentlichen Dienstes eine Straftat begangen hat, weil es zur Aufgabenerfüllung der dienstvorgesetzten Behörde gehört, Dienstvergehen disziplinarrechtlich zu ahnden. Ordnungswidrigkeiten führen grundsätzlich nicht zu disziplinarrechtlichen Maßnahmen. Nach der Rechtsprechung in Disziplinarsachen ist außerdienstliches, nichtkriminelles Verhalten eines Beamten nur dann disziplinarrechtlich zu verfolgen, wenn es dienstliche Belange berührt. Das private Verkehrsverhalten eines Polizeibeamten, der nicht im Bereich der Verkehrsüberwachung eingesetzt ist, ist grundsätzlich nicht geeignet, dienstliche Belange zu berühren. Im vorliegenden Fall war noch weiter zu berücksichtigen, daß es sich um keinen bedeutenden Verkehrsverstoß gehandelt hatte.

2. Über einen Abgeordneten bin ich auf folgenden Sachverhalt aufmerksam gemacht worden:

   Eine Frau, die auf offener Straße von einem Unbekannten geschlagen worden war, ist von einer Polizeibehörde geladen worden. Ihr sollten Lichtbilder von möglichen Verdächtigen zur eventuellen Identifizierung des Täters vorgelegt werden. Auf das der Frau zugegangene Ladungsschreiben hat die Polizei Namen, Vornamen und Geburtsdaten dreier Personen vermerkt, die der Polizei als Täter oder Verdächtige von Körperverletzungsdelikten bekannt waren.

   Diese namentliche Nennung von drei Personen, die offensichtlich früher einmal Körperverletzungen begangen haben, war unzulässig. Ich habe dies beanstandet. Für die Übermittlung der Personalien fehlte es an einer Rechtsgrundlage. Vor allem war die Übermittlung zur Feststellung des Täters nicht erforderlich.

   Meine Ermittlungen haben allerdings auch ergeben, daß es sich hierbei um einen Einzelfall, keinesfalls um die bei der Polizei übliche Praxis gehandelt hat. Ein polizeiinterner Hinweis, mit dem sogenannte Vergleichslichtbilder beigezogen werden sollten, war versehentlich auf das Ladungsschreiben gesetzt worden. Die Polizeibehörde hat unmittelbar nach Bekanntwerden des Vorfalls ihre Dienststellen unter Hinweis auf das vorliegende Fehlverhalten angewiesen, der Einhaltung datenschutzrechtlicher Vorschriften besondere Aufmerksamkeit zu schenken.

4.8. Datenspeicherung in Zusammenhang mit der Wiederaufarbeitungsanlage Wackersdorf

Im Berichtszeitraum habe ich ermittelt, welche Dateien und Karteien im Zusammenhang mit der Wiederaufarbeitungsanlage in Wackersdorf von der Polizei angelegt worden sind. In diese Ermittlungen habe ich das Landeskriminalamt, das Polizeipräsidium Niederbayern/Oberpfalz und das Landesamt für Verfassungsschutz einbezogen.

Die Polizeidirektion Amberg führt eine sogenannte Ermittlungsdatei, deren Zweck es ist, strafrechtlich relevante Erkenntnisse, bei denen Bezug zur Errichtung der Wiederaufarbeitungsanlage Wackersdorf gegeben ist, zusammenzuführen. Daneben führt das Polizeipräsidium Niederbayern/Oberpfalz noch eine Ermittlungs- und Verwaltungsdatei zur Wiederaufarbeitungsanlage Wackersdorf, die der Bewältigung von Verwaltungsaufgaben sowie als Einsatz- und Führungshilfsmittel im Zusammenhang mit polizeilichen Maßnahmen anläßlich der Errichtung der Wiederaufarbeitungsanlage dient. Außerdem führt das Landeskriminalamt eine Datei für Ermittlungen gegen überörtliche Täter im Zusammenhang mit der Wiederaufarbeitungsanlage. Diese Datei dient schwerpunktmäßig der Aufklärung von Straftaten des Landfriedensbruchs und schweren Landfriedensbruchs. Beim Landesamt für Verfassungsschutz bestehen nach eigener Erklärung im Zusammenhang mit der Wiederaufarbeitungsanlage in Wackersdorf keine speziellen Karteien oder Dateien. Meine Ermittlungen haben nichts Gegenteiliges ergeben.

Bei Stichprobenprüfungen der im Bereich des Polizeipräsidiums Niederbayern/Oberpfalz geführten Dateien vor Ort haben sich keine Anhaltspunkte für Zweifel an der Erforderlichkeit dieser Dateien ergeben. Bei der Ermittlungsdatei waren in allen Fällen die Anknüpfungspunkte für die polizeiliche Aufgabenerfüllung erkennbar. Für beide Dateien ist nach der Errichtungsanordnung jeweils halbjährlich eine Erforderlichkeitsprüfung durch das Polizeipräsidium Niederbayern/Oberpfalz durchzuführen. Diese Prüfung ist nach meinen Feststellungen bisher durchgeführt worden.

Ich habe allerdings gerügt, daß die aufgrund der Errichtungsanordnung oder sonstiger polizeilicher Vorschriften vorgegebenen Aussonderungsfristen nicht maschinell überprüft werden können. So ist etwa auch die Beachtung der nach den Richtlinien zu kriminalpolizeilichen Sammlungen erforderlichen verkürzten Aussonderungsprüffrist bei der Speicherung von Jugendlichen nicht gewährleistet. Auch ist eine Verkürzung der Aussonderung bei Vorgängen geringerer Bedeutung, das gilt z.B. für Ordnungswidrigkeiten, nicht sichergestellt.

Bei der vom Landeskriminalamt geführten Ermittlungsdatei zur Wiederaufarbeitungsanlage habe ich festgestellt, daß entgegen der vom Innenministerium erteilten Freigabe, die sich ersichtlich nur auf die Speicherung von bestimmten Straftaten zu deren generellen Aufklärung und vorbeugenden Bekämpfung bezieht, auch Betroffene von Ordnungswidrigkeiten sowie Verdächtige anderer Straftaten gespeichert werden. Das Landeskriminalamt vertritt hierzu die Auffassung, daß die von der Freigabe nicht erfaßten Daten als Spuren für „konkrete Ermittlungsverfahren" dienen. Es hat aber zugesagt, künftig auf eine strikte Trennung von allgemeinen Arbeitsdateien und Dateien zu konkreten Ermittlungsverfahren zu achten.

Auch bei dieser Datei des Landeskriminalamts habe ich im übrigen festgestellt, daß eine automationsgestützte Aussonderung entsprechend der in der Errichtungsanordnung vorgesehenen Aussonderungsfrist nicht sichergestellt ist.

Zwar bestehen alle drei Dateien derzeit noch nicht so lange, daß auch die kurzen Aussonderungsfristen schon abgelaufen wären. Auch werden die beiden im Bereich des Polizeipräsidiums Niederbayern/Oberpfalz geführten Datei-

en halbjährlich auf ihre Erforderlichkeit hin überprüft, so daß wegen der mangelnden automatisierten Aussonderung für die Betroffenen keine Nachteile entstanden sind. Doch muß durch entsprechende weitere Maßnahmen für die Zukunft sichergestellt sein, daß Daten nicht über den vorgesehenen Zeitraum hinaus gespeichert bleiben.

Diese Dateien werde ich in nächster Zeit weiter prüfen und hierbei insbesondere auch die Berechtigung einzelner Eintragungen kontrollieren.

Im Zusammenhang mit der sogenannten „Herbstaktion 1987" gegen die Wiederaufarbeitungsanlage in Wackerdorf haben sich viele Bürger an mich gewandt mit der Bitte, die datenschutzrechtliche Zulässigkeit einer etwaigen Datenspeicherung zu prüfen.

Tatsächlich waren im Rahmen dieser Aktionstage von der Polizei mehrere Kontrollstellen eingerichtet worden, an denen die Personalien der Demonstranten kontrolliert worden sind. Außerdem wurden Demonstranten erkennungsdienstlich behandelt. Meine Ermittlungen aufgrund dieser Eingaben haben ergeben, daß die Personalienüberprüfung an einer Kontrollstelle nicht zu einer Speicherung in einer polizeilichen Datei geführt hat, also weder Daten in die Datei APIS noch in die im Zusammenhang mit der Wiederaufarbeitungsanlage angelegten Dateien aufgenommen worden sind.

Soweit es nicht bei einer bloßen Kontrolle geblieben ist, sondern gegen Verdächtige im Rahmen der Ermittlungen erkennungsdienstliche Maßnahmen durchgeführt worden sind, das Verfahren aber nach § 170 Abs. 2 Strafprozeßordnung (kein zu einer Verurteilung ausreichender Tatnachweis) eingestellt worden ist, werden die erkennungsdienstlichen Unterlagen auf entsprechenden Antrag der Betroffenen hin regelmäßig gelöscht. Ebenfalls gelöscht wurden im Rahmen meiner auf Eingaben hin durchgeführten datenschutzrechtlichen Ermittlungen etwaige in diesen Fällen vorgenommene Speicherungen in den WAW-Dateien und in APIS. Ich werde darauf drängen, daß nicht mehr gerechtfertigte Speicherungen auch ohne Antrag gelöscht werden.

4.9. Meldung betrunkener Verkehrsteilnehmer

Ein kommunaler Datenschutzbeauftragter fragte an, ob die Polizei das Gesundheitsamt über alle betrunken angetroffenen Verkehrsteilnehmer in Form von Trunkenheitsmeldungen und Anzeigen von Trunkenheitsfahrten benachrichtigen dürfe.

Die Zulässigkeit dieser Meldungen ist nach Art. 17 Abs. 1 BayDSG zu beurteilen. Das Staatsministerium des Innern hält eine Meldung an das Gesundheitsamt in den Fällen für erforderlich, in denen der konkrete Verdacht auf chronischen Rauschmittelmißbrauch besteht. Es verweist darauf, daß nach Art. 11 Abs. 1 Nr. 2 des Gesetzes über den öffentlichen Gesundheitsdienst (GDG) für das Gesundheitsamt der Aufgabenbereich der gesundheitlichen Beratung eröffnet sei gegenüber Personen, die an einer Sucht leiden oder von ihr bedroht sind. Diesem Personenkreis solle durch vorsorgliche Maßnahmen des Gesundheitsamtes die notwendige Hilfe für eine gesundheitliche Wiederherstellung und soziale Eingliederung gegeben werden.

Dieser Auffassung habe ich mich angeschlossen. Eine polizeiliche Meldung betrunkener Verkehrsteilnehmer an das Gesundheitsamt ist zulässig, wenn aus der Sicht der Polizei eine Beratung durch das Gesundheitsamt in Betracht kommt. So ist eine Meldung beispielsweise gerechtfertigt, wenn trotz eines hohen Blutalkoholwertes beim Betroffenen keine Ausfallerscheinungen wahrnehmbar waren oder dieser durch wiederholte Trunkenheit im Straßenverkehr aufgefallen ist. In einem solchen Fall liegt der konkrete Verdacht der Alkoholgewöhnung und des chronischen Alkoholmißbrauches nahe. Eine Meldung an das Gesundheitsamt ist in diesen Fällen nicht etwa deshalb unzulässig, weil die Polizei den Verkehrsteilnehmer selbst auf die Möglichkeit der freiwilligen Beratung durch das Gesundheitsamt hinweisen könnte. Ein solcher Hinweis wäre in der gegebenen Konfliktsituation nach aller Lebenserfahrung „in den Wind gesprochen".

4.10. Arbeitsdatei PIOS Innere Sicherheit (APIS)

4.10.1. Speicherung von Volkszählungsboykotteuren

Anfang des Jahres berichteten die Medien, daß Volkszählungsgegner in APIS gespeichert seien. Daraufhin habe ich vom Bayer. Landeskriminalamt einen Ausdruck sämtlicher von Bayern im Zusammenhang mit der Volkszählung gespeicherter Personendatensätze angefordert. Bei meiner datenschutzrechtlichen Prüfung bin ich im Hinblick auf die Zweckbestimmung der Datei APIS Hilfe zur Verhütung und Aufklärung von Straftaten mit staatsfeindlicher Zielsetzung von folgenden Grundsätzen ausgegangen:

- Keine Speicherung der nur versuchten und damit straflosen Aufforderung zu Straftaten im Zusammenhang mit der Volkszählung
- Keine Speicherung von Ordnungswidrigkeiten
- Bei Personen mit hohem Lebensalter ist die Voraussetzung zur Speicherung wegen der „Verhütung" weiterer Staatsschutzdelikte sehr streng zu prüfen. Hier wird es in besonderem Maße auf Rüstigkeit und Agilität der Senioren ankommen
- Soweit Verantwortliche im Sinne des Presserechts gespeichert sind, ist eindeutig festzustellen, ob die im Impressum genannten Personen tatsächlich für das Schriftwerk verantwortlich sind oder nur zur Tarnung der tatsächlich Verantwortlichen in das Impressum aufgenommen sind
- Sind Organisationen als Verantwortliche genannt, darf eine dieser Organisation angehörige Einzelperson nur gespeichert werden, wenn deren Verantwortlichkeit für das Druckwerk eindeutig feststeht. Dies ist auch bei einzelnen Vorstandsmitgliedern einer Organisation nicht ohne nähere Prüfung anzunehmen
- Soweit Straftaten „bei Gelegenheit" von Veranstaltungen und Demonstrationen begangen worden sind, ist genau zu prüfen, ob diese Straftaten tatsächlich dem Veranstalter zuzurechnen sind
- Das Motiv des Straftäters muß sich gegen die freiheitlich-demokratische Grundordnung richten. Bloße Sachbeschädigungen durch Herausschneiden der Ordnungsnummer aus dem Volkszählungsbogen ohne gleichzeitige öffentliche Aufforderung zum Boykott lassen ein solches Motiv in der Regel nicht erkennen. Die Strafbarkeit dieser Handlung allein ist nicht entscheidend für die Aufnahme in APIS. Gleiches muß für inzwischen einsichtige Opfer der Kampagne gegen die Volkszählung gelten.

Das Landeskriminalamt hat nach ersten Gesprächen mit mir im Hinblick auf die zu diesem Zeitpunkt weitgehend

abgeschlossene Volkszählung und unter Berücksichtigung des letzten Standes der polizeilichen Ermittlungen von sich aus sofort 50 und auf meine Anregung hin kurzfristig noch weitere 10 Personendatensätze gelöscht. Damit waren bereits Mitte Februar von Bayern nur noch 71 Personen wegen Straftaten im Zusammenhang mit der Volkszählung in APIS gespeichert. In diesen Fällen hatte ich aufgrund der vorliegenden Erkenntnisse gegen die vom Landeskriminalamt angenommene Erforderlichkeit einer weiteren Speicherung keine datenschutzrechtlichen Bedenken erhoben.

In einer Presseerklärung hatte ich zur Kritik an der APIS-Speicherung von straffälligen Volkszählungs-Boykotteuren folgendes geäußert: „Die Fundamentalkritiker der APIS-Speicherung von Straftätern, welche die Volkszählung boykottieren wollten, verkennen Aufgabe und Bedeutung von APIS, den Sicherheitsbehörden im Kampf gegen politisch motivierte Kriminalität dringend benötigte Ansatzpunkte zur Aufklärung und Verhütung von Straftaten zu liefern. APIS ist nämlich von ihrer Zweckbestimmung her keineswegs nur eine „Terroristen-Datei". Es kann auch keinen Zweifel daran geben, daß Personen, die im Rahmen des landesweit organisierten Gesetzesboykotts die vom Parlament beschlossene und vom Bundesverfassungsgericht bestätigte Volkszählung kippen wollten, die rechtsstaatliche Ordnung und die freiheitlich demokratische Grundordnung erschüttern möchten. Um so weniger kann einleuchten, weshalb politisch motivierte Straftäter durch eine Nichtaufnahme in APIS privilegiert werden sollten."

In der Folgezeit haben sich sehr viele Bürger an mich gewandt, die die Befürchtung geäußert haben, wegen ihrer Ablehnung der Volkszählung in APIS gespeichert zu sein. In der weit überwiegenden Zahl aller Fälle war ihre Sorge unbegründet, was im Hinblick auf die Speicherung von nur 71 Personen Mitte Februar auch nicht anders zu erwarten war. Soweit Personen tatsächlich in APIS gespeichert waren, sind inzwischen die Daten der Personen gelöscht worden, die wegen des Verdachts von Straftaten im Zusammenhang mit der Volkszählung freigesprochen worden sind oder gegen die das Verfahren nach § 170 Abs. 2 der Strafprozeßordnung (kein ausreichender Nachweis der Straftat) eingestellt worden ist.

Gegenwärtig führe ich noch Gespräche mit dem Landeskriminalamt, inwieweit Personen, gegen die das Verfahren gegen Auflagen (z.B. Zahlung eines Geldbetrages) wegen geringer Schuld nach § 153a StPO eingestellt worden ist, ebenfalls in der Datei APIS zu löschen sind. Derzeit sind in APIS im Zusammenhang mit der Volkszählung nur noch 60 Personen gespeichert (Stand: 9.11.1988).

Weitere Dateien im Zusammenhang mit der Volkszählung führt das Landeskriminalamt nicht. Eine sogenannte Spurendokumentations-Datei „Ereignisübersicht in Zusammenhang mit Boykott-Aktionen gegen die Volkszählung" wurde nur wenige Monate geführt. Der Datenbestand ist zwischenzeitlich vollständig gelöscht worden.

4.10.2. Verantwortlichkeit und Kontrolle der Datensätze in APIS

In der Datei APIS gilt anders als im polizeilichen Informationssystem „INPOL" das „Besitzerprinzip" nicht. Das heißt, daß jedes Landeskriminalamt in den in APIS geführten Datensätzen Änderungen vornehmen kann, unabhängig davon, ob der Datensatz von diesem oder einem anderen Landeskriminalamt oder dem Bundeskriminalamt gespeichert worden ist. Aus der Sicht des Datenschutzes ist es grundsätzlich notwendig, daß Speicherungen in Dateien durch Nachweise in Akten oder sonstigen Unterlagen auf ihre Richtigkeit und Aktualität hin überprüft werden können. Voraussetzung dafür ist jedoch, daß erkennbar ist, wer die Speicherung vorgenommen hat. Bei APIS ist hinsichtlich der Erkennbarkeit des Urhebers folgendes zu bemerken:

Wird ein neuer Datensatz angelegt, werden also zu einer Person erstmalig Daten gespeichert, ist das speichernde Landeskriminalamt anhand einer Nummer zu erkennen. Dies gilt gleichermaßen, wenn zu einem bereits bestehenden Datensatz ein neuer Vorgang hinzugefügt wird. Anders ist es allerdings, wenn in einem bereits bestehenden Vorgang Änderungen vorgenommen werden, also einzelne Daten ersetzt, überschrieben oder ergänzt werden. In diesem Fall ist nicht ersichtlich, wer die Änderung veranlaßt hat.

Um nachteilige Auswirkungen dieser mangelnden Erkennbarkeit auszugleichen, verfährt das Bayer. Landeskriminalamt aus eigener Initiative bei Änderungen in bestehenden Datensätzen anderer Bundesländer wie folgt:

Handelt es sich um eine bedeutsame Information, z.B. Änderung des gesamten Sachverhalts durch eine zusätzliche Vernehmung, so wird dies dem Landeskriminalamt, das die erste Speicherung durchgeführt hat, schriftlich, fernschriftlich oder auf anderem Wege mitgeteilt. Es obliegt dann dem jeweiligen Landeskriminalamt, inwieweit dieses selbst eine Änderung in APIS für erforderlich hält. Sind nur geringfügige Änderungen, z.B. Änderung einer Anschrift, erforderlich, nimmt diese das Bayer. Landeskriminalamt selbst vor. Allerdings unterrichtet das Bayer. Landeskriminalamt auch in diesem Fall das als verantwortlich gespeicherte Landeskriminalamt von dieser Änderung. Zusätzlich dokumentiert das Bayer. Landeskriminalamt diese Änderung im Rahmen der Vorgangsverwaltung. Das verantwortliche Landeskriminalamt kann aufgrund der Unterrichtung durch das Bayer. Landeskriminalamt diese Mitteilung über die Änderung dokumentieren.

Damit ist – zumindest was durch das Bayer. Landeskriminalamt veranlaßte Änderungen angeht – die Nachvollziehbarkeit und Kontrollierbarkeit der Änderungen weitgehend gewährleistet.

4.11. Staatsschutzkarteien

Prüfungen von Staatsschutzkarteien haben in den vergangenen Jahren zur Feststellung zahlreicher datenschutzrechtlicher Verstöße geführt. Das Staatsministerium des Innern hat auf meine Kritik hin die Polizeidienststellen aufgefordert, die bestehenden Staatsschutzkarteien zu bereinigen und, abgestimmt auf die Bedeutung der Angelegenheit im Einzelfall, unterschiedliche Aufbewahrungs- und Überprüfungsfristen festzulegen. Auch ist die Weisung ergangen, Verwaltungsvorgänge nicht in die Staatsschutzkartei aufzunehmen, sondern gesondert zu verwahren. Außerdem wurde die Empfehlung ausgesprochen, exakte Feststellungsanordnungen für bereits bestehende Staatsschutzkarteien zu erlassen.

Diese Weisungen des Staatsministeriums des Innern haben, wie meine Prüfungen im Berichtszeitraum ergeben haben, aus datenschutzrechtlicher Sicht zu einer deutlichen Verbesserung des Inhalts der Staatsschutzkarteien geführt.

Hierbei mag auch eine Rolle spielen, daß die Bedeutung der Staatsschutzkarteien wohl zunehmend zurückgeht.

Staatsschutzkarteien sind generell gesondert untergebracht. Zugang haben nur die jeweils zuständigen Sachbearbeiter. Die Voraussetzungen für eine zeitgerechte Aussonderung sind durch die Vergabe von eindeutigen Aussonderungsprüfdaten geschaffen. Tatsächlich habe ich auch keine Karteikarte gefunden, für die die vorgesehene Speicherungsfrist bereits abgelaufen war. Oftmals finden sich auf den Karteikarten sogar Hinweise auf ergangene Strafurteile, was die richtige Bewertung des vermerkten Vorgangs erleichtert.

In einzelnen Fällen ist mir allerdings nach wie vor aufgefallen, daß Informationen vorgehalten werden, die keinen Staatsschutzbezug erkennen lassen. Ihre Speicherung wäre allenfalls im allgemeinen Kriminalaktennachweis zulässig gewesen. Teilweise war der Bezug zwischen Karteikarte und zugrunde liegendem Vorgang, der häufig erst eine abschließende Bewertung der Bedeutung und Richtigkeit der Information zuläßt, nur schwer oder kaum möglich. Hier sind Verbesserungen notwendig. In einer Staatsschutzkartei habe ich auch festgestellt, daß für Vorgänge, die im Zusammenhang mit der Volkszählung 1987 angelegt worden sind, abweichend von der sonst üblichen 5-Jahresfrist, meist eine 10-jährige Aussonderungsfrist vergeben worden ist. Für diese Sonderbehandlung habe ich keine sachgerechte Begründung erfahren. Ich habe diese Stelle deshalb aufgefordert, die Staatsschutzrelevanz aus heutiger Sicht nochmals zu prüfen und jedenfalls kürzere Aussonderungsfristen zu vergeben.

Wie eingangs bemerkt, nimmt die Bedeutung dieser Staatsschutzkarteien wohl zunehmend ab. Dies mag zum einen darin liegen, daß nun dem Landeskriminalamt die Datei APIS zur Verfügung steht, die einen bundesweiten Überblick über Verdächtige und Täter von Staatsschutzdelikten zuläßt. Daneben erlauben aber neuere Aktennachweisverfahren wie etwa der Ballungsraum-KAN (siehe 4.4.1) Auswertungen der bei den Polizeibehörden gespeicherten Daten auch unter Staatsschutzgesichtspunkten. Damit entsteht faktisch eine Staatsschutzdatei. Bereits bei der Speicherung von Zusatzinformationen in solchen Aktennachweissystemen muß deshalb Sorge dafür getragen werden, daß die gleichen Anforderungen an die datenschutzrechtliche Zulässigkeit entsprechender Zusatzvermerke gestellt werden, wie sie heute für die Staatsschutzkarteien gelten. Bei meinen weiteren Prüfungen werde ich auf diese Entwicklung ein besonderes Augenmerk richten.

4.12. Bayerische Grenzpolizei

4.12.1. Grenzaktennachweis

Unter der Bezeichnung „Grenzaktennachweis" (GAN) führt die bayerische Grenzpolizei einen Nachweis ihrer Kriminalakten, ihrer Akten über grenzpolizeiliche Vollzugsmaßnahmen sowie zu Unterlagen über Tätigkeiten der Gefahrenabwehr. Dieser als „Landes-GAN" geführte Grenzaktennachweis entspricht in seinem technisch-organisatorischen Aufbau weitgehend dem „Kriminalaktennachweis" der Landespolizei. Unterschiede gegenüber dem Kriminalaktennachweis ergeben sich aus dem erweiterten Datenvolumen. So werden neben strafrechtlich relevanten Sachverhalten auch Verwaltungsentscheidungen und Verkehrsordnungswidrigkeiten nachgewiesen.

Gegen diese Erweiterung des Landes-GAN gegenüber dem vergleichbaren Kriminalaktennachweis hatte ich zunächst Bedenken erhoben. Dabei hatte ich insbesondere darauf hingewiesen, daß nach den Richtlinien für kriminalpolizeiliche Sammlungen Verkehrsordnungswidrigkeiten in Kriminalakten nicht aufgenommen werden dürfen. Deren Speicherung im Landes-GAN habe ich als eine faktische Umgehung dieses Verbotes angesehen. Doch hat das Staatsministerium des Innern meine Bedenken damit zerstreut, daß es ausdrücklich erklärt hat, es werde an dem Grundsatz festgehalten, daß die Unterlagen über Verkehrsordnungswidrigkeiten nicht in eine Kriminalakte aufgenommen werden. Weiter hat es die Notwendigkeit der entsprechenden Speicherung von Verwaltungsakten und Verkehrsordnungswidrigkeiten im Landes-GAN mit den besonderen Aufgaben der Grenzpolizei im Grenzbereich begründet. Weil sichergestellt ist, daß Daten über Verkehrsordnungswidrigkeiten und Verwaltungsakte nur der Grenzpolizei und nicht der sonstigen Landespolizei zur Verfügung stehen, sind prinzipielle datenschutzrechtliche Einwendungen somit nicht zu erheben.

Inzwischen ist die Datei „Grenzaktennachweis" um eine weitere Datengruppe erweitert worden, die der Überwachung des grenzüberschreitenden Omnibus- und LKW-Verkehrs dient. Mit dieser Datei sollen Täter wiedererkannt werden, die im grenzüberschreitenden LKW- und Omnibusverkehr schwerwiegende Verstöße gegen Vorschriften zum Schutz der Sicherheit im Straßenverkehr sowie gegen das Güterkraftverkehrsgesetz, Fahrpersonalgesetz und das Personenbeförderungsgesetz begangen haben. Den besonderen Anliegen des Datenschutzes wird dadurch Rechnung getragen, daß Daten aus dieser zusätzlich geschaffenen Datengruppe durch die Verwendung besonderer Schlüsselzahlen ausschließlich für die Grenzpolizeidienststellen zur Verfügung stehen. Außerdem sind kurze Speicherungsfristen festgelegt. Weiter wird auf meine Anregung hin sichergestellt, daß wegen des Grundsatzes der Verhältnismäßigkeit geringe Verstöße, wie etwa Verkehrsordnungswidrigkeiten, außerbayerischen Grenzdienststellen nicht zum Abruf zur Verfügung stehen.

Datenschutzrechtliche Prüfungen des Grenzakten-Nachweises vor Ort haben positive Ergebnisse erbracht: Die im Grenzakten-Nachweis gespeicherten Daten sind gut dokumentiert und lassen somit die Prüfung der Richtigkeit und Aktualität der gespeicherten Daten zu. Der Ausgang etwaiger Strafverfahren, der erst die abschließende Bewertung über einen strafrechtlich relevanten Vorgang zuläßt, wird in den Unterlagen geführt. Durch die Festlegung von Aussonderungsprüfdaten ist gewährleistet, daß die Speicherung nur über den notwendigen Zeitraum erhalten bleibt. Auch die Herkunft der einzelnen Informationen ist anhand der Unterlagen nachvollziehbar.

Fehler habe ich in einigen Fällen bei der Festlegung des Beginns der Aussonderungsfrist festgestellt. Maßgebend ist hier nicht der Zeitpunkt einer aufgrund einer früheren Straftat vorgenommenen Abschiebung, sondern der Zeitpunkt der der Abschiebung zugrunde liegenden Straftat.

In zwei Fällen habe ich auch Speicherungen von HIV-Infizierungen vorgefunden, die nicht vom Landeskriminalamt – wie vorgesehen – in den Personendatensatz des Betroffenen (vgl. 4.5.1), sondern von den Grenzpolizeidienststellen in eine andere ihnen zugängliche Datengruppe

eingestellt worden sind. Damit ist eine wünschenswerte zentrale Prüfung, zu welchen Personen ein Hinweis auf eine HIV-Infizierung gespeichert ist, nicht gewährleistet. In diesem Zusammenhang wird auch die Frage zu klären sein, ob Informationen über HIV-Infizierungen, die der Arzt den für die Abschiebung ins Ausland Verantwortlichen mitteilt, auch bei Gelegenheit des Grenzübertritts in polizeiliche Informationssysteme eingespeichert werden dürfen.

5. Verfassungsschutz

5.1. Prüfungen beim Bayer. Landesamt für Verfassungsschutz

5.1.1. Kontrolle von Einzelvorgängen

Beim Landesamt für Verfassungsschutz finden im Laufe eines Jahres zahlreiche datenschutzrechtliche Prüfungen statt. Das Schwergewicht liegt dabei eindeutig auf der Kontrolle von Einzelvorgängen, die durch Eingaben von Bürgern veranlaßt sind. Weil sich Bürger aus allen Lebensbereichen an mich wenden, erhalte ich durch diese Einzelkontrollen einen guten Einblick in die Verarbeitung personenbezogener Daten beim Landesamt für Verfassungsschutz. Den meisten Eingaben liegt die Befürchtung zugrunde, zu Unrecht bei Verfassungsschutzbehörden gespeichert zu sein und deshalb möglicherweise Nachteile im Berufsleben erleiden zu müssen.

Vorweg kann ich sagen, daß keine einzige Eingabe Anlaß zu einer Beanstandung beim Landesamt für Verfassungsschutz gegeben hat. Selbstverständlich sind mir wie schon in den Jahren zuvor alle für diese Prüfungen angeforderten Unterlagen (Akten, Bücher u. ä.) vorgelegt worden. Und obwohl gegenüber Verfassungsschutzbehörden nach Art. 8 Abs. 2 Nr. 5 Bayer. Datenschutzgesetz für den Bürger kein Auskunftsanspruch besteht und deshalb auch der Landesbeauftragte für den Datenschutz sich bei der Weitergabe der bei seinen Prüfungen in Einzelsachen gewonnenen Erkenntnisse an den Petenten zurückzuhalten hat, konnte ich mit Zustimmung des Landesamtes für Verfassungsschutz in zahlreichen Fällen Näheres über meine Prüfungsergebnisse mitteilen. Dies begrüße ich, dienen doch meine Auskünfte an den Bürger in aller Regel zum Abbau seiner Ängste und Vorbehalte.

5.1.2. Generelle Prüfung

Neben diesen Einzelkontrollen habe ich wiederum wie in den vergangenen Jahren eine kurze generelle Prüfung durchgeführt und mich außerdem intensiv mit dem auch in der Öffentlichkeit stark diskutierten Fall „Bruck" und dessen Umfeld befaßt.

Schwerpunkte meiner allgemeinen datenschutzrechtlichen Prüfung waren das nachrichtendienstliche Informationssystem (NADIS), die Registrierung der Informationen beim Landesamt und die Abwicklung der Sicherheitsüberprüfungen für die Privatwirtschaft. Auch dieses Mal habe ich bei meinen Prüfungen keine wesentlichen Datenschutzverstöße festgestellt. Es hat sich ganz im Gegenteil gezeigt, daß das Landesamt meine Anregungen aus den vergangenen Jahren weitgehend in seine Praxis der Datenverarbeitung umgesetzt hat.

NADIS

Im Mittelpunkt der NADIS-Prüfung stand die Frage, inwieweit in der Öffentlichkeit besonders in Erscheinung getretene Gegner der Volkszählung wegen dieser Gegnerschaft von Verfassungsschutzbehörden gespeichert werden. Die Stichproben mit den Namen von über 60 Betroffenen aus diesem Personenkreis haben gezeigt, daß die Tatsache der Gegnerschaft zur Volkszählung, auch wenn sich diese in Straftaten geäußert hat, nicht zu einer Speicherung in NADIS geführt hat. Offensichtlich ist hier zu Recht zwischen allenfalls staatsschutzrechtlich relevanten und verfassungsschutzrelevanten Vorgängen unterschieden worden. Dies ist positiv hervorzuheben.

Allerdings sind mir bei der Prüfung auch einige Fehler aufgefallen:

- So wird das für die Festlegung der Aussonderungsfrist maßgebliche Datum noch immer teilweise falsch berechnet. Maßgebend ist der Zeitpunkt des relevanten Ereignisses und nicht etwa der im Einzelfall mehrere Monate spätere Zeitpunkt der Speicherung.
- In mehreren Fällen war aus den Unterlagen des Landesamtes keine plausible Erklärung für den festgestellten Zeitpunkt des Beginns der Aussonderungsfrist zu entnehmen. Dies habe ich gerügt.
- Erneut habe ich darauf hingewiesen, daß die Voraussetzungen für eine erstmalige Speicherung in NADIS besonders genau geprüft werden müssen. Eine Ordnungswidrigkeitenanzeige wegen wilden Plakatierens genügt in der Regel den Anforderungen nicht, die an eine Ersteinspeicherung zu stellen sind. In mehreren Fällen hat das Landesamt die Löschung oder zumindest eine intensive erneute Prüfung der Relevanz der Vorgänge veranlaßt.

Bei der Prüfung der Registrierung der beim Landesamt für Verfassungsschutz angefallenen Vorgänge sind keine datenschutzrechtlichen Fehler festgestellt worden. Durch besondere Maßnahmen ist zudem sichergestellt, daß nur ein eng begrenzter Personenkreis auf die Registraturdaten zugreifen kann.

Sicherheitsüberprüfungen

Schließlich habe ich, wie im letzten Tätigkeitsbericht angekündigt, sämtliche Sicherheitsüberprüfungen in der Privatwirtschaft, an denen das Landesamt im Zeitraum von August 1987 bis Februar 1988 mitgewirkt hat, überprüft:

Hierbei ist nur kurz darauf hinzuweisen, daß nach Art. 2 Abs. 2 Ziffer 2 des Gesetzes über die Errichtung eines Landesamtes für Verfassungsschutz die Mitwirkung beim Sabotageschutz in der Privatwirtschaft dem Landesamt als Aufgabe zugewiesen ist. Zwar fehlt es noch an einer besonderen gesetzlichen Regelung für die Sicherheitüberpüfung in der Privatwirtschaft. Diese ist in Vorbereitung. Doch sind Sicherheitsüberprüfungen derzeit im Hinblick auf die verfassungsgerichtliche Rechtsprechung zum „Übergangsbonus" nicht rechtswidrig.

Aus Sicherheitsgründen kann ich Einzelheiten des Ablaufs dieser Mitwirkung bei Sicherheitsüberprüfungen in der Privatwirtschaft nicht schildern. Folgendes kann ich jedoch mitteilen:

- Es ist sichergestellt, daß insbesondere in den Fällen, in denen Sicherheitsbedenken geäußert werden, die Rich-

tigkeit der zugrunde liegenden Erkenntnisse und der daraus gezogenen Bewertung mehrfach geprüft wird.
- Wegen der derzeit noch fehlenden besonderen gesetzlichen Regelung für die Sicherheitsüberprüfungen sehen die Sicherheitsrichtlinien, wie von mir gefordert, nun vor, daß der Betroffene schriftlich seine Einwilligung in seine Sicherheitsüberprüfung erklären muß. Allerdings habe ich festgestellt, daß in mehreren Fällen Sicherheitsüberprüfungen durchgeführt worden sind, ohne daß die erforderliche schriftliche Einwilligung des Betroffenen vorgelegen hat. Diese Fälle lagen jedoch sämtlich in den ersten Monaten nach Inkrafttreten der neuen Sicherheitsrichtlinien. In einem Fall habe ich festgestellt, daß die Einverständniserklärung für die Sicherheitsüberprüfung erst fünf Monate nach dem Antrag auf Sicherheitsüberprüfung und bereits nach deren Abschluß nachgereicht worden ist. Auch diese Sachbehandlung entspricht nicht den Sicherheitsrichtlinien.
- Des weiteren sind Sicherheitsüberprüfungen von zwei Firmen durchgeführt worden, die nicht auf der Liste besonders sabotagegefährdeter Unternehmen eingetragen waren. Auch wenn diese Firmen von ihrem Aufgabenbereich her aus meiner Sicht als sabotagegefährdet angesehen werden können, lege ich jedoch Wert darauf, daß die Firmen von sachkundiger Stelle eindeutig und klar festgelegt werden, für die die Voraussetzungen derartiger Sicherheitsüberprüfungen gegeben sind.
- Auch habe ich bemängelt, daß in einer Reihe von Fällen die Funktion, die die zu überprüfende Person bei der sabotagegefährdeten Firma bekleiden soll, nicht hinreichend exakt genannt worden ist. Diese Bezeichnung ist eine Voraussetzung dafür, daß das Landesamt feststellen kann, ob ein Fall seiner Mitwirkung an einer Sicherheitsüberprüfung vorliegt. So habe ich etwa Formulierungen „Zugang zum Wehrbereich", „Tätigkeit im sicherheitsempfindlichen Bereich" oder „Aushilfskraft" als zu allgemein bezeichnet.
- Auch sehe ich die Erforderlichkeit einer Mitwirkung bei einer Sicherheitsüberprüfung dann nicht für gegeben an, wenn von vornherein mitgeteilt wird, daß die zu überprüfende Person ohnehin nicht weiterbeschäftigt oder in Kürze entlassen wird.
- Zum Verfahren selbst habe ich aus den bei der Prüfung gewonnenen Erkenntnissen dem Landesamt einige Anregungen gegeben. Besonderen Wert lege ich auch darauf, daß Mitteilungen, die aufgrund von Sicherheitsüberprüfungen an die sabotagegefährdete Firma gemacht werden, in den Unterlagen des Landesamtes eindeutig dokumentiert werden. Hier sind im Einzelfall noch Verbesserungen notwendig. Schließlich habe ich festgestellt, daß die auf Formblättern vorgedruckten Einverständniserklärungen zu einer Sicherheitsüberprüfung bei den einzelnen Firmen sehr unterschiedlich formuliert und nicht immer als ausreichende Einwilligungserklärung auszulegen waren. Hier wird auf die Firmen entsprechend einzuwirken sein, andernfalls die Mitwirkung bei der Sicherheitsüberprüfung abzulehnen ist (siehe auch 5.4).

5.1.3. „Fall Bruck"

Unter dem Stichwort „Fall Bruck" haben die Medien zwar ausführlich, teilweise aber recht irreführend über Tätigkeiten des Landesamtes für Verfassungsschutz berichtet, welche die Informationserhebung im weiteren Umfeld der Wiederaufarbeitungsanlage in Wackersdorf betroffen haben.

Meine Ermittlungen in dieser Sache haben ergeben, daß Mitarbeiter des Landesamtes für Verfassungsschutz in Bruck und anderen Gemeinden Meldedaten von ca. 100 Personen erhoben haben. In einzelnen Fällen wurden Paßbilder fotografiert.

Rechtsgrundlagen für dieses Vorgehen des Landesamtes für Verfassungsschutz sind Art. 2 Abs. 1 Nr. 1 Gesetz über die Errichtung eines Landesamtes für Verfassungsschutz, Art. 31 Abs. 1 und 3 Meldegesetz, §§ 21, 22 Paßgesetz, §§ 2 a, 2 b Personalausweisgesetz i.V.m. Art. 14 Ausführungsgesetz zum Personalausweisgesetz. Nach diesen Bestimmungen darf das Landesamt für Verfassungsschutz in Melde-, Paß- und Personalausweisregistern unter der Voraussetzung Einsicht nehmen,
- daß es hierzu aufgrund eines Gesetzes berechtigt ist (hier Gesetz über die Errichtung eines Landesamtes für Verfassungsschutz),
- ohne Kenntnis dieser Daten seine ihm obliegende Aufgabe nicht erfüllen könnte und
- die Daten nicht beim Betroffenen selbst oder bei ihm nur mit unverhältnismäßig hohem Aufwand erhoben werden könnten.

Nebenbei ist zu bemerken, daß auch Lichtbilder personenbezogene Daten im Sinne dieser gesetzlichen Bestimmung sind.

Als Ergebnis meiner umfangreichen Überprüfung ist festzustellen, daß sich das Landesamt bei der Erhebung von Daten aus Melde-, Paß-, Personalausweisregistern und beim Fotografieren von Lichtbildern im Rahmen seines gesetzlichen Auftrags und seiner Befugnisse gehalten hat. Die Aktion war rechtmäßig. Für den Datenschutzbeauftragten gibt es aus den Stellungnahmen, Einvernahmen und eingesehenen Unterlagen keinerlei Anhaltspunkte dafür, daß die Überprüfungsaktion des Verfassungsschutzes auf die Einschüchterung von WAA-Gegnern oder der Bevölkerung der Oberpfalz gerichtet war, wie dies gelegentlich behauptet worden ist. Das Landesamt für Verfassungsschutz ist im übrigen auch seinen ihm gesetzlich auferlegten besonderen Aufzeichnungspflichten über diese Datenerhebungen nachgekommen, wovon ich mich durch Stichprobenprüfungen ebenfalls überzeugt habe.

