Der Bayerische Landesbeauftragte

für den Datenschutz

17. Tätigkeitsbericht, 1996

Stand: 13.12.1996

1. Einführung - Motto

Das im Layout geänderte Deckblatt des 17. Tätigkeitsberichts, meines zweiten, trägt das Motto "Datenschutz ist Grundrechtsschutz".

Warum dieses Motto? Aus zwei Gründen: Einmal scheint mir gerade in der Öffentlichkeit das Ziel des Datenschutzes und die Funktion des Datenschutzbeauftragten - vorsichtig gesprochen - nicht immer ganz klar zu sein. Vielfach herrscht die Meinung vor, Datenschutz diene dem Schutz der "Daten", und der Landesbeauftragte und seine Mitarbeiter hätten dafür zu sorgen, daß "die Daten" geschützt würden. Dementsprechend sprechen zwar viele dem Datenschutz einen hohen Stellenwert zu, realisieren aber nicht, daß es bei dieser Aufgabe nicht um den Schutz irgendwelcher, von der Person quasi abstrahierter Daten und Fakten geht, sondern ganz zentral um den Schutz der Person selbst. Es geht um den Schutz des Rechts des Bürgers, selbst zu entscheiden, wer was über ihn weiß, wem dieses Wissen übermittelt wird und zu welchen Zwecken dieses Wissen verwendet wird. Es geht darum, der Berechtigung des Satzes "Wissen ist Macht" dieses Selbstentscheidungsrecht des Bürgers als staatlich garantiertes Korrektiv entgegenzusetzen.

Meine Aufgabe ist es deshalb nicht, die "Daten" zu schützen, sondern den Bürger vor unberechtigten Eingriffen in dieses Selbstentscheidungsrecht. Dieses Recht hat nach der Rechtsprechung des Bundesverfassungsgerichts Grundrechtsqualität, deswegen das Motto "Datenschutz ist Grundrechtsschutz".

Man mag mir vorwerfen, daß nach inzwischen 26 Jahren institutionalisierten Datenschutzes in Deutschland diese Erkenntnis eine Trivialität darstellt, die nicht besonders hervorgehoben werden muß. Das mag für die Fachwelt zutreffen. Im übrigen halte ich es aber wegen der Mißverständnisse in der Öffentlichkeit durchaus für zweckdienlich, diese Grundlagen hervorzuheben.

Damit keine Irrtümer entstehen, möchte ich hier - wie schon in meinem 16. Tätigkeitsbericht - ebenso ausdrücklich darauf hinweisen, daß dieses Recht nicht absolut gilt, sondern vom Gesetzgeber im überwiegenden Interesse der Allgemeinheit eingeschränkt werden kann. Der Gesetzgeber kann sich dabei aber nicht auf reine Datennutzungregelungen nach dem Motto beschränken,

zulässig ist, was aus der Sicht des Datenverarbeiters erforderlich ist. Nötig ist, neben dem genannten überwiegenden Interesse der Allgemeinheit, eine klare Festlegung der Eingriffsvoraussetzungen und Eingriffsgrenzen. Diese sind um so enger zu ziehen, je tiefer der Eingriff ist.

Daß diese Erwägungen keine reine Theorie sind, glaube ich an einigen Beispielen in diesem Bericht, etwa anhand der Fragen in Zusammenhang mit der diskutierten Einführung der akustischen Wohnraumüberwachung ("Großer Lauschangriff") und dem Entwurf eines Bayerischen Sicherheitsüberprüfungsgesetzes deutlich machen zu können.

1.1 Ziele des Tätigkeitsberichts

Ich habe erwogen, den Inhalt des Tätigkeitsberichts auf einen reinen "Mängelbericht" zu reduzieren. Der Bericht wäre dadurch "schlanker" und vielleicht im Zusammenhang auch leichter lesbar geworden. Wegen des im Hinblick auf den neuen Zweijahresturnus gestiegenen Umfangs hätte auch von daher einiges für diese Verfahrensweise gesprochen. Auf der anderen Seite hat sich die Verwendung des Tätigkeitsberichts zur Klärung immer wieder auftretender strittiger und spezieller Fragen des Datenschutzes bewährt. Ich möchte deshalb diese zusätzliche Funktion als Beitrag zur Lösung aktueller datenschutzrechtlicher Fragen aus dem Berichtszeitraum doch beibehalten. Wegen des dadurch bedingten Umfangs des Berichts bitte ich um Verständnis.

1.2 Bilanz zum 16. Tätigkeitsbericht

Es würde den Rahmen dieses Berichtes sicher sprengen, zu jeder offenen Frage jetzt auszuführen, wie sie inzwischen beantwortet wurde. Ich möchte aber doch zu einigen wenigen ausgewählten Fragen über das Ergebnis der weiteren Diskussionen berichten. Ich kann hier einige Erfolge nennen, in anderen Punkten wurden meine Anregungen und Forderungen nicht aufgenommen.

Eine positive Bilanz kann ich u. a. in nachstehenden Punkten ziehen:

- Zum Thema Aufnahmen, insbesonders Videoaufzeichnungen, von Versammlungsteilnehmern, hat das Staatsministerium des Innern inzwischen eine Regelung erlassen, die im wesentlichen meine Forderung erfüllt, daß nur von solchen Versammlungsteilnehmern gezielte Aufzeichnungen gefertigt werden, von denen eine erhebliche Gefahr für die öffentliche Sicherheit und Ordnung ausgeht.

- Das Staatsministerium der Justiz hat sich inzwischen bereit erklärt, für das in Bayern einzurichtende zentrale staatsanwaltschaftliche Verfahrensregister - STARIS - die rechtlichen Grenzen einzuhalten, die im Verbrechensbekämpfungsgesetz für ein zentrales staatsanwaltschaftliches Verfahrensregister auf Bundesebene vorgesehen sind.

- Im Bereich Justizvollzugsanstalten wurde meine Anregung aufgegriffen, daß Gefangene so

rechtzeitig von Führungen informiert werden, daß sie sich einer "Besichtigung" entziehen können.

- Seit längerem erstmals muß ich nicht mehr über mißbräuchliche Nutzung von Kfz-Halterdaten im Zusammenhang mit der Ermittlung von "säumigen" Kurbeitragszahlern berichten.

- Der Erhebungsumfang im Mikrozensusgesetz wurde auf Anregung nicht nur von mir deutlich vermindert, auf die Freiwilligkeit der Beantwortung wird nunmehr unmißverständlich hingewiesen.

- In der Frage, welchen Umfang darf die Datenübermittlung zu Abrechnungszwecken von kassenärztlichen bzw. -zahnärztlichen Vereinigungen an Krankenkassen haben, sind positive Schritte in Richtung einer datenschutzgerechten Lösung erkennbar. Mit Ausnahme bisher des Verbands der Angestelltenkrankenkassen sind nunmehr alle gesetzlichen Krankenkassen bereit, im Bereich der Abrechnung zahnärztlicher Rechnungen einer Reduzierung der zu übermittelnden Daten zuzustimmen, die wohl dem gesetzlichen Gebot einer Übermittlung der abgerechneten Patientendaten nur fallbezogen, nicht versicherten-, d. h. nicht personenbezogen, gerecht wird. Ein entsprechendes Ergebnis für den Bereich der niedergelassenen Ärzte steht leider noch aus.

Keinen Erfolg hatte ich bisher u. a. bei folgenden Fragen:

- Das Staatsministerium des Innern lehnt meine Anregung nach wie vor ab, bei der Protokollierung von Abfragen aus polizeilichen Dateien auch einen Hinweis auf den Zweck der Abfrage aufzunehmen. Dies sei zu verwaltungsaufwendig und wenig effektiv. Ich bin im Gegensatz dazu der Auffassung, daß eine derartige Zweckangabe schon eine präventive Wirkung gegen Mißbrauch der Abfragemöglichkeiten hätte.

- Zur Frage mißbräuchlicher Einsichtnahmen in Gefangenenpersonalakten vertritt das Staatsministerium der Justiz nach wie vor die Auffassung, daß die von mir zumindest geforderte Dokumentierung der Einsichtnahmen als Maßnahme gegen Mißbrauch zu verwaltungsauf-

wendig und auch nicht effektiv sei. Auch hier hielte ich eine positive Präventionswirkung für gegeben.

- Im Steuerbereich lehnt das Staatsministerium der Finanzen es nach wie vor ab, auf meine Vorschläge zur Wahlmöglichkeit hinsichtlich der Geltendmachung eines Behindertenfreibetrages entweder durch Eintrag auf der Lohnsteuerkarte oder über die Einkommensteuerveranlagung einzugehen. Ich bedaure das, da auf diese Weise der Behinderte eine Kenntnisnahme durch die Gemeinde oder den Arbeitgeber von seiner Behinderung hätte vermeiden können.

  Ebenfalls abgelehnt hat es meinen Vorschlag, in Fällen konfessionsverschiedener Ehen Einkommensdaten des nicht dieser Religionsgemeinschaft angehörigen Partners dieser Konfession auch nicht zu übermitteln. Das Staatsministerium verweist dazu auf die Rechtsprechung des Bundesfinanzhofs, die die Rechtmäßigkeit des bisherigen Verfahrens feststellt.

  Rechtmäßigkeit schließt nicht aus, daß das Verfahren datenschutzrechtlich verbessert werden könnte.

- Im technisch-organisatorischen Bereich muß ich bei Prüfungen immer wieder fast regelmäßig zum Teil nicht unerhebliche Sicherheitsmängel feststellen (sorgloser Umgang mit DV-Systemen, s. Nr. 18.2.2). Ich sehe das als Negativpunkt meiner Bilanz an, weil diese Fragen ebenso regelmäßig in den Tätigkeitsberichten in der Vergangenheit enthalten waren, ein signifikantes Abnehmen dieser Mängel aber nicht festzustellen ist. Ich bin deswegen der Auffassung, daß diesen Fragen von den datenschutzrechtlich verantwortlichen Stellen (Art. 25 Bayerisches Datenschutzgesetz) mit höherer Intensität nachgegangen werden muß.

- Die im letzten Tätigkeitsbericht aufgeworfene Frage meiner Kontrollkompetenz muß ich ebenfalls im Negativkatalog vermerken. Die Staatsregierung ist bisher nicht bereit, im Sinne meiner Forderung nach Ausweitung meiner Kontrollkompetenz für Akten zumindest im Bereich verdeckter Datenerhebung für eine Gesetzesänderung initiativ zu werden. Das gleiche

gilt für das Problem der Einschränkung meiner Kontrollkompetenz über Datenerhebungsmaßnahmen während des Laufes eines Strafverfahrens gemäß Art. 30 Abs. 4 Bayerisches Datenschutzgesetz. Durch letztere Einschränkung läuft zudem die bundesgesetzlich vorgesehene Information des Landesdatenschutzbeauftragten von einer Rasterfahndung und von Gruppenauskünften für Strafverfolgungsbehörden nach dem Ausländerzentralregistergesetz leer.

- Unabhängig von der Frage, daß in der konkreten Prüfungspraxis die Behörden zu weitgehender Zusammenarbeit bereit sind und die von mir gewünschten Unterlagen im Regelfall vorlegen, halte ich die gegebene Rechtslage für eine Effektivprüfung in den genannten Bereichen nach wie vor nicht für ausreichend. Ich habe mich deshalb entsprechend auch in einer Stellungnahme zu einer Popularklage gegen das Bayerische Datenschutzgesetz gegenüber dem Bayerischen Verfassungsgerichtshof geäußert. Die Forderung nach effektiven Kontrollmöglichkeiten ist auch im Hinblick auf neue verdeckte Ermittlungsmaßnahmen - siehe unten "Großer Lauschangriff" - aktueller denn je.

In der Frage der Kontrolle von G 10-Maßnahmen habe ich mich mit dem Vorsitzenden der G 10-Kommission dahingehend abgestimmt, daß von der G 10-Kommission nicht nur die Datenerhebung, sondern auch die weitere Verarbeitung der durch eine G 10-Maßnahme gewonnenen Daten geprüft wird, und zwar nicht nur in einer G 10-Akte, sondern auch in sonstigen Unterlagen des Landesamts für Verfassungsschutz. Ich habe auf die damit verbundenen Schwierigkeiten hingewiesen und meine Mitwirkung nach Art. 30 Abs. 3 Bayerisches Datenschutzgesetz angeboten.

1.3 Überblick über meine Stellungnahmen zu Gesetzgebungsverfahren und Verfahren vor Verfassungsgerichten

Im Berichtszeitraum habe ich zu einer ganzen Reihe von Gesetzentwürfen Stellung genommen, wobei ich dazu bemerke, daß ich teilweise erst sehr spät von den Staatsministerien eingeschaltet wurde. Dazu gehören wichtige Gesetzentwürfe bzw. Überlegungen zu Entwürfen aus dem Sicherheitsbereich, dem Justizbereich, dem Gesundheitsbereich, dem Steuer- und Statistikbereich und dem Telekommunikations-, Teledienst- und Medienbereich. Weiter habe ich - wie bereits bemerkt - Stellung genommen zu einer Popularklage gegen das Bayerische Datenschutzgesetz, betreffend vor allem die Kontrollkompetenz des Datenschutzbeauftragten, sowie zu einer Klage vor dem Bundesverfassungsgericht gegen die durch das Verbrechensbekämpfungsgesetz eingefügte Befugnis für den BND, auch durch Überwachung und Aufzeichnung des internationalen Funkfernmeldeverkehrs Nachrichten zu sammeln.

Herausgreifen an dieser Stelle möchte ich fünf Vorhaben, nämlich die Absichten zur Einführung des sogenannten "Großen Lauschangriffs", den Entwurf der Bayerischen Staatsregierung für ein Sicherheitsüberprüfungsgesetz, meine Haltung zum Bayerischen Ergänzungsgesetz zur bundesrechtlichen Regelung des Schwangerschaftsabbruchs und zu den Vorschlägen zum Telekommunikations-, Teledienst- und Medienrecht, sowie meine Stellungnahme zu einem Gesetzentwurf der Bundesregierung zur Weiterentwicklung der gesetzlichen Krankenversicherung.

- Zu den Absichten, Möglichkeiten zur akustischen Wohnraumüberwachung einzuführen, habe ich zusammen mit den anderen Datenschutzbeauftragten des Bundes und der Länder folgende Begrenzungsmaßnahmen gefordert, die angesichts des tiefen Eingriffs in die Intimsphäre erforderlich sind:
  - engere Begrenzung der Einsatzvoraussetzungen - durch einen wesentlichen schlankeren Straftatenkatalog - und des Einsatzumfanges;
  - bessere verfahrensmäßige Sicherungen bei der Einsatzanordnung - grundgesetzlich abgesicherte Genehmigung durch ein Richterkollegium - und bei der nachgehenden Kontrolle; Kontrolle auch durch aussagekräftige Berichterstattung gegenüber der Öffentlichkeit;

- Einsatz nur als letztes Mittel und unter größtmöglicher Schonung Dritter;
- strenge Zweckbindung der gewonnenen Erkenntnisse;
- regelmäßige Prüfung anhand einer Erfolgskontrolle über die weitere Notwendigkeit dieses Fahndungshilfsmittels.

In diesem Sinn haben sich die Datenschutzbeauftragten des Bundes und der Länder an die Entscheidungsträger gewandt. Ich möchte dabei nicht verhehlen, daß ich, zusammen mit einigen anderen Datenschutzbeauftragten, die Einführung des Großen Lauschangriffs angesichts der von der Polizei dargelegten Notwendigkeit dieses Fahndungshilfsmittels für vertretbar halte, wenn Begrenzungs- und Sicherungsmaßnahmen in obigem Sinn eingeführt werden. Derartige Begrenzungen und Sicherungen halte ich aber für zwingend erforderlich.

- Sicherheitsüberprüfungsgesetz

Mit dem zur Zeit dem Bayerischen Landtag zur Beschlußfassung vorliegenden Sicherheitsüberprüfungsgesetz (SÜG) sollen u. a. die rechtlichen Voraussetzungen für die Maßnahmen des Landesamts für Verfassungsschutz im Bereich seiner Mitwirkung bei Sicherheitsüberprüfungen im einzelnen geschaffen werden. Ich bin im Zuge der Erstellung des Entwurfs beteiligt worden. Eine Reihe meiner Vorschläge, u. a. zur klaren Begrenzung der Datenerhebungs- und Verarbeitungsbefugnisse, wurde in den Entwurf übernommen. Offen sind Forderungen meinerseits zur besseren Absicherung, daß die bei der Sicherheitsüberprüfung gewonnenen Erkenntnisse grundsätzlich nur für diese Zwekke verwendet werden. Ausnahmen von diesem verfassungsrechtlich statuierten Zweckbindungsgrundsatz halte ich nur dann für vertretbar, wenn es um überragend wichtige Angelegenheiten der Allgemeinheit geht. Ich habe mich deshalb für eine Beschränkung der vorgesehenen Ausnahmen vom Zweckbindungsgrundsatz eingesetzt.

- Bayerisches Ergänzungsgesetz zum Schwangeren- und Familienhilfegesetz des Bundes

Hier habe ich mich dafür eingesetzt, daß die von der Schwangeren angegebenen Gründe nicht dokumentiert werden, sowie für ein Verfahren, welches ohne Offenlegung der Umsatzzahlen des Arztes gegenüber der Kontrollbehörde auskommt. Beides wurde über-

nommen, letzteres durch die Möglichkeit des Nachweises der Einhaltung der Grenzen durch die Bestätigung eines Wirtschafts- oder Steuerberaters. Eine Einsichtnahme in patientenbezogene Unterlagen kommt nach den Regelungen des Gesetzes nicht in Betracht.

- Telekommunikations-, Teledienst- und Medienrecht

  Zusammen mit den anderen Datenschutzbeauftragten des Bundes und der Länder habe ich möglichst datenschutzfreundliche Regelungen gefordert. Diese wurden in das Telekommunikationsgesetz sowie in die vorliegenden Entwürfe eines Teledienstgesetzes und eines Medienstaatsvertrages zu einem großen Teil übernommen. Besonders hervorheben möchte ich hier die Bestimmungen in den letztgenannten Entwürfen, wonach die Anbieter von Teledienst- und Mediendienstleistungen, soweit technisch möglich und zumutbar, zumindestens alternativ auch die Möglichkeiten einer anonymen Nutzung dieser Dienste anbieten sollen, d. h. ohne daß personenbezogene Datenspuren beim Dienstleister verbleiben. Hier wird es darauf ankommen, inwieweit dieser Ansatz der datensparsamen Nutzung tatsächlich umgesetzt und inwieweit er vom Verbraucher angenommen wird.

- Gesetzentwurf zur Weiterentwicklung der gesetzlichen Krankenversicherung

  Der Gesetzentwurf über Modellvorhaben zur "Weiterentwicklung der Versorgung" war zunächst im Vermittlungsverfahren gescheitert. Ich hatte gegenüber dem Bundesbeauftragten für den Datenschutz zur Vermeidung von personenbezogenen Versichertenkonten angeregt, daß Angaben über Versicherte nur fallbezogen, nicht versichertenbezogen verarbeitet werden dürften. Im Gesetzentwurf war immerhin eine schriftliche Einwilligung der Betroffenen zu diesen Datenverarbeitungen vorgesehen.

  Im nunmehrigen Gesetzentwurf eines Zweiten GKV-Neuordnungsgesetzes wird diese Einwilligung nicht mehr vorgesehen. Vielmehr sollen die Krankenkassen die für die Durchführung des Modellvorhabens erforderlichen personenbezogenen Daten nutzen dürfen, die Leistungserbringer sollen entsprechende Befugnisse zur Offenbarung von Patientendaten gegenüber den Kassen haben. Eine Zweckbindung ausschließlich für Nutzung für Modellvorhaben ist aus dem Entwurf nicht erkennbar. Diese Entwicklung ist äußerst bedenklich.

1.4 Stellungnahmen zu Einrichtungs-übergreifenden EDV-Verfahren

Neben dem von mir bereits erwähnten Dienststellen-übergreifenden staatsanwaltschaftlichen Informationssystem STARIS nenne ich hier die beratende Mitwirkung meines technischen Referats bei der Einrichtung eines bayerischen Behördennetzes. Wir haben uns hier vor allem dafür eingesetzt, daß durch die Einrichtung dieses Netzes die Sicherheit, Vertraulichkeit und Nachweisbarkeit der behördeninternen Datenübermittlung nicht verschlechtert wird. Wir haben dazu die entsprechenden Verschlüsselungs-, Abschottungs-, Identifizierungs- und Dokumentationssysteme gefordert.

Bei dieser Gelegenheit weise ich darauf hin, daß die datenschutzrechtliche Verantwortlichkeit nach Art. 25 Bayerisches Datenschutzgesetz bei den jeweiligen Institutionen liegt. Ich wirke gern beratend bei der Einführung von solchen neuen Systemen mit, die beratende Mitwirkung ändert aber nichts daran, daß die jeweiligen Dienststellen selbst für ihren Bereich das Einhalten der Forderungen des Bayerischen Datenschutzgesetzes sowie anderer Rechtsvorschriften über den Datenschutz sicherzustellen haben. Wie ich in meinem Positionspapier "Aktuelle Aspekte des Datenschutzes" vom Mai 1996 ausgeführt habe, ist Datenschutz Unternehmensaufgabe, bzw. Aufgabe der jeweiligen Dienststellen, und nicht nur Sache des Landesbeauftragten für den Datenschutz.

1.5 Regelmäßige Prüfungen, Anlaßprüfungen, Eingaben

In den vergangenen zwei Jahren fanden wieder zahlreiche Prüfungen - regelmäßig und aus besonderem Anlaß - bei staatlichen Stellen, Kommunen und kommunalen Dienststellen, bei öffentlichen Körperschaften und bei weiteren Stellen statt, die meiner Prüfungskompetenz unterliegen. Das geht von Polizeidienststellen, einer Staatsanwaltschaft, zwei Justizvollzugsanstalten, dem Landesamt für Verfassungsschutz, zwei Krankenhäusern, einer Krankenkasse und dem medizinischen Dienst der Krankenkassen, über diverse Steuerämter, Staatliche Lotterieverwaltung, die Personalverwaltungen diverser staatlicher und kommunaler Dienststellen bis hin zur Bayerischen Medien-Service-Gesellschaft. Die Prüfungen betrafen sowohl den rechtlichen wie auch den technisch-organisatorischen Bereich im Hinblick auf technische Maßnahmen für den Datenschutz und die Datensicherheit. Daneben bin ich wieder zahlreichen einzelnen datenschutzrechtlichen Fragen aufgrund von Bürgereingaben nachgegangen. Ein erheblicher Teil der Eingaben betraf den privaten Bereich, für dessen Datenschutzkontrolle ich rechtlich nicht zuständig bin. Diese Eingaben habe ich jeweils an die zuständigen Aufsichtsbehörden weitergeleitet.

Ein allgemeines Prüfungsfazit zu ziehen, ist schwierig. Zu unterschiedlich sind die Erfahrungen in den einzelnen Prüfungen. In Teilbereichen habe ich wachsende Bereitschaft festgestellt, Datenschutzgesichtspunkte vermehrt zu berücksichtigen, wenn auch manchmal erst nach langen Diskussionen. Wie nicht anders zu erwarten, lassen sich nicht alle Vorschläge durchsetzen, wobei ich darin jedenfalls dann kein strukturelles Problem sehe, soweit über das Grundanliegen und die Berechtigung datenschutzrechtlicher Belange Einigkeit besteht.

In diesem zusammenfassenden Abschnitt kann ich nur einige besondere Problemkomplexe herausstellen, die mir geeignet erscheinen, auf die Situation des Datenschutzes in Bayern Schlaglichter zu werfen.

- In technisch-organisatorischer Richtung, d. h. in der Frage des technischen Datenschutzes und der Datensicherheit, haben meine Mitarbeiter vor allem im Bereich von nachgeordneten Dienststellen und bei den geprüften Kommunen leider wieder teilweise erhebliche Mängel festgestellt. Das erscheint mir besonders problematisch im Hinblick auf die immer weiter zunehmende Datenverarbeitung und auch im Hinblick auf die neuartigen Gefährdungen bei der

Nutzung der neuen IuK-Techniken. Ich betone hier nochmals meinen Hinweis aus obigem Abschnitt, daß Datenschutz auch zu den wesentlichen Aufgaben der datenverantwortlichen Dienststelle gehört und daß dafür auch die notwendigen Mittel aufgebracht werden müssen. Ich unterstreiche den Satz meines Kollegen Bäumler aus Schleswig-Holstein: "Datenschutz muß Chefsache sein."

- Für neu eingeführte, immer tiefer in das informationelle Selbstbestimmungsrecht eingreifende Datenerhebungsbefugnisse halte ich Erfolgskontrollen für notwendig, die Schlüsse darauf ermöglichen sollen, ob der damit angestrebte Zweck - mit dem sie gerechtfertigt wurden - wirklich erreicht wird. So hat das Staatsministerium des Innern meine Anfrage, in welchem Umfang im Verhältnis zur Gesamtzahl bei den neuen anlaßlosen polizeilichen Identitätskontrollen ("Schleierfahndung") wirklich Fälle der internationalen organisierten Kriminalität aufgegriffen wurden, mit dem Argument abgetan, hierzu würden keine Statistiken geführt und die Zuordnung einer bestimmten Maßnahme zu einem bestimmten Erfolg sei methodisch fragwürdig. Ich bedaure diese Auffassung und meine, daß meine Frage durchaus beantwortet werden könnte.

- Bei meinen Prüfungen im Polizeibereich habe ich festgestellt, daß zwei wesentliche Datenverarbeitungsmaßnahmen aufgenommen wurden, obwohl die Errichtungsanordnungen noch nicht vorlagen bzw. noch nicht in Kraft gesetzt worden waren. Mit den Errichtungsanordnungen wird im einzelnen festgelegt, wer von der Datenverarbeitung in welchem Umfang und für welche Dauer erfaßt werden kann. Sie sind deshalb wesentlich für die Abgrenzung der konkreten Datenverarbeitungsbefugnisse. Im einzelnen wurde die Errichtungsanordnung für die Arbeitsdatei Geldwäsche erst geraume Zeit nach Speicherungsbeginn in Kraft gesetzt, damit erhielten wir von den Verarbeitungen auch zunächst keine Kenntnis; weiter fehlte die Errichtungsanordnung für eine Datei für gewaltbereite Personen aus dem Extremismusbereich. Bei dem wichtigen Datenverarbeitungssystem AFIS, dem automatischen Fingerabdruckidentifizierungssystem der Polizei - wofür allerdings der Bund zuständig ist - fehlt die Anordnung ebenfalls. Zu den genannten fehlenden Errichtungsanordnungen aus dem bayerischen Bereich weise ich darauf hin, daß es sich um Einzelfälle aufgrund besonderer Umstände handelt, die nicht zu verallgemeinern sind. Gleichwohl erscheinen sie mir wegen der wesentlichen Funktion der Errichtungsanordnung für die genaue Abgrenzung der Datenverar-

beitungsbefugnisse auch an dieser Stelle erwähnenswert. So habe ich bei der Errichtungsanordnung für eine bayerische Staatsschutzdatei auf eine klare Abgrenzung zu den Aufgaben des Verfassungsschutzes gedrungen. Das Staatsministerium des Innern hat meine Forderungen übernommen. Im übrigen hatte ich bei meinen Prüfungen im Polizeibereich zwar Anlaß zu einer Reihe von Einzelbemerkungen, ich hatte aber keine strukturellen Mängel vermerken müssen. Ich konnte im Gegenteil erfreulicherweise wiederum bei den Prüfungen der Polizeidienststellen große Bereitschaft zur Berücksichtigung auch der datenschutzrechtlichen Anforderungen feststellen.

- Die gleiche positive Tendenz in der Bereitschaft, meine Forderungen aufzugreifen, ergab sich im Bereich des Landesamts für Verfassungsschutz (LfV) zum Komplex "Mitwirkung bei Sicherheitsüberprüfungen". Hier hatte ich bei der vorletzten Prüfung zum Teil mißverständliche, zum Teil unerhebliche, d. h. überflüssige Feststellungen aufgegriffen. Das LfV ist zu einer Umstellung des Erhebungssystems mit dem Ziel des Vermeidens dieser Mängel bereit und hat bereits mit Umsetzungsmaßnahmen begonnen. Das LfV hat auf meine Bedenken im Bereich seiner Beteiligung bei der Bekämpfung der Organisierten Kriminalität zu Fragen der Festlegung des betroffenen Personenkreises, der Speicherkriterien und der Speicherfristen berücksichtigt. Kritisch habe ich bei meiner letzten Prüfung im LfV festgestellt, daß einzelne Personen im Zusammenhang mit dem Weltwirtschaftsgipfel 1992 in der Sachbearbeitung dienenden Unterlagen gespeichert sind, ohne daß mir für diese Personen Extremismuserkenntnisse genannt werden konnten. Die für eine abschließende Bewertung notwendige Stellungnahme des LfV liegt mir noch nicht vor.

- Im Gesundheitsbereich muß den Outsourcing-Tendenzen große Aufmerksamkeit gewidmet werden. Sie gewinnen aus wirtschaftlichen Gründen immer größere Bedeutung, sie dürfen aber nicht dazu führen, daß dadurch das Arztgeheimnis ausgehöhlt wird. Ich hatte verschiedene Stellen auf Anfragen zur Frage der datenschutzgerechten Gestaltung von Outsourcing-Maßnahmen beraten, teilweise mußte ich auch Bedenken erheben.

- Im Bereich der Datenverarbeitung in den sozialen Sicherungssystemen waren die informationellen Beziehungen zwischen Leistungserbringern und gesetzlichen Krankenkassen ein Schwerpunkt meiner Arbeit. Hier gibt es vor allem zwei Probleme: Das Sicherstellen der

Einhaltung der gesetzlichen Grenzen der Übermittlung von Abrechnungsdaten von Leistungserbringern zu gesetzlichen Krankenkassen und die sichere Gestaltung des technischen Übermittlungsvorganges. Zur Datenübermittlung von kassenärztlichen bzw. -zahnärztlichen Vereinigungen an die Krankenkassen habe ich mich oben bereits geäußert. Die gesetzliche Regelung hat hier zum Ziel, daß bei den Kassen kein patientenbezogenes "Gesundheits-" oder "Krankheits"-Konto entsteht. Der "gläserne Patient" bei den gesetzlichen Krankenkassen will vom Gesetz verhindert werden. Dafür enthält das Gesetz die Vorschrift, daß Abrechnungsdaten (mit den Diagnosen) nur fallbezogen, nicht versicherten-, also nicht patientenbezogen, übermittelt werden dürfen. Bei einer Prüfung einer AOK-Direktion habe ich festgestellt, daß meiner Forderung Rechnung getragen wird, aus der von mir bereits beanstandeten übergangsweise noch durchgeführten (auch) versichertenbezogenen Übermittlung von Abrechnungsdaten kein versichertenbezogenes Leistungskonto aufzubauen.

Zweiter Schwerpunkt in diesem Bereich war die technische und organisatorische Sicherstellung von Datenschutz und Datensicherheit bei der Übermittlung von patientenbezogenen Daten online oder über Datenträger von Leistungserbringern über kassenärztliche bzw. -zahnärztliche Vereinigungen an Krankenkassen. Die Diskussion hierüber dauert noch an.

- In einzelnen Gemeinden wurden Bürgerdaten mißbräuchlich zu von den Gesetzen nicht vorgesehenen Zwecken ausgewertet, was zu einzelnen Beanstandungen geführt hat. Auch hier möchte ich nochmals betonen, daß die einer Verwaltungsdienststelle vorliegenden Bürgerdaten grundsätzlich nur zu dem Zweck genutzt werden dürfen, zu dem sie erhoben worden sind. Ausnahmen von diesem für den Datenschutz wesentlichen Zweckbindungsgrundsatz sind nur in den Fällen zulässig, in denen sie vom Gesetz im überwiegenden Allgemeininteresse zugelassen sind. Werden diese Daten, z. B. Namen von Bürgern auf Eintragungslisten für Volksbegehren oder Bürgerbegehren, zu anderen Zwecken genutzt, z. B. zu vom Gesetz nicht vorgesehenen Auswertungen über das Wahlverhalten oder über die Frage, inwieweit sich Gemeindebedienstete an Bürgerbegehren beteiligen, so mußte ich das beanstanden.

- Schließlich möchte ich noch drei spektakuläre Einzelfälle erwähnen, auf die ich zum Teil durch die Presse, zum Teil von einem Mitglied des Bayerischen Landtags aufmerksam gemacht worden bin:

- Bei einem Privatbetrieb ging seit Jahren fehlerhaft per Fax Post an ein Amtsgericht mit zum Teil vertraulichen Unterlagen ein, zuletzt ein 40-seitiges Protokoll einer Telefonüberwachungsmaßnahme nach der Strafprozeßordnung. Dieser Fall zeigt die Sicherheitsrisiken, die mit der Versendung per Fax verbunden sind. Ich habe das zum Anlaß genommen, gegenüber den Staatsministerien allgemein auf die notwendige Sorgfalt im Umgang mit dem Fax hinzuweisen und gegenüber den Staatsministerien des Innern und der Justiz speziell auf die Problematik des Versendens derartig vertraulicher Unterlagen über Fax einzugehen.

- Das Staatsministerium des Innern lehnte es zunächst ab, einem fremdsprachigen, vom Bundesinnenministerium im Zusammenhang mit der Rückführung vietnamesischer Staatsangehöriger vorgegebenen Fragebogen, dessen Ausfüllung mit zum Teil sensiblen personenbezogenen Daten unbestritten freiwillig war, einen klaren Hinweis auf diese Freiwilligkeit ebenfalls in der fremden Landessprache beizufügen. Die Amtssprache sei deutsch, derartige fremdsprachige Hinweise könnten bei der Vielzahl von Datenerhebungen im Ausländerbereich nicht geleistet werden. Ich habe diese Weigerung beanstandet, da eine klare Information des Betroffenen über die Freiwilligkeit seiner Angaben essentiell für seine Entscheidung ist, die Fragen zu beantworten oder dies zu unterlassen. Zudem sehe ich nicht ein, warum umfangreiche Fragen in der fremden Sprache gestellt werden können, der einfache Hinweis aber, daß die Beantwortung dieser Fragen freiwillig ist, nicht möglich sein soll.

  Das Staatsministerium des Innern hat inzwischen einen entsprechenden Hinweis bei derartigen fremdsprachigen Fragebögen "im Rahmen des rechtlich und tatsächlich Möglichen" für die Zukunft zugesagt.

- Zu großer weiterer Presseresonanz haben schließlich Berichte über angebliche Kontrollmaßnahmen gegenüber Bewohnern einer Asylbewerber-Erstaufnahmeeinrichtung in einer oberbayerischen Stadt geführt. Ich bin diesen Vorwürfen nachgegangen, habe dabei eine Observierungsmaßnahme außerhalb der Einrichtung durch den Leiter des dort eingesetzten Wachdienstes, die der verantwortlichen Regierung allerdings nicht zugerechnet werden konnte, kritisiert und die Frage weiterer Kontrollmaßnahmen innerhalb des Heimes untersucht. Dabei konnte ich trotz entsprechender Hinweise bei einem Ortstermin nicht mit

letzter Sicherheit feststellen, daß unzulässige, rein vorbeugende An- und Abwesenheitskontrollen stattgefunden haben. Im Laufe meiner Befassung mit dieser Erstaufnahmeeinrichtung wurde ich aber auf einen Fall einer Briefkontrolle aufmerksam gemacht. Nach meiner Überzeugung hatte der Betroffene einen an ihn gerichteten Brief nicht freiwillig einem Angehörigen des Wachdienstes übergeben. Dies habe ich beanstandet.

1.6 Zusätzliche Arbeitsschwerpunkte

Zusätzliches Schwergewicht neben der allgemeinen Prüfungs- und Beratungstätigkeit habe ich im Berichtszeitraum auf die datenschutzrechtliche Begleitung der neuen Informationstechnologien gelegt. Ich habe dazu ein Positionspapier "Aktuelle Aspekte des Datenschutzes" verfaßt, das ich Anfang 1996 den Mitgliedern der Bayerischen Staatsregierung und den Fraktionen des Bayerischen Landtags übergeben habe. Ich habe darin besonders auf die Tatsache hingewiesen, daß mit der Nutzung der neuen IuK-Techniken regelmäßig das Hinterlassen von Datenspuren auf den Rechnern der Netzbetreiber und Diensteanbieter verbunden ist und habe Regelungen und Maßnahmen gefordert, die die Nutzung dieser Daten grundsätzlich auf das zur Betriebsabwicklung Erforderliche begrenzen. Zudem hatte ich mich in dem Positionspapier für die Entwicklung einer datenschutzfreundlichen Technik eingesetzt. Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat sich mit diesen Fragen bereits sehr frühzeitig befaßt und auf den letzten Konferenzen entsprechende Beschlüsse gefaßt.

Die Gedanken dieser Beschlüsse haben in die Datenschutzregelungen des neuen Telekommunikationsrechts und in die Entwürfe eines Teledienstgesetzes und eines neuen Medien-Staatsvertrages Eingang gefunden.

Zusammenfassend erscheinen mir die Datenschutzprobleme, die sich im Zusammenhang mit der Nutzung der modernen IuK-Technik - die sich weltweit abspielt - ergeben, eine der Hauptfragen zu sein, mit denen sich der Datenschutz in Zukunft auseinanderzusetzen hat.

1.7 Teilnahme an nationalen und internationalen Datenschutzkonferenzen

Wie bereits im Jahr 1994 habe ich auch in den vergangenen beiden Jahren wieder an den internationalen Datenschutzkonferenzen, diesmal Kopenhagen und Ottawa, und an den Konferenzen der Datenschutzbeauftragten des Bundes und der Länder in Deutschland teilgenommen. Wesentliches Thema der Konferenzen waren u. a. die oben skizzierten Fragen im Zusammenhang mit der Nutzung der Informations- und Kommunikationstechnik, wobei dazu vor allem von der internationalen Konferenz in Kopenhagen wesentliche Anregungen ausgingen. Bei dieser Konferenz wurden Verfahren vorgestellt, wie unter Zuhilfenahme der modernen Datenverarbeitungstechnik datenschutzfreundliche Lösungen für die Nutzung der digitalisierten IuK-Technik gefunden werden können. Diese Anregungen wurden von der deutschen Datenschutzkonferenz aufgegriffen und werden jetzt in einer Arbeitsgruppe des Arbeitskreises Technik dieser Konferenz unter bayerischer Federführung weiter verfolgt.

Die Zusammenarbeit in den genannten Konferenzen, besonders in der Konferenz der Datenschutzbeauftragten des Bundes und der Länder ist ausgezeichnet. Es haben sich in allen Fällen konsensfähige Lösungen zu teilweise schwierigen Problembereichen finden lassen. Auch hier kann ich als Beispiel die Haltung der 52. Datenschutzkonferenz zum Thema "Lauschangriff" oder zum Thema "Neue Eingriffsinstrumente der Strafverfolgungsbehörden im Bereich der modernen Informationstechnologie" nennen.

Vorstehende Zusammenfassung konnte und sollte nur einen allgemeinen Überblick über die wesentlichen Fragen des Berichtszeitraumes geben. Wegen der Einzelheiten darf ich auf nachstehende Abschnitte verweisen.

---

2. Allgemeines Datenschutzrecht

2.1 Verabschiedung der EG-Datenschutzrichtlinie

Die EG-Datenschutzrichtlinie vom 24.10.1995 muß bis 24.10.1998 in Bundes- und dann in Landesdatenschutzrecht umgesetzt sein. Der knappe zeitliche Rahmen muß intensiv genutzt werden, damit die anstehenden Probleme gelöst werden und nicht nur eine Minimallösung gesucht wird.

Am 24.10.1995 wurde die EG-Datenschutzrichtlinie endgültig verabschiedet. Die Richtlinie soll sowohl der Erleichterung des Waren- und Dienstleistungsverkehrs innerhalb der Gemeinschaft dienen, wie auch der Sicherung der Grundrechtsposition, insbesondere hinsichtlich der Achtung der Privatsphäre.

Die Richtlinie ist in drei Jahren umzusetzen. Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat unter meiner Beteiligung im Frühjahr 1996 eine detaillierte Entschließung verabschiedet, die als Anlage 1 zu diesem Tätigkeitsbericht abgedruckt ist.
Bis Ende 1998 ist die Richtlinie auch in Bayern umzusetzen. Angesichts dieser knappen Zeitvorgabe besteht die Gefahr, daß das jetzt geltende Recht nur in den wichtigsten Punkten geändert wird. Dies hielte ich für unzureichend und gefährlich. Die Novellierung muß vor allem Antworten auf die Fragen finden, die sich durch die technische Entwicklung ergeben haben. Dabei muß der inzwischen eingetretenen technischorganisatorischen Entwicklung Rechnung getragen werden, die sich vor allem durch die Stichworte "Miniaturisierung" und "Vernetzung" charakterisieren läßt. Die am Beispiel des Internet sichtbar werdenden Probleme lassen erst erahnen, welche Fragen die explosionsartig zunehmende Vernetzung in der Zukunft noch aufwerfen wird. Dabei muß auch die Frage gestellt werden, inwieweit das Schutzniveau im privaten Bereich zu verbessern ist.

Bei der Umsetzung der Richtlinie beschränkt sich der gesetzgeberische Handlungsbedarf nicht auf den Bereich, den die allgemeinen Datenschutzgesetze regeln. Auch alle bereichsspezifischen Vorschriften müssen daraufhin überprüft werden, ob sie den Vorgaben der Richtlinie genügen. Der damit verbundene Aufwand ist erheblich. Um so dringender ist es, sich dieser Aufgabe unverzüglich zu stellen.

Um den in Bayern bestehenden Handlungsbedarf zu verdeutlichen, habe ich die erwähnte Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder sowohl an den Bayerischen Staatsminister des Innern als auch an den Leiter der Bayerischen Staatskanzlei übersandt. Staatsminister Dr. Beckstein hat in seiner Antwort auf die zeitliche Problematik und auf die Notwendigkeit hingewiesen, daß zunächst der Bund rasch das Bundesdatenschutzgesetz novelliere, da ansonsten die Länder nicht einerseits den Umsetzungstermin 24.10.1998 einhalten und andererseits die Orientierung am Bundesdatenschutzgesetz wahren könnten.

Dafür habe ich Verständnis. Es wäre höchst unerwünscht, wenn sich Bundes- und Landesrecht in wichtigen Punkten auseinander entwickeln würden. Sollte der Bund allerdings die Novellierung des Bundesdatenschutzgesetzes nicht mit der gebotenen Eile durchführen, bestünde gleichwohl eine Handlungspflicht für den bayerischen Gesetzgeber.

Wenig erfreulich ist es, daß die Europäische Union bisher für ihren eigenen Bereich, also insbesondere auch für die Behörden der Europäischen Kommission, noch keine Datenschutzvorschriften geschaffen hat. Sofern sich dieser Zustand nicht ändert, würde das die Glaubwürdigkeit der mit der EG-Datenschutzrichtlinie angestrebten Ziele beeinträchtigen. Ich habe eine entsprechende Entschließung der Konferenz der Europäischen Datenschutzbeauftragten mit der Bitte um Unterstützung an die Bayerische Staatsregierung übermittelt. Wie mir Herr Staatsminister Dr. Beckstein mitgeteilt hat, hat sich die deutsche Delegation, die in der Datenschutzgruppe nach Art. 29 der EG-Datenschutzrichtlinie vertreten ist, in den Sitzungen dieser Gruppe nachhaltig dafür ausgesprochen, verbindliche Datenschutzvorschriften für die Verwaltungsbehörden der Europäischen Union zu schaffen. Da die Forderung auch von anderen Mitgliedern der Gruppe erhoben wurde, hoffe ich, daß in absehbarer Zeit die gebotenen Vorschriften vorhanden sein werden.

Falls ein Grundrechtskatalog auf europäischer Ebene geschaffen wird, erscheint es geboten, in diesen Katalog auch ein europäisches Grundrecht auf Datenschutz aufzunehmen. Dies hat die Konferenz der Datenschutzbeauftragten der Europäischen Union bei ihrer Konferenz in Kopenhagen am 08. September 1995 auf Vorschlag der deutschen Delegation mit meiner Zustimmung gefordert (siehe dazu auch die als Anlage 3 abgedruckte Entschließung der Konferenz der Daten-

schutzbeauftragten des Bundes und der Länder vom November 1995).

Sofern bei der Datenschutzaufsicht übertriebener Bürokratismus bei den Meldepflichten gemäß Art. 18 der EG-Datenschutzrichtlinie vermieden werden soll, wird es erforderlich sein, zumindest vom Grundsatz her bei allen bayerischen öffentlichen Stellen die Berufung interner Datenschutzbeauftragter gesetzlich vorzuschreiben. Nur dann kann nämlich die Bestimmung des Art. 18 Abs. 2 2. Spiegelstrich der EG-Datenschutzrichtlinie zur Anwendung kommen, wonach unter dieser Voraussetzung Ausnahmen von der Meldepflicht oder Vereinfachungen der Meldung vorgesehen werden können. Zusätzliche Belastungen für die öffentlichen Stellen werden damit durchweg nicht verbunden sein. Schon jetzt schreibt die Vollzugsbekanntmachung zum Bayerischen Datenschutzgesetz für staatliche öffentliche Stellen unter gewissen Voraussetzungen interne Datenschutzbeauftragte vor. Im kommunalen Bereich, für den lediglich eine entsprechende Empfehlung gilt, haben zumindest alle größeren Kommunen dieser Empfehlung Rechnung getragen, weil ihnen die Wichtigkeit dieser Funktion aus den täglichen Erfahrungen im Umgang mit dem Bürger bekannt ist.

2.2 Datenschutz bei Einwilligung

Problem der Zwangslage bei Abgabe von Einwilligungen, des Umfanges der Einwilligung, von Einwilligungen "auf Vorrat" sowie der Information vor Einwilligung

Der Umgang mit personenbezogenen Daten in Form der Erhebung, Verarbeitung oder Nutzung ist nur zulässig, wenn hierfür entweder eine gesetzliche Rechtsgrundlage besteht oder aber der Betroffene in die Erhebung, Verarbeitung oder Nutzung in rechtswirksamer Weise eingewilligt hat (vgl. Art. 15 Abs. 1 BayDSG). Eine wirksame Einwilligung des Betroffenen hat also denselben rechtlichen Stellenwert wie eine ausdrückliche Befugnis, die der Gesetzgeber einer öffentlichen Stelle einräumt.

Diese Gleichsetzung erweist sich im Einzelfall immer wieder als problematisch. Während der Gesetzgeber bei der Schaffung einer gesetzlichen Befugnis für die Erhebung, Verarbeitung oder Nutzung von personenbezogenen Daten die berührten Belange gegeneinander abwägen und zu einem angemessenen Ausgleich bringen muß und kann, sieht sich der Betroffene bei der Erteilung einer Einwilligung häufig in einer mehr oder weniger stark empfundenen Zwangslage, die es ihm nicht mehr ohne weiteres ermöglicht, sein Persönlichkeitsrecht angemessen zur Geltung zu bringen.

Dies gilt in der Praxis vor allem dann, wenn der Betroffene die Gewährung finanzieller Leistungen durch öffentliche Stellen erreichen will, deren Bewilligung an den Nachweis bestimmter Voraussetzungen gebunden ist, oder wenn er sich um die Einstellung in ein Arbeits- oder Dienstverhältnis bemüht und den Nachweis führen muß, daß er die Einstellungsvoraussetzungen erfüllt. Rein formal betrachtet steht es dem Betroffenen in solchen Fällen frei, ob er zum Nachweis der geforderten Voraussetzungen eine Einwilligung in die Erhebung, Verarbeitung oder Nutzung seiner personenbezogenen Daten erteilt. Faktisch betrachtet befindet er sich jedoch in einer Zwangslage, da ihm die begehrten Leistungen oder die erstrebte Einstellung mit hoher Wahrscheinlichkeit verweigert werden, wenn er die Einwilligung nicht erteilt und er die geforderten Nachweise nicht anderweitig erbringen kann.

Patentlösungen sind angesichts der Vielfältigkeit der Problematik nicht möglich. Wo immer dies durchführbar erscheint, sollten eindeutige gesetzliche Rechtsgrundlagen geschaffen werden, die das Einholen von Einwilligungen überflüssig machen.

Sofern das Einholen einer Einwilligung des Betroffenen nicht zu umgehen ist, müssen sich **Inhalt und Reichweite** der Einwilligung **strikt an den Aufgaben** der öffentlichen Stelle orientieren. Ein Umgang mit personenbezogenen Daten kann von vornherein nur insoweit erforderlich sein, wie er von den Aufgaben der öffentlichen Stelle gedeckt ist. Daten, **die zur Aufgabenerfüllung nicht erforderlich sind,** dürfen **auch nicht auf der Grundlage einer Einwilligung des Betroffenen erhoben, verarbeitet oder genutzt** werden. So dürfen z.B. Gesundheitsdaten, die für die Entscheidung über eine Einstellung nicht erforderlich sind, von einer Einstellungsbehörde auch dann nicht erhoben werden, wenn der Bewerber darin eingewilligt hat. Die Erhebung, Verarbeitung oder Nutzung wäre trotz Vorliegens einer Einwilligung des Betroffenen rechtswidrig. Ebenso wäre es rechtswidrig, wenn sich eine öffentliche Stelle in einer Vielzahl von Fällen Einwilligungen erteilen läßt, obwohl von vornherein absehbar ist, daß sie von diesen Einwilligungen nur in wenigen Einzelfällen Gebrauch machen muß. Das Einholen solcher "Einwilligungen auf Vorrat" wäre mit dem Übermaßverbot nicht zu vereinbaren.

Besonderes Gewicht kommt beim Einholen einer Einwilligung der Information des Betroffenen zu - Informed consent - (vgl. dazu vor allem Art. 15 Abs. 2 BayDSG). Insbesondere ist der Zweck einer Datenerhebung und einer vorgesehenen Übermittlung genau und nicht nur formelhaft zu bezeichnen. Nur so kann der Betroffene prüfen, ob der vorgesehene Zweck es aus seiner Sicht rechtfertigt, in den Umgang mit seinen personenbezogenen Daten einzuwilligen.

3. Gesundheitswesen

3.1 Informationstechnologie im Gesundheitswesen

3.1.1 Chipkarten im Gesundheitswesen

Bemühungen um einen datenschutzgerechten Einsatz von freiwilligen Gesundheitskarten der verschiedensten Art sind heute weltweit in allen Industriestaaten zu verzeichnen. So hat der Datenschutzbeauftragte aus Quebec bereits auf der Internationalen Datenschutzkonferenz in Den Haag im Herbst 1994 ein Pilotprojekt "Gesundheitskarte von Quebec" ("Rimonski Health Smartcard Project") vorgestellt, das den Informationsfluß zwischen den Kartenbenutzern und den Angehörigen der medizinischen Berufe verbessern soll. Das Projekt geht von einer freiwilligen Beteiligung der Betroffenen aus. Wie ich bei der Präsentation des Vorhabens und aus dem inzwischen vorliegenden Abschlußbericht des Projekts feststellen konnte, nahmen Überlegungen zu Datenschutzfragen bei der Konzeption des Vorhabens und seiner Durchführung erheblichen Raum ein. So sind die Zugriffsberechtigungen auf die gespeicherten Daten sehr differenziert nach Berufssparten und Datengruppen behandelt und die Datenschutzbehörde von Quebec hat z.B. gefordert, daß die Karten nicht für Zwecke des Arbeitgebers verwendet werden dürfen. Gerade dieser Punkt spielt auch bei der Datenschutzdiskussion in Deutschland eine wichtige Rolle. Die Europäische Kommission und die Gruppe der G 7-Staaten befassen sich gleichfalls mit dem Einsatz von freiwilligen Gesundheitskarten und berücksichtigen dabei auch die damit verbundenen Datenschutzfragen.

Wie im 16. Tätigkeitsbericht vermerkt, hat die Konferenz der Datenschutzbeauftragten des Bundes und der Länder bereits am 9./10. März 1994 einen Beschluß zu der Thematik gefaßt. Wegen der seitdem zu verzeichnenden dynamischen Entwicklung befaßte sich die Konferenz am 9./10. November 1995 in einem zweiten umfangreichen Beschluß nochmals mit dem Thema. Er ist in der Anlage 4 zu diesem Tätigkeitsbericht abgedruckt. Die wesentlichen Punkte dieser Entschließung sind folgende:

- die besondere Schutzwürdigkeit medizinischer Daten,

- die freie Entscheidung der Betroffenen über die Verwendung einer Chipkarte,

- die Forderung, daß mit der Einführung eines Chipkartensystems keine Verschlechterung des Arzt/Patientengeheimnisses verbunden sein darf, und

- die Forderung, daß die Einführung von Chipkarten nicht zur Einrichtung von zentralen Dateien mit Chipkarten-Daten führen darf.

Die Entschließung hat eine lebhafte Diskussion ausgelöst. Dies zeigt sich etwa an einer umfangreichen Stellungnahme der Bundesärztekammer. Ferner war die Entschließung Gegenstand von Gesprächen mit der Arbeitsgemeinschaft "Karten im Gesundheitswesen", in der Verbände, Institutionen und Unternehmen vertreten sind, die sich mit Chipkarten im Gesundheitswesen befassen. Die Gespräche dauern noch an. In Übereinstimmung mit meinen Kollegen beim Bund und den anderen Ländern trete ich dabei dafür ein, daß die oben genannten wesentlichen Punkte ausreichend berücksichtigt werden. Hinreichende Datenschutzvorkehrungen liegen nicht zuletzt im Interesse der Anbieter und Anwender von Chipkarten. Ohne hinreichende Datenschutzmaßnahmen dürfte die Akzeptanz solcher Karten bei den Betroffenen nur gering sein.

3.1.2 Telemedizin

Die Telemedizin eröffnet durch den schnellen Austausch von Patientendaten wesentliche, teilweise faszinierende Möglichkeiten, die Patientenbehandlung qualitativ zu verbessern. Im Rahmen der Initiative Bayern Online fördert das Bayerische Arbeits- und Sozialministerium die Entwicklung eines Bayerischen Gesundheitsnetzes. An dem entsprechenden Arbeitskreis wirke ich beratend mit. Zu den rechtlichen Voraussetzungen der Telemedizin habe ich darauf hingewiesen, daß sie nichts an den Voraussetzungen ändert, unter denen bisher die Übermittlung von Patientendaten zulässig ist. Das heißt, für die ärztliche Datenverarbeitung gegenüber dem Patienten sind maßgebend der Behandlungsvertrag, die Zustimmung des Patienten im Einzelfall, das ärztliche Berufs- und Standesrecht, die Krankenhausgesetze, in Bayern das Bayerische Krankenhausgesetz, und die Datenschutzgesetze; für das Verhältnis zwischen Arzt und gesetzlicher Krankenkasse das SGB V, und nicht zuletzt das strafrechtlich geschützte ärztliche Berufsgeheimnis.

Hieraus ergeben sich folgende Grundprinzipien:

Auch für telemedizinische Anwendungen muß Datenverarbeitung

- im Rahmen des Behandlungsvertrags erforderlich sein,
- für den Betroffenen soweit möglich durchschaubar sein,
- vom Schutz des Arztgeheimnisses abgedeckt sein,
- gewährleisten, daß Daten nur an Berechtigte übermittelt werden,
- den Anforderungen der Datensicherheit entsprechen.
- Schließlich muß die Teilnahme an großen, einrichtungsübergreifenden medizinischen IT-Systemen - jedenfalls auf der Basis der gegenwärtigen Rechtslage - freiwillig, auf der Grundlage ausreichender Information im Sinn eines "Informed consent" erfolgen.

Zu den technisch-organisatorischen Anforderungen für telemedizinische Anwendungen verweise ich auf meine Ausführungen unter Nr. 18.1.2 dieses Berichts hin.

3.2 Landesgesetz über ergänzende Regelungen zum Schwangerschaftskonfliktgesetz und zur Ausführung des Gesetzes zur Hilfe für Frauen bei Schwangerschaftsabbrüchen in besonderen Fällen

Nach den neuen gesetzlichen Vorschriften dürfen die Einnahmen aus Schwangerschaftsabbrüchen ein Viertel der Einnahmen aus der gesamten Tätigkeit einer Einrichtung nicht übersteigen, die Schwangerschaftsabbrüche vornimmt. Um die Einhaltung dieses Gebotes im erforderlichen Umfang kontrollieren zu können, müssen bei den Einrichtungen Daten erhoben werden. Die gesetzliche Regelung konnte jedoch so abgefaßt werden, daß dabei keine patientenbezogenen Daten und arztbezogene Daten nur im unvermeidlichen Umfang erhoben werden.

Das Bundesverfassungsgericht hat in seinem Urteil vom 28.05.1993 dem Gesetzgeber aufgegeben zu prüfen, ob - nach dem französischen Beispiel - der Entstehung von Einrichtungen, die sich auf Schwangerschaftsabbrüche spezialisieren, durch Begrenzung der Anzahl der Abbrüche auf einen bestimmten Anteil der insgesamt vorgenommenen ärztlichen Verrichtungen entgegengetreten werden kann. Um reine Abtreibungskliniken zu verhindern, legt das französische Gesundheitsrecht fest, daß der Anteil von Schwangerschaftsabbrüchen jährlich maximal ein Viertel der in der Einrichtung erbrachten chirurgischen Eingriffe und Entbindungen erreichen darf. Im Bayerischen Schwangerenhilfeergänzungsgesetz vom 09. August 1996 ist nach diesem Beispiel festgelegt worden, daß die Einnahmen aus den in der Einrichtung vorgenommenen Schwangerschaftsabbrüchen ein Viertel der aus der gesamten Tätigkeit der Einrichtung erzielten Einnahmen nicht übersteigen dürfen.

Zur Überprüfung, ob diese Grenze eingehalten wird, müssen Daten erhoben werden. Das Gesetz schreibt daher vor, daß die Einrichtungen der zuständigen Regierung für jedes Jahr die **Zahl** der Schwangerschaftsabbrüche und die **Summe** der für die Schwangerschaftsabbrüche vereinnahmten Vergütungen melden müssen. Insoweit findet keine patientenbezogene Datenerhebung statt. Als Nachweis zur Verifizierung dieser Angaben sieht das Gesetz die Vorlage von Belegen, insbesondere Honorar- und Abrechnungsbelegen von Sozialleistungsträgern, Krankenkassen und der Kassenärztlichen Vereinigung vor (Art. 5 Abs. 4 Satz 1 Nr. 2). Bei patientenbezogener Lei-

stungsabrechnung sind jedoch nicht die patientenbezogenen Unterlagen, sondern nur **nicht patientenbezogene** Bescheinigungen des jeweiligen Leistungsträgers vorzulegen (Art. 5 Abs. 4 Satz 1 a.E.).

Nach der Festlegung der Befugnisse der Gesundheitsämter und Regierungen in Art. 7 Abs. 1 Nr. 1 und 3, Abs. 2 und 3 des Gesetzes können **nur Auskünfte nicht patientenbezogener Art** verlangt werden und **Einsichtnahmen** nur in **nicht patientenbezogene Unterlagen** genommen werden. Die Wahrung der ärztlichen Schweigepflicht gegenüber den Patientinnen, auch in dem Verfahren zur Überprüfung der Einhaltung des 25-%-Anteils, halte ich damit für sichergestellt.

Zur Frage des Datenschutzes in bezug auf den betreffenden Arzt selbst wurde in intensiven Gesprächen mit dem Bayerischen Sozialministerium darüber Einigung erzielt, daß die Ärzte **anstelle von Angaben** über vereinnahmte Vergütungen die **Bescheinigung** eines Wirtschaftsprüfers, vereidigten Buchprüfers, Steuerberaters, Steuerbevollmächtigten oder eines Organs oder eines Mitglieds eines Organs einer Wirtschaftsprüfungs-, Buchführungs- oder Steuerberatungsgesellschaft vorlegen können, aus der sich ergibt, daß aufgrund **einer Prüfung der Buchführung die 25-%-Grenze im Kalenderjahr** nicht überschritten worden ist (Art. 5 Abs. 3 Satz 4). Ich bin der Ansicht, daß durch diese Regelung die Intensität des Eingriffs durch Datenerhebung über Einkommensverhältnisse von Ärzten unter Berücksichtigung des Verhältnismäßigkeitsgrundsatzes hinreichend eingeschränkt wurde.

Im übrigen weise ich auf die Ausführungen in meinem 16. Tätigkeitsbericht hin. Dort habe ich dargestellt, daß ich mich dafür eingesetzt habe, daß Ärzte, die Schwangerschaftsabbrüche durchführen, **nicht** die dargelegten **Gründe für den Abbruch der Schwangerschaft** dokumentieren müssen, sondern sich auf Aufzeichnungen über die **Tatsache der Darlegung** der Gründe zu beschränken haben. Dies entspricht den Ausführungen des Bundesverfassungsgerichts in der Begründung des Urteils vom 28. Mai 1993 (16. TB, Nr. 2.5, Seite 21). Art. 18 Abs. 2 Satz 3 Nr. 2 des bayerischen Heilberufe-Kammergesetzes beschränkt sich nun auf die Dokumentation der Tatsache der Darlegung der Gründe anstelle der Dokumentation der Gründe selbst.

3.3 Medizinische Forschung und Datenschutz

3.3.1 Forschungsgeheimnis

Im letzten Tätigkeitsbericht habe ich mich für die Schaffung eines Forschungsgeheimnisses - "wie beim Arzt" - mit Zeugnisverweigerungsrecht und Beschlagnahmeschutz durch Bundesgesetz eingesetzt. Seit dem letzten Bericht waren verschiedene Äußerungen zu dieser Thematik zu verzeichnen:

So wurde von rechtswissenschaftlicher Seite vor einer völligen Freigabe von Patientendaten nach Einrichtung eines solchen Forschungsgeheimnisses gewarnt, aber auch darauf hingewiesen, daß sich die "unabhängige Forschung" als Institution nicht leicht definieren läßt.

Dem ist gegenüberzustellen, daß die von mir geforderte rechtliche Absicherung von Patientendaten, die für wissenschaftliche Forschungsprojekte gespeichert werden, nicht automatisch die Freigabe der personenbezogenen Patientendaten gegenüber der Forschung zur Folge hat. Vielmehr müßte zunächst der Bundes- bzw. der Landesgesetzgeber unter Abwägung der Forschungsinteressen auf der einen und der Interessen der Patienten an der Geheimhaltung ihrer Befunde auf der anderen Seite eine entsprechende Verarbeitungsbefugnis schaffen, soweit der Patient nicht selbst einwilligt.

Die Arbeitsgemeinschaft der wissenschaftlichen medizinischen Fachgesellschaften - AWMF - vertritt in ihrer Resolution vom Sommer 1995, mit der sie eine Verbesserung des gesetzlichen Geheimnisschutzes für personenbezogene medizinische Forschungsdaten fordert, die Ansicht, daß bereits mit Einrichtung eines medizinischen Forschungsgeheimnisses automatisch eine Zustimmung des Patienten zur Forschungsnutzung seiner geheimnisgeschützten persönlichen Daten nicht mehr erforderlich sei und daß er lediglich ein Widerspruchsrecht haben solle. Ein solcher Schluß würde aber der gebotenen Abwägung zwischen Forschungsinteresse und Wahrung des Patientengeheimnisses nicht gerecht, weil pauschal jede Art von Patientendaten ohne Rücksicht auf Sensibilität freigegeben würde.

Im Rahmen der Diskussion des Forschungsgeheimnisses wurde auch die Ansicht vertreten, daß dieses überflüssig sei, weil alle Landesdatenschutzgesetze Forschungsklauseln mit Zweckbin-

dungsgeboten enthielten und die Forschungsdatennutzung "zumindest, soweit es medizinische Forschung durch ärztliches Personal betrifft", durch Beschlagnahmeverbot und Zeugnisverweigerungsrecht bereits abgesichert sei. Dem ist jedoch entgegenzuhalten, daß landesrechtliche Forschungsklauseln gegen Inanspruchnahme personenbezogener Patientendaten aufgrund bundesrechtlichen Prozeßrechts (StPO) wirkungslos sind, und daß durchaus nicht alle Daten im Bereich medizinischer Forschung durch ärztliches Personal verarbeitet werden. Außerdem erscheint es höchst zweifelhaft, ob allein der Arzt-Status (eines Forschers, der nicht auch behandelnder Arzt der Betroffenen ist) bei Verarbeitung von personenbezogenen Patientendaten für Zwecke wissenschaftlicher Forschung das Beschlagnahmeverbot und das Zeugnisverweigerungsrecht zur Folge hat. Beschlagnahmefrei sind nämlich Unterlagen nur im Gewahrsam der zur Verweigerung des Zeugnisses Berechtigten (§ 97 Abs. 2 StPO). Zur Verweigerung des Zeugnisses sind Ärzte nur über das berechtigt, "was ihnen in dieser Eigenschaft anvertraut worden oder bekanntgeworden ist" (§ 53 Abs. 1 Nr. 3 StPO). Auch die Sanktion der ärztlichen Schweigepflicht in § 203 StGB gilt für Ärzte nur, soweit ihnen Geheimnisse "als Arzt" anvertraut oder sonst bekanntgeworden sind. Höchstrichterliche Entscheidungen zur Frage, wann Daten, die ein wissenschaftliches Institut zu Forschungszwekken erhalten hat, dortigen Ärzten "als Arzt" anvertraut oder bekanntgeworden sind, sind nicht ersichtlich. Dazu kommt, daß auch für die wissenschaftliche Auswertung immer mehr statistische und Datenverarbeitungskenntnisse gebraucht werden, so daß oft die betreffenden Daten in den Händen eines Teams von Informatikern, Statistikern und Ärzten liegen. Nach meiner Auffassung kann deshalb ein Patient nur dann sichergehen, daß seine personenbezogenen Daten bei Forschern "wie beim Arzt" geschützt sind, wenn der Beschlagnahme- und Zeugnisverweigerungsschutz eindeutig auf den Bereich unabhängiger wissenschaftlicher Forschung erstreckt wird. Um dieses Patienteninteresse geht es mir, wenn ich die Einführung des medizinischen Forschungsgeheimnisses fordere.

3.3.2 Sonstige Krankheits-Registrierungen

Fehlbildungs-Registrierung durch mitbehandelnde Ärzte, Registrierung von Nierenbehandlungen zur Qualitätssicherung

- Registrierung von Fehlbildungen - "Münchner Fehlbildungskonsil"

  Im Raum München ist vorgesehen, Fehlbildungen bei Neugeborenen nach dem Vorbild eines in Mainz entwickelten Dokumentationsverfahrens ("Mainzer Modell") ärztlich zu dokumentieren. Bei der Konzeption des Münchner Vorhabens wurden meine Mitarbeiter um Beratung gebeten.

  Ein wesentliches Moment des Schutzes der personenbezogenen Daten von Kind und Eltern im "Mainzer Modell" ist, daß die Daten dort von einer **mitbehandelnden** Ärztin gesammelt und ausgewertet werden, die **ihrerseits** von den geburtshilflichen Kliniken **konsultiert** wird. Die Daten stehen daher - auch nach Ansicht des Datenschutzbeauftragten von Rheinland-Pfalz - bei der mitbehandelnden Ärztin wie beim behandelnden Arzt unter dem Schutz der ärztlichen Schweigepflicht.

  Die Daten werden in der Dokumentation ohne Namen, jedoch mit vollständigem Geburtsdatum des Kindes registriert. Auch die Klinik ist festgehalten. Da die dokumentierten Daten bei mitbehandelnden Ärzten durch Schweigepflicht, Zeugnisverweigerungsrecht und Beschlagnahmeschutz nach StGB und StPO geschützt sind, wurde dieser Anonymisierungsgrad auch für die Einführung im Münchner Raum für ausreichend erachtet. Die Anonymität der Dokumentation wird im übrigen auch dadurch verbessert, daß die örtliche Zuordnung nicht mit der Postleitzahl der elterlichen Anschrift, sondern in stärker aggregierter, mehrere Stadtbezirke umfassender Form festgehalten wird.

  Auch im Münchner Raum ist vorgesehen, daß bestimmte, besonders sachkundige Ärzte zweier großer Pädiatrischer Kliniken, die von den Entbindungskliniken konsiliarisch als (mit-)behandelnde Ärzte bei den Geburten zu Fehlbildungsfragen eingeschaltet werden, ihre Dokumentation führen und wissenschaftlich auswerten. Diese Münchner Version des

"Mainzer Modells" trägt daher auch den Namen "Münchner Fehlbildungskonsil". Eine Herausgabe von personenbezogenen bzw. nicht ausreichend anonymisierten Angaben oder Unterlagen durch diese Ärzte an andere Personen oder Stellen ist nicht vorgesehen.

Das Sozialministerium hat darauf hingewiesen, daß die Finanzierung/Realisierung des "Münchner Fehlbildungskonsils" zur Zeit noch offen ist.

- QuaSi-Niere

Um die Qualität von Nierenersatztherapien (z.B. von Behandlungen mit der sog. "künstlichen Niere") zu sichern, soll ein bundesweites Nierenbehandlungsregister aufgebaut werden, das den Projektnamen "QuaSi-Niere" trägt. Dabei ist folgendes Vorgehen geplant: Die einzelnen Behandlungseinrichtungen (z.B. Dialysezentren) liefern patientenbezogene Daten, die für die Qualitätssicherung bedeutsam sind, mittels eines Formblatts an einen **"Datentreuhänder".** Dieser **verschlüsselt** die Daten, indem an die Stelle der Patientendaten ein Pseudonym tritt, das nur dem Datentreuhänder bekannt ist. Unter diesem Pseudonym werden die Daten an eine Projektgeschäftsstelle übermittelt, die derzeit bei der Ärztekammer Berlin angesiedelt ist. Dort werden die pseudonymisierten Daten gespeichert und verarbeitet. Dadurch sollen Parameter für die Qualitätssicherung ermittelt werden, zum Beispiel, wie sich bei bestimmten Ausgangssituationen spezifische Behandlungsmethoden auf die Überlebensdauer von Patienten auswirken. Im Mittelpunkt des Interesses steht also nicht das Schicksal eines konkreten einzelnen Patienten, sondern das Schicksal von Patientengruppen. Dementsprechend sollen von der Projektgeschäftsstelle an die Behandlungseinrichtungen keine Daten zurückfließen, die sich auf konkrete einzelne Patienten beziehen, sondern nur aggregierte Daten, die Aussagen über Patientengruppen ermöglichen, z.B. Aussagen darüber, wie sich die in einer Behandlungseinrichtung übliche Behandlungsdosis auf die Behandlungsdauer auswirkt.

Ob es zur Durchführung des Projekts einer Einwilligung der Betroffenen bedarf, wird derzeit noch diskutiert. Zum Teil wird die Meinung vertreten, daß in § 137 SGB V, wonach insbesondere Krankenhäuser verpflichtet sind, sich an Maßnahmen zur Qualitätssicherung zu beteiligen, eine hinreichende gesetzliche Rechtsgrundlage vorhanden ist. Da es hierzu jedoch auch Gegenmeinungen gibt, gehe ich einstweilen davon aus, daß eine

Einwilligung der Betroffenen erforderlich ist. Im übrigen würde auch das Bestehen einer gesetzlichen Grundlage nichts daran ändern, daß eine möglichst frühzeitige Anonymisierung angestrebt werden muß.

3.3.3 Einzelne Datenschutzfragen im Zusammenhang mit Forschungsprojekten

Telefonumfragen - Daten Verstorbener - Anonymisierung

- Gesundheitsdatenerhebung durch Telefonumfragen

Aufgrund der Anfrage eines Universitätsklinikums hatte ich mich mit datenschutzrechtlichen Aspekten von Telefonumfragen für eine wissenschaftliche Fragestellung zu befassen. Ich habe für die Telefoninterviews u.a. folgende Ratschläge gegeben:

- Es muß eindeutig feststehen, für welche Stelle die Daten erhoben werden - im betreffenden Fall war dies das Hochschulklinikum.
- Vor der Datenerhebung muß dem Betroffenen der Zweck der Erhebung ausreichend verdeutlicht werden (Art. 16 Abs. 3 Satz 1 BayDSG).
- Die Befragten müssen vorab auf die Freiwilligkeit ihrer Angaben hingewiesen werden (Art. 16 Abs. 3 Satz 2 BayDSG).
- Es müssen geeignete Maßnahmen ergriffen werden um der Gefahr zu begegnen, daß Dritte, die von der telefonischen Datenerhebung erfahren, unter Vorspiegelung eines Anrufes der Universitätsklinik Personen über gesundheitliche Verhältnisse ausfragen - z.B. Rückruf der Betroffenen.
- Die Vorschriften des Art. 23 BayDSG über die Verarbeitung und Nutzung personenbezogener Daten durch Forschungseinrichtungen müssen beachtet werden (u.a. Zweckänderung für Forschung, Anonymisierung).

- Wissenschaftliche Auswertung von Daten (verstorbener) Patienten in einer Klinik

Bei einer internationalen Fallkontrollstudie stellte sich die Frage nach der rechtlichen Befugnis zur Nutzung personenbezogener Daten von verstorbenen Patienten der Klinik für wissenschaftliche Zwecke der Klinik. Das Bayerische Krankenhausgesetz, das für alle bayerischen Krankenhäuser gilt, auf die das Bundeskrankenhausfinanzierungsgesetz Anwendung findet, sieht in Art. 27 ("Datenschutz") in Abs. 4 vor, daß u.a. Krankenhausärzte die im Gewahrsam des Krankenhauses befindlichen Patientendaten auch nutzen dürfen, soweit dies zu Forschungszwecken im Krankenhaus oder im Forschungsinteresse des Krankenhauses erforderlich ist. Insofern kommt es bei den bayerischen Krankenhäusern, auf die das Bayerische Krankenhausgesetz Anwendung findet, auf die Wirksamkeit einer Einwilligung nicht an.

Zur Absicherung der beteiligten Personen im Krankenhaus habe ich jedoch empfohlen, in der Klinik ausdrücklich schriftlich zu dokumentieren,

- daß es sich um eine Nutzung von Patientendaten "zu Forschungszwecken im Krankenhaus", oder "im Forschungsinteresse des Krankenhauses" handelt und
- daß und weshalb es im Einzelfall erforderlich war, andere Personen als Personal des Krankenhauses selbst zu beauftragen.

Diese Befugnis aus Art. 27 Abs. 4 BayKrG kann auch für noch lebende Patienten einer Klinik in Anspruch genommen werden, wenn ihre Daten für Forschungszwecke der Klinik benötigt werden.

- Anonymisierung

Sollen im Rahmen der Forschungsarbeit Daten aus dem behandelnden Krankenhaus nach außen übermittelt werden, so müssen sie ausreichend anonymisiert sein (Art. 27 Abs. 4 BayKrG). Zu einer ausreichenden Anonymisierung gehört nicht nur das Weglassen von Namen, Anschrift und Geburtsdatum der Betroffenen, sondern auch der Verzicht auf andere

Hinweise, die mit Zusatzwissen eine Identifikation der Betroffenen durch Dritte erlauben (z.B. seltene Berufe, seltene Staatsangehörigkeiten, etwa in Kombination mit anderen selteneren Merkmalen). Problematisch wegen des im Einzelfall hohen Reidentifikationsrisikos ist in diesem Zusammenhang auch die Angabe einer vollständigen 5-stelligen Postleitzahl. Im Zuge unserer Beratung für ein Forschungsprojekt wurden daher anstelle der Postleitzahl andere regionale Merkmale gewählt, die eine solche Identifizierung nicht erlauben. Eine Verkürzung der Postleitzahl auf die ersten beiden Ziffern, die nur für die 97 Postleitzahl-Regionen stehen, wird im Regelfall zu einer ausreichenden Anonymisierung beitragen. 3-stellige oder gar noch längere Postleitzahlen müßten im Einzelfall (von Projektseite) auf ihr Reidentifikationsrisiko untersucht werden. Dabei ist auf die Kombination mit den anderen Angaben zu achten, die zusammen mit einer auch verkürzten Postleitzahl eine Reidentifikation erleichtern.

3.4 Datenschutzfragen aus dem Bereich von Krankenhäusern

3.4.1 Outsourcing im Krankenhausbereich

3.4.1.1 Überblick

Outsourcing berührt die Vertraulichkeit des Arzt-Patienten-Verhältnisses. Der rechtliche und technische Schutz der Patientendaten muß daher erweitert werden!

Gerade in Krankenhäusern wurden traditionell nahezu alle Unternehmensfunktionen, vom Erbringen ärztlicher Leistungen für den Patienten bis hin zur Durchführung von Putzarbeiten, hausintern durch eigenes, fest angestelltes Personal wahrgenommen. Das Hinzuziehen externer Unternehmen (etwa zur Vornahme von Wartungsarbeiten an medizinischen Geräten) kam zwar vor, war aber insgesamt gesehen die Ausnahme.

Dies hat sich gerade in den letzten beiden Jahren teilweise grundlegend geändert. Vor allem aus wirtschaftlichen Gründen werden zahlreiche, zum Teil fachlich durchaus anspruchsvolle Aufgaben "ausgelagert" und einem außenstehenden (typischerweise privaten) Unternehmen übertragen. Dieses nimmt diese Aufgaben entweder räumlich außerhalb des Krankenhauses in eigenen Geschäftsräumen wahr oder es entsendet Personal in das Krankenhaus, um die Aufgaben dort erledigen zu lassen.

Beide Varianten der "Nutzung externer Ressourcen" (outside resources using, abgekürzt Outsourcing) werfen erhebliche datenschutzrechtliche Fragen auf. Sie ergeben sich in erster Linie aus der Pflicht des Krankenhauses gegenüber dem Patienten, die ärztliche Schweigepflicht strikt zu wahren. Nach der Rechtsprechung, beispielsweise des Bundesgerichtshofs, ist auch bei durchaus berechtigten eigenen wirtschaftlichen Interessen eines Krankenhauses auf das Geheimhaltungsbedürfnis des Patienten möglichst weitgehend Rücksicht zu nehmen. Rücksicht zu nehmen ist auch darauf, daß die Sicherheit von Patientendaten vor Beschlagnahme durch Herausgabe der Patientendaten nach außerhalb des Krankenhauses an Auftragnehmer verloren gehen kann, weil diese Sicherheit nach § 97 StPO nur "im Gewahrsam einer Krankenanstalt" besteht.

Im folgenden zeige ich Lösungsansätze für einige Problemkreise auf, die im weitesten Sinn dem Begriff des Outsourcing zugerechnet werden können und mit denen ich im Berichtszeitraum

konfrontiert war. Ich muß dabei betonen, daß hier vielfach rechtliches Neuland vorliegt, so daß ich nicht immer abschließende Lösungen anbieten kann.

3.4.1.2 Vergabe einer Organisationsanalyse an eine externe Beratungsgesellschaft

Um die tarifliche Einstufung des Krankenhauspersonals korrekt durchführen zu können, beauftragte ein Krankenhausträger eine Wirtschaftsprüfungsgesellschaft mit der Durchführung einer Organisationsuntersuchung. Dabei wurden Fragebögen verwendet, auf denen "für evtl. Rückfragen" auch Namen des jeweiligen Patienten vermerkt waren.

Ich habe den Krankenhausträger darauf hingewiesen, daß ich keinen Grund dafür sehe, wieso der Name des Patienten für Rückfragen benötigt werde. Eine fortlaufende Nummer auf dem Erhebungsbogen oder ähnliche Daten, über die im Bedarfsfall ermittelt werden kann, um welchen Patienten es ging, könnten denselben Zweck erfüllen. In der Weitergabe der Patientennamen an die Wirtschaftsprüfungsgesellschaft lag somit eine Verletzung der ärztlichen Schweigepflicht gemäß § 203 Abs. 1 Nr. 1 SGB, die mangels Erforderlichkeit der Datenweitergabe auch durch Art. 27 Abs. 5 Satz 1 Bayerisches Krankenhausgesetz nicht gerechtfertigt war. Daran ändert auch die gesetzliche Verschwiegenheitspflicht der Wirtschaftsprüfer nichts. In der Rechtsprechung zur ärztlichen Schweigepflicht ist es seit jeher unbestritten, daß auch zwischen Personen, von denen jede selbst der ärztlichen Schweigepflicht unterliegt, Daten nicht ohne weiteres weitergegeben werden dürfen. Ich habe daher die **Weitergabe** der Patientennamen an die Wirtschaftsprüfungsgesellschaft **beanstandet.**

3.4.1.3 Einschaltung eines externen Inkassounternehmens

Ein Inkassounternehmen hatte einem Krankenhausträger angeboten, für diesen das **vorgerichtliche** Inkasso von Forderungen aus Behandlungsverträgen mit Selbstzahlern zu übernehmen. Der Krankenhausträger wandte sich deswegen an mich mit der Bitte um Beratung, die ergab, daß dies nur unter engsten Voraussetzungen in Betracht kommt.

Die Tatsache, der ärztlichen Behandlung als solche gehört ebenso wie Behandlungsdaten (z.B. Diagnoseangaben) zu den Daten, die der ärztlichen Schweigepflicht gemäß § 203 Abs. 1 Nr. 1 StGB unterliegen. Insofern stellt die Mitteilung jeglicher Angaben über das Behandlungsverhältnis an ein Inkassounternehmen eine Offenbarung von Daten dar, für die eine Befugnis im Sinne von § 203 Abs. 1 Nr. 1 StGB vorliegen muß.

Eine solche Befugnis kann sich nach den konkreten Umständen entweder aus einer rechtswirksamen Einwilligung des Patienten oder aus Art. 27 Abs. 5 Satz 1 Bayerisches Krankenhausgesetz ergeben.

Eine Einwilligung des Patienten dürfte dann, wenn die Zahlungsschwierigkeiten bereits aufgetreten sind, ausscheiden. Sofern eine entsprechende Einwilligungsklausel in die allgemeinen Geschäftsbedingungen aufgenommen wird, die der Patient bei seiner Aufnahme in das Krankenhaus schriftlich anerkennt, sind die Vorgaben des Gesetzes über allgemeine Geschäftsbedingungen zu beachten. Dabei wird insbesondere eine Rolle spielen, daß rein wirtschaftliche Interessen normalerweise hinter dem Geheimhaltungsinteresse des Patienten zurücktreten müssen.

Da in dem mir vorgelegten Fall eine entsprechende Klausel in den allgemeinen Geschäftsbedingungen nicht enthalten war, stellte sich die Frage nach der Reichweite der Befugnis aus Art. 27 Abs. 5 Satz 1 Bayerisches Krankenhausgesetz. Nach dieser Bestimmung ist die Übermittlung von Patientendaten an Dritte unter anderem zulässig zur verwaltungsmäßigen Abwicklung des Behandlungsverhältnisses. Diese Vorschrift kann vom Grundsatz her die Weitergabe von Daten an ein Inkassounternehmen zum Zwecke des vorgerichtlichen Forderungseinzugs rechtfertigen. Allerdings müßte der Krankenhausträger dabei unter Wahrung des Verhältnismäßigkeitsgrundsatzes so schonend wie möglich vorgehen, um das Arztgeheimnis möglichst weitgehend zu wah-

ren. Hieraus müssen insbesondere folgende Konsequenzen gezogen werden:

- Die Einschaltung eines Inkassounternehmens muß dem Betroffenen vorher angekündigt werden (z.B. durch einen deutlichen Hinweis im letzten Mahnschreiben vor der Einschaltung des Inkassounternehmens). Dabei muß der Betroffene auch darauf hingewiesen werden, welches Inkassounternehmen eingeschaltet werden soll und welche Daten diesem Unternehmen offenbart werden sollen.

- Mitgeteilt werden darf nur die Tatsache der Behandlung und die Rechnungssumme, nicht jedoch nähere Einzelheiten wie zum Beispiel die GOÄ-Nummern, Behandlungszeiten und Diagnosen.

- Sofern der Patient Einwendungen gegen die geltend gemachte Forderung erhebt, müßten diese Einwendungen unmittelbar zwischen dem Krankenhaus und dem Patienten abgeklärt werden. Es wäre unzulässig, dem Inkassounternehmen auch die Bearbeitung solcher Schuldnereinwände zu übertragen.

- Eine Nutzung der Daten durch das Inkassounternehmen für andere Zwecke (z.B. für die Erteilung von Bonitätsauskünften an andere Stellen) müßte vertraglich ausgeschlossen werden. Dabei wäre zu überlegen, ob der Einhaltung dieser vertraglichen Verpflichtung nicht durch die Vereinbarung einer angemessenen Vertragsstrafe für den Fall ihrer Verletzung gesichert werden sollte.

Ergänzend ist darauf hinzuweisen, daß ein reines Inkassounternehmen nicht der Schweigepflicht gemäß § 203 Abs. 1 Nr. 1 StGB unterliegt, so daß ein entsprechender strafrechtlicher Schutz von Patientendaten in einem solchen Unternehmen ebenso wenig gewährleistet wäre wie der daraus resultierende strafprozessuale Beschlagnahmeschutz. Auch deshalb muß die Weitergabe von Daten an ein Inkassounternehmen auf das unbedingt erforderliche Maß beschränkt werden.

3.4.1.4 Externes Catering

Ein Krankenhaus übertrug die Verpflegung der Patienten einem selbständigen Privatunternehmen. Das externe Catering-Unternehmen erhält jeweils folgende Daten: Name und Vorname des Patienten, Patientenaufnahmenummer, Station, Angaben zu besonderen Verpflegungsformen (etwa Diät).

Zumindest einzelne Patienten wünschen, daß ihre Daten nicht in dieser Weise weitergegeben werden, da sie fürchten, ihr Aufenthalt im Krankenhaus könnte in einer unerwünschten Weise Dritten bekannt werden.

Ich habe gegen die Einschaltung eines externen Catering-Unternehmens aus datenschutzrechtlicher Sicht keine Bedenken erhoben, **sofern** im Verhältnis zwischen Patient und Krankenhaus folgende Bedingungen erfüllt werden:

- Der Patient wird in den Aufnahmebedingungen informiert, daß ein externes Catering-Unternehmen eingeschaltet wird und welche Daten an dieses Unternehmen übermittelt werden.

- Er wird in den Aufnahmebedingungen auch auf die Möglichkeit hingewiesen, der Weitergabe seiner Daten zu widersprechen.

- Falls ein Patient widerspricht, verwendet die Klinik für diesen Patienten ein Pseudonym.

Im Vertrag zwischen dem Krankenhaus und dem Catering-Unternehmen müssen zumindest folgende Festlegungen getroffen werden:

- Verpflichtung des Unternehmens zur ausschließlich zweckgebundenen Verwendung der Daten für Zwecke des Catering und Ausschluß der Weitergabe von Daten an Dritte; die Sicherung der Einhaltung dieser Verpflichtung könnte z.B. durch die Vereinbarung einer Vertragsstrafe erfolgen.

- Verpflichtung des Catering-Unternehmens, die Daten innerhalb des räumlichen Bereichs des Krankenhauses zu belassen; diese Verpflichtung ist deshalb wichtig, weil nur in diesem Fall der Beschlagnahmeschutz des § 97 StPO in Bezug auf die Daten zum Tragen kommt.

- Verpflichtung des Catering-Unternehmens, die ihm überlassenen Daten im Klinikum zu löschen, sobald sie für die Durchführung der Verpflegung nicht mehr benötigt werden.

Nach meinen Erfahrungen stehen Catering-Unternehmen den vorstehend aufgezeigten Anforderungen aufgeschlossen gegenüber und sind zu entsprechenden Vereinbarungen bereit.

3.4.1.5 Externe Archivierung von Krankenunterlagen

Um sich ein eigenes Archiv ganz oder teilweise zu ersparen, beabsichtigte ein Krankenhaus, die Archivierung von Krankenunterlagen durch ein externes Privatunternehmen durchführen zu lassen. Dabei war daran gedacht, daß die Firma dem Krankenhaus verschließbare Behälter für die Krankenunterlagen zur Verfügung stellt, die nur das jeweilige Krankenhaus öffnen kann. Diese Behälter sollten nicht mit dem Namen des Krankenhauses versehen sein, sondern mit einem Code. Für den Fall, daß eine bestimmte Unterlage benötigt wird, sollte das Krankenhaus die Codenummer des Behälters angeben. Das Archivunternehmen hätte den Behälter daraufhin zum Krankenhaus transportiert. Das Krankenhaus hätte die Unterlage entnehmen, den Behälter wieder verschließen und an das Archivunternehmen zurückgeben können.

Erhebliche Bedenken gegen eine solche Lösung ergeben sich insbesondere daraus, daß die Daten in einem solchen Fall voraussichtlich keinen Beschlagnahmeschutz gemäß § 97 StPO genießen. Auf der Basis der bisherigen Rechtsprechung ist nämlich davon auszugehen, daß das Krankenhaus bei dieser Konzeption an den Archivbehältern keinen "Gewahrsam" mehr im Sinne dieser Vorschrift hat. Ich muß mich deshalb gegen diese Vorgehensweise aussprechen.

3.4.2 Digitale Archivierung von Krankenakten

Der Einsatz von WORM-Platten als Archivmedium für Krankenakten erfordert eine intelligente Lösung des Löschungsproblems. Dabei muß auf die Beweismittel-Qualität der Speicherung Rücksicht genommen werden.

Angesichts der wachsenden Menge von Krankenakten erwägen immer mehr Krankenhäuser, Krankenakten digital zu archivieren (beispielsweise unter Einsatz von WORM-Platten). Die Ziele dieser Bemühungen gehen bisher offensichtlich weniger dahin, Ablageraum zu sparen, als vielmehr dahin, den Zugriff auf die Krankenakten zu erleichtern.

Ablauforganisatorisch erscheint der Einsatz optischer Speicherplattensysteme vor allem in folgenden beiden Formen denkbar:

- Optisches Zusatzarchiv

  Bei dieser Variante wird das Patientenarchiv wie bisher konventionell in Papierform geführt. Daneben tritt das optische Speichermedium, das meist nur einige wenige Schriftstücke je Patient enthält, die von besonderer Bedeutung sind und auf die erfahrungsgemäß besonders häufig zurückgegriffen werden muß (z.B. Anamnese-Bögen und Entlaßberichte).

- Optisches Alleinarchiv

  Bei dieser Variante fällt das konventionell in Papierform geführte Archiv völlig weg. Alle Unterlagen, die sonst dort aufzubewahren wären, sind auf einem optischen Speichermedium festgehalten. Vorhandene Originalunterlagen werden nach dem Einscannen vernichtet.

Mit der Variante des optischen Zusatzarchivs war ich im Rahmen meiner Prüftätigkeit im Gegensatz zu optischen Alleinarchiven mehrfach befaßt.

Die digitale Archivierung von Krankenakten wirft eine Reihe von Fragen in verschiedenen Rechtsgebieten auf. Zu nennen sind hier einmal die Fragen im Zusammenhang mit der gegenüber dem Patienten bestehenden Dokumentationspflicht. In prozeßrechtlicher Hinsicht, insbesondere im Zivilprozeßrecht, stellt sich die Frage, welchen Beweismittelwert ein optisches Speichermedium hat. Schließlich besteht keine einheitliche Auffassung darüber, ob die handels- und steuerrechtlichen Aufbewahrungspflichten auch dadurch erfüllt werden können, daß nicht Originale (insbesondere in Papierform), sondern optische Speichermedien bereitgehalten werden. Im Rahmen dieses Tätigkeitsbericht ist auf diese Fragen nicht näher einzugehen.

In datenschutzrechtlicher Hinsicht ergeben sich vor allem bei der Erfüllung von Löschungspflichten Schwierigkeiten.

Das Problem bei der digitalen Archivierung besteht darin, wie die speichernde Stelle Löschungsverpflichtungen gemäß Art. 12 Abs. 1 BayDSG nachkommen kann. Dabei ist zu beachten, daß das Bayerische Datenschutzgesetz ein "Löschen" nur dann annimmt, wenn die betreffenden Daten unlesbar gemacht werden (vgl. Art. 4 Abs. 6 Satz 2 Nr. 5 BayDSG). Die Daten müssen also letztlich vernichtet werden. Genau dies war bei optischen Speicherplatten bisher regelmäßig nicht möglich. Die üblicherweise eingesetzten Platten konnten nur einmal beschrieben werden; ein nachträgliches Überschreiben einzelner darauf enthaltener Daten oder ein nachträgliches Entfernen war nicht möglich. Somit konnte die speichernde Stelle einer Löschungsverpflichtung nach Art. 12 Abs. 1 BayDSG nicht nachkommen.

Die zur Lösung bisher denkbaren zwei Wege, nämlich das Umschreiben der nicht zu löschenden Daten auf eine neue Platte, oder das Anlegen einer Indexdatei, in der vermerkt wird, welche Daten eigentlich gelöscht werden müßten, warfen entweder zivilrechtliche Probleme auf (Inhalt der umgeschriebenen Platte nicht unmittelbar, sondern quasi durch Kopieren gewonnen) oder es entstehen datenschutzrechtliche Probleme (das Anlegen einer Indexdatei mit Hinweisen auf zu löschende Daten bedeutet gerade keine Löschung, sondern lediglich eine Sperrung, die zudem mit geringem Aufwand umgangen werden kann).

Eine Lösung der Frage könnte sich durch den Fortschritt der Technik abzeichnen, nämlich dadurch, daß neuerdings optische Speicherplatten zur Verfügung stehen, die ein Wiederbeschreiben erlauben. Es erscheint daher zweifelhaft, ob es sich noch hinreichend begründen läßt, anstelle einer Löschung lediglich eine Sperrung vorzunehmen. Dabei sei nicht verschwiegen, daß sich bei dieser Variante der optischen Speichermedien im Bereich des Zivilprozesses ähnliche Fragen stellen wie bei der oben erwähnten Möglichkeit, die nicht zu löschenden Daten auf eine neue Platte umzuschreiben, denn die Möglichkeit, Daten nachträglich zu verändern, mindert die Beweisqualität, da Manipulationen zumindest möglich sind.

In jedem Fall darf das Einscannen von Originalbelegen nicht außerhalb von Krankenhäusern erfolgen. Die Regelung des Art. 27 Abs. 4 Satz 6 Bayerisches Krankenhausgesetz ist auch hier anzuwenden. Der hinter dieser Regelung stehende Gedanke (insbesondere das Bestreben, durch Aufrechterhaltung des Gewahrsams der Klinik im Sinne von Art. 97 StPO die Beschlagnahmefreiheit von Krankenunterlagen auch während des Vorgangs der Verfilmung zu sichern) gilt auch für das Einscannen von Dokumenten. Diesem Aspekt werde ich bei Prüfungen besonderes Augenmerk widmen.

3.4.3 Anlageverzeichnis und Freigabe automatisierter Verfahren nach Art. 27 BayDSG in öffentlichen Krankenhäusern

Das neue BayDSG, das am 01.03.1994 in Kraft getreten ist, hat für die öffentlichen Krankenhäuser Änderungen beim Freigabeverfahren und bei der Pflicht gebracht, ein Verzeichnis der eingesetzten Anlagen und Verfahren zu führen.

Öffentliche Krankenhäuser sind - mit Ausnahme von Hochschulkliniken und Bezirkskrankenhäusern - Stellen, die gemäß Art. 3 Abs. 1 BayDSG am Wettbewerb teilnehmen. Während das frühere BayDSG für solche Wettbewerbsunternehmen weder datenschutzrechtliche Freigaben noch das Führen von Anlagen- und Verfahrensverzeichnissen vorschrieb, gilt nach dem neuen BayDSG folgendes:

- Da Art. 26 BayDSG auch auf Wettbewerbsunternehmen Anwendung findet (vgl. Art. 3 Abs. 1 Satz 3 BayDSG), ist bei Vorliegen der Voraussetzungen dieser Bestimmung ein Freigabeverfahren durchzuführen.

- Für Verfahren, die bereits vor dem 01.03.1994 und damit vor dem Inkrafttreten des neuen Bayerischen Datenschutzgesetzes eingesetzt wurden, bestand damals keine Freigabepflicht. Für sie muß die Freigabe nicht nachgeholt werden. Etwas anderes gilt nur bei wesentlichen Änderungen der Verfahren.

- Da auch Art. 27 BayDSG auf Wettbewerbsunternehmen Anwendung findet, muß ein Anlagen- und Verfahrensverzeichnis erstellt sein, das den Anforderungen dieser Bestimmung genügt.

  Auch Altverfahren, für die nach den obigen Ausführungen keine Pflicht zur (nachträglichen) Freigabe besteht, sind in das Verfahrensverzeichnis aufzunehmen.

  Entsprechende Verzeichnisse mußten bereits zum 01.03.1995 eingerichtet sein (vgl. Art. 39 Abs. 1 Satz 4 BayDSG). Stellen, die dieser Pflicht nicht nachgekommen sind, müssen bei einer datenschutzrechtlichen Prüfung mit einer Beanstandung rechnen. Es ist nicht erkennbar, wie eine Stelle ihrer datenschutzrechtlichen Verantwortung gemäß Art. 25

BayDSG gerecht werden kann, wenn keine Übersicht über die eingesetzten Anlagen und Verfahren vorliegt.

3.4.4 Übermittlung von Daten für Zwecke der Krankenhausseelsorge

Wie Anfragen von Krankenhausträgern zeigen, bestehen Unsicherheiten, inwieweit Listen von Patienten, die einer bestimmten Pfarrei angehören, an Besuchsdienste weitergegeben werden dürfen, die aus ehrenamtlich tätigen Laien bestehen und die im Auftrag der Heimatpfarrei des Patienten Besuche im Krankenhaus durchführen.

Ausschlaggebend für die Beurteilung der Weitergabe dieser häufig sprachlich etwas mißverständlich als "Pfarrerlisten" bezeichneten Unterlagen, ist der (ggf. mutmaßliche) Wille des Patienten. Einerseits muß eine derartige Betreuung ermöglicht werden, wenn der Patient dies wünscht. Andererseits muß zuverlässig vermieden werden, daß Angaben über einen Krankenhausaufenthalt eines Patienten an einen Besuchsdienst seiner Heimatpfarrei weitergegeben werden, wenn er damit nicht einverstanden ist.

Mit der Übermittlung einer "Pfarrerliste" an eine Kirchengemeinde zur Weitergabe an deren Besuchsdienst wird gleichzeitig die Tatsache offenbart, daß die in der Liste aufgeführten Patienten in das Krankenhaus aufgenommen wurden. Diese Tatsache unterliegt der ärztlichen Schweigepflicht. Die Durchbrechung der ärztlichen Schweigepflicht setzt eine rechtliche Befugnis voraus, das heißt regelmäßig eine Einwilligung des Patienten. Sofern (wie vielerorts üblich) nur das Einverständnis des Patienten mit einem eventuellen Besuch eines Seelsorgers eingeholt wird, kann nicht unterstellt werden, daß damit auch der Weitergabe der Daten an Mitglieder eines Besuchsdienstes zugestimmt wurde. Mir sind Fälle bekannt geworden, in denen Patienten, beispielsweise aus Sorge um ihren Arbeitsplatz, nicht wünschen, daß ihre Aufnahme in ein Krankenhaus am Heimatort bekannt wird. Teilweise lassen sich die Patienten aus diesem Grund sogar in ihrem Urlaub im Krankenhaus behandeln. In solchen Fällen wäre ein Patient keineswegs damit einverstanden, daß ein Besuchsdienst seiner Heimatpfarrei Angaben zu seinem Aufenthalt im Krankenhaus erhält.

Um auch solchen Konstellationen gerecht zu werden, halte ich es für erforderlich, den Patienten klar darauf hinzuweisen, daß eine solche Weitergabe erfolgt und daß er ihr widersprechen kann. Die Weitergabe von Daten an Pfarreien muß zeitlich so gestaltet sein, daß ein Widerspruch, der entweder bei der Aufnahme selbst oder spätestens am Tag danach erklärt wird, noch effektiv

berücksichtigt werden kann.

Aus der Angabe der Konfession im Aufnahmeformular kann nicht geschlossen werden, daß der Patient auch mit dem Besuch eines ehrenamtlich tätigen Besuchsdienstes seiner Heimatpfarrei einverstanden ist. Meines Erachtens kann eine solche Angabe lediglich dahin interpretiert werden, daß der Patient mit der Verständigung eines haupt- oder nebenamtlich am Krankenhaus tätigen Seelsorgers einverstanden ist. Da kirchliche Besuchsdienste vielfach erst in den letzten Jahren eingerichtet wurden, ist es nämlich vielen Patienten noch nicht bewußt, daß solche Dienste existieren.

Keine Frage des Datenschutzes ist es, wenn ein Krankenhausseelsorger nach seinem Ermessen Patienten in ihrem Zimmer aufsucht und sich dort als Seelsorger vorstellt. Ein solches Handeln gehört zum rein innerkirchlich zu regelnden Bereich der Krankenhausseelsorge. Eine datenschutzrechtlich relevante Mitwirkung des Krankenhauses erfolgt dabei nicht. Sie läge nur vor, wenn der Krankenhausseelsorger vorher seitens des Krankenhauses Listen von Patienten erhält. In diesem Fall wäre bei der Weitergabe dieser Liste an den Seelsorger nach den oben dargestellten Grundsätzen zu verfahren.

3.4.5 Vorsorgliche Anmeldung nach § 121 BSHG

Wer - als Selbstzahler - die Krankenhausrechnung nicht innerhalb von zwei Monaten seit Aufnahme bezahlt, riskiert, dem Sozialamt gemeldet zu werden - auch wenn er die Rechnung gerade erst erhalten hat:

Bei Personen, die im Krankenhaus als Selbstzahler auftreten, stellt sich nach der Rechnungstellung bisweilen heraus, daß sie die Rechnung nicht mit eigenen Mitteln begleichen können. Das Krankenhaus hat in diesem Fall die Möglichkeit, beim zuständigen Sozialamt einen Antrag auf Kostenübernahme gemäß § 121 BSHG zu stellen. In § 121 BSHG ist allerdings festgelegt, daß dies binnen einer "angemessenen Frist" geschehen muß. Die angemessene Frist beträgt laut Rechtsprechung 2 Monate und beginnt mit dem Datum der Behandlung bzw. dem Datum der Aufnahme in das Krankenhaus. Sie wird von der Rechtsprechung als Ausschlußfrist gewertet, weshalb die Krankenhäuser darauf achten, entsprechende Anträge vor Ablauf der Frist zu stellen.

Durch die Eingabe einer Bürgerin wurde ich darauf aufmerksam gemacht, daß ein bayerisches Krankenhaus alle Selbstzahler routinemäßig unter Angabe der Diagnose an das zuständige Sozialamt meldet, sofern der Betroffene die Behandlungskosten nicht vor Ablauf von 2 Monaten nach dem Behandlungsdatum bzw. dem Datum der Aufnahme in das Krankenhaus beglichen hat. Dabei nimmt das Krankenhaus nach eigenem Bekunden ausdrücklich **keine Rücksicht** darauf, ob das **Zahlungsziel** der dem Patienten zugesandten Rechnung **bereits erreicht ist** oder nicht.

Im konkreten Fall führte diese Verfahrensweise dazu, daß bereits am 4. Tag nach Absendung der Rechnung an die Patientin ein Antrag gemäß § 121 BSHG beim zuständigen Sozialamt gestellt wurde. Die Patientin, eine Frau in gesicherter Stellung, war sehr überrascht, als sie vom zuständigen Sozialamt umgehend vorgeladen wurde, um mit ihr die Kostentragung zu besprechen.

Das Vorgehen des Krankenhauses habe ich gemäß Art. 31 Abs. 1 Satz 1 BayDSG beanstandet. Es verstößt gegen Art. 27 Abs. 5 Satz 1 Bayerisches Krankenhausgesetz und dürfte auch im Widerspruch zu § 203 Abs. 1 Strafgesetzbuch stehen. Zwar kann das Stellen eines Antrags gemäß § 121 BSHG beim zuständigen Sozialamt grundsätzlich zur verwaltungsmäßigen Abwicklung eines Behandlungsverhältnisses erforderlich sein und rechtfertigt dann die Übermittlung der zur

Bearbeitung des Antrags erforderlichen Patientendaten an das zuständige Sozialamt. Entscheidend sind jedoch stets die Umstände des Einzelfalles. Sofern der betroffene Patient den Umständen nach die Rechnung noch überhaupt nicht bezahlt haben kann, weil er sie entweder noch überhaupt nicht in Händen hält, oder sie ihm erst vor wenigen Tagen zugegangen ist, ist die Einschaltung des Sozialamts nicht erforderlich.

Es obliegt dem Krankenhaus, die Rechnung so rechtzeitig zu stellen, daß dem Patienten noch vor Ablauf der 2-Monats-Frist gemäß § 121 BSHG hinreichend Zeit für das Begleichen der Rechnung bleibt. Die im geschilderten Fall gewählte Vorgehensweise, schematisch alle Selbstzahler kurz vor Ablauf der 2-Monats-Frist dem zuständigen Sozialamt zu melden, ist als unzulässiges Stellen von "Vorratsanträgen" zu werten. Dieses Vorgehen führt dazu, daß den Sozialämtern Daten über eine Vielzahl von Personen übermittelt werden, die in ihrer überwiegenden Mehrheit die entstandenen Kosten ordnungsgemäß begleichen. Ein solches Vorgehen vernachlässigt die Interessen der Betroffenen in unvertretbarer Weise.

3.4.6 Überprüfung von Patientenakten einer psychiatrischen Klinik durch den Landesrechnungshof

Durch Beschluß vom 29.04.1996 hat das Bundesverfassungsgericht entschieden, eine Verfassungsbeschwerde nicht zur Entscheidung anzunehmen, die sich mit der Einsichtnahme eines Landesrechnungshofs in Patientenunterlagen einer psychiatrischen Klinik befaßte. Die vom Bundesverwaltungsgericht vertretene Auffassung, daß Regelungen in der Art von Art. 95 BayHO als ausreichende Befugnis im Sinne von § 203 StGB anzusehen sind, wurde vom Bundesverfassungsgericht "angesichts der damaligen Aktenführung und Abrechnungsweise" in der überprüften Klinik nicht beanstandet.

Nach meiner Auffassung ist die Entscheidung des Bundesverfassungsgerichts dahin zu verstehen, daß keine grundsätzlichen Bedenken gegen die Einsichtnahme des Rechnungshofs in Behandlungsunterlagen bestehen, **sofern** nach den konkreten Umständen **eine solche Einsichtnahme zur Erfüllung der Aufgaben des Rechnungshofs erforderlich ist.** Dies schließt nicht aus, sondern setzt im Gegenteil voraus, daß der Rechnungshof auf die Sensibilität dieser Unterlagen Rücksicht nimmt und auf sie im Sinne eines stufenweisen Vorgehens erst dann zugreift, wenn die Einsichtnahme in weniger sensible Unterlagen (beispielsweise in bloße Abrechnungsunterlagen statt in die Behandlungsunterlagen selbst) zur Aufgabenerfüllung nicht ausreicht.

3.5 Gesundheitsämter

3.5.1 Eingliederung der staatlichen Gesundheits- und Veterinärämter in die Landratsämter Sicherung der ärztlichen Schweigepflicht im eingegliederten Gesundheitsamt: Akten- und Registraturorganisation, gemeinsamer Außendienst, diskrete Beratung, Posteinlaufbehandlung

Seit am 01.01.1996 das "Gesetz über die Eingliederung der staatlichen Gesundheitsämter und der staatlichen Veterinärämter in die Landratsämter" vom 23.12.1995 (GVBl. S. 843) in Kraft getreten ist, sind die staatlichen Gesundheits- und Veterinärämter keine selbständigen staatlichen Behörden mehr, sondern Teile des jeweils örtlich zuständigen Landratsamtes.