5.2. Bereichsspezifische Datenschutzregelungen bei Verfassungsschutzbehörden und Nachrichtendiensten

Die Notwendigkeit der Schaffung bereichsspezifischer Datenschutzregelungen für die personenbezogene Datenverarbeitung durch Verfassungsschutzbehörden und Nachrichtendienste habe ich bereits in den letzten Tätigkeitsberichten betont. Inzwischen liegen Entwürfe eines Bundesverfassungsschutzgesetzes, das auch die Zusammenarbeit zwischen Verfassungsschutz- und Staatsschutzbehörden regeln soll, eines Gesetzes über den militärischen Abschirmdienst und eines BND-Gesetzes vor. Wegen der richtungsweisenden Wirkung des Bundesverfassungsschutzgesetzes für die Novellierung des Bayer. Verfassungsschutzrechtes habe ich mich zu jenem geäußert. Da inzwischen weiter entwickelte Entwürfe vorliegen und die abschließende Beratung durch die Bundesregierung noch aussteht, weise ich nur auf einige mir wichtige Anliegen hin:

Die Beschreibung der Aufgaben der Verfassungsschutzbehörden und die Zuteilung der Befugnisse müssen dem tatsächlichen Aufgabenvolumen der Verfassungsschutzbe-

hörden entsprechen. Es wäre falsch, die Verfassungsschutzbehörden nur als Informations-Sammelstellen darzustellen. Sie haben darüber hinausgehende weitere Aufgaben, wie sich z.B. aus der Legaldefinition in Art. 73 Nr. 10b Grundgesetz ergibt. Danach wird Verfassungsschutz umfassend als „Schutz der freiheitlichen demokratischen Grundordnung, des Bestandes und der Sicherheit des Bundes oder eines Landes" definiert. Deshalb gehören zu den Aufgaben des Verfassungsschutzes beispielsweise auch die „Beobachtung" von Bestrebungen und geheimdienstlichen Tätigkeiten (Spionageabwehr) und das Sichverschaffen von Informationen.

Bei der Regelung der Befugnisnormen ist darauf zu achten, daß nicht nur die Befugnisse zur Datenverarbeitung in umfangreichen Bestimmungen niedergelegt werden, sondern daß auch die Befugnisse für die gesamte übrige Tätigkeit der Verfassungsschutzbehörden ausreichend und klar festgehalten werden.

Auch das Verfahren, in dem die Aufgaben der Verfassungsschutzbehörden zu erfüllen sind, darf nicht nur ansatzweise geregelt werden. Dies liegt im Interesse der Transparenz und damit der Verständlichkeit für den Bürger, und ist auch im Hinblick auf die Praktikabilität der Vorschriften für die Mitarbeiter der Verfassungsschutzbehörden sinnvoll.

Zusammenfassend ist festzustellen, daß die Entwurfverfasser das selbstgesetzte Ziel „Rechtsgrundlagen und Tätigkeiten des Bundesamtes für Verfassungsschutz klarer zu beschreiben und insbesondere näher zu bestimmen", möglichst in die Tat umsetzen sollten.

5.3. Richtlinien für die Sicherheitsüberprüfung von Personen im Rahmen des Geheimschutzes im öffentlichen Bereich

Am 1. September 1988 sind neue Sicherheitsrichtlinien in Kraft getreten. Sie regeln insbesondere, unter welchen Voraussetzungen Personen, die eine sicherheitsempfindliche Tätigkeit ausüben sollen, einer Sicherheitsüberprüfung zu unterziehen sind; nicht zu verwechseln mit den unter 5.4 behandelten „Sicherheitsüberprüfungen in der Privatwirtschaft".

Aus der Sicht des Datenschutzes ist hierzu folgendes zu bemerken:
Die Sicherheitsüberprüfungen von Personen im Rahmen des Geheimschutzes in der öffentlichen Verwaltung greifen zum Teil intensiv in den privaten, durch Art. 2 Abs. 1 und Art. 1 Abs. 1 Grundgesetz geschützten Lebensbereich ein. Sie bedingen nämlich die Erhebung und die Verarbeitung sehr sensibler personenbezogener Daten, weshalb auch das Recht auf informationelle Selbstbestimmung berührt wird. Beschränkungen dieses Rechts bedürfen einer verfassungsmäßigen gesetzlichen Grundlage, aus der sich die Voraussetzungen und der Umfang der Beschränkungen klar und für den Bürger erkennbar ergeben, und die dem rechtstaatlichen Gebot der Normenklarheit entsprechen muß (BVerfGE 65,1/44).

An einer solchen Rechtsgrundlage fehlt es derzeit. Zwar wirkt das Landesamt für Verfassungsschutz nach Art. 2 Abs. 2 Nr. 1 Gesetz über die Errichtung eines Landesamtes für Verfassungsschutz bei der Überprüfung von Personen mit, denen im öffentlichen Interesse geheimhaltungsbedürftige Tatsachen, Gegenstände oder Erkenntnisse anvertraut werden, oder die Zugang dazu erhalten sollen oder ihn sich verschaffen können. Von dieser gesetzlichen Aufgabenzuweisung zur Mitwirkung des Landesamtes für Verfassungsschutz an Sicherheitsüberprüfungen abgesehen, fehlt es an präzisen gesetzlichen Regelungen für die Durchführung von Sicherheitsüberprüfungen – jedenfalls für den Bereich außerhalb des öffentlichen Dienstes. Tatsächlich ist auch derzeit ein Bundesgeheimschutzgesetz in Vorbereitung.

Allerdings gilt auch für die Durchführung von Sicherheitsüberprüfungen, daß für einen geordneten Verwaltungsvollzug für eine Übergangszeit der vom Bundesverfassungsgericht und vom Bayer. Verfassungsgerichtshof generell anerkannte „Übergangsbonus" besteht. Soweit Sicherheitsüberprüfungen neuerdings auch auf Dritte erstreckt werden, (z.B. Angehörige, Personen, die in eheähnlicher Gemeinschaft leben, sonstige Dritte) kann es jedoch zweifelhaft sein, inwieweit die durch eine Sicherheitsüberprüfung bedingten Eingriffe mit dem Hinweis auf den „Übergangsbonus" zu rechtfertigen sind. Hier dürfte es sich empfehlen, wenn es ohne Gefährdung des Überprüfungsergebnisses möglich ist, die Einwilligung dieser Personen in die Sicherheitsüberprüfung einzuholen und es nicht nur mit einer Unterrichtung bewenden zu lassen.

Aus datenschutzrechtlicher Sicht muß es Ziel eines Geheimschutzgesetzes in Verbindung mit den Sicherheitsrichtlinien sein, festzulegen,
- welche Personen einer Sicherheitsüberprüfung unterzogen werden,
- welche Behörden am Verfahren beteiligt sind,
- wie das Verfahren im einzelnen abzuwickeln ist,
- welche Befugnisse den einzelnen Stellen einzuräumen sind,
- welche Zuständigkeiten sie im einzelnen haben,
- unter welchen Voraussetzungen Sicherheitsbedenken anzunehmen sind und
- welche personenbezogenen Daten erhoben, verarbeitet und an welche Stellen übermittelt werden.

Die Grundentscheidungen müssen im Gesetz selbst getroffen werden. Das Verfahren muß für den Betroffenen durchschaubar sein. Er ist nach Möglichkeit zumindest in groben Zügen über das Ergebnis der ihn betreffenden Sicherheitsüberprüfungen zu unterrichten. Dem Betroffenen sollte grundsätzlich in allen Fällen wenigstens Gelegenheit zur Stellungnahme zu für ihn nachteiligen Ergebnissen gegeben werden, damit er bei Personenverwechslungen oder offensichtlichen Fehleinschätzungen der Sicherheitsbehörden – wenigstens durch Einschaltung des Landesbeauftragten für den Datenschutz – die Informationen berichtigen lassen kann.

Auf der Grundlage dieser Grundsätze kann ich feststellen, daß die neuen Sicherheitsrichtlinien gegenüber der bisher geltenden Fassung datenschutzrechtlich gesehen wesentliche Verbesserungen enthalten. Dies begrüße ich.

Wie bereits bei den Sicherheitsüberprüfungen für die Privatwirtschaft werde ich auch die Praxis dieser Sicherheitsüberprüfungen beim Landesamt für Verfassungsschutz überprüfen.

5.4. Sicherheitsüberprüfungen in der Privatwirtschaft

In meinem letztjährigen Tätigkeitsbericht hatte ich im Zusammenhang mit Sicherheitsüberprüfungen in der Privatwirtschaft zum Zwecke des Sabotageschutzes angeregt, den von einer Sicherheitsüberprüfung Betroffenen darauf hinzuweisen, daß er sich bei Zweifeln an der ordnungsgemäßen Durchführung der Sicherheitsüberprüfung an den Landesbeauftragten für den Datenschutz wenden kann (zum Prüfungsergebnis siehe 5.1.2).

Das Staatsministerium des Innern hat auf diese Anregung hin seine Regelungen zu Sicherheitsüberprüfungen im Rahmen des vorbeugenden personellen Sabotageschutzes um folgende Weisung ergänzt: „Der zu Überprüfende ist schriftlich darauf hinzuweisen, daß er die Möglichkeit hat, sich an den Bayer. Landesbeauftragten für den Datenschutz, 8000 München 22, Postfach 22 03 02, mit der Bitte um datenschutzrechtliche Überprüfung zu wenden, wenn er nicht eingestellt oder umgesetzt wird und glaubt, daß diese Entscheidung auf erhobenen Sicherheitsbedenken beruht. Dieser Hinweis kann vorsorglich auch mit der Aufforderung an den Betroffenen verbunden werden, das Einverständnis zur Überprüfung schriftlich zu erklären".

Diese Ergänzung der Sicherheitsrichtlinien für die Privatwirtschaft begrüße ich außerordentlich. Sie ist ein Ausgleich dafür, daß der Betroffene wegen der sich aus der Natur der Sache ergebenden Geheimhaltungsbedürftigkeit die Einzelheiten, die im Rahmen einer Sicherheitsüberprüfung über ihn bekanntgeworden sind, nicht selbst vollständig überprüfen kann. Ich lege allerdings größten Wert darauf, daß die sabotagegefährdeten Unternehmen die Personen, die sie einer Sicherheitsüberprüfung unterziehen lassen, tatsächlich, ausdrücklich und eindeutig auf diese Anrufungsmöglichkeit des Datenschutzbeauftragten hinweisen. Obgleich ich selbst keine unmittelbaren Einwirkungsmöglichkeiten auf die Privatwirtschaft habe, bin ich mit einem Münchener Großunternehmen im Gespräch, um dies nun endlich sicherzustellen. Andernfalls müßte ich die Mitwirkung des Landesamtes für Verfassungsschutz an den Sicherheitsüberprüfungen in der Privatwirtschaft künftig beanstanden.

6. Justiz

6.1. Überblick

Automatisierung
Der Trend zur Automatisierung im Justizbereich, den ich bereits im letzten Tätigkeitsbericht festgestellt habe, hat sich fortgesetzt. Aus der Vielzahl von EDV-Verfahren stelle ich diejenigen, die mich in diesem Jahr besonders beschäftigt haben, kurz vor.

Kontrolle und Information
Die zunehmende Automatisierung erfordert eine begleitende Datenschutzkontrolle. Ich habe wiederum eine Staatsanwaltschaft und erstmals eine Justizvollzugsanstalt geprüft. Darüber hinaus habe ich mich u. a. über das sog. „integrierte" ADV-Verfahren beim Grundbuchamt München informiert.

Gesetzgebung
Die Diskussion in der Justiz, welche Gesetze als Folge des Volkszählungsurteils von 1983 überarbeitet oder neu geschaffen werden müssen, dauert an. Eine Novelle zur Strafprozeßordnung und ein Justizmitteilungsgesetz sind in Vorbereitung. Die Diskussion wurde „bereichert" durch eine Entscheidung des Oberlandesgerichts Frankfurt aus jüngster Zeit:

Nach Meinung dieses Gerichts fehlt für die Speicherung personenbezogener Daten in Zentralen Namenskarteien der Staatsanwaltschaften (z.B. Name, Vorname, Geburtsdatum, Aktenzeichen) eine ausreichende gesetzliche Grundlage. Das Recht auf informationelle Selbstbestimmung sei verletzt, weil weder § 152 StPO oder eine sonstige strafverfahrensrechtliche Norm noch § 7 Hess. Datenschutzgesetz, der in etwa Art. 4 BayDSG entspricht, eine ausreichende Ermächtigungsgrundlage für den Grundrechtseingriff darstellten. Den Gesetzgebungsorganen wird zur Behebung dieses Zustands eine Frist bis zum Ende der Legislaturperiode des Deutschen Bundestages im Jahr 1990 eingeräumt.

Nach meiner Auffassung bietet jedoch in Bayern Art. 16 BayDSG für die Speicherung personenbezogener Daten in Zentralen Namenskarteien der Gerichte und Staatsanwaltschaften auch für die Zukunft eine Rechtsgrundlage. Danach ist die Speicherung zulässig, wenn sie zur rechtmäßigen Erfüllung der durch Rechtsnorm der speichernden Stelle zugewiesenen Aufgaben erforderlich ist. Diese allgemein gehaltene Ermächtigungsgrundlage ist ausreichend. Die Forderung nach einer bereichsspezifischen Regelung für einen verhältnismäßig geringfügigen Eingriff halte ich für maßlos überzogen. Sie trägt nur zum Anwachsen der Vorschriftenflut bei.

Sollte sich jedoch die Auffassung des Oberlandesgerichts Frankfurt durchsetzen, so müssen in einigen Bereichen der Justiz in kurzer Zeit eine ganze Reihe von Gesetzgebungsvorhaben verwirklicht werden. Neben der Novellierung der StPO – einem der wohl schwierigsten Gesetzgebungsvorhaben – sind hiervon beispielsweise das Justizmitteilungsgesetz und das Strafvollzugsgesetz, aber auch die Personaldatenverarbeitung betroffen.

Eingaben
Zahlreiche Bürgereingaben haben mich zum Justizbereich erreicht. Ich habe die in der Presse breit behandelten Memminger Strafverfahren wegen Schwangerschaftsabbrüchen herausgegriffen und näher beleuchtet. Daneben hatte ich mich im Bereich des Strafverfahrens u. a. mit Fragen des Bundeszentralregisters, mit der angeblich unrichtigen Übermittlung personenbezogener Daten aus einer Polizeidatei an eine Staatsanwaltschaft, der Bekanntgabe gerichtlicher Geldauflagen an Dritte, mit Problemen von Strafgefangenen und der Befragung eines Versicherungsangestellten in einem Strafverfahren wegen unerlaubten Entfernens vom Unfallort zu beschäftigen. Im Zivilrechtsbereich äußerte ich mich u. a. zur Weitergabe der Versicherungsnummer eines Schuldners an dessen Gläubiger, der Bekanntgabe von Kundendaten eines Unternehmens im Unterhaltsverfahren, zu einer Verwechslung bei der Zustellung eines Mahnbescheids, zum Ausschluß der Öffentlichkeit bei Sitzungen, zu einem Datenschutzproblem bei Rechnungen einer Oberjustizkasse und zur angeblichen Weitergabe von Informationen über Immobilien aus Justizverfahren. Darüber hinaus beschäftigte ich mich wiederum mit Fragen des Datenschutzes im Notariat. Auch mit der Weitergabe personenbezogener Daten durch Justizbehörden an Wissenschaftler hatte ich mich zu befassen.

Arbeitskreis (AK) Justiz
Zur gemeinsamen Aufarbeitung von Problemen, zum Gedankenaustausch sowie zur Vorbereitung der DSB-Konferenzen haben die Datenschutzbeauftragten verschiedene Arbeitskreise gebildet. Dem AK Justiz stehe ich vor. Zu den im Jahr 1988 behandelten Themen gehören: – Novellierung der Strafprozeßordnung – Datenschutz im Strafvollzug – Probleme des Grundbuchrechts – Justizmitteilungsgesetz – Justizautomation

6.2. Automatisierungsvorhaben

6.2.1. Erstellung eines zentralen Handelsregisters

Das Handelsregister wird dezentral bei den Amtsgerichten geführt. Nun plant eine private Firma die Einrichtung eines zentralen Handelsregisters für das gesamte Bundesgebiet. Hierfür verlangt diese Firma die Herausgabe der bei den Gerichten vorhandenen Handelsregisterdaten.

Mit dem Staatsministerium der Justiz bin ich der Auffassung, daß die Herausgabe des gesamten Handelsregisterinhalts aller Amtsgerichte an eine Privatfirma zur Erstellung eines zentralen Handelsregisters nicht zulässig ist. Eine so umfassende Herausgabe des Registerinhalts kann nicht mehr als Einsicht in das Register, die nach § 9 Handelsgesetzbuch (HGB) jedermann ohne Nachweis eines berechtigten Interesses offensteht, bewertet werden. Außerdem hat der Gesetzgeber in § 8 HGB bestimmt, daß das Handelsregister von den Gerichten geführt wird. Damit hat er zum Ausdruck gebracht, daß ein zentrales Handelsregister, das von einer Privatfirma geführt wird, nicht seinen Vorstellungen entspricht.

6.2.2. Computerunterstützung in Wirtschaftsstrafsachen (COWISTRA)

Seit 1987 erproben zwei Staatsanwaltschaften den Einsatz des ADV-Verfahrens COWISTRA zur Unterstützung der Ermittlungen in umfangreichen Strafsachen, insbesondere in Wirtschaftsstrafsachen und in Fällen organisierter Kriminalität. Hierbei hat der Sachbearbeiter die Möglichkeit, zur Bewältigung der Aufgaben des Ermittlungsverfahrens eigene Dateien und DV-Anwendungen zu erstellen.

Für das nächste Jahr ist eine Datenschutzkontrolle zu COWISTRA vorgesehen.

6.2.3. Büroautomation

Die Büroautomation im gerichtlichen Geschäftsstellenbetrieb, die zunächst nur bei einem Gericht erprobt wurde, soll nun auf weitere Geschäftsstellen ausgedehnt werden. Das Verfahren ist nach Art. 26 BayDSG freigegeben, erste Meldungen zum Datenschutzregister sind eingegangen. Datenschutzrechtliche Probleme hat das Verfahren bisher nicht aufgeworfen, letzte technische und organisatorische Datensicherheitsprobleme kläre ich derzeit mit der Justizverwaltung ab.

Sollte sich jedoch die Auffassung des OLG Frankfurt durchsetzen, wonach es derzeit für die Führung Zentraler Namenskarteien der Staatsanwaltschaften an einer Rechtsgrundlage fehle, müßte die Geschäftsstellenautomation eingestellt werden (vgl. hierzu 6.1.).

6.2.4. Sonstige Verfahren

Weitere ADV-Verfahren der Justiz werden in anderem Zusammenhang erläutert (vgl. z. B. Stichwort „Strafvollzugsgesetz"). Vorarbeiten, das Personalwesen automationsunterstützt zu verwalten, ruhen derzeit. Gleichwohl kann festgestellt werden, daß die automatisierte Datenverarbeitung in der Justiz ganz erheblich zunimmt, was zwangsläufig zu einer Ausweitung meiner beratenden und kontrollierenden Tätigkeit führen wird.

6.3. Datenschutzrechtliche Prüfungen

6.3.1. Prüfung einer Staatsanwaltschaft

Wie im Vorjahr habe ich die Datenverarbeitung bei einer Staatsanwaltschaft geprüft. Hierbei richtete ich meine Aufmerksamkeit wiederum vor allem auf das Zentrale Namensregister. Dieses Verzeichnis ist derzeit ein Hilfsmittel zur Aktenführung; allerdings bestehen Bestrebungen, das Register zu einem staatsanwaltschaftlichen Informationssystem auszubauen. Um Gefährdungen für die Betroffenen auszuschalten, müssen Schutzvorkehrungen getroffen werden:

Bei stichprobenartigen Überprüfungen einiger im Namensverzeichnis gespeicherter Datensätze stellte ich gelegentlich Ungenauigkeiten fest wie unzutreffender Erledigungskennbuchstabe, oder keine Berichtigung des Tatvorwurfs bei erheblicher Abweichung zwischen ursprünglich vorgeworfenem und letztendlich nachgewiesenem Tatvorwurf. In einem reinen Aktennachweissystem kommt dem erheblich geringere Bedeutung zu als bei einem Informationssystem.

Für grundsätzlich fragwürdig halte ich die Speicherung von zur Tatzeit strafunmündigen 7- oder 8-jährigen Kindern, die in einigen Fällen vor vier Jahren bei einem Diebstahl ertappt wurden. Einem Entwurf zur Novellierung der Strafprozeßordnung entnehme ich, daß derartige Daten auch künftig – allerdings nur zwei Jahre lang – gespeichert werden sollen. Demgegenüber hat das Innenministerium die Polizei angewiesen, Kinder unter 10 Jahren in manuellen oder automatisierten Datensammlungen grundsätzlich nicht zu speichern. Das Staatsministerium der Justiz hat mitgeteilt, daß die Daten über strafunmündige Kinder im automatisierten Zentralen Namensregister nach 3 Jahren gelöscht werden. Es prüfe derzeit unter Beteiligung der staatsanwaltschaftlichen Praxis, ob es möglich ist, diese Daten schon früher zu löschen.

Wenn ich auch insgesamt feststellen konnte, daß die Staatsanwaltschaft auf die Einhaltung datenschutzrechtlicher Bestimmungen große Mühen verwendet, so mußte ich doch beanstanden, daß eine Aussonderung von Daten nach Angaben der Staatsanwaltschaft nur bei UJs-Verfahren (Verfahren mit unbekannten Tätern) möglich war. Obwohl die Justizverwaltung differenzierte Aussonderungsfristen, beginnend 1986, vorgesehen hatte, fand im Juni 1988 eine Aussonderung noch nicht statt. Wie die Justizverwaltung zwischenzeitlich mitgeteilt hat, war die Unterlassung der Aussonderung auf einen Bedienungsfehler bei der Staatsanwaltschaft zurückzuführen. Die Aussonderung wird nunmehr durchgeführt. Außerdem wurden sämtliche bayerischen Staatsanwaltschaften bei einem Erfahrungsaustausch mit der Justizverwaltung nochmals um rechtzeitige Aussonderung gebeten. Die ADV-Verbindungsstellen bei den Oberlandesgerichten Nürnberg und Bamberg werden

die Staatsanwaltschaften bei den Aussonderungsläufen künftig gezielt unterstützen.

Außerdem habe ich festgestellt, daß die Staatsanwaltschaft im Vorzimmer des Behördenleiters eine Personalkartei führt, in der u. a. die Daten Hochzeitstag, Geburtsname der Ehefrau, (Nicht-)Bestehen sowie Ergebnis und Platzziffer von teilweise Jahrzehnte zurückliegenden Prüfungen sogar noch nach der Pensionierung des Bediensteten vorgehalten werden. Ich habe Zweifel geäußert, ob die Speicherung der vorgenannten Daten zur rechtmäßigen Erfüllung der durch Rechtsnorm der Staatsanwaltschaft zugewiesenen Aufgaben erforderlich ist und dies in meinem Prüfungsbericht zum Ausdruck gebracht.

Die Justizverwaltung hält die Kartei für grundsätzlich erforderlich. Sie teilt allerdings meine Auffassung, daß die Speicherung von Angaben zum Religionsbekenntnis, zum Hochzeitstag und zu nicht bestandenen Prüfungen nicht erforderlich ist. Sie hat die Staatsanwaltschaft gebeten, diese Daten in der Kartei unkenntlich zu machen und künftig nicht mehr aufzunehmen. Weiterhin hat sie angeordnet, daß die Kartei ständig unter Verschluß zu halten ist, so daß ein Zugriff Unbefugter nahezu ausgeschlossen ist.
Der Beirat beim Landesbeauftragten wünschte, daß der Inhalt dieser Kartei noch weiter zurückgeführt wird.

6.3.2. Prüfung einer Justizvollzugsanstalt (JVA)

Die datenschutzrechtliche Prüfung einer JVA endete mit einem erfreulichen Ergebnis: Die JVA mißt dem Datenschutz einen hohen Stellenwert bei. Datenschutzrechtliche Verstöße waren nicht zu beanstanden.

Anlaß für die Prüfung gab die zunehmende Automatisierung der Geschäftsabläufe in den Justizvollzugsanstalten. Während die Arbeits- und Wirtschaftsverwaltung sowie die Vollzugsgeschäftsstelle bereits bei mehreren Justizvollzugsanstalten EDV-unterstützt betrieben werden, wird in der geprüften JVA zusätzlich ein automatisiertes Alarm- und Kommunikationssystem erprobt. Den Vollzugsbediensteten stehen über diese Anlage die Stammdaten der Gefangenen, begrenzte Informationen zur Tätigkeit und zur finanziellen Situation der Gefangenen sowie zur Haftraumbelegung zur Verfügung. Darüber hinaus sind in der Anlage sog. Sicherheitsvermerke (Fluchtgefahr, gewalttätig, Freitodgefahr, Trennungsvermerk usw.) gespeichert, deren Vergabe besondere Sorgfalt erfordert, da eine unrichtige Speicherung diskriminierend wirken kann.

Nach Abschluß des Probelaufs müssen die Voraussetzungen für die Aufnahme eines Sicherheitsvermerks, dessen Speicherungsdauer und die Löschungsfristen in einer Dienstanweisung geregelt werden, wobei im medizinischen Bereich u. U. besondere Sicherheitsmaßnahmen veranlaßt sind. Insoweit habe ich der Justizverwaltung Anregungen gegeben.

Weiterhin habe ich zur Erforderlichkeit und zum Umfang einzelner, derzeit verwendeter Sicherheitsvermerke Anregungen gegeben. Die Justizverwaltung wird meine Überlegungen bei der endgültigen Festlegung des Inhalts der einzelnen Datensätze berücksichtigen.

Bei der Erhebung und Eingabe von Gefangenendaten im Rahmen der EDV-Unterstützung der Vollzugsgeschäftsstelle habe ich Anregungen zur Datensicherheit gegeben: Die Gefangenendaten werden zunächst auf einem Erhebungsbogen erfaßt und dann über ein Terminal, das mehreren Bediensteten zugänglich ist, in eine Datei eingestellt. Welcher Bedienstete eine Eingabe, Änderung oder Löschung veranlaßt hat, kann derzeit nicht festgestellt werden. Die Vergabe eines Kennworts an jeden berechtigten Bediensteten würde diesen Mißstand beheben, wenn gleichzeitig sichergestellt würde, daß sich jeder Benutzer bei Beendigung eines Arbeitsvorgangs vom System abmeldet oder den Bildschirm „deaktiviert".

Die Gefangenen werden bei der Entlassung auf die Möglichkeit hingewiesen, die im Vollzug gewonnenen erkennungsdienstlichen Unterlagen löschen zu lassen (§ 86 Abs. 3 StVollzG). Einen entsprechenden Antrag können sie nach der Praxis der JVA jedoch erst nach der Entlassung stellen. Anträge sind daher selten. Diese Sachbehandlung entspricht zwar dem Wortlaut, aber nicht Sinn und Zweck der Vorschrift.

6.4. Grundbuchrecht

6.4.1. EDV-Eigentümer-/Grundstücksverzeichnis beim Grundbuchamt München

Das Grundbuchamt München hat im September 1986 begonnen, die für das Auffinden der Grundbuchstellen benötigten Verzeichnisse mit Hilfe der EDV zu führen. Zwischenzeitlich wird dieses Verfahren in etwa einem Viertel der 78 Münchener Grundbuchbezirke angewandt. Aufgrund einer Reihe technischer Probleme wird am endgültigen Programm noch gearbeitet.

Hierbei ergeben sich eine Reihe technischer und rechtlicher Probleme: So haben die Mitarbeiter von Notaren, Behörden und künftig möglicherweise auch Mitarbeiter von Banken und Sparkassen über einen Bildschirm Zugang zum EDV-Eigentümerverzeichnis, das u. a. den Namen, das Geburtsdatum und die Anschrift des Grundstückseigentümers sowie Angaben zu den Eigentumsverhältnissen am Grundstück enthält und der Auffindung einer gesuchten Grundbuchstelle dient. Außerdem besteht kein besonderer Datenschutz bei Daten, denen aufgrund der Person des Betroffenen Sensibilität zukommen kann.

Die Justiz prüft derzeit die damit verbundenen datenschutzrechtlichen Fragen und sucht nach Lösungsmöglichkeiten, die sowohl dem Anspruch auf Grundbucheinsicht wie auch dem Datenschutz gerecht werden.

6.4.2. Protokollierung der Einsicht in das Grundbuch

Eine Fälschung im Geschäftsbereich des Grundbuchamts München, die beinahe zu einem Millionenschaden geführt hätte, beschäftigte in letzter Zeit die Medien. Das Staatsministerium der Justiz hält weitere Vorschriften zum Schutz des Grundbuchs gleichwohl weder für zweckmäßig noch für geboten. Dem kann ich mich nicht anschließen.

Nach § 12 Grundbuchordnung (GBO) ist die Einsicht des Grundbuchs jedem gestattet, der ein berechtigtes Interesse darlegt. Eine Protokollierung derartiger Vorgänge findet nicht statt, obwohl durch die Einsichtnahme sensible, personenbezogene Daten bekannt werden können.

Mit dem Recht auf informationelle Selbstbestimmung ist eine Rechtsordnung nicht vereinbar, in der Bürger nicht mehr wissen können, wer was wann und bei welcher Gelegenheit über sie weiß. Das Grundrecht auf informationelle Selbstbestimmung legt es somit nahe, dem Bürger

durch eine Protokollierung der Grundbucheinsichtnahme die Möglichkeit zu geben, sich entsprechend zu unterrichten, wer über die Rechtsverhältnisse an seinem Grundstück Auskunft erhalten hat.

Ich verkenne nicht, daß damit ein nicht unerheblicher Verwaltungsmehraufwand verbunden wäre und neue Datenschutzfragen geschaffen würden: Durch die Protokollierung entstehen neue Bestände an personenbezogenen Daten (hier: insbesondere der Einsichtnehmenden), die mit einigem Aufwand vor Mißbrauch zu schützen wären. Andererseits ist zu berücksichtigen, daß beispielsweise § 36 Straßenverkehrsgesetz (StVG), der den automatisierten Abruf von Kraftfahrzeug- und Halterdaten durch hoheitliche Stellen regelt, erhebliche Protokollierungspflichten vorsieht, die bei der Grundbucheinsicht – durch Private – um so dringlicher erscheinen. Gleichzeitig würde damit auch ein besserer Schutz des Grundbuchs dadurch erreicht, daß ein Täter, der bei Gelegenheit der Einsicht eine Fälschung vornimmt, leichter als derzeit ermittelt werden kann.

Die Notwendigkeit der Protokollierung belegt auch eine Eingabe: Zwei Bürger hatten sich darüber beschwert, daß ein Grundbuchamt einem Dritten zu Unrecht Einsicht in das Grundbuch gewährt habe. Politische Gegner würden die dabei gewonnenen Erkenntnisse über Belastungen und Hypothekengläubiger zum Nachteil der Beschwerdeführer ausnutzen. Das Grundbuchamt konnte mir auf Anfrage keine eindeutige Auskunft über eine etwaige Einsichtnahme geben, weil nicht einmal über die Person des Einsichtnehmenden eine Aufzeichnung gemacht wird. Dieser Umstand muß Unberechtigte zur Einsichtnahme geradezu ermuntern.

Gleichwohl besteht – wie bereits erwähnt – seitens der Justiz wohl wegen des bürokratischen Aufwands derzeit wenig Bereitschaft, § 12 GBO zu novellieren. Der Arbeitskreis Justiz der Datenschutzbeauftragten hat daher beschlossen, zu diesen Fragen ein grundlegendes Papier zu erarbeiten und anschließend nochmals an die Justizverwaltungen heranzutreten.

6.4.3. Mitteilungen von Grundbuchämtern anläßlich von Eintragungen und Grundbuchumschreibungen

Wiederum haben – wie auch schon in den Vorjahren – Bürger die Frage an mich herangetragen, ob es datenschutzrechtlich zulässig sei, bei Umschreibungen des Grundbuchs oder Eintragungen in das Grundbuch allen Betroffenen umfassende Grundbuchauszüge mit Eigentumsverhältnissen sowie Namen, Geburtsdaten und Wohnort der Eigentümer zu übersenden.

Obwohl ich für dieses Anliegen durchaus Verständnis habe, konnte ich den Bürgern nicht helfen: Nach Art. 2 Abs. 2 BayDSG gehen besondere Vorschriften über Verfahren der Rechtspflege den Bestimmungen dieses Gesetzes vor. Zu den besonderen Vorschriften in diesem Sinn gehören auch die in der Grundbuchverfügung (GBVfg.) und der GBO getroffenen Regelungen über Mitteilungen aus dem Grundbuch. So schreibt § 39 Abs. 3 Satz 1 GBVfg. vor, daß die Umschreibung des Grundbuchblattes u. a. dem Eigentümer mitzuteilen ist. Nach § 55 GBO soll jede Eintragung u. a. dem Antragsteller und dem eingetragenen Eigentümer mitgeteilt werden. In welcher Form die hiernach vorgesehenen Mitteilungen erfolgen, hat der Rechtspfleger zu entscheiden. Dieser wiederum ist nach § 9 Rechtspflegergesetz selbständig, ihm können von der Justizverwaltung keine Hinweise über das einzuhaltende Verfahren gegeben werden.

Eine Reduzierung des Datenflusses ist grundsätzlich möglich, ohne daß dadurch die Rechte der Betroffenen geschmälert werden. Eine Verbesserung des Datenschutzes wäre de lege ferenda zu erreichen, wenn formblattmäßig die Tatsache der Änderung den Betroffenen mitgeteilt und anheimgegeben würde, einen Grundbuchauszug anzufordern.

6.5. Gesetzgebung

6.5.1. Strafprozeßordnung

Der Bundesjustizminister bereitet die Novellierung der Strafprozeßordnung (StPO) vor, d.h. die Ergänzung um Regelungen für Fahndungsmaßnahmen, Fahndungshilfsmittel, die Speicherung, Nutzung und Übermittlung personenbezogener Daten durch die Strafverfolgungsbehörden sowie für die Akteneinsicht im Strafverfahren. Als Kernproblem hat sich die Abstimmung der neuen StPO-Bestimmungen mit dem Polizeirecht herauskristallisiert, worauf ich schon in meinem letzten Tätigkeitsbericht hingewiesen hatte. Dieser Frage kommt auch weitreichende Bedeutung zu, da hierbei zu entscheiden ist, wer die Verantwortung für Datensammlungen trägt und damit Herr des Strafverfahrens ist. Darüber hinaus sollen die Zentralen Namensregister der Staatsanwaltschaften offenbar zu einem umfassenden Informationssystem ausgebaut werden. Dies würde eine grundlegende Überarbeitung des ADV-Verfahrens voraussetzen, um Gefährdungen des Persönlichkeitsrecht zu begegnen (vgl. auch 6.1).

Aus datenschutzrechtlicher Sicht stellt der letzte Entwurf, der derzeit beim Bundesminister der Justiz wiederum überarbeitet wird, keine Verbesserung dar: Die Straftatenkataloge zur Zulässigkeit der Rasterfahndung und der „Polizeilichen Beobachtung" wurden erweitert, Unterrichtungs- und Löschungsvorschriften zu Lasten des Betroffenen vereinfacht und die Akteneinsicht ebenfalls erweitert.

6.5.2. Jugendgerichtsgesetz (JGG)

Die JGG-Novelle behandelt Fragen des Datenschutzes allenfalls am Rande. Die Justizverwaltung hat allerdings eingeräumt, daß insoweit ein Regelungsbedarf besteht. Zu prüfen sind insbesondere die Datenflüsse zwischen Jugendgericht, Jugendgerichtshilfe, Jugendamt, Bewährungshelfer, Stellen, gegenüber denen Auflagen oder Weisungen zu erfüllen sind, Eltern und sonstigen Bezugspersonen (vgl. § 24 Abs. 2, § 38 Abs. 2 JGG i. V. m. §§ 67 ff SGB X).

6.5.3. Strafvollzugsgesetz

Die Justiz arbeitet im Strafvollzug in einigen Bereichen schon derzeit EDV-unterstützt. Bei den Ein- und Auszahlungsstellen findet z.B. das Verfahren „ADV-Gefangenengelderbuchführung" und „Lastschrifteinzugsverfahren" Anwendung. Außerdem wird das ADV-Verfahren „Lohnabrechnung der Gefangenen" benutzt. Das EDV-System einer Alarm- und Kommunikationsanlage wurde bereits beschrieben (vgl. zu diesen Verfahren auch 6.3.2).

Eine Sachkommission „ADV im Strafvollzug" der Justizverwaltung entwickelt nunmehr ein Grundkonzept für die erweiterte Datenverarbeitung in den Vollzugsanstalten.

Außerdem sollen die Möglichkeiten eines Datenträgeraustausches zwischen den Vollzugsanstalten untersucht und gemeinsame DV-technische Ordnungsbegriffe festgelegt werden. Gesetzliche Rahmenbedingungen hierfür sind nicht festgelegt. Der Bundesminister der Justiz hatte zwar vor einigen Jahren einen datenschutzrechtlich durchaus erfreulichen Gesetzentwurf zur Änderung des Strafvollzugsgesetzes vorgelegt. Die Landesjustizverwaltungen haben diesen Entwurf jedoch ebenso entschieden abgelehnt wie den Entwurf eines Jugendstrafvollzugsgesetzes im Jahr 1984, der allerdings keinerlei Datenverarbeitungsvorschriften enthielt.

Regelungsbedürftig dürften insbesondere folgende Gebiete sein: Im Strafvollzugsgesetz das Aufnahmeverfahren, die ärztliche Untersuchung, der Vollzugsplan, die Überwachung des Schriftwechsels der Gefangenen. Die Vorschriften über erkennungsdienstliche Maßnahmen sind zu ergänzen oder abzuändern. Rechtsgrundlagen für die Verarbeitung von personenbezogenen Daten Dritter, d.h. von Personen außerhalb der Justizvollzugsanstalten, sind neu zu schaffen. Die zahlreichen Datenübermittlungen an öffentliche Stellen wie auch an Private bedürfen einer gesetzlichen Regelung. Fristen zur Löschung von Daten sind vorzusehen.

6.5.4. Schuldnerverzeichnis

Verschiedentlich haben mich Bürgereingaben erreicht, in denen z. B. Klage geführt wurde, daß unaufgefordert von mehr oder weniger seriösen Kreditinstituten Finanzierungsangebote unterbreitet wurden. In anderen Fällen wurde gutsituierten Personen, etwa einem seit Jahrzehnten etablierten Zahnarzt, ein kleiner Kredit wegen angeblicher Kreditunwürdigkeit verweigert.

Die bayerischen Amtsgerichte führen nach § 915 Zivilprozeßordnung (ZPO) ein Schuldnerverzeichnis, in das alle Personen eingetragen werden, welche die eidesstattliche Versicherung über ihr Vermögen abgegeben haben oder gegen die wegen Nichtabgabe der eidesstattlichen Versicherung Haft angeordnet ist. Über das Bestehen oder Nichtbestehen einer bestimmten Eintragung in das Schuldnerverzeichnis wird nach § 915 Abs. 3 ZPO jedermann auf Antrag Auskunft erteilt. Der Nachweis eines berechtigten Interesses ist nicht erforderlich.

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

Die für die Erteilung von Auskünften und Abschriften aus dem Schuldnerverzeichnis maßgebenden Rechtsgrundlagen sind seit längerer Zeit als änderungsbedürftig erkannt, was mehrere Novellierungsversuche des Bundesministers der Justiz belegen. Unbeschadet dessen ist das Verfahren gegenwärtig aus datenschutzrechtlicher Sicht im Hinblick auf die Regelungen in der Zivilprozeßordnung grundsätzlich noch nicht zu beanstanden. Allerdings wird eine Novellierung immer dringlicher.

Soweit den Eingaben Personenverwechslungen zugrunde liegen – dies war bei dem eingangs erwähnten Zahnarzt der Fall –, ist regelmäßig bereits von der Justizverwaltung das Notwendige veranlaßt. Allerdings lassen sich nicht sämtliche Nachteile, die unbescholtene Bürger erleiden, ausgleichen. Aufgrund des weiten Bezieherkreises der IHK-Schuldnerlisten ist im übrigen ein Mißbrauch kaum zu verhindern wie die Angebote von Kredithaien an Schuldner zeigen. Diese Gefährdungen müssen bei einer baldigen Novellierung angemessen berücksichtigt werden.

6.6. Memminger Strafverfahren wegen Schwangerschaftsabbrüchen

Eine Reihe von Anfragen betrafen die bei den Justizbehörden in Memmingen anhängigen Verfahren gegen zahlreiche Frauen und einen Arzt wegen Verdachts des Schwangerschaftsabbruchs. Die Strafverfahren wurden von der örtlichen Steuerfahndungsstelle in Gang gebracht, welche die Praxisräume des Arztes aufgrund richterlichen Beschlusses wegen des Verdachts von Steuerstraftaten durchsucht hatte. Aus der beschlagnahmten Patientenkartei ergab sich der Verdacht verbotener Schwangerschaftsabbrüche.

Ärztliche Karteikarten betreffen nach einer Entscheidung des Bundesverfassungsgerichts den privaten Bereich der Patienten. Damit nehmen sie am Schutz der Privatsphäre nach Art. 2 Abs. 1 i. V. m. Art. 1 Abs. 1 Grundgesetz (GG) teil. Wer sich in ärztliche Behandlung begibt, kann erwarten, daß Kenntnisse des Arztes über den Gesundheitszustand im Regelfall geheim bleiben. Ausnahmsweise kann aber u. a. das öffentliche Interesse an einer möglichst vollständigen Wahrheitsermittlung im Strafprozeß das private Geheimhaltungsinteresse dann überwiegen, wenn der Arzt selbst einer Straftat beschuldigt wird oder der Teilnahme an einer strafbaren Handlung des beschuldigten Patienten verdächtig ist, sofern es zur Aufklärung derartiger Straftaten des Einblicks in die Patientenkartei bedarf. Sind diese Voraussetzungen erfüllt, dann sind die Einblicknahme und die Verwertung der dabei gewonnenen Informationen zulässig (Bundesverfassungsgerichts, amtliche Sammlung, 32. Band, S. 373 ff).

Die vorstehend aufgezählten Fragen sind von den zuständigen Gerichten entschieden worden. Ich habe daher im Hinblick auf die von Art. 97 GG und Art. 85 Bayerische Verfassung geschützte richterliche Unabhängigkeit davon abgesehen, eine rechtliche Wertung vorzunehmen, um nicht in unzulässiger Weise in den meiner Kompetenz nicht unterworfenen Bereich der Rechtspflege einzugreifen.

Im übrigen hat die Staatsanwaltschaft zur Bewältigung der zahlreichen Strafverfahren eine Datei angelegt, zu der ich frühzeitig Empfehlungen zur Datensicherung gegeben habe.

7. Regierungen, Städte, Gemeinden

7.1. Datenschutzlücke im Gemeinderat

Mehrfach mußte ich der Presse und Eingaben entnehmen, daß der Datenschutz der Bürger bei der Behandlung persönlicher Angelegenheiten in nichtöffentlichen Sitzungen verletzt wird. So beklagen sich Bürger darüber, daß aus dem Gemeinderat heraus persönliche Angaben über sie öffentlich bekannt würden, beispielsweise ihr Einkommen,

ihre wirtschaftlichen Belastungen, Geschäftsbeziehungen, Eigentumsverhältnisse u. ä..

Diese Verletzungen des Datenschutzes durch Indiskretionen aus dem Gemeinderat heraus verwundern um so weniger, als die gesetzlichen Vorschriften zum Schutz der Persönlichkeitsrechte der Bürger im Gemeinderat auf eine Zeit zurückgehen, als „Datenschutz" noch ein Fremdwort war, und der Schutz der Bürger vor Mißbrauch ihrer personenbezogenen Daten im Gemeinderat entsprechend unterentwickelt ausgestaltet ist.

Zwar sind Beratungsgegenstände, bei denen sensible personenbezogene Daten eines Bürgers zur Sprache kommen, nach der Gemeindeordnung in nichtöffentlicher Sitzung zu behandeln. Diese Schutzbestimmung geht aber ins Leere, wenn sie allzu locker gehandhabt wird und die Anwesenheit in der nichtöffentlichen Sitzung auch Personen gestattet wird, die weder Gemeinderatsmitglied noch in der Gemeindeverwaltung mit der behandelten Angelegenheit befaßt oder mit dem ordnungsgemäßen Ablauf der Gemeinderatssitzung betraut sind. Das gilt auch für die unzulässige Anwesenheit von Vertretern der Presse.

Für den Datenschutz im Gemeinderat gänzlich unbefriedigend sind die in der Gemeindeordnung vorgesehenen Sanktionen bei Verletzungen der Verschwiegenheitspflicht. Die Strafvorschrift des § 353 b StGB (Verletzung von Dienstgeheimnissen und besonderen Geheimhaltungsvorschriften eines Amtsträgers) scheidet als Schutzvorschrift zugunsten des Bürgers aus, weil eine Gefährdung wichtiger öffentlicher Interessen vorausgesetzt wird. Die Verletzung des Persönlichkeitsrechts eines Bürgers oder seiner privaten Belange reicht nicht aus.

Zwar haben Gemeinderäte über die ihnen bekanntgewordenen Angelegenheiten Verschwiegenheit zu wahren, soweit diese Umstände nicht offenkundig sind. Zuwiderhandlungen können mit Ordnungsgeld bis zu 500 DM belegt werden (Art. 20 Abs. 2 und 3 der Gemeindeordnung). Es darf aber mit Fug und Recht bezweifelt werden, ob der Umstand, lediglich ein Ordnungsgeld in eher geringer Höhe zu riskieren, den Persönlichkeitsschutz der Bürger im gebotenen Maß gewährleisten kann. Zudem liegt es im freien Ermessen des Gemeinderats, gegen eines seiner Mitglieder Ermittlungen anzustellen und ein Bußgeld festzusetzen. Von einem effektiven Schutz der Betroffenen kann bei einer solchen „Sanktion" keine Rede sein. Für notwendig halte ich hingegen eine angemessene Strafvorschrift. Nach Auffassung des Datenschutzbeirats sollte geprüft werden, ob von der Möglichkeit, Ordnungsgelder zu verhängen, ausreichend Gebrauch gemacht wird, oder eine Verschärfung der Gesetzesbestimmungen notwendig ist.

7.2. Prüfungen

7.2.1. Prüfung einer Regierung

Erstmals wurde eine Regierung auf die Einhaltung des Datenschutzes hin überprüft. Die Prüfung sollte nicht nur eventuelle datenschutzrechtliche Mängel aufdecken. Meine Mitarbeiter sollten auch eine Beratung bei datenschutzrechtlichen Problemen und Zweifelsfragen anbieten.

Bei der Kontrolle wurden erfreulicherweise nur wenige gravierende Mängel festgestellt, die im wesentlichen die Bereiche Beihilfeverwaltung und Datensicherheit betrafen. Abgesehen von teilweise unzulänglicher und nicht datenschutzgerechter Aufbewahrung war der größte Teil der insgesamt 28 überprüften Dateien nicht zu beanstanden.

Im wesentlichen ergaben sich folgende Mängel, die ich formal beanstandet habe:

- Beihilfeverwaltung
  Die Beihilfeverwaltung befolgte nicht die vom Staatsministerium des Innern für seinen Geschäftsbereich festgelegten Grundsätze, wonach die Bediensteten Beihilfeanträge und Belege in einem verschlossenen Umschlag einreichen sollen und diese Umschläge nur von den Beihilfestellen geöffnet werden dürfen. Bei der geprüften Regierung wurden die an die Beihilfestelle adressierten Umschläge hingegen bereits von der Poststelle geöffnet, bevor sie an die Beihilfestelle weitergeleitet wurden. Die Regierung hat mir inzwischen mitgeteilt, daß neue Beihilfeantragsformulare ausgegeben werden, die den Hinweis enthalten, Beihilfeanträge in einem mit dem Wort „Beihilfe" versehenen Umschlag einzureichen. So gekennzeichnete Briefumschläge werden künftig von der Einlaufstelle ungeöffnet an die Beihilfestelle weitergeleitet.

  Auch die Organisation des Schreibdienstes in der Beihilfeverwaltung war nicht geeignet, das Persönlichkeitsrecht der Bediensteten und ihrer Angehörigen im gebotenen und möglichen Umfang zu wahren. Zum Fertigen der Auszahlungsanordnungen und der Überweisungsträger wurde dem Schreibdienst, der nicht ausschließlich für die Beihilfeverwaltung schrieb, der gesamte Beihilfeakt zugeleitet, der zum aktuellen Antrag auch noch die Arztrechnungen mit Diagnosen enthielt. Auch der Verschluß der Akten nach Dienstschluß war nicht gewährleistet.

- Erforderlichkeit der Daten
  Bei der Durchsicht einzelner Dateien (z.B. Hebammen-Kartei, Kartei der ausländischen Ärzte und Zahnärzte) wurden Datenarten festgestellt, die zur Aufgabenerfüllung nicht erforderlich waren (z.B. Religionszugehörigkeit der Hebamme, Beruf des Ehegatten der Hebamme) oder deren Erforderlichkeit bezweifelt und noch geklärt werden muß (z.B. Staatsangehörigkeit der Ehefrau und Anzahl der Kinder der ausländischen Ärzte und Zahnärzte). Soweit feststand, daß die Daten nicht erforderlich sind, habe ich ihre Löschung gefordert; dieser Forderung ist entsprochen worden.
- Dauer der Aufbewahrung von Daten in Dateiform
  Beanstandet werden mußte, daß Daten in Dateiform zu lange bereitgehalten werden über Fälle, die bereits abgeschlossen waren und in denen die vorgehaltenen Daten nur noch zum Beantworten von Anfragen anderer Behörden genutzt wurden. Eine Aufbewahrung solcher Daten in einer Kartei über einen Zeitraum von 5 Jahren erachte ich noch als angemessen. Nach dieser Zeit ist die Karteikarte zum Akt zu nehmen. Die Regierung hat mir mittlerweile mitgeteilt, daß bei der konkret beanstandeten Datei Karteikarten nach Abschluß des Falles künftig sogleich zum Akt genommen werden.
- Datensicherheit
  Mängel zeigten sich auch bei der Aufbewahrung der Daten. Häufig wurden Akten und Karteien mit personenbezogenen Daten in nicht verschließbaren oder nur mit einem einfachen Schloß gesicherten Schränken und Schreibtischen aufbewahrt. Einfaches, nur mit einem

Rolloverschluß versehenes Mobiliar, unverschlossene und unbefestigte verschließbare Karteikästen sind jedenfalls dann keine geeigneten Aufbewahrungsmittel, wenn darin besonders sensible Daten verwahrt werden sollen. In diesem Punkt sind inzwischen von der Regierung Maßnahmen zu einer datenschutzgerechteren Aufbewahrung getroffen worden. Alle wegen mangelnder Datensicherung beanstandeten Dateien sind nun zumindest in einem abschließbaren Schrank untergebracht.

- Meldungen zum Datenschutzregister
  Bei einigen Dateien fehlte die vorgeschriebene Meldung zum Datenschutzregister. Auch dies habe ich beanstandet. Ein Teil der Meldungen wurde inzwischen nachgeholt.

Im übrigen konnte ich einige Anregungen zu einem sorgsameren Umgang mit personenbezogenen Daten geben sowie einzelne bei der Besichtigung aufgetretene Fragen, vor allem hinsichtlich der Erforderlichkeit bestimmter Datennutzungen, klären. Meine Hinweise, die sämtlich berücksichtigt worden sind, betrafen vor allem folgende Punkte:

- Gleitzeiterfassung
  Wie allgemein üblich, sollte es den Mitarbeitern freistehen, ihren Namen in die Zeiterfassungskarte vor Abgabe der Karte an den Sachgebietsleiter einzutragen, wenn die Karten während des Abrechnungsmonats in einem für jeden zugänglichen Kartenfächer aufbewahrt werden.
- Telefondatenerfassung
  Bei der Telefondatenerfassung sollten die technischen Möglichkeiten des entsprechenden Systems zu datenschutzgerechten Lösungen wahrgenommen werden, so z.B. der nur verstümmelte Ausdruck der Zielnummer auf der Rechnung für private Telefongespräche.
- Unterrichtung des internen Datenschutzbeauftragten
  Der interne Datenschutzbeauftragte sollte einen aktuellen Überblick über die bei der jeweiligen Behörde geführten Dateien haben. Er ist daher sowohl über neue als auch über die Vernichtung oder Abgabe bestehender Dateien zu unterrichten.
- Datenverarbeitung im Auftrag
  Betreibt eine Behörde Datenverarbeitung im Auftrag, so sollte sichergestellt sein, daß die mit der Datenverarbeitung befaßten Mitarbeiter über die rechtliche Bedeutung dieser Art der Datenverarbeitung unterrichtet sind.

7.2.2. Prüfungen bei Gemeinden

Wie bereits im 9. Tätigkeitsbericht angekündigt, habe ich meine Kontrolltätigkeit im Bereich der automatisierten Melderegisterführung im Berichtszeitraum verstärkt und insbesondere Gemeinden geprüft, die selbst automatisierte Einwohnerverfahren einsetzen.

Dabei hat sich bestätigt, daß sich ein von der AKDB angebotenes teildezentrales Einwohnerverfahren in melderechtlicher, aber auch in softwaremäßiger Hinsicht wohltuend von den geprüften Verfahren privater Anbieter abhebt. Auch das AKDB-Verfahren ist nicht absolut mängelfrei. Die nachstehenden Mängel habe ich bei Verfahren privater Anbieter beanstandet:

- Keine Reduzierung der Datenspeicherung bei Nebenwohnung (Nr. 3.2 Satz 2 VollzBekMeldeG);
- keine Reduzierung der Datensätze verstorbener oder weggezogener Bürger (Art. 11 Abs. 2 MeldeG);
- keine überwachungsfähige Speicherung von Aufenthaltsfragen gem. Art. 3 Abs. 2 Nr. 6 MeldeG (2-Jahresfrist wird nicht überwacht);
- keine Löschung des Feldinhaltes „Anschrift am 1. September 1939" gem. Nr. 33 Nr. 3 VollzBekMeldeG;
- unzulässige Speicherung sowie Auswertungsmöglichkeiten des Datums „Familienvorstand" in der Hierarchie des Familienverbandes;
- unzulässige Hinweise auf bereits vollzogene Adoption; (entgegen Nr. 3.1.5 VollzBekMeldeG)
- unzulässige Querverweise auf die Eltern Volljähriger (Nr. 3.1.4 VollzBekMeldeG);
- keine Differenzierung zwischen personenstandsrechtlichem Familienstand „verheiratet" und lohnsteuerrelevantem Status „dauernd getrennt lebend";
- unzulässige Speicherung des Feldes „zählt zur Wohnbevölkerung" bei Nebenwohnungen;
- unzulässige Speicherung der Datenfelder „Berufsgruppe", „Nummer des Ausländerzentralregisters" und „Aufenthaltserlaubnis";
- unzulässige Speicherung von Pflegschaftsdaten und Daten des Pflegers bei Wahlrechtsausschlüssen (Art. 3 Abs. 2 Nr. 1 MeldeG);
- unzureichende Begrenzung auf männliche Deutsche bei „Wehr // Zivildienstüberwachung" sowohl bei Speicherung als auch bei Datenübermittlung an Wehrersatzbehörde (Datum „Wehrüberwachung" darf nur aufgrund besonderer Mitteilungen der Wehrersatzbehörde bei über 32-jährigen gespeichert werden; Datum „Zivildienstüberwachung" ist unzulässig);
- unzulässige Speicherung von Bankverbindungen Feuerwehrabgabepflichtiger;
- unzureichende Schlüssel für „Art des Ausweises", insbesondere bei ausländischen Personalpapieren (diese werden generell als „sonstiger (vorläufiger) Ausweis" gespeichert);
- unzureichende Differenzierung bei Übermittlungs- und Auskunftssperren sowie zwischen Ausschluß vom Wahlrecht und von der Wählbarkeit (z.B. werden eingelegte Widersprüche gem. Art. 35 Abs. 1 MeldeG = Wahlwerbung und Art. 35 Abs. 2 MeldeG = Jubiläumsdaten als „allgemeine Auskunftssperre" generiert; zwischen Ausschluß vom Wahlrecht und dem der Wählbarkeit wird nicht unterschieden);
- unzulässige Speicherung von Gründen, die zu bestimmten Maßnahmen führten: Beispiele: Gründe für Vornamensänderungen, Namensänderungen, Adreßbuchsperren, Konfessionswechsel, Eintragung einer gesetzlichen Vertretung, Staatsangehörigkeitswechsel; Ehescheidungs- und Eheaufhebungsgründe sowie Todesursachen.
- fehlende Plausibilitätskontrollen beim Aufbau eines Datensatzes, die sich bei Einsatz der EDV sehr empfehlen (z.B. werden bei Familienstand „ledig", „verwitwet", „geschieden" Angaben über einen nicht mitzuziehenden Ehegatten nicht abgewiesen; beim Familienstand „ledig" wird eingegebenes Eheschließungsdatum nicht abgewiesen; Eheschliessungsdatum, das in der Zukunft liegt, wird nicht abgewiesen; Zuzugsdatum, das in der Zukunft liegt, wird nicht abgewiesen; Feuerschutzabgabepflicht wird trotz Geburtsdatum 1987 und trotz Nebenwohnung akzeptiert; ebenso wurde trotz Geburtsdatum 1987 ein

Altersfreibetrag bei der Lohnsteuerkartenstelle akzeptiert);
- keine Begrenzung der Bildschirmmaskeninhalte auf das zur jeweiligen Aufgabenerfüllung erforderliche Maß bei Online-Anschlüssen (vgl. auch Nr. 8.8 des 9. Tätigkeitsberichts);
- keine variable „erweiterte" Melderegisterauskunft im automatisierten Verfahren möglich (nur Standardausdruck);
- Verfahren verhindert nicht, daß Daten (Nur-)Deutscher an die Ausländerbehörde übermittelt werden; – unzulässige Übermittlung von Personalausweis-/Paßdaten Weggezogener oder Verstorbener an die Polizei (durch § 7 Abs. 3 BayMeldeDÜV ausgeschlossen);
- keine ausreichende Begrenzung des Familienstandes auf „verheiratet oder nicht verheiratet" gem. Art. 32 Abs. 1 Nr. 9 MeldeG bei Datenübermittlungen an die Kirchen;
- verschiedene regelmäßige Datenübermittlungen ohne ausreichende Rechtsgrundlage (Art. 31 Abs. 4 und 5 MeldeG, BayMeldeDÜV) an andere öffentliche Stellen (z.B. Gesundheitsamt, Abwasserzweckverband);
- keine Benachrichtigung der Stellen (über berichtigte Daten), denen im Rahmen regelmäßiger Datenübermittlungen unrichtige Daten mitgeteilt wurden (Art. 10 Satz 2 MeldeG);
- unberechtigte Unterdrückung erforderlicher Datenübermittlungen an andere öffentliche Stellen, weil eine Auskunftssperre nach Art. 34 Abs. 5 MeldeG (u.a.) gespeichert ist (§ 13 BayMeldeDÜV wird nicht berücksichtigt).

Die geprüften Gemeinden wurden von mir gem. Art. 30 Abs. 1 BayDSG beanstandet. Die Beseitigung der Mängel wurde in angemessener Frist gefordert.

Die Prüftätigkeit in diesem Bereich wird fortgesetzt.

7.3. Oberbürgermeister: „Direkter Zugriff zur Datenverarbeitung"

Unter dieser Überschrift berichtete eine Tageszeitung, daß ein Oberbürgermeister nun ein ADV-Terminal im Amtszimmer stehen habe, das ihm „in Sekundenschnelle Zugriff zu allen Bereichen der zentralen elektronischen Datenverarbeitung" erlaube. Der Oberbürgermeister erhalte rund um die Uhr – auch am Wochenende wertvolle Informationen. Ihn interessierten insbesondere Finanzwesen, Einwohnermeldewesen, Kasse und Personalabteilung. Ein Bürger dieser Stadt äußerte daraufhin gegenüber dem Datenschutzbeauftragten Zweifel, ob dieser Direktzugriff rechtmäßig sei.

Die datenschutzrechtliche Überprüfung führte zu keiner Beanstandung. Dabei ist allerdings zu berücksichtigen, daß der Oberbürgermeister nicht auf „alle Daten aller Abteilungen der Stadtverwaltung" Zugriff hat, sondern aus dem Kreis der personenbezogenen Daten der Gemeindebürger in Wirklichkeit nur Meldedaten abrufen kann, und daß ihm das Meldewesen durch Stadtratsbeschluß zur selbständigen Erledigung übertragen ist. Daneben kann der Oberbürgermeister noch auf Stammdaten des städtischen Personals zugreifen.

Beim Direktzugriff des Oberbürgermeisters auf die Meldedaten hat das Staatsministerium des Innern in seiner Stellungnahme darauf abgestellt, daß dem Oberbürgermeister nach der Geschäftsordnung für den Stadtrat das Meldewesen übertragen ist. Es bestünden daher keine rechtlichen Bedenken dagegen, daß der Oberbürgermeister im Einzelfall Zugriff auf die Meldedaten nimmt, wenn dies entweder zur Entscheidung eines Einzelfalls oder zur Überwachung der Gemeindeverwaltung erforderlich sei. Dies gelte auch, wenn, wie in größeren Stadtverwaltungen notwendig und üblich, der Oberbürgermeister die Aufgaben der laufenden Verwaltung nicht selbst wahrnimmt, sondern an Gemeindebedienstete delegiert habe.

Den Direktzugriff auf Personalstammdaten hält das Staatsministerium des Innern für erforderlich, da der Oberbürgermeister Personalentscheidungen des Stadtrats vorzubereiten habe, soweit er diese Aufgabe nicht ohnehin aufgrund Übertragung durch den Stadtrat selbst wahrnimmt. Auch für die Dienstaufsicht über die städtischen Bediensteten hält das Innenministerium den Direktzugriff auf die Daten für erforderlich.

In meiner Bewertung bin ich davon ausgegangen, daß die Einrichtung eines Direktzugriffs des Oberbürgermeisters auf Daten der Bürger grundsätzlich deren Recht auf informationelle Selbstbestimmung berühren kann: Einmal, weil der Kreis der Personen, die die erhöhte Verfügbarkeit der Daten in der automatisierten Datei nutzen können, um Personen erweitert wird, die in die laufende Arbeitsabwicklung des Meldeamts normalerweise nicht eingebunden sind. Zum anderen, weil von einer zentralen Stelle aus der Direktzugriff auf Bürgerdaten nicht nur des Melderegisters, sondern auch aus anderen Dateien – etwa aus Steuer-, Sozial-, Krankenhausdateien oder Dateien des Ordnungsamtes möglich wäre. Je nach Umfang der Automatisierung in der Stadtverwaltung könnte dies dazu führen, daß von einer Stelle aus ein recht weitgehendes Datenprofil bestimmter einzelner Einwohner abrufbar wäre. Es gibt aber weder eine Befugnis noch ist es notwendig, daß e i n e Person oder Stelle innerhalb der Stadtverwaltung alle von den verschiedenen Dienststellen über denselben Bürger gespeicherten Daten – und das auch noch im Direktzugriff – kennt. Auch die Dienstaufsicht erfordert eine so umfassende Kenntnis und den Direktzugriff des Oberbürgermeisters auf eine Vielzahl von Daten eines Bürgers nicht.

Aus kommunalrechtlicher Sicht ist es wohl erforderlich, daß dem Bürgermeister die für die Wahrnehmung seiner Zuständigkeiten einschließlich der Dienstaufsichtsbefugnis erforderlichen Daten zur Verfügung stehen. Auch das Staatsministerium des Innern erkennt allerdings an, daß gerade der Online-Zugriff Probleme aufwerfen kann, wenn von einem einzigen Terminal aus die verschiedensten personenbezogenen Daten von Gemeindebürgern durch Direktzugriff abrufbar sind. Im vorliegenden Fall war diese Grundsatzfrage jedoch nicht zu entscheiden, da der Oberbürgermeister über keinen Direktzugriff zu allen Bürgerdaten verfügte, sondern nur über einen kleinen Ausschnitt.

7.4. Bauwesen

7.4.1. Gesetzliche Vorkaufsrechte der Gemeinden nach den Vorschriften des Baugesetzbuches

Erneut habe ich mich mit der Frage befaßt, unter welchen Voraussetzungen ein Notar einer Gemeinde zur Ausübung des Vorkaufsrechts den gesamten notariellen Kaufvertrag übermitteln darf. Hierbei ist zu berücksichtigen, daß öffentliche Stellen vom Inhalt eines zwischen Privaten abgeschlossenen Kaufvertrages nur Kenntnis erhalten

dürfen, soweit dies zur Erfüllung ihrer Aufgaben erforderlich ist.

Zwei Abgeordnete wandten sich an den Landtag mit dem Antrag, die Staatsregierung möge prüfen, ob das von der Landesnotarkammer Bayern vorgeschlagene zweistufige Verfahren zur Ausübung des Vorkaufsrechts der Gemeinden eingeführt werden könne. Dieses zweistufige Verfahren sieht vor, daß der Notar der Gemeinde zur Prüfung der Frage, ob ein Vorkaufsrecht besteht, zunächst nicht den gesamten notariellen Kaufvertrag übersendet. Vielmehr soll die Gemeinde in einem ersten Schritt über die Umstände unterrichtet werden, die es ihr erlauben zu entscheiden, ob für das verkaufte Grundstück überhaupt ein Vorkaufskaufsrecht besteht. Kommt die Ausübung des Vorkaufsrechts in Betracht, so kann die Gemeinde in einem zweiten Schritt die Übermittlung des vollständigen Inhalts des Kaufvertrages verlangen.

Allein dieses zweistufige Verfahren entspricht dem Grundsatz, daß nur die jeweils notwendigen Daten an andere Stellen übermittelt werden. Der Bayer. Gemeindetag hat inzwischen auf Bitten des Staatsministeriums des Innern die Städte, Märkte und Gemeinden über das zweistufige Verfahren unterrichtet.

7.4.2. Fehlbelegung im Wohnungsbau

Anläßlich einer Eingabe habe ich das Verfahren beim Vollzug des Gesetzes über den Abbau der Fehlsubventionierung im Wohnungsbau einer datenschutzrechtlichen Überprüfung unterzogen. Die Eingabe bezog sich auf die Wohnungsfürsorge für Beschäftigte des Freistaates Bayern (Vergabe von Staatsbedienstetenwohnungen). Der Petent rügte konkret, daß als Nachweis eine Kopie des vollständigen Arbeitsvertrages vorzulegen war.

Ich konnte nach einem Schriftwechsel mit der Bezirksfinanzdirektion München eine datenschutzfreundlichere Gestaltung der Vordrucke erreichen. Weggefallen sind z.B. Angaben über den Änderungstermin des Familienstandes und Fragen zum Inhaberwechsel der Wohnung, die zum Vollzug des Gesetzes über den Abbau der Fehlsubventionierung im Wohnungsabbau nicht erforderlich waren. In einem beigelegten Merkblatt wird nunmehr darauf hingewiesen, daß die Angaben über Behinderung, Aussiedler oder junge Ehepaare freiwillig sind; im Arbeitsvertrag können die Daten, die für die Festsetzung der Fehlbelegungsabgabe nicht benötigt werden, unkenntlich gemacht werden. Vorzulegende Nachweise (Ernennungsurkunden, Versetzungsverfügung, Arbeitsvertrag) können vom Betroffenen hinsichtlich der nichterforderlichen Daten ebenfalls unkenntlich gemacht werden.

7.4.3. Auskunftspflichten im Zusammenhang mit Bausanierungen

Gem. § 138 Abs. 1 des Baugesetzbuches (BauGB) sind Eigentümer, Mieter, Pächter und sonstige zum Besitz oder zur Nutzung eines Grundstückes, Gebäudes oder Gebäudeteils Berechtigte sowie ihre Beauftragten verpflichtet, der Gemeinde oder ihren Beauftragten Auskunft über die Tatsachen zu erteilen, deren Kenntnis zur Beurteilung der Sanierungsbedürftigkeit eines Gebietes oder zur Vorbereitung oder Durchführung der Sanierung erforderlich ist. An personenbezogenen Daten können insbesondere Angaben der Betroffenen über ihre persönlichen Lebensumstände im wirtschaftlichen und sozialen Bereich, namentlich über die Berufs-, Erwerbs- und Familienverhältnisse, das Lebensalter, die Wohnbedürfnisse, die sozialen Verflechtungen sowie über die örtlichen Bindungen, erhoben werden.

Die einzelnen Auskunftspflichten sind in einem Fragebogen zusammengefaßt. Eine Gemeinde wandte sich an mich mit der Bitte um datenschutzrechtliche Überprüfung des Fragebogens.

Aus datenschutzrechtlicher Sicht bestehen gegen die inhaltliche Gestaltung des Fragebogens keine Einwendungen. Der Fragebogen hat den vorgegebenen rechtlichen Rahmen eingehalten. Die Erforderlichkeit der einzelnen Fragen ergibt sich erkennbar aus dem angestrebten Sanierungsziel. Ich habe die Gemeinde jedoch darauf aufmerksam gemacht, daß die Auskunftspflicht der Betroffenen davon abhängt, ob die Gemeinde die Vorbereitung der Sanierung bereits förmlich durch einen Beschluß über den Beginn der vorbereitenden Untersuchungen eingeleitet hat.

7.5. Fehlerhafte Personalausweise und Reisepässe

In Nr. 7.1 des 9. Tätigkeitsberichtes habe ich die seinerzeit festgestellten Fehlerquellen, die zur Doppelvergabe von Personalausweisnummern führten, dargestellt und eine Verfahrensänderung bei der Bundesdruckerei für unbedingt erforderlich erachtet (Prüfung, ob eingehende Personalausweisnummern schon einmal vergeben worden sind).

Meines Wissens wurden diese Plausibilitätskontrollen inzwischen auf bundesweiten Druck hin realisiert. Gleichwohl wurden mir im Berichtszeitraum weitere Verfahrensmängel, die eine fehlerhafte Erstellung von Personalausweisen und Pässen durch die Bundesdruckerei zur Folge hatten, bekannt.

Obwohl die Ausweisbehörden die Anträge richtig ausgefüllt an die Bundesdruckerei geschickt hatten, häuften sich die Fälle, daß Buchstaben weggelassen oder hinzugefügt oder Ziffern verstümmelt auf den Ausweisen wiedergegeben wurden. Ebenso war es nicht gerade selten, daß von der Bundesdruckerei falsche Paßnummern in den nicht fälschungssicheren Teil der Reisepässe eingestanzt wurden. Ohne die Aufmerksamkeit der Ausweisbehörden würden nicht wenige Bundesbürger mit fehlerhaften oder falschen Personalpapieren ausgestattet sein, was bei Kontrollen die schutzwürdigen Belange der Betroffenen u.U. beeinträchtigen könnte.

Meine Erkenntnisse habe ich laufend dem für die Kontrolle der Bundesdruckerei zuständigen Bundesbeauftragten für den Datenschutz mit der Bitte mitgeteilt, um Abhilfe besorgt zu sein.

Ich werde die weitere Entwicklung beobachten.

7.6. Personenstandswesen

Versand von Standesamtsmitteilungen auf offener Postkarte

Ein völlig Unbeteiligter hat mich davon benachrichtigt, daß er in seinem Briefkasten eine Standesamtsmitteilung auf offener Postkarte über eine ihm fremde Person vorgefunden habe.

Dem von mir beanstandeten Standesamt habe ich mitgeteilt, daß der Versand von standesamtlichen Mitteilungen auf Postkarte im Hinblick auf § 103 der Dienstanweisung für die

Standesbeamten und deren Aufsichtsbehörden unzulässig ist.

Ganz allgemein sollte die Verwaltung beachten, daß (sensible) Sachverhalte, die geeignet sind, die schutzwürdigen Belange des Betroffenen zu beeinträchtigen, generell nicht mit offener Postkarte mitgeteilt werden.

7.7. Nutzung kommunaler Unterlagen zur Erstellung einer Kartei über Bevölkerungsgruppen

Immer wieder wird die Frage an mich herangetragen, unter welchen datenschutzrechtlichen Gesichtspunkten kommunale Unterlagen (z.B. alte Meldekarteien, Personenstandsbücher) für die Erstellung von besonderen Karteien (z.B. über Juden während der Zeit des Nationalsozialismus) genutzt werden dürfen. Solche Karteien sollen das Erteilen von Auskünften oder zeitgeschichtliche Forschung erleichtern. Obgleich ich nicht verkenne, daß eine solche Kartei im Einzelfall der Arbeitserleichterung dienen mag, dürfen die mit solchen Karteien verbundenen Risiken nicht übersehen werden.

Ganz abgesehen von den melde-, personenstands- und archivrechtlichen Schranken, die das Anlegen solcher Karteien ohne schriftliche Einwilligung noch lebender Betroffener oder Hinterbliebener zumindest nicht ohne weiteres zulassen, rate ich im Hinblick auf die nicht völlig auszuschließende Gefährdung schutzwürdiger Belange der Betroffenen und auf die politische Brisanz dringend von der Einrichtung solcher Dateien ohne Zustimmung der Betroffenen ab (siehe auch 16.2).

7.8. Datenübermittlungen

7.8.1. Weitergabe der Anschriften von Vorsitzenden und Jugendleitern eingetragener Vereine

Veranlaßt durch Anfragen einiger Landratsämter und eine parlamentarische Anfrage an die Staatsregierung war zu prüfen, ob bayerische Behörden die Privatanschriften von Vorsitzenden und Jugendleitern eingetragener Vereine an Veranstalter von Seminaren und anderer Fortbildungsveranstaltungen übermitteln dürfen.

Zum Grundsätzlichen ist hier zu sagen, daß nach dem Datenschutzrecht Auskünfte an private Dritte nur zulässig sind, wenn schutzwürdige Belange der Betroffenen nicht beeinträchtigt werden. Weitere Voraussetzung ist für Auskünfte über mehrere vom Empfänger nicht namentlich bezeichnete Personen (Gruppenauskunft) im Regelfall, daß sie im öffentlichen Interesse liegen.

Dem konkreten Fall lag die Anfrage einer Stiftung zugrunde, die Jugendleiter, Betreuer und Jugendliche in Sportvereinen zu Fortbildungsveranstaltungen einladen und die Adressen ausschließlich zu diesem Zweck verwenden wollte.

In Übereinstimmung mit dem Staatsministerium des Innern habe ich die Auffassung vertreten, daß bei eingetragenen Sportvereinen der Name des Vereins, der Name des Vorsitzenden und die Anschrift des Vereins übermittelt werden dürfen. Da es sich um fachspezifische Fortbildungsveranstaltungen handelte, war auch ein öffentliches Interesse zu bejahen. Schutzwürdige Belange der Vereinsvorsitzenden waren nicht beeinträchtigt, da diese Personen den Verein auch sonst nach außen vertreten und ihre Namen auch in dem für jedermann einsehbaren Vereinsregister eingetragen sind. Die Mitteilung einer Vereinsanschrift ist auch dann zulässig, wenn sie mit der Privatanschrift des Vorsitzenden übereinstimmt.

Dagegen erachte ich die Übermittlung der Privatadresse des Vorsitzenden, soweit sie von der Vereinsanschrift abweicht, und der Privatanschriften der Jugendleiter nicht für zulässig, da sich hier eine Beeinträchtigung schutzwürdiger Belange nicht ausschließen läßt. Von dieser Rechtsauffassung wurden sowohl die anfragenden Landratsämter als auch die Regierungen als Aufsichtsbehörden der Landratsämter unterrichtet.

Anders als in dem oben geschilderten Fall fehlt es jedoch am öffentlichen Interesse, wenn Unternehmen, z.B. Versicherungen, Vereinsdaten für Werbezwecke anfordern. Das Interesse des einzelnen Unternehmens an Werbung ist zwar ein „berechtigtes Interesse", gehört aber nicht zu den „öffentlichen" Interessen. Die Weitergabe von Namen oder Anschriften von Vereinsvorsitzenden oder anderen Vereinsmitgliedern im Rahmen der Gruppenauskunft ist hier datenschutzrechtlich unzulässig.

7.8.2. Veröffentlichung von Gewerbetreibendendaten im Stadtadreßbuch

Durch die Eingabe eines aufmerksamen Bürgers habe ich erfahren, daß eine Stadtverwaltung in ihrem Amtsblatt auf die beabsichtigte Übermittlung von Einwohner- und Gewerbetreibendendaten an einen Adreßbuchverlag öffentlich hingewiesen hat, wobei den Betroffenen, die nicht im Adreßbuch erscheinen wollen, die Möglichkeit zur Einlegung eines Widerspruchs eingeräumt wurde.

Während die Meldebehörden nach Art. 35 Abs. 3 MeldeG Namen, akad. Grad und Wohnanschrift aller über 18-jährigen Bürger, die nicht widersprochen haben, zum Zwecke der Veröffentlichung im Adreßbuch an einen Adreßbuchverlag übermitteln dürfen, kennt das Gewerberecht eine vergleichbare grundsätzliche Ermächtigung zur Übermittlung von Gewerbetreibendendaten an Adreßbuchverlage derzeit nicht. Datenübermittlungen aus der Gewerbekartei in den privaten Bereich sind deshalb an den allgemeinen Datenschutzvorschriften (hier Art. 18 BayDSG), insbesondere aber an Nr. 6.2.2 der Allgemeinen Verwaltungsvorschrift für die Behandlung von Anzeigen nach den §§ 14 und 55 c Gewerbeordnung (GewAnzVwV) vom 2.1.1980 (WVMBl. S.1) zu messen. Danach ist die Weitergabe von Gewerbetreibendendaten an Adreßbuchverlage nur mit deren (vorheriger) schriftlicher Einwilligung zulässig (vgl. auch Art. 4 Abs. 1 Nr. 2 und Abs. 2 BayDSG).

Seit 2.1.1980 (Inkrafttreten der GewAnzVwV) hatten die Gewerbetreibenden die Möglichkeit, eine entsprechende Einwilligungserklärung bei der Gewerbeanmeldung abzugeben. Alle die Gewerbetreibenden, die bereits vor dem 2.1.1980 ihr Gewerbe angemeldet hatten, konnten diese Entscheidung nicht treffen. Das aber hat zur Folge, daß die Übermittlung jener „Alt"-Gewerbetreibendendaten an den Adreßbuchverlag ohne eine von der Stadt vorher einzuholende schriftliche Einwilligung ausscheiden muß.

Ich habe der Stadt deshalb anheimgestellt, ortsüblich auf diese rechtliche Situation hinzuweisen und die „Alt"-Gewerbetreibenden auf das Erfordernis der schriftlichen Einwilligung zur Datenübermittlung an den Adreßbuchverlag aufmerksam zu machen.

Die Stadt ist dieser Anregung durch wiederholte Veröffentlichung im Amtsblatt gefolgt. Interessant war für mich, daß die über das Amtsblatt zur Abgabe der Einwilligungserklärung aufgerufenen „Alt"-Gewerbetreibenden kaum reagierten. Offenbar wird der von den Adreßbuchverlagen stets behaupteten Werbewirksamkeit der Branchenverzeichnisse von den Gewerbetreibenden selbst keine Bedeutung beigemessen.

7.8.3. Bekanntgabe von Wahlvorschlägen an einen Verlag zu Werbezwecken

Ein nordrhein-westfälischer Verlag hat die bayerischen Gemeinden ohne Nennung von Gründen gebeten, die Wahlvorschlagsdaten der letzten Kommunalwahl zu übersenden.

Erfreulicherweise haben sich zahlreiche Gemeinden an meine Geschäftsstelle gewandt, um sich nach der Zulässigkeit einer solchen Datenübermittlung zu erkundigen.

Da sich bei meinen Ermittlungen herausstellte, daß der Verlag die Adressen der kommunalen Mandatsbewerber zu kommerziellen Zwecken (Werbung für eine Loseblattsammlung über Reden vor der Öffentlichkeit zu privaten Anlässen und in der Politik, Rhetorik und Körpersprache usw.) verwenden wollte, habe ich das Staatsministerium des Innern gebeten, die bayerischen Gemeinden von der Unzulässigkeit der Datenübermittlung zu unterrichten.

Dem hat es mit folgendem Hinweis entsprochen: „Nach Art. 22 Abs. 1 Gemeindewahlgesetz i.V.m. § 42 Abs. 1 Gemeindewahlordnung sind die Wahlvorschläge zwar öffentlich bekanntzumachen, doch ist diese Bekanntgabe in örtlichem und zeitlichem Zusammenhang mit der jeweiligen Wahl zu sehen. Eine Herausgabe der Wahlvorschläge an Dritte (etwa zu kommerziellen Zwecken) ohne einen solchen Zusammenhang – erscheint nicht sachgerecht und deshalb nicht zulässig."

7.8.4. Angebliche Weitergabe von Daten von Führerscheinneulingen an Sparkassen

Ein Bankenverband sah in folgendem Vorgang – wohl auch aus Wettbewerbsgründen – eine unzulässige Datenübermittlung an Sparkassen:

Die Landesverkehrswacht Bayern und die örtlichen Verkehrswachten bieten seit einigen Jahren Führerscheinneulingen das Programm „Könner durch Erfahrung" an. Das Programm ist für Personen gedacht, die seit etwa einem Jahr die Fahrerlaubnis Klasse 1 oder 3 besitzen und durch eine freiwillige Nachschulung ihre Fahrfertigkeiten verbessern wollen. Die Teilnehmer des Kurses haben die Chance, Preise (z.B. Motorrad, Auto, Bausparverträge) zu gewinnen; die Preise stiften die Sparkassen und die Bayer. Landesbausparkasse. Die Oberbürgermeister und die Landräte schreiben nun „ihre" Führerscheinneulinge an; beigelegt ist dem Schreiben eine Teilnahmekarte, mit der sich die Führerscheinneulinge beim örtlichen Träger des Programms (Verkehrswacht oder Sparkasse) anmelden können. Die Oberbürgermeister und Landräte erhalten die hierzu notwendigen Daten der Führerscheinneulinge von ihren Fahrerlaubnisbehörden.