Dabei ergibt sich folgende Problematik:

Bei den in Art. 6 i.V.m. Art. 11 Gesundheitsdienstgesetz (GDG) genannten Aufgaben sind besondere Geheimhaltungspflichten und Verwertungsverbote zu beachten. Dabei handelt es sich im wesentlichen um freiwillige Beratung (z.B. Ehe- und Familienberatung, Beratung Drogensüchtiger, psychisch Kranker oder Behinderter, Aids-Beratung) und freiwillige Begutachtung. Es gibt aber auch weitere Fälle, die einen besonderen Vertrauensschutz notwendig machen, z.B. ärztliche Mitteilungen an den Amtsarzt, Datenerhebungen zur Schulgesundheitsuntersuchung, im Einzelfall unter Umständen auch vertrauliche ärztliche Mitteilungen im Rahmen einer Datenerhebung für den Vollzug des Bundesseuchengesetzes.

Aufgrund meiner Erfahrungen aus Prüfungen bei Gesundheitsämtern in den letzten Jahren gebe ich folgende Hinweise zur Wahrung der Geheimhaltungspflichten und Verwertungsverbote:

1. **Unterlagen des Gesundheitsamtes** über ein- und dieselbe Person aus freiwilliger Beratung oder freiwilliger Begutachtung einerseits und hoheitlicher Tätigkeit (z.B. Vollzug des Bundesseuchengesetzes) andererseits sind **nicht** in einer **Einheitsakte** zu führen, weil sonst beim Ziehen der Akte zum Vollzug hoheitlicher Maßnahmen die durch Art. 6 GDD besonders geschützten vertraulichen Angaben zur Kenntnis genommen würden.

2. Eine **Zentraldatei oder Registraturdatei** darf nicht so aufgebaut werden, daß die gemäß Art. 6 besonders zu schützenden Angaben in anderem Zusammenhang gelesen werden können. Ich habe daher darauf gedrungen, daß weder in der Zentraldatei noch in der automatisierten Registraturdatei erkennbar ist, **wegen welcher** gesundheitlichen Probleme jemand zur freiwilligen Beratung oder Begutachtung vorgesprochen oder korrespondiert hat.

3. Bei Tätigkeit von **gemeinsamem Außendienstpersonal,** etwa des Sozialamtes und des Gesundheitsamts, muß sichergestellt werden, daß die Betroffenen, bevor sie diesen Personen etwas im Rahmen freiwilliger Beratung nach dem GDG anvertrauen, erfahren, ob diese Angaben auch für Zwecke des Sozialamtes genutzt werden sollen (s. auch Art. 16 Abs. 3 Satz 1 BayDSG - der Erhebungszweck ist jeweils vollständig anzugeben).

4. Ein möglichst **unbeobachtetes Aufsuchen** der Angebote der Schwangerschaftsberatung und sonstiger freiwilliger **Beratung** des Gesundheitsamtes sollte organisatorisch ermöglicht werden. Die Tatsache der Vorsprache oder telefonischen Kontaktaufnahme darf nicht anderen Personen oder Stellen im Amt bekannt werden.

5. Der **Posteinlauf** für das Gesundheitsamt muß im künftigen Landratsamt-Gesundheitsamt so organisiert werden, daß der Einlauf für die Arbeitsbereiche freiwillige Beratung bzw. freiwillige Begutachtung **unmittelbar** dem hierfür zuständigen ärztlichen, veterinärärztlichen bzw. sonstigen **Fachpersonal** des Gesundheitsamtes zugeleitet wird. Andere Referate des Amtes dürfen keinen Zugang zu solchen Schreiben erlangen.

Für die **organisatorische Umsetzung** bedeutet das:

- Grundsätzlich dürfen in der zentralen Eingangsstelle des Landratsamtes an das Gesundheitsamt gerichtete Sendungen wie normale Behördenpost geöffnet und weiterbehandelt werden. Läßt ein Eingang aber erkennen, daß einer der o.a. Ausnahmefälle gegeben ist (z.B. weil er "an die Familienberatung" oder an einen Behördenmitarbeiter gerichtet ist, der in einem der sensiblen Aufgabenbereiche tätig ist), muß er ungeöffnet weitergeleitet werden. Um solche Fälle leichter erkennen zu können, könnte den Klienten empfohlen werden, beim weiteren

Schriftwechsel auf den Briefumschlägen entsprechende Zusätze anzubringen. Werden Briefe in der Eingangsstelle geöffnet, weil der sensible Aufgabenbereich aus der Beschriftung auf dem Umschlag nicht erkennbar ist, muß sichergestellt sein, daß das Schreiben - abweichend vom üblichen Postlauf (vgl. § 14 der Musterdienstordnung für die Landratsämter) - unmittelbar an die zuständige Stelle weitergeleitet wird. Zweckmäßigerweise sollte das Personal der Eingangsstelle eingehend über die sensiblen Aufgabenbereiche unterrichtet werden.

- Als "angemessene organisatorische Maßnahme" zur Sicherstellung des Verwertungsverbotes i.S. von Art. 6 Abs. 1 Satz 5 n.F. GDG wird nur eine strikte Trennung der Akten aus dem Bereich der freiwilligen gesundheitlichen Beratung und der freiwilligen Begutachtung von den übrigen Aktenbeständen des Gesundheits- und Veterinärwesens anzusehen sein. Inwieweit die übrigen Unterlagen des Gesundheits- und Veterinärwesens wegen darin enthaltener vertraulicher Mitteilungen (z.B. des Hausarztes an den Amtsarzt) von den Aktenbeständen der anderen Abteilungen des Landratsamtes getrennt zu halten sind, müßte im Einzelfall mit dem Ziel der Wahrung des Vertrauensschutzes geprüft werden.

Das Bayerische Staatsministerium des Innern hat diese Hinweise allen Regierungen und Landratsämtern bekanntgegeben. Bei künftigen Prüfungen von Landratsämtern werde ich ein besonderes Augenmerk darauf richten, ob diese Maßstäbe eingehalten werden und ob möglicherweise zusätzliche Maßnahmen erforderlich sind, um die Einhaltung der Geheimhaltungspflichten und Verwertungsverbote sicherzustellen. Leitlinie muß dabei nach meiner Auffassung sein, daß die Eingliederung der staatlichen Gesundheits- und Veterinärämter in die Landratsämter für die Betroffenen nicht zu einer Verschlechterung ihrer datenschutzrechtlichen Position gegenüber dem bisherigen Zustand führen darf.

3.5.2 Verschwiegenheitspflicht der Gesundheitsämter

Wieviel darf das Gesundheitsamt nach der Untersuchung eines Beamten dem Dienstherrn über den Gesundheitszustand mitteilen?

Teilt ein Beamter seiner Beschäftigungsbehörde mit, daß er erkrankt sei, so hat er auf Anordnung des Dienstvorgesetzten ein amtsärztliches Zeugnis beizubringen (s. § 20 Abs. 2 Satz 2 der Verordnung über den Urlaub der bayerischen Richter und Beamten). Ferner ist ein Beamter anläßlich der Entscheidung über eine mögliche Versetzung in den Ruhestand wegen dauernder Dienstunfähigkeit verpflichtet, sich nach Weisung seines Dienstvorgesetzten ärztlich untersuchen zu lassen (s. Art. 56 Abs. 1 Satz 3 Bayerisches Beamtengesetz). In einem Fall, der mir durch eine Eingabe bekanntgeworden ist, hatte ein Beamter den Chefarzt eines Krankenhauses von der Schweigepflicht **gegenüber dem zuständigen Gesundheitsamt** entbunden. Der Chefarzt übersandte dem Gesundheitsamt einen detaillierten Abschlußbericht über die durchgeführte Behandlung.

Den Inhalt dieses Berichts gab das Gesundheitsamt vollständig an den Dienstvorgesetzten weiter.

Ich habe die Weitergabe dieses Berichts durch das Gesundheitsamt gemäß Art. 31 Abs. 1 Satz 1 Bayerisches Datenschutzgesetz beanstandet. Maßgebend waren dafür folgende Gründe:

- Bei einer Untersuchung zur Erstellung eines Zeugnisses im Krankheitsfall gemäß § 20 Abs. 2 Satz 2 der Urlaubsverordnung handelt es sich ebenso um eine freiwillige Untersuchung wie bei einer Untersuchung gemäß Art. 56 Abs. 1 Satz 3 Bayerisches Beamtengesetz zur Klärung der dauernden Dienstunfähigkeit. Zwar sind Beamte gemäß diesen Vorschriften verpflichtet, sich in dienstrechtlichen Angelegenheiten ärztlich untersuchen zu lassen, der Dienstherr kann sie aber zu einer solchen Untersuchung nicht zwingen. Dies ergibt sich vor allem aus Art. 56 Abs. 1 Satz 4 BayBG, wonach der Beamte bei ungenügender Mitwirkung so behandelt werden kann, wie wenn seine Dienstunfähigkeit amtlich festgestellt worden wäre, ohne daß die Möglichkeit einer zwangsweisen Untersuchung vorgesehen wäre. Dies zeigt, daß im Sinne der Geheimhaltungsvorschriften, insbesondere des Art. 6 GDG, eine freiwillige Untersu-

chung vorliegt. Entsprechend heißt es in der amtlichen Begründung zu Art. 6 Abs. 1 Satz 1 2. Spiegelstrich GDG: "Der **2. Spiegelstrich** bezieht sich auf die Fälle, in denen zwar eine gesetzliche Verpflichtung des Betroffenen besteht, sich ärztlich untersuchen zu lassen, die ärztliche Untersuchung von der Behörde aber nicht erzwungen werden kann (Untersuchung und Begutachtung von Personen auf behördliche Aufforderung hin, z.B. Dienstfähigkeitsüberprüfung nach Art. 56 Abs. 1 Satz 3 BayBG, ..." (s. LT-Drs. 10/8972 vom 15.01.1986, Ziffer 2.6.2, Seite 14).

Der materielle Grund für diese gesetzliche Regelung liegt darin, daß auch derartige amtsärztliche Untersuchungen ein gewisses Vertrauensverhältnis zwischen dem Untersuchten und dem Arzt des Öffentlichen Gesundheitsdienstes voraussetzen, weil der Untersuchte dem Arzt nur dann das Erforderliche anvertrauen wird. Nur so ist eine objektive, ärztlich gesicherte Beurteilung möglich.

Die gegenteilige Auffassung müßte sich mit dem Problem auseinandersetzen, daß die Rechtsordnung an anderer Stelle (etwa zur Durchsetzung von Vorschriften zur Bekämpfung von Seuchen oder Geschlechtskrankheiten) durchaus ausdrückliche Befugnisse zur Durchführung von zwangsweisen Untersuchungen enthält, während im Beamtenrecht keine derartige Befugnis gegeben ist.

Sofern eine Untersuchung im Rahmen eines Antrags auf Ruhestandsversetzung gemäß Art. 57 Abs. 1 BayBG erfolgt, könnte der betreffende Beamte seinen Antrag jederzeit zurücknehmen; dies hätte zur Folge, daß die Befugnis des Arztes zur Mitteilung der Untersuchungsergebnisse an den Dienstherrn ab diesem Zeitpunkt entfiele.

Das Staatsministerium der Finanzen ist dagegen der Auffassung, daß die ärztliche Schweigepflicht zurücktritt, soweit die Weitergabe ärztlicher Erkenntnisse für die vom Dienstherrn zu treffende Feststellung der Dienstunfähigkeit erforderlich ist. Der begutachtende Amtsarzt, der aufgrund seiner gesetzlich in den Art. 56 und 57 BayBG verankerten Gutachtenspflicht tätig werde, handele dann im Sinne von § 203 Abs. 1 StGB

nicht unbefugt. Diese gesetzliche Gutachtenspflicht bestehe unabhängig davon, ob der Beamte selbst die Versetzung in den Ruhestand beantragt habe (Art. 57 BayBG) oder ob die Behörde die Zwangspensionierung (Art. 58 BayBG) betreibe. Zur Begründung seiner Auffassung beruft sich das Staatsministerium der Finanzen auf hergebrachte Grundsätze des Berufsbeamtentums.

Aus den oben dargelegten Gründen vermag ich diese Auffassung nicht zu teilen.

- Geheimnisse, die Amtsangehörigen eines Gesundheitsamtes im Zusammenhang mit einer Untersuchung oder Begutachtung anvertraut oder sonst bekannt geworden sind, der sich der Betroffene freiwillig unterzogen hat, dürfen nur zur Erfüllung der Aufgabe verarbeitet oder genutzt werden, in deren Wahrnehmung die Erkenntnisse gewonnen wurden (Art. 6 Abs. 1 Sätze 1 und 4 Gesundheitsdienstgesetz). Dies folgt auch aus der persönlichen Verpflichtung zur Wahrung des Berufsgeheimnisses (vgl. § 203 Abs. 1 Nr. 1 Strafgesetzbuch).

- Die Geheimhaltungspflicht gemäß Art. 6 Gesundheitsdienstgesetz und die ärztliche Schweigepflicht gemäß § 203 Abs. 1 Nr. 1 Strafgesetzbuch bestehen auch im Verhältnis zwischen einem Amtsarzt und dem Dienstherrn eines Beamten. Eine Weitergabe von Daten, die dem Schutz der genannten Vorschriften unterliegen, ist somit nur mit der ausdrücklichen oder mutmaßlichen Einwilligung des betroffenen Beamten zulässig.

- Unterzieht sich ein Beamter einer Untersuchung, so willigt er damit zwar konkludent in die **Weitergabe des** vom Gesundheitsamt erstellten ärztlichen **Gutachtens** an den Dienstherrn ein. Inhaltlich darf dieses Gutachten jedoch nicht über das hinausgehen, was für die beamtenrechtliche Entscheidung unbedingt erforderlich ist. Deshalb kommt auch die Angabe der ärztlichen Diagnose im engeren Sinne regelmäßig nicht in Betracht.

- Auch eine ausdrückliche Einwilligung des Beamten könnte nicht zur Weitergabe von Daten ermächtigen, die nicht als erforderlich anzusehen sind.

Diese Grundsätze wurden im wesentlichen bereits in einem Schreiben des Bayerischen Staatsmi-

nisteriums des Innern vom 19.01.1993 (Az.: IE1-5111/10-1/93) den Gesundheitsämtern zur Kenntnis gegeben. Die Gesundheitsämter sind gehalten, weiterhin nach diesen Vorgaben zu verfahren.

4. Sozialbehörden

4.1 Gesetz-Entwurf zur Weiterentwicklung der GKV

Beim einstweilen gescheiterten, aber nicht zu den Akten gelegten Entwurf eines Gesetzes zur Weiterentwicklung der Strukturreform in der gesetzlichen Krankenversicherung (GKVWeiterentwicklungsgesetz - GKVWG -) standen die neu gefaßten Vorschriften über Modellvorhaben zur "Weiterentwicklung der Versorgung" und Ziel einer Verbesserung der Qualität und der Wirtschaftlichkeit der Versorgung im Interesse des Datenschutzes. Ich hatte mich hierzu mit dem Bundesbeauftragten für den Datenschutz eingehend beraten:

Um sicherzustellen, daß im Rahmen dieser Modellvorhaben **keine personenbezogenen** Versichertenkonten entstehen, die ein umfassendes Bild der Gesundheitssituation, des gesundheitsbedeutsamen Verhaltens und der hierdurch verursachten Kosten ergeben, wurde von mir gegenüber dem Bundesbeauftragten für den Datenschutz für das Gesetzgebungsverfahren angeregt, daß Angaben über Versicherte im Rahmen von Modellvorhaben **nur fallbezogen, nicht versichertenbezogen** erhoben, verarbeitet und genutzt werden dürfen; eine derartige Regelung hätte auch der Förderung der Bereitschaft zur freiwilligen Teilnahme der Versicherten gedient. Um die datenschutzrechtlich gebotene Zweckbindung erhobener Daten zu gewährleisten, wurde weiter eine gesetzliche Regelung vorgeschlagen, wonach die im Rahmen eines Modellvorhabens erhobenen und gespeicherten Daten nur für Zwecke des Modellvorhabens verwendet werden dürfen und von den für Zwecke der Abrechnung und Wirtschaftlichkeitsprüfung zu übermittelnden Daten bei Kassenärztlichen Vereinigungen und Krankenkassen getrennt zu führen sind. Diese Forderungen wurden leider nicht mehr aufgenommen.

Allerdings sollten nach den Gesetzentwurf personenbezogene Daten nur mit schriftlicher Einwilligung der Betroffenen für Modellvorhaben erhoben, verarbeitet und genutzt werden dürfen (§ 63 Abs. 5 Satz 3 SGB V, Art. 1 Nr. 11 GKVWG -Bundesratsdrucksache 346/96 vom 24.05.1996).

Im Entwurf war auch nicht festgelegt, welche Arten von Datensammlungen und Auswertungen konzipiert werden könnten, da der **gesetzliche** Rahmen, in dem sich die Erhebung, Verarbeitung und Nutzung personenbezogener Daten für Modellvorhaben zu halten haben, sehr vage erschien;

das nähere sollten gemäß § 65 Abs. 3 SGB V die Vereinbarungen über die Durchführung von Modellvorhaben enthalten. Die **Grenzen** personenbezogener Datenverarbeitung von Gesundheitsdaten den Vereinbarungen der Verbände und den Satzungen zu überlassen, hätte dem Gebot, daß der Gesetzgeber so wesentliches selbst festlegen muß, wohl kaum entsprochen.

Nunmehr liegt ein neuer Gesetzentwurf vor, -2. GKV-Neuordnungsgesetz- (Bundesratsdrucksache 822/96 vom 08.11.1996). Darin wird die Einwilligung der Betroffenen in die personenbezogene Erhebung, Verarbeitung und Nutzung ihrer Daten bei Modellvorhaben nicht mehr vorgesehen. Vielmehr wird den Krankenkassen erlaubt, "die für **die Durchführung eines Modellvorhabens erforderlichen** personenbezogenen Daten" zu erheben, zu verarbeiten und zu nutzen. Den Leistungserbringern werden entsprechende Befugnisse zur Offenbarung von Patientendaten gegenüber Krankenkassen eingeräumt.

Der Eingriff in das informationelle Selbstbestimmungsrecht der Betroffenen wird damit massiv verstärkt. Es ist nach dem Entwurf auch **nicht erkennbar,** daß die für ein Modellvorhaben erhobenen und gespeicherten Daten **nur für Zwecke des Modellvorhabens verwendet werden dürften.** Es ist daher zu befürchten, daß z.B. wesentlich umfangreichere Informationen über Patienten als bisher personenbezogenen **erfaßt** und verarbeitet werden. Es ist auch zu befürchten, daß derartige, nur für Modellvorhaben erhobene Daten nach § 69 Abs. 1 Nr. 1 SGB X an andere Sozialleistungsträger übermittelt werden, z.B. an eine Berufsgenossenschaft. Nach den Regelungen des SGB X kommt sogar eine Übermittlung personenbezogener Erkenntnisse aus Modellvorhaben an Stellen außerhalb des Sozialleistungsbereichs und für ganz andere Zwecke in Betracht, z.B. nach § 71 Abs. 3 SGB X an das Vormundschaftsgericht oder nach § 73 SGB X an Strafverfolgungsorgane. Mit Satzungen von Krankenkassen, die allenfalls noch datenschutzrechtliche Vorsorge treffen könnten, lassen sich solche gesetzlich zugelassenen Nutzungsmöglichkeiten nicht verhindern. Dies hätte in einer auf Modellvorhaben zugeschnittenen Datenschutzregelung geschehen müssen.

Diese Entwicklung ist äußerst bedenklich.

4.2 Gesetzliche Krankenversicherung

4.2.1 Probleme mit dem ICD-10-Code zur Verschlüsselung von Diagnosen

Die durch das SGB V eingeführte Diagnoseverschlüsselung (ICD-10) hat zu heftigen Protesten der Ärzteschaft geführt. Die Zwecktauglichkeit des Codes wurde auch aus Datenschutzsicht in Frage gestellt, da eine Reihe von Einzel-Codes zu umfangreicheren Datenübermittlungen an die gesetzlichen Krankenkassen führen konnte, als zur dortigen Aufgabenerfüllung erforderlich. Der ICD-10 wurde daraufhin vom Bundesgesundheitsminister zur Überarbeitung und anschließenden Erprobung ausgesetzt. Erst Anfang 1998 soll er verbindlich eingeführt werden.

4.2.2 Erfährt es die Krankenkasse, wenn der Arzt nur "Verdacht auf ..." hatte oder zum "Ausschluß von ..." untersuchte?

Gleichzeitig mit der Einführung des ICD-10 ergab sich noch ein anderes Problem: Von einer Ärztin wurde ich darauf aufmerksam gemacht, daß nicht sichergestellt war, daß von Ärzten in ihrer Abrechnung gegenüber der Krankenversicherung angegebene, ganz entscheidende Zusätze bei Diagnosen, wie "V" = "Verdacht auf" oder "A" = "Ausschluß von" zusammen mit der Diagnose von der Kassenärztlichen Vereinigung an die gesetzliche Krankenversicherung weitergeleitet werden. Das hätte bedeutet, daß z.B. auch Diagnosen aus dem für die Betroffenen besonders belastenden psychotherapeutischen Bereich (die grundsätzlich auch von Internisten, Kinderärzten u.a. im Zuge der Abrechnung übermittelt werden könnten) bei der gesetzlichen Krankenkasse als **bestätigte** Diagnosen ankommen konnten und dementsprechend gespeichert und verarbeitet würden, ohne daß die vom behandelnden Arzt gegenüber der Kassenärztlichen Vereinigung angegebenen relativierenden Hinweise, daß es sich jeweils nur um Verdachtsfälle oder um Untersuchungen zum Ausschluß bestimmter Krankheiten handelte, mitberücksichtigt würden.

Zwar ist nach § 296 Abs. 2 SGB V im Regelfall die Abrechnungs-Datenübermittlung der Kassenärztlichen Vereinigung an die gesetzlichen Krankenkassen nur fallbezogen und nicht versichertenbezogen.

Für Ausnahmefälle gilt das nach dem Datenträgeraustauschvertrag aber nicht, z.B. bei Weitergabe an andere Kostenträger wegen Unzuständigkeit oder in Regreßfällen und für Wirtschaftlichkeitsprüfungen. Weiter werden für eine Übergangszeit Abrechnungsdaten noch personenbezogen

an die Krankenkassen übermittelt (vgl. meine Beanstandung im 16. Tätigkeitsbericht).

In all diesen Fällen würden mithin mißverständliche Diagnosen personenbezogen ohne die für ihre Richtigkeit wesentlichen Zusätze an die gesetzlichen Krankenkassen übermittelt.

Ich habe der Kassenärztlichen Vereinigung Bayerns unter Hinweis auf eine mögliche Beanstandung mitgeteilt, daß ich diese Informationsverkürzung, soweit sie personenbezogen ist, für einen schweren Datenschutzverstoß halte und gefordert, die Übermittlung dieser Zusätze sicherzustellen. Die KVB hat zugesichert, daß die Zusätze zusammen mit den Diagnosen unverändert an die Krankenkassen weitergeleitet werden.

4.2.3 Datenübermittlung von der Kassenzahnärztlichen Vereinigung Bayerns an die gesetzlichen Krankenkassen

Nach § 295 Abs. 2 des V. Buches des Sozialgesetzbuches (SGB V) übermitteln die Kassenzahnärztlichen Vereinigungen zum Zwecke der **Abrechnung** an die gesetzlichen Krankenkassen

- die **erforderlichen** Angaben über die von den Zahnärzten abgerechneten Leistungen,

- und zwar **"fallbezogen, nicht versichertenbezogen".**

Nach § 295 Abs. 3 SGB V vereinbaren die Spitzenverbände der Krankenkassen und die Kassenzahnärztliche Bundesvereinigung in Verträgen das Nähere über Einzelheiten des Datenträgeraustauschs. Da eine solche Vereinbarung nicht zustandekam, hat das zuständige Bundesschiedsamt mit Schiedsspruch vom 20.02.1995 den Umfang der Datenübermittlung für Abrechnungszwecke zwischen Kassenzahnärztlichen Vereinigungen und gesetzlichen Krankenkassen festgelegt.

Die in dem Schiedsspruch vorgesehenen Datenübermittlungen lassen sich aber mit dem Gebot des § 295 Abs. 2 SGB V, die Übermittlung von Abrechnungsdaten nur fallbezogen und nicht versichertenbezogen durchzuführen, nicht vereinbaren: Die vorgesehene Verfahrensweise führt

dazu, daß die Versicherten aus den von den KZVen zu übermittelnden Daten ohne Schwierigkeit reidentifiziert werden können. Außerdem ist von seiten der gesetzlichen Krankenkassen zu einigen im Schiedsspruch zur Übermittlung vorgesehenen Daten die Erforderlichkeit für Zwecke der Abrechnung nicht dargelegt worden. Die Spitzenverbände der gesetzlichen Krankenkassen haben dazu erklärt, daß genauere Begründungen für die Erforderlichkeit einzelner Daten erst gegeben werden könnten, wenn das von ihnen betriebene DV-Projekt für das Abrechnungsverfahren auf Kassenseite weit genug entwickelt sei. Von seiten der Kassenzahnärztlichen Vereinigungen wurde die Erforderlichkeit einer ganzen Reihe von Daten, die nach dem Schiedsspruch zu Abrechnungszwecken zu übermitteln wären, massiv bestritten. Der Nachweis, daß sich der automatisierte Datenaustausch von Kassenzahnärztlichen Vereinigungen zu den gesetzlichen Krankenkassen in dem durch § 295 Abs. 2 SGB V gezogenen Erforderlichkeits-Rahmen hält, steht damit noch aus.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat sich in der Frühjahrs- und Herbstsitzung 1996 mit diesen Fragen befaßt und in der Sitzung am 22./23. Oktober 1996 eine Entschließung zur automatisierten Übermittlung von Abrechnungsdaten durch Kassenzahnärztliche Vereinigungen an gesetzliche Krankenkassen gefaßt (siehe Anlage 3 dieses Berichts). Die Datenschutzbeauftragten begrüßen darin, daß inzwischen der größte Teil der gesetzlichen Krankenkassen in den "Protokollnotizen" vom 22. März 1996 den Umfang der zu übermittelnden Daten so reduziert hat, daß das Risiko der Identifizierbarkeit des Versicherten deutlich verringert wurde. Die Datenschutzbeauftragten fordern in der Entschließung den VdAK, der die Datenreduzierung noch nicht mitgetragen hat, auf, sich der Linie der anderen gesetzlichen Krankenkassen anzuschließen.
Die vorstehenden Ausführungen beziehen sich auf die Datenübermittlung für Zwecke der **Abrechnung** nach § 295 SGB V. Das Sozialgesetzbuch enthält darüber hinaus spezielle detaillierte Vorschriften für die Prüfung der Wirtschaftlichkeit der ärztlichen Abrechnung und sieht die Übermittlung ganz bestimmter Daten von den Kassenärztlichen und Kassenzahnärztlichen Vereinigungen an die GKV für diese Zwecke vor. Die Einschränkung des Umfanges der für Abrechnungszwecke zu ermittelnden Daten auf das nach § 295 SGB V gebotene Maß beeinflußt also nicht den Umfang der gesetzlich zulässigen Datenübermittlung für Zwecke der Wirtschaftlichkeitsprüfung.

Ich habe die gesetzlichen Krankenkassen in meiner Zuständigkeit und die Kassenzahnärztliche Vereinigung Bayerns aufgefordert umgehend mitzuteilen, in welchem Umfang nunmehr der maschinelle Datenaustausch KZVB/GKV, der Anfang 1997 aufgenommen werden soll, festgelegt wird. Das Bayerische Sozialministerium wurde hierüber unterrichtet.

4.2.4 Datenübermittlung von der Kassenärztlichen Vereinigung Bayerns an die gesetzlichen Krankenkassen fallbezogen - nicht versichertenbezogen

Im 16. Tätigkeitsbericht ist dargestellt worden, daß der für die Übergangszeit bis zur automatisierten Datenübermittlung zwischen KV und GKV vorgesehene Papierdatenaustausch den Vorgaben des § 295 Abs. 2 SGB V nicht entspricht und daher beanstandet werden mußte.

Die inzwischen im Bereich des Datenaustauschs zwischen Kassen**zahn**ärztlicher Vereinigung und gesetzlicher Krankenversicherung gewonnenen Erkenntnisse zur Beschränkung des Datenaustausches auf das erforderliche Maß und zur Übermittlung nur fallbezogen - nicht versichertenbezogen (siehe hierzu den vorstehenden Beitrag in diesem Tätigkeitsbericht) zeigen, daß auch im Bereich des automatisierten Datenaustauschs KV - GKV Nachbesserungen in diesen beiden Punkten erforderlich sind.

Ich habe daher die meiner Kontroll-Zuständigkeit unterliegenden gesetzlichen Krankenkassen und die Kassenärztliche Vereinigung Bayerns mit Schreiben vom 07.06.1995 sowie vom 15.04.1996 auf die im Zahnarztbereich gewonnenen Erkenntnisse hingewiesen und die Notwendigkeit der Anpassung des Datenaustauschs im Bereich der niedergelassenen Ärzte dargestellt. Mit Schreiben vom 21.08.1996 an die Gesetzliche Krankenversicherung in Bayern und vom 25.09.1996 an die Kassenärztliche Vereinigung Bayerns habe ich nochmals auf die Problematik der **leichten Zusammensortierbarkeit** der nach dem Datenaustauschvertrag getrennt zu übermittelnden Versicherten- und Leistungsdaten und zum Problem des **erforderlichen Datenumfangs** aufmerksam gemacht und auf die im Bereich der Kassenzahnärztlichen Vereinigungen unternommenen erheblichen Anstrengungen hingewiesen, die **Datenübermittlung nur fallbezogen** und **auf den erforderlichen Datenumfang beschränkt** durchzuführen. Nachdem ich auf beide Umstände bereits Mitte 1995 deutlich aufmerksam gemacht hatte, war hinreichend Zeit, sich mit den notwendigen Konsequenzen zu befassen. Ich habe die beteiligten Stellen ausdrücklich darauf hingewiesen, daß auch bei dem von ihnen vorgesehenen maschinellen Datenaustausch zur Abrechnung bei niedergelassenen Ärzten das Risiko eines Verstoßes gegen die Vorschrift des § 295 Abs. 2 SGB V besteht. Einen solchen würde ich ggf. beanstanden. Die in der Anlage 3 abgedruckte Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom Oktober 1996 habe ich an die gesetzlichen Krankenkassen und die Kassen-

ärztliche Vereinigung Bayerns übersandt.

Wie im Zahnarztbereich, so ist auch im Bereich der Abrechnung für niedergelassene Ärzte zu beachten, daß die Übermittlung von Daten für die Zwecke der Überprüfung der Wirtschaftlichkeit der ärztlichen Abrechnung im Gesetz speziell und ausführlich geregelt ist, so daß von der Beschränkung der Datenübermittlung für Abrechnungszwecke entsprechend den Vorgaben des § 295 Abs. 2 SGB V deshalb keine Einschränkungen für die Datenübermittlung für die gesetzlich vorgesehene Wirtschaftlichkeitsprüfung ausgehen.

4.2.5 Prüfung der Kassenärztlichen Vereinigung Bayerns (KVB) - Datenschutzrechtliche Kontrolle bei einer KVB-Bezirksstelle

Im Rahmen meiner Prüfung der Kassenärztlichen Vereinigung Bayerns habe ich eine datenschutzrechtliche Kontrolle bei einer KVB-Bezirksstelle vorgenommen. Gegenstand der Kontrolle waren die Erhebung personenbezogener Daten durch Formulare, die Nutzung erhobener Daten sowie regelmäßige Datenübermittlungen aus Karteien und Dateien.

Die Prüfung der Bezirksstelle konzentrierte sich auf die bezirksstellen-spezifische Datenverarbeitung der Abteilungen Abrechnung, Prüfung und Sicherstellung, umfaßte jedoch auch den Bereich Geschäftsführung mit Disziplinarausschuß. Sie führte zu keinen Erinnerungen gegen die bezirksstellen-spezifische Datenverarbeitung für die Abrechnung der Vertragsärzte und die Sicherstellung der vertragsärztlichen Versorgung. Es ergaben sich nur die beiden folgenden Anmerkungen:

a) Datei "Übersicht über Disziplinarverfahren (Disziplinarausschuß)"

Die Bezirksstelle speichert in dieser Datei Ärzte, gegen die im Rahmen einer Disziplinarmaßnahme durch den Disziplinarausschuß ermittelt wurde; gespeichert werden auch die getroffenen Maßnahmen, z.B. "Verfahren eingestellt", "Verweis" usw. Dort fanden sich auch noch sehr lange zurückliegende Eintragungen, während nach Aussage der Bezirksstelle entsprechende Eintragungen **in der Arztakte** bereits nach fünf Jahren gelöscht werden. Ich habe die KVB aufgefordert, die Verfahrensweise zu überprüfen. Inzwischen hat die Bezirksstelle alle über diese Frist hinausgehenden Eintragungen aus der Datei gelöscht.

b) "Vergütungsliste"

Der Leiter der Personalstelle führt für jede Abteilung der Bezirksstelle die sog. "Vergütungsliste", die zur Entscheidung über Umgruppierungen aufgrund der Vorschriften des Personalvertretungsgesetzes und des Betriebsverfassungsgesetzes dient. U.a. ist darin folgende Fußnote enthalten: "Schwerbehinderung in % angeben".

Nach Auskunft der Bezirksstelle signalisiert die Angabe "Schwerbehinderung in %", daß für Betroffene mit einem Grad der Behinderung (GdB) von mindestens 30 % bei gesonderter Entscheidung des Betriebsarztes Zusatzurlaub gewährt werden kann, wie dies für Bedienstete ab einem GdB von mindestens 50 % bereits kraft Gesetzes der Fall ist. Die Angabe, ob der GdB mindestens 50 % beträgt, ist für die Meldungen über die Betroffenen an die Landesgeschäftsstelle der KVB zur Erfüllung der Meldepflichten nach § 13 Schwerbehindertengesetz nötig.

Ich habe um Überprüfung gebeten, ob die Angabe des GdB in der Vergütungsliste mit den Abstufungen "mindestens 30" und "mindestens 50" genügt, da die konkrete Angabe des GdB über die genannten Abstufungen hinaus in der Vergütungsliste bzw. möglicherweise für die gesamte Tätigkeit der Personalstelle nicht erforderlich ist.

c) Datenerhebungsformulare:

Bei der Prüfung wurden zwei Formulare, mit denen personenbezogene Daten von Ärzten erhoben werden, festgestellt, auf denen die vorgeschriebene Datenschutzklausel fehlte.

Die KVB-Bezirksstelle hat die Ergänzung der Formulare um entsprechende Datenschutzklauseln zugesichert.

d) Aufbewahrungsfristen:

Bei der Prüfung wurde eine uneinheitliche Handhabung von Aufbewahrungsfristen mancher Unterlagen festgestellt. Die KVB hat mitgeteilt, daß die Organisationsanweisung über die Aufbewahrungsfristen überarbeitet und eine einheitliche Handhabung der Fristen in die Bezirksstellen sichergestellt wird.

4.2.6 Prüfung der Datenverarbeitung bei einer AOK-Direktion im Zusammenhang mit der Leistungsabrechnung

Gegenstand der Kontrolle waren Datenerhebung, -verarbeitung und -nutzung für die Abrechnung der Leistungen niedergelassener Ärzte - insbesondere der personenbezogene Datenfluß zwischen der Kassenärztlichen Vereinigung Bayerns (KVB) und der AOK-Direktion - sowie für die Wirtschaftlichkeits- und Stichprobenprüfungen. Überprüft wurden auch die Datenerhebung und -verwendung für nicht über die KVB laufende Leistungsabrechnungen (Apotheken, sonstige Leistungserbringer). Wesentliche Ergebnisse waren:

a) Datenübermittlung KVB-AOK "nur fallbezogen":

Zum Datenfluß zwischen KVB und AOK-Direktion zur Abrechnung ärztlicher Vergütungen wurde festgestellt, daß keine **ausschließlich fallbezogene und nicht versichertenbezogene** Abrechnungsdaten-Übermittlung an die Krankenkasse erfolgt, wie § 295 Abs. 2 SGB V dies vorschreibt. Diesen Verstoß hatte ich gegenüber der KVB und den Bayer. Krankenkassen bereits im November 1994 beanstandet (Ziffer 3.2.1 des 16. Tätigkeitsberichts 1994) und gefordert, daß die von der KVB übermittelten versichertenbezogenen Leistungsdaten mit Diagnosen auf Kassen-Seite nur so verarbeitet und genutzt werden, daß der Versichertenbezug - soweit nicht gesetzlich zugelassen - nicht genutzt und kein versichertenbezogenes Leistungskonto über ambulante Leistungen aufgebaut wird. Ein Verstoß gegen meine obige Forderung wurde bei der Kontrolle nicht festgestellt.

b) Versichertendaten im gemeinsamen Prüfungsausschuß von KVB und gesetzlichen Krankenkassen:

Bei der Wirtschaftlichkeitsprüfung erhalten AOK-Mitarbeiter im Prüfungsausschuß personenbezogene Behandlungsscheine bzw. "erweiterte Leistungsnachweise" nur bei Bedarf im Einzelfall (maximal bei ca. 5% der zu prüfenden Ärzte) vorgelegt. Die Datennutzung dieser Unterlagen erstreckt sich in fast allen Fällen praktisch ausschließlich auf die

Fallbeurteilung und nicht auf die Person (Identität) des Versicherten. Weil dieser Personenbezug im Normalfall nicht benötigt wird, habe ich gefordert, den **Versichertennamen für die Tätigkeit des Prüfungsausschusses maschinell zu unterdrücken,** sobald dies technisch möglich ist.

§ 14 Abs. 4 der bayerischen Prüfungsvereinbarung über das Verfahren zur Überwachung und Prüfung der Wirtschaftlichkeit (Auffälligkeitsprüfung ärztlicher Verordnungsweise) schreibt vor, für einen von der Prüfung betroffenen Vertragsarzt "dem Prüfungsausschuß die Behandlungsausweise des betreffenden Zeitraumes **mit den Arzneiverordnungsblättern** zur Verfügung zu stellen. Dabei sind für eine repräsentative Zahl von Behandlungsfällen (10%, mindestens aber 30 Fälle) die Arzneiverordnungsblätter **nach Patienten zu sortieren**." Außer für die Einzelfallprüfung nach § 298 SGB V (§ 15 Prüfungsvereinbarung) ist eine **gesetzliche Befugnis hierzu nicht ersichtlich**. Das Bayer. StMAS wurde um Äußerung gebeten, ob die **auf Einzelfälle abstellende** Vorschrift des § 298 SGB V diese nach der Prüfungsvereinbarung vorgesehenen Datenübermittlungen abdeckt.

c) Kenntnisnahme der gesetzlichen Krankenkasse von Versichertendaten bei "Plausibilitätsprüfungen" nach § 83 Abs. 2 SGB V:

Gemäß § 83 Abs. 2 Satz 1 SGB V können **Kassenärztliche Vereinigungen Plausibilitätskontrollen** ärztlicher Abrechnungen vornehmen. Für eine Beteiligung der **Krankenkassen** an einem "Abstimmungsgespräch" zwischen KVB und Verbänden der Krankenkassen im Vorfeld der eigentlichen Plausibilitätsprüfung kann allenfalls darauf hingewiesen werden, daß nach der genannten Vorschrift in den Gesamtverträgen Verfahren zu vereinbaren sind, die Plausibilitätskontrollen ermöglichen. Es ist jedoch keine Rechtsvorschrift im SGB V ersichtlich, die eine Übermittlung arztbezogener Daten zur Vorbereitung dieses Abstimmungsgesprächs in der "ergänzenden Übersicht zur Tagesstatistik für die ermittelten meistfrequentierten Behandlungstage" (KVB-Statistik) und die Übermittlung der arztbezogenen Ergebnisse durchgeführter Plausibilitätsprüfungen durch die KVB an die Krankenkassen gestatten würden. Ich habe diese Problematik an die AOK

Bayern - Zentrale - herangetragen und sie auch im Rahmen der noch nicht abgeschlossenen Prüfung der Kassenärztlichen Vereinigung Bayerns zur Sprache gebracht.

4.2.7 Angabe von Diagnosen auf Heil- und Hilfsmittelverordnungen

Auf den Rezepten für Heil- und Hilfsmittel - z.B. Massage, Rollstuhl - stehen in der Regel Diagnosen. Die "Leistungserbringer" - z.B. Masseure - geben die Rezepte mit Diagnose zur Abrechnung an die Krankenkasse weiter. Das Sozialgesetzbuch gibt jedoch den Leistungserbringern keine Befugnis zur Offenbarung der versichertenbezogenen Diagnose gegenüber der Krankenkasse. Die Datenschutzbeauftragten setzen sich daher für eine Veränderung der Verfahrensweise ein.

Nach den vom Bundesausschuß der Ärzte und Krankenkassen erlassenen Heil- und Hilfsmittel-Richtlinien müssen die Vertragsärzte auf dem Verordnungsblatt (Rezept) grundsätzlich auch die Diagnose angeben. Nach den Richtlinien der Spitzenverbände der Krankenkassen über das Abrechnungsverfahren der "sonstigen Leistungserbringer" müssen letztere die Verordnungsblätter (Rezepte) mit Diagnose im Original an die Krankenkassen übermitteln. Daher erhält - im Gegensatz zu Apotheken-Rezepten - die Krankenkasse bei Rezepten für "sonstige Leistungserbringer" Kenntnis von der Diagnose.

Die genannten Richtlinien sind jedoch keine Rechtsgrundlage für die Mitteilung der Diagnosen **an die Krankenkassen**. Die Diagnose-Angabe auf den ärztlichen Verordnungen wird zwar in den meisten Fällen notwendig sein, damit die Heil- und Hilfsmittelerbringer ihre Leistung überhaupt richtig erbringen können; die Übergabe der Verordnung an den Leistungserbringer enthält die konkludente Einwilligung des Patienten in **diese** Offenbarung. Für eine Übermittlung von Diagnose und ggf. Befunden **durch Leistungserbringer an die Krankenkassen** im Zuge der Abrechnung fehlt aber eine gesetzliche Befugnis (§ 302 SGB V). Die Annahme, in der Weitergabe der ärztlichen Verordnung an den Leistungserbringer liege eine konkludente Einwilligung des Versicherten in die Weitergabe der Verordnung mit Diagnose/Befund durch den Leistungserbringer an die Krankenkasse, halte ich für unzutreffend.

Die Krankenkassen argumentieren, nur in Kenntnis der Diagnose und ggf. weiterer Befunde könnten sie ihre Leistungspflicht prüfen und klären, ob die erbrachte Leistung im Sinne der §§ 2 und 12 SGB V notwendig und wirtschaftlich gewesen sei. Es gehöre im übrigen zu den Mitwirkungspflichten des Versicherten, dem Leistungsträger die für die Leistungsgewährung erforder-

lichen Tatsachen anzugeben und auf Verlangen des Leistungsträgers einer Übermittlung der Angaben durch Dritte zuzustimmen; eine Verweigerung der Zustimmung würde die Möglichkeit eröffnen, die Leistung einstweilen zu verweigern.

Ich halte jedoch die Erforderlichkeit der Diagnosen-Kenntnis durch die Krankenkassen im Regelfall der Verordnungsabrechnung für nicht ausreichend dargelegt. Für **Wirtschaftlichkeitsprüfungen der Verordnungen** dürfen Diagnosen nur bei Einzelfallprüfungen nach § 298 und Stichprobenprüfungen nach § 297 SGB V den Krankenkassen versichertenbezogen zur Verfügung gestellt und von diesen genutzt werden. Für diese gesetzlich vorgesehenen Prüfzwecke könnte die Kasse die vom Arzt gefundenen Diagnosen wie bei der Einzelfall- und Stichprobenprüfung von **Arznei**verordnungen von der Kassenärztlichen Vereinigung erhalten. Auf **Arznei**verordnungen sind keine Diagnosen oder Befunde angegeben, obwohl die Interessen der Krankenkassen an derartigen Kenntnissen durchaus identisch sein könnten. Da Diagnosen bei der Abrechnung **vom Arzt erbrachter Leistungen** nur fall- und nicht versichertenbezogen an die Krankenkassen übermittelt werden dürfen (§ 295 Abs. 2 SGB V), können Arzneiverordnungen nur über die Hilfestellung der Kassenärztlichen Vereinigung in gesetzeskonformer Weise **und nur in den vom Gesetz vorgesehenen Fällen** mit den Diagnosen zusammengeführt werden; mangels weitergehender gesetzlicher Regelung muß dies auch für Verordnungen von Heil- und Hilfsmitteln gelten.

Ich habe meinen Datenschutz-Kollegen und der Arbeitsgemeinschaft der Krankenkassenverbände in Bayern vorgeschlagen, daß Diagnosen und ggf. Befunde zwar auf dem Rezept-Exemplar für den Leistungserbringer, nicht aber auf einem für die Krankenkasse bestimmten **weiteren Exemplar bzw. Durchschlag** lesbar sein dürfen. Die auch auf Bundesebene geführte Diskussion hierzu ist noch nicht abgeschlossen.

4.2.8 Beanstandung der Herausgabe eines "erweiterten Leistungsnachweises" für ein Ermittlungsverfahren

Im Rahmen eines Ermittlungsverfahrens der Staatsanwaltschaft gegen einen Frauenarzt wegen Verdachts der fahrlässigen Tötung einer Patientin legte der Witwer einen sog. "erweiterten Leistungsnachweis" (Abrechnungsunterlagen) für die betreffende Arztpraxis vor, der über die Daten der verstorbenen Patientin hinaus auch **Namen, Geburtsdatum, Diagnosen bzw. Befunde** sowie die **Behandlungs-** und **Abrechnungsdaten 37 weiterer unbeteiligter** Patientinnen enthielt. Meine Ermittlungen ergaben, daß der Witwer die Praxis-Abrechnungsunterlagen bezüglich seiner verstorbenen Frau von der **Krankenkasse** zur Unterstützung bei der Verfolgung von Schadensersatzansprüchen aus Behandlungsfehlern (§ 66 SGB V) erhalten hatte; daß dabei datenschutzwidrig auch die sensiblen personenbezogenen Daten 37 unbeteiligter Patientinnen herausgegeben bzw. vorher nicht unkenntlich gemacht worden waren, wurde seitens der Krankenkasse als "bedauerlicher, individueller Arbeitsfehler" des Krankenkassenmitarbeiters kommentiert.

Ich habe angesichts der Schwere und Offensichtlichkeit dieses Verstoßes gegen die Verpflichtung zur Wahrung des Sozialgeheimnisses eine Beanstandung gemäß Art. 31 BayDSG ausgesprochen, auch wenn sich der dargestellte Datenschutz-Verstoß aufgrund von Änderungen im Abrechnungsverfahren mit den Krankenkassen in dieser Form nicht wiederholen kann.

4.3 Pflegeversicherung

4.3.1 Pflegebedürftigkeitsrichtlinien - Formular-Gutachten zur Pflegebedürftigkeit

Nach dem Gesetz hat der MDK der Pflegekasse nur "das Ergebnis seiner Prüfung" mitzuteilen. Richtlinien der Pflegekassen und das eingesetzte DV-Verfahren zwingen den MDK jedoch dazu, der Pflegekasse den gesamten Inhalt seines Erhebungsformulars zu übermitteln. Die Datenschutzbeauftragten bemühen sich daher um eine Änderung der Richtlinien und des DV-Verfahrens.

Auf Grund § 17 SGB XI haben die Spitzenverbände der Pflegekassen bundeseinheitliche Pflegebedürftigkeitsrichtlinien beschlossen (PflRi vom 7.11.1994/21.12.1995). Nach diesen wird der Medizinische Dienst der Krankenversicherung (MDK) verpflichtet, das "Ergebnis seiner Prüfung" der Pflegekasse in einem den Richtlinien als Anlage beigefügten umfangreichen Gutachten-Formular mitzuteilen. Meines Erachtens geht dieses Gutachten-Formular inhaltlich über die nach § 18 Abs. 5 SGB XI vorgesehene **Ergebnis**mitteilung an die Pflegekasse hinaus, weil das Formular auch detaillierte Angaben zur gesundheitlichen Situation des Betroffenen und zu seinen "Fähigkeiten in Bezug auf die Aktivitäten des täglichen Lebens" enthält, die der MDK zwar zur Ergebnis**findung** benötigt, deren vollständige Übermittlung an die Pflegekasse aber die **gesetzlich gerade nicht vorgesehene Mitteilung aller** vom MDK erhobenen Daten bedeutet. Im gesetzlich vorgesehenen Rahmen der Ergebnismitteilung liegen wohl hauptsächlich die Inhalte der Ziffern 5 - 7 des Gutachtens, nämlich die Angaben über die "Bestimmung der Pflegebedürftigkeit", das "Ergebnis der Prüfung des Vorliegens von Pflegebedürftigkeit" und die "Empfehlungen an die Pflegekasse/individueller Pflegeplan" und allenfalls **einzelne** Angaben aus den o.a. vorangehenden Ziffern.

Meine datenschutzrechtliche Kontrolle beim MDK in Bayern - Hauptverwaltung - ergab, daß diese Gutachten unter Verwendung des DV-Systems "ISmed" erstellt werden, das den MDKStellen in den Ländern zentral und einheitlich vom Medizinischen Dienst der Spitzenverbände (MDS) zur Verfügung gestellt wird (siehe auch Ziffer 4.4.1). Der MDK in Bayern hat derzeit keine Möglichkeit, den maschinellen Ausdruck des Gutachtens zu beeinflussen - etwa durch Nicht-Ausdruck einzelner Angaben, die über das mitzuteilende Ergebnis seiner Prüfung hinausgehen.

Nach Auffassung der Spitzenverbände der Pflegekassen würde - wenn ausschließlich die Angaben in den Ziffern 5 - 7 des Gutachtens übermittelt würden - faktisch eine Entscheidungskompetenz des MDK begründet, mit bindender Wirkung für die Pflegekassen festzustellen, ob und welche Leistungen durch die Pflegeversicherung zu gewähren sind. Angaben aus dem gesamten Gutachten würden desweiteren zur Begründung des Verwaltungsakts benötigt. Das Bundesministerium für Arbeit teilte dem Bundesbeauftragten für den Datenschutz hierzu u.a. mit, eine eigene Entscheidungskompetenz des MDK über die Pflegebedürftigkeit sei nicht gegeben, der MDK würde die anhand des MDK-Gutachtens zu treffende Verwaltungsentscheidung der Pflegekasse nur vorbereiten. Die Pflegekasse sei berechtigt, sich über alle gutachterlichen Feststellungen des MDK im Verfahren zur Feststellung der Pflegebedürftigkeit umfassend zu informieren.

Ich räume ein, daß die fachliche Feststellung der für die Entscheidung der Pflegekasse über die Leistungsgewährung erforderlichen Angaben schwierig ist. Aber auch der MDK in Bayern neigt zu der Auffassung, daß grundsätzlich nicht alle vom MDK für die Untersuchung benötigten, erhobenen und im EDV-Gutachten festgehaltenen Angaben für die Entscheidung **der Pflegekasse** erforderlich sind. Ich habe den MDK gebeten, sich nochmals detailliert mit dieser Frage auseinanderzusetzen und mir Vorschläge zum Umfang reduzierter Ergebnismitteilungen zu übermitteln. Ein verfahrenstechnischer Lösungsansatz könnte evtl. darin bestehen, daß der MDK durch Erweiterung des ISmed-Verfahrens in die Lage versetzt wird, ohne größeren Aufwand EDV-technisch eine **inhaltlich reduzierte Gutachtensversion für die Pflegekasse** zu erstellen, gleichwohl aber **den Ausdruck des vollständigen Gutachtens beim MDK aufzubewahren**; im Falle der Anfechtung des von der Pflegekasse erteilten Bescheids durch die Pflegebedürftigen könnten vom MDK ggf. erforderliche detailliertere Angaben "nachgeliefert" werden. Insbesondere bei vollständiger Gewährung beantragter Leistungen wäre eine Beschränkung auf wenige Ergebnisdaten denkbar, zumal in diesen Fällen gemäß § 35 Abs. 2 Nr. 1 SGB X keine Begründung des Verwaltungsakts der Pflegekasse erforderlich ist.

Das Staatsministerium für Arbeit und Sozialordnung, Familie, Frauen und Gesundheit hat zu meinen Vorstellungen darauf hingewiesen, daß nach den o.g. **Richtlinien** das Formulargutachten in vollem Umfang an die Pflegekasse zu übermitteln ist. Dem ist jedoch entgegenzuhalten, daß die Richtlinien keine gesetzliche Datenübermittlungsgrundlage ersetzen können. Sobald die vom MDK erbetenen Vorschläge vorliegen, werde ich mich daher an den Bundesbeauftragten für den

Datenschutz wenden, um auf Bundesebene eine Änderung der Richtlinien anzustoßen.

4.3.2 Gemeinsame Verarbeitung und Nutzung personenbezogener Daten durch Pflegekasse und Krankenkasse gemäß § 96 SGB XI

Wenn gesetzliche Pflegekassen z.B. Diagnosen aus Krankenkassenunterlagen verwenden wollen, brauchen sie in vielen Fällen die Einwilligung der Betroffenen

Gemäß § 96 SGB XI können die Spitzenverbände der Pflegekassen und der Krankenkassen gemeinsam und einheitlich festlegen, daß Pflegekassen und Krankenkassen die in dieser Vorschrift näher genannten Arten von personenbezogenen Daten gemeinsam verarbeiten und nutzen, soweit sie für ihre jeweiligen Aufgaben dieselben Daten benötigen bzw. soweit dies zur Vermeidung von Doppelleistungen erforderlich ist. Nach dieser Vorschrift müssen **die Daten, die gemeinsam verarbeitet und genutzt werden sollen, abschließend** unter Beteiligung des Bundesbeauftragten für den Datenschutz und des BMA **festgelegt werden**. Eine erste Version eines solchen Katalogs liegt vor; sie ist jedoch angesichts des hinsichtlich verschiedener Datenarten unzureichenden Differenzierungsgrads noch verbesserungsbedürftig.