Aus meiner Sicht ist der Vorgang datenschutzrechtlich wie folgt zu beurteilen:

Die Fahrerlaubnisbehörden sind Teil der Stadtverwaltung bzw. des Landratsamtes. Der Vollzug des Fahrerlaubnisrechts ist den kreisfreien Städten und Landratsämtern als staatliche Aufgabe zugewiesen. Oberbürgermeister und Landrat sind insoweit oberste Leiter der Fahrerlaubnisbehörden. Somit liegt keine Datenübermittlung im Sinne von Art. 5 Abs. 2 Nr. 2 BayDSG vor. Doch kann dies letztlich dahinstehen, weil die Herausgabe der Daten der Führerscheinneulinge an Oberbürgermeister oder Landrat auch unter Anwendung der Voraussetzungen des Art. 17 Abs. 1 BayDSG datenschutzrechtlich nicht zu rügen ist. Oberbürgermeister und Landrat haben in dieser Eigenschaft als oberste Leiter der Fahrerlaubnisbehörden auch die durch Rechtsnorm zugewiesene Aufgabe, für die Fahrsicherheit der Anfänger zu sorgen.

Entscheidend ist, daß die Fahrerlaubnisbehörden die Daten der jungen Fahrerlaubnisinhaber nicht an die örtliche Verkehrswacht oder die Sparkasse herausgeben, sondern an den Oberbürgermeister oder Landrat. Die von diesen angeschriebenen Führerscheinneulinge können sich dann mit Hilfe des beigelegten Formulars bei der örtlichen Verkehrswacht oder bei der Sparkasse zur Teilnahme am Schulungsprogramm anmelden. Eine Datenübermittlung an Stellen außerhalb des öffentlichen Bereichs (Art. 18 BayDSG) findet insoweit also nicht statt. Die Teilnahme an den Fahrkursen ist freiwillig. Ein Zwang wird auf die Führerscheinneulinge nicht ausgeübt.

7.9. Vollzugsdefizit bei der Freigabe automatisierter Verfahren

Nach Art. 26 Abs. 2 BayDSG sind der erstmalige Einsatz sowie wesentliche Änderungen von automatisierten Verfahren, mit denen personenbezogene Daten verarbeitet werden, hinsichtlich der Datenarten (Speicherungsdatensatz) und der regelmäßigen Datenübermittlungen (Übermittlungsdatensätze) durch die oberste Dienstbehörde oder die von ihr ermächtigte Stelle datenschutzrechtlich schriftlich freizugeben. Hiervon ist der Landesbeauftragte für den Datenschutz zu unterrichten (Art. 26 Abs. 4 BayDSG).

Auf diese Verpflichtung habe ich wiederholt in früheren Tätigkeitsberichten, aber auch in konkreten Einzelfällen hingewiesen. Trotzdem stelle ich immer wieder fest, daß insbesondere die kleineren Verwaltungseinheiten ADV-Verfahren einsetzen, ohne daß eine datenschutzrechtliche Verfahrensfreigabe erfolgt ist. Die Gemeinden und Verwaltungsgemeinschaften, die meist über kein oder nur wenig geschultes EDV-Personal verfügen, übernehmen die Verfahren von Herstellern im Vertrauen darauf, daß die Grundsätze der Rechtmäßigkeit und Erforderlichkeit beachtet und alle datenschutzrechtlichen Erfordernisse durch die Herstellerfirma erfüllt wurden. Das aber hat regelmäßig zur Folge, daß die datenschutzrechtliche Verfahrensfreigabe nach Art. 26 BayDSG – meist aus Unkenntnis dieser Bestimmung – nicht vorgenommen wird und eine Unterrichtung meiner Geschäftsstelle unterbleibt.

Das Staatsministerium des Innern hat sich mit verschiedenen Herstellern in Verbindung gesetzt, um Wege zu finden, wie die Gemeinden und Verwaltungsgemeinschaften am zweckmäßigsten ihren Verpflichtungen nach Art. 26 BayDSG nachkommen können.

Zwischenzeitlich konnte aufgrund der vom Staatsministerium des Innern zur Verfügung gestellten Hinweise zum

besseren Vollzug des Art. 26 BayDSG und durch kooperatives Verhalten verschiedener Herstellerfirmen erreicht werden, daß deren Kunden über die Verpflichtung zur datenschutzrechtlichen Freigabe unterrichtet wurden. In den letzten Wochen war bereits ein starker Zustrom von datenschutzrechtlichen Verfahrensfreigaben in meiner Geschäftsstelle zu verzeichnen. Ich gehe davon aus, daß sich diese Situation noch weiter verbessern wird, sobald die nachgeordneten Behörden unmittelbar durch das Staatsministerium des Innern – wie vorgesehen – generell über die Erfordernisse des Art. 26 Abs. 2 und 4 BayDSG unterrichtet werden.

7.10. Änderung des Telex-Anschlusses beim Landesamt für Statistik und Datenverarbeitung

Anlaß zu datenschutzrechtlichen Ermittlungen gab die Pressemitteilung einer Partei im Landtag. Sie befürchtete, daß geschützte personenbezogene Daten aus der Volkszählung, die für das Landesamt für Statistik und Datenverarbeitung bestimmt waren, in falsche Hände gelangt seien. Ein früherer Telex-Anschluß des Landesamtes sei nun für einen Privaten vergeben. Dies sei in Behördenverzeichnissen der Regierung von Oberbayern nicht berichtigt.

Diese Befürchtung der Falschübermittlung von Daten der Volkszählung haben meine Ermittlungen nicht bestätigt.

Allerdings habe ich festgestellt, daß der vom Landesamt für Statistik und Datenverarbeitung aufgegebene und inzwischen an einen privaten Dritten vergebene Telex-Anschluß in den genannten Behördenverzeichnissen trotz einer entsprechenden Benachrichtigung durch das Landesamt nicht gelöscht worden war. Es lagen mir jedoch keine Hinweise vor, daß personenbezogene Daten an den neuen Inhaber der Telex-Nummer übermittelt wurden.

Ich habe das Staatsministerium des Innern gebeten, die nachgeordneten Behörden auf die Notwendigkeit einer umgehenden Überarbeitung der Adressen- und Telefonverzeichnisse hinzuweisen. Von einer Beanstandung der Regierung von Oberbayern habe ich nur deshalb abgesehen, weil es sich bei dem Telefonverzeichnis der Regierung um keine Datei handelt.

Gleichzeitig wandte ich mich an den Bundesbeauftragten für den Datenschutz mit der Bitte, das Problem der Vergabe von gekündigten Telex-Anschlüssen von Behörden, die sensible Daten verarbeiten, mit der Deutschen Bundespost zu erörtern. Der Bundesminister für das Post- und Fernmeldewesen erläuterte hierzu, daß sich Fehlübermittlungen allein schon durch die richtige Bedienung des Telex-Gerätes vom sendenden Teilnehmer verhindern ließen. Eine Telex-Kennung bestehe aus einem Zifferteil (Telex-Rufnummer), der von der Deutschen Bundespost vergeben werde, und einem Buchstabenteil, der im Rahmen der technischen Vorschriften vom Kunden selbst gewählt werden kann. Bei Anwahl eines Telex-Anschlusses werde grundsätzlich nur der Zifferteil eingegeben. Nach Beendigung der Wahl werde die Kennung (Ziffern- und Buchstabenteil) des erreichten Endgerätes beim sendenden Endgerät dargestellt, so daß hier eine zusätzliche Kontrolle gegeben ist, ob der richtige Empfänger erreicht wurde. Jeder Telex-Teilnehmer sei gehalten, diesen Kennungsgebervergleich durchzuführen oder von seinem Endgerät automatisch durchführen zu lassen. Fehlübermittlungen ließen sich auf diese Weise verhindern.

Darüber hinaus erklärte sich der Bundesminister jedoch auch bereit, die bislang bestehende Sperrfrist von 6 Monaten für die Neuvergabe von Telex-Rufnummern zunächst auf 1 Jahr zu erhöhen.

Damit ist dem Anliegen des Datenschutzes ausreichend Rechnung getragen, wenn bei der sendenden Behörde von der Möglichkeit des Kennungsgebervergleiches Gebrauch gemacht wird.

7.11. Verhalten einer oberbayerischen Kreditauskunftei gegenüber den Bürgern und den Behörden

Eine Kreditauskunftei hatte sich an eine Gemeinde mit dem Ersuchen gewandt, ihr eine Auskunft über melderechtliche Daten zu erteilen. Die Auskunftei hatte dabei mehr Daten erbeten, als nach den melderechtlichen Vorschriften zulässigerweise übermittelt werden durften. Die Gemeinde ist entgegen Art. 34 des Bayer. Meldegesetzes diesem Ersuchen nachgekommen. Ich habe die Meldebehörde beanstandet. Zudem habe ich das zuständige Landratsamt gebeten, die kreisangehörigen Gemeinden an die strikte Einhaltung der für Auskünfte aus dem Melderegister und aus der Gewerbekartei maßgeblichen Bestimmungen zu erinnern. Die Auskunftei schreckte auch nicht davor zurück, durch Druck auf die Betroffenen an möglichst viele und genaue Informationen über Bürger zu gelangen. Beispielsweise erhielten die Bürger ein Anschreiben der Auskunftei, das überwiegend geschätzte Daten – z.B. über Jahresumsatz des Betroffenen – enthielt, mit der Aufforderung, die Daten zu berichtigen. Sollte dieser Aufforderung nicht Folge geleistet werden, muß der Bürger wohl damit rechnen, daß die geschätzten und daher weitgehend falschen Daten als richtig unterstellt und an Auskunftssuchende weitergegeben werden. Daß dadurch schutzwürdige Belange des Betroffenen beeinträchtigt werden können, liegt auf der Hand.

Das Staatsministerium des Innern hat als oberste Aufsichtsbehörde für den Datenschutz im nichtöffentlichen Bereich diesen Vorgang zum Anlaß genommen, die Regierungen als örtliche Aufsichtsbehörden darauf hinzuweisen, daß sie bei ihren Prüfungen der Auskunfteien diesem Problem besonderes Augenmerk schenken. Die Regierungen sollen bei ihren Prüfungen den Auskunfteien ein Formblatt für Anfragen bei den Meldebehörden zur Verfügung stellen, das sich an die Vorgaben von Nr. 34.3 VollzBekMeldeG hält.

8. Einwohnermeldewesen

8.1. Rechtliche Entwicklung

Das seit 1.4.1983 geltende bayerische Melderecht hat sich grundsätzlich bewährt. In Einzelfragen sind jedoch Probleme und Zweifelsfragen aufgetreten, die der Klärung durch den Gesetzgeber bedürfen. Das Staatsministerium des Innern beabsichtigt daher, aufgrund der bisherigen Erfahrungen sowie der Wünsche und Anregungen verschiedener vom Melderecht betroffener Behörden und Institutionen, Verbesserungen durch Änderung der Meldegesetze anzustreben.

Auch ich habe dem Innenministerium eine Reihe von Änderungs- und Ergänzungsvorschlägen übermittelt mit dem Ziel, das Melderecht noch praxisgerechter und

bürgerfreundlicher zu gestalten, ohne dabei allerdings den angemessenen Datenschutz zu vernachlässigen.

Vor allem in folgenden Punkten sollte der Gesetzgeber für Klarheit sorgen und Verbesserungen des Melderechts, nämlich des Melderechtsrahmen- und des Bayer. Meldegesetzes vorsehen: – Erleichterung genealogischer Forschung während der 50-jährigen Aufbewahrungsfrist von Meldedaten Verstorbener und Weggezogener (Art. 11 Abs. 3 MeldeG läßt lediglich die Bekanntgabe der Anschrift und des Sterbetages während dieser Zeit zu); – Erleichterung bei der Ermittlung der Erben und Hinterbliebenen durch zweckgebundene Wiedereinführung des „Familienverbundes" (nach Volljährigkeit der Kinder); – Regelung der Datenübermittlungen und Auskünfte über Melderegisterdaten von Krankenhaus- und Pflegeheiminsassen sowie von pflegebedürftigen oder behinderten Personen in Einrichtungen, die der Rehabilitation oder der Heimerziehung dienen (Art. 28 Abs. 1 MeldeG), sowie über Daten von Strafgefangenen (Art. 25 Abs. 3 MeldeG) (Unwirksamkeit des Art. 25 Abs. 4 MeldeG in der Praxis); – Maßnahmen zur Verringerung des Verwechslungsrisikos bei Melderegisterauskünften gem. § 21 MRRG, Art. 34 MeldeG; – Wahrung des Adoptionsgeheimnisses im Melderegister durch verbesserte Mitteilungspraxis zwischen Standesamt und Meldebehörde sowie durch Löschung der Auskunftssperre nach vollzogener Adoption.

8.2. Widerspruchsrechte der Bürger nach dem Bayer. Meldegesetz (MeldeG)

Immer wieder wenden sich Bürger an mich, deren Daten zu Wahlwerbezwecken an politische Parteien und Wählergruppen oder zur Bekanntgabe von Alters- und Ehejubiläen an die Presse übermittelt werden oder deren Daten in Adreßbüchern erscheinen.

Art. 35 MeldeG läßt grundsätzlich solche Datenübermittlungen und Veröffentlichungen zu, räumt aber den Bürgern Widerspruchsrechte ein. Da die gesetzliche Regelung besagt, daß der Betroffene lediglich bei seiner Anmeldung auf diese Widerspruchsrechte hinzuweisen ist, ist das Widerspruchsrecht bei den Bürgern, die bereits vor Inkrafttreten des Meldegesetzes am 1.4.1983 in der Gemeinde gemeldet waren, regelmäßig nicht bekannt.

Wie bereits in früheren Tätigkeitsberichten rege ich daher nochmals an, die Bürger von Zeit zu Zeit in ortsüblicher Weise auf die vom Meldegesetz vorgesehenen Widerspruchsrechte hinzuweisen.

8.3. (Gäste-)Meldescheine in Fremdenverkehrs-/Kurorten

Gestaltung der Meldescheine

Obwohl § 2 Abs. 2 der Durchführungsverordnung zum Bayer. Meldegesetz (DVMeldeG) den Gemeinden, in denen Kurbeiträge oder Kurtaxen erhoben werden, seit 1.9.1983 verbindlich vorschreibt, Meldescheine nach den Mustern der Anlagen 5 und 5 a zur DVMeldeG zu verwenden, stelle ich bei Beschwerden und eigenen Überprüfungen immer wieder fest, daß von den Gästen mehr Daten als erlaubt erhoben werden.

Mehrere durch mich ausgesprochene Beanstandungen von (Gäste-) Meldescheinen, die nicht der DVMeldeG entsprachen, haben das Staatsministerium des Innern veranlaßt, in einem Rundschreiben alle bayerischen Fremdenverkehrsgemeinden zur ausschließlichen Verwendung des amtlich vorgeschriebenen Meldescheins anzuhalten.

Nutzung der Meldescheine

Bei meinen Überprüfungen ist mir aufgefallen, daß aus den der Berechnung des Kurbeitrages zugrundeliegenden Meldescheinen (für Beherbergungsstätten) Angaben zur Berechnung des Fremdenverkehrsbeitrags (Übernachtungspauschale) gemäß § 5 Abs. 3 der Mustersatzung des Staatsministeriums des Innern für den Fremdenverkehrsbeitrag entnommen werden. Dies steht jedoch im Widerspruch zu Art. 29 Abs. 1 MeldeG, wonach die Gemeinden Gästedaten nur zum Zwecke der Festsetzung des Kurbeitrags (der Kurtaxe) sowie für Zwecke der Beherbergungs- und Fremdenverkehrsstatistiken, nicht aber für den Fremdenverkehrsbeitrag auswerten und verarbeiten dürfen (Nutzungsbeschränkung).

Das ist für die Gemeinden unbefriedigend, weil sie zur Erhebung des Fremdenverkehrsbeitrags eine gesonderte Erhebung bei den Beherbergungsbetrieben durchführen müßten. Eine vernünftige unbürokratische Lösung ist nach meiner Auffassung nur durch eine Änderung von Art. 29 MeldeG möglich. Ich habe das Staatsministerium des Innern um Überprüfung gebeten und eine Lösung gefordert.

8.4. Übermittlung von Melderegisterdaten an die öffentlich-rechtlichen Religionsgesellschaften

Die Meldebehörden dürfen nach Art. 32 MeldeG bestimmte Daten von Religionszugehörigen und in beschränktem Umfang auch von deren Ehegatten, Eltern und Kindern, die nicht derselben oder keiner öffentlich-rechtlichen Religionsgesellschaft angehören, zur rechtmäßigen Aufgabenerfüllung an die Kirchen übermitteln.

Verschiedenen Beschwerden und eigenen Feststellungen zufolge halten sich einige Meldebehörden jedoch immer noch nicht an den durch Art. 32 MeldeG vorgeschriebenen Datenkatalog und übermitteln mehr Daten als erlaubt, oder Daten solcher Personen, die nach Art. 32 MeldeG überhaupt nicht übermittelt werden dürfen (z.B. Daten geschiedener Personen, die keiner Religionsgesellschaft angehören).

Es erreichen mich auch Anfragen zur Verarbeitung personenbezogener Daten durch die öffentlich-rechtlichen Religionsgesellschaften. Da die Kirchen gemäß Art. 140 Grundgesetz i.V.m. Art. 137 Abs. 3 Weimarer Reichsverfassung ihre Angelegenheiten selbständig ordnen und verwalten, unterliegt die kirchliche Datenverarbeitung nicht meiner Kontrolle. Ich verweise daher die Petenten wegen fehlender Zuständigkeit an die kirchlichen Datenschutzbeauftragten.

8.5. Telefonische Melderegisterauskünfte an Inkassobüros, Auskunfteien u.ä.

Kreditauskunfteien, Inkassobüros und ähnliche Einrichtungen sind vielfach auf „erweiterte" Melderegisterauskünfte unter den in Art. 34 Abs. 2 MeldeG genannten Voraussetzungen angewiesen. Um den Auskunftsvorgang zu beschleunigen, streben sie Vereinbarungen mit den Gemeinden an, die telefonische Auskunftserteilungen ermöglichen sollen (z.B. Kennwortvereinbarung).

Zur telefonischen Auskunftserteilung – auch mit Kennwortvereinbarung – vertrete ich folgende Auffassung:

Art. 34 Abs. 2 MeldeG sieht eine besondere Form der Auskunftserteilung aus dem Melderegister nicht vor. Damit sind auch fernmündliche Auskünfte nicht von vorneherein ausgeschlossen, wenn die Identität des Auskunftsersuchenden eindeutig feststeht, was durch die Vereinbarung eines Kennwortes grundsätzlich erreicht werden kann. Allerdings besteht bei fernmündlichen „erweiterten" Auskünften an Auskunfteien, Inkassobüros, Rechtsanwälte usw. wohl eher die Gefahr, daß die in Nr. 34.3 der Vollzugsbekanntmachung genannten Vollzugshinweise, insbesondere was den Datenumfang betrifft, nicht ausreichend beachtet werden. Außerdem erfordern fernmündlich erteilte „erweiterte" Auskünfte Aufzeichnungen durch den Sachbearbeiter, um den Betroffenen gemäß Art. 34 Abs. 2 Satz 2 MeldeG benachrichtigen zu können. Auch sind Hörfehler nicht auszuschließen, die zu Personenverwechslungen oder unrichtigen Datenübermittlungen führen können. Aus diesen Gründen gebe ich für den Regelfall einer schriftlichen Auskunftserteilung unbedingt den Vorzug. Fernmündliche Auskünfte sollten auf den eiligen Einzelfall beschränkt bleiben. Im übrigen geht das Staatsministerium des Innern für die Erteilung von erweiterten Auskünften an Auskunfteien von einem schriftlich, mit Formblättern abzuwickelnden Verfahren aus (IMS an die Regierungen vom 17.10.1988, I G 3 1085.3/4).

8.6. Bestimmung der Hauptwohnung bei mehreren Wohnungen (Bereinigung von Altfällen im Melderegister)

Nach Art. 40 MeldeG hätten die Meldebehörden anhand der Unterlagen der ausgefallenen Volkszählung 1983 beim Vorhandensein mehrerer Wohnungen, eine Wohnung als Hauptwohnung bestimmen müssen.

Diese Bestimmung ist allerdings durch das Urteil des Bundesverfassungsgerichts zum Volkszählungsgesetz vom 15.12.1983 (BVerfGE 65/1 ff) gegenstandslos geworden. Einen Melderegisterabgleich mit Daten aus der Volkszählung hat das Bundesverfassungsgericht mit Gesetzeskraft untersagt.

Um jedoch die Fälle, in denen ein Einwohner bei Inkrafttreten des Bayer. Meldegesetzes am 1.4.1983 mit mehreren Wohnungen gemeldet war, auf den objektivierten Hauptwohnungsbegriff umstellen zu können, hat das Staatsministerium des Innern als Ersatz für den Melderegisterabgleich die Meldebehörden angewiesen, den betroffenen Personenkreis in einer besonderen Befragungsaktion über Haupt- und Nebenwohnung(en) bis spätestens 30.4.1988 zu befragen und die Melderegister ggf. zu bereinigen.

Diese Melderegisterbereinigung war erforderlich, weil die Bürger mit mehr als einer Wohnung nach früherem Melderecht selbst bestimmen konnten, welche der Wohnung Haupt- und welche Nebenwohnung ist. Nach neuem Melderecht wird dagegen zwischen Haupt- und Nebenwohnung nach objektiven Kriterien unterschieden mit der Folge, daß der Bürger keine Wahlmöglichkeit mehr hat. Die Feststellung der Hauptwohnung ist für die Gemeinde aber notwendig, weil viele Behördenzuständigkeiten (z.B. Ausweiserstellung, Lohnsteuerkarten) damit verbunden sind, aber auch Rechte und Pflichten des Bürgers (z.B. Wahlrecht) daran anknüpfen.

In zahlreichen Eingaben haben betroffene Bürger wegen des zeitlichen Zusammenhangs mit der Volkszählung 1987 befürchtet, daß Volkszählungsdaten Auslöser oder Grundlage für die Befragungsaktion sein könnten.

Nach meinen Feststellungen haben aber die Gemeinden nach der Weisung des Staatsministeriums – völlig unabhängig von der Volkszählung – gehandelt, so daß die Befürchtungen der Petenten unbegründet waren. Gerade weil die gemeindlichen Einwohnermeldeämter als Folge des Volkszählungsurteils keine Daten aus der Volkszählung erhalten haben, ist die Umfrageaktion notwendig geworden.

8.7. Online-Zugriff auf Melderegisterdaten

Im 9. Tätigkeitsbericht (Nr. 8.8) habe ich gefordert, daß die Einwohnermeldeämter die Bildschirmmasken-Inhalte auf das für die Erfüllung der jeweiligen Verwaltungsaufgabe tatsächlich erforderliche Maß beschränken.

Zwar konnte ich im Berichtszeitraum feststellen, daß dieses datenschutzrechtliche Anliegen noch nicht vollständig verwirklicht ist. Immerhin sind jedoch inzwischen verschiedene Anbieter dabei, für die Gemeinden variable Bildschirmmasken zu konzipieren, die eine Begrenzung des Inhalts auf das jeweils erforderliche Maß ermöglichen. Diese begrüßenswerte Entwicklung werde ich weiter beobachten und unterstützen.

Im Zusammenhang mit der Überprüfung und Überarbeitung der Bildschirmmasken-Inhalte sollte allerdings schon jetzt von Gemeinden und Anbietern überlegt werden, wie gewährleistet wird, daß die Zulässigkeit des Online-Abrufs im Einzelfall kontrolliert werden kann, zumal bereits nach anderen Spezialvorschriften (z.B. §§ 30a ff StVG, § 22 Abs. 3 PaßG, § 2 b Abs. 3 PAuswG) eine Protokollierungspflicht besteht und in § 9 Abs. 4 des Entwurfs zur Änderung des Bundesdatenschutzgesetzes (Stand 15.9.1988) Stichprobenkontrollen vorgesehen sind.

Über eine Protokollierung kann ein denkbarer unzulässiger Meldedatenabruf leichter entdeckt und verfolgt werden.

8.8. Kennzeichnung von Einwohnern als „Wohngeldempfänger" oder als „Sozialhilfeempfänger"

Bereits im 9. Tätigkeitsbericht (Nr. 8.10) habe ich klargestellt, daß Art. 3 MeldeG die Speicherung des Kennzeichens „Wohngeldempfänger" im Melderegister nicht zuläßt.

Gleichwohl habe ich festgestellt, daß genau dieses Merkmal im Melderegister einer Großstadt gespeichert ist, um der Wohngeldstelle die Überwachung der Voraussetzungen für den Bezug von Wohngeld (insbesondere bei Wegzügen und Sterbefällen) zu erleichtern. Wegen der eindeutigen Gesetzesregelung habe ich die Löschung dieses melderechtlich unzulässigen Kennzeichens gefordert. Gleiches muß für „Sozialhilfeempfänger" gelten.

9. Steuerverwaltung

9.1. Kontrollbefugnis der Datenschutzbeauftragten

Zwischen den Finanzverwaltungen und den Datenschutzbeauftragten des Bundes und der Länder nach wie vor umstritten ist die Datenschutzkontrolle ohne vorherige Einwilligung des Steuerpflichtigen. Im Hinblick auf das Steuergeheimnis wird von den Finanzverwaltungen die Auffassung vertreten, die Datenschutzbeauftragten seien

erst nach ausdrücklicher Einwilligung des Steuerpflichtigen befugt, bei Kontrollen Einsicht in die Steuerdateien zu nehmen. Der Entwurf der Datenschutznovelle macht die Kontrolle des Datenschutzbeauftragten davon abhängig, daß der Steuerpflichtige der Kontrolle nicht widersprochen hat. Eine solche Regelung würde letztlich für eine Datenschutzkontrolle der Steuerverwaltung die vorherige Einwilligung des Steuerpflichtigen voraussetzen. Eine allgemeine Datenschutzkontrolle wäre praktisch unmöglich. Eine Einwilligungslösung ist daher im Interesse des Schutzes der Steuerpflichtigen abzulehnen.

Angesichts dieser grundsätzlichen Streitfrage und wegen der bis vor kurzem bestehenden Personalknappheit wurde bisher auch in Bayern von allgemeinen, d. h. nicht durch eine Beschwerde, ausgelösten Datenschutzkontrollen in der Steuerverwaltung abgesehen. Das mag hinnehmbar sein in den Bereichen, in denen die Interessen von Finanzamt und Steuerpflichtigen gleichgerichtet sind.

Grundsätzlich problematisch ist die Einschränkung der Kontrollbefugnis der Datenschutzbeauftragten jedoch in den zahlreichen Fällen konträrer Interessenlage, wenn es etwa darum geht, ob die Datenschutzvorschriften über die Weitergabe von steuererheblichen Daten an die Finanzämter eingehalten worden sind, ob die Finanzämter über rechtlich zulässiges Wissen verfügen oder unzulässig erlangte Daten speichern und nutzen. Eine effektive Datenschutzkontrolle ist hier nur möglich, wenn nicht vor jeder Einsichtnahme in Steuerdateien die Einwilligung des Steuerpflichtigen eingeholt werden muß.

Der Vorhang des Steuergeheimnisses darf nicht vor, sondern erst nach dem Datenschutzbeauftragten heruntergehen.

9.2. Kontrollmitteilungen an die Finanzämter

Leisten Behörden und öffentlich-rechtliche Rundfunkanstalten an Personen noch nicht versteuerte Zahlungen, dann senden sie Kontrollmitteilungen an die Finanzämter. Nach § 93 a der Abgabenordnung (AO) muß zur Regelung des Kontrollmitteilungsverfahrens noch eine Rechtsverordnung erlassen werden. Diese ist auch im Berichtszeitraum nicht ergangen. Solche Kontrollmitteilungen an die Finanzämter erfolgen daher bisher ohne rechtliche Grundlage. Aus rechtsstaatlichen Gründen ist es dringend notwendig, diese Rechtsverordnung alsbald zu erlassen, damit die Rechtsunsicherheit, wie sie sich bei der Übermittlung von Steuerdaten eines längst verstorbenen Volksschauspielers von einer außerbayerischen Rundfunkanstalt an ein bayerisches Finanzamt gezeigt hat, ausgeräumt wird.

Nach § 93 a Abs. 1 Satz 2 AO ist in den Kontrollmitteilungen nicht die Höhe der unversteuerten Bezüge, sondern nur der Steuerfall anzugeben. Die Höhe der Bezüge hat der Steuerpflichtige in der Steuererklärung selbst zu erklären. Wird trotzdem dem Finanzamt in der Kontrollmitteilung die Höhe der Bezüge mitgeteilt, so sind Speicherung und Nutzung dieses Wertes für die Steuerveranlagung nicht zulässig. Eine unzulässige Speicherung ist zu löschen.

Das Staatsministerium der Finanzen vertritt hingegen die Ansicht, aus einer Mißachtung der Einschränkung des § 93 a AO könne kein Verwertungsverbot abgeleitet werden. Dem Steuerpflichtigen werde bei einer Abweichung von seiner Erklärung rechtliches Gehör gewährt. Im übrigen bestehe für die Übergangszeit bis zum Inkrafttreten der Rechtsverordnung nach § 93 a AO für die Behörden keine Verpflichtung, den Finanzämtern Kontrollmitteilungen zu übersenden.

Das Problem der Speicherung und der weiteren Nutzung von Daten, die den Finanzämtern im Wege der Kontrollmitteilungen ohne Rechtsgrundlage übermittelt werden, ist auch im Hinblick auf den Grundsatz der Gleichmäßigkeit der Besteuerung, dringend regelungsbedürftig.

9.3. Online-Abruf von Steuerdaten durch oberste Finanzbehörden

Mit der Steuerdatenabrufverordnung (StDAV) soll der Direktabruf der von den Finanzbehörden automatisiert gespeicherten Steuerdaten geregelt werden. Dabei sollen Art und Umfang der direkt, d. h. ohne Einschalten des Datenbesitzers, abrufbaren Daten, der Kreis der zum Abruf Berechtigten sowie die erforderlichen Maßnahmen gegen einen unbefugten Abruf festgelegt werden.

Nach dem vorliegenden Entwurf der StDAV sollen neben anderen auch die obersten Finanzbehörden und die Oberfinanzdirektionen in ihren Zuständigkeitsbereichen für den Datenabruf zugriffsberechtigt werden. Dagegen haben die Datenschutzbeauftragten des Bundes und der Länder Bedenken erhoben. Solche zentralen Datenabrufmöglichkeiten sind zur Erledigung der Aufgaben dieser Finanzbehörden nicht erforderlich: – Bei Erfüllung der Aufsichtspflicht müssen im Regelfall ohnehin die Akten beigezogen werden. – Bei der Bearbeitung steuerlicher Einzelfälle herrscht meist kein Zeitdruck. – Direktabrufmöglichkeiten erhöhen das Risiko, daß die dem Steuergeheimnis unterliegenden Daten Personen bekannt werden, die sie zur rechtmäßigen Aufgabenerfüllung nicht benötigen. Diese Auffassung wird vom Staatsministerium der Finanzen geteilt.

Die Konferenz der Datenschutzbeauftragten hat deshalb im Oktober 1988 in einer Entschließung gefordert, daß die obersten Finanzbehörden und die Oberfinanzdirektionen keine Erlaubnis zum Datendirektabruf erhalten sollten.

9.4. Verwendung von Realsteuerdaten der Gemeinden für „sonstige öffentliche Aufgaben"

Nach wie vor ungeregelt ist, ob und in welchem Umfang die Gemeinden Adreßdaten aus ihren Realsteuerdateien (Grund-/Gewerbesteuerdateien) für andere als Steuerzwekke verwenden dürfen (siehe hierzu auch 9. Tätigkeitsbericht Nr. 7.2 und weitere Beiträge im 7. und 8. Tätigkeitsbericht).

Die Bundes- und Länderfinanzverwaltungen beraten seit längerem über eine Novellierung des § 31 Abgabenordnung (AO). Es soll eine Rechtsgrundlage zur Verwendung oder Offenbarung von Adreßdaten aus Realsteuerdateien geschaffen werden. Nach der vorliegenden Entwurfsformulierung zu § 31 AO sollen Adreßdaten aus den Grundsteuerdateien künftig zur Erfüllung „sonstiger hoheitlicher Aufgaben" in den Gemeinden selbst und bei den sonstigen juristischen Personen des öffentlichen Rechts genutzt oder übermittelt werden dürfen.

Ich habe gegenüber dem Staatsministerium der Finanzen und den Datenschutzbeauftragten der Länder und des Bundes die Auffassung vertreten, daß die Formulierung „hoheitliche Aufgaben" in der Praxis wiederum zu

Schwierigkeiten und datenschutzrechtlichen Beanstandungen führen wird, weil sie den praktischen Bedürfnissen nicht gerecht wird. Abgesehen davon, daß der Begriff „hoheitlich" unterschiedlich definiert wird, ist schwer einzusehen, weshalb die wenig sensiblen Adreßdaten nicht auch für nicht-hoheitliche, gleichwohl aber öffentliche Aufgaben der betreffenden Gemeinde genutzt werden dürfen. Hierunter fällt beispielsweise der Vollzug öffentlicher Aufgaben mit privatrechtlichen Mitteln, etwa beim Straßen- oder Leitungsbau. Ich habe deshalb vorgeschlagen, der Gemeinde, die die Adreßdaten besitzt, die Nutzung auch für „sonstige öffentliche Aufgaben" zu gestatten. Bei der Nutzung durch andere juristische Personen des öffentlichen Rechts sollte es bei der Voraussetzung „hoheitliche Aufgaben" verbleiben, zumal sich diese Behörden die Adreßdaten der Eigentümer beim Grundbuchamt beschaffen können.

Bei meinen Überlegungen bin ich davon ausgegangen, daß die Adreßdaten der Grundstückseigentümer schon heute in vielen Gemeinden in diesem Umfang genutzt werden, ihre Verwendung in diesem Rahmen unbürokratisch und bürgerfreundlich ist und diese Daten nicht als besonders sensibel eingestuft werden können. Ich bin auch nicht der Meinung, daß durch eine solche Nutzungsbefugnis das Steuergeheimnis entwertet würde.

9.5. Mitteilungspflicht der Zuwendungsempfänger über Zahlungen an Dritte

Personen und Einrichtungen, die vom Staat Zuwendungen erhielten (Zuwendungsempfänger), mußten bisher aufgrund von Verwaltungsvorschriften zur Bayer. Haushaltsordnung Zahlungen an Dritte, mit denen sie Dienst- oder Werkverträge abgeschlossen hatten (z. B. Gutachter, Vortragende), dem Finanzamt mitteilen. Durch diese Mitteilung sollte das Finanzamt die Erfüllung der Steuerpflicht wirksamer kontrollieren können.

Die Datenschutzbeauftragten des Bundes und der Länder hatten es als rechtlich problematisch angesehen, daß Private gegenüber dem Finanzamt Angaben über an dritte Personen geleistete Zahlungen lediglich aufgrund einer Verwaltungsvorschrift zu machen hatten. Die Preisgabe von Daten einer dritten Person könne insbesondere im Hinblick auf das informationelle Selbstbestimmungsrecht nicht allein auf die Einwilligung des Zuwendungsempfängers gestützt werden.

Nunmehr hat der Bundesminister der Finanzen entschieden, daß für Zuwendungsempfänger ab sofort keine Mitteilungspflicht mehr bestehe. Das Staatsministerium der Finanzen hat diese Entscheidung für Zuwendungsempfänger aus dem Staatshaushalt übernommen und beabsichtigt, die Verwaltungsvorschriften entsprechend zu ändern.

9.6. Übermittlung von Besteuerungsgrundlagen an die Kirchensteuerämter

Mehrere Bürger haben in Eingaben den Datenaustausch zwischen den Finanz- und den Kirchensteuerämtern als Verstoß gegen das Steuergeheimnis bezeichnet.

Dazu ist festzustellen: Nach § 31 Abs. 1 der Abgabenordnung (AO) sind die Finanzämter berechtigt, Besteuerungsgrundlagen, Steuermeßbeträge und Steuerbeträge zur Festsetzung von Abgaben, die an diese Merkmale anknüpfen, an diejenigen Religionsgemeinschaften, die Körperschaften des öffentlichen Rechts sind, zu übermitteln. Zu ihnen gehören u.a. die römisch-katholische und die evangelisch-lutherische Kirche. Die von den beiden Kirchen nach dem Kirchensteuergesetz erhobene Kircheneinkommen- und Kirchenlohnsteuer sind Abgaben in diesem Sinne. Die Datenübermittlung der Finanzämter an die Kirchensteuerämter und die Festsetzung der kirchlichen Abgaben verstoßen deshalb nicht gegen datenschutzrechtliche Bestimmungen. Selbstverständlich dürfen nur die Steuerdaten der Mitglieder der Religionsgemeinschaft an das jeweilige Kirchensteueramt übermittelt werden. Versehentlich übermittelte Daten sind umgehend zu löschen.

10. Personalwesen

10.1. Beihilfedaten und Rechnungsprüfung

Auf Grund einer Behördenanfrage war zu prüfen, unter welchen Voraussetzungen und in welchem Umfang der Bayer. Oberste Rechnungshof (ORH) und die Prüfungsämter im Rahmen einer Rechnungsprüfung von Beihilfedaten Kenntnis nehmen dürfen.

Einerseits ist § 17 Abs. 4 der Beihilfevorschriften zu beachten. Danach „sind die bei der Bearbeitung der Beihilfen bekanntgewordenen Angelegenheiten geheimzuhalten. Sie dürfen nur für den Zweck verwandt werden, für den sie bekanntgegeben sind, es sei denn es besteht eine gesetzliche Berechtigung oder Verpflichtung zur Offenbarung oder der Beihilfeberechtigte oder der Angehörige ist damit schriftlich einverstanden". Andererseits sind nach Art. 95 der Bayer. Haushaltsordnung dem ORH auf Verlangen alle Unterlagen vorzulegen, die er zur Erfüllung seiner Aufgaben für erforderlich hält. Es besteht also die gesetzliche Verpflichtung zur Offenbarung von Beihilfedaten gegenüber dem ORH.

Der ORH hat bei der Festlegung dessen, was er für erforderlich hält, einen weiten Beurteilungsspielraum. Die Offenbarung personenbezogener Beihilfedaten wäre nur ausgeschlossen, wenn die Angaben unter keinem denkbaren Gesichtspunkt zur Erledigung des Prüfauftrags benötigt würden. In diesem Rahmen kann der Datenschutzbeauftragte die Herausgabe von Beihilfedaten an den ORH überprüfen. Von Bedeutung dabei ist, daß der ORH an bestehende Geheimhaltungsvorschriften gebunden ist. Der Präsident des Bayer. Obersten Rechnungshofes hat dies in einem Beitrag in der Bayer. Staatszeitung folgendermaßen ausgedrückt:

> „Selbstverständlich sind auch die Rechnungshöfe gegenüber Dritten an das Datengeheimnis gebunden. Der Vorhang des Datenschutzes geht nicht vor den Prüfungsbehörden, sondern hinter ihnen herunter".

10.2. Auskünfte über Daten aus Personalakten oder -dateien

Ein Oberbürgermeister legte mir die Frage vor, ob aus der automatisierten Personal-Stammdatei Auskünfte über die Daten städtischer Bediensteter erteilt werden dürfen. Eine Gewerkschaft hatte ihn um Mitteilung der bei der Stadt beschäftigten Mütter mit Vorschulkindern gebeten, um in einer Befragung die Bedürfnisse berufstätiger Frauen bei der Unterbringung ihrer Kinder ermitteln zu können.

Aus datenschutzrechtlicher Sicht ist eine solche Datenübermittlung nicht zulässig. Bei Auskünften über Personaldaten ist zu berücksichtigen, daß Personalakten grundsätzlich zu den Vorgängen gehören, die ihrem Wesen nach geheimzuhalten sind. Zu den danach zu schützenden Daten gehören auch Daten, die in einer Personal-Datei gespeichert sind. Aus dem grundsätzlichen Gebot, Personaldaten geheimzuhalten, folgt jedoch nicht zwangsläufig, daß Personalakten stets und in allen Teilen geheimgehalten werden müssen. Auskünfte sind dann erlaubt, wenn der Betroffene zustimmt oder die Erteilung im wohlverstandenen Interesse des Betroffenen liegt. Sie sind ferner gestattet, soweit nach den Umständen des Einzelfalls dem schutzwürdigen Interesse des Betroffenen an der Geheimhaltung ein überwiegend schutzwürdiges Interesse der Allgemeinheit oder auch eines Dritten an der Auskunftserteilung gegenübersteht. Bei der Auskunftserteilung muß auch berücksichtigt werden, ob als Folge der Auskunft die Daten anderen unbefugten Stellen zugänglich werden.

Im vorliegenden Fall muß bei der gebotenen Interessenabwägung auch berücksichtigt werden, daß künftig – nach dem Grundsatz der Gleichbehandlung – auf Anfrage anderer Interessenten ebenfalls Personaldaten nach bestimmten Kriterien ausgewählt und ohne Zustimmung der Betroffenen weitergegeben würden. Eine solche Praxis würde schutzwürdige Interessen der Betroffenen beeinträchtigen. Die Frauen haben ihre Daten der Personalverwaltung nur für deren Verwaltungszwecke offenbart. Sie müssen grundsätzlich darauf vertrauen können, daß ihre Familienverhältnisse Dritten nicht ohne ihre Kenntnis und Billigung bekanntgegeben werden. Außerdem wäre eine Verwendung der Daten durch die Empfänger über den angegebenen Zweck hinaus kaum kontrollierbar. Da die Mütter zudem auch über einen Aushang am „schwarzen Brett" der Stadtverwaltung auf die Möglichkeit einer Teilnahme an der Befragungsaktion aufmerksam gemacht werden können, kam ich bei der Abwägung zu dem Ergebnis, daß das Interesse an der Auskunft das Interesse der Mütter an der ausschließlich für die Personalverwaltung zweckgebundenen Verwendung ihrer Daten nicht überwiegt.

11. Gewerbe und Handwerk

11.1. Veröffentlichung von Name und Anschrift von Jungmeistern durch die Handwerkskammer

Eine Handwerkskammer hatte nach der Freisprechungsfeier einem Bundestagsabgeordneten auf dessen Bitte die Anschriften freigesprochener Jungmeister, die in seinem Wahlkreis wohnten, zur Übersendung eines Glückwunschschreibens übergeben. In der Feier selbst war ein Verzeichnis der Jungmeister mit Namen und Wohnort öffentlich ausgelegt worden. Vor der Meisterfeier hatten alle Jungmeister ein Einladungsschreiben der Handwerkskammer erhalten, in dem sie über die Absicht unterrichtet wurden, ein Verzeichnis der Jungmeister zu erstellen. Der Hinweis enthielt den Zusatz: „Sofern Sie mit der Aufnahme Ihres Namens und Ihrer Anschrift in dieses Verzeichnis nicht einverstanden sind, bitten wir Sie, uns dies auf beiliegender Antwortpostkarte zu erklären". Zwei Jungmeister, die Widerspruch eingelegt hatten, wurden in das Verzeichnis nicht aufgenommen. Auch der Bundestagsabgeordnete erhielt die Daten dieser Personen nicht.

Ich habe die Übergabe der Anschriften der freigesprochenen Jungmeister an den Bundestagsabgeordneten nicht beanstandet, sondern aus datenschutzrechtlicher Sicht noch für vertretbar gehalten. Der Bundestagsabgeordnete hatte ein berechtigtes Interesse daran, Namen und Anschrift der Jungmeister seines Wahlkreises zu erfahren. Hierzu genügt jedes von der Rechtsordnung als schutzwürdig anerkannte ideelle oder vermögenswerte Interesse. Eine Beeinträchtigung schutzwürdiger Belange der Jungmeister im Sinne von Art. 18 Abs. 2, 2. Alternative BayDSG war im Ergebnis nicht anzunehmen, da dem Abgeordneten keine Anschriften von Jungmeistern mitgeteilt wurden, die der Aufnahme in das Verzeichnis widersprochen hatten, und die Handwerkskammer wohl mit Recht davon ausgehen durfte, die Betroffenen würden damit einverstanden sein, daß ihre Namen und Anschriften im vorliegenden Fall im unmittelbaren zeitlichen Zusammenhang mit der Meisterfeier – an einen Teilnehmer der Meisterfeier weitergegeben würden. In dem Einladungsschreiben war ausdrücklich um Widerspruch gebeten worden, wenn mit der Aufnahme von Namen und Anschrift in das Verzeichnis, das jeder Gast mit nach Hause nehmen konnte, kein Einverständnis bestand.

Allerdings habe ich es für wünschenswert bezeichnet, daß die Handwerkskammer künftig in den Einladungsschreiben nicht nur auf die beabsichtigte Auflage eines Namensverzeichnisses, sondern auch auf die eventuelle Absicht der Weitergabe von Namen und Anschriften an andere Personen und Institutionen ausdrücklich hinweist und die Zustimmung der Betroffenen zu einer solchen Datenübermittlung einholt.

Der Vorsitzende des Datenschutzbeirates und sein Stellvertreter haben in der Weitergabe der Anschriften an den Bundestagsabgeordneten einen Verstoß gegen Datenschutzvorschriften gesehen.

Das Staatsministerium für Wirtschaft und Verkehr hat mitgeteilt, die Mitgliedskammern des Bayerischen Handwerkstages würden künftig bereits im Schreiben, das die Zulassung zur Meisterprüfung bestätigt, ausdrücklich auf die beabsichtigte Veröffentlichung der Daten hinweisen. Auch hierzu habe ich nochmals erklärt, daß in dem Schreiben um eine ausdrückliche Zustimmung nachgesucht werden sollte, wenn Namen und Anschriften in einem zur Auslegung vorgesehenen Namensverzeichnis aufgeführt oder an Dritte z.B. an Organisationen und Firmen, weitergegeben würden.

11.2. Weitergabe von Daten eines Gewerbebetriebes an eine Auskunftei

Der Inhaber eines Handwerksbetriebes vermutete, Behörden hätten Daten über seinen Betrieb an eine Auskunftei weitergegeben. Er teilte folgenden Sachverhalt mit:

Nach der Übergabe des Betriebes vom Vater meldete der Sohn dies beim gemeindlichen Gewerbeamt an. Der Wechsel des Inhabers wurde auch dem Finanzamt, der allgemeinen Ortskrankenkasse und der zuständigen Berufsgenossenschaft mitgeteilt. Wenige Monate später erhielt der neue Inhaber von einer privaten Auskunftei, die auch als Inkassobüro tätig ist, einen „Auskunftsentwurf" mit der Bitte, die Angaben des Entwurfs zu überprüfen. Die im Entwurf vorgesehenen Angaben über den Betrieb sollten

wohl auf Anfrage allen Kunden der Auskunftei mitgeteilt werden. Er enthielt neben den Angaben zur Person des neuen Betriebsinhabers wie Name, Beruf, Geburtsdatum, Privatanschrift, Familienstand auch Name und Geburtsdatum der Ehefrau sowie die Zahl der Kinder, ferner Angaben über das Immobilieneigentum und dessen Wert sowie Angaben zum Gewerbebetrieb, z. B. Aktiva, Passiva, Bankenverbindungen, Jahresumsatz und Zahl der Mitarbeiter. Ferner waren die Betriebsübernahme, der vorherige Betriebsinhaber sowie dessen Immobilieneigentum mit Wertangaben vermerkt.

Der neue Betriebsinhaber verwies darauf, daß weder er noch sein Vorgänger diese Informationen an die Geschäftsbanken oder sonstige Stellen gegeben hätten, und bat zu klären, ob die weitgehend zutreffenden Daten der Auskunftei von öffentlichen Stellen zur Verfügung gestellt worden seien.

Meine Ermittlungen ergaben keinen Anhaltspunkt dafür, daß Daten an die Auskunftei von öffentlichen Stellen, die Kenntnis von der Betriebsübergabe erhalten hatten, gegeben wurden. Die Finanzverwaltung ist wegen des Steuergeheimnisses nach § 30 der Abgabenordnung (AO) zu besonderer Verschwiegenheit verpflichtet. Eine Verletzung dieser Verschwiegenheitspflicht, d. h. des Steuergeheimnisses, würde erhebliche Strafen und disziplinäre Folgen für Bedienstete des Finanzamts nach sich ziehen. Die AOK darf die personenbezogenen Daten des Betriebsinhabers nur unter gesetzlich festgelegten Voraussetzungen (§§ 67 ff Sozialgesetzbuch – SGB X -) bekanntgeben, da diese dem Sozialgeheimnis nach § 35 SGB I unterliegen. Eine Auskunftei ist dort als Datenempfänger nicht vorgesehen. Im vorliegenden Fall sind von der AOK keine Daten an die Auskunftei übermittelt worden.

Das gemeindliche Gewerbeamt kann zwar Auskünfte zu Gewerbebetrieben an Auskunfteien erteilen, ist dabei aber an die zur Gewerbeanzeigenverordnung (GewAnzV) vom 9.10.1979 (BGBl I, S. 1761) ergangene Bekanntmachung vom 2.1.1980, Nr. 4021 – 4/44 – 62194 gebunden. Nach Ziffer 6.2.1 dieser Bekanntmachung dürfen nur der Name, die betriebliche Anschrift und die angemeldete Tätigkeit bekanntgegeben werden. Weitere Daten, insbesondere zu den wirtschaftlichen oder familiären Verhältnissen des Betriebsinhabers, sind zur Weitergabe nicht vorgesehen und wurden der Auskunftei nach Mitteilung des Gewerbeamts auch nicht übermittelt.

Ob aus dem Bereich der Berufsgenossenschaft Daten an die Auskunftei geflossen sind, unterliegt der datenschutzrechtlichen Kontrolle des Bundesbeauftragten für den Datenschutz. Dieser wurde in die Angelegenheit eingeschaltet.

Mit Einverständnis des Betriebsinhabers habe ich bei der Bezirksregierung als datenschutzrechtlicher Aufsichtsbehörde gegenüber der Privatwirtschaft eine Datenschutzkontrolle angeregt. Die Überprüfung ergab, daß schon seit vielen Jahren Daten des betroffenen Gewerbebetriebes im Archiv der Auskunftei geführt und seither laufend aktualisiert worden sind. Die Regierung stellte fest, daß eine derartige Datensammlung für Zwecke der Auskunftserteilung nach dem Bundesdatenschutzgesetz (BDSG) zulässig ist. Auch sonst ergaben die Ermittlungen der Bezirksregierung keinen Verstoß gegen datenschutzrechtliche Vorschriften.

12. Landwirtschaft

12.1. Nutzung der Adressen von Landwirten durch eine Flurbereinigungsdirektion

In einer Eingabe kritisierte ein Landwirt, eine Flurbereinigungsdirektion habe zur Feststellung der Anschriften der an der Flurbereinigung „Beteiligten" zu Unrecht Daten aus der Datei der Empfänger von „Gasöl-Beihilfen" verwendet. In dieser Datei sind nur Landwirte gespeichert. Am Flurbereinigungsverfahren „beteiligt" sind aber auch alle anderen Grundstückseigentümer im Flurbereinigungsgebiet.

Die Überprüfung der Eingabe ergab jedoch keinen Anlaß zu Beanstandung: Die Flurbereinigungsdirektion mußte nämlich zweierlei feststellen: Einmal die „Beteiligten" im Sinne des Flurbereinigungsgesetzes – also sämtliche Grundstückseigentümer im Gebiet, unabhängig davon, ob sie Landwirte sind -, um sie gemäß § 5 Flurbereinigungsgesetz zu unterrichten. Zum zweiten waren nach einer Weisung des Staatsministeriums für Ernährung, Landwirtschaft und Forsten alle praktizierenden Landwirte festzustellen, um speziell deren Einstellung zur Flurbereinigung zu erkunden.

Die Sorge des Landwirts war durch mißverständliche Formulierungen im Informationsschreiben der Flurbereinigungsdirektion ausgelöst worden.

12.2. Bekanntgabe von Grundstücksbelastungen an den Bauernverband

Nach dem Grundstücksverkehrsgesetz bedarf die Veräußerung land- oder forstwirtschaftlicher Grundstücke einer Genehmigung. Bei der Anhörung der land- und forstwirtschaftlichen Berufsvertretung nach § 19 des Grundstücksverkehrsgesetzes erhielt der Bauernverband bisher offenbar Einblick in die vollständigen Kaufverträge, obwohl die Belastung des Grundstücks (etwa durch Hypotheken) bei der Beurteilung des Grundstückswertes nicht zu berücksichtigen ist. Aus der Sicht des Datenschutzes kann aber nicht hingenommen werden, daß diese sensiblen Angaben, die deutliche Rückschlüsse auf die wirtschaftlichen Verhältnisse (etwa beim Verkauf eines Hofes) zulassen, Dritten bekanntgegeben werden, ohne daß dies erforderlich ist.

Ich habe daher eine Überprüfung dieser Praxis angeregt. Das Staatsministerium für Ernährung, Landwirtschaft und Forsten hat daraufhin die Regierungen angewiesen, Kaufverträge vor Übermittlung an die land- und forstwirtschaftliche Berufsvertretung auf entbehrliche Angaben zu überprüfen und von deren Übermittlung abzusehen.

13. Statistik

13.1. Volkszählung 1987

Schwerpunkte des Berichtszeitraums 1988 sind die Weiterbearbeitung der Erhebungsunterlagen beim Landesamt für Statistik und Datenverarbeitung und die anstehende Vernichtung der Volkszählungsunterlagen. Die kontrollierten Behörden haben mir jede erbetene Auskunft erteilt.

Die Überprüfung der Volkszählung 1987 hat auch im Berichtszeitraum 1987/88 die sorgfältige Einhaltung des Datenschutzes bestätigt. Die staatlichen und kommunalen

Stellen waren um eine einwandfreie Durchführung der Volkszählung sehr bemüht. Nur wenige Vorkommnisse mußte ich beanstanden. Bei der Wiedergabe beschränke ich mich auf Vorfälle, die über den Tag hinaus von allgemeinem Interesse sind.

13.1.1. Durchführung der Volkszählung

Diebstahl eines Autos mit Volkszählungsunterlagen

Anfang Februar 1988 wurde in München ein Auto mit 1700 Volkszählungsbögen aus Schwabach (Mittelfranken) gestohlen. Ich habe den Vorfall umgehend überprüft. Es stellte sich folgender Sachverhalt heraus:

Das Auto gehörte einer freien Mitarbeiterin des Landesamtes für Statistik und Datenverarbeitung. Diese Mitarbeiterin hatte ebenso wie ca. 380 andere Mitarbeiter vertraglich vereinbart, zu Hause in den Zählungsbögen Signierarbeiten (Verschlüsseln von Klarsichtangaben in computerlesbare Zeichen) durchzuführen. Haushaltsmantelbögen, welche Namen und Anschriften der Gezählten enthalten, waren unter den gestohlenen Volkszählungsunterlagen nicht enthalten.

Die betroffene Mitarbeiterin ließ die Volkszählungsbögen an jenem Tag im Kofferraum ihres Autos zurück, das in der Tiefgarage ihres Wohnhauses abgestellt war. Dort wurde das Auto mitsamt den Volkszählungsbögen gestohlen; die Bögen tauchten einige Tage später unter mysteriösen Umständen wieder auf.

Ich bewerte den Vorfall wie folgt:

Das Landesamt war bei der Bewältigung der Volkszählungsarbeiten auf freie Mitarbeiter, die zu Hause arbeiten, angewiesen. Dieses Verfahren ist bereits bei der Volkszählung 1970 mit Erfolg praktiziert worden. Es war dem Landesamt nicht möglich, für ca. 380 zusätzliche Mitarbeiter für 7 – 8 Monate geeignete Räume anzumieten.

Das Landesamt hat die freien Mitarbeiter sorgfältig ausgewählt. Es hat ferner die Mitarbeiter schriftlich und mündlich auf die unbedingt einzuhaltenden Sicherungsmaßnahmen hingewiesen. Der betroffenen Mitarbeiterin war bekannt, daß die Volkszählungsunterlagen keinesfalls über Nacht im Auto aufbewahrt werden dürfen. Dennoch hat sie sich an jenem Tag nicht daran gehalten. Gegen die Bequemlichkeit und Fahrlässigkeit Einzelner gibt es trotz aller Vorkehrungen keinen absoluten Schutz. Von dieser Mitarbeiterin hat sich das Landesamt nach dem Vorfall getrennt.

13.1.2. Verarbeitung in der Erhebungsstelle

In einem Zeitungsartikel vom 22.3.1988 mit der Überschrift „Anonymität bei der Volkszählung nicht gewahrt" wurde behauptet, in mindestens zwei Fällen seien durch die Erhebungsstelle der Landeshauptstadt München Angaben aus den Volkszählungsbögen von Münchner Bürgern, die in einer Siedlung zur Miete wohnten, dem Vermieter zur Kenntnis gebracht worden. Einem Architekten im öffentlichen Dienst sei vom Vermieter mitgeteilt worden, diesem sei über die Volkszählung bekannt geworden, daß er seine Wohnung auch teilgewerblich nutze. Er solle deswegen zur Aufklärung bei der Siedlungsverwaltung vorsprechen. Die Angelegenheit habe sich bei der Vorsprache bezüglich der angeblich gewerblichen Nutzung der Wohnung dahingehend erledigt, daß der Architekt diesen Vorwurf habe ausräumen können. Der Sachverhalt stellte sich nach Prüfung ganz anders dar:

Bei der Überprüfung der Vollständigkeit der Volkszählungsunterlagen stellte die Erhebungsstelle fest, daß von dem Architekten kein Arbeitsstättenbogen vorlag, obwohl der Architekt laut Adreßbuch ein Architekturbüro betreibt. Die Erhebungsstelle versuchte, den Architekten unter seiner Privatnummer anzurufen, konnte ihn jedoch nicht erreichen. Die Erhebungsstelle wandte sich deshalb Ende Februar 1988 an die Hausverwaltung der Siedlung. Die Verwaltung teilte der Erhebungsstelle mit, eine Arbeitsstätte des Architekten sei ihr nicht bekannt. Aufgrund dieses Hinweises wurde die Adresse in den Unterlagen der Erhebungsstelle gestrichen. Dies teilte die Erhebungsstelle der Hausverwaltung mit. Weitere Auskünfte wurden von der Erhebungsstelle nicht eingeholt.

Ich beurteile diesen Sachverhalt wie folgt:

Durch die Anfrage der Erhebungsstelle bei der Hausverwaltung wurden keine dem Statistikgeheimnis unterliegenden geschützten Daten aus der Volkszählung an Dritte weitergegeben. Auch war die Anfrage an den Vermieter nach der gewerblich genutzten Wohnung nicht von vorneherein unzulässig. Die Erhebungsstelle hatte im Rahmen ihrer Vollzähligkeitskontrolle nach § 3 Abs. 3 der Verordnung zur Durchführung des Volkszählungsgesetzes festzustellen, ob für eine Arbeitsstätte ein Arbeitsstättenbogen fehlt. Dazu durfte sie auch den Vermieter um Auskunft bitten, solange keine dem Statistikgeheimnis unterliegenden Daten bekanntgegeben werden.

Das war nicht der Fall. Die Frage nach der gewerblichen Nutzung war nämlich nicht durch Angaben des Betroffenen, sondern durch Eintragung im Branchenverzeichnis ausgelöst worden.

Die durch die Nachfrage ausgelösten möglichen Nachteile für den betroffenen Architekten und die Irritationen hätten freilich vermieden werden können. Es wäre sachgerecht, angemessen und zumutbar gewesen, wenn die Erhebungsstelle sich mit der Frage nach der gewerblichen Nutzung der Wohnung zunächst schriftlich an den betroffenen Architekten gewandt hätte. Dadurch hätte sie dessen verständliche Interessen besser berücksichtigt.

13.1.3. Vernichtung der Erhebungsunterlagen

Im Herbst 1988 folgte die Auswertungsphase der Volkszählung, beginnend mit der Bekanntgabe der Einwohnerzahl. Die amtliche Einwohnerzahl wurde in Bayern am 24.11.1988 verkündet.

Dabei taucht gegenüber früheren Volkszählungen erstmals das Problem auf, die von den Auskunftspflichtigen ausgefüllten Erhebungsunterlagen „zum frühestmöglichen Zeitpunkt" zu vernichten (§ 15 Abs. 2 VZG 1987). Das Bundesverfassungsgericht und die Oberverwaltungsgerichte haben in mehreren Entscheidungen gerade auf diese Bestimmung hingewiesen und ihre Einhaltung als wesentlich für die Verfassungsmäßigkeit der Volkszählung herausgestellt. Das Bundesverfassungsgericht hat ferner festgestellt, die statistischen Landesämter seien gehalten, für jede Erhebungsunterlage den jeweils frühestmöglichen Zeitpunkt zu ermitteln und die Vernichtung oder Löschung zu diesem Zeitpunkt vorzunehmen.

In Bayern erfolgt diese Vernichtung wie folgt:

- In den Erhebungsstellen:
  Zählerverzeichnis und Verpflichtungserklärungen wurden nach Auflösung der Erhebungsstelle in der Gemeinde so lange unter Verschluß aufbewahrt, wie sie für die Zählervergütung benötigt wurden, und anschließend vernichtet. Auch die Unterlagen für Mahnverfahren wurden so früh wie möglich vernichtet. Alle sonstigen bei der Erhebungsstelle verbliebenen Erhebungsunterlagen – ohne personenbezogene Angaben – wurden vor Auflösung der Erhebungsstelle vernichtet.
  Das Landesamt ließ sich von den Gemeinden bestätigen, daß alle o.a. Volkszählungsunterlagen vernichtet oder abgeliefert sind. Die entsprechenden Bestätigungen liegen dem Landesamt für Statistik und Datenverarbeitung für die weitaus meisten Gemeinden vor; den wenigen noch ausstehenden Fällen wird das Landesamt noch nachgehen.
  Ich habe stichprobenweise geprüft, ob die Volkszählungsunterlagen bei den Erhebungsstellen vernichtet worden sind. Das war der Fall.
- Im Landesamt für Statistik und Datenverarbeitung wurden die nachfolgend aufgeführten Volkszählungsunterlagen bereits vernichtet:
  - Gebäudebogen
  - ungültige, geknickte oder durchgestrichene ausgefüllte Erhebungsvordrucke
  - Zählerausweise, Verpflichtungserklärungen für Zähler und weitere Unterlagen für die Organisation des Zählereinsatzes, soweit sie nicht bereits von der Gemeinde vernichtet wurden.

  Auch die Vernichtung dieser Unterlagen habe ich stichprobenweise kontrolliert. Sie war korrekt.
- Mit der Vernichtung der weiteren Volkszählungsunterlagen hat das Landesamt eine Papierfabrik beauftragt. Zu vernichten sind noch ca. 220 Tonnen Material aus ganz Bayern. Ich werde mich an Ort und Stelle von der Vernichtung der Unterlagen überzeugen.

13.1.4. Prüfung des Landesamtes für Statistik und Datenverarbeitung

Gegenstand der Prüfung waren die Einhaltung der Datensicherungsmaßnahmen und der rechtlichen Vorgaben aus dem Volkszählungsgesetz. Die Prüfung brachte ein erfreuliches Ergebnis. Eine förmliche Beanstandung war nicht veranlaßt. Folgende Beispiele verdeutlichen das:

- § 15 Abs. 1 VZG 1987 bestimmt, daß die Hilfsmerkmale unverzüglich nach Durchführung der Eingangskontrollen von den Erhebungsmerkmalen zu trennen und gesondert aufzubewahren sind. Konkret bedeutet dies, daß bei der Volkszählung die Mantelbögen von den übrigen Erhebungsbögen und bei der Arbeitsstättenzählung die Seite 1 des Arbeitsstättenbogens von den folgenden Seiten getrennt und bei der Gebäudevorerhebung die Erhebungsvordrucke nach Übertragung der Daten in den Wohnungsbogen vernichtet werden müssen. Die Prüfung hat ergeben, daß das Abtrennen und die gesonderte Aufbewahrung in allen Fällen durchgeführt worden sind.
- Bei selbständig Tätigen, bei denen Wohn- und Arbeitsstätte identisch sind, könnte es unter Umständen bei Verletzung der Datensicherungsvorschriften dazu kommen, daß nach der Speicherung durch einen Vergleich des Personenbogens und des Arbeitsstättenbogens der Auskunftspflichtige identifiziert werden könnte.
  Das Bundesverfassungsgericht hat deshalb im Beschluß vom 18.12.1987 bestimmt, daß eine Speicherung der Erhebungsmerkmale Straße und Hausnummer der Arbeitsstätte zu unterbleiben hat. Der Verzicht auf diese Speicherung sei den statistischen Landesämtern nicht freigestellt, sondern von Verfassungs wegen zum Schutz des Rechts auf informationelle Selbstbestimmung geboten.
  Die Prüfung hat ergeben, daß Straße und Hausnummer bei Selbständigen, bei denen Wohn- und Arbeitsstättenanschriften identisch sind, nicht gespeichert werden.
- Bei der Prüfung wurde lediglich folgender Mangel festgestellt:
  Nach der Eingangskontrolle und nach der Trennung der Hilfsmerkmale von den Erhebungsmerkmalen werden die leeren Personenbögen aus dem sog. Haushaltsheft herausgetrennt. Ebenso werden verschriebene Bögen ausgesondert. Letztere hat das Landesamt bei der Eingangskontrolle mit einem roten Diagonalstrich oder einem roten „Ungültig" gekennzeichnet. Die leeren und verschriebenen Bögen wurden bis zur Vernichtung gemeinsam gesammelt, von einem privaten Müllfahrzeug abgeholt und in Anwesenheit von Beschäftigten des Landesamtes in einem Müllheizkraftwerk verbrannt. Da die mit rotem Diagonalstrich oder „Ungültig" gekennzeichneten Bögen jedenfalls teilweise richtige Einzelangaben und Echtdaten enthalten, waren an ihre Aufbewahrung höhere Anforderungen zu stellen als bei leeren Erhebungsbögen. Ich habe das Landesamt für Statistik und Datenverarbeitung gebeten, die ausgefüllten ungültigen Bögen getrennt zu sammeln und unverzüglich zu vernichten. Das Landesamt hat daraufhin das Verfahren sofort geändert.

13.2. Mikrozensus

Neben der Volkszählung fand 1987 auch eine Erhebung nach dem Mikrozensusgesetz statt. Hierbei wurden in Bayern 99.392 Personen oder 0.9% der Bevölkerung befragt.

Ein Bürger, der zur Mikrozensuserhebung herangezogen wurde, legte dar, daß es in dem Straßenabschnitt, in dem er wohne, zu einer Häufung auskunftspflichtiger Personen gekommen sei.

Eine Nachfrage beim Landesamt für Statistik und Datenverarbeitung ergab, daß diese Häufung dem nach dem Mikrozensusgesetz vorgesehenen Auswahlverfahren entsprach und daher datenschutzrechtlich nicht zu beanstanden war.

14. Schulwesen

Datenschutzrechtlich gravierende Probleme gab es im Berichtszeitraum im Schulbereich nicht.

Dies hat seinen Grund auch darin, daß das Staatsministerium für Unterricht und Kultus schon frühzeitig „Erläuternde Hinweise für die Schulen zum Vollzug des Bayerischen Datenschutzgesetzes" erlassen hat. Die Hinweise wurden im Berichtszeitraum unter wesentlicher Beteiligung meiner Geschäftsstelle überarbeitet. Sie gehen nunmehr den

einzelnen Schulen zu, die sich hiermit über grundsätzliche datenschutzrechtliche Fragen informieren können.

Dennoch haben meine Geschäftsstelle auch aus dem schulischen Bereich wieder zahlreiche Fragen auf fernmündlichem Wege erreicht. Sie konnten zumeist sofort geklärt werden. Ich begrüße das aus der zunehmenden Zahl an fernmündlichen und schriftlichen Anfragen zu entnehmende steigende Datenschutzbewußtsein im Schulbereich.

Bayern ist seit Jahren führend in der schulischen EDV-Ausbildung und der Ausstattung der Schulen mit Computern. Erfreulicherweise legt das Staatsministerium für Unterricht und Kultus Wert auf die Verwendung einheitlicher Schulverwaltungsprogramme, die zentral auf die Beachtung des geltenden Rechts überprüft sind. Abweichende Programme werden nur noch in seltenen Ausnahmefällen genehmigt. Dies garantiert ein erhöhtes Maß an Datenschutz und an Datensicherheit.

14.1. Weitergabe von Lehrerdaten an Lehrerverbände zur Erstellung von Handbüchern

Aufgrund verschiedener Anfragen weise ich darauf hin, daß die Übermittlung von Lehrerdaten durch Schulbehörden an Lehrerverbände grundsätzlich nur zulässig ist, wenn der betroffene einzelne Lehrer eingewilligt hat. Die Lehrerverbände beabsichtigen aufgrund dieser Daten Lehrerhandbücher herzustellen, die in der Vergangenheit positiv aufgenommen wurden. Allerdings besteht keine Veranlassung, einen Lehrer hier gegen seinen Willen aufzuführen.

14.2. Automatisierte Schülerdateien

In Ergänzung zu meinen Ausführungen im letzten Tätigkeitsbericht (Seiten 50/51) weise ich auf einige immer wiederkehrende Probleme hin:

Die mit automatisierten Verfahren beschäftigten Personen sind auf die Wahrung des Datengeheimnisses zu verpflichten. Das Original der Verpflichtungserklärung ist zu den Personalakten zu nehmen, ein Abdruck ist dem Beschäftigten auszuhändigen (Ziff. 14.4 VollzBek zu Art. 14 BayDSG). Die Übersendung an meine Geschäftsstelle ist überflüssig.

In einigen Jahresberichten werden Anschriften von Schülern veröffentlicht. Dies ist nach Art. 62 Abs. 3 BayEUG unzulässig.

Bei der Anmeldung eines Schülers in der Schule darf der Name der Krankenversicherung weder erhoben noch abgespeichert werden, da das Datum regelmäßig für schulische Zwecke nicht benötigt wird. Dies schließt jedoch nicht aus, daß Versicherungsdaten aus Anlaß eines Unfalls des betroffenen Schülers erhoben und an die zuständige Unfallversicherung weitergeleitet werden, soweit dies zur Abklärung der versicherungsrechtlichen Ansprüche erforderlich ist.

Die Angabe der Krankenversicherung kann allerdings bei Schülerfahrten ins Ausland auf einem Begleitbogen für den Lehrer zweckmäßig sein.

14.3. Automatisierte Lehrerdateien (DIAPERS)

Zum Personalverwaltungsverfahren DIAPERS stehe ich sowohl hinsichtlich grundsätzlicher Probleme wie auch wegen Detailfragen mit den Staatsministerien des Innern, für Unterricht und Kultus sowie der Finanzen in Schriftwechsel.

In letzter Zeit ist der Einsatz von DIAPERS im Bereich der Kultusverwaltung in die öffentliche Diskussion geraten; ich werde immer wieder um eine datenschutzrechtliche Bewertung gebeten. Eine solche ist abschließend derzeit noch nicht möglich, da das Verfahren noch im Aufbau begriffen ist. Entscheidend für eine endgültige Bewertung sind die Festlegung der für die Lehrer der einzelnen Schultypen zu speichernden Daten und der Zugriffsberechtigungen der verschiedenen Schulbehörden sowie die Abstimmung mit den weiteren im Kultusbereich geführten Datensammlungen über Lehrer. Bereits jetzt kann jedoch gesagt werden, daß gegen die Einführung des Personalverwaltungsverfahrens im Kultusbereich keine grundsätzlichen datenschutzrechtlichen Bedenken bestehen. Die Datensicherungsmaßnahmen sind nach meinen Vorschlägen konzipiert und teilweise vorbildlich.

Mit Hilfe von DIAPERS wird es möglich sein, einen Überblick über den beruflichen Werdegang (Ausbildung, Prüfungsdaten, Dienstbezeichnung usw.) eines Lehrers zu erstellen. Die automatisierte Fertigung eines Persönlichkeits- oder Leistungsprofils ist dagegen nach der Verfahrenskonzeption nicht möglich, da hierfür weder die Daten noch die Programme vorhanden sind. Sie ist auch nicht beabsichtigt.

14.4. Einsatz von privaten Rechnern staatlicher Lehrkräfte zu Hause zur Unterstützung der Schulverwaltung

Aufgrund einer Anfrage des Staatsministeriums für Unterricht und Kultus hatte ich mich mit der Frage zu beschäftigen, ob staatliche Lehrkräfte private Rechner zur Unterstützung der Schulverwaltung einsetzen dürfen. Ich vertrete hierzu folgende Auffassung:

Ein Lehrer, der zu Hause auf seinem privaten Rechner Schülerdaten verarbeitet, wird als Teil der Behörde „Schule" tätig. Daher ist das Bayer. Datenschutzgesetz anwendbar, denn es kann datenschutzrechtlich keinen Unterschied machen, ob ein Lehrer im Schulbereich am Computer in Anwendung öffentlichen (Schul-) Rechts Schülerdaten verarbeitet oder ob er diese Arbeit zu Hause erledigt. Speichernde Stelle im Sinne des Art. 5 Abs. 3 Nr. 1 BayDSG ist die Schule. Daraus folgt:

Wenngleich die im 8. Tätigkeitsbericht auf Seite 79 geäußerten Bedenken hinsichtlich der Sicherheit der Datenträger beim Einsatz von Kleincomputern in der Schule auch hier gelten, so meine ich dennoch, daß aufgrund der besonderen Situation der Lehrer bei Vorgabe einiger Datenschutzmaßnahmen die Benutzung privater Kleincomputer für schulische Aufgaben zugelassen werden kann. Dem Lehrer steht in der Schule regelmäßig kein ausreichender Arbeitsplatz für die Erledigung von Verwaltungsarbeiten zur Verfügung. Daher ist es schon immer üblich, daß er Unterlagen mit personenbezogenen Schülerdaten (etwa Schülernoten) zu Hause aufbewahrt und bearbeitet. Hiergegen sind rechtliche Bedenken – bei Einhaltung der folgenden Sicherungsmaßnahmen nicht zu erheben:

- Durch ministerielle Richtlinien sollten den Lehrern Vorgaben zur Datensicherheit (Datenträger und weitere Unterlagen jederzeit verschlossen aufbewahren und Dritten nicht zugänglich machen usw.) gegeben werden.

Gleichzeitig sollte jeder Lehrer, der seinen privaten Computer für die Erledigung schulischer Aufgaben nutzen will, verpflichtet werden, dies im vorhinein seiner Schule mitzuteilen und eine Genehmigung zu erholen, sowie nur freigegebene Programme zu verwenden.

- Die Unterrichtung der Schule durch den Lehrer ist auch deshalb erforderlich, weil die Schule als speichernde Stelle verpflichtet ist, entsprechend der Datenschutzregisterverordnung die Verarbeitung personenbezogener Daten mitzuteilen.
- Letztendlich muß eine datenschutzrechtliche Überprüfung beim Lehrer stattfinden können. Die Lehrer, die beabsichtigen, einen privaten Rechner zu nutzen, sind darauf hinzuweisen, daß sie mit einer Kontrolle durch meine Mitarbeiter rechnen müssen und die Genehmigung zur Benutzung eines privaten Computers nur erhalten können, wenn sie die notwendigen Sicherungsmaßnahmen treffen und sich mit einer eventuellen Kontrolle einverstanden erklären.

Das Staatsministerium des Innern teilt für diesen besonderen Fall meine Auffassung, weist aber im übrigen zu Recht darauf hin, daß gegen die Speicherung und Verarbeitung dienstlicher personenbezogener Daten auf privaten EDV-Geräten grundsätzliche datenschutzrechtliche Bedenken bestehen. Die Einhaltung der datenschutzrechtlichen Bestimmungen, insbesondere des Art. 15 BayDSG (technische und organisatorische Maßnahmen), kann in der Regel mit vertretbarem technischem und organisatorischem Aufwand nicht gewährleistet werden. Die bei Schulen vorliegenden besonderen Verhältnisse sind auf andere Behörden nicht ohne weiteres übertragbar.

15. Hochschule

15.1. Abschluß der datenschutzrechtlichen Prüfung der Ludwig-Maximilians-Universität München

Die Ergebnisse meiner Prüfung habe ich bereits im letzten Tätigkeitsbericht (S. 49) mitgeteilt. Zwischenzeitlich hat die Universität zu den Anregungen in meinem Prüfbericht Stellung genommen. Nahezu sämtliche Bedenken meinerseits, etwa zur Belegung einzelner Felder in der Studenten-, der automatisierten Zulassungs-, der Zulassungsdatei/Widerspruchsverfahren und der Personaldatei, konnten ausgeräumt werden. Weiterhin wurden Fragen der Datenaussonderung geklärt. Als einzige noch offene Frage ist die Aufbewahrung der statusrechtlichen Unterlagen der Studenten verblieben. Diese soll nunmehr – entsprechend einer Anregung in meinem Bericht – in einer internen Dienstanweisung an die Studentenkanzlei geregelt werden.

15.2. Änderung des Bayerischen Hochschulgesetzes

Die aufgrund einer Änderung des Hochschulrahmengesetzes erforderliche Überarbeitung des Bayerischen Hochschulgesetzes enthält keine bereichsspezifischen Datenschutzregelungen, obwohl in einem Vorentwurf noch Vorschriften zur Erhebung und Verarbeitung personenbezogener Studentendaten sowie zur Bereitstellung von Daten durch die Prüfungsämter vorgesehen waren. Offenbar soll durch Regelungen in den Querschnittsgesetzen (Datenschutz-, Verwaltungsverfahrensgesetze) die Normenflut begrenzt werden.

Derzeit ist das Bayer. Datenschutzgesetz anwendbar, das jedoch keine Befugnisnorm für die Zulässigkeit der Datenerhebung enthält. Bereits die Erhebung personenbezogener Daten ist aber nach den Grundsätzen des Volkszählungsurteils als Eingriff in das informationelle Selbstbestimmungsrecht anzusehen und kann deshalb nicht ohne Rechtsgrundlage erfolgen. Für statistische Daten enthalten die Statistikgesetze einige Rechtsgrundlagen für die Datenerhebung. Eine Bestimmung für die Erhebung von Verwaltungsdaten fehlt. Ob die bisher im Änderungsentwurf des Verwaltungsverfahrensgesetzes vorgesehene Datenerhebungsregelung für die Bedürfnisse der Hochschule ausreicht, erscheint zweifelhaft. Deshalb würde ich die Aufnahme zumindest einer Datenerhebungsvorschrift im Hochschulgesetz begrüßen.

15.3. Einzelfälle

Von allgemeinem Interesse erscheinen mir folgende Eingaben aus dem Hochschulbereich:

- Eine Universitätsstadt fragte an, ob Daten von Studenten, die sich mit dortigem Wohnsitz immatrikuliert haben, zum Zweck eines Abgleichs mit den dem Einwohnermeldeamt vorliegenden Angaben von der Universität an die Stadt (Einwohnermeldeamt) weitergegeben werden dürfen. Hierdurch sollen nicht Verstöße gegen das Melderecht festgestellt und sanktioniert werden. Vielmehr soll die Stadt die Möglichkeit erhalten, die betreffenden Studenten anzuschreiben und darauf hinzuweisen, daß von der Anmeldung die Zuweisung staatlicher Gelder abhängt.

  Rechtsgrundlage für die Erhebung der Studentendaten durch die Universität sind §§ 4 und 13 Abs. 1 Satz 1 Hochschulstatistikgesetz (HStatG) in Verbindung mit § 15 Bundesstatistikgesetz (BStatG). Die für Zwecke der Statistik erhobenen Daten unterliegen dem Statistikgeheimnis nach § 15 HStatG und § 16 BStatG. Die von der Stadt gewünschte Datenweitergabe fällt nicht unter die dort geregelten Fälle der zulässigen Datenübermittlung. Daher müßten die betreffenden Studenten in die Übermittlung von Einzelangaben an das Einwohnermeldeamt schriftlich einwilligen (§ 16 Abs. 1 Satz 2 Nr. 1 BStatG).

  Nach geltendem Recht können Universität und Stadt daher nur durch Öffentlichkeitsarbeit auf die Rechtslage und die mit der Meldung zusammenhängenden Schlüsselzuweisungen durch den Freistaat aufmerksam machen. Ferner kann die Universität die Studenten auf die Erfüllung der Meldepflicht hinweisen.

- Ein Hochschulabsolvent äußerte mir gegenüber die Vermutung, sein Name, seine Anschrift und seine Examensergebnisse seien einem staatlichen Hochschulforschungsinstitut ohne seine Einwilligung und ohne Rechtsgrundlage zur Verfügung gestellt worden. Dies hat sich als nicht richtig herausgestellt.

  Das Institut hat ein Forschungsprojekt „Professorinnen in der Minderheit" durchgeführt. Da ihm die notwendigen Anschriften der zu befragenden Hochschulabsolventen nicht zur Verfügung standen, hat das Institut zunächst ein nicht adressiertes Anschreiben erstellt, mit dem Hochschulabsolventen freiwillig um Mitarbeit gebeten wurden. Das Anschreiben hat das Institut in einem ebenfalls unadressierten verschlossenen Freiumschlag der Univer-

sität übergeben. Mitarbeiter des Prüfungsamtes der Universität haben die Briefumschläge adressiert und versandt. Das Institut hatte die Universität gebeten, bei der Versendung des Anschreibens nur Absolventen zu berücksichtigen, die im Examen die Promotionsnote erreicht hatten. Das Institut selbst hat also keine personenbezogenen Daten erhalten.

- Die Mitarbeiterin eines Prüfungsamtes fragte bei mir an, ob ein Professor in Prüfungsnoten, die von einem anderen Professor erteilt wurden, Einsicht nehmen darf, und ob Daten eines Bewerbers um einen Arbeitsplatz vom Prüfungsamt an den Fachbereich der gleichen Hochschule, die den Arbeitsplatz anbietet, weitergegeben werden dürfen. Ich habe wie folgt geantwortet:
  Bereits das Bereithalten von Daten (hier: Prüfungsnoten) in einer Kartei zur Ermöglichung der Einsicht von einzelnen Professoren stellt eine Datenübermittlung (vgl. hierzu Art. 5 Abs. 2 Nr. 2 letzte Alternative BayDSG) dar. Die Einsichtnahme ist nach Art. 17 Abs. 1 BayDSG zulässig, wenn sie im Einzelfall zur rechtmäßigen Erfüllung der durch Rechtsnorm der übermittelnden Stelle (Prüfungsamt) oder dem Empfänger (einzelner Professor) zugewiesenen Aufgaben (etwa im Prüfungsverfahren) erforderlich ist. Hieran fehlt es.

  Die Datenübermittlung vom Prüfungsamt an den Fachbereich, der andere Aufgaben als die übermittelnde Stelle (Prüfungsamt) wahrnimmt, und damit Dritter im Sinn des Art. 17 Abs. 3 BayDSG ist, ist unzulässig. Die Überlassung von Noten ohne Einwilligung verstößt gegen Datenschutzrecht.

16. Archivwesen und Forschung

Das Archivwesen und die damit zusammenhängende Forschung haben im Berichtszeitraum keine datenschutzrechtlichen Probleme aufgeworfen.