Nach § 96 **Abs. 2** SGB XI i.V.m. § 76 SGB X dürfen, unabhängig von der abschließenden Festlegung des Datenkatalogs, personenbezogene Daten, die einer Krankenkasse oder Pflegekasse (insbesondere) **von einem Arzt zugänglich gemacht** wurden, nicht ohne weiteres in die gemeinsame Verarbeitung und Nutzung einbezogen werden. Soweit die Pflegekasse Daten aus dem Bereich der Krankenkasse nutzen will, wie etwa Abrechnungsdaten von Krankenhäusern (§ 301 SGB V) oder Diagnosen aus Arbeitsunfähigkeitsbescheinigungen, benötigt sie hierzu **die Einwilligung des Betroffenen** (für die in § 76 **Abs. 2** SGB X genannten Daten aus Begutachtungen oder Bescheinigungen besteht dagegen lediglich ein Widerspruchsrecht des Betroffenen gegen die Übermittlung an/Nutzung durch die Pflegekasse).

Ich habe daher empfohlen, die Einwilligungserklärung in den Anträgen auf Pflegeleistungen etwa folgendermaßen zu ergänzen: "Diese Einwilligung gilt auch für Daten, die der Krankenkasse von einem Arzt oder einer anderen Person, die wie ein Arzt zur Verschwiegenheit verpflichtet ist, zur Verfügung gestellt wurden (z.B. Abrechnungsdiagnosen und Behandlungsdaten von Krankenhäusern sowie Diagnosen aus AU-Bescheinigungen): Ja / Nein". Falls Betroffene z.B.

glauben, daß die der Krankenkasse vorliegenden Diagnosen hinsichtlich der richtigen Beschreibung ihres Gesundheitszustandes irreführend sein könnten, können sie zusätzliche Hinweise auf Daten über ihren tatsächlichen Gesundheitszustand an die Pflegekasse geben oder die Einwilligung (bei einer nachvollziehbaren Begründung) mit der Folge verweigern, daß der MDK ihren Gesundheitszustand umfassender aufklären muß. Auf diese Folge ist der Betroffene hinzuweisen.

Die Diskussion mit den Pflegekassen und dem Staatsministerium für Arbeit und Sozialordnung, Familie, Frauen und Gesundheit zu dieser Problematik konnte noch nicht abgeschlossen werden.

4.4 Medizinischer Dienst der Krankenversicherung (MDK)

4.4.1 Prüfung des MDK in Bayern - Hauptverwaltung -

Entspricht Datenerhebung und Datenverarbeitung beim MDK den gesetzlichen Vorgaben? - Keine Identifizierbarkeit der Betroffenen in der automatisiert auswertbaren medizinischen Datei? Mitteilung an die auftraggebende Krankenkasse nur über das "Ergebnis" der Begutachtung! Keine Mitteilung an behandelnde Ärzte bei Widerspruch des Patienten!

Im Berichtszeitraum habe ich u.a. eine datenschutz**rechtliche** Prüfung bei der Hauptverwaltung des MDK in Bayern durchgeführt. Die Kontrolle der Datenerhebung und -verwendung beschränkte sich auf die Aufgabenabwicklung des MDK im Bereich des Sozialgesetzbuches (SGB). Wesentliche Ergebnisse waren:

a) Automatisierte Gutachtenspeicherung:

Der MDK darf nach den §§ 276 Abs. 2 Satz 6 SGB V/97 Abs. 3 Satz 3 SGB XI **in Dateien** nur Angaben zur Person und **Hinweise** auf bei ihm vorhandene Akten aufnehmen. In Dateien dürfen über die übliche Abwicklungsdauer eines Begutachtungsverfahrens (mit EDV-unterstützter Gutachtenerstellung) hinaus automatisiert auswertbare medizinische

Begutachtungsergebnisse **nur so** gespeichert werden, daß **keine Identifizierung der begutachteten Personen mehr möglich ist**.

Der MDK in Bayern verwendet das bundeseinheitlich vom Medizinischen Dienst der Spitzenverbände (MDS) zur Verfügung gestellte DV-System "ISmed". Zur Beurteilung dieses Verfahrens habe ich noch nähere technische Erläuterungen durch den MDK erbeten, insbesondere inwieweit hier von **einzelnen Dateien** gesprochen werden kann und inwieweit **Querverbindungen** zwischen den einzelnen Anwendungen realisiert werden. Datenschutzrechtlich problematisch erschien mir bei ISmed jedenfalls die sog. "Statistik-Datei" und die "Statistik-Datei Pflege". Auch hier bedarf es noch genauer Erläuterungen über die (auch MDKinternen) Verwendungszwecke dieser Statistik-Dateien. Auf den ersten Blick erscheinen beide Statistik-Dateien nicht patientenbezogen; sie enthalten jedoch Zuordnungsmerkmale, die den begutachteten Versicherten grundsätzlich durch Herstellung von Querverbindungen mit anderen Anwendungen/Dateien im ISmed identifizierbar machen könnten. Hierzu kann insbesondere das Suchkriterium des Geburtsdatums begutachteter Personen herangezogen werden, in Betracht kommen jedoch auch Angaben über das Datum der Begutachtung bzw. der Gutachtenerstellung, über Gutachter sowie über das Institutionskennzeichen der Kranken- bzw. Pflegekasse, bei der "Statistik-Datei Pflege" und über die vollständige Postleitzahl von Wohnung und Aufenthaltsort des Untersuchten. Ich halte es derzeit deshalb **nicht für sichergestellt**, daß ISmed keine Möglichkeit bietet, die genannten Statistik-Datensätze maschinell mit Identitätsdaten betroffener Patienten zu verknüpfen.

Ich habe daher gegenüber dem MDK in Bayern die Forderung erhoben, die Datensätze inhaltlich so zu gestalten, daß den o.g. gesetzlichen Vorschriften Rechnung getragen wird **und versichertenbezogene Auswertungen der Statistik-Dateien nicht realisierbar sind.** Andernfalls könnten möglicherweise Angaben aus den Gutachten über den Gesundheitszustand bzw. bei Pflegebedürftigen auch über deren Lebensumstände bzw. soziale Situation maschinell durchsucht und personenbezogene bzw. -beziehbare Ergebnisse ausgeworfen werden, was der Gesetzgeber gerade verhindern wollte.

b) Mitteilung des Untersuchungsergebnisses an die gesetzliche Krankenkasse:

Gemäß § 277 Abs. 1 SGB V hat der MDK der Krankenkasse das **Ergebnis** der Begutachtung und "die erforderlichen Angaben über den Befund" mitzuteilen. Laut Aussage des MDK stellt der Umfang dieser Mitteilungen ein von verschiedensten Seiten immer wieder diskutiertes, bisher nicht einheitlich gelöstes Problem dar; vereinheitlichte Vorgaben für die Gutachtensinhalte seien aber durchaus erstrebenswert.

Ich habe den MDK gebeten, Vorschläge zum erforderlichen Inhalt und zur technischen Umsetzung dieser Ergebnismitteilungen zu entwerfen und abzustimmen. Beim MDS müßte anschließend evtl. eine Erweiterung des ISmed-Verfahrens angeregt werden, damit der Umfang der Gutachten ohne manuellen Löschungsaufwand variiert werden kann. Das ausgedruckt zur Archivierung beim MDK vorgesehene Gutachten-Exemplar könnte dann im Hinblick auf evtl. Folgebegutachtungen detaillierter gehalten werden, während an die Krankenkasse eine inhaltlich auf das gesetzlich vorgesehene Maß ("Ergebnis" und "erforderliche Angaben über Befund") reduzierte Version weiterzuleiten wäre (derzeit ist dies aufgrund des Zeit- und Arbeitsaufwands dieser bisher nur manuell herstellbaren Alternativen nicht möglich).

Zur ähnlichen Problematik der Erstellung und des Umfangs der **Gutachten zur Feststellung der Pflegebedürftigkeit nach dem SGB XI** wird auf die Ausführungen unter Ziffer 4.3.1 verwiesen.

c) Mitteilung an behandelnde Ärzte:

Der MDK ist nach § 277 SGB V befugt, Ärzten und sonstigen Leistungserbringern, über deren Leistungen er im Auftrag der Krankenkasse eine gutachtliche Stellungnahme abgegeben hat, "die erforderlichen Angaben über den Befund mitzuteilen"; der Versicherte kann dieser Mitteilung jedoch widersprechen. Der MDK in Bayern wies bei der Begutachtung bisher grundsätzlich nur mündlich auf dieses Widerspruchsrecht hin; dokumentiert wurde der Hinweis nur "bei kritischen Fällen" oder sehr sensiblen Erkenntnissen. Ich

habe begrüßt, daß der Hinweis unmittelbar nach der Begutachtung gegeben wird, weil der Betroffene erst nach Kenntnis des Befundes fundiert über seinen Widerspruch entscheiden kann. Zur Nachprüfbarkeit des Hinweises muß dessen Erteilung jedoch in allen Fällen schriftlich dokumentiert werden.

4.4.2 Zuleitung einer ärztlichen Mitteilung an den MDK - unmittelbar oder über die Krankenkasse?

Die "Leistungserbringer" (z.B. Ärzte) sind - wenn die Krankenkassen nach § 275 Abs. 1 bis 3 SGB V eine gutachtliche Stellungnahme oder Prüfung durch den MDK veranlaßt haben - verpflichtet, Sozialdaten **auf Anforderung des MDK** unmittelbar an diesen zu übermitteln, soweit dies für die gutachtliche Stellungnahme und Prüfung erforderlich ist (§ 276 Abs. 2 SGB V). Ärzte und sonstige Leistungserbringer müssen daher bei diesen Fallgestaltungen sicherstellen, daß für den MDK bestimmte personenbezogene Patientendaten diesem unmittelbar übersandt werden. Für den Fall, daß Krankenkassen **anstelle des MDK** derartige Datenübermittlungen erbitten - z.B. wegen einer Überlastungssituation des MDK - muß auf dem der Datenanforderung beigelegten Versand-Kuvert die **Anschrift des MDK** angegeben sein; andernfalls müssen die Leistungserbringer die für den MDK bestimmten Daten so versenden, daß sich in dem Kuvert an die Krankenkasse ein weiteres verschlossenes Kuvert für den MDK befindet, das von der Krankenkasse **ungeöffnet** an diesen weiterzuleiten ist. **Die Kenntnisnahme seitens der Krankenkassen vom Inhalt solcher Datenübermittlungen an den MDK ist angesichts § 276 Abs. 2 SGB V auszuschließen.**

4.4.3 Übermittlung von Fremdbefunden durch Ärzte an den MDK

Unterschiedlich beurteilt wird, ob Ärzte verpflichtet sind, dem MDK für seine gutachtlichen Stellungnahmen oder Prüfungen auch sog. "Fremdbefunde" wie z.B. Krankenhaus-Entlassungsberichte, Arztbriefe mitbehandelnder Ärzte usw. zu übersenden. Diese Verpflichtung kann den Interessen sowohl des übersendenden Arztes als auch des Arztes, von dem die Unterlagen ursprünglich stammen, zuwiderlaufen. Nicht immer sind dem übersendenden Arzt nämlich die Aktualität nicht von ihm selbst stammender Unterlagen und medizinischer Zusammenhänge sowie auch die Vollständigkeit anderweitig durchgeführter Untersuchungen erkennbar.

Soweit der Leistungserbringer die Richtigkeit der Fremdbefunde selbst beurteilen kann und diese mitträgt, ist deren Mitteilung bzw. Übersendung an den MDK aus Datenschutzsicht zulässig; die Übersendung ersetzt dann sowohl weiterreichende und ausführlichere eigene Auskünfte als auch die zeitaufwendige Anforderung von Auskünften Dritter durch den MDK. Allerdings darf meines Erachtens vom Vertragsarzt keine undifferenzierte Vorlage aller bei ihm existierenden Unterlagen gefordert werden; es muß in das pflichtgemäße AuswahlErmessen des auskunftspflichtigen Arztes gestellt werden, welche Unterlagen er zur Abfassung seiner Auskünfte verwendet, ob und welche Befundunterlagen er diesen Auskünften beifügt und ob er statt der Übermittlung von Fremdbefunden dem MDK den erstellenden Arzt benennt.

4.4.4 Erhebung von Daten zur Gesundheit eines Patienten durch die Krankenkasse beim Arzt - stets nur über den MDK oder auch direkt?

§ 275 SGB V regelt, in welchen Fällen Krankenkassen **verpflichtet** sind, beim MDK eine gutachtliche Stellungnahme einzuholen bzw. eine Überprüfung vornehmen zu lassen, und welche Überprüfungen sie "in geeigneten Fällen" durch den MDK vornehmen lassen **können**. **Wenn und soweit die Krankenkassen den MDK einschalten**, sind die Leistungserbringer verpflichtet, Patientendaten im erforderlichen Umfang auf Anforderung des MDK **unmittelbar dorthin** zu übermitteln (vergl. hierzu auch Ziffer 4.4.2).

Ganz allgemein besteht jedoch gemäß § 100 SGB X für Ärzte oder Angehörige eines anderen Heilberufs die Verpflichtung, Leistungsträgern wie z.B. der Krankenkasse im Einzelfall auf Verlangen die zur dortigen Erfüllung von Aufgaben nach dem SGB erforderlichen Auskünfte zu erteilen, **soweit dies gesetzlich zugelassen ist oder der Betroffene im Einzelfall eingewilligt hat**. Diese Vorschrift signalisiert, daß die Erteilung ärztlicher Auskünfte unmittelbar gegenüber der Krankenkasse im Einzelfall grundsätzlich in Betracht kommt; es besteht jedoch ein sog. **Erlaubnisvorbehalt** (Einwilligung oder Übermittlungs- bzw. Offenbarungsbefugnis). Derartige nach § 100 SGB X erforderliche datenschutzrechtliche Befugnisse (bzw. Verpflichtungen) für die ärztliche Korrespondenz mit den Krankenkassen sind im **10. Kapitel** des SGB V (datenschutzrechtliche Bestimmungen) aufgeführt. Die "Ausstellung von Bescheinigungen und Erstellung von Berichten" für Krankenkassen (§ 73 Abs. 2 Nr. 9 SGB V) findet sich im 10. Kapitel des SGB V in dieser Allgemeinheit jedoch ebensowenig wieder wie ein "spiegelbildlicher Reflex" zu § 36 Abs. 1 des Bundesmantelvertrags-Ärzte, der ebenfalls lediglich allgemein zur Information der Krankenkassen verpflichtet (**vertragliche** Vereinbarungen wie der BMVÄ **ohne** entsprechende verfassungsgemäße und normenklare **gesetzliche Ermächtigungsnorm** können keine Eingriffe in das informationelle Selbstbestimmungsrecht Dritter legitimieren!).

Soweit sich also im 10. Kapitel des SGB V keine Korrespondenzbefugnis findet, besteht eine Auskunftspflicht des Arztes gegenüber einer Krankenkasse nach § 100 SGB X nur, soweit der Betroffene im Einzelfall - grundsätzlich **schriftlich** - eingewilligt hat.

Speziell zur Feststellung, ob und wie lange der **Arbeitgeber** zur Entgeltfortzahlung verpflichtet ist, und zur Feststellung der Leistungspflicht seitens der **Krankenkasse** fragen diese Kassen des öfteren unmittelbar bei Ärzten an, ob bestimmte Krankheiten mit anderen Krankheiten im Zusammenhang stehen. Die Krankenkasse ist nicht in allen derartigen Fällen verpflichtet, eine gutachtliche Stellungnahme des MDK einzuholen, vgl. § 275 SGB V; Krankenkasse und MDK sind im Hinblick auf eine zügige Arbeitsabwicklung gar nicht daran interessiert, **alle** medizinischen Fragen im Zusammenhang mit AU durch den MDK klären zu lassen, auch benötigen die Krankenkassen zunächst Entscheidungsmaterial, **ob** der MDK einzuschalten ist. Vertragsärzte sind nach § 295 Abs. 1 Nr. 1 SGB V verpflichtet, der zuständigen Krankenkasse eine **Arbeitsunfähigkeitsbescheinigung** (einschließlich der Diagnosen) zu übermitteln. Diese **im 10. Kapitel** des SGB V (datenschutzrechtliche Bestimmungen) speziell-geregelte Übermittlungspflicht des Arztes an die Krankenkassen - **insoweit** spiegelbildlich zu § 73 Abs. 2 Nr. 9 SGB V - umfaßt m.E. auch **Auskünfte** des Arztes über die der AU-Bescheinigung zugrundeliegenden Inhalte bzw. Hintergründe wie z.B. nach dem Zusammenhang mit Vorerkrankungen, soweit diese Informationen von der Krankenkasse insbesondere für deren (eingeschränkte) Auskünfte an Arbeitgeber bzw. für deren Entscheidung über die Krankengeldzahlung erforderlich sind und die vorliegende Situation erkennbar noch keine Einschaltung des MDK erfordert.

4.5 Soziale Dienste - Parkerleichterungen

Sozialdienste sollen in ihren geparkten Kfz keine Hinweise auf den Einsatzort anbringen.

Nach dem Straßenverkehrsrecht gibt es die Möglichkeit, Handwerksbetrieben und im sozialen Dienst Tätigen Erleichterungen beim Parken auch auf Flächen zu gestatten, die für die Allgemeinheit zum Parken nicht zugelassen sind. Grundsätzlich muß die Inanspruchnahme einer solchen Parkerleichterung kontrolliert werden können, damit nicht Unberechtigte z.B. auf dem Gehsteig parken. Von den Straßenverkehrsbehörden war daher zunächst die Forderung erhoben worden, daß auch im sozialen Dienst Tätige in dem geparkten Fahrzeug hinter der Windschutzscheibe einen Hinweis anbringen müssen, **wo** die im sozialen Dienst tätige Person **gerade tätig** ist - also zum Beispiel einen Hinweis auf Hausnummer und Stockwerk.

Von seiten sozialer Dienste wurde ich um Stellungnahme hierzu gebeten, da in dem Hinweis auf die Wohnung der betreuten Person eine Bekanntgabe von Angaben über oft leicht identifizierbare Personen gesehen wurde, die grundsätzlich der Schweigepflicht unterliegen.

Ich habe dazu ausgeführt, daß die Angabe von Namen oder sonstigen personenbeziehbaren Daten der vom Sozialdienst aufgesuchten Personen auf dem Parkausweis zu unterbleiben hat, soweit im sozialen Dienst Personen tätig werden, die unter § 203 Abs. 1 StGB fallen, d.h. bei denen die unbefugte Bekanntgabe eines solchen Patientengeheimnisses strafbar wäre. Unter § 203 Abs. 1 StGB fallen nicht nur Ärzte oder Angehörige eines anderen Heilberufs (der für die Berufsausübung oder die Führung der Berufsbezeichnung eine staatlich geregelte Ausbildung erfordert), sowie staatlich anerkannte Sozialarbeiter oder staatlich anerkannte Sozialpädagogen, sondern auch deren berufsmäßige Gehilfen und die Personen, die bei ihnen zur Vorbereitung auf den Beruf tätig sind (§ 203 Abs. 3 StGB). Von der Strafdrohung wird also auch der Fall erfaßt, daß etwa ein Sozialarbeiter seine berufsmäßigen Gehilfen oder Personen, die bei ihm zur Vorbereitung auf den Beruf tätig sind, zum Einsatz zu hilfs- bzw. pflegebedürftigen Menschen schickt. Tatsächlich muß daher schon mit Rücksicht auf die genannte Schweigepflicht bei einem Großteil der Einsätze der sozialen Dienste die Nennung von Namen bzw. der genauen Ortsangabe (Wohnung, Stockwerk) wegen der damit verbundenen Bekanntgabe eines Patientengeheimnisses un-

terbleiben.

Da der Hinweis auf die Wohnung eines Pflegebedürftigen im dem geparkten Auto auch von Personen gelesen werden kann, die keine guten Absichten haben und die die teilweise bettlägerigen, hilflosen oder auch behinderten Menschen belästigen oder sonstigen Mißbrauch mit dieser Information treiben könnten, haben die betroffenen Pflegebedürftigen aber auch ein schutzwürdiges Interesse daran, daß eine solche Beeinträchtigung auch bei Einsätzen unterbleibt, bei denen die Helfer nicht unter die o.g. Strafdrohung fallen (z.B. Pflegehilfskraft, die nicht von einer unter die Strafdrohung des § 203 Abs. 1 StGB fallenden Pflegedienstleitung ausgesandt wird). Da in den meisten Fällen diese Interessen der Betroffenen das Interesse, Parkberechtigungen zu kontrollieren, überwiegen dürften, habe ich das Staatsministerium des Innern gebeten, auf die Bekanntgabe des Namens oder der genauen Wohnung in dem geparkten Kraftfahrzeug generell zu verzichten, so daß soziale Dienste stets ohne eine solche Bekanntgabe von der Ausnahmegenehmigung Gebrauch machen können. Das Staatsministerium des Innern hat sich dieser Auffassung angeschlossen und die Straßenverkehrsbehörden entsprechend unterrichtet.

4.6 Sozialhilfe

4.6.1 Umfang der Datenerhebung des Sozialamts bei Anträgen auf heilpädagogische Maßnahmen für Kinder im Vorschulalter

Zur Antragstellung auf Gewährung dieser Leistungen wurde ich gebeten zu bewerten, welche Daten die betroffenen Familien dem Sozialamt im Rahmen ihrer Mitwirkungspflicht mitzuteilen haben. Insbesondere hatte sich das Sozialamt früher mit der Kurzform eines ärztlichen Gutachtens zufriedengegeben und forderte nunmehr eine schriftliche Entbindung der behandelnden Ärzte von der Schweigepflicht sowie Angaben auf einem mehrseitigen Gutachtensvordruck.

In meiner Stellungnahme habe ich grundsätzlich angemerkt, daß es aus datenschutzrechtlicher Sicht erfreulich wäre, wenn der Umfang ärztlicher Datenerhebung gegenüber dem im konkreten Fall angegriffenen Gutachtensformular reduziert werden könnte. Wenn ein reduziertes Gutachten ausreicht, sind darüber hinausgehende Datenerhebungen nicht erforderlich und damit datenschutzrechtlich unzulässig. Meine abschließende Stellungnahme hängt nunmehr von der aus fachlicher Sicht durch das Staatsministerium für Arbeit und Sozialordnung zu entscheidenden Frage ab, welcher Umfang der Sozialdatenerhebung für Entscheidungen der Sozialhilfeträger über Anträge auf Frühförderung erforderlich ist. Die fachliche Diskussion hierzu ist noch im Gange; angestrebt wird die Erstellung eines einheitlichen ärztlichen Gutachtens, das einerseits die berechtigten Interessen der Betroffenen berücksichtigt, andererseits aber dem Sozialleistungsträger genügend fachliche Informationen für eine sachgerechte Entscheidung liefert.

Der betroffene Sozialhilfeträger hat auf mein Betreiben hin die von mir als unzulässig bewertete globale Schweigepflichtsentbindung ("hiermit entbinden wir die behandelnden Ärzte von der Schweigepflicht") abgeändert. Der Zweck einer Schweigepflichtsentbindung bestimmt deren Umfang und muß daher zur Einschränkung ihres Umfangs in der Erklärung angegeben werden. Die Mitwirkungspflichten der Betroffenen (§§ 60 ff SGB I) **rechtfertigen es nicht, den Eltern oder Sorgeberechtigten eine pauschale Einwilligung zur Einholung aller Auskünfte** bei **sämtlichen behandelnden Ärzten abzuverlangen** (vergl. § 65 Abs. 1 Nr. 1 SGB I). Die Schweigepflichtsentbindung **beschränkt sich nunmehr** auf die für die Entscheidung des Sozialhilfeamtes über die Gewährung der beantragten Eingliederungshilfe erforderlichen patientenbezogenen Angaben. Die korrekte Formulierung solcher Erklärungen ist entscheidend für die Klar-

stellung, **welche** Ärzte **in welchem Umfang** von der ärztlichen Schweigepflicht entbunden werden; sie ist auch maßgeblich für die ggf. strafrichterliche Entscheidung, ob ärztliche Äußerungen "befugt" im Sinne des § 203 Abs. 1 StGB sind oder ob eine strafrechtlich relevante Verletzung des Arztgeheimnisses vorliegt, wobei der Arzt im letzteren Fall zusätzlich standesrechtliche Konsequenzen zu befürchten hätte.

4.6.2 Datenerhebung eines Sozialamts beim Vermieter statt beim Leistungsempfänger

Zur Klärung der Frage, ob der Vermieter einer an einen Sozialhilfeempfänger vermieteten Wohnung berechtigt war, den gesamten Grundsteuerbetrag vom Mieter (Sozialhilfeempfänger) als Zusatzzahlung zu verlangen oder ob dieser Betrag nicht bereits - wie üblich - als Bestandteil der monatlich zu zahlenden Nebenkosten beglichen wurde, wandte sich ein Sozialamt **ohne vorherige Einschaltung des Betroffenen** unmittelbar an den Vermieter, der damit vom Sozialhilfebezug seines Mieters erfuhr.

Auch ohne nähere Ausführungen in der Anfrage erhält ein Vermieter schon angesichts der datenerhebenden Stelle Kenntnis vom Kontakt seines Mieters mit dem Sozialamt. Sozialämter sind daher verpflichtet, alle Fragen im Zusammenhang mit einer Leistungsgewährung **zunächst mit oder über den Antragsteller zu klären.** Im angesprochenen Fall hätte die offene Frage möglicherweise bereits durch Vorlage des Mietvertrags oder einer Nebenkosten-Abrechnung ohne Einschaltung des Vermieters geklärt werden können; wenn nicht, hätte das Sozialamt dem Antragsteller/Leistungsbezieher aufgeben können, selbst eine Bestätigung des Vermieters über diese Nebenkostenfrage beizubringen und damit die Offenlegung des Sozialhilfebezugs zu vermeiden.

4.6.3 Anforderung von Kontoauszügen durch ein Sozialamt

Eine zu 100 % geistig und körperlich behinderte Sozialhilfeempfängerin hatte eine Erbschaft erhalten. Zur Überprüfung, ob der Behinderten nach Anfall und Verbrauch der Erbschaft wiederum Sozialhilfe zu gewähren sei, forderte das Sozialamt die Zusendung sämtlicher Kontoauszüge des privaten Girokontos **der Mutter** ab Zufluß der Erbschaft.

Auf meine Anfrage räumte das Sozialamt ein, daß die uneingeschränkte Aufforderung zur Vorlage der lückenlosen Kontoauszüge des privaten Girokontos der Mutter ab Zufluß der Erbschaft nicht korrekt war, da das Sozialamt zur Entscheidung über die Sozialhilfe-Wiedergewährung an das behinderte Kind ausschließlich Kenntnisse über die Verwendung der Erbschaft benötigte und dementsprechend die Datenerhebung über Einkommens- und Vermögensverhältnisse der Mutter nicht erforderlich und daher unzulässig war.

Ergänzend habe ich dem Sozialamt mitgeteilt, die Mutter hätte entweder unmittelbar nach ihrer Mitteilung über den Zufluß der Erbschaft auf die Möglichkeit hingewiesen werden müssen, für den Verwendungsnachweis der Erbschaft ein gesondertes Girokonto zu eröffnen oder das Sozialamt hätte ihr zugestehen müssen, mit der Verwendung der Erbschaft in keinem Zusammenhang stehende Buchungen auf den Kontoauszügen ihres Privatkontos zu schwärzen.

4.6.4 Verwendung einer Quittungsliste für Barauszahlungen von Sozialhilfe

Eine Gemeinde ließ die jeweiligen Zahlungsempfänger den Empfang der Barauszahlung von Sozialhilfeleistungen des Landkreises auf einer Liste quittieren; Zahlungsempfänger konnten darauf auch die Namen der Personen lesen, die vor ihnen unterschrieben hatten. Wie eine Rückfrage ergab, war an sich vorgesehen, bei Unterschrift eines weiteren Zahlungsempfängers die jeweils vorherigen Unterschriften abzudecken; die Gemeinde gab an, daß dieses Verfahren "wohl im Einzelfall nicht funktioniert" habe.

Ich habe dazu festgestellt, daß ein derartiges Verfahren wegen des erheblichen Risikos der Datenoffenbarung an nichtberechtigte Dritte datenschutzrechtlichen Anforderungen nicht entspricht. Die betroffene Stadt verwendet seither derartige Quittungslisten nicht mehr und läßt stattdessen von den Zahlungsempfängern **Einzelquittungen** unterschreiben.

4.6.5 Vermerk "Sozialleistung der Stadt XY" auf Überweisungsträgern - Vermerk "Leistung nach BSHG" auf "Sozialhilfe-Scheck"

In einem mit mir abgestimmten Schreiben vom 23.11.1994 insbesondere an die Regierungen, Landkreise und kreisfreien Städte sowie die Bezirke (Az: IV - 2/0346/2/94) hat das Bayer. StMAS unter Bezug auf das Urteil des Bundesverwaltungsgerichts vom 23.06.1994 (BVerwG 5 C 16.92) darauf hingewiesen, daß der Vermerk "Sozialleistungen" auf Überweisungsträgern eine nach dem SGB **unzulässige, da nicht erforderliche Datenübermittlung an Dritte** (Bedienstete des eingeschalteten Kreditinstituts) und somit einen Bruch des Sozialgeheimnisses darstellt. Anstelle dieses Vermerks genügt zur Individualisierung der erbrachten Leistung gegenüber dem Empfänger regelmäßig auch eine **neutrale**, d.h. für Dritte "nicht sprechende" Kennzeichnung des Verwendungszwecks der Zahlung.

Wie ich feststellen mußte, halten sich noch nicht alle Sozialhilfeträger an diese Vorgaben; gleichermaßen **unzulässig** sind auch **Hinweise auf Herkunft bzw. Verwendungszweck** auf sog. Sozialhilfe-Schecks. Ich betone hier nochmals, daß durch die (nicht erforderliche) Kennzeichnung "Sozialleistungen" - denen im übrigen möglicherweise eine nur kurzfristige Sozialhilfebedürftigkeit zugrundeliegt - die Mitarbeiter des Kreditinstituts unnötig Kenntnis über wirtschaftliche Verhältnisse des Überweisungs- bzw. Scheck-Empfängers erhalten, die **dessen Kreditwürdigkeit massiv beeinträchtigen.** Ich habe diesen Datenschutzverstoß gemäß Art. 31 BayDSG formell beanstandet.

Ich teile die Formulierungsvorschläge in dem o.g. Schreiben des Bayer. StMAS, auf Überweisungsträgern bzw. Schecks der Sozialhilfeträger als Herkunft bzw. Verwendungszweck anzugeben: "Zahlung gemäß Antrag vom ...", "Zahlung gemäß Bescheid vom ..." oder "Zahlung gemäß Az.: ...". Ebenso sind bei im Einzelfall erforderlichen Zahlungen an Dritte (wie z.B. Vermieter, Stadtwerke, Krankenkassen usw.) nur die für die Zahlungsempfänger notwendigen Angaben auf den Überweisungsträgern bzw. Schecks anzubringen (z.B. Name und Vorname des Hilfeempfängers, besser: Mieter-Nr., Abnehmer-Nr., Versicherungs-Nr. etc.); Angaben, die auf Sozialhilfeleistungen schließen lassen, sind zu unterlassen.

4.7 Jugendamt

4.7.1 Datenerhebung durch das Jugendamt zur Feststellung des Unterhalts

Ein Petent bat um Überprüfung eines Datenerhebungsformulars zur Feststellung seiner Leistungsfähigkeit zum Kindesunterhalt. Die Prüfung dieses Erhebungsbogens führte in mehrfacher Hinsicht zu datenschutzgerechten Verbesserungen durch das Jugendamt:

Der Erhebungsbogen forderte u.a. Auskünfte darüber, ob der Ehegatte des Unterhaltsverpflichteten in Arbeit stehe, ggf. mit welchem Nettoverdienst und in welcher Höhe dieser Ehegatte sonstiges Einkommen beziehe. Hierzu habe ich deutlich gemacht, daß den Ehegatten des Unterhaltspflichtigen gegenüber dem nichtehelichen Kind keine Unterhaltspflicht trifft, weshalb **keine Verpflichtung** zu den genannten Angaben besteht. Vielmehr handelt es sich hier nicht um eine Rechtspflicht, sondern um Angaben, die der Unterhaltspflichtige zu seiner **Entlastung machen kann**, da bei der ihm zumutbaren Belastung aus dem Unterhalt für das nichteheliche Kind seine Unterhaltspflicht gegenüber dem Ehegatten berücksichtigt werden muß, **je nach dessen eigenem Verdienst.** Derartige Angaben sind daher zur Aufgabenerfüllung des Jugendamtes **nur dann** erforderlich, wenn der andere Ehegatte vom Unterhaltspflichtigen unterhalten werden muß, worauf hinzuweisen ist. Das betroffene Jugendamt ergänzte daraufhin seine diesbezüglichen Fragen um folgenden Hinweis: "Angaben zu Nummer ... sind nur erforderlich, falls sich Ihre Ehefrau nicht aus eigenem Einkommen unterhalten kann. Machen Sie über das Einkommen Ihrer Ehefrau keine Angaben, gehen wir davon aus, daß sie sich selbst unterhalten kann und daß sie zu den häuslichen Ausgaben anteilmäßig beiträgt."

Verbunden mit der Frage nach dem Nettoverdienst des Unterhaltsverpflichteten erfolgte die Aufforderung, den **Arbeitgeber** zu benennen und eine Verdienstbescheinigung vorzulegen. Gleichzeitig wurde am Ende des Formulars **die Einwilligung in eine Nachfrage beim Arbeitgeber** verlangt. Wie mir aus mehreren Eingaben bekannt ist, empfinden Betroffene immer wieder die Bekanntgabe der Tatsache, daß sie Vater eines nichtehelichen Kindes sind, gegenüber ihrem Arbeitgeber als besonders kritisch und befürchten nicht vorhersehbare Risiken - auch für ihren Arbeitsplatz. Ich habe das Jugendamt daher darauf hingewiesen, daß nach dem allgemeingültigen datenschutzrechtlichen Grundsatz, wonach Daten primär beim Betroffenen selbst zu erheben

sind, das Einholen einer Verdienstbescheinigung **beim Arbeitgeber** erst dann in Frage kommen kann, wenn der Vater eine solche Bescheinigung auf Aufforderung nicht selbst vorlegt und er anschließend darauf hingewiesen wurde, daß das Jugendamt deshalb an den Arbeitgeber herantreten werde. **Auch bei erteilter Einwilligung** ist dem Unterhaltsverpflichteten vorrangig die Möglichkeit einzuräumen, beim Arbeitgeber eine neutrale Bescheinigung über seinen Verdienst zu verlangen, so daß er diesem die Tatsache und Art seiner Beziehung zum Jugendamt nicht zu offenbaren braucht. Das Jugendamt weist nun im Erhebungsbogen ausdrücklich darauf hin, daß eine Anfrage beim Arbeitgeber nur dann erfolgt, wenn der Unterhaltspflichtige die angeforderte Einkommensbescheinigung nicht selbst vorlegt.

4.7.2 Datenschutz bei Amtspflegschaft und Amtsvormundschaft gemäß § 68 SGB VIII

Bei einem Landratsamt bestanden Unsicherheiten, wie im Bereich Amtspflegschaft und Amtsvormundschaft nach § 68 SGB VIII die Aktenvorlage an den Landrat und die zuständige Abteilungsleitung zu beurteilen bzw. zu handhaben ist.

Ausgangspunkt der Klärung dieser Frage ist, daß für den Schutz von Sozialdaten bei ihrer Erhebung, Verarbeitung und Nutzung im Rahmen der Tätigkeit des Jugendamts als Amtspfleger und Amtsvormund nur § 68 SGB VIII gilt. Diese datenschutzrechtliche Sonderstellung ist das Resultat der Besonderheiten dieses Personenkreises nach den §§ 55 und 56 SGB VIII, wonach zwar **das Jugendamt** in den durch das BGB vorgesehenen Fällen der Amtspflegschaft und Amtsvormundschaft Pfleger oder Vormund wird, die **Ausübung der Aufgaben** des Pflegers oder des Vormunds jedoch **einzelnen seiner Beamten oder Angestellten überträgt**. Dementsprechend regelt § 68 Abs. 1 Satz 1 SGB VIII die Zulässigkeit der Sozialdatenerhebung und -verwendung **durch den** hierfür zuständigen **Beamten oder Angestellten**.

Im 2. SGB-Änderungsgesetz vom 13.06.1994 (BGBl I S. 1229) wurde - zur Behebung offenbar in vielen Jugendämtern aufgetretener Differenzen - in § 68 Abs. 1 Satz 2 SGB VIII geregelt, daß die Nutzung der vom Amtsvormund bzw. Amtspfleger erhobenen und verwendeten Sozialdaten **zum Zweck der Aufsicht, Kontrolle oder Rechnungsprüfung** durch die dafür zuständigen Stellen sowie die Übermittlung an diese **"im Hinblick auf den Einzelfall"** zulässig ist. Aus dieser Formulierung ergibt sich, daß eine **regelmäßige Vorlage** von Akten des Amtspflegers/-

vormunds an den Landrat und die zuständige Abteilungsleitung **nicht erlaubt** ist und die Aktenvorlage damit einer restriktiveren Regelung unterliegt als in anderen Tätigkeitsbereichen des Jugendamts und im (übrigen) Anwendungsbereich des SGB X, z.B. im Sozialamt oder in der Wohngeldstelle.

Als "Einzelfall" im Sinne des § 68 Abs. 1 Satz 2 SGB VIII kommen sowohl einzelne konkrete Amtspflegschaften bzw. -vormundschaften als auch z.B. einzelne **Anlässe, die in der Person oder im Verhalten des handelnden Amtspflegers bzw. -vormunds liegen,** zur Wahrnehmung der **Aufsichts- und Kontrollpflicht** durch Abteilungsleiter und Landrat in Betracht. Vereinzelte gelegentliche Stichproben hinsichtlich der Aufgabenerfüllung des Amtspflegers/-vormunds erscheinen gerechtfertigt, allerdings darf dadurch die diesen Personen gesetzlich eingeräumte Sonderstellung nicht ausgehöhlt werden. Selbstverständlich sind Datenübermittlungen und -nutzungen auch im Bereich des § 68 SGB VIII **nur in dem für die Aufsicht, Kontrolle und Rechnungsprüfung erforderlichen Umfang** zulässig. Diese Ausführungen gelten für die Tätigkeit des Jugendamts als Beistand oder Gegenvormund entsprechend (vgl. § 68 Abs. 5 SGB VIII).

Im Tätigkeitsbereich nach § 68 SGB VIII bestehen also Einschränkungen des Informations**rechts** des Landrats sowie der Abteilungsleitung des Jugendamts bei der Aufsicht, Kontrolle oder Rechnungsprüfung, die **vom Gesetzgeber so gewollt** sind, sonst hätte er nicht die Formulierung "im Hinblick auf den Einzelfall" gewählt.

4.7.3 Behandlung des Posteinlaufs für das Jugendamt

Die in der vorangehenden Ziffer dargelegten datenschutzrechtlichen Erwägungen spielen auch bei der Behandlung des Posteinlaufs für das Jugendamt eine Rolle, nach deren Ausgestaltung ich im Berichtszeitraum ebenfalls gefragt wurde. Auf die ähnlich liegende Problematik bei der Behandlung des Posteinlaufs des Gesundheitsamts weise ich hin (s. Nr. 3.5.1 in diesem Bericht).

Während grundsätzlich keine datenschutzrechtlichen Bedenken dagegen bestehen, daß Mitarbeiter der Posteinlaufstelle auch Sozialdaten enthaltende Sendungen öffnen, die z.B. an die Wohngeldstelle oder an das Sozialamt gerichtet sind, ist die dortige Öffnung von an das Jugendamt gerichteten Postsendungen nicht unproblematisch und im einzelnen datenschutzrechtlich wohl auch umstritten. Über die Öffnungsbefugnis von Mitarbeitern der Posteingangsstelle hinaus ist dabei die **Frage der Weiterleitung** von an das Jugendamt gerichteten Postsendungen zu beurteilen, d.h. welche leitenden Mitarbeiter sind befugt, Post für das Jugendamt etwa in der Posteinlaufmappe auf dem Dienstweg einzusehen.

Bei Sendungen an das Jugendamt ist zunächst zu differenzieren, ob die Post an das Jugendamt (a) oder erkennbar an einen dort tätigen Amtspfleger/-vormund adressiert ist (b).

a. Sendungen "An das Jugendamt ...." im Anwendungsbereich nach § 61 **Abs. 1** SGB VIII, die äußerlich keine Besonderheiten erkennen lassen, dürfen m.E. durch die Mitarbeiter der Posteingangsstelle geöffnet werden und sind dort mit dem Eingangsstempel zu versehen. Auch die Post- und Aktenvorlage an den Landrat und die zuständige Abteilungsleitung ist nach den §§ 61 Abs. 1, 64 Abs. 1 SGB VIII und § 67 c SGB X als Sozialdatennutzung im Rahmen der Erforderlichkeit zur Wahrnehmung von Aufsichts-, Kontroll- und Disziplinarbefugnissen zulässig.

Allerdings können sich auch in der allgemein "An das Jugendamt ...." adressierten Post Sendungen befinden, durch deren Inhalt einem Mitarbeiter des Jugendamts Sozialdaten **zum Zweck persönlicher und erzieherischer Hilfe anvertraut** werden, die nach **§ 65 SGB VIII** sogar innerhalb des Jugendamts - erst recht innerhalb der Gebietskörperschaft - einem **besonderen Vertrauensschutz** unterliegen. Da Sozialdaten im Sinne des § 65

SGB VIII **dem einzelnen Mitarbeiter** und nicht dem Jugendamt als solchem anvertraut werden (wie aus dem Gesetzeswortlaut und der Terminologie "weitergeben" abzuleiten ist), ist ein Postlauf über den Landrat bzw. den zuständigen Abteilungsleiter nicht zulässig. Erweist sich also ein nicht bereits außen auf dem Kuvert als "persönlich" oder "vertraulich" gekennzeichnetes Schreiben nach Öffnen in der Poststelle als solche vertrauliche Mitteilung, muß es dem zuständigen Mitarbeiter **unmittelbar zugeleitet** werden. Ist eine derartige Sendung an einen Mitarbeiter des Jugendamts "persönlich" adressiert oder ergibt sich bereits äußerlich erkennbar ein Hinweis auf den vertraulichen Inhalt, ist diese dem Adressaten **ungeöffnet** auszuhändigen; eine Rückgabe an die Eingangsstelle (vgl. § 9 Abs. 1 Satz 3 2. Halbsatz ADO) ist trotz des dienstlichen Inhalts aufgrund § 65 SGB VIII unzulässig.

b. Amtspfleger und Amtsvormund haben gemäß § 61 **Abs. 2** i.V.m. § 68 SGB VIII die oben beschriebene "datenschutzrechtliche Sonderstellung" (vgl. Ziffer 4.7.2); dieser Umstand wirkt sich auch auf die Zuleitung von Sendungen aus, die "An den Amtspfleger/-vormund im Jugendamt ...." adressiert sind. Ob die Mitarbeiter der Posteingangsstelle zum Öffnen derartiger Sendungen berechtigt sind, sollte zwischen der Behördenleitung und dem Amtspfleger/-vormund vereinbart werden. Bei vereinbarter Öffnungsbefugnis ist der Eingangsstempel in der Posteingangsstelle, andernfalls durch den Amtspfleger/-vormund anzubringen.

Solche Post ist in jedem Falle durch die Posteingangsstelle **unmittelbar** dem Amtspfleger/vormund zuzuleiten; sie darf dem Landrat/Bürgermeister bzw. der zuständigen Abteilungsleitung nicht im Wege des regulären Posteinlaufs zur Kenntnis gegeben werden, weil eine Datenverwendung durch die Vorgesetzten des Adressaten **zum Zweck der Aufsicht bzw. Kontrolle** gemäß § 68 Abs. 1 Satz 2 SGB VIII lediglich **für Einzelfälle zulässig** ist (vgl. Ziff. 4.7.2).

Die Ausführungen unter b) gelten auch für die Tätigkeit des Jugendamts als Beistand oder Gegenvormund.

4.8 Kindergärten

4.8.1 Datenübermittlung zwischen Kindergärten zur Bedarfsplanung/Feststellung von Mehrfachanmeldungen

> **Benachbarte, im Wettbewerb zueinander stehende Kindergärten dürfen personenbezogene Daten angemeldeter oder abgelehnter Kindergartenkinder übermitteln und nutzen, soweit dies erforderlich ist, damit die Kindergärten ihre Aufgaben der Bedarfsplanung, Kapazitätsberechnung, der Erkennung von Mehrfachanmeldungen und Vermeidung von Doppelbelegungen erfüllen können, und soweit hierzu kein weniger einschneidender Weg zur Verfügung steht (Verhältnismäßigkeitsgrundsatz); insoweit erfolgen diese Datenübermittlungen und -nutzungen zur Wahrung berechtigter Interessen der Kindergärten sowie der Eltern.**

Nach meiner Auffassung besteht kein Grund zur Annahme, daß die betroffenen Eltern ein schutzwürdiges Interesse am Ausschluß der Datenübermittlung haben, **wenn** die Zuordnung zu einem Kindergarten trotz des Abgleichs **unter Berücksichtigung der Argumente der Eltern** vorgenommen wird. Der aus der Sicht der Kindergärten günstigste - weil wohnortnächste - Kindergarten braucht nicht auch derjenige zu sein, den die **Eltern** für den günstigsten halten (z.B. weil dieser auf dem Weg zur Arbeitsstätte der Mutter/des Vaters liegt).

Um dem gesetzlichen Gebot der Datenerhebung nach Treu und Glauben Rechnung zu tragen (§ 28 Abs. 1 Satz 2 BDSG, Art. 3 Abs. 1 BayDSG), sollten die Eltern **bereits bei der Kindergarten-Anmeldung** und möglichst **im Anmeldeformular** darauf hingewiesen werden, daß ein Abgleich mit Anmeldungen bei benachbarten Kindergärten vorgesehen ist. Im Hinblick auf notwendige Konsequenzen aus dem Abgleich könnten die Eltern gebeten werden, eine evtl. Reihenfolge der von Ihnen bevorzugten Kindergärten zu benennen.

4.8.2 Keine Mitteilung von Namen und Anschriften der Mitglieder von Kindergartenbeiräten an die Aufsichtsbehörde

Nach der bisherigen Fassung des § 9 Abs. 3 der Verordnung über die Bildung und den Geschäftsgang der Kindergartenbeiräte bei den anerkannten Kindergärten (2.DVBayKiG) hat der Träger des Kindergartens nach der ersten Sitzung des neugewählten Kindergartenbeirats der zuständigen Aufsichtsbehörde die Namen und Anschriften der Mitglieder des Kindergartenbeirats schriftlich mitzuteilen. Es wurden Zweifel an mich herangetragen, ob die Mitteilung dieser Daten an die Aufsichtsbehörde zur Aufgabenerfüllung des Kindergartens oder der Aufsichtsbehörde tatsächlich erforderlich ist.

Auf meine entsprechende kritische Rückfrage teilte das Bayer. StMAS in einem Rundschreiben an die Regierungen vom 08.05.1996 mit, daß § 9 Abs. 3 der 2.DVBayKiG im Vorgriff auf eine vorgesehene Aufhebung der Vorschrift mit Wirkung ab dem Kindergartenjahr 1996/97 nicht mehr anzuwenden sei, da diese Meldung für die Aufgabenerfüllung der Aufsichtsbehörden nicht erforderlich sei.

4.9 Datenerhebung in Asylbewerber-Erstaufnahmeeinrichtungen

Ein Pressebericht, der sich auf die Erstaufnahmeeinrichtung Landsberg (Lech) bezog, war für mich Anlaß, dem Umgang mit Daten von Bewohnern und Besuchern in den bayerischen Erstaufnahmeeinrichtungen im Sinn von § 44 Abs. 1 Asylverfahrensgesetz im einzelnen nachzugehen.

In den bayerischen Erstaufnahmeeinrichtungen besteht durchweg die Übung, bei Bewohnern der Einrichtung beim Betreten der Unterkunft die Ausweise zu kontrollieren. Im Hinblick auf Besucher wird eine Besucherliste geführt. Gegen beide Vorgehensweisen habe ich keine Einwendungen. In der Ausweiskontrolle von Bewohnern liegt eine Datenerhebung, die mit Kenntnis der Betroffenen erfolgt. Sie ist erforderlich im Sinne von Art. 16 Abs. 1 BayDSG, um Unbefugte am Betreten der Erstaufnahmeeinrichtung zu hindern und dient auf diese Weise nicht zuletzt auch dem Schutz der Bewohner selbst. Das Erheben und Speichern der Daten von Besuchern wiederum ist - soweit es sich auf den erforderlichen Umfang beschränkt - zur Erfüllung der Aufgaben der Erstaufnahmeeinrichtung erforderlich. Auch sie dient nicht zuletzt dem Schutz der Bewohner.

Darüber hinaus hatte ich folgende Sachverhaltskomplexe in der Erstaufnahmeeinrichtung Landsberg (Lech) datenschutzrechtlich zu bewerten:

- Notierungen wegen des Verdachts unzulässiger Arbeitsaufnahme durch Bewohner der Einrichtung

  Einige Tage wurden die Personen notiert, die in den frühen Morgenstunden die Einrichtung verließen. Grund hierfür war der Verdacht aufgrund von Hinweisen des Sozialamts, daß Bewohner einer nicht angemeldeten Erwerbstätigkeit nachgingen. An Dritte wurden die Daten nicht weitergegeben. Die Unterlagen wurden etwa eine Woche lang aufbewahrt. Die Heimleitung wollte mit dieser Maßnahme feststellen, wer mehrfach zu dieser Zeit das Gelände verließ, um die Betreffenden dann darauf hinweisen zu können, daß eine Arbeitsaufnahme ordnungsgemäß angezeigt werden muß.

  Nach den konkreten Umständen des Einzelfalls war die Erhebung der Daten noch von den Aufgaben der Unterkunftsleitung gedeckt und daher als erforderlich im Sinne von

Art. 16 Abs. 1 BayDSG anzusehen. Es ist nicht zu beanstanden, wenn die Leitung einer solchen Einrichtung eine ihrer Aufgaben darin sieht, die Bewohner vor der offensichtlichen Gefahr einer Strafbarkeit zu bewahren. Dies gilt jedenfalls dann, wenn sich diese Gefahr den Umständen nach aufdrängt und durch Maßnahmen verhältnismäßig geringer Intensität, etwa durch Notizen, mit denen der Betroffene alsbald konfrontiert wird, abgewehrt werden kann. Gegen eine allgemeine Praxis, bei Verdacht auf unangemeldete Arbeitsaufnahmen **heimlich** derartige Aufschreibungen durchzuführen, hätte ich jedoch erhebliche Bedenken.

- Ermittlungen durch den Leiter einer seitens der Regierung von Oberbayern beauftragten Bewachungsfirma außerhalb des Geländes der Einrichtung

  Nach einem Zeitungsbericht hat der Leiter der Bewachungsfirma einen Bewohner außerhalb der Einrichtung verdeckt beobachtet, um festzustellen, ob dieser Bewohner schwarzarbeitet. Diese Maßnahme, die ihrer Rechtsnatur nach eine verdeckte Observierung darstellt, ist als erheblicher Eingriff in die Rechte der Betroffenen anzusehen. Da die Voraussetzungen des Art. 16 Abs. 2 BayDSG offensichtlich nicht erfüllt waren, wäre es der Regierung von Oberbayern verwehrt gewesen, solche Maßnahmen anzuordnen oder in ihrem Verantwortungsbereich zu dulden.

  Da die Regierung von Oberbayern glaubhaft versichert hat, sie habe die Maßnahmen weder veranlaßt noch seien sie mit ihr abgesprochen worden, liegt seitens der Regierung kein Verstoß gegen datenschutzrechtliche Vorschriften vor. Da diese Maßnahme völlig außerhalb des Aufgabenbereichs des Wachdienstes lag, muß sich die Regierung dessen Aufgabenüberschreitung auch nicht zurechnen lassen. Die Regierung ist allerdings gehalten sicherzustellen, daß derartige Aufgabenüberschreitungen in Zukunft unterbleiben.

- Notierungen in unmittelbarem innerem Zusammenhang mit aktuellen polizeilichen Ermittlungen

  In einer nicht mehr genau feststellbaren Zahl von Fällen hatte die Polizeiinspektion Landsberg (Lech) dem Bewachungsdienst an der Pforte der Einrichtung mitgeteilt, daß es zu Straftaten gekommen sei, bei denen der Täter ein Bewohner der Einrichtung sein

könnte. Dabei beschrieb die Polizei jeweils den Täter, soweit dies nach den Umständen möglich war. Der Wachdienst achtete dann darauf, ob Personen den Eingang passierten, auf welche die Beschreibung paßte.

Jeder Bürger hat das Recht, der Polizei Beobachtungen zu melden, die für die Aufklärung von Straftaten bedeutsam sein können. Er darf auch ohne weiteres einer Bitte der Polizei entsprechen, aus aktuellem Anlaß besonders aufmerksam zu sein und mögliche Beobachtungen zu melden. Schon angesichts der generellen Verpflichtung zur Amtshilfe zwischen Behörden kann für Behörden vom Grundsatz her nichts anderes gelten. Ich habe daher keine Bedenken dagegen, daß auch Mitarbeiter einer behördlich beauftragten Wachfirma auf Bitten der Polizei aus aktuellem Anlaß "die Augen offenhalten" und der Polizei verdächtige Wahrnehmungen mitteilen.