16.1. Bayer. Archivgesetz

Aus datenschutzrechtlicher Sicht sehr erfreulich ist allerdings, daß die Staatsregierung am 3.5.1988 den vom Staatsministerium für Unterricht und Kultus vorgelegten Entwurf eines Bayer. Archivgesetzes beschlossen und dem Senat zur Stellungnahme übersandt hat, die zwischenzeitlich der Staatsregierung bereits vorliegt.

Das Gesetzesvorhaben, das ich von Anfang an begleitet habe, trägt meinen Vorstellungen weitgehend Rechnung, was ich bereits in meinem letzten Tätigkeitsbericht angesprochen hatte.

16.2. Benutzung von Archivgut aus dem „Dritten Reich" für Forschungszwecke

Im Berichtszeitraum haben mich Anfragen zur Geltung archiv- und datenschutzrechtlicher Grundsätze für im „Dritten Reich" angefallene Unterlagen erreicht. Hierzu habe ich darauf hingewiesen, daß bis zur Verabschiedung des Bayerischen Archivgesetzes unterschiedliche Rechtsgrundlagen heranzuziehen sind: Für Auskünfte aus dem Melderegister gelten Art. 11 Abs. 3 und 34 Bayerisches Meldegesetz. Auskünfte aus Akten eines Stadtarchivs richten sich nach etwa erlassenen Benutzungsordnungen oder Benutzungssatzungen, die dem grundgesetzlich geschützten Persönlichkeitsrecht Rechnung tragen müssen. Im übrigen können auch die Vorschriften des Bayerischen Datenschutzgesetzes zumindest entsprechend Anwendung finden. Das Grundrecht auf Wissenschaftsfreiheit gewährt regelmäßig kein Recht auf Einsicht in archiviertes amtliches Schriftgut, das sich auf eine noch lebende oder vor weniger als 30 Jahren verstorbene Person bezieht, wenn diese der Einsichtnahme nicht zugestimmt hat und bei der Auswertung der Unterlagen ihr privater Lebensbereich nicht unberücksichtigt bleibt (siehe auch 7.7).

16.3. Wissenschaftliche Forschung

Aufgrund eines Beitrages in der Zeitschrift „Bild der Wissenschaft" (9/1987) mit dem Titel „Der Datenschutz treibt uns Forscher ins Ausland" wurde ich von der Interparlamentarischen Arbeitsgemeinschaft um Stellungnahme zu dieser These gebeten. In dem Artikel wurde vor allem kritisiert, ein großer Teil medizinischer und sozialwissenschaftlicher Untersuchungen sei heute in der Bundesrepublik Deutschland wegen der strengen Datenschutzbestimmungen nicht mehr durchführbar. Nach meiner Auffassung trifft diese Kritik zumindest für Bayern nicht zu:

Die Zulässigkeit der Erhebung, Speicherung, Nutzung und Übermittlung von personenbezogenen Daten im Rahmen von medizinischen Dokumentations- und Forschungsvorhaben ist in erster Linie nach den Grundsätzen der ärztlichen Schweigepflicht gemäß § 203 Strafgesetzbuch (StGB) zu beurteilen. Daneben kommen die allgemeinen Datenschutzgesetze zur Anwendung. Von einer nachhaltigen Erschwerung der Forschungstätigkeit durch den Datenschutz kann daher keine Rede sein.

- Für Daten von Patienten, die in bayerischen Krankenhäusern behandelt werden, gilt Art. 26 Bayerisches Krankenhausgesetz. Diese Bestimmung geht den allgemeinen Datenschutzgesetzen als Spezialgesetz vor. Wegen ihres anderen Regelungsbereichs ist sie zwar unabhängig von § 203 StGB anzuwenden. So darf der Krankenhausarzt zu Forschungszwecken erforderliche Patientendaten im Krankenhaus nutzen.
- Auch nach dem geltenden ärztlichen Standesrecht ist eine Übermittlung von Patientendaten nur in anonymisierter Form oder mit Einwilligung des Patienten zulässig.

Rechtliche Probleme bei der Verwendung von Patientendaten im Rahmen epidemiologischer Forschungsvorhaben ergeben sich in erster Linie aus der im grundsätzlichen unumstrittenen ärztlichen Schweigepflicht und werden nicht durch „neue" Datenschutzbestimmungen hervorgerufen.

Bisherige Erfahrungen mit zahlreichen medizinischen Dokumentations- und Forschungsvorhaben zeigen, daß in der Praxis meist ein Weg gefunden werden kann, der sowohl dem Forschungsinteresse als auch dem Interesse der Patienten an der Wahrung ihrer Geheimnisse gerecht wird. Soweit der Patient nicht oder nicht mehr in der Lage ist, seine Einwilligung zu erteilen, ist – allerdings nur nach sorgfältiger Einzelfallprüfung – auch an eine mutmaßliche Einwilligung zu denken. In einer Vielzahl von Fällen ist die Einholung der Einwilligung des Patienten jedoch überflüssig, da mit anonymisierten Daten gearbeitet werden kann. Es sind Verfahren in Planung und bereits im Einsatz, bei denen der dokumentierende oder forschende Arzt statt des Patientennamens nur eine Nummer kennt, die keine

identifizierenden Hinweise enthält. Unter dieser Nummer kann beispielsweise ein behandelnder Arzt weitere Daten an den Forscher übermitteln. Wenn diese Daten ebenfalls keinen Rückschluß auf den Patienten zulassen, werden keine Patientengeheimnisse im Sinne des § 203 StGB offenbart. Durch eine Anonymisierung der Patientendaten kann damit sowohl dem Interesse der Forschung als auch dem Recht der Patienten auf ärztliche Verschwiegenheit Rechnung getragen werden.

17. Umweltfragen

17.1. Spannungsverhältnis Umweltschutz – Datenschutz

Der Umweltschutz gewinnt rapide an Bedeutung. Gleichzeitig werden die Stimmen immer lauter, die die Namen der Personen und Institutionen veröffentlicht wissen wollen, die im Verdacht stehen, durch hohe Emissionen die Umwelt zu belasten. Soweit nur die Daten juristischer Personen betroffen sind, ist der Datenschutz, der nur natürliche Personen, also die Menschen schützen soll, grundsätzlich nicht berührt. Aber bei Firmendaten von Einzelpersonen oder bei der Nennung von Verantwortlichen in einem Unternehmen kann es durchaus zu einem Spannungsverhältnis zwischen Öffentlichkeitsinteresse und Datenschutz kommen.

Noch war meine Geschäftsstelle nur am Rande mit der Frage befaßt, unter welchen Voraussetzungen die Veröffentlichung oder Bekanntgabe von Emissionsdaten einschließlich der Angabe des Emittenten datenschutzrechtlich zulässig sei. Daß das Thema der Bekanntgabe von Umweltdaten jedoch immer mehr an Bedeutung gewinnt, zeigen auch verschiedene Gesetzesinitiativen zur Auskunft über Umweltdaten und das steigende Interesse der Medien an diesem Problemkreis. Im Berichtszeitraum wurde immer wieder von Versuchen einzelner Gemeinden berichtet, die Öffentlichkeit über Umweltbelastungen durch Unternehmen detaillierter zu informieren. Soweit die zuständigen Aufsichtsbehörden bislang einer Veröffentlichung der Schadstoffdaten von namentlich genannten Unternehmen widersprochen haben, ist dies wohl zum Schutze der Unternehmen und weniger aus Datenschutzgründen geschehen.

Der Bezug zum Datenschutz ergibt sich aber daraus, daß eben auch Umweltdaten, z.B. Daten über den Schadstoffausstoß, im Einzelfall personenbezogen sein können, nämlich dann, wenn der Betreiber der Anlage eine natürliche Person ist. Dann fallen diese Daten unter den Schutz des Bayer. Datenschutzgesetzes. Im übrigen sind auch Daten juristischer Personen geschützt, wie z.B. § 27 Abs. 3 Bundesimmissionsschutzgesetz zeigt, wonach Einzelangaben der Emissionserklärung nicht veröffentlicht werden dürfen, wenn aus diesen Rückschlüsse auf Betriebs- oder Geschäftsgeheimnisse gezogen werden können.

Im Ergebnis kommt es meines Erachtens darauf an, die berechtigten Interessen der Bürger an der Aufklärung über Umweltbelastungen einerseits und die schutzwürdigen Belange der betroffenen Anlagenbetreiber andererseits abzuwägen und die bestehenden Zielkonflikte zwischen Umweltschutz und Datenschutz in Ausgleich zu bringen. Es wäre wünschenswert, wenn die grundsätzlichen Entscheidungen in den jeweiligen Fachgesetzen so präzise wie möglich vom Gesetzgeber selbst getroffen würden.

17.2. Einsatz elektronischer Datenverarbeitung in der Umweltschutzverwaltung

Auch die Umweltschutzverwaltung wird sich künftig bei ihrer Aufgabenerfüllung zunehmend der elektronischen Datenverarbeitung bedienen. Hierbei werden nicht nur sachbezogene Daten, sondern auch personenbezogene Daten, z.B. Daten von Grundstückseigentümern oder Anlagenbesitzern, soweit es sich um natürliche Personen handelt, verarbeitet. Zwei Beispiele für den geplanten Einsatz automatisierter Systeme seien hier genannt:

17.2.1. Bodeninformationssystem (BIS)

Die Staatsregierung beauftragte das Staatsministerium für Landesentwicklung und Umweltfragen, zusammen mit den fachlich betroffenen Ressorts in Bayern ein Bodeninformationssystem einzurichten. In diesem EDV-gestützten System sollen alle wichtigen zum Zweck des Bodenschutzes relevanten Daten enthalten sein, d.h. Informationen über den Zustand, die Nutzung und die Belastbarkeit von Böden. Das Kernstück des Bodeninformationssystems soll der bodenkundliche Teil sein, der am Geologischen Landesamt geführt und auf der Grundlage des Bodenkatasters Bayern aufgebaut wird. Ziel ist, eine zwischen Bund und Ländern abgestimmte und für spezifische Zwecke des Bodenschutzes geeignete Datenbasis zu entwickeln.

Bei meiner datenschutzrechtlichen Prüfung stellte ich fest, daß zwangsweise erhobene personenbezogene Daten verarbeitet werden sollen, wobei nicht in allen Fällen eine scharfe Abgrenzung zwischen naturbezogenen und anthropogenen Einwirkungen mit einer eindeutigen Zuordenbarkeit zu einer natürlichen Person gezogen werden kann. Allerdings ist zu berücksichtigen, daß Daten, die den Wert oder die Geeignetheit eines Grundstücks für eine bestimmte Nutzung bestimmen, eine Angabe über sachliche Verhältnisse des bestimmbaren Eigentümers und damit personenbezogene Daten darstellen.

Für die Datenverarbeitung durch das Geologische Landesamt im Rahmen des Bodeninformationssystems halte ich die derzeit bestehenden Rechtsvorschriften (Gesetz über die Aufgaben des Bayer. Geologischen Landesamtes in Verbindung mit dem Bayer. Datenschutzgesetz) für eine ausreichende Rechtsgrundlage. Im Hinblick auf Art, Umfang und denkbare Verwendung der erhobenen Daten sowie der Gefahr ihres Mißbrauchs ist derzeit eine bereichsspezifische Regelung nicht erforderlich. Die Intensität eines Eingriffs scheint mir derzeit eher gering zu sein. Soweit für die Zukunft eine umfangreichere Verarbeitung personenbezogener Daten geplant ist, sollte jedoch eine gesetzliche Ergänzung der bislang bestehenden Rechtsgrundlagen für die Datenverarbeitung in Erwägung gezogen werden. Allerdings ist bereits zum jetzigen Zeitpunkt im Hinblick auf die vom Bundesverfassungsgericht in seiner Rechtsprechung geforderte Transparenz der Datenverarbeitung von den zuständigen Behörden zu prüfen, ob dem Informationsbedürfnis der Betroffenen durch Hinweise über die Datenerhebung, -speicherung und -übermittlung abgeholfen werden kann.

Wegen des weiteren Fortgangs des Projekts stehe ich mit dem Staatsministerium für Landesentwicklung und Umweltfragen in Verbindung.

17.2.2. Umweltüberwachungssystem (UMSYS)

Seit Januar 1986 wird dieses System in der Umweltschutzverwaltung eines Landratsamtes erprobt. Ziel ist ein umfassendes Überwachungsprogramm, das letztlich bei allen Kreisverwaltungsbehörden eingesetzt werden soll. Im System werden alle notwendigen fachspezifischen umweltrelevanten Daten anlagenbezogen verarbeitet. So soll es z.B. möglich sein, innerhalb kurzer Zeit alle Anlagen in einem Landkreis zu benennen, die ein bestimmtes Produkt, einen bestimmten Abfall oder Luftverunreinigungen erzeugen, oder die bestimmte wassergefährdende Flüssigkeiten lagern.

In Teilbereichen der Umweltverwaltung des Landratsamtes, insbesondere der Luftreinhaltung, Abfallbeseitigung und dem Wasserrecht, werden bereits anlagenbezogene Umweltdaten erfaßt und Auswerteprogramme getestet. Beim Vollzug der Verordnung für wassergefährdende Stoffe und Flüssigkeiten wird das DV-System über den Probebetrieb hinaus auch schon zur Abwicklung von Verwaltungsaufgaben genutzt.

Nach meiner Auffassung stehen grundsätzliche datenschutzrechtliche Bedenken der Errichtung des Umweltüberwachungssystems nicht entgegen. Rechtsgrundlage ist Art. 16 BayDSG i.V.m. den jeweiligen Umweltgesetzen. Detailfragen hinsichtlich der Zulässigkeit einzelner Datenspeicherungen und -übermittlungen sowie Fragen der Datensicherheit werden aber noch zu klären sein.

17.3. Richtlinie „Strahlenschutz in der Medizin"

Nach der Richtlinie „Strahlenschutz in der Medizin" haben Radiologische Kliniken in bestimmten Fällen die Entlassung von Patienten aus der stationären Behandlung der atomrechtlichen Aufsichtsbehörde anzuzeigen; die Entlassung der Patienten bedarf wegen der von ihnen ausgehenden Strahlenbelastung ggf. der Zustimmung der Aufsichtsbehörde. Die Anzeigen der Kliniken enthalten neben Angaben zur durchgeführten Therapie auch die Namen der betroffenen Patienten. Dies stellt eine Durchbrechung der ärztlichen Schweigepflicht dar, die – ohne Einwilligung – nur aufgrund einer Rechtsvorschrift zulässig ist.

Das Landesamt für Umweltschutz hat aufgrund meiner Bedenken das Verfahren bei der Entlassung strahlenbehandelter Patienten geändert:

Bis zu einem bestimmten Grenzwert der Strahlenbelastung wird ein anonymes Anzeigeverfahren durchgeführt. Wird dieser Grenzwert überschritten, so müssen unter Umständen die häuslichen Verhältnisse überprüft werden, da von den Patienten aufgrund ihres noch hohen Restanteils an inkorporierter Radioaktivität eine erhebliche Gefährdung für ihre Umwelt ausgehen kann. Für diese Überprüfung sind personenbezogene Daten notwendig. Eine Entlassungsgenehmigung wird in solchen Fällen daher nach Aussage des Landesamtes für Umweltschutz nur noch erteilt, wenn der hiervon betroffene Patient schriftlich einer derartigen Überprüfung zustimmt. Dieses Verfahren ist aus datenschutzrechtlicher Sicht zu begrüßen.

Die auch von einigen anderen Datenschutzbeauftragten geäußerten Bedenken zur Handhabung der Richtlinie „Strahlenschutz in der Medizin" waren Gegenstand der Erörterung im Länderausschuß für Atomkernenergie – Fachausschuß Strahlenschutz. Der Bundesminister für Umwelt, Naturschutz und Reaktorsicherheit und die Mehrheit der Ländervertreter halten die Übermittlung personenbezogener Daten für einen effektiven Schutz der Bevölkerung vor ionisierenden Strahlen bei der Entlassung von Patienten für geboten. Bei einer Änderung des Atomgesetzes beabsichtigt der Bundesminister eine zusätzliche Regelung hinsichtlich des Datenschutzes einzufügen.

18. Straßenverkehr

18.1. Zentrales Verkehrsinformationssystem (ZEVIS)

Durch eine Novellierung des Straßenverkehrsgesetzes (StVG, näher hierzu Seite 53 des 9. Tätigkeitsberichts) wurden die rechtlichen Grundlagen für den automatisierten Abruf von Kraftfahrzeug- und Halterdaten aus örtlichen Registern wie auch aus dem Zentralen Fahrzeugregister geschaffen. Damit ist mir eine neue Prüfaufgabe erwachsen, die nun anläuft:

Erste Überprüfungen

Das Straßenverkehrsgesetz hat die Protokollierung von Anfragen aus dem Zentralen Fahrzeugregister angeordnet, um die Kontrolle der Rechtmäßigkeit der Anfragen zu ermöglichen. Deshalb wird durchschnittlich bei jeder fünfzigsten Anfrage einer Polizeidienststelle an den Datenbestand des Zentralen Fahrzeugregisters beim Kraftfahrtbundesamt (KBA) in Flensburg der Anfragende automatisch aufgefordert, über die sonst üblichen Anfragedaten hinaus zusätzliche Angaben zu machen. Dies sind insbesondere Angaben zur Identität des Anfragenden und zum Grund der Anfrage. Erst bei ordnungsgemäßer Erfüllung dieser Vorgaben wird die entsprechende Auskunft vom KBA erteilt. Aufzeichnungen über diese Protokolldaten führt in Bayern das Landeskriminalamt.

Der Bundesbeauftragte für den Datenschutz ist vom Bundestag beauftragt, über die Erfahrungen mit dem Datenschutz bei ZEVIS zu berichten. In Zusammenarbeit mit dem Bundes- und den Landesbeauftragten für den Datenschutz habe ich ein Prüfkonzept erarbeitet, um feststellen zu können, ob die Protokollierungspflichten eingehalten werden.

Bei der ersten Prüfung habe ich vom Landeskriminalamt die Aufzeichnungen eines Kalendermonats erbeten und ausgewertet. Hierbei war festzustellen, daß mit Inkrafttreten der Fahrzeugregisterverordnung die Anfragen an das Kraftfahrbundesamt leicht angestiegen sind. Dies deutet darauf hin, daß dieser Form der Anfrage bei der polizeilichen Alltagsarbeit künftig wohl steigende Bedeutung zukommen wird. Nach meinen Feststellungen protokolliert das Landeskriminalamt die Anfragen sowohl zahlenmäßig wie auch inhaltlich vollständig.

Die Qualität der von den Polizeidienststellen angelieferten Protokolldaten ist allerdings noch verbesserungsbedürftig. Deshalb hat das Staatsministerium des Innern auf meine Anregung hin angeordnet, daß ab 1.11.1988 – neben einer erneuten Einweisung und Belehrung der Polizeibeamten, die zu einer ZEVIS-Anfrage berechtigt sind – weitere Aufzeichnungen über Anfragen in den Fällen zu führen sind, in denen eine Anfrage nach der automatischen Protokollauf-

forderung abgebrochen wird. Für jedes ZEVIS-berechtigte Datenendgerät sind dann Nachweise über Datum und Uhrzeit der abgebrochenen Abfrage, die Abfragedaten (z. B. Kfz-Kennzeichen oder Personendaten), die abfragende Person und die Gründe für die Nichtprotokollierung dieser Anfrage einzutragen. Die Nachweise sind ein Jahr aufzubewahren. Diesen Aufzeichnungen werde ich besondere Aufmerksamkeit widmen.

18.2. Einzelfälle

18.2.1. Radarmessungen eines Landratsamtes

Ein Landratsamt hat in eigener Zuständigkeit Radarmessungen vorgenommen. Es beabsichtigt, die dabei gewonnenen Daten (Fahrzeughalter und Geschwindigkeit) in Dateien zu speichern. Auf meine Anfrage zur Zulässigkeit dieser Speicherungen hat das Landratsamt mitgeteilt, es benötige die Erkenntnisse für seine Planungen von Ausbaumaßnahmen an Kreisstraßen und zur Vorbereitung verkehrsrechtlicher Anordnungen. Daneben seien auf dieser Grundlage Maßnahmen der Verkehrserziehung geplant.

Das Staatsministerium des Innern vertritt zu Verkehrssünderkarteien die Ansicht, daß die Polizei solche Dateien nicht anlegen darf. Ich meine, daß dies auch für die Landratsämter gelten muß, und eine personenbezogene Speicherung beim Landratsamt mangels gesetzlicher Aufgabenzuweisung daher datenschutzrechtlich unzulässig ist.

Im übrigen ist kein vernünftiger Grund ersichtlich, weshalb zu Straßenplanungen die Kfz-Halter und die gemessenen Geschwindigkeiten erforderlich sind. Verkehrsrechtliche Anordnungen und erzieherische Maßnahmen können sich zudem nur gegen die Fahrzeugfahrer richten.

Vor einer abschließenden Äußerung gegenüber dem Landratsamt habe ich meine vorgenannte Auffassung dem Staatsministerium des Innern mitgeteilt. Eine Stellungnahme von dort erwarte ich demnächst.

18.2.2. Verwechslungen bei der Halterfeststellung

Wie schon im letzten Jahr erreichten mich im Berichtszeitraum Beschwerden einiger Fahrzeughalter, die aufgrund von Verwechslungen beschuldigt wurden, Verkehrsordnungswidrigkeiten begangen zu haben. Exemplarisch sei folgender Fall genannt:

Ein Rechtsanwalt beschwerte sich darüber, daß sein Mandant eine Geldbuße wegen einer Ordnungswidrigkeit zahlen sollte, die zu einem Zeitpunkt begangen wurde, als er noch längst nicht Eigentümer des Fahrzeugs war. Meine Ermittlungen ergaben, daß der automatisierte Abruf der Halterdaten durch die Polizei aus dem örtlichen Fahrzeugregister ohne Eingabe des Tattages der Ordnungswidrigkeit erfolgte, so daß vom System jeweils der Eigentümer zur Zeit der Anfrage angegeben wurde und der Eigentümerwechsel nicht berücksichtigt werden konnte.

Auf diesen Vorfall hin erfolgen nach meiner Intervention die Abfragen der Polizei nunmehr auch unter Eingabe des Tattages, so daß der Abruf von Daten früherer oder späterer Halter, die für das Ordnungswidrigkeitenverfahren ohne Bedeutung sind, künftig unterbleiben dürfte.

19. Medien

19.1. Presse und Datenschutz

Im 9. Tätigkeitsbericht hatte ich auf Lücken im Persönlichkeitsschutz gegenüber Rundfunk und Presse hingewiesen. Zwischenzeitlich hat die Staatsregierung das Staatsministerium des Innern beauftragt, Vorschläge für eine Verbesserung des Persönlichkeitsschutzes vorzulegen. Die Arbeiten des Staatsministeriums sind noch nicht abgeschlossen.

Ich vertrete die Auffassung, daß

- die Lösung des Bundesdatenschutzgesetzes, bestimmte Medienbereiche von der Geltung der Datenschutzbestimmungen auszunehmen (§ 1 Abs. 3 BDSG; § 37 Entwurf zum BDSG), unter Berücksichtigung des Persönlichkeitsschutzes, der Achtung der Menschenwürde und der freien Entfaltung der Persönlichkeit (Art. 1 Abs. 1 i. V. m. Art. 2 Abs. 1 GG) neu überdacht werden sollte. Verfassungsrechtlich erscheint es zulässig und verfassungspolitisch geboten, das derzeitige Medienprivileg des BDSG auf seinen Kern zurückzuführen. Danach wären die Datenschutzvorschriften grundsätzlich auch im Medienbereich anzuwenden. Allerdings müßte im Hinblick auf Art. 5 Abs. 1 Satz 2 GG durch Ausnahmeregelungen sichergestellt werden, daß der **Kernbereich** der Medienarbeit – insbesondere also die publizistische Vorbereitungstätigkeit, z. B. die Informationsbeschaffung oder die Wahrung des Redaktionsgeheimnisses – ausreichend gewährleistet bleibt.
- Die Grundrechtsordnung sieht für den Medienbereich prinzipiell Staatsfreiheit vor. Daher ist die Kontrolle der Beachtung datenschutzrechtlicher Vorschriften im Rundfunkbereich einem von den Rundfunkorganen bestimmten Datenschutzbeauftragten der jeweiligen Rundfunkanstalt übertragen worden. An eine entsprechende Einrichtung sollte auch im Bereich der Printmedien und des Films gedacht werden, wobei etwa dem Presserat und einem vergleichbaren Organ für den Filmbereich ein Vorschlagsrecht eingeräumt werden könnte. Aus Gründen der Akzeptanz in der Bevölkerung denke ich hierbei an einen externen Datenschutzbeauftragten, dessen Bedeutung etwa dadurch hervorgehoben werden könnte, daß er durch den Bundespräsidenten ernannt wird.
- Das Auskunftsrecht des Bürgers (vgl. §§ 26 und 34 BDSG) sollte in Anlehnung an § 13 BDSG und Art. 8 Abs. 3 BayDSG so ausgestaltet werden, daß grundsätzlich schon im Recherchestadium, jedoch hierbei abhängig von der Einstellung von Daten in eine Datensammlung, ein Auskunftsanspruch gegeben wird. Dieser sollte allerdings entfallen, wenn sich bei einer Abwägung herausstellt, daß die Auskunft an den Bürger die Erfüllung der Aufträge der Medienorgane gefährden würde. Das Vorliegen dieser Voraussetzungen könnte der oben vorgeschlagene Datenschutzbeauftragte bei Überprüfungen feststellen. Denkbar wäre aber auch als eine Art Minimallösung, den Anwendungsbereich der Datenschutzvorschriften nur auf die in zentralen oder dezentralen Archiven gespeicherten Informationen zu erstrecken.

  Ein Auskunftsrecht erst nach einer Verletzung des Persönlichkeitsrechts, wie es derzeit diskutiert wird, scheint mir demgegenüber nicht ausreichend, weil es den

Zweck, den Persönlichkeitsschutz nach vorne zu verlagern, nur unvollkommen erfüllt.

Weiterhin sollte darüber nachgedacht werden, in welchem Umfang Benachrichtigungs-, Berichtigungs- und Löschungsansprüche vorgesehen werden können.

- Vorbild einer Datenschutzregelung im Medienbereich könnten die einschlägigen Normen des Btx-Staatsvertrages werden. Dort wurde der Datenschutz aufgrund der bei Bildschirmtext (Btx) bestehenden besonderen Gefahren besser als im BDSG ausgestaltet. Ansprüche der Btx-Teilnehmer auf Auskunft, Berichtigung und Löschung sind in Art. 9 Abs. 7 Btx-Staatsvertrag besonders vorgesehen.

Meine im 9. Tätigkeitsbericht erhobene Forderung nach Schließung der Datenschutzlücke im Medienbereich ist bei den betroffenen Medien – wie nicht anders zu erwarten – nicht gerade mit Begeisterung aufgenommen worden. In diesem Zusammenhang sei aber darauf hingewiesen, daß einzelne Länderrundfunkgesetze, etwa das Gesetz über den Westdeutschen Rundfunk, bereits wesentlich verbesserte Datenschutzregelungen enthalten. Auch der Gesetzentwurf SPD-geführter Länder für ein neues Bundesdatenschutzgesetz schränkt das Medienprivileg zugunsten des Persönlichkeitsschutzes der Bürger ein.

Der Datenschutz der Bürger verdankt seinen hohen Rang in der Werteskala der öffentlichen Meinung nicht zuletzt dem engagierten Eintreten der Medien für dieses Bürgerrecht. Es könnte der Glaubwürdigkeit dieses Engagements nur förderlich sein, wenn sie, die Medien, den Persönlichkeitsschutz der Bürger auch im eigenen Bereich für sich selbst voll und ganz anerkennen und meine Vorschläge unterstützen würden.

19.2. Prüfung der Bayerischen Landeszentrale für Neue Medien

Im Berichtszeitraum habe ich eine erste datenschutzrechtliche Prüfung bei der Bayerischen Landeszentrale für Neue Medien (BLM) durchgeführt. Hierbei kam ich zu folgenden Ergebnissen:

Die BLM speichert keine Daten von Teilnehmern, es sei denn diese sind gleichzeitig Betreiber einer Individual-Satelliten-Empfangsanlage (zur datenschutzrechtlichen Problematik vgl. 19.3.). Die von mir überprüfte Adreßdatei von Medien- und Verwaltungsratsmitgliedern ist datenschutzrechtlich unbedenklich. Die BLM hat insoweit nur noch festzulegen, wann auf die Speicherung von Daten ausgeschiedener Medien- und Verwaltungsratsmitglieder verzichtet werden kann und entsprechende Löschungsfristen vorzusehen. Auch die Datei „Abrechnung der Aufwandsentschädigungen für Medien- und Verwaltungsräte" begegnet keinen Bedenken.

Gegen die Datenverarbeitung im Rahmen des Medienförderungsprogramms bestehen ebensowenig Bedenken wie gegen die Verarbeitung von Kabelgesellschaftsdaten. Bezüglich der Kabelgesellschaften hat die BLM zahlreiche Aufgaben, wozu sie umfangreiche Angaben benötigt.

Eine abschließende Bewertung der Einhaltung des Datenschutzes bei der BLM konnte ich jedoch nicht vornehmen. Zum Prüfungszeitpunkt war bei der BLM noch nicht endgültig geklärt, welche Karteien und automatisierten Dateien bestehen. Die Landeszentrale hatte zwar vor der Prüfung zu zahlreichen Karteien Material übersandt, die Prüfung vor Ort hatte jedoch ergeben, daß möglicherweise darüber hinausgehend Daten erfaßt werden. Vertreter der BLM erklärten, daß „erfaßt" würde, welche Stelle die Mitglieder des Medienrates benennt, und zu welcher Wahlgruppe im Sinne des Art. 13 Abs. 2 MEG die Mitglieder des Verwaltungsrates gehörten. Die Frage, in welcher Datei und in welcher Abteilung dies erfolge, blieb zunächst offen. Auch die Überprüfung der automatisierten Dateien konnte wegen organisatorischer Probleme der BLM nicht abgeschlossen werden. Es war im Prüftermin nicht möglich, sich einen Überblick über die mit Hilfe des „CADMUS"-Rechners geführten Dateien und die gespeicherten Daten zu verschaffen. Dies gilt sowohl für das Datenbanksystem als auch für das Schreibsystem (Daten der Anbieter, Medien- und Verwaltungsräte).

Zwar mag es für die BLM schwierig gewesen sein, eine vollständige Erfassung aller Dateien vorzunehmen, da ihre sieben Abteilungen nach den Erfahrungen der Prüfer weitgehend selbständig arbeiten. Doch konnte die damalige Situation, in welcher die BLM nicht vollständig übersehen konnte, welche Daten wo in ihrem Zuständigkeitsbereich verarbeitet wurden, nicht hingenommen werden. Wer keinen Überblick über seine Datenverarbeitung hat, ist auch nicht in der Lage, eine sachgerechte Einhaltung des Datenschutzes zu gewährleisten. Dies habe ich gerügt. Allerdings darf hierbei nicht vergessen werden, daß sich die BLM in einer stürmischen Aufbauphase befindet.

Die BLM wurde daher gebeten, noch ausstehende Unterlagen umgehend an meine Geschäftsstelle zu übersenden, was auch geschah. Nach Durchsicht und Auswertung des umfangreichen Materials wird eine weitere Prüfung der Landeszentrale stattfinden.

19.3. Satelliten-Empfangsanlagen

Im letzten Tätigkeitsbericht hatte ich mitgeteilt, daß die BLM regelmäßig die zuständige Kabelgesellschaft über den Betrieb von privaten Individual-Satelliten-Empfangsanlagen in Kenntnis setzt, die ausschließlich dem eigenen Rundfunkempfang dienen. Auf meine Intervention hin hatte die BLM erklärt, auf solche Datenübermittlungen an Kabelgesellschaften wegen fehlender Rechtsgrundlage zu verzichten.

Das gleiche Problem stellt sich auch im Verhältnis Deutsche Bundespost zur BLM. Nach Art. 35 Medienerprobungs- und -entwicklungsgesetz (MEG) ist die BLM Genehmigungsbehörde von Satellitenempfangsanlagen, die Rundfunkprogramme an mindestens 100 angeschlossene Wohneinheiten weiterverbreiten. Insoweit muß die Landeszentrale von der Deutschen Bundespost die Daten der Anlagebetreiber erhalten.

Vertretbar erscheint weiterhin die Rechtsauffassung, daß bei einer Weiterverbreitung an weniger als 100, d. h. an 2 – 99 Betreiber, zwar keine Genehmigung, aber eine Unbedenklichkeitsbescheinigung zu erteilen ist. Auch insoweit kann eine Rechtsgrundlage noch im MEG gesehen werden, auch wenn eine ausdrückliche Klarstellung wünschenswert erschiene.

Von einer Weiterverbreitung kann jedoch nicht die Rede sein bei einer Individual-Satelliten-Empfangsanlage. Das habe ich

eingehend mit der BLM erörtert. Diese stellt sich jedoch auf den Standpunkt, daß auch insoweit eine Unbedenklichkeitsbescheinigung zu erteilen sei, da sie sonst nicht kontrollieren könne, ob eine Weiterverbreitung stattfindet.

Ich habe die Speicherung dieser Daten bei der BLM beanstandet.

19.4. Telekommunikation und Postreform

Aktuelle Probleme des Datenschutzes in der Telekommunikation

Mit Inkrafttreten der Telekommunikationsordnung am 1. Januar 1988 hat die Deutsche Bundespost den Übergang von bisher getrennten Fernmeldenetzen zu einem einzigen, diensteintegrierten digitalen Telekommunikationsnetz für die Übermittlung aller Nachrichtenarten eingeleitet; künftig fallen an zentralen Stellen erheblich mehr und leichter auswertbare personenbezogene Daten an als bisher, die je nach Dienstart mehr oder weniger präzise Rückschlüsse auf das Verhalten der Teilnehmer erlauben. In der Telekommunikationsordnung wurden die Empfehlungen der Konferenz der Datenschutzbeauftragten des Bundes und der Länder zur Verbesserung des Datenschutzes und zur Beherrschung der möglichen Risiken bisher nur zum Teil übernommen.

Auch das Bundesdatenschutzgesetz kann mit seinen allgemeinen Vorschriften die Risiken nicht auffangen; dies gilt auch für die bisher bekanntgewordenen Novellierungsentwürfe. Hier bedarf es weiterer spezieller Regelungen. Bei der Novellierung des Bundesdatenschutzgesetzes muß vor allem sichergestellt werden, daß sämtliche beim Einsatz neuer Telekommunikationstechniken und -dienste anfallenden Daten in den Geltungsbereich des Gesetzes fallen. Deshalb muß z. B. selbstverständlich sein, daß alle personenbezogenen Daten aus der Bild-, Sprach-, Text- und Datenübertragung geschützt werden. Die Regelung der Zulässigkeit der Verarbeitung personenbezogener Daten, deren Kontrolle und die erforderlichen technisch-organisatorischen Maßnahmen müssen an die neuen technischen Gegebenheiten angepaßt werden.

Das Grünbuch der Europäischen Gemeinschaften über die Entwicklung des gemeinsamen Marktes für Telekommunikationsdienstleistungen und Telekommunikationsgeräte zeigt, daß der Datenschutz bei der geplanten europaweiten Liberalisierung des Angebots von Dienstleistungen und Geräten nur unzureichend berücksichtigt wird. Das nationale Datenschutzrecht darf nicht durch ein Gemeinschaftsrecht überlagert werden, das im Ergebnis zu weniger Datenschutz führt als das nationale Recht. Die frühzeitige Einbindung des Datenschutzes in die jetzt folgenden Beratungen – auch auf EG-Ebene – ist daher dringend erforderlich.

Die Länder sind im Rahmen ihrer Zuständigkeit zum Erlaß von Regelungen zur Nutzung der Telekommunikation verpflichtet, auch die notwendigen Datenschutzvorschriften zu erlassen. Der Bildschirmtext-Staatsvertrag kann hierzu als Vorbild dienen. In einem derartigen Staatsvertrag müssen auch die materiellen Voraussetzungen zum Betrieb privater Telekommunikationsdienste und deren Zulassung geregelt werden.

Sicherstellung des Datenschutzes bei der Poststrukturreform

Die Bundesregierung hat dem Parlament den Entwurf eines Poststrukturgesetzes vorgelegt, in dem eine teilweise Privatisierung des Fernmeldewesens vorgesehen ist. Der Entwurf sieht für die künftigen privaten Telekommunikationsanbieter weniger strenge Datenschutzregelungen vor als im Bereich der Bundespost.

Das Poststrukturgesetz muß deshalb über die bisherigen Regelungen hinaus sicherstellen, daß auch in den Bereichen, in denen Endeinrichtungen durch Private betrieben oder sonstige Netzfunktionen durch Private wahrgenommen werden, ebenso strenge Datenschutzregelungen gelten, wie sie im Bereich der Bundespost notwendig sind.

Hierzu reicht die vorgesehene Verordnungsermächtigung, die die Bundesregierung nicht ausreichend zum Tätigwerden verpflichtet, nicht aus. Außerdem könnte der Datenschutz durch private Geschäftsbedingungen unterlaufen werden. Notwendig ist eine abschließende gesetzliche Regelung, die den Umfang der Daten auf das erforderliche Maß beschränkt, eine strenge Zweckbindung vorsieht und für den Bürger die Datenflüsse offenlegt. Dies gilt auch für personenbezogene Daten, die beim Betrieb privater Telekommunikationsdienstleistungen (§ 1 Abs. 4 Entwurf Fernmeldeanlagengesetz) anfallen. Solche Dienstleistungen dürfen nur zugelassen werden, wenn sie den gesetzlichen Anforderungen entsprechen.

Die gesetzliche Regelung sollte von den Unternehmen der Deutschen Bundespost und von den privaten Unternehmen auch verlangen, daß diese technische und organisatorische Maßnahmen durchführen, um eine datenschutzgerechte und sichere Telekommunikation zu gewährleisten. Schließlich muß auch für die privaten Telekommunikationsanbieter eine angemessene Kontrolle vorgesehen werden.

Die Konferenz der Datenschutzbeauftragten hat am 10.10.1988 in Mainz Beschlüsse zu Fragen der Telekommunikation und der Poststrukturreform verabschiedet.

Teilnahme an einer Veranstaltung zu Fragen der Telekommunikation

Am 29.9.1988 fand eine Anhörung der SPD-Landtagsfraktion zum Thema „Neuordnung der Telekommunikation – Wo bleibt der Datenschutz?" im Landtag mit Vertretern der Bundespost und der Firma Siemens statt, an der auch ich teilnahm. Als Fazit dieser Anhörung kann aus meiner Sicht festgehalten werden, daß die inzwischen erlassenen Datenschutzregelungen für die bereits angebotenen Telekommunikationsdienste Anregungen der Datenschutzbeauftragten zu einem beträchtlichen Teil berücksichtigt haben. Die noch offenen Forderungen habe ich oben dargestellt.

20. Gentechnologie und Datenschutz

Die biologisch-medizinischen Möglichkeiten der Genomanalyse eröffnen bisher ungeahnte Einblicke in die Tiefen der menschlichen Persönlichkeit und rufen so zwangsläufig den Datenschutz auf den Plan.

In umfassender Weise hat sich eine vom Deutschen Bundestag eingesetzte Enquete-Kommission mit den „Chancen und Risiken der Gentechnologie" befaßt. Deren

Bericht vom 6.1.1987 gibt wieder, in welchen Lebensbereichen der Genomanalyse Bedeutung zukommen wird. Da von einer sich beschleunigenden Entwicklung der Ergebnisse in der gentechnischen Forschung auszugehen ist, müssen möglichst bald zumindest Anhaltspunkte dafür erarbeitet werden, wie datenschutzrechtliche Probleme gelöst werden könnten. Insbesondere muß die unberechtigte Offenlegung der inneren Struktur eines Menschen verhindert werden.

Die Datenschutzbeauftragten der Länder und des Bundes haben sich in Arbeitskreisen mit datenschutzrechtlichen Fragen befaßt, stehen aber erst am Anfang konkreter Überlegungen. Die Schwierigkeit liegt vor allem darin, daß gegenwärtig noch große Unsicherheit über die tatsächlichen technischen Möglichkeiten der Genomanalyse herrscht. Aus datenschutzrechtlicher Sicht ergeben sich aus dem Bericht der Enquete-Kommission folgende Schwerpunkte:

Genetische Beratung und pränatale Diagnostik

Ziel der genetischen Beratung und vorgeburtlichen Diagnostik ist die Feststellung bestimmter Schäden oder innerhalb einer Gruppe (z.B. innerhalb einer Familie) bestehender späterer Erkrankungsmöglichkeiten auf Grund vererbbarer genetischer Merkmale. Wenn sich Eltern freiwillig der genetischen Beratung oder Untersuchung unterziehen, ist sicherzustellen, daß die gewonnenen Daten ausschließlich den von den Eltern eingeschalteten Beratungsstellen oder Ärzten zur Verfügung stehen.

„Neugeborenen-Screening"

Darunter versteht man Suchtests oder Reihenuntersuchungen auf genetische Merkmale von Mitgliedern einer Gruppe oder auch aller neugeborenen Kinder, selbst wenn keine Erscheinungen von Krankheitssymptomen vorhanden sind.

Sobald derartige Erkenntnisse nicht mehr anonymisiert, sondern personenbezogen gewonnen werden, könnten sie sich für den späteren Erwachsenen nachteilig auswirken, wenn es z.B. um die Eignung zu bestimmten Tätigkeiten oder für den Zugang zu bestimmten Berufsgruppen geht. Eine Sammlung personenbezogener genetischer Daten in öffentlichen Registern oder Dateien ist abzulehnen.

Genomanalyse für Versicherungen

Für Versicherungen könnte die Genomanalyse bei der Abwägung von Risiken im Rahmen eines bestehenden oder künftigen Versicherungsverhältnisses von großem Interesse sein. In erster Linie dürfte das für privatwirtschaftliche Versicherungen (z.B. Lebensversicherung) gelten. Negative Erkenntnisse dürften in der Regel zur Verweigerung des vom Betroffenen angestrebten Versicherungsverhältnisses, zumindest zu höheren Prämien führen. Ob und wieweit die Nutzung der Genomanalyse privaten Versicherungsunternehmen erlaubt sein sollte, muß deshalb eingehend geprüft werden.

Bei der gesetzlichen Sozialversicherung hat die Genomanalyse wohl keine Bedeutung, da die Sozialversicherungsträger nach den Bestimmungen der §§ 165 ff RVO die Mitgliedschaft einer Person nicht ablehnen können. Ihr Beginn richtet sich nach der Erfüllung der gesetzlich vorgesehenen Voraussetzungen. Gesundheitliche Risiken spielen hierbei keine Rolle.

Genomanalyse an Arbeitnehmern

Genetische Daten könnten bei den einzelnen Arbeitnehmern zur Prüfung von Arbeitplatzrisiken herangezogen werden. Zunächst muß noch geklärt werden, welche genetische Eigenschaften im Einzelfall bei der Besetzung eines bestimmten Arbeitsplatzes von Bedeutung sein können. Die Auswirkungen solcher Gen-Tests auf die freie Selbstbestimmung des einzelnen müssen sehr ernst genommen werden.

Dagegen dürfte aus jetziger Sicht der Einsatz der Genomanalyse im Rahmen von Vorsorgeuntersuchungen durch die gesetzliche Unfallversicherung zur Verhütung von Unfällen und Berufskrankheiten differenzierter zu bewerten sein. Dies dürfte letztlich auch für die Einschätzung der Risiken gelten, die beispielsweise für die bei biotechnologischen Produktionsverfahren eingesetzten Arbeitnehmer durch den Umgang mit gentechnisch veränderten Organismen entstehen können.

Genomanalyse im Strafverfahren (genetischer Fingerabdruck)

Schon jetzt ermöglicht ein vor allem in England angewandtes Verfahren neue Möglichkeiten zur Täteridentifizierung und Feststellung der Abstammung in der gerichtlichen und kriminalistischen Praxis. Durch Vergleich von am Tatort zurückgelassenen Körperzellen (Haut, Haare, Samen), aus denen ein sog. genetischer Fingerabdruck abgeleitet werden kann, mit Körperzellen eines Tatverdächtigen wird die Täterermittlung wesentlich erleichtert. Mit dem Staatsministerium der Justiz habe ich gegen die Nutzung des genetischen Fingerabdrucks im Strafverfahren keine rechtlichen Einwände. Nach § 81 a StPO wird die Entnahme einer Blutprobe bei einem Beschuldigten zur Feststellung von Tatsachen, die für das Verfahren von Bedeutung sind, als zulässig angesehen. Deshalb bestehen keine Bedenken gegen den Vergleich der in einer Blutprobe enthaltenen Zellen mit anderen Zellen. § 81a StPO läßt überdies Blutentnahmen nur zu streng verfahrensbezogenen Zwekken zu, die im konkreten Fall einer richterlichen Anordnung bedürfen. Gleiches wird für die Entnahme von Blutproben bei anderen Personen als Beschuldigten zum Zwecke eines Zellvergleichs gelten (§ 81 c Abs. 2 StPO), wenn die dort genannten engen Voraussetzungen vorliegen.

In Übereinstimmung mit der Enquete-Kommission sieht das Justizministerium Verfahren als unbedenklich an, die lediglich auf die Identifizierung des Täters gerichtet sind. Die Feststellung von Persönlichkeitsmerkmalen des Beschuldigten wird in absehbarer Zeit nicht für möglich gehalten. Nur wenn durch eine Genomanalyse im Strafverfahren über die Identifizierung hinaus Einblicke in die Persönlichkeit gewonnen werden, stellt sich die Frage nach einer erweiterten gesetzlichen Regelung.

21. Technischer und organisatorischer Bereich

21.1. Technische Grundsatzfragen

21.1.1. Fortentwicklung der Datensicherung

Der Datensicherheit kommt wachsende Bedeutung zu, wo zentrale Großrechner (Host-Rechner) miteinander kommunizieren, intelligente Datenstationen oder Arbeitsplatzcomputer an Großrechnersysteme angeschlossen sind, Arbeitsplatzsysteme zu Netzen zusammengeschlossen werden,

wobei manche wiederum einen Zugang zu Host-Rechner haben können, und Arbeitsplatzcomputer Büroaufgaben übernehmen oder in ein Bürokommunikationssystem eingebettet sind. In der modernen Informationsverarbeitung wird diese Datensicherheit durch technische und organisatorische Maßnahmen zur Datensicherung erreicht.

Als erste sind die Hersteller von Datenverarbeitungsanlagen aufgerufen, dem Anwender „sichere und vertrauenswürdige Systeme" anzubieten. Bei komplexen DV-Systemen ist diese Forderung allerdings nicht kurzfristig erfüllbar.

Solche Systeme sollen folgende Eigenschaften erfüllen:

Zugangssicherung

Meldet sich ein Benutzer an einer Datensichtstation oder an einem vernetzten Personal Computer an, so hat das jeweilige System zu prüfen, ob der Benutzer überhaupt über eine Zugangsberechtigung zu diesem System verfügt und inwieweit ihm der Zugriff auf die angeforderten Ressourcen eröffnet werden kann. Dem Identifikationsprozeß, Eingabe der Benutzerkennung und des persönlichen Kennwortes (Paßwort), muß eine Authentifizierung folgen. Unter Authentifizierung versteht man hier die maschinelle Überprüfung der Identität eines Benutzers durch das DV-System. Nur so ist der Zugriffsschutz in einem komplexen Kommunikationssystem gewährleistet.

Programmintegrität

Die Datenverarbeitung auf dezentralen Arbeitsplatzcomputern (Individuelle Datenverarbeitung IDV) ist nur dann ordnungsgemäß, wenn sichergestellt ist, daß die verbindlich vorgegebene Verarbeitungslogik nicht unbemerkt verändert oder ganz ausgeschlossen werden kann. Es muß außerdem erkennbar sein, daß ausschließlich die ordnungsgemäß freigegebene Programmversion zur Ausführung kommt. Diese Forderung gewinnt durch das Phänomen der Computer- bzw. Programm-Viren und wegen der zunehmenden Verarbeitung auf vernetzten Arbeitsplatzcomputern zusehends an Bedeutung.

Übertragungssicherheit

In der Datenkommunikation ist es weiter von großer Bedeutung, daß auf Leitungen übertragene Informationen nicht unbemerkt verfälscht oder von Lauschern interpretiert werden können. Gerade die unverschlüsselte Übertragung von sicherheitsrelevanten Daten wie Benutzerkennung und Paßwort, bedeutet für die Datensicherheit in der Datenfernverarbeitung eine empfindliche Schwachstelle.

Revision

In Computernetzen, in denen viele Benutzer arbeiten können, ist die Dokumentation der Ablaufinformationen eine wesentliche Komponente für die Sicherstellung der Revision in der maschinellen Datenverarbeitung.

Dazu ist es notwendig, daß die DV-Systeme, Host-Systeme wie Sub-Systeme, signifikante Ablaufdaten darüber aufzeichnen, wer, wann, mit welchen Mitteln auf welche Dateien zugegriffen hat. Außerdem muß ein Netzwerk über Kontrolleinrichtungen verfügen, die Manipulationen erkennen und abweisen, etwa den Anschluß eines im System nicht zugelassenen Gerätes.

Weiter ist es notwendig, daß auch die Benutzerberechtigungen revisionsfähig dokumentiert werden. Dies läßt sich beispielsweise durch eine Schnittstelle zu einem Data-Dictionary erreichen, in dem Informationen darüber abgelegt werden, wer zu welcher Zeit über welche Zugriffsberechtigungen verfügte oder noch verfügt.

Schließlich sind sowohl auf dem Host-System als auch in der Individuellen Datenverarbeitung Berichtsprogramme, sogenannte AUDIT-Programme, zur Verfügung zu stellen, mit denen die Ablaufdaten problemlos und aussagefähig ausgewertet werden können.

Bürosysteme

Die oben beschriebenen Datensicherheitsmaßnahmen müssen selbstverständlich auch in der Bürokommunikation zur Verfügung stehen. So muß beispielsweise sichergestellt sein, daß die Ressourcen und Benutzerrechte revisionsfähig dokumentiert, ein elektronisch geführtes Archiv nicht unkontrolliert verändert werden kann und die Ablaufdaten in entsprechenden Journalen abgelegt werden.

Gerade beim Einsatz von Bürosystemen muß die Revision feststellen können, wer welche Änderungen an einem Dokument durchgeführt hat. Darüber hinaus ist durch geeignete Maßnahmen sicherzustellen, daß nur ganz bestimmte Benutzer besondere Privilegien erhalten wie etwa die Abfrage bei Bildschirmtext, die Benutzung des Teletex oder den Zugang zu anderen kostenpflichtigen Kommunikationsdiensten. Schließlich muß revisionsfähig festgehalten werden, wann ein Dokument versandt oder empfangen wurde.

Daß die Hersteller auf dem Wege sind, diesen unverzichtbaren Anforderungen der Datensicherheit gerecht zu werden, zeigten Gespräche meiner Mitarbeiter mit Vertretern verschiedener Hersteller.

Auch die Strategiegespräche der Benutzervereinigung SAVE (Siemens-Anwenderverein) mit dem Hersteller bestätigen diese erfreuliche Entwicklung. Den Anforderungen des Datenschutzes und der Datensicherheit soll nach den Aussagen dieses Herstellers durch folgende Entwicklungsziele Rechnung getragen werden:

- Einen wesentlichen Beitrag zur Datensicherheit, insbesondere zur Zugangssicherung, leisten kryptographische Verfahren und Chip-Karte. Durch Kombination von Chip-Karte und Verschlüsselungstechnik läßt sich die Sicherheit der Datenverarbeitung, etwa der Schutz vor Programm-Viren, weiter erhöhen, da die Chip-Karte zur Identifikation und Authentifizierung eines Benutzers gegenüber dem System und gleichzeitig zur Verschlüsselung von Nachrichten und sonstigen Informationen dient. Durch eine sogenannte „elektronische Unterschrift" lassen sich Nachrichten, Texte, Daten und Programme gegen Manipulationen in dieser Weise schützen, daß systemseitig geprüft wird, ob die aus dem Ursprungstext durch ein spezielles DV-Verfahren gebildete „elektronische Unterschrift" zur empfangenen Nachricht oder zum gespeicherten Text paßt (Authentifikation). Ist das nicht der Fall, liegt eine Manipulation vor; das System verarbeitet die Nachricht nicht oder führt das so überprüfte Programm nicht aus. Auf diese Weise werden auch von Viren befallende Programme entdeckt und die Ausbreitung des Virus dadurch unterbunden.

Diese Sicherheitskomponente dürfte schon in wenigen Jahren allgemein verfügbar sein.
- Die Forderung, daß DV-Programme nicht unkontrolliert veränderbar sein dürfen, läßt sich über die sogenannte „Versiegelung" der Programme erreichen. Wie diese Verfahren in der Praxis aussehen werden, steht im einzelnen noch nicht fest. Die Hersteller diskutieren die Lösungsmöglichkeiten u.a. auch mit der Zentralstelle für Chiffrierwesen in Köln.
- Wirkungsvolle Hilfsmittel zur Revision der Datenverarbeitung sollen in einer der nächsten Betriebssystemversionen ebenfalls in wenigen Jahren verfügbar sein.
- Die Dokumentation der Benutzerrechte wird vom Hersteller unterstützt, sobald ein Dictionary-System mit Schnittstellen zum Betriebssystem verfügbar ist. Bis dahin hat sich der Anwender mit Eigenlösungen zu behelfen, die allerdings wegen der fehlenden Einbettung im Betriebssystem manipulierbar sind.

Beispielsweise soll die nächste Version des Betriebssystems eines Großherstellers, die 1990 freigegeben wird, mindestens die Sicherheitsklasse C 1 erreichen. Grundlage dieses Sicherheitsstandards ist die DoD-Klassifizierung (United States Department of Defense) für vertrauenswürdige Computersysteme, kurz „Orange Book" genannt. Andere Hersteller planen ähnliche Sicherheitsstandards. Manche Hersteller können diese Sicherheit bereits heute schon in ihren Betriebssystemen anbieten.

Die Sicherheitsklasse C 1 ist im wesentlichen durch die Abschottung der Benutzer und durch das Schreiben signifikanter Ablaufdaten gekennzeichnet.

Weniger hoffnungsvoll ist die Lage bei den Bürosystemen. Die geforderten Sicherheitskomponenten sind nur fragmentarisch vorhanden, so daß sich der Anwender weitgehend organisatorischer Maßnahmen bedienen muß.

Daß die Entwicklung von Sicherheitskomponenten oft so schleppend vorankommt, hat seinen Grund nicht zuletzt auch darin, daß nicht selten die bereits heute vom Hersteller angebotenen Sicherheitseinrichtungen vom Anwender nicht genützt werden. Die Hersteller sind aber für die Weiterentwicklung der Sicherheitsstandards nur dann zu motivieren, wenn die Anwender die bereits heute verfügbaren Sicherheitskomponenten einsetzen.

21.1.2. Sicherheit bei der Datenkommunikation

Immer wieder wird darüber berichtet, daß es Hackern und Crackern gelungen sei, in Rechnernetze einzudringen und dort zunächst unbemerkt an geheime Informationen gelangt seien. Während ein Hacker sich nur umsieht, verändert ein Cracker Daten und Programme und verursacht Schaden für den Betroffenen wie für den Hersteller von DV-Systemen und systemnaher Software. Erst kürzlich drang ein Hacker, der jedoch über Insider-Wissen verfügte, in ein Rechnernetz ein und legte einige Rechnersysteme lahm. Die pressewirksame Publikation dieses Falles hat bei dem Hersteller und bei den Anwendern beträchtliche Sorge ausgelöst.

Die zum Eindringen in fremde Rechnernetze notwendige technische Ausrüstung, in der Regel ein Home Computer (Personal Computer) und ein Akustikkoppler, ist im Fachhandel zu einem erschwinglichen Preis zu erhalten.

Die Anwender in der öffentlichen bayerischen Verwaltung blieben bisher von solchen Eindringlingen verschont. Das liegt wohl überwiegend in der Tatsache begründet, daß die Datenkommunikation meist in geschlossenen Netzen erfolgt. Im Gegensatz hierzu weisen die offenen Netze, zu denen man über Telefonwählleitungen Systemzugang erhält, mitunter große Sicherheitsprobleme auf. Zur Vermeidung dieser Risiken bedienen sich die öffentlichen Stellen im Freistaat Bayern überwiegend der festen Punkt-zu-Punkt-Verbindung, der sogenannten Standleitung, auch HfD-Verbindung bezeichnet (HfD = Hauptanschluß für Direktrufverbindung).

Werden jedoch aus Kostenersparnisgründen im Einzelfall Wählleitungen eingesetzt, so wird ein Eindringling in der Regel an den umfangreichen Anmeldeprozeduren, den Verständigungsprotokollen sowie an den verfahrensspezifischen Prüfungen scheitern. Üblicherweise tauschen die Rechner beim Aufbau der Verbindung Kennsatzinformationen aus, die auch unveränderliche Hardwaredaten beinhalten und Bestandteil der sogenannten „Shake-hand-Prozedur" sind. Selbstverständlich werden außerdem Benutzerkennung und persönliches Kennwort zur Berechtigungsprüfung herangezogen. Schließlich lassen umfangreiche Protokollierungen aller Verbindungsinformationen, die bei der Datenkommunikation anfallen, Risiken, die nie völlig auszuschließen sind, frühzeitig erkennen und eröffnen somit die Möglichkeit eines präventiven Vorgehens.

Obwohl der Auswahl eines sicheren Systems und der Verwendung eines ebenso sicheren Netzes nach den bereits oben (Ziffer 21.1.1) beschriebenen Kriterien des „Orange Book" eine grundlegende Bedeutung beizumessen ist, müssen insbesondere die verfügbaren Sicherheitskomponenten in noch stärkerem Maße genutzt werden. So gehören Berechtigungsprüfungen beim Systemzugang mit ihren Identifikations- und Authentifizierungsverfahren (User-ID mit Paßwort, Chip-Karte mit elektronischer Unterschrift) ebenso zum üblichen Sicherheitsstandard wie die permanente Kontrolle der Systemnutzung selbst. Zum Nachweis eines Nachrichtentransfers muß der Empfänger der Nachricht einen Sendenachweis und der Sender einen Empfangsnachweis erhalten. Der Schutz der Datenintegrität auf der Wegstrecke vom Sender zum Empfänger kann zudem durch eine der vielen am Markt angebotenen Verschlüsselungsverfahren zusätzlich gesichert werden.

Mit der Einführung des diensteintegrierenden Netzes (ISDN) der Deutschen Bundespost auf breiter Basis zu Beginn der neunziger Jahre wird den Hackern der unerkannte Systemzugang zusätzlich erschwert werden. Die Anschlußkennung des Teilnehmers, der den Verbindungsaufbau anstrebt, wird ohne daß der Anwortende selbst Einfluß darauf nehmen kann, von der Vermittlungsstelle der Deutschen Bundespost dem Angewählten zur Verfügung gestellt und kann somit zur Authentifizierung des Partners herangezogen werden. Bereits während des sogenannten Mischbetriebs von analogen und digitalen Teilnehmerendgeräten ist die Deutsche Bundespost in der Lage, auch die Anschlußkennung des Teilnehmers zu übermitteln, der noch die analogen Fernsprecheinrichtungen nutzt. Bei der Einführung von ISDN bleiben zudem die Dienste Datex-L und Datex-P mit unverändertem Funktionsumfang und in der bisherigen Netzstruktur erhalten. Datex-L und Datex-P umfassen somit auch weiterhin umfangreiche Prüf- und Kontrollmechanismen. Außerdem steht zur Abgrenzung einer Benutzergruppe auch künftig die Möglichkeit der Definition einer „Geschlossenen Benutzergruppe GBG", die

nur den Verbindungsaufbau zwischen den in dieser Gruppe definierten Partnern zuläßt, zur Verfügung. ISDN wird deshalb einen wesentlichen Beitrag zur Datensicherheit leisten.

21.1.3. Personal Computer

Der Einsatz von Personal Computern oder Arbeitsplatzrechnern nimmt auch in der öffentlichen Verwaltung ständig zu. So ist beispielsweise geplant, alle bayerischen Polizeiinspektionen und -stationen mit Arbeitsplatzrechnern auszustatten. Ähnliche Bestrebungen sind im Forstbereich und in der Finanzbauverwaltung festzustellen, wo alle Dienststellen der unteren Verwaltungsebene Personal Computer für die Unterstützung ihrer Aufgaben erhalten sollen. Da, wie bereits in früheren Tätigkeitsberichten beschrieben, eine Reihe von Datensicherungsmaßnahmen bei Einsatz dieser kleinen Datenverarbeitungsanlagen nicht greifen, bereiten die Gewährleistung der Sicherheit und der Ordnungsmäßigkeit der Datenverarbeitung besondere Probleme. Im Hinblick auf diese Probleme gaben die Datenschutzbeauftragten des Bundes und der Länder auf der Konferenz am 10. Oktober 1988 Empfehlungen zur Datensicherheit bei Einsatz kleinerer Datenverarbeitungsanlagen. Der Wortlaut des Beschlusses ist im Anhang abgedruckt.

In dem Beschluß wird die Verantwortlichkeit der speichernden Stelle für die Datensicherheit hervorgehoben. Die speichernde Stelle hat bei der Verarbeitung personenbezogener Daten auf einem Personal Computer die technischen und organisatorischen Maßnahmen zu treffen, die eine der Sensibilität der Daten entsprechende Datensicherheit gewährleisten. Wird mit den verfügbaren Maßnahmen die Datensicherheit nicht in dem erforderlichen Umfang sichergestellt, ist auf den Einsatz solcher Geräte zu verzichten. Weiter werden die Hersteller von kleinen Datenverarbeitungsanlagen, insbesondere von Personal Computern, aufgefordert, Systeme bereitzustellen, die das erforderliche Maß an Datensicherheit gewährleisten. Die getroffenen Sicherheitsmaßnahmen sollen dem neuesten Stand der Technik entsprechen und sich an dem Sicherheitsstandard großer Datenverarbeitungsanlagen orientieren.

Mit der Überprüfung (Evaluierung) von PC-Sicherheitsprodukten hat die Zentralstelle für Chiffrierwesen (ZfCh), Abteilung für Computersicherheit (COMPUSEC), in Köln einen beachtlichen Beitrag zur Erhöhung der Datensicherheit von DV-Systemen geleistet. So gibt es heute bereits eine Reihe von Soft- und Hardwareprodukten, die von dieser Stelle untersucht und zertifiziert wurden.

Produkte, die wirksame Sicherheitsfunktionen auf Personal Computer des Industriestandards übertragen, müssen nach den Maßstäben der Zentralstelle mindestens folgende Eigenschaften garantieren:

- Einschränkung der Nutzung des DV-Systems durch einen Paßwort-Mechanismus auf die zugelassenen Benutzer
- Trennung der Dateien unterschiedlicher Benutzer
- Protokollierung aller abgelaufenen Aktivitäten
- Beschränkung des Systemmanagements auf einen privilegierten Benutzer
- Bereitstellung einer Pausenfunktion, die das DV-System gegen unberechtigen Zugriff mechanisch sperrt.

Wird auf einem PC ein Sicherheitsprodukt mit diesen Eigenschaften installiert, dann können auf diesem Gerät nach Ansicht der Zentralstelle auch vertrauliche Daten verarbeitet werden.

Nach meiner Auffassung ermöglicht eine derartige Ausrüstung auch den Einsatz des PC in der öffentlichen Verwaltung zur Verarbeitung personenbezogener Daten.

21.1.4. Bürokommunikation

Der Einsatz moderner Kommunikationssysteme im Büro gewinnt auch in der öffentlichen Verwaltung in zunehmendem Maße an Bedeutung. In vielen Büros bildet die vorhandene Zweidraht-Telefonleitung die Basis für das Transportnetz der Kommunikationsanlage, wobei das Telefonieren häufig den Einstieg in die ISDN-Technik darstellt. In dieser Technik sollen Sprache, Text und Daten auf einem Transportnetz übertragen werden.

Die heute bekannten und eingesetzten Kommunikationsanlagen stellen dedizierte Systeme dar, bei denen der Anwender die Leistungsmerkmale festlegt, d.h. welche Endgeräte welche Funktionen erhalten sollen. Die Kommunikationsanlage ist kein beliebig programmierbarer Universalrechner. Deshalb kann die auf der K-Anlage installierte Software als änderungssichere oder „versiegelte" Software bezeichnet werden.

Zu den bekannten Mißbrauchsmöglichkeiten ist festzustellen:

- Sofern man an das Übertragungsmedium herankommt, sind Mißbräuche möglich. Allerdings bietet ein Sternnetz, wie es das Telefonnetz darstellt, „mehr Schutz" gegen das Abhören als eine Ringleitung oder ein Busnetz, auf dem die Daten aller Teilnehmer transportiert werden. Im Sternnetz liegen Punkt zu Punkt ähnliche Verbindungen vor, auf denen immer nur die Daten der jeweiligen Endgeräte übertragen werden.
- Analoge Endgeräte, reine Sprachgeräte, sind nicht unkontrolliert anschließbar. Die Mithilfe des Netzadministrators ist hier auf alle Fälle notwendig, da dieser den mechanischen Anschluß am Hauptverteiler durchführen und die Teilnehmernummer freigeben muß. Ist ein Anschlußpunkt vorhanden, ist nur der Anschluß eines Endgerätes mit identischen Funktionen unbemerkt möglich. Bei digitalen Endgeräten erhöht die ISDN-Technik den Anschlußschutz, weil alle Endgeräte bei der Einrichtung des Systems (Systemgenerierung) definiert werden müssen. Eine Netzmanipulation wird dadurch wesentlich erschwert.
- In der Kommunikationszentrale ist der Zugriff auf die dort gespeicherten Netz- und Betriebsdaten mit Hilfe eines Paßwortes möglich. Ein abgeschlossener Betriebsraum für das sogenannte Betriebsterminal der Kommunikationszentrale bietet zusätzlichen Schutz.
- Eine mißbräuchliche Nutzung fremder Endgeräte kann durch den Zugriffsschutz mittels Paßwort-Mimik oder Chip-Karte weitgehend ausgeschaltet werden.
- Eine Abschirmung des Transportmediums gegen kompromittierende Abstrahlung ist bei der Verwendung der Kupferdrahtleitung kaum möglich. Beim Einsatz von Glasfaserkabeln ist dieses Problem jedoch zu vernachlässigen.
- Ansätze für die Revision ergeben sich aus dem von der Kommunikationsanlage geführten Logbuch. Die Revisionsfähigkeit der Benutzerrechte ist jedoch meist nicht gesichert.

21.2. Prüfungstätigkeit

21.2.1. Kontrolle und Beratung

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

- AOK-Rechenzentrum Oberpfalz
- Rechenzentrum des Bayer. Landesversorgungsamtes
- Rechenzentrum des Statistischen Landesamtes
- Rechenzentrum der Landwirtschaftlichen Sozialversicherungsträger Oberfranken-Mittelfranken
- Kommunale Datenzentrale Landshut der Anstalt für Kommunale Datenverarbeitung
- Rechenzentrum im Klinikum Ingolstadt
- Rechenzentrum der Universität Passau
- Rechenzentrum der Kreisfreien Stadt Kaufbeuren
- Landratsamt Erding
- Landratsamt Landsberg
- Landratsamt Passau
- Gemeinde Unterhaching (Landkreis München)
- Gemeinde Taufkirchen (Landkreis München)
- Gemeinde Zorneding (Landkreis Ebersberg).

Informationsbesuche fanden u. a. statt bei einem Finanzamt und bei drei Privatfirmen, die im Auftrag für öffentliche Stellen personenbezogene Daten verarbeiten. Das Finanzamt ist an die Datenverarbeitungsanlage des Zentralfinanzamtes München angeschlossen. Im Mittelpunkt des Interesses standen bei diesem Besuch die Festlegung und Verwaltung der Zugriffsberechtigungen für die Benutzer der Dialog-Verfahren. Bei den Privatfirmen handelte es sich um zwei Datenerfassungsbüros und einen Mikroverfilmungsbetrieb, der COM-Verfilmung durchführt.

Die Beratungen haben in erster Linie das Ziel, Verstöße gegen die Datenschutzgesetze zu verhindern. Darüber hinaus soll aber auch die Sicherheit der maschinellen Datenverarbeitung erhöht werden. Derartige Sicherheitsberatungen wurden bei 5 AOK-Rechenzentren und einer Landesversicherungsanstalt durchgeführt.

Die bayerischen Bezirksregierungen sollen bis Anfang der 90er Jahre mit DV-Anlagen ausgestattet sein. Im Berichtszeitraum wurden die Regierung der Oberpfalz und die Regierung von Niederbayern bei der Festlegung der Sicherungsmaßnahmen für ihre Rechenzentren beraten.

Schließlich wurden 7 Landratsämter, 3 Krankenhäuser, 3 Krankenkassen, 3 größere Gemeinden und 3 Bezirksverwaltungen bei Neubaumaßnahmen oder bei der Einrichtung elektronischer Datenverarbeitung sicherheitstechnisch beraten.

Die Kontakte zu den Herstellern sind für die Beurteilung der neuen DV-Techniken und für die Entwicklung von geeigneten Sicherheitsmaßnahmen sehr wichtig. Wie im Jahre 1987 wurde auch im Berichtszeitraum der Kontakt mit Hard- und Softwareherstellern weiter gepflegt.

21.2.2. Ergebnisse der Kontrolltätigkeit

Die Kontrollen ergaben, daß der Stand der technischen und organisatorischen Maßnahmen zur Datensicherung noch recht unterschiedlich ist. So wurden einerseits Datensicherungsmaßnahmen hoher Qualität angetroffen, andererseits waren bei manchen Stellen in Teilbereichen beachtliche Defizite festzustellen.

Da jede geprüfte Behörde einen umfangreichen Prüfungsbericht erhält, der auf alle Bereiche der maschinellen und manuellen Verarbeitung personenbezogener Daten eingeht und alle getroffenen bzw. noch zu treffenden Datensicherungsmaßnahmen ausführlich beschreibt, soll die oben getroffene Feststellung an dieser Stelle lediglich beispielhaft erläutert werden.

Bei manchen Stellen sind besonders positiv aufgefallen:
- die Installation ausgeklügelter Zugangskontroll- und Alarmsysteme;
- die vollständige Dokumentation von DV-Verfahren einschließlich aller Änderungsnachweise;
- Nachweise über alle auf einem DV-System abgelaufenen Aktivitäten;
- die Einrichtung von DV-Sicherheitsräumen;
- die Katastrophenvorsorge durch Erstellung von Notfallkonzepten und Wiederanlaufplänen bei einem Totalausfall der DV-Anlage;
- die Dokumentation revisionsfähiger Zugriffsberechtigungen.

Auf der anderen Seite wurden vereinzelt auch Mängel festgestellt, wie:
- hohe Brandlasten im Maschinensaal und Datenträgerarchiv;
- große Differenzen zwischen den von der Fachabteilung vorgegebenen und den in der DV-Anlage gespeicherten Zugriffsberechtigungen;
- mangelhafte Sicherung des Rechenzentrums und der Datenfernverarbeitungskomponenten;
- das Fehlen von Nachweisen, welche Aufgaben wann auf der DV-Anlage abgelaufen sind;
- das Fehlen von Dokumentationsunterlagen über bereits länger im Einsatz befindliche DV-Verfahren;
- unzureichende Entsorgung von Datenträgern mit personenbezogenen Daten;
- fehlende bzw. unzureichende Brandschutzmaßnahmen im Rechenzentrum.

Ein weiteres Problem, das häufig anzutreffen ist und deshalb an dieser Stelle etwas ausführlicher beschrieben wird, betrifft die Funktionsbereitschaft installierter Alarmanlagen in geschützten Bereichen, vor allem in Rechenzentren. Häufig verfügen Rechenzentren über umfangreiche Außen- und Innenraumsicherungen, die aber erst nach Beendigung der Spätschicht, manchmal erst gegen 22 Uhr, scharf geschaltet werden. In der Zeit vom allgemeinen Dienstschluß bis zum Ende der Spätschicht, in der sich nur noch wenige Personen im Gebäude, insbesondere in den manchmal weitläufigen Rechenzentren aufhalten, greifen diese Sicherheitsmaßnahmen nicht. Zum Schutz des Rechenzentrums und anderer geschützter Bereiche habe ich deshalb vorgeschlagen, eine Teilscharfschaltung der Alarmanlage für solche Bereiche einzuführen, die unbeaufsichtigt sind und zum geschützten Bereich gehören. Dabei ist es unerheblich, ob ein Alarm während dieser Zeit an das Bewachungsunternehmen oder an eine noch personell besetzte Stelle im Hause geleitet wird. Unverzichtbar ist allerdings die Alarmerkennung, das heißt, daß die den Alarm verfolgende Stelle Kenntnis darüber erhält, an welcher Stelle welcher Alarm ausgelöst wurde.

Weiter ist bei der Konzipierung von Alarmanlagen darauf zu achten, daß die Zeit, die zwischen Alarmgebung und dem Wirksamwerden von Gegenmaßnahmen vergeht, ausreicht,

einen Schadenseintritt weitgehend zu verhindern. Wichtige Objekte werden deshalb gegen Eindringungsversuche von außen durch unterschiedliche Alarmgeber gesichert. Ein Eindringling, der die erste Hürde überwunden hat, muß für die Überwindung der nächsten, vielleicht letzten Hürde so viel Zeit verwenden, daß er noch vor dem Überwinden dieser Hürde gefaßt wird.

Bei meinen Prüfungen bei Anwendern (Gemeinden, Landratsämter, Krankenhäuser), die DV-Systeme der Anstalt für kommunale Datenverarbeitung (AKDB) einsetzen, habe ich die Erfahrung gemacht, daß die Anwender nicht alle verfügbaren Maßnahmen zur Gewährleistung des Datenschutzes und der Datensicherung kannten. Beispielsweise wußten viele Anwender nicht, daß sie die persönlichen Kennwörter selbst ändern und vergeben und dadurch den Zugriffsschutz ganz wesentlich erhöhen können. Dasselbe gilt für die eigenständige Revision der Datenverarbeitung. Auf meine Anregung hat die AKDB ihre Kunden aufgefordert, sich über die möglichen Sicherheitsmaßnahmen zu unterrichten und die Mitarbeiter zu schulen.

21.3. Datensicherung durch Einsatz der Rückrufautomatik

Aus wirtschaftlichen Gründen machen die Behörden auch von der Datenübertragung im öffentlichen Fernsprechnetz, das jedermann zugänglich ist, Gebrauch. Wählleitungsanschlüsse befinden sich fast in jedem Rechenzentrum, sei es nur zur Fernwartung der DV-Anlage. Wählleitungen gelten aber, wie oben bereits (siehe 21.1.2.) gezeigt, als die Schwachstelle in der Datenfernverarbeitung und der Angriffspunkt für Hacker, weil der Angerufene meist keine Möglichkeit hat, den Anrufenden zu identifizieren. Deshalb muß sich der Anwender um zusätzliche technische Sicherungen bemühen.

Zur Sicherung der Wählleitungsanschlüsse wurde die sog. Rückrufautomatik entwickelt. Am Host-Rechner befindet sich dazu ein Sicherheitsmodul mit einem Speicher, in dem die Identifikationen und die dazugehörigen Telefonnummern aller Benutzer des Wählleitungsanschlusses abgespeichert sind. Wählt nun ein Teilnehmer über das öffentliche Fernsprechnetz ein mit Rückrufautomatik ausgestattetes DV-System an, wird er aufgefordert, zur Identifizierung seine persönliche, mit dem zentralen System vereinbarte Kennung anzugeben. Danach wird die Verbindung von der Zentrale gelöst und geprüft, ob der Anrufer eine gültige Zugangsberechtigung besitzt. Ist ein Zugang erlaubt, liest das System die Rufnummer des anrufenden Teilnehmers aus dem Speicher des Sicherheitsmoduls und wählt diesen von sich aus automatisch an. In diesem automatischen Rückruf soll die Sicherheit des Verfahrens liegen. Trotzdem enthält dieses Verfahren eine Schwachstelle:

In der Literatur wurde darauf hingewiesen, daß es ein „hacker software package" gibt, mit dem die Rückrufautomatik überlistet werden kann. Voraussetzung dafür ist allerdings, daß der Hacker über eine gültige Kennung mit Paßwort im angerufenen DV-System verfügt.

Es gibt jedoch eine Reihe von Sicherheitsmaßnahmen, die ein Überlisten der Rückrufautomatik wirksam unterbinden können. Den Anwendern der Rückrufautomatik stehe ich zur Beratung jederzeit zur Verfügung.

21.4. Automation des Rechenzentrumsbetriebs

Softwareprodukte und Sicherheitssysteme, die eine geplante und zugleich kontrollierte Nutzung eines Rechnersystems in allen Bereichen gewährleisten, gewinnen wegen der Komplexität der Aufgaben und Zusammenhänge in einem Großrechenzentrum zunehmend an Bedeutung. Die handvermittelte Steuerung von Produktionsaufträgen entspricht nicht mehr dem heute üblichen Stand der Technik. Außerdem entstehen in den komplexen Rechnersystemen eine Vielzahl von steuerungsrelevanten, den Rechenzentrumsablauf beeinflussenden Informationen, die einer unmittelbaren, eindeutigen und möglichst fehlerlosen Reaktion bedürfen. Deshalb sollte die Planung, Steuerung und Kontrolle des Betriebes eines Großrechenzentrums automatisierten Verfahren übertragen werden. Von einer solchen Maßnahme gewinnen nicht nur die für die Sicherheit des Rechenzentrums Verantwortlichen, sondern in einem erheblichen Maße auch diejenigen, die sich mit der Revision der Datenverarbeitung und der Überprüfung der Einhaltung des Datenschutzes befassen müssen.

Nahezu alle namhaften Hard- und Softwarehersteller haben diesen Trend erkannt und bieten inzwischen eine Vielzahl von Produkten und Organisationskonzepten an, die als sogenannte InformationsManagement-Software auf den Markt gekommen ist. Neben der Sicherheit steigern diese Produkte auch maßgeblich die Produktivität eines Rechenzentrums und gestatten zugleich die automationsgestützte Verwaltung nahezu aller Bereiche.

Wichtige Aufgabe eines Rechenzentrums ist die Schaffung eines automatisierten Betriebsablaufs mit den Funktionen des Betriebsablauf-Managements unter gleichzeitiger Berücksichtigung der Datensicherheit und der Revision. Nicht weniger bedeutungsvoll sind Systeme, die eine Betriebsablaufsteuerung gewährleisten, die die Netzwerk-, Änderungs- und Problemverwaltung unterstützen, die die ständig anwachsenden Kapazitätsanforderungen einplanen und überwachen sowie den DV-Service für alle Benutzer eines Rechenzentrums sicherstellen. Zur Steuerung des Betriebsablaufs und für die Planung, Vorbereitung und Durchführung von Batchaufgaben sowie zur Kontrolle der Online-Anwendungen unter optimaler Nutzung aller vorhandenen Ressourcen werden in erster Linie Produktions-, Planungs-, Steuerungs- und Kontrollprodukte angeboten. Diese Systeme sind betriebssystemabhängig. Sie werden bisher allerdings nur im Großrechnerbereich eingesetzt. Es überrascht, daß lediglich etwa ein Viertel aller deutschen Großrechenzentren solche Produkte einsetzt.

Eine derartige Software umfaßt im wesentlichen folgende Leistungen:

- Steuerung des Ablaufs aller Batchprogramme in einem Rechenzentrum anhand vorgegebener Ablaufparameter wie Terminvorgaben, früheste Start- bzw. Endezeit sowie Abhängigkeiten zwischen einzelnen Jobs und Datenbeständen
- Erstellung von Planungs- und Steuerungsunterlagen für das Rechenzentrum (Arbeitsvorbereitung, Arbeitsnachbereitung, Operating und RZ-Leitung) und alle beteiligten Fachbereiche in Form von vorab erstellten Terminplänen
- Sie unterstützt insbesondere die Tätigkeiten der Arbeitsvorbereitung und trägt so zur Verringerung der Fehler in diesem Bereich bei.

- Sie gestattet, Arbeitsabläufe effektiver zu gestalten, die Arbeitsvorgänge zu rationalisieren, eine optimale Ressourcenausnützung zu erzielen und dem Sicherheitsbedürfnis aller Beteiligten Rechnung zu tragen.
- Sie bietet eine Vielzahl zusätzlicher, abgestufter Schutz- und Kontrollmechanismen.
- Sie trägt durch die unterschiedlichsten Protokollebenen den Forderungen der Datensicherheit und des Datenschutzes Rechnung.
- Sie stellt revisionsfähige Unterlagen über alle Änderungen an Jobabläufen und Benutzerberechtigungsprofilen zur Verfügung.
- Sie gestattet einen Soll/Ist-Vergleich und protokolliert alle aufgetretenen Abweichungen.
- Schließlich unterstützt die Software den Wiederanlauf und berücksichtigt je nach Situation dabei auch, daß sich Jobabläufe ändern können.

Besuche in Großrechenzentren, die ihre Aufgaben unter der Kontrolle eines Produktions-, Planungs-, Steuerungs- und Kontrollsystems ausführen, haben gezeigt, daß man dort auf den Einsatz eines derartigen Systems nicht mehr verzichten möchte. In einem Großrechenzentrum ist der Einsatz einer Steuerungssoftware auch aus der Sicht des Datenschutzes nur zu empfehlen, weil die Abläufe transparenter werden und Fehler bei der Steuerung abnehmen.

21.5. Datensicherung bei Betrieb von mittleren DV-Anlagen

Während der Markt für Großsysteme gesättigt scheint, verzeichnet der Markt für DV-Systeme mittlerer Größe nach wie vor hohe Zuwachsraten. Viele Gemeinden und andere Institutionen im öffentlichen Bereich bedienen sich bei der Abwicklung ihrer Aufgaben solcher DV-Anlagen. Die Abhängigkeit von der Funktionsfähigkeit der maschinellen Datenverarbeitung ist in diesem Bereich aber nicht geringer als bei den Betreibern großer DV-Anlagen. Unterschiede sind allenfalls in der Personalkapazität festzustellen: Während in der Groß-EDV das Wissen auf mehrere Personen verteilt ist und alle auftretenden Probleme meist im eigenen Hause gelöst werden können, reduziert sich das Expertenteam beim Betreiber mittlerer DV-Systeme auf wenige Personen, manchmal sogar auf eine einzige. Wie bedenklich diese Entwicklung ist, zeigen immer wieder die in der Datenverarbeitung auftretenden Schadensfälle, über die in der Literatur berichtet wird.

Für die Groß-EDV existieren schon seit langem Checklisten und Maßnahmenkataloge zur Datensicherung und zum Datenschutz. Leider lassen sich die dort vorgeschlagenen Maßnahmen nicht so ohne weiteres auf den Betrieb von DV-Anlagen mittlerer Größe übertragen.