- **Präventive** Notierungen des Betretens und Verlassens der Einrichtung **ohne unmittelbaren** inneren Zusammenhang mit aktuellen polizeilichen Ermittlungen

  Insoweit bin ich zu dem Ergebnis gekommen, daß zwar starke Indizien dafür sprechen, daß es solche präventiven Aufzeichnungen ohne unmittelbaren inneren Zusammenhang mit aktuellen polizeilichen Ermittlungen gegeben hat. Mit letzter Sicherheit ließ sich ein entsprechender Nachweis jedoch nach Lage der Dinge nicht führen.

  Ungeachtet dieser Ausgangslage erscheint mir insoweit der allgemeine Hinweis geboten, daß **präventive** Speicherungen des Betretens und Verlassens der Einrichtung durch die Aufgaben einer Erstaufnahmeeinrichtung nicht mehr gedeckt wären. Das allgemeine präventive Tätigwerden zur Verhinderung von Straftaten gehört nicht zu den Aufgaben einer Erstaufnahmeeinrichtung.

- Behandlung von Post, die an einen Bewohner der Einrichtung gerichtet war

  Obgleich trotz intensiver Bemühungen zur Klärung des Sachverhalts eine Reihe von Einzelheiten strittig blieb, steht folgender Sachverhalt unstreitig fest: Ein Mitarbeiter des von der Regierung von Oberbayern beauftragten Wachdienstes hat einem Auftrag der Heim-

leitung entsprechend einem Bewohner der Erstaufnahmeeinrichtung einen Brief verschlossen ausgehändigt, der an diesen Bewohner gerichtet war. Der Mitarbeiter des Wachdienstes fragte den Betroffenen, was in dem Brief stehe. Daraufhin übergab der Betroffene dem Wachmann den geöffneten Brief. Nach Lage der Dinge ist davon auszugehen, daß diese Herausgabe nicht aufgrund eines freien Entschlusses erfolgte. Die Übergabe des geöffneten Briefes geschah aufgrund einer ausdrücklichen Aufforderung des Wachmannes, der sich auf Veranlassung der Unterkunftsleitung über den Inhalt des Briefes informieren wollte.

In der Entgegennahme des Schreibens und in der Kenntnisnahme seines Inhalts liegt eine Datenerhebung, die einer Rechtsgrundlage bedürfte. Eine solche Rechtsgrundlage liegt nicht vor. Insbesondere kann nicht davon ausgegangen werden, daß die allgemein gefaßte Vorschrift des Art. 16 Abs. 1 BayDSG ein irgendwie geartetes Einwirken der Erstaufnahmeeinrichtung auf den Asylbewerber wegen des Verdachts der unangemeldeten Arbeitsaufnahme rechtfertigen würde, einen an ihn gerichteten Brief zu übergeben, vorzulesen oder seinen Inhalt bekanntzugeben. Ein solches Vorgehen stellt eine Verletzung des Briefgeheimnisses dar, für die keine Rechtsgrundlage bestand. Ich habe diesen Vorgang deshalb gemäß Art. 31 Abs. 1 BayDSG beanstandet.

4.10 Rentenversicherung

Gegenseitige Beauftragung der Träger der gesetzlichen Rentenversicherung mit der Versichertenbetreuung

Gesetzlich Rentenversicherte können sich künftig auch bei einer anderen als der zuständigen Landesversicherungsanstalt Beratung holen - welche datenschutzrechtlichen Fragen ergeben sich?

Die Träger der gesetzlichen Arbeiter-Rentenversicherung haben sich zur Verstärkung ihrer Zusammenarbeit bei der Versichertenbetreuung gegenseitig mit der Anforderung, Erstellung, Aushändigung und Erläuterung von Versicherungsverläufen, Renten- und Lückenauskünften sowie Auskünften über Beitragserstattungen und mit der dafür erforderlichen Verarbeitung und Nutzung von Sozialdaten beauftragt. Der einzelne Versicherte kann damit die von ihm gewünschten Informationen über sein Versicherungsverhältnis und über bisher erworbene Anwartschaftsrechte auch bei einem anderen Rentenversicherungsträger als dem nach den einschlägigen Organisations- und Kompetenzvorschriften für ihn zuständigen RV-Träger erhalten. Das ist wohl zweckmäßig, weil in einer Vielzahl von Fällen in der Arbeiter-Rentenversicherung nicht die für den Wohnsitz des Versicherten zuständige LVA auch dessen Versicherungskonto führt.

Wegen der umfassenden Zugriffsmöglichkeit auf wesentliche Renteneckdaten aller Versicherten der angeschlossenen RVTräger gilt es, ein Höchstmaß an technischen und organisatorischen Sicherungsmaßnahmen im Sinne von § 78 a SGB X vorzusehen.

Notwendig sind die

- Begrenzung der Anzahl der zur Dialognutzung zugelassenen Mitarbeiter auf der erforderliche Maß,

- technische Beschränkung der Zugriffsmöglichkeiten der zugelassenen Mitarbeiter auf das für ihre Aufgabenerfüllung erforderliche Maß,

- Unterweisung und datenschutzrechtliche Sensibilisierung der zugelassenen Mitarbeiter,

- Identitätsprüfung des Antragstellers anhand eines Lichtbildausweises,

- Schriftlichkeit des Antrags (formularmäßig),

- sichere Identifizierung und Authentisierung,

- Protokollierung der EDV-Zugriffe sowohl beim zuständigen als auch beim anfordernden RV-Träger und stichprobenmäßige Kontrolle, daß für protokollierte Zugriffe ein Antrag vorliegt sowie auf Gleichlauf der beiden Protokolle.

Sofern die Sozialdaten im Dialogverfahren nicht mehr über ein herkömmliches rentenversicherungsinternes Standleitungsnetz aus festgeschalteten Verbindungen übermittelt werden sollen, ist wegen der sonst bestehenden Möglichkeit der unbefugten Kenntnisnahme und einer ohne Abgleich nicht erkennbaren Verfälschung außerdem eine Verschlüsselung erforderlich.

Es bleibt einer Prüfung bei LVAen vorbehalten festzustellen, ob sich die Beratungen noch im Rahmen einer "Datenverarbeitung im Auftrag" i.S. des § 80 SGB X halten oder ob die Beratung eine darüber hinausgehende eigene intellektuelle Leistung von Mitarbeitern der (unzuständigen) LVAen ist, die auf § 80 SGB X nicht gestützt werden kann.

5. Polizei

5.1 Schwerpunkte

Schwerpunkte meiner Tätigkeit im Polizeibereich waren

- **allgemeine Kontrollen** von Dateien und Karteien, insbesondere von Dateien zur Gefahrenabwehr und Strafverfolgung (sog. GAST-Dateien), der Datei "Polizeiliche Sachbearbeitung/Vorgangsverwaltung-Verbrechensbekämpfung (PSV)", der Anhaltedatei (AFB-Anhaltedatei), der Datei "Kfz-Fahndung-Anhaltemitteilung (AHM)", der Lichtbildvorzeigekartei" sowie verschiedener Lagedateien (z.B. Rauschgiftlage) und des "Kriminalaktennachweises (KAN)"

- Prüfung neuer bzw. überarbeiteter **Errichtungsanordnungen** für polizeiliche Dateien (Staatsschutzdatei Bayern, Personen- und Fall-Auskunftdatei - PFAD, Arbeitsdatei "Geldwäsche", Spudok-Datei "Gewaltbereite Personen aus den Bereichen Rechts- und Linksextremismus, politisch motivierte Skinheads und Ausländergruppen - OFR-GEPE-S", GAST-Dateien "Lagebild Fabrikschloß" und "SEKTEN")

- Prüfung von **Dateimeldungen** (z.B. Prostitutionsdatei)

- Mitwirkung im **Arbeitskreis Sicherheit**

- **Bürgereingaben**

5.2 Allgemeine Prüfungen

Allgemeine Querschnittsprüfungen habe ich bei folgenden Polizeibehörden vorgenommen:

- Bayerisches Landeskriminalamt
- Polizeipräsidium München
- Polizeipräsidium Oberfranken mit der Polizeidirektion Hof
- Polizeipräsidium Schwaben mit der Polizeidirektion Augsburg

Die Prüfungen lassen erkennen, daß die datenschutzrechtlichen Vorschriften von der Polizei grundsätzlich **beachtet** werden und Mängel sowie Verstöße gegen den Datenschutz nach wie vor die **Ausnahme** bilden. Dies ist auch deshalb hervorzuheben, weil die technische Ausstattung bei den Polizeidienststellen vorangeschritten ist und die zu verarbeitende Datenmenge nach Angaben der Polizei hohe Zuwächse verzeichnet. Auch diesmal konnte ich eine große Bereitschaft der Polizei feststellen, mich bei meinen Prüfungen aktiv zu unterstützen.

5.2.1 Kriminalaktennachweis (KAN)

Bei meinen Prüfungen habe ich festgestellt, daß die Auflösung des Regional-KAN (vgl. 15. Tätigkeitsbericht, Nr. 4.1.4 und 16. Tätigkeitsbericht, Nr. 5.2.1) zwischenzeitlich **abgeschlossen** ist. Die von mir geprüften Dienststellen hatten die Regional-KAN-Bestände aufgelöst und die entsprechenden Nachweise in der Datei gelöscht. Besonders habe ich darauf geachtet, daß frühere Regional-KAN-Bestände nur dann in den Landes-KAN überführt wurden, wenn die Voraussetzungen für eine landesweite Speicherung vorlagen. Gravierende Fehler waren im Zusammenhang mit der Neuordnung des KAN-Konzeptes nicht festzustellen:

Die Prüfung des Landes-KAN und der dort nachgewiesenen Vorgänge hat im übrigen erneut bestätigt, daß die datenschutzrechtlichen Vorgaben bei der Datei- und Aktenführung weitgehend beachtet werden. Stichproben haben aber auch in Einzelfällen Mängel erkennen lassen:

So konnte bei verschiedenen Kriminalakten die Erforderlichkeit einer Speicherung nicht nachvollzogen werden, da nach Einstellung des Verfahrens nach § 170 Abs. 2 Strafprozeßordnung kein ausreichender Tatverdacht verblieben war. So wurde in einem Fall weiterhin vom Tatverdacht der Beleidigung ausgegangen, obwohl die während des Vorfalls anwesende Zeugin bekundete keine Beleidigungen gehört zu haben. In anderen Akten fehlte die Mitteilung über den Verfahrensausgang gänzlich, obwohl nach dem Zeitablauf der Abschluß des Verfahrens angenommen werden konnte.

Für **gravierender** halte ich jedoch die Feststellung, daß im Rahmen der Fristvergabe in Fällen von geringerer Bedeutung, bei denen Jugendliche von der Speicherung betroffen waren, Speicherungsfristen von 5 Jahren vergeben wurden, obwohl Art. 38 Abs. 2 Satz 4 PAG die Vergabe **kürzerer** Fristen **verbindlich** vorschreibt. Da die Regelfrist bei Jugendlichen bereits 5 Jahre beträgt, müssen hier kürzere Aussonderungsprüfdaten vergeben werden.

Auch diesmal habe ich die Polizei wieder auf Mängel bei der Vergabe des besonders sensiblen personengebundenen Hinweises (PHW) "geisteskrank" aufmerksam gemacht. Wie bereits in den Vorjahren (vgl. 16. Tätigkeitsbericht, Nr. 5.2.1) enthielten die überprüften Kriminalakten nicht die in der Errichtungsanordnung sowie in internen polizeilichen Dienstanweisungen geforderten

ärztlichen Bestätigungen.

Auf meine Anregung hin hat das Innenministerium folgende **Änderung** der Errichtungsanordnung vorgenommen:

Danach darf der PHW "geisteskrank" - dessen Vergabe insbesondere der Eigensicherung der einschreitenden Polizeibeamten und dem Schutz des Betroffenen dienen soll - **nur** gespeichert werden, wenn **ärztlich** festgestellt ist, daß der Betroffene an einer Geisteskrankheit leidet. Hierzu ist **zwingend** eine ärztliche Feststellung notwendig. Liegt diese schriftlich nicht vor, genügt auch die mündliche Aussage des Arztes oder die mündliche Übermittlung einer solchen ärztlichen Feststellung durch eine Behörde, die jedoch umgehend **schriftlich** zu bestätigen ist. Die mündliche Übermittlung ist in der Kriminalakte formlos zu **dokumentieren**. Mündliche Aussagen anderer Personen (einschließlich engster Angehöriger), die nicht durch eine schriftlichen ärztliche Feststellung belegt werden können, reichen für eine Vergabe **nicht** aus.

Ich hoffe, daß diese Präzisierung der Errichtungsanordnung zu einer besseren Nachvollziehbarkeit der Vergabe des PHW "geisteskrank" führen wird. Eine entsprechende Nachprüfung habe ich vorgesehen.

5.2.2 Datenerhebungen durch "Verdeckte Ermittler" oder "sonstige nicht offen ermittelnde Polizeibeamte"

Als Reaktion auf die qualitativen Veränderungen der Erscheinungsformen der Organisierten Kriminalität hat der Gesetzgeber im Jahre 1992 in der Strafprozeßordnung (StPO) bereichsspezifische Regelungen zum Einsatz **Verdeckter Ermittler** durch die Strafverfolgungsbehörden geschaffen. Wie sich aus den Gesetzesmaterialien ergibt, sollte daneben der Einsatz eines **gelegentlich verdeckt** auftretenden Polizeibeamten, insbesondere eines Scheinaufkäufers weiterhin nach den allgemeinen Vorschriften zulässig sein (Bundestags-Drs. 12/989, S. 41 ff).

Die Unterscheidung von Verdeckten Ermittlern und nicht offen ermittelnden Polizeibeamten bereitet Schwierigkeiten, denn in beiden Fällen offenbart der Polizeibeamte während seines Einsatzes gegenüber Dritten weder seine berufliche Aufgabe noch seine wahre Identität. Gerade die zutreffende rechtliche Einordnung des eingesetzten Beamten durch die Staatsanwaltschaft bzw. die Polizei ist aber von erheblicher Bedeutung, da sich die gesetzlichen Voraussetzungen für den Einsatz eines Verdeckten Ermittlers bzw. eines nicht offen ermittelnden Polizeibeamten wesentlich unterscheiden:

Im Ermittlungsverfahren darf ein Verdeckter Ermittler nur zur Aufklärung **bestimmter Straftaten** nach Zustimmung der Staatsanwaltschaft bzw. des Gerichts eingesetzt werden. Zur Gefahrenabwehr kommt der Einsatz eines Verdeckten Ermittlers nach Art. 33 Abs. 3 Nr. 2 Polizeiaufgabengesetz (PAG) nur bei **Straftaten von erheblicher Bedeutung** nach Zustimmung der im Gesetz vorgesehenen Entscheidungsträger in Betracht. Dagegen kann sich der Einsatz eines sonstigen nicht offen ermittelnden Polizeibeamten nur auf die allgemeinen Bestimmungen der Strafprozeßordnung und des Polizeiaufgabengesetzes stützen, die dem Beamten zwar keine besonderen Befugnisse einräumen, allerdings auch keine besonderen Schranken für seinen Einsatz vorsehen.

Die richtige Einordnung stellt sicher, daß Polizeibeamte nicht als "nicht offen ermittelnde Polizeibeamte" eingesetzt werden, wenn sie wegen der besonderen Intensität des Eingriffs in das Recht auf informationelle Selbstbestimmung der Betroffenen als Verdeckte Ermittler zu qualifizieren sind, deren Einsatz nur in den gesetzlich gezogenen engen Grenzen zulässig ist. Daß diese

Schwierigkeiten auch praktischer Natur sind, zeigen Entscheidungen bayerischer Instanzgerichte, die den Einsatz nicht offen ermittelnder Polizeibeamter als den Einsatz verdeckter Ermittler bewertet haben.

Es ist deshalb notwendig, Hilfestellung bei der Anwendung der gesetzlichen Definition des Verdeckten Ermittlers (vgl. § 110 a StPO) und seiner Abgrenzung zum nicht offen ermittelnden Polizeibeamten zu geben. Dies sollte in den entsprechenden Richtlinien des Innenministeriums geschehen.

Anhaltspunkte für eine Regelung gibt die Rechtsprechung des Bundesgerichtshofs. Sie geht davon aus, daß die innerdienstliche Bezeichnung des Beamten für die Unterscheidung zwischen Verdecktem Ermittler und nicht offen ermittelndem Polizeibeamten unerheblich ist. Entscheidend sei die Qualität des Einsatzes des Beamten. Diese sei anhand einer Gesamtwürdigung aller Umstände des Einzelfalles, insbesondere anhand der Dauer des Einsatzes, der Zahl der zu täuschenden Personen, dem Erfordernis, die Identität des Beamten geheimzuhalten, und der Intensität der Beeinträchtigung der Beschuldigtenrechte zu beurteilen (Urteil des BGH vom 06. Februar 1996, Neue Juristische Wochenzeitschrift 1996, S.2108).

Dagegen ist nicht entscheidend, ob es sich bei dem verdeckt eingesetzten Beamten um einen Scheinaufkäufer handelt oder nicht. Sowohl der nicht offen ermittelnde Polizeibeamte als auch der Verdeckte Ermittler können mit dem Ziel eingesetzt werden, einen Scheinkauf zu tätigen. Gerade beim Scheinkauf größerer Mengen illegaler Waffen, Drogen oder Falschgeld muß der verdeckt operierende Beamte gegebenenfalls durch mehrere Treffen über einen Zeitraum von Monaten ein gewisses Vertrauensverhältnis zu einem oder mehreren Tatverdächtigen aufbauen. In manchen Fällen benötigt auch der Scheinkäufer eine ausgearbeitete Legende.

Eine verdeckte Datenerhebung durch einen nicht offen ermittelnden Polizeibeamten - auf der Grundlage der allgemeinen gesetzlichen Bestimmungen - sollte nach meiner Auffassung auf kurzfristige, "punktuelle" Einsätze beschränkt werden. Greift der Beamte intensiver in das informationelle Selbstbestimmungsrecht des Betroffenen ein, indem er unter Verwendung einer falschen Identität über einen längeren Zeitraum gegen ihn ermittelt (z.B. auch im Rahmen von Scheinkaufverhandlungen), sollte dem Einsatz eines Verdeckten Ermittlers der Vorzug gegeben

werden.

In den Richtlinien sollte klargestellt werden, daß nicht jeder Scheinaufkäufer als bloßer "nicht offen ermittelnder Polizeibeamter" auftritt, sondern daß je nach Intensität der Einsatztiefe durchaus auch das Vorliegen eines Verdeckten Ermittlers in Frage kommen kann, für dessen Einsatz dann die entsprechenden Voraussetzungen der Strafprozeßordnung bzw. des Polizeiaufgabengesetzes gegeben sein müssen.

Ich habe mich in diesem Sinne an das Staatsministerium des Innern gewandt.

Das Innenministerium hat hierzu mitgeteilt, daß es die aktuelle Rechtsprechung unter Beteiligung der Justiz durch eine Analyse zur Abgrenzung von Verdeckten Ermittlern und nicht offen ermittelnden Polizeibeamten habe untersuchen lassen. Die Abgrenzungsprobleme seien in mehreren Besprechungen mit den Polizeipräsidenten und dem Bayerischen Landeskriminalamt erörtert worden.

Ich begrüße diese Diskussion, halte aber eine Umsetzung im Sinne der oben geforderten Klarstellung für erforderlich.

5.2.3 Dateien/Karteien

5.2.3.1. Dateien zur Gefahrenabwehr und Verfolgung von Straftaten und Ordnungswidrigkeiten - GAST-Dateien

GAST-Dateien stellen mittlerweile ein **wichtiges Hilfsmittel** der Polizei bei der Bewältigung der Informationsverarbeitung dar. Aufgrund der stetig verbesserten Ausstattung der Polizeidienststellen mit sog. Arbeitsplatzcomputern (APC) nahm die Zahl der bei mir eingegangenen Dateimeldungen **stark zu**. Ich konnte feststellen, daß bei der Polizei manuell geführte Datensammlungen verstärkt **aufgelöst** und als GAST-Anwendungen weitergeführt werden.

Die automatisierte Verarbeitung der Daten erleichtert einerseits die Datenpflege, wie beispielsweise die **Überwachung von Speicherungsfristen**, andererseits erleichtert sie aber auch die **Zugriffs- und Auswertungsmöglichkeiten**. Einer datenschutzgerechten Anwendung von GAST-Dateien kommt deshalb in diesem Bereich hohe Priorität zu. Dies gilt insbesondere auch deshalb, weil aufgrund der Vielzahl der Anwendungen in ganz Bayern nur ein geringer Teil unmittelbar vor Ort kontrolliert werden kann. Aus diesem Grunde habe ich alle bei mir eingegangenen Dateimeldungen einer sorgfältigen Prüfung unterzogen.

Anhand der mir übersandten polizeiinternen Genehmigungen der einzelnen GAST-Dateien habe ich die **Erforderlichkeit** der Dateien, die **Rechtmäßigkeit** der Datenerhebung und -verarbeitung überprüft.

Beispielhaft sind folgende Dateien zu nennen:

- Verantwortlichendatei - FIRMA
- Erkenntnisdatei - OK/OBB
- delinquente Jugendliche - JUBAN
- Prostitution - PROFU und PRORE/ZU
- Streifenbericht - ZEG
- polizeilich relevante Veranstaltungen - POLVA
- Kontaktbereich sowie Ein- und Auslauf
- Doping

- gruppentypische Aggressionsdelikte/kriminogene Gruppierungen - AKRI
- Lage- und ermittlungsunterstützende Dateien für unterschiedliche Deliktsbereiche (z.B. organisierte Kriminalität, Rauschgiftdelikte, Trickdiebstahl)
- Sekten.

Bei einigen Dateien fiel auf, daß **unzureichende** Festlegungen zur

- **Zweck**bestimmung der Datei
- Speicherungs**dauer** der Daten und zum
- **betroffenen Personenkreis**

getroffen waren.

Gerade bei der Bezeichnung des von der Speicherung betroffenen Personenkreises haben verschiedene Polizeidienststellen die **Rahmenvorgaben der GAST-Errichtungsanordnung** übernommen, ohne sich auf die Personengruppen zu beschränken, deren Speicherung im konkreten Einzelfall zur Aufgabenerfüllung erforderlich ist.

So waren z.B. "Mitteiler, Anzeigeerstatter, Geschädigte, Verletzte" zur suchfähigen Speicherung vorgesehen, ohne daß eine Notwendigkeit hierfür erkennbar war.

Ohne nähere Konkretisierung wurde vereinzelt die Gruppe "sonstige Personen" in die Dateigenehmigung aufgenommen.

Überprüfungsfristen/Speicherungsdauer waren für einzelne Dateien nur durch Bezugnahme auf die gesetzlichen Regelungen und die Richtlinien für die Speicherung polizeilicher personenbezogener Sammlungen festgelegt. Entsprechend dem oftmals **differenzierten** von einer Speicherung betroffenen Personenkreis (z.B. Beschuldigte, Geschädigte), wäre es aus datenschutzrechtlicher Sicht notwendig gewesen, **differenzierte Fristen** für die einzelnen Personengruppen zu vergeben, damit der gesetzlichen Forderung nach Transparenz der Speicherung genügt wird.

Ich habe in solchen Fällen mit der Polizei zusammen nach vertretbaren Lösungen gesucht und in der Regel auch gefunden.

5.2.3.1.1 Datei "GAST-SEKTEN"

Eine Polizeidienststelle hat mir eine Errichtungsanordnung für eine Datei "GAST-SEKTEN" übersandt.

Gemäß Ziff. 3 der Errichtungsanordnung ist Zweck der Datei die Abwehr von Gefahren für die öffentliche Sicherheit und Ordnung, die von Sekten, okkultischen Gruppen u.ä. Organisationen ausgehen. Die Datei soll insbesondere der Lagedarstellung über ansässige Gruppierungen, der inhaltlichen Gliederung der Informationssammlung über Sekten für die Sachbearbeitung und der Darstellung personeller Verbindungen, organisatorischer und wirtschaftlicher Zusammenhänge einzelner Gruppierungen und Unterorganisationen dienen. Darüber hinaus sollen Erkenntnisse für Strategien und ermittlungstaktisches Vorgehen gewonnen werden. Gespeichert werden u.a. Angehörige dieser Organisationen, die Schlüsselpositionen einnehmen. Was unter dem Begriff der "Sekte" oder "okkultischen Gruppierungen" verstanden wird, ist nicht näher ausgeführt.

Ich habe der Polizei mitgeteilt, daß ich aus datenschutzrechtlicher Sicht erhebliche Bedenken gegen die Führung einer solchen Datei habe. Nach meiner Auffassung ist die Errichtungsanordnung zu unbestimmt und damit zu weit gefaßt.

Als Sekte kann man jeden Zusammenschluß von Personen mit einem gemeinsamen religiösen Selbstverständnis außerhalb der anerkannten, insbesondere christlichen Glaubensrichtungen bezeichnen. Auf der Grundlage der Errichtungsanordnung könnten folglich Angehörige aller religiöser Gruppierungen, die nicht zu den anerkannten Religionen gehören, gespeichert werden. Eine Beschränkung auf Sekten, von denen im Einzelfall aufgrund tatsächlicher Anhaltspunkte angenommen werden kann, daß von ihnen Gefahren für die öffentliche Sicherheit und Ordnung ausgehen, ist nicht vorgesehen. Eine solche Beschränkung halte ich aber für eine grundlegende Voraussetzung der Speicherung.

Zwar kann die Polizei nach Art. 31 Polizeiaufgabengesetz auch personenbezogene Daten zur vorbeugenden Bekämpfung von Straftaten erheben, eine rein vorsorgliche Speicherung von Anhängern religiöser Glaubensrichtungen im Vorfeld polizeilicher Gefahrenlagen ohne Erkenntnisse für eine entsprechende Gefahrenprognose halte ich jedoch für unzulässig. Dies gilt insbesondere im Hinblick auf Art. 4 Grundgesetz (Glaubens-, Gewissens- und Bekenntnisfreiheit). Da-

nach steht jedem das Recht auf ungestörte Religionsausübung zu. Dieses Grundrecht umfaßt sowohl die individuelle als auch die kollektive Glaubensfreiheit, also das Recht, sich zu einer religiösen oder weltanschaulichen Gemeinschaft zusammenzuschließen. Die Glaubensfreiheit wird faktisch beeinträchtigt, wenn der einzelne befürchten muß, allein wegen seiner Aktivitäten in einer religiösen Gruppierung in einer polizeilichen Datei gespeichert zu werden.

Ich habe die Polizei aufgefordert, diesen Bedenken Rechnung zu tragen und mich darüber zu unterrichten.

Die Polizei hat inzwischen einen Vorschlag zur Begrenzung der Datei auf Sekten und okkultistische Organisationen vorgelegt, von denen Gefahren für die öffentliche Sicherheit und Ordnung ausgehen. Damit wurde mein Anliegen im Grundsatz aufgegriffen. Über die genaue Formulierung der Abgrenzung bin ich mit der Polizei noch im Gespräch.

5.2.3.1.2 GAST-Datei "Lagebild Fabrikschloß"

Bei einer von mir geprüften Polizeidirektion habe ich festgestellt, daß dort eine Datei geführt wird, in der aus polizeilicher Sicht relevante **Bewohner** und **Besucher** einer Unterkunft für Asylbewerber gespeichert werden. Nach Auskunft der Polizei sollen die in dieser Datei gespeicherten Daten **einsatztaktischen und logistischen Zwecken** dienen und sind für die **Erstellung eines Lagebildes** erforderlich. Als **Grund** für diese Maßnahme wurde von der Polizei ein überproportionaler **Anstieg der Kriminalität** in und um die Unterkunft angegeben. So sei die Unterkunft wie auch das Umfeld nach polizeilichen Erkenntnissen zu einem bedeutenden **Drogenumschlagplatz** geworden.

Nach der Errichtungsanordnung dürfen in der Datei personenbezogene Daten von **Verdächtigen** gespeichert werden, von denen aufgrund **tatsächlicher Anhaltspunkte** (verdeckte Ermittlungen oder offene Kontrollen) feststeht bzw. anzunehmen ist, daß sie sich in der Unterkunft **nur** zur Begehung von Straftaten **treffen** bzw. sich dort **aufhalten**.

Meine Prüfung hat ergeben, daß in einer Reihe von Fällen auch Personen in der Datei gespeichert waren, die **nicht** die in der Errichtungsanordnung genannten Voraussetzungen für eine Speicherung (u.a. besondere Intensität des kriminellen Verhaltens) erfüllten. So hatte die Polizei z.B. Personen erfaßt, die wegen Leistungserschleichung oder Ladendiebstahl in Erscheinung getreten waren.

Die Polizei hat aufgrund meiner Einwände die von mir kritisierten Vorgänge überprüft und aus der Datei **gelöscht**.

5.2.3.2 SPUDOK-Datei "Gewaltbereite Personen aus den Bereichen Rechts- und Linksextremismus, politisch motivierte Skinheads und Ausländergruppen - OFR-GEPE-S"

Die Datei wurde zur Unterstützung polizeilicher Ermittlungs- und Fahndungsmaßnahmen bei der Bekämpfung des **politisch motivierten gewalttätigen und gewaltbereiten Extremismus** eingesetzt.

Für die Datei, die von den Polizeidirektionen eines Polizeipräsidiums geführt wird, fehlt die erforderliche Errichtungsanordnung, die der Zustimmung des Innenministeriums bedarf und mir mitzuteilen ist und aus der sich insbesondere konkrete Festlegungen zum **betroffenen Personenkreis** sowie zu **Löschungs- und Aussonderungsfristen** ergeben.

Wie ich festgestellt habe, wurde die Datei im Gegensatz dazu ohne Errichtungsanordnung auf der Grundlage einer generellen Freigabe für SPUDOK-**Einzelermittlungsverfahren** von dem zuständigen Polizeipräsidium genehmigt, obwohl es sich bei der Datei **nicht um eine Datei zur Bearbeitung einzelner Ermittlungsverfahren**, sondern um eine nicht ermittlungsverfahrenbezogene, deliktsgruppenspezifische Arbeitsdatei handelt.

Wie mir das Polizeipräsidium nunmehr mitgeteilt hat, wurde die Datei inzwischen **gelöscht** und Speicherungen nach entsprechender Prüfung in die **Staatsschutzdatei Bayern (SDBY)** (vgl. Nr. 5.2.3.3) übernommen. Ich werde diese Übernahme prüfen, sobald meine Verhandlungen mit dem Innenministerium über die von mir für erforderlich gehaltenen Änderungen der Errichtungsanordnung für die Staatsschutzdatei abgeschlossen sind.

5.2.3.3 Errichtung einer bayerischen Staatsschutzdatei (SDBY)

Das Staatsministerium des Innern hat eine Errichtungsanordnung für eine bayernweite Staatsschutzdatei vorgelegt. Durch die Schaffung einer eigenständigen Landesdatei sollen staatsschutzrelevante personenbezogene Erkenntnisse auf Landesebene zentral gespeichert werden, die durch die Staatsschutzdienststellen der bayerischen Polizei abgerufen werden können. Die Staatsschutzdatei Bayern, die beim Bayerischen Landeskriminalamt geführt wird, soll die bislang bei den Dienststellen der bayerischen Polizei geführten manuellen Staatsschutzkarteien ablösen. Während in den manuellen Staatsschutzkarteien bislang nur Daten zur Verhütung und Verfolgung von Staatsschutzdelikten gesammelt und ausgewertet wurden, sollte die Staatsschutzdatei daneben auch der Verhütung und Aufklärung von Ordnungswidrigkeiten und verfassungsfeindlichen Handlungen **sowie** "sonstiger Verhaltensweisen im Sinne der Richtlinien für den Kriminalpolizeilichen Meldedienst in Staatsschutzsachen" dienen.

Ich habe in meiner Stellungnahme zu der Errichtungsanordnung gegenüber dem Staatsministerium des Innern auf folgende Punkte hingewiesen:

Die Einrichtung der Staatsschutzdatei Bayern führt zu einer erheblichen räumlichen (landesweite Abfragemöglichkeit) und sachlichen Erweiterung der Datenverarbeitung in dem besonders sensiblen Bereich des Staatsschutzes. Dabei ist besonders darauf zu achten, daß die Polizei nur die Aufgaben wahrnimmt, die ihr vom Gesetzgeber übertragen wurden, und nicht die Grenzen überschreitet, die sie von dem Bereich des Verfassungsschutzes trennt. Die Gefahr, die Trennung zwischen Polizei und Verfassungsschutz zu verletzen, besteht vor allem dort, wo weder Straftaten noch Ordnungswidrigkeiten in Frage stehen und sich der Aufgabenbereich der Polizei und die Zuständigkeit des Landesamtes für Verfassungsschutz bei der Verhütung verfassungsfeindlicher Handlungen berühren.

Die Beobachtung verfassungsfeindlicher Bestrebungen im Vorfeld rechtswidriger Handlungen ist Aufgabe des Verfassungsschutzes. Die Polizei ist im Bereich der Prävention einmal auf die vorbeugende Kriminalitätsbekämpfung, zum anderen auf die Verhütung verfassungsfeindlicher Handlungen beschränkt. Dabei muß die Begehung der verfassungsfeindlichen Handlungen in naher Zukunft zu befürchten sein, weil sonst eine Abgrenzung zu den Aufgaben des Verfas-

sungsschutzes nicht mehr gewährleistet wäre.

Außerdem muß die Errichtungsanordnung zu einer bayernweiten Staatsschutzdatei dem Recht auf informationelle Selbstbestimmung durch ausgewogene und verhältnismäßige Regelungen Rechnung tragen.

Aus datenschutzrechtlicher Sicht habe ich zusammengefaßt folgendes gefordert:

- Der Zweck der Datei muß aus der Errichtungsanordnung verständlich und nachvollziehbar umschrieben sein. Es muß unter Beachtung der Grenzen des polizeilichen Aufgabenbereichs klar festgelegt werden, welches Verhalten Anlaß für eine Speicherung in der Datei ist.

- Der Kreis der betroffenen Personen darf nicht zu weit gefaßt sein. Nicht jeder Kontakt einer Person zu extremistischen Personen oder Organisationen rechtfertigt die generelle Möglichkeit der Speicherung dieser Person in einer Staatsschutzdatei.

- Bei dem Umfang der erfaßten personenbezogenen Daten sollte eine Differenzierung nach Personengruppen stattfinden. So genügt es nach meiner Auffassung, wenn bei geschädigten oder gefährdeten Personen - sofern deren Speicherung im Einzelfall erforderlich ist - einige wenige wesentliche Informationen wie Personalien, Anschrift gespeichert werden.

- Aussonderungsprüffristen sowie die Speicherungsdauer sollten sich an den bisherigen Regelungen zu den manuell geführten Staatsschutzkarteien orientieren, soweit nicht die Erforderlichkeit längerer Fristen plausibel dargelegt werden kann.

Das Staatsministerium des Innern hat mir zwischenzeitlich den Entwurf einer geänderten Errichtungsanordnung übersandt. Darin sind meine datenschutzrechtlichen Forderungen zu einem wesentlichen Teil berücksichtigt, insbesondere ist der Zweck der Datei jetzt klar entsprechend der polizeilichen Aufgaben und Befugnisse auf die Verhütung und Aufklärung von Straftaten und Ordnungswidrigkeiten, verfassungsfeindlichen Handlungen und Gefährdungen von Personen beschränkt. Der unklare Hinweis auf "sonstige Verhaltensweisen im Sinn des Kriminalpolizeilichen Meldedienstes in Staatsschutzsachen" ist entfallen. Wegen der Speicherungsdauer der

Daten von Personen, die weder Beschuldigte noch Verdächtige sind, stehe ich mit dem Innenministerium noch in Kontakt.

Ich werde die Angelegenheit weiterverfolgen.

5.2.3.4 Speicherungen in der Lichtbildvorzeigekartei

Die Lichtbildvorzeigekartei (LVK) dient der **Ermittlung unbekannter tatverdächtiger Personen**. In die LVK können nach den landesweit geltenden Richtlinien für die Führung der Lichtbildvorzeigekartei Lichtbilder von Personen aufgenommen werden, die

- **verurteilt** oder
- einer rechtswidrigen Tat **dringend verdächtig** sind **und**
- bei denen nach Beurteilung ihres bisherigen Verhaltens **Wiederholungsgefahr** besteht.

Die stichprobenartige Prüfung gab nur in einem Fall Anlaß zu datenschutzrechtlicher Kritik:

Zu einem Lichtbild in der Kartei konnte **keine** Kriminalakte gefunden werden. Meine Nachforschungen ergaben, daß die Kriminalakte zu der Person bereits **vernichtet** worden war, es jedoch versäumt wurde, auch die LVK entsprechend zu bereinigen. Dies wurde umgehend nachgeholt.

Ich habe diese Feststellung zum Anlaß genommen, die Polizeidirektion aufzufordern, den übrigen Bestand der LVK auf gleichartige Fälle zu überprüfen und sicherzustellen, daß für die Zukunft entsprechende Mängel abgestellt werden.

5.3 Bayerisches Landeskriminalamt (BLKA)

Im Berichtszeitraum habe ich das Automatische FingerabdruckIdentifizierungssystem (AFIS), die Ausschreibungen zur Polizeilichen Beobachtung im Schengener Informationssystem (SIS) und die Speicherung von Verdachtsanzeigen nach dem Geldwäschegesetz (GwG) geprüft.

Darüber hinaus habe ich mich beim BLKA über die Maßnahmen zur verdeckten Datenerhebung durch sog. verdeckte Ermittler und nicht offen ermittelnde Polizeibeamte (vgl. Nr. 5.2.2) informiert.

5.3.1 Automatisches Fingerabdruck-Identifizierungssystem - AFIS

Nach dem Asylverfahrensgesetz vom 30. Juni 1993 sind grundsätzlich **alle Asylbewerber erkennungsdienstlich zu behandeln**.

Zur erkennungsdienstlichen Behandlung gehört auch die Abnahme der **Fingerabdrücke**, die eine sichere Identifizierung des Betroffenen ermöglichen. Dazu werden die Fingerabdrücke bei der Polizei abgenommen, vom Bundeskriminalamt (BKA) verformelt, gespeichert und ggf. mit anderen Fingerabdrücken verglichen.

Seit Dezember 1992 werden die Fingerabdrücke von Asylbewerbern durch das BKA mit AFIS verarbeitet. Für die Zwecke der **Kriminalitätsbekämpfung** (Spurenvergleich) wird AFIS seit Ende 1993 genutzt.

Beim Landeskriminalamt wurden sog. Erfassungsstationen installiert. Von dort werden zur Spurenverursacheridentifizierung Tatortspuren (Fingerabdrücke oder Fingerabdruckfragmente) automatisiert an das BKA übermittelt. Dort werden die Tatortspuren mit den in AFIS vorhandenen Fingerabdrücken verglichen. "Treffer" werden dem polizeilichen Sachbearbeiter am Bildschirm aufgezeigt. Wird ein Spurenverursacher ermittelt, können seine Personalien anhand der daktyloskopischen Nummer des verarbeiteten Fingerabdrucks über die Datei Informationssystem für die Polizei (INPOL) festgestellt werden. Bis zur Feststellung des Spurenverursachers läuft der Spurenvergleich anonym, d.h. ohne die Verwendung von Personalien ab.

Ein Vergleich von **Tatortspuren mit Fingerabdrücken von Asylbewerbern (AFIS-Asyl)** ist unter den Voraussetzungen des Asylverfahrensgesetzes (§ 16 Abs. 5) zur

- Feststellung der Identität oder der
- Zuordnung von Beweismitteln zulässig,

wenn **bestimmte Tatsachen** die Annahme begründen, daß dies zur Aufklärung einer Straftat führen wird oder es zur Abwehr einer erheblichen Gefahr für die öffentliche Sicherheit erforderlich ist.

Meine Prüfung sollte klären, ob diese Grenzen beachtet werden. Durch Einsichtnahme in ausgewählte Unterlagen zu Recherchen im sog. Gesamtbestand der Datei (einschließlich AFIS-Asyl) habe ich mich vom #

- **Anlaß** der Recherche in AFIS
- Vorliegen der **Abfragevoraussetzungen** im Gesamtbestand von AFIS und von der
- **Dokumentation der Gründe** für die Abfragen #
-

überzeugt.

Die von mir geprüften Fälle ließen deutliche Hinweise auf eine **Tatbeteiligung von bzw. Zusammenhänge mit Asylbewerbern** erkennen, die eine Recherche im Gesamtbestand rechtfertigen. Die Dokumentation der Verdachtsgründe war in den meisten Fällen vorgenommen worden.

Einen gravierenden Mangel stellt allerdings das **Fehlen einer Errichtungsanordnung für AFIS** und einer **fallbezogenen Protokollierung der Anfragen** im sog. Asylbestand von AFIS dar. Dies gilt umso mehr, da AFIS bereits seit Jahren ohne die erforderliche Grundlage vom BKA betrieben wird.

Darauf habe ich das Innenministerium nachdrücklich hingewiesen.

5.3.2 Speicherung von Verdachtsanzeigen nach dem Geldwäschegesetz (GwG)

In meinem 16. Tätigkeitsbericht (Nr. 5.11) habe ich ausführlich über das Inkrafttreten des GwG sowie über die Speicherung sog. Verdachtsanzeigen von Banken und bestimmten anderen Gewerbetreibenden bei der **Polizei** und der **Staatsanwaltschaft** berichtet.

Wie mir das BLKA mitgeteilt hat, gehen beim zuständigen Sachgebiet derzeit ca. 600 Verdachtsanzeigen pro Jahr ein. Diese wurden zum Zeitpunkt der Prüfung ausnahmslos in einer Arbeitsdatei gespeichert, die das BLKA neu eingerichtet hatte. Bezüglich der **Speicherungsdauer** wurde unterschieden in Fälle

- bei denen eine Straftat eher **unwahrscheinlich** erscheint (Speicherungsdauer: **2 Jahre**)

- von **Relevanz**, in denen von der Staatsanwaltschaft weiter ermittelt wird (Speicherungsdauer: **6 Jahre**).

Daneben werden Fälle, bei denen ein sog. **OK-Hintergrund** wahrscheinlich ist, in der Arbeitsdatei **APOK** (OK-Datei des Bundes) gespeichert.

Eine Speicherung im **Kriminalaktennachweis (KAN)** erfolgt dann, wenn das Verfahren durch die Staatsanwaltschaft nicht eingestellt, sondern an die örtlich zuständige Staatsanwaltschaft zur weiteren Ermittlung abgegeben wird.

Wie für jede andere DV-Anwendung der Polizei mit der personenbezogene Daten verarbeitet werden, muß auch für diese Datei eine Errichtungsanordnung vorliegen.

Wie ich festgestellt habe, bestand zwar zum Prüfungszeitpunkt eine Errichtungsanordnung für eine Arbeitsdatei Geldwäsche, die mir entgegen Art. 47 Abs. 1 Satz 2 PAG aber erst im Zuge meiner Prüfungsvorbereitungen mitgeteilt wurde. Darüber hinaus war die Datei auch **nicht** in die **Dateien- und Karteienübersicht** des BLKA aufgenommen worden. Das BLKA hatte aber bereits vor der Zustimmung des Innenministeriums zur Errichtungsanordnung (vgl. Art. 47 Abs. 2 PAG) die Datei in Betrieb genommen und personenbezogene Daten gespeichert. Mit Vorlage der

Errichtungsanordnung wurde die Datei nicht auf diese Grundlage umgestellt und entsprechend weitergeführt, vielmehr erfolgen die Speicherungen **datenschutzfreundlicher** (kürzere Speicherungsdauer), aber abweichend von den Vorgaben der Errichtungsanordnung.

Zwischenzeitlich hat mir das Innenministerium - aufgrund meiner Prüfungsfeststellungen - die überarbeitete Fassung der Errichtungsanordnung übersandt. Bezüglich des von der Speicherung **betroffenen Personenkreises** wie auch bezüglich der Dauer der **Überprüfungsfristen**, die teilweise zu einer Verschlechterung des Datenschutzes gegenüber der Praxis des BLKA führen, habe ich mich erneut an das Innenministerium gewandt und datenschutzrechtliche Verbesserungen gefordert.

5.3.3 Ablage von geklärten Spurenfällen beim Bayerischen Landeskriminalamt (BLKA)

Beim BLKA als polizeilicher Zentralstelle in Bayern werden alle von bayerischen Polizeidienststellen gesicherten Tatortspuren gespeichert und auf sog. Spurenkarten aufbewahrt. Im Rahmen meiner Prüfung habe ich festgestellt, daß in der Dienststelle "daktyloskopischer Erkennungsdienst" die dem BLKA übersandten **Spurenkarten von geklärten Fällen**, nach Jahrgängen geordnet, aufbewahrt werden. Wie das BLKA erläuterte, handelt es sich dabei sowohl um Fälle, die in kriminalistischer Hinsicht (Spur stammt von identifiziertem Täter) als auch aus daktyloskopischer Sicht (Spur stammt vom Berechtigten) geklärt sind.

Aus datenschutzrechtlicher Sicht unbefriedigend war die Tatsache, daß die Spurenkarten sowie die dazugehörigen Unterlagen (Originalspur, Gutachten) **10 Jahre** aufbewahrt werden und bei der Speicherungsfrist **keine Unterscheidung** nach Kindern, Jugendlichen oder Erwachsenen vorgenommen wurde.

Das BLKA hat aufgrund meiner Feststellung folgende Neuregelung getroffen:

- Die Ablage wurde bereinigt. Spurenkarten von **Berechtigten** in geklärten Fällen werden sofort nach dem Vergleich **vernichtet** und die Vergleichsabdrücke -wie auch schon bisher- über die zuständige Polizeidienststelle dem Geschädigten zurückgesandt.

- Spurenkarten zu identifizierten **Tatverdächtigen** werden grundsätzlich nach **5 Jahren ausgesondert**.

Die Aussonderung der Spurenkarten von tatverdächtigen Kindern wird durch eine elektronische Anbindung an den Kriminalaktennachweis nach 2 Jahren sichergestellt.

5.4 Polizeipräsidium München

Beim Polizeipräsidium München habe ich in mehrtägigen Prüfungen folgende Bereiche kontrolliert:

- Speicherungen im Zusammenhang mit den Vorkommnissen beim **Münchner Weltwirtschaftsgipfel 1992**
- Speicherungen in der **Haftanstalt** des Polizeipräsidiums
- Datei "AFB-**Anhaltedatei**"
- Datei "Kfz.-Fahndung-**Anhaltemitteilung** - AHM".

Im Ergebnis konnte ich feststellen, daß, abgesehen von einzelnen Mängeln, die Vorschriften des Datenschutzes beachtet werden.

5.4.1 Speicherungen im Zusammenhang mit den Vorkommnissen beim Münchner Weltwirtschaftsgipfel 1992

Aus Anlaß des Weltwirtschaftsgipfels im Juli 1992 in München richtete das Polizeipräsidium München eine Datei ein, in der zur Bewältigung der polizeilichen Aufgaben im Zusammenhang mit diesem Großereignis Daten gespeichert wurden. Diese Datei wurde zum 01. März 1993 aufgelöst. Personenbezogene Daten wurden aber - soweit nach Einschätzung der Polizei zur Aufgabenerfüllung erforderlich - in andere polizeiliche Dateien übernommen.

Dies betraf 479 Personen, gegen die die Polizei im Zusammenhang mit dem Verdacht auf Straftaten anläßlich des Weltwirtschaftsgipfels Ermittlungsverfahren eingeleitet hatte (vgl. meinen 16. Tätigkeitsbericht, Nr. 5.4.7). Den Beschuldigten wurde vorgeworfen, versucht zu haben, durch lautes Schreien und Pfeifen mit mitgebrachten Trillerpfeifen den Abbruch der Begrüßungszeremonie für den Weltwirtschaftsgipfel zu erzwingen (Vorwurf der versuchten Nötigung und der Verunglimpfung des Staates und seiner Symbole). Gegen einen Teil der Beschuldigten wurde außerdem wegen Widerstandshandlungen, Körperverletzung, Beleidigung u.a. im Zusammenhang mit der polizeilichen Festnahme ermittelt.

Die Staatsanwaltschaft hat zwischenzeitlich sämtliche Ermittlungsverfahren abgeschlossen. In 287 Fällen hat sie nach Mitteilung des Polizeipräsidiums München die Verfahren nach § 170 Abs. 2 Strafprozeßordnung (StPO) eingestellt, da den Beschuldigten weder eine Teilnahme an Störhandlungen beim Weltwirtschaftsgipfel noch an Delikten anläßlich der polizeilichen Ingewahrsamnahme nachgewiesen werden konnte. In 188 Fällen stellte die Staatsanwaltschaft die Verfahren nach § 153 StPO wegen geringer Schuld ein. In einer Reihe von Fällen erfolgte daneben eine Teilverfahrenseinstellung nach § 170 Abs. 2 StPO, wenn beispielsweise die Ermittlungen nur Anhaltspunkte für die Teilnahme an Widerstandshandlungen bei der Festnahme, nicht jedoch an Störungen bei der Begrüßungszeremonie des Weltwirtschaftsgipfels ergaben. In weiteren 4 Fällen hat das Polizeipräsidium München den Verfahrensausgang nicht mitgeteilt. Hierzu habe ich eine ergänzende Stellungnahme angefordert.

Das Polizeipräsidium München hat nach eigenen Bekundungen in allen 287 Fällen, die nach § 170 Abs. 2 StPO eingestellt wurden, zwischenzeitlich eine Löschung der gespeicherten Daten

durchgeführt. Außerdem wurden die der Speicherung zugrundeliegenden polizeilichen Unterlagen aus den Kriminalakten der Beschuldigten entnommen und vernichtet. Ich habe dies stichprobenartig überprüft. In einem Fall habe ich festgestellt, daß sich die entsprechende Unterlage nach wie vor in der Kriminalakte eines Beschuldigten befand, obwohl das Verfahren zwischenzeitlich eingestellt worden war. Eine Vernichtung der Unterlagen war jedoch nicht möglich, da in der Unterlage nicht nur das Verhalten des Beschuldigten beim Weltwirtschaftsgipfel, sondern - in enger räumlicher und sachlicher Verbindung - auch ein weiterer Vorfall zwei Tage später dokumentiert war.

In den 188 Fällen, in denen die Staatsanwaltschaft die Verfahren nach § 153 StPO wegen geringer Schuld (ggf. in Verbindung mit § 170 Abs. 2 StPO) eingestellt hatte, speichert die Polizei die erhobenen personenbezogenen Daten weiterhin im KAN. Für die Speicherungen wurde eine 5-jährige Aussonderungsprüffrist festgesetzt.

Aus datenschutzrechtlicher Sicht kann die weitere Speicherung in diesen Fällen nicht beanstandet werden. Nach Art. 38 Abs. 2 PAG kann die Polizei insbesondere personenbezogene Daten, die sie im Rahmen strafrechtlicher Ermittlungsverfahren oder von Personen gewonnen hat, die verdächtig sind, eine Straftat begangen zu haben, speichern, verändern und nutzen, soweit dies zur Gefahrenabwehr, insbesondere zur vorbeugenden Bekämpfung von Straftaten erforderlich ist. Die Daten sind zu löschen, wenn der der Speicherung zugrundeliegende Verdacht entfällt.

Die Staatsanwaltschaft hat die Ermittlungsverfahren **wegen geringer Schuld** eingestellt. Sie ist danach bei ihrer Entscheidung offensichtlich davon ausgegangen, daß die Beschuldigten im Zusammenhang mit dem Weltwirtschaftsgipfel strafbare Handlungen begangen haben. Auch das Oberlandesgericht München hat in seiner Entscheidung über Schmerzensgeldforderungen ausgeführt, daß die von der Polizei Festgenommenen jedenfalls eines Vergehens der versuchten Nötigung verdächtig gewesen sind (Urteil des OLG München vom 8.8.1996, Az. 1 U 3098/94).

Meine datenschutzrechtliche Prüfung ist eine **Rechtmäßigkeitskontrolle**. Trifft die Polizei eine Entscheidung im Rahmen des ihr zustehenden Ermessens- und Beurteilungsspielraums, kann ich dies nicht beanstanden. Im Hinblick auf die Entscheidungen der Staatsanwaltschaft und des OLG München muß die Annahme der Polizei, der Tatverdacht bestehe fort, auch von mir als vertret-

bar angesehen werden.

In einigen Fällen hat meine datenschutzrechtliche Prüfung allerdings ergeben, daß die im KAN festgelegten Aussonderungsprüffristen nicht auf die vorgesehene Dauer von 5 Jahren begrenzt waren. Dies hat die Polizei zwischenzeitlich korrigiert.

Korrekturbedürftig erscheint mir allerdings noch die Festsetzung einer Aussonderungsprüffrist von 5 Jahren in den Fällen, in denen die Beschuldigten zum Zeitpunkt des Weltwirtschaftsgipfels noch Jugendliche waren. Da für die erwachsenen Beschuldigten die Aussonderungsprüffrist von 10 Jahren auf 5 Jahre verkürzt wurde, sollte auch bei den Jugendlichen eine entsprechende Verkürzung der im Gesetz vorgesehenen Höchstfrist von 5 Jahren erfolgen. Dies habe ich dem Polizeipräsidium München mitgeteilt.

Neben den Speicherungen im KAN hat die Polizei im Zusammenhang mit dem Weltwirtschaftsgipfel auch Speicherungen in der Staatsschutzdatei Bayern (vgl. Nr. 5.2.3.3) vorgenommen. In Einzelfällen erfolgte außerdem die Vergabe des sog. KAN-Merkers 6 (Handeln zur Verfolgung extremistischer Ziele und fremdenfeindliche Straftaten), der eine bundesweite Speicherung bewirkt.

Ich habe die Polizei darauf hingewiesen, daß nach meiner Auffassung **allein** die Teilnahme an Störhandlungen beim Weltwirtschaftsgipfel oder an geringfügigen Widerstandshandlungen, Beleidigungen und ähnlichen Delikten im Zusammenhang mit der Festnahme der Betroffenen ohne sonstige einschlägige Vorerkenntnisse die Speicherung in einer Staatsschutzdatei oder die Vergabe des KAN-Merkers 6 nicht rechtfertigt. Ich sehe in einem solchen Verhalten noch keine ausreichenden Anhaltspunkte für die Annahme, daß sich die Betroffenen damit gegen die freiheitlich demokratische Grundordnung wenden.

Die Diskussion mit der Polizei in diesem Punkt ist noch nicht abgeschlossen.

5.4.2 Speicherungen in der Haftanstalt des Polizeipräsidiums

Beim Polizeipräsidium besteht aus organisatorischen und arbeitstechnischen Gründen eine **Polizeihaftanstalt**. Die dort eingelieferten und untergebrachten Personen sind im sog. **Haftbuch** zu dokumentieren. Neben dem Haftbuch wird auch eine alphabetische Schnellübersicht (sog. Renner) geführt.

Bei meiner Prüfung habe ich festgestellt, daß insgesamt 10 Haftbücher mit Renner aufbewahrt wurden, bei denen teilweise die letzten Eintragungen aus dem Jahr 1984 stammten.

Dies entspricht **nicht** den Vorgaben der Haftvollzugsordnung der Polizei (HVOPol). Danach ist der Aufnahmenachweis (Haftbuch) **5 Jahre** - gerechnet vom Zeitpunkt des letzten Eintrags - aufzubewahren.

Auf meinen entsprechenden Hinweis hat das Polizeipräsidium die Bücher umgehend **vernichtet**.

Außerdem befanden sich in einem separaten, für Vollzugsbeamte aber zugänglichen Raum in einem verschlossenen Rollschrank (Schlüssel beim Dienststellenleiter)

- sog. **Arzt-Bücher**, deren Eintragungen den Zeitraum vom 11.12.62 bis 23.7.80 sowie ab September 1980 bis zur Gegenwart umfaßten. In diesen Büchern vermerkt der hinzugezogene Arzt Anamnese, Befund und Therapie bei behandelten Gefangenen.

- sog. **Erste-Hilfe-Bücher**, deren Eintragungen den Zeitraum vom 1.1.73 bis 30.9.81 sowie ab September 1981 bis zur Gegenwart umfaßten. In diesen Büchern werden Hilfeleistungen des Sanitäters für Polizeibedienstete dokumentiert.

- das **Gefangenen-Krankenbuch**, deren Eintragungen den Zeitraum vom 1.1.74 bis 30.11.93 umfaßten. In diesem Buch wird in Kurzform der medizinische Befund des Sanitäters dokumentiert.

Ferner befanden sich im sog. Sanitätsraum die aktuell geführten Exemplare der o.g. Bücher. Zugriff auf diese Bücher hatten neben dem Polizeisanitäter auch der Dienststellenleiter und der

diensthabende Schichtleiter der Polizeihaftanstalt.

Spezielle gesetzliche Vorschriften für die Dauer der Aufbewahrung ärztlicher Unterlagen bestehen nicht. Jedoch schreibt § 11 der Berufsordnung für die Ärzte Bayerns vor, daß ärztliche Aufzeichnungen **10 Jahre nach Abschluß der Behandlung** aufzubewahren sind. **Nicht** zustimmen konnte ich der Auffassung des Polizeipräsidiums, die Frist sei ab Abschluß des jeweiligen - unter Umständen sehr umfangreichen - Buches zu berechnen. Ich halte es für zumutbar, daß auch das Polizeipräsidium für jedes Jahr ein neues Buch beginnt, welches zum Jahresende abgeschlossen und dann für 10 Jahre aufbewahrt wird.

Das Polizeipräsidium München hat aufgrund meiner Prüfung das Gefangenen-Krankenbuch **abgeschafft**. Das zuletzt geführte Gefangenen-Krankenbuch wird - wie die anderen o.g. Bücher - noch 5 Jahre nach dem letzten Eintrag aufbewahrt und dann vernichtet bzw. an den Ärztlichen Dienst der Bayerischen Polizei (Arzt-Buch) abgegeben.

Wegen des Abschlusses der Bücher zum Ende des Jahres bin ich mit dem Polizeipräsidium München noch im Gespräch.

5.4.3 Datei "AFB-Anhaltedatei"

Bei der Polizeiinspektion 11 des Polizeipräsidiums, die für den gesamten Altstadtbereich in München zuständig ist, wird zur **Unterstützung der polizeilichen Aufgabenerfüllung**, insbesondere im Altstadt-Fußgänger-Bereich (AFB), dem sog. Stachus-Bauwerk und dem Marienplatz-Untergeschoß eine Datei geführt, in die von polizeilichen Anhaltungen Betroffene gespeichert werden können. Die Datei soll der **Unterstützung des polizeilichen Einschreitens** und der **schnellen Informationsgewinnung** bei der Bearbeitung von Ermittlungsvorgängen (insbesondere Ordnungswidrigkeiten-Anzeigen) dienen.

Hintergrund für die Einrichtung der Datei sind Sicherheitsprobleme im Altstadtbereich, die durch das schwerpunktmäßige Auftreten insbesondere von Betäubungsmittelkonsumenten und -dealern, Jugendbanden, männlichen und weiblichen Prostituierten sowie Obdachlosen verursacht werden. Ich habe mich durch Einblick in die entsprechenden Unterlagen von der besonderen Kriminalitätslage und der konkreten Bedrohungssituation und von der grundsätzlichen Erforderlichkeit der Datei zur polizeilichen Aufgabenerfüllung überzeugt.

Unbefriedigend sind aus datenschutzrechtlicher Sicht aber die Festlegungen des "betroffenen Personenkreises" und der "Überprüfungsfristen" in der Errichtungsanordnung:

- Nach der zur Zeit der Prüfung gültigen **Errichtungsanordnung** dient die Datei dem Erkennen des Personenkreises, der sich im Umfeld von und in U/S-Bahnhöfen bzw. deren Untergeschossen **aufhält** und bei dem eine **Identitätsfeststellung** (Art. 13 Abs. 1 PAG) zulässig ist. Es können Personen aufgenommen werden, die sich in den oben genannten Bereichen ohne erkennbare Zweckbindung häuslich niederlassen sowie insbesondere Betäubungsmitteldealer und -konsumenten und Prostituierte, die die öffentliche Sicherheit und Ordnung stören.

- Die Festlegung des **betroffenen Personenkreises** ist nicht - wie aus datenschutzrechtlicher Sicht zu fordern - eindeutig und nachvollziehbar. Sie erlaubt ihrem Wortlaut nach **neben** der Speicherung der o.g. Personengruppen auch die Speicherung von anderen Personen, bei denen "nur" die Voraussetzungen der Identitätsfeststellung nach Art. 13 Abs. 1 PAG (z.B. der

bloße Aufenthalt an einem sog. verrufenen Ort wie Stachus-Untergeschoß) vorliegen. Tatsächlich speichert die Polizei z.B. auch Personen, die der Punker-Szene zugeordnet werden, ohne daß von ihnen konkrete Störungen ausgehen müssen. Zur Begrenzung des betroffenen Personenkreises bedarf es präziser Bestimmungen, aus denen im vorhinein erkennbar ist, wer Betroffener einer Speicherung werden kann. Ich habe deshalb das Polizeipräsidium München aufgefordert, eine **abschließende** Aufzählung des betroffenen Personenkreises vorzunehmen und habe angeregt, zu diesem Zweck folgende zusätzliche Kategorie aufzunehmen: "sonstige Personen, wenn konkrete Anhaltspunkte dafür vorliegen, daß von ihnen Gefahren für die öffentliche Sicherheit und Ordnung ausgehen."

Das Polizeipräsidium München ist meiner Anregung gefolgt.

5.4.4 Datei "Kfz.-Fahndung-Anhaltemitteilung - AHM

Die Datei dient der Unterstützung polizeilicher Fahndungsmaßnahmen bei der **Bekämpfung der internationalen Kfz-Verschiebung**. Mit der Datei wurde ein seit Jahren bestehendes Formblattverfahren durch ein automatisiertes Verfahren abgelöst.

Zum Zeitpunkt der datenschutzrechtlichen Kontrolle waren sechs Personen gespeichert. Bei drei Speicherungen habe ich festgestellt, daß auch Rechercheversuche in der Datei und das Ausfüllen einer **Leermaske** mit Schulungsdaten zu einer **Datenspeicherung** führen.

Ich habe das Polizeipräsidium aufgefordert, die fehlerhaften Daten zu löschen.

5.4.5 Presseberichte

Beim Polizeipräsidium München habe ich die Presseberichte für einen bestimmten Zeitraum anhand der Entschließung der Datenschutzbeauftragten des Bundes und der Länder zur Übermittlung personenbezogener Daten der Strafverfolgungsbehörden an die Medien (vgl. Anlage 5) überprüft.

Ich habe gegenüber dem Polizeipräsidium deutlich gemacht, daß dem allgemeinen Informationsinteresse der Öffentlichkeit in der Regel ohne Namensnennung entsprochen werden kann und Namen und Berufsbezeichnung der als Täter ermittelten Person nur in begründeten Ausnahmefällen und nur bekanntgegeben werden darf, wenn die Bekanntgabe einem überwiegenden öffentlichen Interesse entspricht. Dabei ist auch zu berücksichtigen, daß nicht nur durch die vollständige Bekanntgabe des Namens des Betroffenen eine Identifizierung ermöglicht wird. Auch durch Hinweis auf sonstige personenbezogene Angaben, wie Wohnort, Alter, Beruf oder familiäre Verhältnisse usw. können Rückschlüsse auf die Person des Täters oder Opfers möglich sein. In zwei Fällen werden nach meiner Auffassung Presseberichte des Polizeipräsidiums München diesen datenschutzrechtlichen Anforderungen nicht in vollem Umfang gerecht. So können Personen, gegen die ermittelt wird oder die Opfer einer Straftat geworden sind, von Nachbarn oder Arbeitskollegen anhand der in der Presseerklärung enthaltenen Hinweise identifiziert werden, ohne daß ich für die Bekanntgabe der Daten der Betroffenen im konkreten Fall das erforderliche überwiegende öffentliche Interesse erkennen kann.

Wegen der von mir angesprochenen grundsätzlichen datenschutzrechtlichen Fragen im Zusammenhang mit polizeilichen Presseerklärungen hat sich das Polizeipräsidium München an das Innenministerium gewandt.

Eine Äußerung des Staatsministeriums des Innern steht noch aus.

Zur ähnlich liegenden Problematik der Übermittlung von Anklagesätzen und Sitzungslisten für Pressevertreter vgl. den Beitrag Nr. 7.6.3.

5.5 Anwendung des Polizeiaufgabengesetzes (PAG)

5.5.1 Übermittlung personenbezogener Daten gewalttätiger Fußballfans durch die Polizei an Fußballvereine

Mit der Einführung eines "Nationalen Konzeptes Sport und Sicherheit" sollen als eine Maßnahme gegen die Gewalt rund um den bezahlten Fußball sog. "bundesweite Stadionverbote" für auffällig gewordene Fußballfans ermöglicht werden. Zur Erteilung eines bundesweit wirksamen Stadionverbotes kommt es dann, wenn der jeweils örtliche Fußballverein beim Deutschen Fußballbund ein solches Verbot gegen eine bestimmte Person beantragt und der Deutsche Fußballbund das Stadionverbot ausspricht. Anlaß für einen derartigen Antrag des örtlichen Fußballvereins sind Informationen über evtl. Fehlverhalten eines Fußballfans im Rahmen der Sportveranstaltung oder in deren erweiterten Umfeld (Anfahrtswege, Gastronomie im Umfeld, öffentliche Verkehrsmittel). Diese Informationen erhält der Fußballverein entweder durch einen eigenen Ordnungsdienst **oder durch die Polizei**.

Wie mir das Bayerische Staatsministerium des Innern sowie das Innenministerium Nordrhein-Westfalen als Geschäftsstelle des nationalen Ausschusses Sport und Sicherheit mitgeteilt haben, übermittelt die bayerische Polizei entsprechend den Vorschlägen der Arbeitsgruppe "Nationales Konzept Sport und Sicherheit" Fußballvereinen bei Straftaten die Personalien von Tatverdächtigen sowie die Bezeichnung der zugrundeliegenden Straftat **von sich aus**, wenn Motivation und Art der Ausführung des Delikts den für Fußballrowdies typischen Charakter aufweisen. Dies gilt sowohl für Straftaten, die im Hausrechtsbereich des Veranstalters begangen werden, als auch für Straftaten außerhalb des Stadions, soweit ein Zusammenhang mit dem Fußballspiel besteht.

Die Datenübermittlung erfolgt auf der Grundlage des Art. 41 Abs. 1 Bayerisches Polizeiaufgabengesetz zu Recht. Nach dieser Vorschrift kann die Polizei von sich aus personenbezogene Daten an Personen oder Stellen außerhalb des öffentlichen Bereichs u.a. dann übermitteln, soweit dies zur Erfüllung polizeilicher Aufgaben erforderlich ist und kein Grund zur Annahme besteht, daß der Betroffene ein schutzwürdiges Interesse an dem Ausschluß der Übermittlung hat.

Zweck der Datenübermittlung ist nicht nur, dem geschädigten Verein die Gelegenheit zu geben,

seine zivilrechtlichen Ansprüche gegenüber einem Schädiger geltend machen zu können. Das gesamte Konzept zielt vielmehr darauf ab, durch die Erteilung von Stadionverboten für gewalttätige Fußballfans Ausschreitungen bei zukünftigen Spielen zu verhindern. Auf diese Weise werden zum einen friedliche Zuschauer vor potentiellen gewaltbereiten Personen geschützt. Zum anderen wird verhindert, daß Dritte während eines Fußballspiels zu Straftaten angestiftet werden. Die Polizei hat selbst nicht die rechtliche Möglichkeit, einem gewalttätigen Fußballfan den Besuch weiterer Veranstaltungen zu untersagen. Das Ziel, Ausschreitungen im Zusammenhang mit Fußballspielen mit Hilfe von Stadionverboten zu verhindern, kann nur dadurch erreicht werden, daß die betroffenen Fußballvereine von den Personalien gewalttätiger Fans in Kenntnis gesetzt werden und Stadionverbote verhängen. Die Datenübermittlung ist damit erforderlich zur Erfüllung einer polizeilichen Aufgabe, nämlich der Abwehr von Gefahren für die öffentliche Sicherheit und Ordnung bei künftigen Fußballspielen. Anlaß hierfür können nicht nur Straftaten im Stadionbereich, sondern auch Delikte außerhalb des Stadions im Zusammenhang mit dem Fußballspiel sein.

5.5.2 Meldung über Drogen- und Rauschmittelkonsum durch die Polizei an das Gesundheitsamt und die Führerscheinstelle

Eine Stadtverwaltung hat sich mit folgendem Anliegen an mich gewandt:

Eine Polizeidienststelle hatte sowohl das Gesundheitsamt als auch die Führerscheinstelle der Stadt darüber informiert, daß nach den polizeilichen Ermittlungen eine im Stadtgebiet wohnhafte, namentlich benannte Person gelegentlich Drogen konsumiert.

Auf meine Nachfrage hat das Staatsministerium des Innern mitgeteilt, daß die Polizei Führerscheinstellen personenbezogene Erkenntnisse über Drogen- und Rauschmittelkonsum mitteilt, wenn bei Fahrerlaubnisinhabern Anhaltspunkte für eine Rauschmittelabhängigkeit oder zumindest für einen regelmäßigen Konsum von Rauschmitteln bestehen. Beim Verdacht auf Drogenabhängigkeit sowie bei Erkenntnissen über intravenösen Drogenkonsum einer Person erfolgt außerdem eine polizeiliche Meldung an die Gesundheitsämter.

Aus datenschutzrechtlicher Sicht beurteile ich die Datenübermittlung wie folgt:

Nach Art. 40 Abs. 3 Polizeiaufgabengesetz kann die Polizei von sich aus die ihr bei Erfüllung ihrer Aufgaben bekannt gewordenen personenbezogenen Daten an andere Behörden oder öffentliche Stellen übermitteln, soweit diese für die Gefahrenabwehr zuständig sind und die Kenntnis der Daten zur Erfüllung der Aufgaben des Empfängers erforderlich erscheint.

Führerscheinstellen haben nach § 15 Straßenverkehrszulassungsordnung die Aufgabe, zur Wahrung der Verkehrssicherheit Personen auf ihre Eignung zum Führen von Kraftfahrzeugen zu überprüfen. Hat die Polizei konkrete Anhaltspunkte dafür, daß eine Person nicht geeignet ist, ein Kraftfahrzeug zu führen, kann sie diese Anhaltspunkte der Führerscheinbehörden mitteilen. Ein Indiz für einen Eignungsmangel eines Führerscheininhabers kann der **regelmäßige** Konsum von Drogen sein. Auch der Hinweis auf die **gewohnheitsmäßige Einnahme sog. "weicher" Drogen** kann die ernsthafte Besorgnis begründen, daß der Betroffene zur Führung eines Kraftfahrzeugs ungeeignet ist.

Nach dem Gesetz über den öffentlichen Gesundheitsdienst beraten die Gesundheitsämter Personen, die drogensüchtig sind oder regelmäßig Rauschmittel konsumieren. Außerdem haben die Gesundheitsämter die Aufgabe, Maßnahmen zur Verhütung und Bekämpfung der Immunschwächekrankheit AIDS zu ergreifen (§ 31 ff Bundesseuchengesetz). Hierzu zählt auch die körperliche Untersuchung von Personen, die im Verdacht stehen, aidsinfiziert zu sein. Personen, die intravenös Drogen einnehmen, erkranken überdurchschnittlich häufig an AIDS und zählen deshalb nach der Bekanntmachung des Staatsministeriums des Innern vom 19. Mai 1987 zum Bundesseuchengesetz zu den ansteckungsverdächtigen Personen (MABl 1987, S. 246). Hat die Polizei Anhaltspunkte für einen intravenösen Drogenkonsum eines Verdächtigen, muß sie dies der Gesundheitsbehörde mitteilen, damit das Gesundheitsamt nach dem Bundesseuchengesetz tätig werden kann.

Die vom Innenministerium dargelegte Praxis der polizeiliche Datenübermittlung von Hinweisen auf den gewohnheitsmäßigen bzw. intravenösen Drogenkonsum einer Person an die zuständigen Führerschein- und Gesundheitsbehörden dient damit der Gefahrenabwehr und erscheint zur Erfüllung der Aufgaben dieser Behörden erforderlich. Sie ist aus datenschutzrechtlicher Sicht nicht zu beanstanden.

5.5.3 Mitteilungen und Auskünfte der Polizei gegenüber der Deutschen Telekom

Die Polizei hat sich mit der Frage an mich gewandt, ob die Deutsche Telekom AG nach ihrer Umstrukturierung nunmehr als privates Unternehmen oder als öffentliche Stelle bzw. Behörde im Sinne der Übermittlungsvorschriften des Polizeiaufgabengesetzes anzusehen sei.

Ich habe der Polizei hierzu folgende Auskunft erteilt:

Art. 40 PAG regelt die Datenübermittlung der Polizei innerhalb des öffentlichen Bereichs. Nachdem das Polizeiaufgabengesetz keine Definition des Begriffs "öffentliche Stelle" enthält, ist bei der Auslegung die Legaldefinition des Bayerischen Datenschutzgesetzes heranzuziehen. Gem. Art. 4 Abs. 2 BayDSG zählen zu den öffentlichen Stellen bei Datenübermittlungen auch die öffentlichen Stellen des Bundes nach § 2 BDSG. Dazu gehören auch die aus dem Sondervermögen Deutsche Bundespost durch Gesetz hervorgegangenen Unternehmen, **solange** ihnen ein ausschließliches Recht nach dem Postgesetz oder dem Gesetz über Fernmeldeanlagen zusteht. Dies ist bei der Telekom noch bis zum 31.12.1997 der Fall (vgl. meinen 16. Tätigkeitsbericht, Nr. 5.6.2).

Auf der anderen Seite ist zu berücksichtigen, daß nach Art. 143 b Abs. 1 Grundgesetz i.V.m. dem Gesetz zur Neustrukturierung des Post- und Fernmeldewesens und der Deutschen Bundespost die Telekom nunmehr grundsätzlich privatrechtlich tätig wird. Sie erbringt nicht nur Leistungen im Monopolbereich des Fernmeldeanlagengesetzes, sondern auch Leistungen, bei denen sie mit privaten Unternehmen konkurriert, etwa beim Verkauf von Telefonanlagen. Es besteht kein sachlicher Grund, die Telekom in diesem Bereich gegenüber privaten Konkurrenzunternehmen zu privilegieren. Trotz der grundsätzlichen Einordnung der Telekom als öffentliche Stelle sind deshalb die Vorschriften zur Datenübermittlungen an nicht-öffentliche Stellen entsprechend anwendbar, **soweit die Telekom** wie andere privatrechtliche Unternehmen **am Wettbewerb** teilnimmt.

Diese differenzierte Auffassung zur Rechtsstellung der Telekom wird vom Innenministerium geteilt.

5.5.4 Dokumentation der Datenübermittlungen der Polizei an andere öffentliche Stellen

Im täglichen Verwaltungsvollzug kommt es in einer Vielzahl von Fällen zu Übermittlungen personenbezogener Daten von Polizeibehörden an andere öffentliche Stellen. So bitten beispielsweise regelmäßig die Kreisverwaltungsbehörden um Übermittlung von polizeilichen **Erkenntnissen**, um für die Entscheidung über die Erteilung eines Waffenscheines, einer Gaststättenerlaubnis o.ä. die **Zuverlässigkeit** des Antragstellers überprüfen zu können.

Allerdings darf die Polizei bei einer allgemein gehaltenen Anfrage nach "Erkenntnissen" nicht wahllos jedes von ihr in den verschiedenen polizeilichen Dateien und Akten gespeicherte personenbezogene Datum übermitteln. Vielmehr hat sie **vor** der Datenübermittlung eine **Auswahl** unter dem Gesichtspunkt der **Erforderlichkeit** der Daten für die Aufgabenerfüllung durch die anfragende Behörde zu treffen.

Im Interesse der Nachvollziehbarkeit polizeilichen Handelns, insbesondere die notwendigen Grundlagen zur Prüfung der Rechtmäßigkeit der Datenübermittlung sicherzustellen, hat die Polizei nach innerdienstlichen Richtlinien, die datenschutzrechtliche Forderungen berücksichtigen, festzuhalten, an **wen** sie Erkenntnisse weitergegeben hat, wenn Auskünfte aus polizeilichen personenbezogenen Sammlungen an Berechtigte außerhalb der aktenführenden Dienststelle erteilt wurden. Soweit nichts Abweichendes in der Akte vermerkt wird, gilt der zu diesem Zeitpunkt bestehende Umfang an Sachverhalten als übermittelt.

Zur Überprüfung der vorgeschriebenen Dokumentation bei einer Polizeidirektion wurde, mangels entsprechender Auswertungsmöglichkeiten polizeilicher Dateien, von einer Sicherheitsbehörde (Landratsamt) eine Liste mit Namen solcher Personen erbeten, zu denen in einem bestimmten Zeitraum **Erkenntnisanfragen** bei einer Polizeiinspektion gestellt worden waren.

Nur in einem Fall konnte ich in diesem Zusammenhang in der **Vorgangsverwaltung** der Polizeiinspektion eine Speicherung feststellen, die sich offenbar auf eine Erkenntnisanfrage des Landratsamtes in einer Waffensache bezog. Der Speicherung konnte aber nicht entnommen werden, **ob** und **in welchem Umfang** die Polizei in diesem Fall personenbezogene Daten an das Landratsamt übermittelt hatte. Es stellte sich heraus, daß die Dienststellen innerhalb der Polizeidirektion nur bestimmte Anfragen in der Vorgangsverwaltung dokumentieren. So dokumentiert

---

die Polizeiinspektion beispielsweise Erkenntnisanfragen im Zusammenhang mit der Wiedererteilung der Fahrerlaubnis, die Kriminalpolizei beispielsweise Anfragen betreffend die Erteilung von Waffenerlaubnissen. Ferner entstand der Eindruck, daß bei beiden Dienststellen **nicht** sichergestellt ist, daß die Übermittlung von Erkenntnissen entsprechend den Vorgaben in den Richtlinien **dokumentiert** wird.

Aufgrund meiner Prüfungsfeststellungen hat die Polizeidirektion für ihre Dienststellen eine **Dienstanweisung** erlassen, die eine ausreichende Dokumentation sicherstellen soll. Dazu wurde auch der entsprechende **Dateibildschirm** der Vorgangsverwaltung überarbeitet und den Notwendigkeiten im Rahmen der Dokumentation angepaßt.

5.5.5 Polizeiliche Beobachtung

Bei einer Polizeidirektion habe ich erneut den Einsatz der polizeilichen Beobachtung (PB) überprüft. Bei allen von mir kontrollierten Einzelvorgängen waren die Voraussetzungen für die Anordnung der Maßnahme gegeben. Ich habe aber festgestellt, daß die **Dauer** der Maßnahme stets auf 1 Jahr angeordnet wurde, obwohl die Jahresfrist im Gesetz (Art. 36 Abs. 3 Satz 2 PAG) als Höchstfrist konzipiert ist. Auch war offensichtlich keine Überprüfung der **Notwendigkeit der Fortführung** der Maßnahme während des Laufs der Jahresfrist erfolgt. Gerade im Hinblick auf die besondere Eingriffsintensität der Maßnahme sollten nicht pauschal die gesetzlichen Möglichkeiten ausgenutzt, sondern **fallbezogen** eingesetzt werden. Dazu gehört auch eine begleitende polizeiliche Kontrolle der Maßnahme um ggf. zu erkennen, daß die Löschung der Ausschreibung zur polizeilichen Beobachtung veranlaßt ist, etwa weil der Zweck der Maßnahme nicht mehr erreicht werden kann.

Bemängelt habe ich auch die **Führung** der PB-Unterlagen. So war in einem Fall der Vorgang nach fast 1 Jahr nach Abschluß der Ausschreibung noch nicht der Kriminalakte beigegeben worden. In einem anderen Fall wurden Unterlagen bei zwei verschiedenen Dienststellen aufbewahrt. Dadurch war eine zeitgerechte **Aussonderung** und **Vernichtung** der Unterlagen, die nicht der entsprechenden Kriminalakte beigegeben waren, gefährdet.

Ich habe die Polizei auf diese Überlegungen hingewiesen und werde mich durch eine erneute Kontrolle davon überzeugen, ob die Maßnahme von einer fallbezogenen Erforderlichkeitsprüfung abhängig gemacht wird.

5.5.6 Zusatzprotokollierung bei Abfragen im Informationssystem der Bayerischen Polizei

Auf die Notwendigkeit der Zusatzprotokollierung (Zweck der Abfrage, ggf. Aktenzeichen des bearbeiteten Vorgangs) bei Abfragen im Informationssystem der Bayerischen Polizei habe ich eingehend im 16. Tätigkeitsbericht (Nr. 5.5.3) hingewiesen. Das Staatsministerium des Innern lehnt die von mir angeregte Zusatzprotokollierung mit der Begründung **ab**, es sei damit ein unverhältnismäßiger Verwaltungsaufwand sowie eine unzumutbare Mehrbelastung der Rechneranlagen verbunden. Außerdem sei nicht in allen Fällen, in denen Abfragen aus polizeilichen Informationssystemen erforderlich sind, ein Aktenzeichen vorhanden.

Ich bedauere diese Entscheidung und habe darauf hingewiesen, daß eine Zusatzprotokollierung nach meiner Ansicht eine **wesentliche Verbesserung** des Datenschutzes darstellen würde. Meine bisherigen Erfahrungen anläßlich praktischer Kontrollen haben gezeigt, daß die nach dem Polizeiaufgabengesetz zum Zwecke des Datenschutzes zulässige Auswertung der Protokollbestände ohne die Protokollierung zusätzlicher Angaben regelmäßig nicht für die datenschutzrechtliche Beurteilung der Zulässigkeit von Abfragen ausreicht. Folgerichtig ist für polizeiliche Abfragen im Zentralen Verkehrsinformationssystem in Flensburg auch der Anlaß der Abfrage zu protokollieren. Dies - ergänzt durch das Aktenzeichen des Vorgangs, soweit vorhanden - sollte auch für Abfragen im Informationssystem der Bayerischen Polizei (IBP), in Bundesdateien (INPOL) sowie in den über IBP erschließbaren Dateien möglich sein.

5.6 Übersendung von TÜ-Protokollen per Fax

Von der Presse wurde ich informiert, daß eine Firma seit Jahren Unterlagen per Fax erhalten hat, die für ein Amtsgericht bestimmt waren. Zuletzt erhielt die Firma ein 40-seitiges Telefonabhörprotokoll per Fax, das die Polizei dem Ermittlungsrichter beim Amtsgericht übersenden wollte. Ursache für die zahlreichen Fehlleitungen war eine große Ähnlichkeit der Faxnummer des Amtsgerichts mit der Faxnummer der betroffenen Firma. So war es auch im vorliegenden Fall nach Mitteilung der Polizei zu einer fehlerhaften Eingabe der Faxnummer und damit zu einem Fehlversand gekommen.

Ich habe den Vorfall zum Anlaß genommen, beim Direktor des Amtsgerichts die Änderung der Fax-Nummer des Amtsgerichts anzuregen. Nach Mitteilung des Amtsgerichtsdirektors ist eine solche Änderung nicht mehr erforderlich, da die betreffende Firma ihren Geschäftssitz verlegt und eine neue Faxnummer erhält. Er werde sich darum bemühen, daß die bisherige Faxnummer der Firma nicht mehr vergeben werde. Die Polizei hat die Beamten im Hinblick auf die fehlerhafte Eingabe der Faxnummer ausdrücklich darauf hingewiesen, daß bei der Versendung von Dokumenten per Fax besondere Sorgfalt geboten ist.

Unabhängig von dem konkreten Einzelfall habe ich gegenüber den Amtschefs der Staatskanzlei und der Ressorts auf die grundsätzliche Problematik der Übersendung von vertraulichen Unterlagen per Fax aufmerksam gemacht.

Gegenüber den Staatsministerien des Innern und der Justiz habe ich in diesem Zusammenhang darüber hinaus auf die besondere Sensibilität der durch eine Telefonüberwachung gewonnenen personenbezogenen Daten hingewiesen. Das Abhören und Aufzeichnen von Telefongesprächen durch die Strafverfolgungsbehörden stellt nicht nur einen Eingriff in das informationelle Selbstbestimmungsrecht, sondern auch einen Eingriff in das grundgesetzlich geschützte Fernmeldegeheimnis dar. Betroffen sind regelmäßig nicht nur Verdächtige, sondern auch unbeteiligte Dritte, wie beispielsweise Gesprächspartner oder Familienangehörige verdächtiger Personen. Die erfaßten Gespräche können einen vertraulichen oder darüber hinaus intimen Inhalt haben.

Protokolle über eine Telefonüberwachung sind daher besonders schutzbedürftig. Die Gefahr, daß

unbefugte Dritte vom Inhalt solcher Telefonüberwachungsprotokolle Kenntnis erlangen, muß im Rahmen der Verhältnismäßigkeit möglichst gering gehalten werden. Eine Versendung solcher Unterlagen per Fax halte ich deshalb aus datenschutzrechtlicher Sicht im Regelfall für problematisch, sofern nicht durch sonstige Maßnahmen - etwa durch den Einsatz von Verschlüsselungstechniken - der besonderen Sensibilität der Daten Rechnung getragen wird.

Das Justizministerium hat dahingehend Stellung genommen, daß es sich bei Protokollen über eine Telefonüberwachung in der Regel um besonders schutzwürdige Unterlagen handele, bei denen im Einzelfall stets sehr sorgfältig geprüft werden müsse, ob unter Berücksichtigung der datenschutzrechtlichen Belange eine Übermittlung der Unterlagen per Fax erfolgen könne.

Das Innenministerium hat mein Schreiben zum Anlaß genommen, die nachgeordneten Behörden und Dienststellen auf die Gefahren von Fehlübertragungen beim Datentransport mit Telefax hinzuweisen und darauf aufmerksam zu machen, daß vor dem Versand von schutzwürdigen Daten mit dem Telefaxdienst die Erforderlichkeit und Angemessenheit der Versandart zu prüfen ist.

Das Innenministerium wird die Problematik in einer gemeinsamen Dienstbesprechung mit den Polizeipräsidenten, an der auch Vertreter des Justizministeriums und der Staatsanwaltschaften teilnehmen sollen, erörtern.

Ich begrüße die vom Staatsministerium des Innern ergriffenen Maßnahmen als einen ersten notwendigen Schritt zur Verbesserung der Sicherheit beim Versand sensibler personenbezogener Daten über Telefax. Gleichwohl bin ich der Auffassung, daß dies nur der Anfang in der Verbesserung des Datenschutzes in diesem Bereich sein kann. Für möglichst zuverlässige Sicherheit bei der Übermittlung sensibler Daten sind wegen der Fehlerempfindlichkeit der Faxverwendung und des Abhör- und Eingriffsrisikos auch technische Maßnahmen notwendig, insbesondere die Verschlüsselung. Ich bin deshalb der Auffassung, daß zumindest mittelfristig das Sicherheitssystem durch Verschlüsselung vervollständigt werden sollte, wenn sensible Daten über offene Netze übermittelt werden. Auf die Ausführungen im technisch-organisatorischen Teil meines Berichts (Nr. 18.3.6) weise ich hin.

5.7 Errichtungsanordnung für die polizeilichen Dateien "Polizeiliche Sachbearbeitung/Vorgangsverwaltung - Verbrechensbekämpfung" (PSV) und für die "Personen- und Fall-Auskunftsdatei" (PFAD)

Das Innenministerium hat mir mit Schreiben vom 20.7.1995 die oben genannte Errichtungsanordnung, die seit 1.1.1996 bei den Dienststellen der Bayerischen Polizei Anwendung findet, übersandt. Die Datei PFAD ist als **landesweite** Datei zentraler Bestandteil des **Informationssystems der Bayerischen Polizei (IBP)**.

Die bisherigen **separaten Errichtungsanordnungen** für landesweite **Einzeldateien**

- Personenfahndung
- Sachfahndung
- Erkennungsdienst
- Personenbeschreibung
- Haft
- Kriminalaktennachweis und
- Polizeiliche Kriminalstatistik

werden in PFAD **zusammengefaßt** und mit dem Begriff **"Bereich"** als eigene Anwendung kenntlich gemacht. Den Regelungen zu PFAD wurden in der gemeinsamen Errichtungsanordnung die Regelungen zur PSV vorangestellt.

Gegen die Konzeption der Errichtungsanordnung, insbesondere die Zusammenfassung bisher selbständiger Dateien, habe ich **keine** grundsätzlichen datenschutzrechtlichen Bedenken, da sich Speicherungsumfang und -dauer sowie der Kreis der Zugriffsberechtigten dadurch nicht erweitern. Die Zusammenfassung führt auch nicht zu einer Erweiterung der Abfragemöglichkeiten. Geplant ist allerdings die Einrichtung einer landesweiten Recherche bei Straftaten mit bekanntem und unbekanntem Täter. Recherchen in polizeilichen Dateien anhand von personenbezogenen Daten (z.B. Personenmerkmale, Tatbegehungsweise), die der Polizei im konkreten Fall bekannt geworden sind, halte ich grundsätzlich für datenschutzrechtlich zulässig. Welche datenschutzrechtlichen Anforderungen an das Verfahren im einzelnen zu stellen sind, etwa wegen einer evtl. Nähe zur Rasterfahndung, kann ich erst nach genauer Kenntnis der geplanten Maß-

nahme beurteilen.

Im einzelnen habe ich das Innenministerium aber insbesondere zu folgenden Punkten um Stellungnahme gebeten:

- Die Errichtungsanordnung für PFAD sieht unter der Rubrik "Grunddaten" die Speicherung der **"Volkszugehörigkeit"** vor. Auch wenn es sich bei dem Datum "Volkszugehörigkeit" um kein Pflichtdatum handelt, so ist seine Verwendung - zumindest in der hier vorliegenden allgemeinen Form ohne Hinweis auf die Notwendigkeit der besonderen Prüfung der Erforderlichkeit im Einzelfall - aus datenschutzrechtlicher Sicht **problematisch**.

- Das Datum **"Lebenslauf"** ist nunmehr zur Speicherung unter der Rubrik "Personenbeschreibung" vorgesehen. Das Innenministerium hat mir auf Anfrage mitgeteilt, daß in der Datei lediglich die Tatsache der Erstellung, nicht aber auch der Inhalt des Lebenslaufs gespeichert werden soll. Der Betroffene sollte in schriftlicher Form auf die Freiwilligkeit der Erstellung eines Lebenslaufes hingewiesen werden.

- Nach der Errichtungsanordnung PFAD ist die weitere Speicherung einer zunächst in der Eigenschaft als Beschuldigter/Tatverdächtiger/Betroffener gespeicherten Person auch nach Wegfall dieser Eigenschaft zulässig, wenn dies für Zwecke der Vorgangsverwaltung/**Sachbearbeitung** weiterhin erforderlich erscheint. In solchen Fällen sind die Personalien im Datenblock "Beschuldigter" zu löschen und in den Datenblock "Zeugen" mit der Kennung "E" (Ermittlungsdaten) zu übernehmen.

  Diese Verfahrensweise trägt meines Erachtens den gesetzlichen Vorgaben (Löschung der personenbezogenen Daten, wenn der zugrundeliegende Tatverdacht entfallen ist) **nicht ausreichend Rechnung**, da die Vergabe von Z-Personalien mit der zusätzlichen Kennung "E" die **frühere** Beschuldigteneigenschaft weiter erkennen läßt, da die zusätzliche Kennung nur für diesen Personenkreis vergeben wird.

5.8 Prüfung der Erforderlichkeit von erkennungsdienstlichen Behandlungen durch die Polizei

Anläßlich meiner datenschutzrechtlichen Prüfung beim Polizeipräsidium München habe ich auch die Erforderlichkeit einzelner erkennungsdienstlicher Behandlungen geprüft. Die Polizei hat in diesem Zusammenhang die Auffassung vertreten, daß sich meine Kontrollbefugnis nur auf die Einhaltung der formalen Regelungen über die Art und Weise der Erhebung beziehe. Die Befugnisnormen im Polizeiaufgabengesetz und in der Strafprozeßordnung seien keine datenschutzrechtlichen Vorschriften, sondern die Rechtsgrundlage für die Maßnahmen der Polizei. Es obliege den Gerichten, die Rechtmäßigkeit von polizeilichen Maßnahmen zu überprüfen. Eine Verletzung datenschutzrechtlicher Vorschriften käme dagegen in Betracht, wenn unzulässige Erhebungsmethoden angewandt oder wenn personenbezogene Daten vermeidbar an Unberechtigte preisgegeben wurden.

Dieser einschränkenden Auffassung zum Umfang meiner Kontrollkompetenz bin ich entgegengetreten. Gemäß Art. 30 Abs. 1 Satz 1 Bayerisches Datenschutzgesetz (BayDSG) ist es meine Aufgabe, bei den öffentlichen Stellen die Einhaltung der Vorschriften über den Datenschutz zu kontrollieren. § 81 b Strafprozeßordnung bzw. Art. 14 Bayerisches Polizeiaufgabengesetz sind Normen, die die Zulässigkeit erkennungsdienstlicher Maßnahmen und damit die Voraussetzungen der Erhebung personenbezogener Daten regeln. Sie eröffnen nicht nur die Möglichkeit der erkennungsdienstlichen Behandlung, sondern legen auch die Grenzen für die Durchführung der Maßnahme fest. Sie zählen deshalb zu den Vorschriften des Datenschutzes. Auf ihrer Grundlage kann von mir geprüft werden, ob die Voraussetzungen für die erkennungsdienstliche Behandlung vorlagen und ob die weitere Speicherung der dabei gewonnenen Informationen und Unterlagen zulässig ist (vgl. auch Nr. 5.12). Meine Kontrollbefugnis besteht unabhängig von der Möglichkeit des Betroffenen, derartige Maßnahmen im Wege verwaltungsgerichtlicher oder strafprozessualer Rechtsmittel überprüfen zu lassen. Nach Art. 30 Abs. 4 Satz 1 BayDSG ist meine Prüfkompetenz lediglich insoweit eingeschränkt, als ich die Erhebung personenbezogener Daten der Strafverfolgungsbehörden bei der Verfolgung von Straftaten erst nach Abschluß des Strafverfahrens kontrollieren kann. Wurde die Datenerhebung der Strafverfolgungsbehörden gerichtlich überprüft, findet eine weitere Kontrolle gemäß Art. 30 Abs. 4 Satz 2 BayDSG nicht statt. Auch daraus läßt sich ableiten, daß allein die Möglichkeit des Betroffenen, verwaltungsgerichtliche oder strafprozessuale Rechtsmittel gegen eine Maßnahme zu ergreifen, meine Kontrollkompe-

tenz nicht tangiert.

Das Innenministerium hat sich meiner Rechtsauffassung ausdrücklich angeschlossen und gegenüber die Polizei darauf hingewiesen, daß die Frage der Erforderlichkeit einer erkennungsdienstlichen Behandlung einen spezifischen datenschutzrechtlichen Bezug hat und von mir in vollem Umfang überprüft werden kann.

5.9 Videoaufnahmen der Polizei bei Versammlungen/Veranstaltungen

5.9.1 Anfertigung von Bild- und Tonaufnahmen von Teilnehmern öffentlicher Versammlungen

In meinem 16. Tätigkeitsbericht (Nr. 5.15) habe ich, ausgelöst durch eine Bürgerbeschwerde, zu der Frage Stellung genommen, unter welchen Voraussetzungen die Polizei bei Versammlungen Bild- und Tonaufnahmen anfertigen darf.

Das Innenministerium hatte die Auffassung vertreten, daß das rein vorsorgliche Aufnehmen von Teilnehmern auch friedlicher Versammlungen auf Video rechtlich zulässig sei, wenn die Polizei Anhaltspunkte für bevorstehende Störungen habe, aber nicht feststellbar sei, von welchen Teilnehmern im einzelnen Störungen zu erwarten sind. Bei dieser Fallgestaltung könne die Polizei jeden Teilnehmer der Versammlung filmen. Aus polizeitaktischen Gründen könne auf diese Verfahrensweise nicht verzichtet werden.

Ich habe in mehreren Gesprächen mit dem Innenministerium und Herrn Staatsminister Dr. Beckstein nachhaltig darauf hingewiesen, daß ich diese Auffassung für unvereinbar mit § 12 a Versammlungsgesetz halte. Nach dem eindeutigen Gesetzeswortlaut dürfen Bild- und Tonaufzeichnungen nur von solchen Teilnehmern einer Versammlung angefertigt werden, bei denen tatsächliche Anhaltspunkte die Annahme rechtfertigen, daß **von ihnen** erhebliche Gefahren für die öffentliche Sicherheit und Ordnung ausgehen.

Im einzelnen bedeutet dies:

Kommt die Polizei aufgrund einer umfassenden Einzelfallprüfung zu der Erkenntnis, daß im Zusammenhang mit der geplanten Versammlung erhebliche Gefahren für die öffentliche Sicherheit und Ordnung bevorstehen, sind nach meiner Auffassung folgende Fallkonstellationen zu unterscheiden:

Können einzelne Personen als potentielle Störer identifziert werden, dürfen von diesen Personen Bild- und Tonaufnahmen gemacht werden, sofern nicht ohnehin weitergehende polizeiliche Maßnahmen zur Abwehr der prognostizierten Gefahr erforderlich sind.

Bei Veranstaltungen **homogener Gruppierungen** kann je nach den Umständen die Annahme gerechtfertigt sein, daß **von allen Teilnehmern eine erhebliche Gefahr** ausgeht. Die Annahme einer homogenen Gruppe kann sich auf Erkenntnisse über die Versammlungsteilnehmer, das Thema bzw. Ziel der Veranstaltung und die Person des Veranstalters stützen. Bei solchen Gruppen ist dann eine individualisierte Gefahrenprognose als Voraussetzung für die Anfertigung von Bild- und Tonaufnahmen nicht erforderlich.

Anders zu beurteilen sind jedoch die Vielzahl von **heterogen zusammengesetzten** Veranstaltungen, an denen neben friedlichen Teilnehmern nach Erkenntnissen der Polizei auch nicht identifizierte gewaltbereite Personen teilnehmen. Art. 8 Grundgesetz schützt die personenbezogenen Daten des Betroffenen bei der Vorbereitung von Demonstrationen und Versammlungen und während ihrer Durchführung vor staatlicher Ausspähung. Derjenige, der sich im Rahmen des Schutzbereiches des Art. 8 Grundgesetz friedlich versammelt, muß nicht dulden, daß er bei Ausübung seines Grundrechts auf Versammlungs- und Demonstrationsfreiheit gefilmt wird. Wer damit rechnen muß, daß er als Versammlungsteilnehmer behördlich registriert wird, wird möglicherweise auf die Ausübung seines Grundrechts ganz verzichten. Die Polizei ist vielmehr gehalten, durch Ergreifung sonstiger zulässiger Maßnahmen (z.B. verstärkte Kontrollen nach Waffen oder gefährlichen Gegenständen, erhöhter Personaleinsatz etc.) die friedlichen Versammlungsteilnehmer vor Störungen durch radikale Personen oder Gruppierungen zu schützen.

Die Anfertigung von Bild- und Tonaufnahmen auch der friedlichen Teilnehmer solcher Versammlungen ist nicht von § 12 a Versammlungsgesetz gedeckt.

Keine durchgreifenden Bedenken habe ich gegen den Einsatz von Kameras zur Bildübertragung **ohne Aufzeichnung des Geschehensablaufs auf einen Datenträger** zum Zwecke der Einsatzleitung. Einer solchen Vorgehensweise steht § 12 a Versammlungsgesetz nicht entgegen, da keine Bild- und Tonaufnahmen gefertigt werden. Insoweit ist der Einsatz einer Videokamera vergleichbar mit der Verwendung sonstiger "technischer Sehhilfen" wie z.B. Ferngläsern. Allerdings ist darauf hinzuweisen, daß die gezielte Beobachtung einzelner Versammlungsteilnehmer - sei es mit Hilfe von Videokameras oder mit Hilfe sonstiger technischer Geräte - ebenfalls die Versammlungsfreiheit nach Art. 8 Grundgesetz tangieren kann. Einzelne Demonstranten dürfen nur dann gezielt beobachtet werden, wenn man aufgrund ihres Verhaltens oder aufgrund sonsti-

ger Erkenntnisse mit Störungen durch diese Teilnehmer rechnen muß und wenn eine solche Beobachtung unter Berücksichtigung des Grundrechts der Versammlungsfreiheit zur Abwehr der bevorstehenden Störung der öffentlichen Sicherheit und Ordnung erforderlich und verhältnismäßig ist.

Um vor Ort einen Eindruck über die praktischen Probleme zu erhalten, habe ich den polizeilichen Einsatz bei einer Versammlung verfolgt. Hierbei hat sich gezeigt, daß die von mir aufgezeigten Schranken des § 12 Versammlungsgesetz auch unter Berücksichtigung der polizeitaktischen Erfordernisse durchaus eingehalten werden können.

Das Innenministerium hat sich nunmehr grundsätzlich meiner Auffassung angeschlossen. Es hat die nachgeordneten Polizeidienststellen angewiesen, in Zukunft die von mir geforderten Vorgaben bei der Anfertigung von Bild- und Tonaufnahmen von Teilnehmern öffentlicher Versammlungen zu beachten.

5.9.2 Videoaufzeichnungen der Polizei bei der Feststellung der Personalien von Fußballfans anläßlich eines Fußballspiels

Aufgrund einer Eingabe habe ich von folgendem Sachverhalt Kenntnis erlangt:

Die Polizei hat anläßlich eines Fußballspiels die Personalien von Fußballfans, die aus einer bestimmten Gegend angereist waren, festgestellt. Hierzu hat die Polizei die Namen und die Anschrift der kontrollierten Personen aus den Ausweispapieren vorgelesen und gleichzeitig Videoaufzeichnungen von den Betroffenen gefertigt. Anlaß für die polizeiliche Maßnahme waren Hinweise, daß zu dem Fußballspiel mit der Anreise von ca. 150 gewaltbereiten und 20 gewaltsuchenden Fans zu rechnen war. Bereits in der vorangegangenen Saison hatten bei einem Fußballspiel Fans einer bestimmten Mannschaft aus dem Schutz der Menge heraus Straftaten verübt.

Aus datenschutzrechtlicher Sicht beurteile ich das Vorgehen der Polizei wie folgt:

Unter den gegebenen Umständen lagen zwar die gesetzlichen Voraussetzungen nach Art. 13 Abs. 1 Ziff. 1 Polizeiaufgabengesetz (PAG) für eine Identitätsfeststellung zur Gefahrenabwehr vor. Dagegen war die Polizei nicht befugt, von der Identitätsfeststellung Videoaufzeichnungen zu fertigen, soweit die davon betroffenen Personen Ausweispapiere bei sich führten. Bei diesen Personen konnte die Identität bereits anhand ihrer Papiere festgestellt werden.

Nach Art. 14 Abs. 3 Ziff. 2 PAG zählt die Aufnahme von Lichtbildern von einer Person durch die Polizei zu den **erkennungsdienstlichen Maßnahmen**. Für die Qualifizierung einer polizeilichen Maßnahme als erkennungsdienstliche Maßnahme ist es nicht erforderlich, daß die Polizei alle in Art. 14 Abs. 3 PAG genannten Maßnahmen (z.B. auch Abnahme von Fingerabdrücken) durchgeführt hat. Zu den erkennungsdienstlichen Maßnahmen zählen vielmehr alle Feststellungen über Merkmale des äußeren Erscheinungsbildes einer **bestimmten Person, die ihre Wiedererkennung ermöglichen**, also auch Videoaufnahmen einer Person. Zum Zwecke der Gefahrenabwehr kann die Polizei nach Art. 14 Abs. 1 Nr. 1 PAG nur dann erkennungsdienstliche Maßnahmen bei einer Person vornehmen, **wenn** eine nach Art. 13 PAG zulässige Identitätsfeststellung auf andere Weise nicht oder nur unter erheblichen Schwierigkeiten möglich ist.

Zwar kann die Polizei auch von den **für eine Gefahr Verantwortlichen** bei oder im Zusammenhang mit öffentlichen Veranstaltungen oder Ansammlungen Bild- und Tonaufnahmen anfertigen, wenn tatsächliche Anhaltspunkte die Annahme rechtfertigen, daß **dabei** Ordnungswidrigkeiten von erheblicher Bedeutung oder Straftaten begangen werden (Art. 32 Abs. 1 PAG). Diese Vorschrift ermächtigt die Polizei, **einen Geschehensablauf** auf Video aufzuzeichnen, der sich nach den polizeilichen Erkenntnissen zu einer Störung der öffentlichen Sicherheit und Ordnung entwickeln könnte (z.B. Fan-Kurven eines Fußballstadions). Kommt es im Verlauf einer Veranstaltung oder Ansammlung dann zu Ausschreitungen, dient die Videoaufzeichnung als Beweismittel zur Dokumentation der Situation und erleichtert die Feststellung von Straftatenverdächtigen.

Im vorliegenden Fall hatte die Polizei aber nicht eine gefahrenträchtige Situation gefilmt, sondern gezielt einzelne Personen auf Video aufgezeichnet und **gleichzeitig deren Personalien festgehalten**. Ebensogut hätte die Polizei die kontrollierten Personen fotografieren und die Fotos anschließend mit den Personalien der Betroffenen versehen können. Bei dieser Sachlage können die Videoaufzeichnungen nicht als Datenerhebung nach Art. 32 PAG, sondern nur als Identitätsfeststellung verbunden mit einer erkennungsdienstlichen Maßnahme (Aufnahme von Bildern) eingestuft werden. Die polizeiliche Maßnahme habe ich deshalb **förmlich beanstandet**.

5.10 Polizeiliches Formblatt "Einwilligung zur Weitergabe personenbezogener Daten"

Die bayerische Polizei verwendet in strafrechtlichen Ermittlungsverfahren seit längerem Formblätter, mit denen Beschuldigte oder Zeugen ihre Einwilligung zur Weitergabe ihrer personenbezogenen Daten durch einzelne oder mehrere der dort aufgelisteten Personen, Behörden oder Stellen an die Polizei oder Staatsanwaltschaft erklären können. Berufsgeheimnisträger (z.B. Arzt, Rechtsanwalt) sollen damit von ihrer gesetzlichen Schweigepflicht entbunden werden, Sozialbehörden und Finanzämter insoweit vom Sozialgeheimnis und vom Steuergeheimnis befreit werden. Auf der Grundlage der Erklärung soll die Polizei ohne die wegen ihrer besonderen Schutzbedürftigkeit vom Gesetz vorgesehenen Einschränkungen personenbezogene Auskünfte erhalten können.

Ich habe das Staatsministerium des Innern auf die **grundsätzlichen Bedenken gegen eine formularmäßig erklärte Einwilligung zur Weitergabe personenbezogener Daten im Ermittlungsverfahren, insbesondere durch den Beschuldigten**, hingewiesen und Änderungen des Formblattes gefordert.

Auf meine Anregung hin hat das Staatsministerium des Innern das polizeiliche Formblatt überarbeitet und in folgenden Punkten meinen datenschutzrechtlichen Forderungen Rechnung getragen:

- Der Unterzeichner des Formblattes ermächtigt nicht mehr pauschal 13 verschiedene Behörden oder Institutionen, Auskunft über seine personenbezogenen Daten zu erteilen. Die Behörde oder Stelle, die von der Schweigepflicht befreit wird, muß nunmehr genau bezeichnet und durch Unterstreichen gekennzeichnet werden.