Basierend auf einem umfangreichen Fragenkatalog, der auf die Bedürfnisse des Betreibers einer DV-Anlage mittlerer Größe zugeschnitten ist, wurde eine „Orientierungshilfe zur Datensicherheit beim Einsatz von Datenverarbeitungsanlagen des Typs Hewlett Packard 3000" im Sinne der Forderungen der Datenschutzgesetze zusammengestellt, die an alle HP-Anwender der AKDB verteilt wurde.

Weitere Orientierungshilfen dieser Art sind bisher bei der Geschäftsstelle erhältlich für DV-Anlagen des Typs Mannesmann-Kienzle 9000, NCR ITX 10000 und Nixdorf 8870. Die Palette soll ergänzt werden durch ähnliche Papiere für WANG VS 100, DEC VAX und Siemens MX 2 und MX 500.

Die Orientierungshilfe gliedert sich in
- Installationsanforderungen
- Maßnahmen beim Betrieb der DV-Anlage
- Maßnahmen beim zusätzlichen Anschluß von Personal Computern
- Fragen zur Notfall- und Katastrophenvorsorge.

21.6. Technische Einzelprobleme

21.6.1. Gebäude- und Zutrittssicherung

An einem Beispiel aus der Praxis sollen die Anforderungen an die Gebäude- und Zutrittssicherung kurz dargestellt werden: Im Berichtsjahr hat eine Behörde ein ausgeklügeltes Gebäude- und Zutrittssicherungssystem in einem Dienstgebäude, in dem u.a. ein großes Rechenzentrum untergebracht ist, installiert und freigegeben.

Die Sicherungseinrichtungen betreffen die Gebäudeein- und -ausgänge, Treppenhäuser und Flure sowie die Außenfronten und Aufzüge des Dienstgebäudes. Die installierten Alarmanlagen entsprechen ebenso wie die Innenraumsicherungseinrichtungen dem neuesten Stand der Technik: Unterschiedliche Alarmschleifen lassen an einem zentralen Alarmtableau Ort und Art des aufgelaufenen Alarms erkennen. So ist feststellbar, ob es sich um einen Einbruch, ein Feuer oder einen sonstigen technischen Defekt handelt. In Abhängigkeit von der Alarmart erfolgt die Alarmweitergabe zur Polizei, Feuerwehr oder zu einem privaten Bewachungsunternehmen, das u.a. auch die Scharfschaltung der Alarmeinrichtungen nach Dienstende überprüft. Ein Druckabfall in den Wasser- oder Heizleitungen löst einen technischen Alarm aus. Bei jedem Alarmfall werden zusätzlich noch die zuständigen Sicherheitsbeauftragten der Behörde benachrichtigt. Es wurde auch darauf geachtet, daß die Alarmzentrale im Hause und die einzelnen Alarmleitungen selbst gegen Sabotage gesichert sind, damit eine ständige Funktionsbereitschaft gewährleistet ist.

Eigens gesichert ist das Hauptblockschloß, über das alle Alarmeinrichtungen scharf geschaltet werden. Unterblockschlösser, an die bestimmte Sicherheitsbereiche angeschlossen sind, können unabhängig vom Hauptblockschloß aktiviert werden, so daß die Alarmeinrichtungen dieser Bereiche zu jeder Zeit unabhängig von der Gesamtsicherung eingeschaltet werden können. Auf diese Weise läßt sich die von mir in anderen Fällen geforderte Möglichkeit der Teilscharfschaltung bestimmter Alarmeinrichtungen erreichen.

An zentralen Stellen im Gebäude sind Handfeuerlöscher installiert, die je nach Art der Brandbekämpfung mit Halon, Kohlendioxyd oder Schaum gefüllt sind.

Das Zutrittssicherungssystem verwendet Codekarten mit Magnetstreifen in Scheckkartengröße. Für die geschützten Bereiche sind verschiedene Raumzonen eingerichtet. Zum Teil sind diese Bereiche zusätzlich durch eine Zeitzone abgesichert, die den Zutritt der berechtigten Personen nur während eines festgelegten Zeitabschnittes gestattet. Zutrittsversuche Unberechtigter werden über den Protokolldrucker des Zutrittssicherungssystems dokumentiert.

Bei der Konzeption dieses Gebäude- und Zutrittssicherungssystems wurden auch die Erfahrungen meiner Dienststelle auf diesem Gebiet berücksichtigt.

21.6.2. Zugriffsschutz im IDVS II

Das AOK-Rechenzentrum Oberpfalz in Regensburg hat im Auftrag des Bundesverbands der Ortskrankenkassen (BdO) im Rahmen von IDVS II (Informations- und Datenverarbeitungssystem der Ortskrankenkassen) den Programm-Modul IK1800 entwickelt. IDVS II ist ein bundesweit zum Einsatz kommendes Programmpaket, mit dem die Allgemeinen Ortskrankenkassen (AOK) ihre verschiedenen Verwaltungsaufgaben DV-unterstützt abwickeln können. Der Einsatz und der Nutzungsumfang von IDVS II ist in den einzelnen Kassen noch unterschiedlich. Derzeit ist der Modul IK1800 nur bei einem Großhersteller verfügbar. Da der Zugriffsschutz in diesem Programmsystem mustergültig realisiert wurde, soll an dieser Stelle näher darauf eingegangen werden.

Der Modul IK1800 gestattet jedem Benutzer (Sachbearbeiter) ein eigenes detailliertes Zugriffsberechtigungsprofil zuzuordnen. Damit entfällt die bisher in IDVS II systembedingte Beschränkung auf eine begrenzte Anzahl von Benutzerklassen. Das Zugriffsberechtigungsprofil des einzelnen Sachbearbeiters, das von der Fachabteilung erstellt wird, enthält die Zugriffserlaubnisse, mit denen er, seiner organisatorischen Zuordnung entsprechend, auszustatten ist. So kann festgelegt werden, auf welche Programme und Transaktionen (Arbeitsschritte) und damit auf welche Datensatzarten und Datensatzfelder ein Zugriff gestattet wird. Mit der Eingabe von Transaktionscodes ist der Aufruf von Bildschirmmasken in verschiedenen Arbeitsvorgängen möglich. Während Urlaubs- oder Krankheitszeiten eines Sachbearbeiters kann die Nutzung seiner Benutzerrechte gesperrt werden. Auch für die Erlaubnis, Mitarbeiterdaten der Personalkrankenkasse bearbeiten zu können, ist im Benutzerprofil eine besondere Kennung vorgesehen. Über Zeitvorgaben zur Gültigkeitsdauer des individuellen Paßwortes kann die Nutzungsberechtigung des Benutzerprofils gesteuert werden.

Die Übernahme der Benutzerprofile ins IDVS II wird vom DV-Beauftragten der zuständigen AOK selbst besorgt. Dieser muß auch die einzelnen berechtigten Benutzer dem DV-System bekannt machen. Dazu wird eine Benutzerkennung und ein zunächst allgemeines Paßwort für die Erstanmeldung vergeben, mit dem allerdings nur das Programm aufgerufen werden kann, das der Sachbearbeiter zur Eingabe seines individuellen Paßwortes benötigt. Erst dann ist der Sachbearbeiter dem System gegenüber arbeitsberechtigt. Dem Systembeauftragten ist das persönliche Paßwort des Sachbearbeiters unbekannt und bleibt es auch, da es im DV-System einwegverschlüsselt abgespeichert wird. So wird sichergestellt, daß der Systembeauftragte nur über ein Teilwissen verfügt und eine unbefugte Nutzung von Benutzerprofilen ausgeschlossen ist. Ein Sachbearbeiter kann jederzeit ohne Mitwirkung eines Dritten sein persönliches Paßwort verändern. Durch die Speicherung seiner beiden zuletzt verwendeten Paßworte wird bewirkt, daß bei einer Paßwortänderung ein von den beiden letzten abweichendes Paßwort verwendet werden muß und nicht wechselweise auf vorher benützte zurückgegriffen wird.

Unerlaubte Zugriffsversuche werden mit Hinweis auf die verwendete Benutzerkennung und auf das tätig gewordene Terminal protokolliert.

Aus der Sicht des Datenschutzes stellt das Programm IK1800 eine bedeutsame Verbesserung des Datenschutzes dar, dessen Verwendung bei allen IDVS II einsetzenden AOK's unbedingt zu empfehlen ist. Mit IK1800 wird ein optimaler Zugriffsschutz gewährleistet, weil ein genaues, dem Beschäftigungsauftrag des Sachbearbeiters entsprechendes Benutzerprofil erzeugt werden kann. Die bisher verwendeten Benutzerklassen lassen eine derartige gezielte Vergabe der Zugriffsberechtigungen nicht zu.

21.6.3. Datensicherung beim Postversand

Beim Versand von Datenträgern (Briefen) gibt es immer wieder Unsicherheiten über die zu wählende Versandart.

Auf Anregungen des Senats hat das Staatsministerium des Innern festgelegt, welche Versendungsart für Schreiben der Meldebehörde an Bürger im Zuge von Aktionen zur Berichtigung der Melderegister angemessen ist.

Grundsätzlich hängt die Versendungsart von der Sensibilität der zu übermittelnden Daten ab. Die Schreiben der Meldebehörde enthielten im vorliegenden Falle neben Namen und Anschrift des Betroffenen in der Gemeinde die Anschriften weiterer Wohnungen in anderen Gemeinden und das Geburtsdatum. Nach den postalischen Vorschriften sind für die Versendung als Drucksache oder Briefdrucksache folgende Verschlußarten zulässig:
- Offene Sendung (Umschlag mit eingesteckter Lasche)
- Umschlag mit Punktverschluß,
- Umschlag mit Adhäsionsverschluß,
- bei mindestens 100 Sendungen derselben Gewichtsstufe verschlossene Umschläge.

Vom Zustand der Postsendung ausgehend, ist der Adhäsionsverschluß, der sowohl für Drucksachen als auch für Briefdrucksachen zugelassen ist, bei der Versendung von Schreiben mit Daten der oben beschriebenen Sensibilität als ausreichend sicher anzusehen. Ein Adhäsionsverschluß ist praktisch genauso schwierig zu öffnen und vor allem wieder zu schließen, wie ein sonst normal verschlossener Briefumschlag.

Von der Versendung der Schreiben in einem Umschlag mit eingesteckter Lasche oder mit Punktverschluß hat das Innenministerium den Gemeinden abgeraten.

21.6.4. Computer-Viren

Bereits im 8. Tätigkeitsbericht bin ich auf das Problem der Computer-Viren eingegangen und habe Vorschläge zum Schutz gegen die Computer- oder Programm-Viren gemacht.

Der beste Schutz ist nach wie vor, möglichst wenigen Benutzern die Befugnis einzuräumen, Benutzer- oder Systemprogramme zu ändern.
- Die Hersteller arbeiten bereits an Virenerkennungsmechanismen. So gibt es für Personal Computer Programme, die vor dem Start eines Programms prüfen, ob es seit seiner Freigabe verändert worden ist. In diesem Falle wird es nicht ausgeführt und damit eine Ausbreitung des Virus verhindert.
- Bei der Auswahl von Systemprogrammen ist besondere Vorsicht geboten, denn der Anwender ist gegen Viren, die in die Systemsoftware eingepflanzt wurden, machtlos. Ein virusinfizierter Compiler (Programmübersetzer) könnte beispielsweise in alle zu übersetzenden Programme ein Virus einpflanzen. Ein besonderes Risiko der Einschleusung von Viren besteht, wenn Mitarbeiter am

behördeneigenen Personal Computer private, etwa Spielprogramme einsetzen sollten. Dies muß unterbunden werden. Im Berichtszeitraum sind mir keine Fälle von Computer-Viren im Bereich der öffentlichen Verwaltung bekanntgeworden.

21.6.5. Persönlichkeitsschutz

Bei meinen technisch-organisatorischen Kontrollen mache ich die geprüfte Stelle immer darauf aufmerksam, daß sie das Recht des Bürgers auf den Schutz seiner Persönlichkeit auch am Behördenschalter zu gewährleisten hat. Das gilt vor allem dort, wo viel Publikumsverkehr abgewickelt wird oder sensible Informationen zwischen Bürger und Verwaltung ausgetauscht werden müssen.

Als geeignete Maßnahmen zum Persönlichkeitsschutz bieten sich an:
- Einlaß nur einer Person in das Dienstzimmer (Hinweis oder Steuerung durch Lichtsignalanlage)
- Hinweis auf Sachbehandlung in einem gesonderten Raum
- Einbau von Gesprächskabinen im Dienstzimmer
- Aufstellen von schallschluckenden Trennelementen zwischen den einzelnen Schaltern
- räumliche Trennung der Warte- von der Bearbeitungszone (ggf. durch Bodenmarkierungen kennzeichnen)
- Schaffung einer „Diskretionszone" in größeren Räumen wie Schalterhalle und Großraumbüro
- Anweisung der Dienstkräfte, auf den Persönlichkeitsschutz zu achten.

Werden in Bereichen mit regem Parteiverkehr zur Abwicklung von Dienstgeschäften Bildschirmgeräte genutzt, müssen diese so aufgestellt werden, daß wartende Personen Bildschirminhalte nicht zur Kenntnis nehmen können.

22. Datenschutzregister

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

Wegen des Umfanges dieser Veröffentlichungen und ihres geringen Nutzens für den Bürger wurde 1984 letztmals eine Übersicht über den Gesamtinhalt des Datenschutzregisters in zwei Teilen veröffentlicht. In den Folgejahren wurde von der Möglichkeit Gebrauch gemacht, lediglich Nachträge zu veröffentlichen. Auch diese Nachträge haben mittlerweile einen Umfang von ungefähr 100 Druckseiten pro Jahr erreicht. Der 4. Nachtrag berücksichtigt die Meldungen automatisierter Dateien von speichernden Stellen, die vom 5. Oktober 1987 bis 4. November 1988 eingegangen sind. Er gibt zudem in den Fällen, in denen sich in diesem Zeitraum die Art oder die Zahl der eingesetzten automatisierten Verfahren bei speichernden Stellen verändert hat, den aktuellen Stand wieder.

Am Stichtag für den 3. Nachtrag, umfaßte das Datenschutzregister 16899 meldepflichtige Dateien von insgesamt 4804 speichernden Stellen. Ein gutes Jahr später waren zum Datenschutzregister 17871 Dateien von 5124 speichernden Stellen gemeldet.

Die Zunahme ist in erster Linie auf das Anwachsen der Schülerdateien in Gymnasien, Realschulen und Volksschulen zurückzuführen. Im Kommunalbereich gibt es nunmehr kaum noch eine Gemeinde, die sich bei der Abwicklung ihrer Aufgaben nicht der automatisierten Datenverarbeitung bedient. Vor allem ist die Anzahl der meldepflichtigen Adreßdateien als Folge des Einsatzes von Textautomaten und Personalcomputern stark angestiegen.

Die Pflege des Datenschutzregisters umfaßte im Berichtsraum folgende Arbeiten:

Neueintragen einer speichernden Stelle	339
Neueintragen einer Datei bei einer speichernden Stelle	1436
Datenänderung bei einer speichernden Stelle	229
Dateibezogene Datenänderung	27
Löschen einer speichernden Stelle	19
Löschen einer Datei	466

Die hohe Zahl gelöschter Dateien ist dadurch zu erklären, daß viele speichernde Stellen alte EDV-Verfahren durch neue ersetzen, die eine Neumeldung erfordern.

23. Datenschutz beim Bayerischen Rundfunk

23.1. Bericht des Rundfunkbeauftragten

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

Bei der Überwachung der Datenverarbeitung beim Bayerischen Rundfunk (BR) im Zeitraum vom 1.1. bis 31.12.1987 hat der Datenschutzbeauftragte wiederum keine Datenschutzverstöße festgestellt. Im Mittelpunkt standen wie auch im letzten Jahr Fragen des Personal- und des Programmbereichs.

Zum Thema „Persönlichkeitsschutz gegenüber Presse und Rundfunk" teilt der Datenschutzbeauftragte des BR meine Ansicht (vgl. 19.1) nicht. Er teilt mit, daß es im BR drei verschiedene Archive gibt:
- das Zeitungsarchiv, das Originalzeitungsausschnitte in Themenmappen enthält;
- das Schallarchiv, das sämtliche am Markt verfügbaren Tondokumente und alle archivierungswürdigen Eigenproduktionen enthält; auch hier findet eine automatisierte Datenverarbeitung nicht statt, vielmehr werden die Tondokumente über Karteikarten erschlossen und
- das Fernseharchiv, das die beim BR anfallenden Daten vorhandener und in Planung befindlicher Fernsehsendungen automatisiert verarbeitet. Hierbei besteht auch ein Datenverbund zu anderen Rundfunkanstalten.

In allen Archiven würden somit keine sensiblen personenbezogenen Daten gespeichert, vielmehr würde allein bereits veröffentlichtes oder sonst allgemein zugängliches Material archiviert. Soweit überhaupt personenbezogene Daten vorhanden seien, dienten sie ausschließlich eigenen publizistischen Zwecken, d. h. sie unterliegen nach Ansicht des BR dem Medienprivileg.

Auf dieser Grundlage lehnt der Datenschutzbeauftragte des BR auch meine Forderungen in diesem Bereich (vgl. 16.1) ab.

23.2. Datenschutz beim Rundfunkgebühreneinzug

Die Datenschutzbeauftragten der Rundfunkanstalten haben vorgeschlagen, einheitliche Datenschutzregelungen für den Rundfunkgebühreneinzug zu schaffen. Die Vorschriften sollen im Rundfunkgebühren-Staatsvertrag angesiedelt werden.

Die Vorstellungen der Datenschutzbeauftragten der Rundfunkanstalten sind nach meiner Auffassung nur erste Vorschläge. Der Wortlaut einer Vorschrift legt den Schluß nahe, daß die Rundfunkdatenschutzbeauftragten ihre Zuständigkeit auf Datenübermittlungen von öffentlichen Stellen an Rundfunkanstalten ausweiten wollen. Weiter begegnet eine Generalklausel zur Datenerhebung Bedenken. Auch die Speicherungsdauer von Daten aus Bußgeldverfahren erscheint noch reduzierbar.

23.3. Datenanforderung der Finanzämter bei der GEZ

Dem Tätigkeitsbericht des Datenschutzbeauftragten des Bayer. Rundfunks für 1987 ist weiter zu entnehmen, daß Finanzämter versuchen, bei der Gebühreneinzugszentrale (GEZ) Bankkonten von Vollstreckungsschuldnern zu erfragen, um Guthaben auf diesen Konten pfänden zu können. Von diesen Konten werden von der GEZ die monatlichen Rundfunk- und Fernsehgebühren abgebucht.

Ich habe das Staatsministerium der Finanzen dazu um Stellungnahme gebeten und darauf hingewiesen, daß ein auf § 93 der Abgabenordnung (AO) gestütztes Auskunftsersuchen der Finanzverwaltung den Versuch einer Sachverhaltsaufklärung beim Steuerpflichtigen (Vollstreckungsschuldner) selbst voraussetzt. Erst wenn diese Sachverhaltsaufklärung nicht zum Ziele führt oder keinen Erfolg verspricht, kann die GEZ um Auskunft gebeten werden (Subsidiaritätsprinzip).

Das Staatsministerium der Finanzen hat darauf mitgeteilt, daß von Finanzämtern nur vereinzelt Auskunftsersuchen an die GEZ gestellt worden seien. Bei Auskunftsersuchen nach § 93 AO seien in jedem Fall das Subsidiaritätsprinzip und der Grundsatz der Verhältnismäßigkeit beachtet worden. Durch die Vollstreckungsmaßnahmen werde weder die Liquidität oder die Finanzausstattung des Bayer. Rundfunks gefährdet noch tangierten sie den verfassungsmäßig geschützten Kernbereich der Rundfunkfreiheit.

In der vom Staatsministerium der Finanzen geschilderten Vorgehensweise kann ich keine Verletzung datenschutzrechtlicher oder bereichsspezifischer Vorschriften der AO erkennen. Im Hinblick auf den Grundsatz der Gleichmäßigkeit der Besteuerung müssen die Finanzämter gesetzliche Möglichkeiten zur Begleichung geschuldeter Steuerrückstände ausschöpfen dürfen (vgl. auch 9.).

24. Der Beirat

Die Mitglieder des Beirats werden nach Art. 29 Abs. 2 BayDSG für 4 Jahre, die Mitglieder aus dem Bayer. Landtag für die Wahldauer des Landtags bestellt. Seit der Landtagswahl 1986 gehören dem Beirat an:

Ordentliche Mitglieder	Vertreter
Die Landtagsabgeordneten	
Franz Brosch	Willi Baumann
Adolf Dinglreiter	Franz Xaver Werkstetter
Dieter Heckel	Anneliese Fischer
Peter Welnhofer	Adolf Beck
Klaus Warnecke	Armin Nentwig
Carmen König	Hedda Jungfer
Die Senatoren	
Wolfgang Burnhauser	Hartwig Reimann
Für die Staatsregierung	
Dr. Klaus Geiger Ministerialdirigent im Bayer. Staatsministerium der Finanzen	Joachim Schweinoch Ministerialdirigent im Bayer. Staatsministerium des Innern
Für die Kommunalen Spitzenverbände	
Dr. Georg Wilhelm Geschäftsleitender Direktor der Anstalt für kommunale Datenverarbeitung in Bayern	Klaus Eichhorn Direktor der Anstalt für kommunale Datenverarbeitung in Bayern
Für die Sozialversicherungsträger	
Franz Martin Fehn Erster Direktor der Landesversicherungsanstalt Oberfranken und Mittelfranken	Herbert Schmaus Verwaltungsdirektor beim AOK-Landesverband Bayern
Für den Verband der Freien Berufe in Bayern e.V.	
Dr. med. Hans Braun Präsident des Verbandes der Freien Berufe in Bayern e.V.	Winfried Wachter Präsidiumsmitglied des Verbandes der Freien Berufe in Bayern e.V.

Den Vorsitz im Beirat führt MdL Franz Brosch, sein Stellvertreter ist MdL Klaus Warnecke.

Der Beirat befaßte sich in seinen drei Sitzungen am 16.12.1987, 14.4.1988 und 7.7.1988 mit folgenden Themen:

- Beratung des 9. Tätigkeitsberichts
- Berichte von den Konferenzen der Datenschutzbeauftragten des Bundes und der Länder
- Bericht des Staatsministeriums des Innern vom 15.10.1987 zum Beschluß des Bayer. Landtages vom 21.5.1987 betreffend Datenschutz in Bayern
- Übermittlung von Wähleranschriften an politische Parteien und Wählergruppen
- Herausgabe von Anschriften der Jungmeister durch eine Handwerkskammer
- Prüfprogramm 1988
- Notwendigkeit der Novellierung des Polizeiaufgabengesetzes
- Jährliche Veröffentlichung der Übersicht über das Datenschutzregister
- Gesetzentwurf der SPD-Fraktion zur Änderung des Bayer. Datenschutzgesetzes
- Bericht über die Prüfung der Aktion des Landesamtes für Verfassungsschutz in der Gemeinde Bruck sowie Erörterung der grundsätzlichen Zulässigkeit der Ablichtung von Lichtbildern aus Paß-/Personalausweisantragsregistern

- Datensicherungsmaßnahmen beim Postversand für die Berichtigungsaktion der Melderegister
- Presseberichte über Äußerungen der Präsidenten der Obersten Rechnungshöfe wegen Behinderung der Prüftätigkeit durch datenschutzrechtliche Bestimmungen
- Bericht über Prüfungen und Beanstandungen.

25. Konferenz der Datenschutzbeauftragten

Im Jahre 1988 trafen sich die Datenschutzbeauftragten der Länder und des Bundes und die Datenschutzkommission Rheinland-Pfalz zu drei Konferenzen, in denen u. a. folgende Themen erörtert wurden:

- Neufassung des Bundesdatenschutzgesetzes und Änderung des Verwaltungsverfahrensgesetzes
- Gesetz über die Zusammenarbeit des Bundes und der Länder in Angelegenheiten des Verfassungsschutzes (Bundesverfassungsschutzgesetz)
- Gesetz über Mitteilungen in Angelegenheiten des Staats- und Verfassungsschutzes sowie der nachrichtendienstlichen Tätigkeit (Verfassungsschutzmitteilungsgesetz)
- Gesetz über den Militärischen Abschirmdienst (MAD-Gesetz)
- Gesetz über das Bundeskriminalamt
- Gesetz zur Strukturreform im Gesundheitswesen
- Gesetz zur Einführung eines Sozialversicherungsausweises und zur Änderung anderer Sozialgesetze
- Fehlende gesetzliche Grundlagen für die Datenverarbeitung im Sicherheitsbereich (Übergangsbonus)
- Datenschutzprobleme im Zusammenhang mit der Neuordnung der Deutschen Bundespost
- Aktuelle Probleme des Datenschutzes in der Telekommunikation
- Persönlichkeitsschutz gegenüber Rundfunk und Presse
- Kontrolle der Einhaltung der Datenschutzvorschriften zu ZEVIS
- Veröffentlichung personenbezogener Daten durch EG-Behörden
- Datensicherheit beim Einsatz kleinerer Datenverarbeitungsanlagen

Zu mehreren Punkten konnten nach intensiven Beratungen einstimmige Beschlüsse gefaßt werden. Zu keinen Konferenzbeschlüssen, zu denen Einstimmigkeit erforderlich ist, kam es hingegen bei den Stellungnahmen zur Novellierung des Bundesdatenschutzgesetzes und zu den Themen im Sicherheitsbereich. Unterschiedliche Auffassungen traten zutage bei der Interpretation des Volkszählungsurteils des Bundesverfassungsgerichts von 1983 und den aus dem Urteil zu ziehenden Folgerungen. Keine Übereinstimmung gab es in der vielfach entscheidenden Frage, welches Gewicht den Anforderungen der inneren Sicherheit in Abwägung mit dem Grundrecht auf informationelle Selbstbestimmung beigemessen werden solle. Angesichts zunehmender Kriminalität, vor allem der Gewalt-, Banden- und Rauschgiftkriminalität, sowie sinkender Aufklärungsziffern ist nach Überzeugung des Bayerischen Landesbeauftragten für den Datenschutz eine Aufweichung der Sicherheitsgesetze, eine Behinderung der Arbeit der Polizei oder gar eine partielle Lahmlegung ihrer Informationstätigkeit nicht zu verantworten. Bei den Sicherheitsgesetzen kann es deshalb im wesentlichen nur darum gehen, die Befugnisse der Sicherheitsbehörden auf eine tragfähige rechtliche Grundlage zu stellen. Die weit darüber hinausgehenden Forderungen der Mehrheit der Datenschutzbeauftragten nach radikaler Beschränkung der Informationstätigkeit der Sicherheitsbehörden würden die innere Sicherheit gefährden und waren für mich deshalb nicht akzeptabel. Für völlig überzogen halte ich auch die grundsätzlichen Vorbehalte der Mehrheit gegen die Einführung eines Sozialversicherungsausweises und die darin vorgesehene Verwendung der Rentenversicherungsnummer.

Ich werde mich in der Datenschutzkonferenz auch weiterhin um einen vernünftigen Datenschutz bemühen.

26. Arbeitsbedingungen in der Geschäftsstelle des Bayerischen Landesbeauftragten für den Datenschutz

Im 8. Tätigkeitsbericht habe ich mitgeteilt, daß ich von drei Abordnungsstellen eine Entlastung der angespannten Personalsituation erwarte. Damals hat allein das Staatsministerium der Finanzen einen Beamten an den Datenschutzbeauftragten abgeordnet. Die beiden anderen Stellen konnten dagegen nicht besetzt werden.

Inzwischen hat sich die Personalsituation gebessert: Im Doppelhaushalt 1987/88 wurden zwei der Abordnungsstellen in echte Planstellen umgewandelt. Demzufolge konnten ein Beamter des höheren und eine Beamtin des gehobenen Dienstes zusätzlich eingestellt werden. Ich hoffe nun, daß im Doppelhaushalt 1989/90 auch die dritte Abordnungsstelle in eine echte Planstelle umgewandelt wird. Bis dahin ist die Stelle von einer Beamtin besetzt, die dankenswerterweise vom Staatsministerium für Arbeit und Sozialordnung an die Geschäftsstelle abgeordnet wurde.

Nach entsprechender Einarbeitung der neuen Mitarbeiter steht weitgehend das Personal zur Verfügung, das der Landesbeauftragte für den Datenschutz zur Erledigung der ihm übertragenen Aufgaben benötigt. Die personelle Ausstattung erlaubt nun auch im gebotenen Umfang Datenschutzkontrollen vor Ort im Bereich der Kommunal-, Sozial- und Gesundheitsverwaltung. Im kommenden Jahr sollen allerdings auch die Bereiche Umwelt, Landwirtschaft und Forsten sowie die Krankenhäuser verstärkt kontrolliert werden.

Eine spürbare Personalbelastung bringt allerdings die Nachfrage nach Referenten für Veranstaltungen über Datenschutzrecht mit sich. Sollte die Nachfrage weiter zunehmen, wird sie nicht mehr wie bisher überwiegend in Nebentätigkeit, sondern im vermehrten Umfang in hauptberuflicher Tätigkeit zu befriedigen sein und die Einstellung weiteren Personals erforderlich machen.

27. Seminare und Vorträge über Datenschutz

Mit der zunehmenden Automatisierung in der Verwaltung und dem Einzug der Informatik in den Schulunterricht nahm bei meiner Geschäftsstelle die Nachfrage nach Referenten für Vorträge zum Datenschutz weiter zu. Wegen der Arbeitsbelastung meiner Geschäftsstelle durch Datenschutzkontrollen konnten allerdings nicht alle Wünsche erfüllt werden.

Am Landesamt für Statistik und Datenverarbeitung sowie an der Verwaltungsschule wurden 16 Vorträge gehalten. Neben allgemeinen in den Datenschutz einführenden Referaten handelte es sich um Vorträge zu den Themen „Datenschutz im Krankenhaus" und „Datenschutz im Melde-, Paß- und Personalausweisrecht", „Datenschutz im Sicherheits- und Ordnungsrecht", ferner um Vorträge im Rahmen der Aus- und Weiterbildung behördlicher Datenschutzbeauftragter. Dabei wurden auch die erforderlichen technischen und organisatorischen Datensicherungsmaßnahmen behandelt. Zehnmal waren Referate im Bereich der Lehrerfortbildung zu halten. In die verstärkt aufgenommene informationstechnische Bildung an den bayerischen Schulen wird auch der Datenschutz einbezogen. Zahlreiche Fachvorträge waren bei den Fort- und Ausbildungseinrichtungen der bayerischen Polizei zu halten. Wiederholt haben meine Mitarbeiter und ich auf Fortbildungsveranstaltungen der Hanns-Seidel-Stiftung zum Thema „Polizei und Datenschutz" referiert. Die Entwicklung der Telekommunikation hat auch zur Nachfrage nach Datenschutzreferaten geführt. Auch im Bereich des Archivwesens war ein datenschutzrechtlicher Fachvortrag zu halten.

Die Ausbildung der Rechtsreferendare im Datenschutzrecht habe ich fortgeführt.

28. Anhang:

Beschluß

der Konferenz der Datenschutzbeauftragten des Bundes und der Länder sowie der Datenschutzkommission Rheinland-Pfalz

vom 10. Oktober 1988

Datensicherheit beim Einsatz kleinerer Datenverarbeitungsanlagen

Beim Einsatz kleinerer Datenverarbeitungsanlagen, vor allem von persönlichen Computern (PC), bereiten die Datensicherheit und die Ordnungsmäßigkeit der Verarbeitung personenbezogener Daten besondere Probleme. Im Hinblick auf diese Probleme geben die Datenschutzbeauftragten des Bundes und der Länder folgende Empfehlungen:

1. Vor jeder Entscheidung, ob für die Arbeiten eines Aufgabengebiets ein PC oder eine sonstige kleinere Datenverarbeitungsanlage eingesetzt werden kann, muß geprüft werden, ob die dabei erzielbare Datensicherheit ausreichend ist. Bei dieser Prüfung müssen insbesondere die Empfindlichkeit der Daten und der Grad der Verbindlichkeit der Verarbeitungslogik berücksichtigt werden. Die Verarbeitung personenbezogener Daten mit einem automatisierten Verfahren, das keine angemessene Datensicherheit bietet, verstößt gegen die Datenschutzgesetze.

2. Eine speichernde Stelle hat auch bei der Verarbeitung personenbezogener Daten auf einem PC oder einer sonstigen kleineren Datenverarbeitungsanlage die technischen und organisatorischen Maßnahmen zu treffen, die je nach Art der zu schützenden Daten geeignet sind, die Datensicherheit zu gewährleisten. Sofern die Datensicherheit mit den verfügbaren Maßnahmen nicht in dem erforderlichen Umfang gewährleistet werden kann, muß auf den Einsatz des PC oder der kleineren Datenverarbeitungsanlage verzichtet werden.

   Um die Datensicherheit zu gewährleisten, sind insbesondere die dem neuesten Stand entsprechenden technischen Maßnahmen zu treffen. Weisungen sollten schriftlich erfolgen und in einer Dienstanweisung zusammengefaßt werden. Durch Kontrollen der Arbeitsdurchführung ist sicherzustellen, daß alle Vorschriften und Weisungen befolgt werden.

3. Die Hersteller von Hard- und Software werden aufgefordert, für kleinere Datenverarbeitungsanlagen einschließlich der persönlichen Computer Verfahren zu entwickeln und bereitzustellen, die einen Betrieb dieser Geräte mit einem Maß an Datensicherheit ermöglichen, das demjenigen großer Rechenzentren entspricht. Vor allem müssen Hilfsmittel verfügbar gemacht werden, die es einer datenverarbeitenden Stelle ermöglichen,

   - ohne organisatorisch strukturiertes Rechenzentrum und damit auch ohne Funktionstrennungen bei der Arbeitsabwicklung,
   - ohne organisatorische Trennung zwischen Anwendung und Durchführung der automatisierten Datenverarbeitung und
   - trotz Verzichts auf Detailkenntnisse der automatisierten Datenverarbeitung bei Vorgesetzten und der für die Revision zuständigen Organisationseinheit

   sicherzustellen, daß bei der Verarbeitung auf der eingesetzten Datenverarbeitungsanlage eine verbindlich vorgeschriebene Verarbeitungslogik eingehalten wird. Dazu ist es unter anderem erforderlich, Verfahren bereitzustellen, die gewährleisten, daß Programme ausschließlich in der freigegebenen Fassung zum Ablauf kommen. Systemprogramme und Anwendungsprogramme könnten dazu mit einem geeigneten kryptografischen Verfahren versiegelt werden, wodurch Manipulationen erkennbar würden.

   Für persönliche Computer und sonstige kleinere Datenverarbeitungsanlagen sollten zur Datensicherung Systemprogramme und systemnahe Programme mit einem an der Ausstattung großer Anlagen orientierten Leistungsumfang zur Verfügung gestellt werden. Wesentliche, der Datensicherheit dienende Komponenten sollten in das Betriebssystem integriert werden, um Manipulationen und Umgehungsmöglichkeiten zu erschweren.

Erläuterungen:

Die Zuverlässigkeit der automatisierten Datenverarbeitung ist eine als selbstverständlich unterstellte Voraussetzung des Verwaltungshandelns. Insbesondere dann, wenn die Verarbeitungslogik der durchzuführenden Arbeiten verbindlich ist, ist die speichernde Stelle darauf angewiesen, eine den Vorschriften und Weisungen entsprechende Arbeit sicherstellen zu können. Ein Abweichen von der als verbindlich vorgeschriebenen Verarbeitungslogik durch individuelle Einflußnahme auf die Datenverarbeitung kann nicht hingenommen werden.

In den vergangenen Jahrzehnten wurden Organisationsformen und Verfahren entwickelt, die es in großen Rechenzentren ermöglichen, die Datenverarbeitung sehr sicher

abzuwickeln. Für große Rechenzentren sind heute die zur Datensicherung erforderlichen Hilfsmittel verfügbar. Große Rechenzentren können in einem der jeweiligen Aufgabenstellung angemessenen Umfang sicherstellen, daß die Datenverarbeitung entsprechend den geltenden Vorschriften und Weisungen erfolgt. Der Datensicherheit dienen dabei vor allem

- eine den Anforderungen angepaßte Strukturierung der Organisation mit geeigneten Funktionstrennungen,
- automatisierte Aufzeichnungen und Sicherungen der Datenverarbeitungsanlage,
- die detaillierte Regelung des Arbeitsablaufs durch eine Dienstanweisung und
- eine institutionalisierte Kontrolle der Arbeitsdurchführung, die den jeweiligen Erfordernissen angepaßt ist.

Bezüglich der Arbeit großer Rechenzentren ist unbestritten, daß ein sicherer Betrieb ohne strukturierte Organisation und ohne geeignete Funktionstrennungen nicht möglich ist. Daher ist es bedenklich, wenn heute in zunehmender Zahl kleinere Datenverarbeitungsanlagen installiert werden, bei denen wegen der geringen Mitarbeiterzahl keine hinreichende Strukturierung der Organisation verwirklicht werden kann. Es erhebt sich in diesen Fällen die Frage, ob die speichernden Stellen in angemessenem Umfang in der Lage sind, eine den Vorschriften und Weisungen entsprechende Verarbeitung der Daten sicherzustellen.

Kleinere Datenverarbeitungsanlagen werden fast immer so eingesetzt, daß von einer organisatorischen Strukturierung des Rechenzentrums, wie sie bei großen Rechenzentren selbstverständlich ist, nicht mehr die Rede sein kann. Selbst die organisatorische Trennung von Programmierung, Maschinenbedienung (Rechenzentrum) und Anwenderbereich wird teilweise aufgehoben. Zum Überwachen und Prüfen der automatisierten Arbeitsdurchführung fehlen der datenverarbeitenden Stelle im allgemeinen die fachlichen Voraussetzungen.

Zwar gibt es häufig noch eine Funktion, die man organisatorisch als Rechenzentrum bezeichnen könnte. Diese Rechenzentrumsfunktion wird aber nur von wenigen Mitarbeitern oder einem einzigen Mitarbeiter wahrgenommen. Möglicherweise ist dieser einzige Mitarbeiter sogar nur während eines sehr kurzen Teils seiner Arbeitszeit für die Maschinenbedienung und im übrigen innerhalb des Anwenderbereichs tätig. Vielleicht sind ihm auch gleichzeitig Programmieraufgaben zur selbständigen Erledigung übertragen. Zur Vertretung des Maschinenbedieners werden häufig Mitarbeiter aus dem Anwenderbereich vorgesehen.

Eine interne Überwachung und Prüfung der Arbeitsdurchführung ist in vielen Fällen nicht institutionalisiert, weil kein Mitarbeiter mit der dafür erforderlichen Fachkunde verfügbar ist. Häufig ist selbst der Vorgesetzte des Maschinenbedieners zu einer Beurteilung der Arbeit seines Mitarbeiters, soweit diese die Durchführung der automatisierten Datenverarbeitung betrifft, nicht in der Lage.

Bei dem Einsatz eines persönlichen Computers, der dem Benutzer während der Benutzung alleine zur Verfügung steht, kann sogar nicht mehr von einer organisatorisch abgrenzbaren Rechenzentrumsfunktion gesprochen werden. Der Benutzer ist Anwender und Maschinenbediener in einer Person. In vielen Fällen liegt bei ihm auch die Aufgabe des Programmierens.

Wegen dieser personellen Situation lassen sich wesentliche Maßnahmen zur Datensicherung, die bei großen Rechenzentren heute als selbstverständlich und unverzichtbar angesehen werden, bei Einsatz kleinerer Datenverarbeitungsanlagen nicht verwirklichen. Funktionstrennungen und eine den Anforderungen der Datensicherheit entsprechend strukturierte Organisation bedürfen einer hinreichenden Mitarbeiterzahl. Falls nur wenige Mitarbeiter die Aufgaben des Rechenzentrums wahrnehmen, ist eine Strukturierung der Organisation im allgemeinen praktisch nicht möglich. Bei Einsatz eines einzigen Mitarbeiters gibt es keine Strukturierung der Organisation.

Dadurch ist die Datensicherheit beim Betrieb kleinerer Datenverarbeitungsanlagen und insbesondere auch beim Einsatz eines PC, der seinem Benutzer während der Benutzung alleine zur Verfügung steht, beeinträchtigt. Diese Beeinträchtigung ist im allgemeinen so stark, daß sie bei einem großen Rechenzentrum – jedenfalls für die Verarbeitung personenbezogener Daten nach verbindlich vorgegebener Verarbeitungslogik – als nicht hinnehmbar angesehen würde.

Es gibt Wege, die Datensicherheit beim Einsatz kleinerer Datenverarbeitungsanlagen in angemessenem Umfang zu verbessern. Dazu müßten allerdings von den Herstellern systemtechnische Voraussetzungen entwickelt und bereitgestellt werden. Erste Lösungen sind am Markt bereits als Angebote für Kreditinstitute erhältlich und unter anderem in Geldausgabeautomaten eingesetzt.

Der vorliegende Beschluß betrifft ausschließlich die Datensicherheit. Selbstverständlich gelten auch bei Einsatz eines PC oder einer sonstigen kleineren Datenverarbeitungsanlage die übrigen Vorschriften des Datenschutzes wie etwa diejenigen zur Zulässigkeit der Datenverarbeitung, zu den Rechten der Betroffenen und den Pflichten der speichernden Stelle in gleichem Umfang wie bei Einsatz einer großen Datenverarbeitungsanlage.