- In das Formblatt wurde ein Hinweis aufgenommen, daß für jede Stelle, die von der Schweigepflicht entbunden wird, ein gesondertes Formblatt zu verwenden ist. Dadurch wird der Gefahr einer unzulässigen Datenübermittlung entgegengewirkt. Die Polizei kann nunmehr eine Kopie der Einverständniserklärung des Betroffenen an die von der Schweigepflicht entbundene Stelle übersenden, ohne daß diese erfährt, welche weiteren Stellen der Betroffene von der Schweigepflicht entbunden hat.

- Das Formblatt enthält nunmehr einen eigenen Abschnitt zur Festlegung des sachlichen und zeitlichen Umfangs der zu erteilenden Auskunft. Sowohl für den Betroffenen als auch für die von der Schweigepflicht entbundene Stelle ist dadurch konkret und individuell auf den Einzelfall bezogen erkennbar, welche personenbezogenen Daten gegenüber den Ermittlungsbehörden offenbart werden dürfen.

- Die Hinweise auf die Datenschutzbestimmungen heben nunmehr die Freiwilligkeit der Abgabe der Einwilligungserklärung besonders hervor.

Das überarbeitete polizeiliche Formblatt zur Erteilung einer Einwilligung zur Weitergabe personenbezogener Daten im Ermittlungsverfahren wird den datenschutzrechtlichen Anforderungen wesentlich besser gerecht. Allerdings sind die "Datenschutzhinweise" im Formblatt nach meiner Auffassung nach wie vor nicht geeignet, den Betroffenen hinreichend darüber aufzuklären, daß ohne sein Einverständnis eine Datenerhebung bei Geheimnisträgern durch die Ermittlungsbehörden häufig durch gesetzliche Regelungen ausgeschlossen oder zumindest erheblich eingeschränkt wird. Der Hinweis in dem Formular, daß die genannten Behörden und Geheimnisträger ohne Einwilligung des Betroffenen nur unter den in verschiedenen Gesetzen näher bestimmten Voraussetzungen zur Auskunft an die Polizei, Staatsanwaltschaft oder Gerichte berechtigt oder verpflichtet sind, reicht nicht aus. Das gilt insbesondere dann, wenn im folgenden darauf hingewiesen wird, daß die Polizei bei Abgabe der Einwilligungserklärung in der Regel nicht gezwungen sei, die erforderlichen Daten durch Vernehmung von Nachbarn, Bekannten oder Freunden zu erheben und auf die Einholung gerichtlicher Anordnungen verzichtet werden könne.

Im übrigen fehlt der Hinweis auf die Möglichkeit des Widerrufs der Einwilligung.

Das Innenministerium hat eine weitere Nachbesserung des Formblattes leider abgelehnt.

5.11 Paßeintragungen "Homo-Szene" und "Homo-Strich" bei polizeilichen Kontrollen

Wie in mehreren Tageszeitungen berichtet wurde, haben Polizeibeamte bei der Kontrolle zweier Ausländer die Tatsache der polizeilichen Kontrolle, die Kontrollzeitpunkte sowie Zusatzvermerke "Homo-Szene" und "Homo-Strich" in die Pässe eingetragen. Auf meine Anfage hat die Polizei mitgeteilt, daß die betreffenden Beamten in sechs bis sieben Fällen vergleichbare Eintragungen in die Ausweise kontrollierter Ausländer vorgenommen haben.

Ich habe die Polizei darauf hingewiesen, daß die Eintragungen über eine polizeiliche Kontrolle sowie über die Tatsache, daß die Betroffenen im homosexuellen Milieu angetroffen wurden, in die Ausweise der Betroffenen als Speicherung personenbezogener Daten zu qualifizieren ist. Weder das Polizeiaufgabengesetz noch andere Rechtsvorschriften enthalten eine Rechtsgrundlage für die Speicherung der Vermerke "HomoSzene" oder "Homo-Strich". Die Eintragung dieser Vermerke in die Ausweise kontrollierter Ausländer durch die Polizei war somit rechtswidrig und wurde von mir beanstandet.

5.12 Datenschutzrechtliche Kontrolle bei der Erhebung personenbezogener Daten durch Strafverfolgungsbehörden (Verhältnis Datenschutzkontrolle/Dienstaufsicht)

In meinem 16. Tätigkeitsbericht habe ich berichtet, daß zum Umfang meiner Kontrollkompetenz im Bereich der Staatsanwaltschaft unterschiedliche Auffassungen festzustellen waren (siehe Nr. 7.3.1 des 16. Tätigkeitsberichts).

Ich habe dies zum Anlaß genommen, mich grundsätzlich mit der Frage auseinanderzusetzen, ob und ggf. in welchem Umfang die Strafverfolgungsbehörden bei strafrechtlichen Erhebungsmaßnahmen einer datenschutzrechtlichen Kontrolle unterworfen sind und in welchem Verhältnis die Datenschutzkontrolle zur Dienstaufsicht steht.

1. Verhältnis Datenschutz/allgemeine Dienstaufsicht

Meiner Prüfung unterliegt nur die Einhaltung der **datenschutzrechtlichen Vorschriften**. Die Normen der Strafprozeßordnung zur Datenerhebung bei strafrechtlichen Ermittlungen sind einerseits Befugnisnormen, die festlegen, unter welchen Voraussetzungen der Betroffene Eingriffe in seine Privatsphäre zum Zwecke der Aufklärung von Straftaten dulden muß. Andererseits schützen sie den einzelnen vor einer unzulässigen Beeinträchtigung seines Rechtes auf informationelle Selbstbestimmung durch die Erhebung personenbezogener Daten, indem sie die Grenzen staatlicher Eingriffsbefugnisse normieren. Es handelt sich damit um typische Vorschriften über den Datenschutz im Sinne von Art. 30 Abs. 1 BayDSG, deren Einhaltung ich grundsätzlich in vollem Umfang überprüfen kann. Die Einhaltung datenschutzrechtlicher Vorschriften kann unabhängig davon auch von der Dienstaufsicht überprüft werden.

Von der Dienstaufsicht unterscheidet sich die Datenschutzkontrolle hinsichtlich des **Kontrollumfangs** in folgenden wesentlichen Punkten:

Die Datenschutzkontrolle ist eine Rechtmäßigkeitskontrolle. Sie entspricht der Kontrolle durch die Verwaltungsgerichte. Ermessensentscheidungen, Beurteilungsspielräume und

Prognosen sind zu akzeptieren, wenn sie vertretbar sind. Die Auslegung von unbestimmten Rechtsbegriffen kann dagegen in vollem Umfang nachgeprüft werden.

Liegen die gesetzlichen Voraussetzungen für eine Datenerhebung nicht vor oder handelt die Strafverfolgungsbehörde nicht mehr im Rahmen des ihr eingeräumten Beurteilungsspielraums bzw. Ermessens, kann der Datenschutzbeauftragte die Datenerhebung beanstanden. Bei folgenden Fallgruppen werden beispielsweise die Grenzen der zulässigen Datenerhebung überschritten:

- Die Ermittlungsbehörden mißachten spezifische Datenerhebungs- oder Verwertungsverbote, wie z.B.
-
  - durch Beschlagnahme von Gegenständen, die nach § 97 StPO beschlagnahmefrei sind oder
  - durch Erholung von Auskünften bei Behörden unter Umgehung der Steuer- und Sozialgeheimnisse,

- Zeugen/Beschuldigte werden ohne Belehrung über ihr Zeugnis-/Aussageverweigerungsrecht vernommen,
- der Vollzug der Maßnahme hält sich nicht an den durch Beschluß des Gerichts vorgegebenen Rahmen (z.B. Überwachung eines nicht im Beschluß bezeichneten Telefonanschlusses),
- aufgrund der Intensität des Grundrechtseingriffs wäre für eine Maßnahme eine spezielle Befugnisnorm erforderlich, die jedoch nicht existiert.

2. Verhältnis Datenschutzkontrolle / Gerichtliche Kontrolle

Eine wesentliche Beschränkung der datenschutzrechtlichen Kontrolle bei strafverfolgenden Datenerhebungen folgt aus dem Grundsatz, daß bereits richterlich überprüfte Erhebungsmaßnahmen nicht mehr datenschutzrechtlich geprüft werden können (Art. 30 Abs. 4 Satz 2 BayDSG). Hierzu zählen Maßnahmen, die gerichtlich angeordnet wurden oder deren Rechtmäßigkeit gerichtlich im Wege einer Beschwerde oder inzident im Rahmen

des Strafverfahrens bei der Frage der Verwertbarkeit der gewonnenen Beweise überprüft wurde.

Eine Reihe von Datenerhebungsmaßnahmen der Strafverfolgungsbehörden werden jedoch weder gerichtlich angeordnet (z.B. unaufschiebbare Ermittlungen bei Gefahr im Verzug) noch im Verlauf eines Verfahrens gerichtlich überprüft. So stellt die Staatsanwaltschaft in der Praxis eine Vielzahl von Verfahren mangels hinreichendem Tatverdachts nach § 170 StPO ein, ohne daß ein Gericht über die Rechtmäßigkeit einer polizeilichen oder staatsanwaltschaftlichen Maßnahme entscheidet. In diesem Fall kann ich nach Abschluß des Strafverfahrens im Rahmen des Art. 30 Abs. 1 Satz 2 BayDSG in vollem Umfang überprüfen, ob die Strafverfolgungsbehörden im Ermittlungsverfahren die gesetzlichen Beschränkungen bei der Datenerhebung eingehalten haben.

Unerheblich für das Bestehen meiner Kontrollkompetenz ist, ob eine Maßnahme gerichtlich überprüft werden kann. Eine datenschutzrechtliche Kontrolle ist nur ausgeschlossen, wenn und soweit über die Rechtmäßigkeit einer Maßnahme gerichtlich entschieden wurde. Aber auch in diesen Fällen kann datenschutzrechtlich überprüft werden, ob beim Vollzug der Maßnahme die gesetzlichen und gerichtlichen Vorgaben gewahrt wurden, etwa ob die Polizei bei einer Durchsuchung Unterlagen beschlagnahmt hat, die im gerichtlichen Beschluß nicht aufgeführt waren.

Das Staatsministerium der Justiz, dem ich meine Überlegungen mitgeteilt habe, hat sich dazu noch nicht geäußert.

5.13 Gesetz zur Änderung polizeirechtlicher Vorschriften - Erfolgskontrolle bei verdachtsunabhängigen polizeilichen Kontrollen

Am 01.01.1995 wurde durch das Gesetz zur Änderung polizeirechtlicher Vorschriften u.a. Art. 13 Abs. 1 Nr. 5 Polizeiaufgabengesetz (PAG) geändert. Danach besteht nunmehr die Möglichkeit verdachtsunabhängiger polizeilicher Personenkontrollen im Grenzgebiet bis zu einer Tiefe von 30 km sowie auf Durchgangsstraßen (Bundesautobahn, Europastraßen und an deren Straßen von erheblicher Bedeutung für den grenzüberschreitenden Verkehr) und in öffentlichen Einrichtungen des internationalen Verkehrs zur Verhütung oder Unterbindung der unerlaubten Überschreitung der Landesgrenze oder des unerlaubten Aufenthalts und zur Bekämpfung der grenzüberschreitenden Kriminalität.

Die gesetzliche Regelung, die als Ausgleich für den Wegfall der bisherigen Kontrollmöglichkeiten an den Binnengrenzen geschaffen wurde, erweitert Eingriffsmöglichkeiten der Polizei in erheblichem Umfang. Während bislang verdachtsunabhängige Identitätsfeststellungen nach Art. 13 Abs. 1 Nr. 5 PAG auf die Bekämpfung unerlaubter Grenzübertritte und auf den Grenzbereich sowie auf Flugplätze beschränkt waren, kann diese polizeiliche Maßnahme nunmehr auf große Teile des Straßennetzes des gesamten Staatsgebietes ausgeweitet, auf sämtliche Anlagen des internationalen Verkehrs, also auch auf entsprechende Bahnhöfe und Verkehrsmittel erstreckt und allgemein auf die Bekämpfung der grenzüberschreitenden Kriminalität ausgedehnt werden.

Ich habe gegenüber dem Innenministerium darauf hingewiesen, daß gerade bei einer polizeilichen Befugnis, die sich hinsichtlich ihrer Voraussetzungen grundlegend von den bisherigen Befugnissen der Art. 13, 21, 22 PAG zur Identitätsfeststellung und zur Durchsuchung von Personen und Sachen unterscheidet, und die vor dem Hintergrund "rasch angewachsener, international verflochtener Kriminalität" gefordert wurde, die Erfahrungen, die bei ihrer Anwendung gemacht wurden, erfaßt, bewertet und dargestellt werden sollten. Eine solche Erfolgskontrolle, die insbesondere Zahl und Ort der getroffenen Maßnahmen sowie ihre Ergebnisse (Erfolge) beinhalten sollte, ist für die Beurteilung dieser zusätzlichen polizeilichen Eingriffsbefugnis von erheblicher Bedeutung.

Ich habe deshalb angeregt, eine begleitende Erhebung und Auswertung durchzuführen.

Vom Innenministerium wurde meine Anregung einer Erfolgskontrolle verdachtsunabhängiger polizeilicher Kontrollen leider abgelehnt. Das Innenministerium hat darauf verwiesen, daß eine statistische Erfassung der Kontrolltätigkeit/-erfolge nach der neu geschaffenen Rechtsgrundlage mit einem unvertretbar hohen zusätzlichen Arbeitsaufwand verbunden sei. Davon abgesehen könne die Notwendigkeit und Wirksamkeit polizeilicher Befugnisse nicht in einer "Erfolgsstatistik" erfaßt werden. Fraglich sei bereits, wie man den Begriff "Erfolg" definiere. Die verdachtsunabhängige Personenkontrolle sei außerdem keine isolierte Befugnis. Regelmäßig seien weitere Ermittlungshandlungen zur Sachverhaltsaufklärung nötig, so daß sich die Frage der Zurechnung eines "Erfolgs" stellen würde. Im übrigen würden die bislang vorgelegten Tätigkeitsberichte der Fahndungs- und Kontrollgruppen ausreichend die Erforderlichkeit der neu geschaffenen polizeilichen Eingriffsbefugnis dokumentieren.

Die Argumentation des Innenministeriums zur Problematik einer Definition des Erfolges einer polizeilichen Maßnahme und der Zuordnung der Erfolge zu konkreten polizeilichen Maßnahmen halte ich nicht für stichhaltig. Gerade bei verdachtsunabhängigen polizeilichen Kontrollen sollte es möglich sein, die Zahl der durchgeführten polizeilichen Kontrollen (getrennt nach Bundesautobahn, Europastraßen und anderen Straßen) der Zahl der Fälle gegenüberzustellen, bei denen Anhaltspunkte für **grenzüberschreitende Kriminalität** weitere polizeiliche Maßnahmen notwendig gemacht haben. Hierzu enthalten die allgemeinen Berichte der Polizei zu verdachtsunabhängigen Identitätskontrollen nicht die erforderlichen Informationen.

Ich werde weiterhin aufmerksam beobachten, wie sich der Vollzug des Gesetzes in der Praxis gestaltet und ggf. auf meine Forderungen zurückkommen.

5.14 Gesetzentwürfe zur Einführung der akustischen Wohnraumüberwachung (Lauschangriff)

Zur Zeit wird innerhalb der Bundesregierung eine Verfassungsänderung mit einem Gesetzentwurf diskutiert, der die akustische Überwachung von Wohn- und Geschäftsräumen zum Zweck der Beweismittelgewinnung im Strafverfahren (sog. Großer Lauschangriff) vorsieht. Eine solche Änderung des Art. 13 Grundgesetz und der dazugehörigen gesetzlichen Regelungen würde einen erheblichen Eingriff in das Persönlichkeitsrecht des Einzelnen darstellen, der von der Mehrheit der Datenschutzbeauftragten aus grundsätzlichen Erwägungen abgelehnt wird. Sollten die Pläne der Bundesregierung zur Einführung des Großen Lauschangriffs trotzdem weiterverfolgt werden, erfordert der Schutz der Privatsphäre eine klare Begrenzung und verfahrensmäßige Sicherung der Maßnahme. Solche Beschränkungen und Sicherungen sollten vom Grundsatz her im Grundgesetz selbst und nicht erst im ausführenden Gesetz festgelegt sein.

Bereits im Vorfeld der endgültigen Entscheidungsfindung auf Bundes- und Länderebene habe ich - in Übereinstimmung mit der Konferenz der Datenschutzbeauftragten - für den Fall einer derartigen Regelung in einem Schreiben an den Bayerischen Ministerpräsidenten die Berücksichtigung folgender Punkte gefordert:

1. Im Grundgesetz selbst ist festzulegen,

   - daß der Einsatz technischer Mittel zur Wohnraumüberwachung nur zur Verfolgung schwerster Straftaten, die im Hinblick auf ihre Begehungsform oder Folgen die Rechtsordnung nachhaltig gefährden und die im Gesetz einzeln bestimmt sind und

   - nur auf Anordnung eines Kollegialgerichts erfolgen darf.

2. Die Maßnahme darf sich nur gegen den Beschuldigten richten. Erfolgt ein Lauschangriff in der Wohnung eines Dritten, müssen konkrete Anhaltspunkte die Annahme rechtfertigen, daß sich der Beschuldigte in der Wohnung aufhält. In allen Fällen muß die durch Tatsachen begründete Erwartung vorliegen, daß in der überwachten Wohnung zur Strafverfolgung relevante Gespräche geführt werden.

3. Das Mittel der Wohnungsüberwachung darf nur angewandt werden, wenn andere Methoden zur Erforschung des Sachverhalts erschöpft oder untauglich sind. Bei einem Lauschangriff in Wohnungen dritter Personen bedeutet dies auch, daß die Maßnahme nur durchgeführt werden darf, wenn aufgrund bestimmter Tatsachen anzunehmen ist, daß ihre Durchführung in der Wohnung des Beschuldigten allein nicht zur Erforschung des Sachverhalts oder zur Ermittlung des Aufenthaltsorts des Täters führen wird.

4. Das Zeugnisverweigerungsrecht von Berufsgeheimnisträgern und Personen, die aus persönlichen Gründen zur Verweigerung des Zeugnisses berechtigt sind, muß gewahrt werden.

5. Die Dauer der Maßnahme wird zeitlich eng begrenzt. Auch die Möglichkeit der Verlängerung der Maßnahme ist zu befristen.

6. Eine anderweitige Verwendung der erhobenen Daten (Zweckänderung) ist weder zu Beweiszwecken noch als Ermittlungsansatz für andere als Katalogtaten zulässig. Personenbezogene Erkenntnisse aus dem Lauschangriff dürfen zur Abwehr von konkreten Gefahren für gewichtige Rechtsgüter verwendet werden.

7. Wenn sich der ursprüngliche Verdacht nicht bestätigt, sind die durch den Lauschangriff erhobenen Daten unverzüglich zu löschen.

8. Die Betroffenen müssen unverzüglich und vollständig über die Durchführung der Maßnahme informiert werden, sobald dies ohne Gefährdung des Ermittlungsverfahrens möglich ist.

9. Eine Verfahrenssicherung durch den Zwang zur eingehenden Begründung und detaillierte jährliche Berichtspflichten der Staatsanwaltschaft für die Öffentlichkeit ähnlich den gerichtlichen Wire-Tap-Reports in den USA einschließlich einer Erfolgskontrolle ist vorzusehen. Anhand der Berichte ist jeweils - wegen der Schwere des Eingriffs - in entsprechenden Fristen zu überprüfen, ob die gesetzliche Regelung weiterhin erforderlich ist.

10. Die effektive Kontrolle der Abhörmaßnahmen und der Verarbeitung und Nutzung der durch sie gewonnenen Erkenntnisse durch Gerichte und Datenschutzbeauftragte ist sicherzustellen.

Das Gesetzesvorhaben war bei Redaktionsschluß noch nicht abgeschlossen.

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

Der von der Bundesregierung vorgelegte Entwurf eines Gesetzes über das Bundeskriminalamt und die Zusammenarbeit des Bundes und der Länder in kriminalpolizeilichen Angelegenheiten (Bundeskriminalamtgesetz - BKAG) wurde zwischenzeitlich in den Bundesratsausschüssen und im Plenum des Bundesrates beraten. Es liegt nunmehr ein überarbeiteter Regierungsentwurf vor (Bundestags-Drucksache 13/1550).

Aus der Sicht des Datenschutzes ist es zu begrüßen, daß die seit langem überfälligen bereichsspezifischen Regelungen zur bundesweiten polizeilichen Datenverarbeitung, insbesondere im polizeilichen Informationssystem (INPOL) in das Gesetzgebungsverfahren eingebracht werden. Der Gesetzesentwurf enthält im Vergleich zu den Vorentwürfen eine Reihe von Vorschriften, die datenschutzrechtlich positiv zu werten sind. So dürfen nach dem aktuellen Entwurf beispielsweise personenbezogene Daten über Zeugen und mögliche Opfer nur mit **Einwilligung** des Betroffenen gespeichert werden. Die von mir in meinem 16. Tätigkeitsbericht (Nr. 5.10.3) kritisierte Möglichkeit einer flächendeckenden Speicherung ganzer Personengruppen scheidet damit aus. Aufgenommen wurden außerdem Übermittlungsverbote bei überwiegenden schutzwürdigen Interessen der Betroffenen oder bei entgegenstehenden gesetzlichen Verwendungsregelungen sowie Regelungen, die die Beachtung landesgesetzlicher Löschungsfristen sicherstellen.

Andererseits begegnet der Gesetzentwurf jedoch nach wie vor gewichtigen Bedenken, da er tiefe Eingriffe in die Rechte von Betroffenen ermöglicht, deren Voraussetzungen und Reichweite unklar oder nicht durch überwiegende Interessen der Allgemeinheit gerechtfertigt sind. Dies gilt insbesondere für folgende Punkte:

- Mehrfach wird der Begriff der "Straftaten von erheblicher Bedeutung" verwendet, ohne daß näher definiert wird, um welche Tatbestände es sich handelt. Damit ist nicht voraussehbar, wann die an diesen Begriff anknüpfenden Eingriffsbefugnisse (z.B. Verarbeitung von Daten über Kontakt- und Begleitpersonen) zur Datenverarbeitung eröffnet sind.

- Es werden dem Bundeskriminalamt als Zentralstelle Befugnisse zur selbständigen Datenerhebung und Übermittlung bis hin zum automatisierten Datenverbund mit ausländischen und zwischenstaatlichen Stellen **ohne Einvernehmen mit den** für die von ihnen gelieferten personenbezogenen Daten jeweils verantwortlichen **Länderpolizeien** eingeräumt.

- Es fehlen klare Regelungen zur Abgrenzung der Datenverarbeitungsbefugnisse im Hinblick auf die unterschiedlichen Befugnisse des Bundeskriminalamts zur Strafverfolgung, Gefahrenabwehr, Verhütung von Straftaten und Vorsorge für künftige Strafverfolgung sowie zur Zweckbindung und Zweckänderung.

- Vorgesehen ist eine Befugnis zur verdeckten Datenerhebung aus Wohnungen zum Schutz gefährdeter Ermittler, ohne die Verwendung der dabei gewonnenen personenbezogenen Daten auf diesen Zweck zu beschränken.

Hierauf haben die Datenschutzbeauftragten des Bundes und der Länder in ihrer Entschließung der 49. Konferenz hingewiesen. Sie haben darüber hinaus klare verfassungskonforme Regelungen zur Auskunftserteilung an Betroffene und der Prüfrechte von INPOL-Daten dahingehend gefordert, daß die Datenschutzkontrollrechte bei der datenschutzrechtlichen Verantwortung der Stellen anknüpfen, die die Speicherung im INPOL-System selbst vornehmen oder veranlassen.

Das Gesetzesvorhaben war bei Redaktionsschluß noch nicht abgeschlossen.

5.16 Polizeiliche Zusammenarbeit im Rahmen der Europäischen Union - Europäisches Polizeiamt (Europol)

Am 26.07.1995 haben die ständigen Vertreter der Mitgliedstaaten der Europäischen Union in Brüssel die Konvention zur Errichtung eines Europäischen Polizeiamtes (Europol) gezeichnet. Offen blieb zunächst noch die Frage möglicher Entscheidungskompetenzen des Europäischen Gerichtshofs (EuGH).

Über die Frage der Zuständigkeit des EuGH wurde auf dem Europäischen Rat in Florenz am 21./22.06.1996 Einigkeit erzielt. Die Vertragsstaaten haben sich auf eine sog. "Vorabentscheidungskompetenz" des EuGH geeinigt. Die Konvention ermöglicht dem betroffenen Bürger, Europol wegen vertraglicher oder außervertraglicher Haftungsansprüche vor den **nationalen Gerichten** zu verklagen. Hält es das nationale Gericht für erforderlich, für seine Entscheidung die Auslegung der Europol-Konvention hinsichtlich der im konkreten Fall anstehenden Frage vom EuGH klären zu lassen, ist es befugt, dem EuGH diese Frage zur Vorabentscheidung vorzulegen. Eine Klage eines Bürgers gegen Europol vor dem EuGH ist dagegen nicht vorgesehen.

Zum Inkrafttreten der Konvention bedarf es nunmehr der Ratifizierung. Dazu liegt mir ein Entwurf eines Europol-Ratifizierungs- und Ausführungsgesetzes des Bundesministeriums des Innern vor. Darin ist der aus der Sicht des Datenschutzes wichtige Grundsatz der datenschutzrechtlichen Verantwortlichkeit der Länder für die von ihnen übermittelten Daten und die Sicherstellung der Beteiligung der Landesbeauftragten an der Kontrolle der bei Europol verarbeiteten Daten nur zum Teil berücksichtigt. Ich habe deshalb gegenüber dem Staatsministerium des Innern folgende Ergänzungen gefordert:

- Übermittelt **das BKA Landesdaten** an Europol, ist ausschließlich das BKA für die Änderung, Berichtigung und Löschung von Landesdaten zuständig. Nach meiner Auffassung sollte für diesen Fall eine Regelung in den Entwurf aufgenommen werden, wonach das BKA für die Änderung, Berichtigung oder Löschung der Landesdaten zu sorgen hat, sofern hierzu aufgrund von Mitteilungen der innerstaatlich für die Daten verantwortlichen Landesbehörden gegenüber dem BKA Anlaß besteht.

- Es sollte klargestellt werden, daß sich die Zuständigkeit des Bundesbeauftragten für den Datenschutz als nationale Kontrollinstanz auf das Bundeskriminalamt als nationale Zentralstelle bezieht, die Zuständigkeiten für die Datenschutzkontrolle bei Landesbehörden, die nach dem Entwurf die datenschutzrechtliche Verantwortung tragen, aber unberührt bleiben.

- Nach § 6 Abs. 2 des Entwurfs ist vorgesehen, daß das Bundesministerium des Innern die Vertreter für die gemeinsame Kontrollinstanz gemäß Art. 24 des Übereinkommens ernennt, davon einen auf Vorschlag des Bundesbeauftragten für den Datenschutz, einen weiteren auf Vorschlag des Bundesrates. Als weiterer Vertreter kann damit auch eine Person ernannt werden, die nicht zu dem Kreis der Landesbeauftragten für den Datenschutz zählt. Zur Sicherstellung der Beteiligung der Landesbeauftragten für den Datenschutz sollte aus meiner Sicht eine Ergänzung des § 6 Abs. 2 dahingehend erfolgen, daß ein Vertreter aus dem Kreis der Landesbeauftragten ernannt wird.

Das Gesetzesvorhaben war bei Redaktionsschluß noch nicht abgeschlossen.

Daneben müssen noch eine Reihe von Durchführungs- und Ausführungsbestimmungen zur Konvention erlassen werden, da Europol seine Tätigkeit erst aufnehmen kann, wenn bestimmte vorgesehene Rechtsakte in Kraft getreten sind. Besonders umstritten sind in diesem Zusammenhang die Durchführungsbestimmungen zu den sog. Arbeitsdateien zu Analysezwecken. Diese Arbeitsdateien sind nach Art. 10 der Europol-Konvention ein wesentlicher Bestandteil der Informationsverarbeitung durch Europol. In einem ersten Entwurf zu den Durchführungsbestimmungen war u.a. die Speicherung besonders sensibler personenbezogener Daten aus dem Privat- und Intimleben, wie z.B. die politische Anschauung, religiöse Überzeugungen sowie nähere Angaben zum Sexualleben, vorgesehen. Durch eine solche Regelung könnten in den Analysedateien umfassende Persönlichkeitsbilder einer Vielzahl von Personen erstellt werden. Dies ist aus datenschutzrechtlichen Gründen entschieden abzulehnen. Nach Mitteilung des Staatsministerium des Innern wurden diese Bestimmungen von allen Innenministerien der Länder und auch vom Bundesinnenministerium von Anfang an in Frage gestellt. Die Verhandlungen auf europäischer Ebene dauern an.

5.17 Bürgereingaben

Auch in diesem Berichtszeitraum wandten sich wieder zahlreiche Bürger an mich, die eine rechtswidrige Erhebung, Verarbeitung oder Nutzung ihrer personenbezogenen Daten durch die Polizei befürchteten.

In den meisten Fällen erwiesen sich diese Befürchtungen als unbegründet. Ich habe jedoch in Einzelfällen die Löschung bzw. Berichtigung von Daten und die Vernichtung polizeilicher Unterlagen durch die Polizei oder auch die Verkürzung von Speicherfristen gefordert sowie die Weitergabe von Daten gerügt.

Einzelne Bürger baten um Überprüfung, ob Polizeibeamte ihre zur Aufgabenerfüllung bestehende Möglichkeit des Zugriffs auf polizeiliche Informationssysteme für private Interessen genutzt hatten. So wurde beispielsweise folgender Sachverhalt an mich herangetragen:

Ein Polizeibeamter hatte die personenbezogenen Speicherungen aus polizeilichen Dateien abgefragt und sich bei meiner Überprüfung auf dienstliche Gründe berufen. Zum Zeitpunkt der Abfrage bestand zwischen dem Polizeibeamten und dem Betroffenen, die im selben Anwesen wohnen, allerdings eine private Konfliktlage. Ich habe das Polizeipräsidium München darauf aufmerksam gemacht, daß bei dieser Sachlage eine objektive und unparteiische Amtsausübung nicht mehr sichergestellt ist. In solchen Fällen besteht die Gefahr der Vermischung privater und beruflicher Interessen. Statt sich auf die formale "Allzuständigkeit" eines Polizeivollzugsbeamten zu stützen, sollten in vergleichbaren Fällen Abfragen aus polizeilichen Dateien - entsprechend dem Gedanken der Art. 20, 21 Bayerisches Verwaltungsverfahrensgesetz (Ausschluß wegen Besorgnis der Befangenheit) - von anderen Polizeibeamten durchgeführt werden, die keinen privaten Kontakt zu dem Betroffenen haben.

Ich habe allerdings von einer förmlichen Beanstandung gemäß Art. 31 BayDSG abgesehen, da eine dienstliche Veranlassung der Datenabfrage vom Polizeipräsidium angenommen wurde und von mir jedenfalls nicht auszuschließen war.

Wegen zweier weiterer Bürgeranfragen, in denen der Verdacht geäußert wurde, daß Polizeibe-

amte polizeiliche Informationssysteme ohne dienstlichen Anlaß abgefragt haben könnten, habe ich die Protokolldatei ausgewertet. Dabei stellte ich fest, daß zwar personenbezogene Daten der Betroffenen abgefragt worden waren, jedoch nur die Stammnummer (Personalkennziffer) des Abfragenden, nicht aber auch die **Kennung des die Abfrage Veranlassenden** protokolliert war.

Eine solche Teilprotokollierung ist unzureichend. Sie ermöglicht keine ausreichende Datenschutzkontrolle und entspricht nicht den bestehenden innerdienstlichen Richtlinien.

Ist der Abfragende (Bediener) nur Datenmittler für einen anderen berechtigten Auskunftbegehrenden (überwiegend Beschäftigte der Einsatzzentralen), so ist **verpflichtend** die Zusatzprotokollierung mit den **Identifizierungsdaten** des auskunftbegehrenden Bediensteten vorgeschrieben. Welche zusätzlichen Identifizierungsdaten zu verwenden sind, richtet sich nach den tatsächlichen Möglichkeiten, dem verwendeten Kommunikationsmittel des Auskunftbegehrenden und den zu beachtenden Sicherheitsvorschriften.

Ich habe die Polizei aufgefordert auf die Einhaltung dieser Vorgaben zu achten.

---

6. Verfassungsschutz

6.1 Prüfung der Verfassungsmäßigkeit von Vorschriften des Bayerischen Verfassungsschutzgesetzes und des Bayerischen Datenschutzgesetzes durch den Verfassungsgerichtshof

Beim Verfassungsgerichtshof ist eine Popularklage zu mehreren Vorschriften des Bayerischen Verfassungsschutzgesetzes (BayVSG) und des Bayerischen Datenschutzgesetzes (BayDSG) anhängig. Die angefochtenen Normen betreffen u.a. die datenschutzrechtliche Kontrolle bei der Verarbeitung und Nutzung von Daten in Akten (Art. 30 Abs. 1 Satz 2 BayDSG) und den Auskunftsanspruch des Betroffenen gegenüber dem Landesamt für Verfassungsschutz (Art. 11 Abs. 1 Satz 2 BayVSG).

Ich habe hierzu wie folgt Stellung genommen:

1. **Zu Art. 30 Abs. 1 Satz 2 BayDSG**

   Nach Art. 30 Abs. 1 BayDSG kontrolliert der Landesbeauftragte unbeschränkt die in Dateien gespeicherten Daten. Hierzu kann er Einsicht in die jeweils zugrundeliegenden Akten verlangen. Werden Daten allerdings ausschließlich in Akten verarbeitet oder genutzt, ist nach dem BayDSG (wie auch im BDSG) lediglich eine Anlaßkontrolle bestimmt. In diesem Fall besteht eine Kontrollkompetenz nur dann, wenn der Betroffene hinreichende Anhaltspunkte für eine Verletzung seiner Rechte darlegt oder wenn dem Landesbeauftragten hinreichende Anhaltspunkte für eine derartige Verletzung vorliegen.

   Im Polizei- und Sicherheitsrecht ermöglichen eine Reihe von Vorschriften verdeckte Datenerhebungen. Auch wenn unter bestimmten Voraussetzungen zur Sicherstellung einer wirksamen Strafverfolgung und Verbrechensbekämpfung und damit zum Schutz überwiegender Allgemeininteressen eine solche Datenerhebung ohne Wissen des Betroffenen erforderlich sein kann, muß zum Ausgleich eine Kontrolle der Datenerhebung, -verarbeitung und -nutzung durch unabhängige und an keine Weisung gebundene staatliche Organe sichergestellt werden. Der verfassungsrechtlich gebotene Schutz des informationellen Selbstbestimmungsrechts ist im Bereich der verdeckten Datenerhebung nicht hinreichend gewährleistet. Die Beschränkung meiner Kontrollbefugnis bei der Verarbeitung und Nutzung von Daten in Akten in Art. 30 Abs. 1 Satz 2 BayDSG führt vielmehr zu einem empfindlichen Kontrolldefizit. Werden über den Betroffenen ohne dessen Wis-

sen Daten erhoben und verarbeitet, kann er eine Rechtsverletzung nicht erkennen und nicht für einen effektiven Rechtsschutz - sei es durch die Anrufung des Datenschutzbeauftragten oder des Gerichts - sorgen. Sowohl die G 10- Kommission als auch das Gericht prüfen nur in Teilbereichen die Rechtmäßigkeit der Datenerhebung und -verarbeitung bei verdeckten Maßnahmen der Sicherheitsbehörden. Das Grundrecht auf informationelle Selbstbestimmung wird damit in einem wesentlichen Kernbereich verletzt, da ein effektiver Rechtsschutz bei erheblichen Eingriffen fehlt. Diese Lücke ist auch nicht durch überwiegende Allgemeininteressen gerechtfertigt. Dem Bedürfnis nach wirksamer Verbrechensbekämpfung und Strafverfolgung kann auch bei einer anlaßunabhängigen Aktenkontrolle durch den Datenschutzbeauftragten in vollem Umfang Rechnung getragen werden.

Wie ich bereits in meinem 16. Tätigkeitsbericht (Nr. 1.5) dargelegt habe, halte ich für den Bereich der verdeckten Datenerhebung eine anlaßunabhängige Kontrollbefugnis des Datenschutzbeauftragten auch dann für verfassungsrechtlich geboten, wenn die personenbezogenen Daten in Akten verarbeitet oder genutzt werden.

2. **Art. 11 Abs. 1 Satz 2 BayVSG**

Gemäß Art. 11 Abs. 1 Satz 2 BayVSG hat der einzelne keinen Anspruch auf Auskunft gegenüber dem Landesamt für Verfassungsschutz über Dateien oder Akten. Nur wenn ein **besonderes Interesse** an einer Auskunft geltend gemacht wird, entscheidet das Landesamt nach pflichtgemäßem Ermessen über das Auskunftsbegehren.

Der uneingeschränkten Offenlegung personenbezogener Daten durch das Landesamt steht ein staatliches Geheimhaltungsbedürfnis entgegen. Die Wahrnehmung der Aufgaben des Landesamts wäre erheblich erschwert oder in Teilen sogar unmöglich, wenn das Landesamt für Verfassungsschutz Dritten gegenüber auf Anfrage uneingeschränkt Einblick in seine Arbeitsweise und Erkenntnisse gewähren müßte. Zur Abwehr einer systematischen Ausforschung des Landesamts hat der Gesetzgeber unter angemessener Berücksichtigung des Rechts auf informationelle Selbstbestimmung eine differenzierte Re-

gelung zur Auskunftserteilung in Art. 11 BayVSG getroffen.

Allerdings dürfen nach meiner Auffassung an den Begriff des "besonderen Interesses" keine allzu hohen Anforderungen gestellt werden. Es muß ausreichend sein, wenn der Betroffene über das bei jedem Bürger gleichermaßen vorhandene Interesse an der Speicherung von personenbezogenen Daten hinaus ein Interesse darlegt, das eine zusätzliche Bedeutung der Auskunftserteilung für ihn erkennen läßt. Hierzu zählen beispielsweise die Darlegung beruflicher oder sonstiger vergleichbarer Nachteile sowie ausreichende Anhaltspunkte für die Befürchtung der Beobachtung durch das Landesamt für Verfassungsschutz.

6.2 Entscheidung des Bundesverfassungsgerichts zur strategischen Fernmeldeüberwachung durch den Bundesnachrichtendienst (BND)

Durch das Gesetz zur Änderung des Strafgesetzbuches, der Strafprozeßordnung und anderer Gesetze (Verbrechensbekämpfungsgesetz) vom 28.10.1994 wurden eine Reihe von Regelungen des Gesetzes zu Art. 10 des Grundgesetzes (G-10-Gesetz) geändert. Insbesondere wurden die Befugnisse des BND zur Überwachung des nicht leitungsgebundenen internationalen Fernmeldeverkehrs erheblich erweitert. Der BND ist nunmehr ermächtigt, diesen Fernmeldeverkehr **ohne konkreten Verdacht** zu überwachen, um die Gefahr der Planung oder Begehung bestimmter Straftaten rechtzeitig zu erkennen und einer solchen Gefahr zu begegnen. Dazu können Suchbegriffe verwendet werden, die auf das Vorliegen solcher Gefahren hindeuten können (sog. verdachtslose Rasterfahndung). Unter bestimmten, in § 3 Abs. 3 G-10-Gesetz genannten Voraussetzungen dürfen die durch die Maßnahme erlangten personenbezogenen Daten zur Verhinderung, Aufklärung und Verfolgung von bestimmten schweren Straftaten verwendet werden. Der BND ist verpflichtet, die erlangten Daten zu diesem Zweck vollständig an die Strafverfolgungs- und Sicherheitsbehörden weiterzugeben, soweit dies zur Erfüllung ihrer Aufgaben erforderlich ist. Eine Einschaltung der unabhängigen Kontrollkommission sieht das Gesetz insoweit nicht vor.

Gegen diese gesetzlichen Regelungen hatte zunächst ein Beschwerdeführer Klage beim Bundesverfassungsgericht erhoben. Dazu habe ich mich gegenüber dem Bundesverfassungsgericht wie folgt geäußert:

Aufgabe des Bundesnachrichtendienstes ist es, Erkenntnisse über das Ausland zu sammeln, die von außen- und sicherheitspolitischer Bedeutung für die Bundesrepublik Deutschland sind. Von sicherheitspolitischer Bedeutung können neben militärischen Bedrohungen auch von außen erfolgende Bedrohungen durch bestimmte Formen besonders schwerwiegender Kriminalität sein. Nach wie vor ist es jedoch nicht Aufgabe des Bundesnachrichtendienstes, inländische Strafverfolgung zu betreiben. Dies ist allein Sache der Staatsanwaltschaft und der Polizei. Auch im Hinblick auf die in § 3 G-10-Gesetz genannten Delikte hat der BND lediglich die Aufgabe, durch Vorfeldbeobachtung im Ausland Erkenntnisse zu gewinnen, die für die Sicherheitsinteressen der Bundesrepublik Deutschland erheblich sind. Hierzu ist er befugt, den internationalen Funkfernmeldeverkehr durch Verwendung geeigneter Suchbegriffe zu überwachen.

Die Problematik der Neuregelung sehe ich darin, daß die erhobenen personenbezogenen Daten nicht nur zur Erfüllung der primären Aufgaben des BND genutzt werden dürfen, sondern eine Verwendung der Daten unter bestimmten Voraussetzungen zur Gefahrenabwehr und Strafverfolgung zugelassen ist. Durch den Einsatz von Suchbegriffen bei der Überwachung des gesamten internationalen nicht leitungsgebundenen Fernmeldeverkehrs sind vielfältige Zufallserkenntnisse über bevorstehende oder bereits begangene Straftaten zu erwarten. Diese - zwar nicht gezielte - aber doch zwangsläufige und absehbare Folge der strategischen Fernmeldeüberwachung durch den BND rückt die Maßnahme faktisch in die Nähe der Verhütung und Verfolgung von Straftaten.

Präventive Telefonüberwachung ist aber nach den Polizeigesetzen der Länder nicht zulässig. Repressive Telefonüberwachung muß sich nach den strafprozessualen Regelungen der §§ 100 a ff. Strafprozeßordnung richten, die einen Anfangsverdacht bezüglich einer Katalogtat voraussetzt, einer richterlichen Anordnung bedarf und im übrigen der Kontrolle der Datenschutzbeauftragten hinsichtlich der Einhaltung richterlicher Vorgaben bei der Datenerhebung, der Datenverarbeitung und Nutzung unterliegt.

Die strategische Fernmeldeüberwachung darf nicht zu einer Umgehung der für die Ermittlung strafrechtlich relevanter Vorgänge maßgebenden gesetzlichen Regelungen führen. Daraus folgt aus meiner Sicht, daß die vom BND bei der Überwachung des internationalen Funkfernmeldeverkehrs gewonnenen Daten grundsätzlich nur zur strategischen Vorfeldbeobachtung benutzt werden dürfen. Eine Nutzung zur Strafverfolgung darf nicht schon dann zulässig sein, wenn der bloße Anfangsverdacht besteht, daß jemand eine bestimmte Straftat plant, begeht oder begangen hat. Für die Zulässigkeit der Datenübermittlung ist vielmehr aus meiner Sicht ein qualifizierter Verdachtsgrad erforderlich.

Außerdem halte ich eine lückenlose Kontrolle der Datenerhebung, -verarbeitung und -nutzung der durch die Fernmeldeüberwachung gewonnenen Daten durch ein unabhängiges Gremium für unabdingbar.

Mit Beschluß vom 05. Juli 1995 hat das Bundesverfassungsgericht vorläufig entschieden, daß die bei der Überwachung des internationalen Fernmeldeverkehrs gewonnenen personenbezoge-

nen Daten zur Verhinderung, Aufklärung oder Verfolgung von Straftaten nur dann verwendet werden dürfen, wenn **bestimmte Tatsachen** den Verdacht begründen, daß jemand eine in **§ 3 Abs. 3 G-10-Gesetz genannte Straftat** plant, begeht oder begangen hat. Nur unter diesen Voraussetzungen ist der Bundesnachrichtendienst bis auf weiteres befugt, anderen Behörden, insbesondere Polizei und Staatsanwaltschaft durch die Fernmeldeüberwachung erlangte personenbezogene Daten zu übermitteln.

Das Bundesverfassungsgericht hat mit dieser Entscheidung die Zulässigkeit der Verwendung und Weitergabe personenbezogener Informationen, die der Bundesnachrichtendienst durch die erweiterte Befugnis zum Abhören des internationalen Funkfernmeldeverkehrs gewonnen hat, erheblich eingeschränkt. Es stellt sich damit der Gefahr entgegen, daß durch die Kombination des flächendeckenden Abhörens mit weitgehenden Befugnissen des BND zur Datenübermittlung an Strafverfolgungsbehörden eine Vielzahl von Bürgern unberechtigt Betroffene strafrechtlicher Ermittlungen werden können. Das Bundesverfassungsgericht stellt sicher, daß die Eingriffsschwelle für Telefonabhörmaßnahmen zugunsten der Strafverfolgung nicht unvertretbar abgesenkt wird.

Die Entscheidung bestätigt die von mir geäußerten Bedenken gegen eine zu weitgehende Datenübermittlung zwischen Bundesnachrichtendienst und Strafverfolgungsbehörden. Ich hoffe darüber hinaus, daß sich das Bundesverfassungsgericht in seiner nachfolgenden Entscheidung in der Hauptsache auch zur Frage der "erforderlichen verfahrensmäßigen Sicherungen" äußern wird. In meiner Stellungnahme bin ich dafür eingetreten, den jeweiligen Datenschutzbeauftragten von Datenübermittlungen zu unterrichten und seine Zuständigkeit auch für Aktenkontrollen festzustellen.

Ein Termin für eine Entscheidung in der Hauptsache steht derzeit noch nicht fest.

6.3 Entwurf eines Bayerischen Sicherheitsüberprüfungsgesetzes

Das Staatsministerium des Innern hat den Entwurf eines Gesetzes über die Voraussetzungen und das Verfahren von Sicherheitsüberprüfungen des Freistaates Bayern - Bayerisches Sicherheitsüberprüfungsgesetz - (BaySÜG) vorgelegt. Der Entwurf orientiert sich in wesentlichen Punkten an dem Sicherheitsüberprüfungsgesetz des Bundes, das am 29.04.1994 in Kraft getreten ist.

Aus datenschutzrechtlicher Sicht ist es zu begrüßen, daß Sicherheitsüberprüfungen, die bislang auf der Grundlage von Sicherheitsrichtlinien durchgeführt wurden, nunmehr in einem Gesetz bereichsspezifisch geregelt werden sollen.

Zu dem Gesetzesentwurf habe ich mehrfach Stellung genommen. Insbesondere in folgenden Punkten hat das Staatsministerium des Innern meine Forderungen aufgegriffen:

- In der Gesetzesbegründung wird deutlich gemacht, daß

  - die Gründe für die Anordnung der nächsthöheren als der ursprünglich erforderlichen Stufe der Sicherheitsüberprüfung in der Akte zu dokumentieren sind.

  - die nächsthöhere Stufe der Sicherheitsüberprüfung nur insoweit durchgeführt wird, wie es zur Klärung der sicherheitserheblichen Erkenntnisse erforderlich ist.

  - im Falle des Wechsels der Behörde oder des Arbeitgebers die Sicherheitsakte an die zuständige Stelle verschlossen mit dem Hinweis weitergegeben wird, daß die Sicherheitsakte nur geöffnet werden darf, wenn dem Bediensteten eine Tätigkeit übertragen wird, für die eine Sicherheitsüberprüfung erforderlich ist. Übernimmt der Bedienstete keine sicherheitsrelevante Tätigkeit mehr, ist die ungeöffnete Sicherheitsakte nach Ablauf von fünf Jahren zu vernichten.

  Das Staatsministerium des Innern hat mitgeteilt, daß Einzelheiten dazu in Vollzugshinweisen geregelt werden.

- Im Fall der Sicherheitsüberprüfung für nicht-öffentliche Stellen erhält die nicht-öffentliche Stelle nur Kenntnis von bestimmten und nicht von allen in der Sicherheitserklärung enthaltenen personenbezogenen Daten des Betroffenen. Besonders sensible personenbezogene Daten, wie z.B. Angaben über frühere Zwangsvollstreckungsmaßnahmen oder anhängige Strafverfahren, werden damit nicht mehr im Wege der Sicherheitserklärung dem privaten Arbeitgeber des Betroffenen mitgeteilt.
- Ausdrücklich wird geregelt, daß die Durchführung einer Sicherheitsüberprüfung ein "besonderes Interesse" an einer Auskunftserteilung im Sinne des Bayerischen Verfassungsschutzgesetzes begründet.

- Die Datenerhebung und Datenübermittlung durch das Landesamt für Verfassungsschutz wird **abschließend** im Bayerischen Sicherheitsüberprüfungsgesetz geregelt. Eine Erweiterung der diesbezüglichen Befugnisse des Landesamtes durch eine Verweisung auf Vorschriften des Bayerischen Verfassungsschutzgesetzes ist entfallen.

Der überarbeitete Gesetzentwurf zum BaySÜG (Stand: 16.10.1996) enthält gleichwohl noch eine Reihe von Regelungen, die ich aus datenschutzrechtlicher Sicht für bedenklich halte:

- Nach Art. 26 Abs. 1 Satz 3 des Entwurfs darf das Landesamt für Verfassungsschutz als mitwirkende Behörde die im Rahmen der Sicherheitsüberprüfung gespeicherten personenbezogenen Daten über die Zwecke der Sicherheitsüberprüfung hinaus auch zur Erfüllung seiner sonstigen gesetzlichen Aufgaben nach Art. 3 Abs. 1 Bayerisches Verfassungsschutzgesetz (BayVSG) nutzen und übermitteln. Dies bedeutet, daß das Landesamt für Verfassungsschutz die aus der Sicherheitsüberprüfung erlangten Erkenntnisse zur Erfüllung **aller** ihm nach dem Bayerischen Verfassungsschutzgesetz zugewiesenen Aufgaben verwenden kann.

  Eine solche weitgehende Zweckänderung halte ich im Hinblick auf den verfassungsrechtlichen Grundsatz der Zweckbindung aus datenschutzrechtlicher Sicht für höchst problematisch. Nach der Rechtsprechung des Bundesverfassungsgerichts (BVerfG 65,1 ff.) dürfen personenbezogene Daten grundsätzlich nur für Zwecke gespeichert, verändert oder genutzt werden, für die sie erhoben worden sind. Eine anderweitige Verwendung ist nicht mehr von der Freiwilligkeit bzw. der bereichsspezifischen Verpflichtung gedeckt, aufgrund der der Betroffene die Daten ursprünglich angegeben hat. Ausnahmen sind nur

zulässig, wenn diese im **überwiegenden Allgemeininteresse** erforderlich sind.

In Anwendung dieses Grundsatzes und in Übereinstimmung mit der Regelung in § 21 Abs. 1 Satz 4 des Sicherheitsüberprüfungsgesetzes des Bundes erscheint mir eine **Beschränkung** der Zweckänderung auf die Beobachtung von Bestrebungen und Tätigkeiten der Organisierten Kriminalität im Geltungsbereich des Grundgesetzes, die Aufklärung von sicherheitsgefährdenden oder geheimdienstlichen Tätigkeiten für eine fremde Macht oder von Bestrebungen, die darauf gerichtet sind, Gewalt anzuwenden oder Gewaltanwendung vorzubereiten sowie auf die Aufklärung sonstiger Bestrebungen von **erheblicher** Bedeutung geboten.

- Der Entwurf sieht vor, daß Erkenntnisse aus der Sicherheitsüberprüfung zum Zwecke der Verfolgung **jedweder** Straftat verwendet werden können. Die im Vorentwurf vorgesehene Beschränkung der Zweckänderung auf die Verfolgung von Straftaten von **erheblicher** Bedeutung ist entfallen. Eine solche Aufweichung des verfassungsrechtlichen Grundsatzes der Zweckbindung ist nach meiner Auffassung für die Verfolgung von sog. Bagatelldelikten nicht gerechtfertigt. Ziel einer Sicherheitsüberpüfung ist es, festzustellen, ob eine Person mit der Durchführung sicherheitsempfindlicher Tätigkeiten betraut werden kann. Nur zu diesem Zweck ist der Betroffene damit einverstanden, daß das Landesamt für Verfassungsschutz seine personenbezogenen Daten erhebt. Je nach Art der Sicherheitsüberprüfung befragt das Landesamt für Verfassungsschutz auch Referenzpersonen zum Privatleben des Betroffenen sowie seiner Ehegatten bzw. Lebenspartner und erlangt dadurch in erheblichem Umfang Kenntnis von besonders sensiblen Daten. Ist der Betroffene mit einer solchen Ausforschung seiner persönlichen Lebensumstände durch den Verfassungsschutz nicht einverstanden, ist ihm eine berufliche Tätigkeit in einem sicherheitsempfindlichen Bereich verwehrt.

  Unter diesen Umständen sind an die Voraussetzungen für eine Zweckänderung erhöhte Anforderungen zu stellen. Die allgemeinen Regelungen in Art. 17 Abs. 2 Ziff. 10 BayDSG, wonach zu anderen Zwecken erhobene personenbezogene Daten auch gespeichert, verändert oder genutzt werden können, soweit es zur Verfolgung von Straftaten erforderlich ist, wird den o.g. Besonderheiten der Datenerhebung im Rahmen einer Sicherheitsüberprüfung nicht gerecht. Erforderlich ist hier eine einschränkende bereichsspezifische Regelung, die den Interessen des Betroffenen im Hinblick auf die besondere Sensi-

bilität der Materie stärker Rechnung trägt und nur bei Straftaten von **erheblicher** Bedeutung aus überwiegenden Allgemeininteressen eine Zweckänderung zuläßt. Eine Notwendigkeit für eine weitergehende Datennutzung und -übermittlung konnte aus den Erfahrungen der Vergangenheit auch nicht dargelegt werden.

- Der Entwurf sieht vor, daß zu den Aufgaben des Landesamtes für Verfassungsschutz auch die Erteilung amtlicher Auskünfte nach Maßgabe der Art. 14 BayVSG, insbesondere in Einbürgerungs- und Ordensverfahren zur Verleihung des Verdienstordens der Bundesrepublik Deutschland - mit Ausnahme der Verdienstmedaille - und des Bayerischen Verdienstordens, sowie nach Art. 15 BayVSG zählt. Damit wäre das Landesamt für Verfassungsschutz nach Art. 5 Satz 1 BayVSG befugt, eigens zu diesem Zweck personenbezogene Daten zu erheben. Eine solche Befugnis erscheint mir - jedenfalls soweit Anfragen in Ordensangelegenheiten in Frage stehen - in dieser Allgemeinheit nicht gerechtfertigt. Vielmehr sollte das Landesamt für Verfassungsschutz wie im Fall der Überprüfung der Verfassungstreue einer Person, die sich um eine Stelle im öffentlichen Dienst bewirbt, bei Ordensangelegenheiten grundsätzlich darauf beschränkt sein, über **bestehende** Erkenntnisse Auskunft zu erteilen. Datenerhebungen sollte es entsprechend Art. 5 Satz 2 BayVSG nur im Rahmen von Nachermittlungen durchführen dürfen, soweit das zur Überprüfung bereits vorliegender Informationen erforderlich ist.

Das Gesetzesvorhaben war bei Redaktionsschluß noch nicht abgeschlossen.

6.4 Generelle Prüfungen 1995 und 1996

Im Berichtszeitraum habe ich beim Landesamt für Verfassungsschutz wieder in mehrtägigen Prüfungen verschiedene **Dateien** und aus gegebenem Anlaß auch **Akten** kontrolliert.

Prüfungs**schwerpunkte** waren insbesondere Speicherungen

- im Zusammenhang mit der Beobachtung der **organisierten Kriminalität (OK)**
- im Zusammenhang mit dem **Weltwirtschaftsgipfel 1992**
- aufgrund von **Sicherheitsüberprüfungen**
- in den Dateien **NADIS** und **IBA**.

Dabei habe ich festgestellt, daß die datenschutzrechtlichen Bestimmungen weitgehend beachtet werden.

6.4.1 Sicherheitsüberprüfung

Im Berichtszeitraum habe ich erneut stichprobenartig Sicherheitsüberprüfungen - die in einer automatisierten Datei und in Akten beim Landesamt dokumentiert sind - kontrolliert (vgl. 16. Tätigkeitsbericht, Nr. 6.4.2). Die für diesen Zweck erhobenen Daten sind von besonderer **Sensibilität**, da sie sich auch auf Persönlichkeitsmerkmale des Betroffenen beziehen. Solchen personenbezogenen Daten kann im Einzelfall erhebliche Bedeutung zukommen.

Ich habe deshalb auf der Grundlage meiner Erfahrungen aus der vorangegangenen Prüfung und den Prüfungserfahrungen anderer Datenschutzbeauftragter besonders den Bereich der **Datenerhebung** durch die Befragung von Referenzpersonen und die Speicherung der Befragungsergebnisse geprüft.

Dabei habe ich festgestellt, daß teilweise neben mißverständlichen Wertungen, Mitteilungen von Referenzpersonen aufgezeichnet und zur Sicherheitsüberprüfungsakte genommen wurden, die nach meiner Einschätzung für die Beurteilung des Betroffenen unter **sicherheitserheblichen Aspekten** im Hinblick auf seine zukünftige Tätigkeit ohne konkrete Bedeutung waren. Darauf habe ich das Landesamt für Verfassungsschutz unter genauer Bezeichnung der einzelnen Speicherungen hingewiesen. Das Landesamt hat sich meiner Auffassung angeschlossen und die fraglichen Daten durch Schwärzen gelöscht.

Eine im Jahr 1996 durchgeführte Nachkontrolle und die dabei geführten Gespräche zeigten mir die Bereitschaft des Landesamtes zur Berücksichtigung datenschutzrechtlicher Belange und eine deutliche Verbesserung der Erhebungs- und Speicherungspraxis.

6.4.2 Beobachtung der Organisierten Kriminalität durch das Landesamt für Verfassungsschutz

Mit der Änderung des Bayerischen Verfassungsschutzgesetzes (Art. 3 Abs. 1 Nr. 4) wurde dem Landesamt für Verfassungsschutz die Aufgabe der Beobachtung von Bestrebungen und Tätigkeiten der Organisierten Kriminalität neu zugewiesen. Das Landesamt darf auch zur Erfüllung dieser Aufgabe unter den Voraussetzungen des Art. 7 Bayerisches Verfassungsschutzgesetz personenbezogene Daten in Akten und Dateien speichern und verändern. Das Landesamt hat die Voraussetzungen für die Speicherung in einer automatisierten Datei zwischenzeitlich in einer Errichtungsanordnung geregelt.

Ergänzend zu der Errichtungsanordnung hat das Landesamt Vorgaben für die Verarbeitung personenbezogener Daten zur Beobachtung von Bestrebungen und Tätigkeiten der Organisierten Kriminalität in einer Arbeitsanweisung festgelegt. Ich habe insbesondere Bedenken wegen zu weitgehender Speicherungsmöglichkeiten, einer zu geringen Konkretisierung des betroffenen Personenkreises und einer zu wenig differenzierten Festlegung von Speicherungsfristen geäußert und dazu eine Reihe von Änderungen der Arbeitsanweisung angeregt. Das Landesamt hat diese Anregungen aufgegriffen und die Arbeitsanweisung entsprechend überarbeitet. Meinen Bedenken wurde dabei in vollem Umfang Rechnung getragen.

6.4.3 Beobachtung der Organisierten Kriminalität (OK) durch das Landesamt für Verfassungsschutz (Prüfung von Speicherungen in Dateien)

Nachdem ich mich zum Ende des letzten Berichtszeitraumes beim Landesamt für Verfassungsschutz (LfV) eingehend über die datenschutzrechtlich relevanten Aspekte der Arbeit des Landesamtes in diesem Bereich **informiert** hatte, habe ich im Rahmen einer mehrtägigen Prüfung **Datenerhebung und -speicherung in Dateien** zur Beobachtung der organisierten Kriminalität **kontrolliert**.

Maßstab für meine datenschutzrechtliche Kontrolle waren neben den gesetzlichen Grundlagen des Verfassungsschutzgesetzes, die von mir zuvor geprüfte **Errichtungsanordnung** für die in diesem Bereich eingesetzte automatisierte Datei.

Prüfungsgegenstand im einzelnen waren insbesondere

- das Vorliegen **tatsächlicher Anhaltspunkte** für Bestrebungen und Tätigkeiten der organisierten Kriminalität als Voraussetzung des Einsatzes nachrichtendienstlicher Mittel zur Datenerhebung

- der von **Speicherungen** betroffene **Personenkreis**, die **Speicherungsdauer** sowie die **Dokumentation** der verfassungsschutzinternen, gesetzlich vorgeschriebenen Prüfungen der Erforderlichkeit der weiteren Speicherung nach festgesetzten Fristen.

- **Datenübermittlungen an** das LfV, insbesondere deren weitere Behandlung durch das LfV.

In Einzelfällen habe ich Mängel bei der Speicherung festgestellt. Das Landesamt hat daraufhin die personenbezogenen Daten in einem Fall **gelöscht** und in mehreren anderen die Speicherungsdauer **reduziert**.

6.4.4 Registraturwesen des Bayerischen Landesamtes für Verfassungsschutz

Das Landesamt für Verfassungsschutz setzt zur Erfassung ein- und ausgehender Schriftstücke

ein EDV-unterstütztes Registratur- und Schriftgutverwaltungsverfahren ein. Nach der Errichtungsanordnung können in der Datei auch personenbezogene Daten des Empfängers, des Einsenders sowie die im Betreff des zu registrierenden Schriftstücks genannten Personen gespeichert werden.

Ich habe das Landesamt darauf hingewiesen, daß diese Datei nicht nur als reines Vorgangsverwaltungssystem anzusehen ist, sondern auch fachliche Recherchen nach bestimmten Personen ermöglicht. Zu fachlichen Zwecken dürfen Daten einer Person beim Verfassungsschutz jedoch nur unter den engen Voraussetzungen des Art. 7 Bayerisches Verfassungsschutzgesetz (BayVSG) in einer Datei suchfähig gespeichert und genutzt werden. Nach meiner Auffassung muß deshalb die Möglichkeit einer fachlichen Recherche in der Vorgangsverwaltungsdatei durch eine entsprechende Regelung in der Errichtungsanordnung beschränkt werden. Eine unmittelbare oder mittelbare Nutzung der Vorgangsverwaltungsdatei zum Zwecke der Aufgabenerfüllung durch die Fachabteilungen muß grundsätzlich ausgeschlossen sein. Fachliche Recherchen kommen nur dann in Betracht, wenn die gesetzlichen Voraussetzungen für die Speicherung der davon betroffenen Person nach Art. 7 BayVSG gegeben sind.

Der diesbezügliche Meinungsaustausch mit dem Landesamt für Verfassungsschutz ist noch nicht abgeschlossen.

6.4.5 Speicherungen im Zusammenhang mit dem Münchener Weltwirtschaftsgipfel 1992

Anläßlich des Münchener Weltwirtschaftsgipfels im Jahre 1992 wurden nach Sicherheitsstörungen von der Polizei 491 Personen festgenommen und wegen unterschiedlicher Delikte - wie Nötigung, Verunglimpfung des Staates und seiner Symbole, Landfriedensbruch - angezeigt.

Die eingeleiteten strafrechtlichen Ermittlungsverfahren wurden teils nach § 170 Abs. 2 StPO, teils nach § 153 StPO **eingestellt**; zu Verurteilungen kam es **nicht**.

Wie ich aus meiner datenschutzrechtlichen Prüfung beim Polizeipräsidium München wußte (vgl. Nr. 5.4.1), wurden die Personalien der Festgenommenen von der Polizei auch dem Landesamt für Verfassungsschutz übermittelt. **Ziel** meiner Prüfung war deshalb festzustellen, **ob** und ggf. **in welchen Dateien** mit welcher Dauer und welchem Umfang das Landesamt Speicherungen dieses Personenkreises vorgenommen hatte.

Ich konnte mich durch Stichprobenkontrollen davon überzeugen, daß Speicherungen in **Fachdateien** des LfV (wie z.B. NADIS und IBA) nur aus Anlaß der Vorkommnisse beim Weltwirtschaftsgipfel **nicht** vorhanden waren.

Es waren jedoch Daten von Festgenommenen in der Vorgangsverwaltungsdatei des Landesamtes gespeichert. Zu einzelnen dieser Speicherungen waren schriftliche Unterlagen in sog. Sachakten der Fachabteilung abgelegt. Da diese Speicherungen für fachliche Zwecke des Landesamtes genutzt werden können, sind sie nach meiner Auffassung nur unter den Voraussetzungen des Bayerischen Verfassungsschutzgesetzes zulässig (vgl. dazu Nr. 6.4.4).

Bei einer Reihe von Speicherungen konnte ich die **Erforderlichkeit** zur Aufgabenerfüllung des Landesamtes nicht feststellen. Ich habe deshalb das Landesamt um Stellungnahme gebeten. Diese steht noch aus.

7. Justiz

7.1 Gesetzgebungsverfahren

7.1.1 Gesetzgebungsarbeiten zu einem Strafverfahrensänderungsgesetz

Im Rahmen der Gesetzgebungsarbeiten zu einem Strafverfahrensänderungsgesetz (siehe dazu die ausführliche Darstellung in meinem 16. Tätigkeitsbericht, Nr. 7.2.1) habe ich mich zu drei Themenbereichen nochmals an das Staatsministerium der Justiz gewandt:

1. In einem Forderungspapier zur "Stärkung der Persönlichkeitsrechte von Verfahrensbeteiligten bei der Gewährung von Akteneinsicht durch die Staatsanwaltschaft" habe ich für die Zeit bis zu einer ausreichenden Regelung der Gewährung von Akteneinsicht in der Strafprozeßordnung am Erforderlichkeits- und Verhältnismäßigkeitsgrundsatz orientierte Grundsätze für die Gewährung von Akteneinsicht während einer Übergangszeit aufgestellt. Wesentlich erscheinen mir dabei folgende Punkte:

   - Voraussetzung für eine Akteneinsicht muß stets ein **überwiegendes** berechtigtes **materielles** Interesse sein, weshalb etwa ein Bescheidungsanspruch nach § 171 StPO des nicht verletzten Stellers eines Antrags auf Erhebung einer öffentlichen Klage nicht ausreicht.

   - Grundsätzlich muß die Erteilung von Auskünften Vorrang vor der Gewährung von Akteneinsicht haben.

   - Der Akteneinsicht Begehrende hat sein berechtigtes Interesse daran so darzulegen und zu begründen, daß erkennbar ist, welche in der Ermittlungsakte enthaltenen Informationen von dem berechtigten Interesse an der Übermittlung umfaßt werden.

   - Die Akteneinsicht ist grundsätzlich auf diejenigen Aktenteile zu beschränken, für deren Kenntnisnahme ein berechtigtes Interesse nachvollziehbar dargelegt ist.

   - Besonders sensible Daten enthaltende Aktenteile sollten besonders geheftet werden, damit Gericht und Staatsanwaltschaft in die Lage versetzt werden, im Einzelfall die Zulässigkeit der Offenbarung dieser Daten im Wege der Akteneinsicht be-

sonders prüfen zu können.

- Durch strafbewehrte Zweckbindungsregelungen soll Vorsorge dagegen getroffen werden, daß die durch Akteneinsicht gewonnenen Informationen für sachfremde Zwecke mißbraucht werden.

Zu der dringend notwendigen gesetzlichen Regelung des Akteneinsichtsrechts habe ich anstatt des der bisherigen Praxis entsprechenden "berechtigten Interesses" ein **rechtliches** Interesse an der Einsichtnahme gefordert. D.h., es soll nicht mehr jedes anzuerkennende wirtschaftliche oder sonstige Interesse zur Gewährung der Einsichtnahme ausreichen; notwendig ist vielmehr ein rechtliches Interesse, z.B. zur Begründung eines Schadensersatz- oder sonstigen Anspruchs.

2. Auch ein von der Konferenz der Datenschutzbeauftragten des Bundes und der Länder zustimmend zur Kenntnis genommenes Forderungspapier zur Regelung der Öffentlichkeitsfahndung im Strafverfahren habe ich dem Justizminister übersandt mit der Bitte um Berücksichtigung bei Maßnahmen der Öffentlichkeitsfahndung. Kernpunkte des Papiers sind Forderungen nach

   - strikter Ausrichtung der Voraussetzungen einer öffentlichen Fahndung am Verhältnismäßigkeitsgrundsatz, insbesondere bei der Fahndung nach Zeugen,

   - grundsätzlichem Richtervorbehalt für Maßnahmen öffentlicher Fahndung bis zum Abschluß des strafrechtlichen Erkenntnisverfahrens,

   - Aufnahme von Maßnahmen der öffentlichen Fahndung in den Katalog der entschädigungspflichtigen Strafverfolgungsmaßnahmen des § 2 Abs. 2 des Gesetzes über die Entschädigung für Strafverfolgungsmaßnahmen.

   Der Justizminister sieht die bestehenden Verwaltungsvorschriften für die öffentliche Fahndung als ausreichend an und hält eine gesetzliche Regelung nicht für erforderlich. Die Angelegenheit wurde auf der letzten Sitzung des Ausschusses der Justizministerkonferenz "Richtlinien für das Strafverfahren und das Bußgeldverfahren" erörtert. Eine Änderung der Richtlinien wurde leider nicht für erforderlich gehalten.

Ich werde mich dafür einsetzen, daß die o.g. datenschutzrechtlichen Anliegen im weiteren Gesetzgebungsverfahren zu einem Strafverfahrensänderungsgesetz berücksichtigt werden.

3. Schließlich habe ich normenklare gesetzliche Regelungen für die Aufbewahrung, Aussonderung und Vernichtung von Akten und die Speicherung personenbezogener Daten durch Gerichte, Staatsanwaltschaften und Strafvollzugsbehörden gefordert. Ich habe dazu dem Staatsministerium der Justiz die Entschließung der 49. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 09./10. März 1995 zu "Aufbewahrungsbestimmungen und Dateiregelungen im Justizbereich" (vgl. Anlage 6) übersandt.

Die Entschließung geht zurück auf den datenschutzrechtlichen Befund, daß der Gesetzgeber im Bereich der Justiz den verfassungsrechtlichen Anforderungen nach ausreichenden normenklaren Regelungen über die Aufbewahrung von Akten und die Speicherung personenbezogener Daten in Dateien bisher nicht nachgekommen ist. Notwendig erscheint es, die Aufbewahrung, Aussonderung und Vernichtung der Akten und die Speicherung personenbezogener Daten in Dateien im Bereich der Justiz nach den Grundsätzen des Bundesverfassungsgerichts im sog. Volkszählungsurteil für die Gerichte, Staatsanwaltschaften und Strafvollzugsbehörden gesetzlich zu regeln, wobei sich die Aufbewahrungsdauer am Recht auf informationelle Selbstbestimmung einerseits und am Zweck der Speicherung andererseits zu orientieren hat. Dabei sollte der Gesetzgeber die grundlegenden Entscheidungen zur Aufbewahrungsdauer selbst treffen. Einzelheiten können durch Rechtsverordnung bestimmt werden. Die bestehenden Aufbewahrungsfristen sind konsequent zu vereinfachen und soweit sachlich vertretbar zu verkürzen.

Vorsorglich habe ich darauf hingewiesen, daß es nicht akzeptabel wäre, wenn eine gesetzliche Regelung wegen Fragen der Gesetzgebungszuständigkeit (Bundeskompetenz für Strafverfahrensrecht/Landeskompetenz für Gerichtsverwaltungsangelegenheiten) zurückgestellt würde.

Mittlerweile sind die Aufbewahrungsbestimmungen für das Schriftgut der ordentlichen Gerichtsbarkeit, der Staatsanwaltschaften und der Justizvollzugsbehörden, die derzeit maßgebliche

---

Verwaltungsvorschrift für die Aufbewahrung des Schriftguts, in zahlreichen Punkten geändert worden. Vielfach wurden dabei auch Verkürzungen der Aufbewahrungsdauer vorgenommen. Das Anliegen einer gesetzlichen Regelung der Aufbewahrung besteht jedoch unverändert fort.

Das Gesetzesvorhaben war bei Redaktionsschluß noch nicht abgeschlossen.

7.1.2 Justizmitteilungsgesetz

Nach längeren Vorarbeiten hatte die Bundesregierung am 31. August 1992 den Entwurf eines Gesetzes über Mitteilungen der Justiz von Amts wegen in Zivil- und Strafsachen (Justizmitteilungsgesetz - JuMiG) in den Bundestag eingebracht (siehe dazu 14. Tätigkeitsbericht 1992, Nr. 6.1.1). Dieser Gesetzentwurf sollte endlich die Rechtsgrundlage für die zahlreichen Übermittlungen sensibler personenbezogener Daten schaffen, die bisher lediglich auf der Grundlage bundeseinheitlicher Verwaltungsvorschriften (Anordnungen über Mitteilungen in Zivilsachen - MiZi - und Mitteilungen in Strafsachen - MiStra) vorgenommen werden. Da der Entwurf nicht weiterbehandelt wurde, ist er zwischenzeitlich der Diskontinuität verfallen. Mittlerweile wurde der Entwurf - in veränderter Form - am 13. Dezember 1995 erneut von der Bundesregierung beschlossen.

Ich habe meine Auffassung zu den vorgesehenen gesetzlichen Regelungen gegenüber dem Staatsministerium der Justiz in zwei ausführlichen Schreiben zum Ausdruck gebracht und dabei ausdrücklich den Fortgang der Gesetzgebungsarbeiten begrüßt. Darüber hinaus hat sich auf meine Initiative hin die Konferenz der Datenschutzbeauftragten des Bundes und der Länder mit einem Schreiben vom 13. November 1995 an die Vorsitzende der Justizministerkonferenz gewandt und zentrale datenschutzrechtliche Anliegen formuliert.

Der Gesetzentwurf bleibt vor allem in folgenden Punkten hinter den datenschutzrechtlichen Anforderungen zurück:

7.1.2.1 Anordnungskompetenz

Die Regelung des Entwurfs 1992, nach der die Anordnungskompetenz für Mitteilungen in bestimmten Fällen dem Richter, Staatsanwalt oder Rechtspfleger vorbehalten war, wurde ersatzlos gestrichen.

Dies halte ich nicht für sachgerecht. In Fällen, in denen es einer besonders sorgfältigen Abwägung und/oder juristischen Bewertung bedarf, sollte die Entscheidung über die Vornahme einer Mitteilung dem Richter, Staatsanwalt oder Beamten des gehobenen Justizdienstes vorbehalten bleiben. Da solche Mitteilungen erhebliche Auswirkungen für den Betroffenen haben können und schwierige Abwägungsvorgänge voraussetzen, sehe ich in der Streichung des o.g. Entscheidungsvorbehalts einen deutlichen Rückschritt im Hinblick auf die Wahrung des Rechts auf informationelle Selbstbestimmung.

Darüber hinaus findet sich im Entwurf keine Regelung mehr, in welchen Fällen auch die Begründung einer Entscheidung übermittelt werden darf. Aus meiner Sicht sollte diese Bestimmung als Ausprägung des allgemeinen Grundsatzes, daß Mitteilungen nur im Rahmen des Erforderlichen statthaft sind, wieder aufgenommen werden.

7.1.2.2 Benachrichtigung des Betroffenen

Im Entwurf 1992 war vorgesehen, daß der von der Datenübermittlung Betroffene gleichzeitig mit der Übermittlung von Amts wegen über deren Inhalt und Adressaten zu unterrichten ist. Demgegenüber soll dem Betroffenen oder seinem gesetzlichen Vertreter nunmehr - von Ausnahmen abgesehen - lediglich **auf Antrag** Auskunft darüber erteilt werden.

In diesem Zusammenhang habe ich nachdrücklich darauf hingewiesen, daß auf eine Benachrichtigung von Amts wegen nur verzichtet werden kann, wenn für den Bürger aufgrund der Rechtsnormen zu ersehen ist, daß und welche Daten zu welchen Zwecken übermittelt werden. Dazu müßten die Übermittlungspflichten im Gesetz so konkret geregelt sein, daß der Bürger **im Einzelfall** erkennen kann, ob und in welchem Umfang er von einer Datenübermittlung betroffen sein kann. Diese Voraussetzungen sehe ich durch den vorliegenden Entwurf nicht erfüllt, da die vorgesehenen Bestimmungen lediglich einen Rahmen abstecken, innerhalb dessen Mitteilungen **erfolgen dürfen**. Zur Regelung der Frage, in welchen Fällen oder für welche Fallgruppen Mitteilungen tatsächlich zu erfolgen haben, sollen ergänzend Verwaltungsvorschriften erlassen werden. Dies genügt jedoch nicht, da der Bürger aus dem Gesetz selbst nicht entnehmen kann, ob in seinem Fall eine Mitteilung erfolgt.

Es sollte deshalb an einer Unterrichtung des Betroffenen von Amts wegen festgehalten werden.

7.1.2.3 Datenübermittlung im Bereich besonderer Schutzvorschriften

Zur Lösung des Spannungsverhältnisses zwischen Steuergeheimnis, Sozialgeheimnis, ärztlicher Schweigepflicht und Mitteilungen, vor allem an den Dienstherrn bzw. die Anstellungsbehörde habe ich datenschutzkonforme gesetzliche Regelungen gefordert, die der Bedeutung der speziellen Geheimhaltungsvorschriften in ausreichendem Maße Rechnung tragen. Insoweit sehe ich noch Nachbesserungsbedarf:

So erklärt der Entwurf die Offenbarung von dem Steuergeheimnis unterliegenden Daten bei Beamten ausdrücklich für zulässig. Demgegenüber enthält der Entwurf für Arbeiter und Angestellte im öffentlichen Dienst eine solche Befugnis nicht. Eine Übermittlung von geschützten Steuerdaten wäre bei dieser Personengruppe daher nur nach den strengeren Kriterien des § 30 Abs. 4 Nr. 5 Abgabenordnung (AO), das heißt bei Vorliegen eines zwingenden öffentlichen Interesses, zulässig. Ein solches "zwingendes öffentliches Interesse" dürfte allerdings nur in Fällen schwerer Kriminalität angenommen werden können.

Mir erscheint es fraglich, ob diese Ungleichbehandlung von Beamten und Angestellten/Arbeitern, deren Tätigkeit vielfach vergleichbar ist, allein aufgrund ihres unterschiedlichen Status (besondere Treuepflicht des Beamten nach §§ 35, 36 Beamtenrechtsrahmengesetz - BRRG) gerechtfertigt ist. Dieselbe Problematik stellt sich bei der vorgesehenen Regelung der Übermittlung von Sozialdaten. Nach dem Entwurf ist die Übermittlung lediglich bei Beamten zulässig, nicht jedoch bei Angestellten und Arbeitern des öffentlichen Dienstes.

Das Gesetzesvorhaben war bei Redaktionsschluß noch nicht abgeschlossen.

7.1.3 Viertes Gesetz zur Änderung des Strafvollzugsgesetzes

Nachdem ein Vorentwurf aus dem Jahre 1991 nicht weiterverfolgt worden war, liegt nunmehr ein überarbeiteter Referentenentwurf eines Vierten Gesetzes zur Änderung des Strafvollzugsgesetzes vor.

Der Gesetzentwurf verfolgt entsprechend den Vorgaben des Bundesverfassungsgerichts im sog. Volkszählungsurteil vom 15. Dezember 1983 in erster Linie das Ziel, im Strafvollzugsgesetz bereichsspezifische Rechtsgrundlagen für die Erhebung, Verarbeitung und Nutzung personenbezogener Daten zu schaffen.

Ich habe gegenüber dem Staatsministerium der Justiz zu dem Referentenentwurf Stellung genommen. Zwar konnte ich feststellen, daß der nunmehr vorliegende, überarbeitete Entwurf im Vergleich zu dem Vorentwurf datenschutzrechtliche Verbesserungen aufweist, die aber in einzelnen Punkten noch nicht ausreichend sind:

- In den Regelungsbereich des § 29 Abs. 2, der Schreiben des Gefangenen an bestimmte Institutionen von der Briefkontrolle ausnimmt, sollen nunmehr auch die Datenschutzbeauftragten des Bundes und der Länder einbezogen werden. Dies ist zu begrüßen. Jedoch sollten auch die Antwortschreiben der aufgeführten Stellen an den Gefangenen von einer Überwachung jedenfalls dann ausgenommen werden, wenn die Identität des Absenders zweifelsfrei festgestellt werden kann.

- Unter Berücksichtigung der zentralen Bedeutung der Gefangenenpersonalakte sollten im Gesetz Regelungen zum Begriff, Inhalt sowie Gliederung und Gestaltung der Akten aufgenommen werden.

- In die Schweigepflicht gegenüber der Vollzugsanstalt sollte nicht nur der Anstaltsarzt, sondern auch die Berufspsychologen oder Sozialarbeiter der Anstalt einbezogen werden.

- Nicht nur Gesundheitsakten und Krankenblätter sollten getrennt von der Gefangenenpersonalakte geführt und besonders gesichert werden, sondern auch andere, besonders sensible

personenbezogene Daten enthaltende Vorgänge wie etwa Unterlagen über psychologische oder sozialtherapeutische Behandlungen sowie Erkenntnisse aus der Überprüfung von Besuchern oder der Briefkontrolle.

- Die im Entwurf vorgesehenen Aufbewahrungsfristen von 30 Jahren (für Gefangenenpersonalakten, Gesundheitsakten und Krankenblätter) und 50 Jahren (für Gefangenenbücher) sollten verkürzt werden. Diese Verkürzung sollte aber nicht Verwaltungsvorschriften der Landesjustizverwaltungen überlassen werden. Vielmehr sollte die Aufbewahrung vom Gesetzgeber selbst entschieden werden. Soweit sich die 30-jährige Aufbewahrungsdauer im Interesse des Strafgefangenen an der Verjährungsfrist des § 195 BGB orientiert, sollte dem Betroffenen die Möglichkeit gegeben werden, die Vernichtung der Unterlagen bereits zu einem früheren Zeitpunkt zu beantragen. Für eine 50-jährige Aufbewahrung der Gefangenenbücher sehe ich kein Erfordernis. Darüber hinaus sollte vorgegeben werden, daß die Gefangenenbücher jahrgangsweise geführt werden, damit die Dauer der Speicherung personenbezogener Daten nicht auch wesentlich vom Umfang des Buches und dem Zeitpunkt der Eintragung abhängt.

- Es sollte klargestellt werden, daß auch die Bestimmungen der Landesdatenschutzgesetze über die Kontrolle durch die Landesbeauftragten für den Datenschutz unberührt bleiben, nachdem der Entwurf bisher eine solche Regelung nur im Hinblick auf Schadensersatz-, Straf- und Bußgeldvorschriften enthält.

Das Gesetzesvorhaben war bei Redaktionsschluß noch nicht abgeschlossen.

7.1.4 Referentenentwurf eines Gesetzes zur Reform des Kindschaftsrechts

Im Zusammenhang mit diesem Gesetzentwurf habe ich mich mit folgendem an das Staatsministerium der Justiz gewandt:

In Art. 6 Ziff. 2 des Entwurfs ist vorgesehen, § 35 a des Gesetzes über die freiwillige Gerichtsbarkeit dahingehend zu ergänzen, daß Gerichte und Behörden dem Vormundschafts- oder Familiengericht personenbezogene Daten übermitteln dürfen, wenn deren Kenntnis aus ihrer Sicht für vormundschafts- oder familiengerichtliche Maßnahmen erforderlich ist und soweit nicht für die übermittelnde Stelle erkennbar ist, daß schutzwürdige Interessen des Betroffenen an dem Ausschluß der Übermittlung das Schutzbedürfnis eines Minderjährigen oder Betreuten oder das öffentliche Interesse an der Übermittlung überwiegen. Die Übermittlung soll dann unterbleiben, wenn **besondere bundesgesetzliche oder entsprechende landesgesetzliche Verwendungsregelungen** entgegenstehen.

Insoweit sehe ich ein Schutzbedürfnis vor allem in Fällen, in denen der Betroffene den Träger eines Berufsgeheimnisses nur für ein bestimmtes gerichtliches oder behördliches Verfahren von der Schweigepflicht entbunden hat und gerade diese Daten an das Familiengericht oder Vormundschaftsgericht übermittelt werden sollen.

Da Art. 22 Bayerisches Datenschutzgesetz und § 39 Bundesdatenschutzgesetz nicht als "besondere Verwendungsregelungen" des Entwurfs anzusehen sein dürften, sollte der Gesetzgeber klarstellen, daß personenbezogene Daten, die einem Berufs- oder besonderen Amtsgeheimnis unterliegen und dem Gericht bzw. der Behörde vom Verschwiegenheitsverpflichteten befugt übermittelt wurden, einer besonderen Zweckbindung unterliegen.

Das Gesetzesvorhaben war bei Redaktionsschluß noch nicht abgeschlossen.

7.1.5 Entwurf eines Zweiten Gesetzes zur Entlastung der Rechtspflege (strafrechtlicher Bereich)

Nach Ziff. 45 des Entwurfs sollen die Straftatbestände des § 201 Abs. 1 und Abs. 2 StGB (Verletzung der Vertraulichkeit des Wortes) in den Katalog der **Privatklagedelikte** des § 374 StPO aufgenommen werden. Das Privatklageverfahren ist nach § 374 Abs. 1 StPO bei bestimmten leichten Vergehen zulässig, die die Allgemeinheit in der Regel wenig berühren. Die Staatsanwaltschaft verfolgt Privatklagedelikte nur, wenn dies im öffentlichen Interesse liegt (§ 376 StPO).

Aus datenschutzrechtlicher Sicht kommt der unbeobachteten Kommunikation, der Vertraulichkeit des Wortes ein hoher Stellenwert zu. Ihr Schutz verdient - auch im Interesse der Allgemeinheit und nicht zuletzt wegen der verbesserten technischen Abhörmöglichkeiten - besondere Beachtung. Die Einbeziehung in den Katalog der Privatklagedelikte wird dem nicht gerecht. Dagegen spricht auch die Höhe der Strafdrohung, die immerhin eine Freiheitsstrafe von bis zu drei Jahren beträgt.

Ich habe das Staatsministerium der Justiz gebeten, mein diesbezügliches Anliegen zu unterstützen.

Das Gesetzesvorhaben war bei Redaktionsschluß noch nicht abgeschlossen.

7.2 Automatisierte Datenverarbeitung bei Staatsanwaltschaften

7.2.1 Geschäftsstellenautomationsverfahren für Staatsanwaltschaften SIJUS-STRAF-STA

In meinem 15. Tätigkeitsbericht (Nr. 6.4.1) habe ich ausführlich über das bislang im Probebetrieb (mit Echtdaten) eingesetzte Geschäftsstellensystem für Staatsanwaltschaften SIJUS-STRAF-STA berichtet.

Zwischenzeitlich hat das Staatsministerium der Justiz mit Datum vom 26. April 1995 die Freigabe des automatisierten Verfahrens gemäß Art. 26 Abs. 1 Satz 1 BayDSG verfügt. Darüber hinaus hat das Justizministerium mir im Frühjahr 1996 den Entwurf einer Dienstanweisung für das Verfahren SIJUS-STRAF-STA mit der Bitte um Stellungnahme übersandt.

Ich habe zum Entwurf der Dienstanweisung eingehend Stellung genommen und dabei neben Anforderungen zur Datensicherheit vor allem darauf hingewiesen, daß

- die wesentlichen Aktivitäten des Systemverwalters vollständig und überschreibungssicher aufgezeichnet werden sollen,

- die wesentlichen Zugriffe auf den SIJUS-Datenbestand - auch hinsichtlich der Art - (Anmeldeversuch, kopieren, löschen, eintragen, verändern), protokolliert werden,

- die Zugriffsrechte der verschiedenen Nutzer (z.B. Staatsanwälte, Geschäftsstellen, Rechtspfleger) festgelegt werden,

- bei Verfahren, in denen der Tatverdacht gegen den Betroffenen entfallen ist oder in denen nicht (mehr) von einer strafbaren Handlung ausgegangen wird, sichergestellt werden sollte, daß die Personen- und Verfahrensdaten nur noch zu Zwecken der Vorgangsverwaltung genutzt werden können. Dies könnte etwa dadurch gewährleistet werden, daß solche Verfahren besonders gekennzeichnet werden und der Zugriff auf so gekennzeichnete Verfahren nur den Beschäftigten der Registratur möglich ist. Insbesondere sollte sichergestellt sein, daß solche Verfahren nicht mehr in Verfahrenslisten aufgenommen werden. Personen- und Verfahrensdaten, die nur noch zu Zwecken der Vorgangsverwaltung gespeichert werden, könnten ent-

sprechend behandelt werden.

Mittlerweile hat das Staatsministerium der Justiz die Dienstanweisung als Verwaltungsvorschrift erlassen und dabei meine Anregungen in einigen Punkten aufgegriffen, in anderen ein Erfordernis für Änderungen nicht gesehen:

So soll das vom Systemverwalter geführte sog. Logbuch als Nachweis für Tätigkeit und Eingaben des Systemverwalters ausreichen, eine systemtechnische Protokollierung der einzelnen Aktivitäten des Systemverwalters wird (weiterhin) nicht für erforderlich gehalten. Hinsichtlich einer Protokollierung der Zugriffe auf den SIJUS-Datenbestand weist das Justizministerium darauf hin, daß automatisch der jeweils letzte Zugriff auf einen Datensatz mit Datum und Benutzerkennung im jeweiligen Datensatz aufgezeichnet wird. Eine Dokumentation früherer Zugriffe sei nicht geboten. Darüber hinaus machten Aufzeichnungen aller Einzelzugriffe auf jeden Datensatz und die Aufbewahrung entsprechender Daten zusätzliche Festplatten- und Hauptspeicherkapazitäten sowie zusätzliche Auswertungsprogramme erforderlich, deren Kosten die "Wirtschaftlichkeit des Gesamtverfahrens" stark beeinträchtigen würden. Auch je nach Funktion und Zuständigkeit differenzierte Zugriffs- bzw. Bearbeitungsrechte werden vom Justizministerium abgelehnt. Dabei wird u.a. darauf verwiesen, daß im Justizbereich zur Steigerung der Effizienz sog. Service-Teams mit Mischarbeitsplätzen eingerichtet würden. Generelle Aussagen über Zugriffs- und Bearbeitungsrechte bestimmter Mitarbeitergruppen würden eine wünschenswerte Änderung der Organisation im vorgenannten Sinne mit dem Ziel einer Steigerung der Leistungsfähigkeit einer Behörde erschweren oder gar unmöglich machen. Über eine - technisch mögliche - Einschränkung von Rechten müsse deshalb die jeweilige Behörde anhand der konkreten Ablauforganisation entscheiden.

Eine Arbeitsgruppe der Datenschutzbeauftragten des Bundes und der Länder zum Thema "Datenschutzrechtliche Forderungen zum Einsatz von staatsanwaltschaftlichen Informationssystemen" hat sich unter meiner Mitwirkung mit grundlegenden datenschutzrechtlichen Forderungen aus juristischer und technischer Sicht befaßt. Ich werde mich nach Vorliegen entsprechender Ergebnisse erneut mit dem Justizministerium in Verbindung setzen.

7.2.2 Aufbau eines zentralen staatsanwaltschaftlichen Verfahrensregisters in Bayern (STARIS - vormals: BAYSIS)

Bereits in meinem 16. Tätigkeitsbericht (Nr. 7.2.3) habe ich ausführlich über die Konzeption des Staatsministeriums der Justiz für den Aufbau eines zentralen staatsanwaltschaftlichen Verfahrensregisters auf Landesebene berichtet. Dieses Register soll nunmehr unter der Bezeichnung "STARIS" realisiert werden.

Das Staatsministerium der Justiz hält weiterhin an der Auffassung fest, daß die allgemeinen Bestimmungen des Bayerischen Datenschutzgesetzes i.V.m. dem Strafverfolgungsauftrag der Strafprozeßordnung eine hinreichende Rechtsgrundlage für das beabsichtigte Datenverarbeitungssystem darstellen und hat dazu eine unterstützende Stellungnahme des Staatsministeriums des Innern vorgelegt.

Unter Berücksichtigung der Rechtsprechung des Bundesverfassungsgerichts halte ich nach wie vor daran fest, daß vor Inbetriebnahme eines solchen **landesweiten** Verfahrensregisters eine bereichsspezifische gesetzliche Grundlage erforderlich ist, in der der Gesetzgeber gerade diese Art der Datenverarbeitung für zulässig erklärt.

Nachdem der Bundesgesetzgeber im Verbrechensbekämpfungsgesetz die rechtlichen Grundlagen für ein **bundesweites** staatsanwaltschaftliches Informationssystem geschaffen hat, in dem auch die dort vorgesehenen personenbezogenen Daten "bayerischer Verfahren" eingestellt und entsprechende Auskünfte u.a. an die Staatsanwaltschaften erteilt werden, habe ich dem Justizministerium mitgeteilt, daß ich von einer **förmlichen Beanstandung** für den Fall einer Aufnahme des Betriebs von STARIS mit Echtdaten absehen werde, **soweit Art und Umfang der in STARIS gespeicherten personenbezogenen Daten und die Auswertungsmöglichkeiten in diesem System nicht über das bundesweite Informationssystem hinausgehen**.

Mittlerweile hat mir das Justizministerium dargelegt, daß Art und Umfang der in STARIS gespeicherten Daten nicht über den in § 474 Abs. 2 Strafprozeßordnung für das bundesweite Register vorgegebenen Rahmen hinausgehen. Es hat mir nach einem längeren Schriftwechsel nunmehr auch mitgeteilt, daß jedenfalls vorläufig in Anlehnung an § 476 Abs. 2 Satz 2 Strafprozeßordnung statt der bislang für STARIS vorgesehenen Regellöschungsfrist von fünf Jahren von

einer zwei-jährigen Löschungsfrist ausgegangen wird.

7.3 Kontrollen im Justizbereich

7.3.1 Kontrolle einer Staatsanwaltschaft

Im Berichtszeitraum habe ich eine Staatsanwaltschaft geprüft, bei der das automatisierte Geschäftsstellenverfahren SIJUS-STRAF-STA eingesetzt wird. Schwerpunkte dieser Prüfung waren die Aktualisierung des Tatvorwurfs entsprechend dem Ermittlungsfortgang und die Übernahme von Altverfahren in SIJUS-STRAF-STA, sowie die Gewährung von Akteneinsicht an Nichtverfahrensbeteiligte und die Mitteilungen in Strafsachen.

Gravierende Verstöße gegen den Datenschutz habe ich nicht festgestellt. Folgende Punkte habe ich jedoch gegenüber dem Staatsministerium der Justiz und der Staatsanwaltschaft aufgegriffen:

7.3.1.1 Aktualisierung des Tatvorwurfs in SIJUS-STRAF-STA entsprechend dem Ermittlungsfortgang

In SIJUS-STRAF-STA wird im Bereich der sog. personenbezogenen Verfahrensdaten u.a. der Tatvorwurf gegen den Beschuldigten unter Angabe der Strafvorschrift aufgeführt. Anhand zahlreicher Ermittlungsverfahren wegen Vergewaltigung, Totschlags und räuberischen Diebstahls wurde überprüft, ob bei einer **wesentlichen** Änderung des Tatvorwurfs im Zuge der staatsanwaltschaftlichen Ermittlungen eine entsprechende Korrektur der Speicherung stattgefunden hat.

In einem der Verfahren lautete der Tatvorwurf bei Abschluß der polizeilichen Ermittlungen "versuchte Vergewaltigung". Anklage war wegen "sexueller Nötigung" erhoben worden. Eine solche Änderung halte ich nicht für so wesentlich, daß eine Berichtigung des Tatvorwurfs in SIJUS-STRAF-STA erforderlich gewesen wäre.

Anderes gilt im Falle eines weiteren Ermittlungsverfahrens. Hier wurde dem Beschuldigten in der polizeilichen Anzeige "räuberischer Diebstahl" vorgeworfen. Angeklagt wurde er in der Folge jedoch nur wegen "einfachen Diebstahls". In SIJUS-STRAF-STA war weiterhin "räuberischer Diebstahl" als Tatvorwurf erfaßt. Insoweit bin ich der Auffassung, daß es einer Korrektur des Tatvorwurfs bedurft hätte, da sich die vorgenannten Straftatbestände erheblich unterscheiden: Während der Diebstahl nach § 242 Strafgesetzbuch (StGB) ein Vergehen ist, das mit Freiheitsstrafe bis zu fünf Jahren oder mit Geldstrafe sanktioniert ist, stellt der räuberische Diebstahl nach § 252 StGB ein Verbrechen dar, das mit einer Freiheitsstrafe von nicht unter einem Jahr bedroht ist. Neben einer Änderung des Tatvorwurfs in SIJUS-STRAF-STA sollte in solchen Fällen auch der auf dem Aktendeckel angebrachte Tatvorwurf (zumindest handschriftlich) entsprechend korrigiert werden.

Mittlerweile hat mir das Staatsministerium der Justiz eine Dienstanweisung für den Einsatz des Programmsystems SIJUS-STRAF-STA übermittelt, die hierzu vorschreibt, daß bei wesentlichen Änderungen des Tatvorwurfs im Zuge des staatsanwaltschaftlichen Ermittlungsverfahrens die ursprüngliche Bezeichnung in SIJUS-STRAF-STA **unverzüglich, spätestens zum Zeitpunkt der staatsanwaltschaftlichen Erledigung (z.B. bei Anklageerhebung), zu berichtigen ist**. Damit verbunden ist nach Mitteilung des Justizministeriums eine Aktualisierung des auf dem

Aktendeckel vermerkten Tatvorwurfs.

Damit ist den datenschutzrechtlichen Anforderungen Rechnung getragen.

7.3.1.2 Überprüfung von Mitteilungen in Strafsachen

Anhand von etwa 20 Ermittlungsverfahren gegen "Lehrer", "Beamte" und "Soldaten" wurden die Mitteilungen an den Dienstherrn überprüft. In allen Fällen waren die Voraussetzungen der Nr. 15 bzw. Nr. 20 der Anordnung über Mitteilungen in Strafsachen (MiStra) vom 15. März 1985 erfüllt. Die gesetzliche Grundlage für die derzeit noch aufgrund von Verwaltungsvorschriften vorgenommenen Mitteilungen wird derzeit im Zuge der Gesetzgebungsarbeiten zu einem Justizmitteilungsgesetz geschaffen.

Ob die gefertigten Mitteilungen den Voraussetzungen der Nr. 15 Abs. 3 MiStra (Adressierung an den Leiter der Behörde oder seinen Vertreter im Amt und Kennzeichnung als "Vertrauliche Personalsache") entsprachen, konnte nur überprüft werden, soweit der sachbearbeitende Staatsanwalt selbst die genaue Adressierung und Kennzeichnung verfügt hatte. Dies war bei den überprüften Akten jedoch häufig nicht der Fall.

Angesichts der Sensibilität der Mitteilung erscheint es aus datenschutzrechtlicher Sicht wünschenswert, wenn zum Zwecke der späteren Nachvollziehbarkeit eine Durchschrift der Mitteilung bei den Ermittlungsakten verbliebe oder doch zumindest die genaue Adressierung aus der Akte ersichtlich wäre.

Das Justizministerium hat dazu mitgeteilt, daß es grundsätzlich meinem Anliegen offen gegenübersteht. Es verweist in diesem Zusammenhang auf die mögliche Einführung EDV-gestützter Mitteilungen, bei denen in den Textbausteinen standardisierte Empfängerangaben vorgegeben werden, wodurch die Adressierung nachvollziehbar und damit überprüfbar würde.

Die Umsetzung dieser Verbesserungen bleibt abzuwarten. Ich werde den Fortgang der Angelegenheit im Auge behalten.

7.3.2 Kontrolle von Justizvollzugsanstalten

Im Berichtszeitraum habe ich in zwei Justizvollzugsanstalten eine datenschutzrechtliche Prüfung durchgeführt. In beiden Fällen konnte ich feststellen, daß sich die Anstalten der hohen Bedeutung des Datenschutzes bewußt sind. Schwerwiegende datenschutzrechtliche Mängel konnten nicht festgestellt werden.

Schwerpunkt meiner Kontrollen waren folgende Bereiche:

7.3.2.1 Aktenverwaltung

Im Hinblick auf meine Ausführungen im 16. Tätigkeitsbericht (Nr. 7.3.3.1) und die Erfahrungen von Kollegen bei der Prüfung außerbayerischer Justizvollzugsanstalten galt mein besonderes Augenmerk der Frage, inwieweit personenbezogene Daten aus der Gefangenenpersonalakte bzw. dem sog. A-Bogen den Vollzugsangehörigen allgemein zugänglich sind bzw. nur übermittelt bzw. zugänglich gemacht werden, soweit dies zur konkreten Aufgabenerfüllung erforderlich ist.

7.3.2.2 Gefangenenpersonalakten

In beiden Anstalten mußte ich feststellen, daß die Gefangenenpersonalakten in der Vollzugsgeschäftsstelle zwar sicher in verschließbaren Aktenschränken verwahrt werden, jedoch (weiterhin) undifferenziert jedem Vollzugsbediensteten zugänglich sind, ohne daß der Datenzugriff dokumentiert wird. Das von den Anstalten im Interesse der Aktenkontrolle geführte Fehlblatt, in das nur die Mitnahme der Akte eingetragen wird, stellt keine ausreichende Dokumentation dar.

Ich halte diesbezüglich an meiner Auffassung fest, daß zur Vorbeugung vor mißbräuchlichen Zugriffen, aber auch im Interesse einer späteren Nachvollziehbarkeit sowohl die Entnahme von als auch die Einsichtnahme in Gefangenenpersonalakten auf der Geschäftsstelle unter Angabe von Datum, Handzeichen bzw. Unterschrift und Entnahme-/Einsichtsgrund dokumentiert werden, sofern der Zugriff nicht durch die Anstaltsleitung oder das Geschäftsstellenpersonal erfolgt. Da das Justizministerium eine solche Dokumentation weiterhin u.a. wegen des damit verbundenen Verwaltungsaufwands ablehnt, habe ich den Beirat (nochmals) mit der Problematik befaßt. Der Beiratsvorsitzende hat die im Beirat vertretenen Landtagsabgeordneten gebeten, das Thema

mit den Anstaltsbeiräten zu erörtern.

7.3.2.3 Behandlung "sensibler" Unterlagen

Angehaltene Briefe des Gefangenen werden in verschlossenem Umschlag zum Personalakt des Gefangenen genommen, falls sie Bedeutung als Beweismittel haben können. Ansonsten werden die Briefe zur Habe des Gefangenen genommen. Die Leiter beider Anstalten gaben dazu an, daß solche Briefanhaltungen jedoch mit Blick auf die jüngere Rechtsprechung des Bundesverfassungsgerichts (Schutz der Privatsphäre auch bei Briefüberwachung, bei Beleidigungen weniger Kundgabecharakter als Akt der Selbstentfaltung) sehr selten vorkämen.

Von einer der Anstalten wurde darüber hinaus mitgeteilt, daß Berichte von Fachdiensten (Sozialarbeiter, Psychologen, Lehrer, Psychiater) grundsätzlich nicht zur Gefangenenpersonalakte genommen, sondern beim jeweiligen Fachbediensteten aufbewahrt würden. Dies gelte insbesondere für die sog. Sozialberichte, die zu den Krankenakten des Gefangenen genommen würden.

Datenschutzrechtliche Einwendungen sind hiergegen nicht zu erheben. Es muß jedoch sichergestellt sein, daß die Unterlagen der Fachdienste - soweit sie nicht zur Gefangenenpersonalakte genommen werden - spätestens nach Entlassung des Gefangenen vernichtet werden.

7.3.2.4 Übermittlung der Daten des sog. A-Bogens

Nach Mitteilung einer Anstalt werden sämtliche im Personalblatt (sog. A-Bogen) enthaltenen Daten an insgesamt 16 verschiedene Stellen der Anstalt (beispielsweise Sozialarbeiter, Psychologen, Psychiater, Anstaltsgeistlicher, Arbeitsbetrieb usw.) übermittelt.

Es wurde nicht dargetan, weshalb jede der angesprochenen Stellen der Justizvollzugsanstalt **sämtliche Daten des A-Bogens** (wie beispielsweise Bekenntnis, Name und Wohnung der nächsten Angehörigen, erlernter Beruf bzw. ausgeübte Tätigkeit, Zahl der Vorstrafen bzw. früheren Maßregeln) für die jeweilige Aufgabenerfüllung benötigt. Die zahlreichen Daten des A-Bogens sollten an die einzelnen Stellen der Anstalt nur in dem Umfang übermittelt werden, in dem sie für die Sachbearbeitung tatsächlich benötigt werden.

7.3.2.5 Führung einer "Sicherheitsliste" und besondere Vermerke auf dem Personalblatt

In einer der Anstalten wird eine sog. "Sicherheitsliste" geführt, die monatlich fortgeschrieben wird. Ablichtungen dieser Sicherheitsliste befinden sich auf den Stationen und beim Hausdienstleiter. Die Entscheidung über die Aufnahme eines Gefangenen in die Sicherheitsliste trifft der Anstaltsleiter (bei Zugang des Gefangenen) oder der Abteilungsleiter. Unmittelbare Folge der Aufnahme eines Gefangenen in die Liste sei lediglich das Gebot besonderer Vorsicht für die Bediensteten. Weitere Folgen, z.B. verstärkte oder häufigere Haftraumkontrollen, seien damit nicht verbunden. Kriterien für die Aufnahme in die Sicherheitsliste seien etwa vorangegangene Entweichungen, Entweichungsversuche oder Suizidgefährdung. Die Vorexemplare der monatlich neu aufgelegten Sicherheitsliste würden noch zwei Jahre lang aufbewahrt. Dies habe den Zweck, auch im nachhinein noch nachvollziehen zu können, ob beispielsweise zu einem bestimmten Zeitpunkt bei einem Gefangenen erkennbar Selbstmordgefahr bestanden habe oder bei späteren besonderen Vorkommnissen festzustellen, wann und weshalb der Gefangene von der Sicherheitsliste gestrichen worden sei.

Gegen die Führung einer solchen Sicherheitsliste bestanden nach Grund und Umfang keine Bedenken. Eine stichprobenartige Überprüfung von Eintragungen in der Sicherheitsliste anhand der Gefangenenpersonalakten ergab stets den erforderlichen Aktenrückhalt. Die Notwendigkeit der Aufbewahrung der alten Sicherheitslisten für etwa zwei Jahre wurde von der Anstalt nachvollziehbar begründet.

7.3.2.6 Datenübermittlungen an Dritte

Der praktisch wichtigste Fall betrifft Anfragen von Vollstreckungsgläubigern die wissen wollen, ob der Vollstreckungsschuldner in der Anstalt einsitzt und wann er entlassen wird.

In beiden Justizvollzugsanstalten wird zunächst der Strafgefangene befragt, ob er mit der Erteilung einer Auskunft einverstanden ist. Ist dies der Fall oder hat der Vollstrekkungsgläubiger ein berechtigtes Interesse nachgewiesen, so wird ihm Auskunft erteilt. Dabei wird der **voraussichtliche Entlassungstermin** nur angegeben, wenn die Entlassung binnen eines Monats bevorsteht. Von einer Anstalt wurde ergänzend mitgeteilt, daß bei bereits entlassenen Gefangenen lediglich der neue Wohnort (falls bekannt) und nicht die vollständige Entlassungsanschrift angegeben werde. Wegen weiterer Daten werde an die Meldebehörde verwiesen. Bei beiden Anstalten werden die Unterlagen des Auskunftsvorgangs sodann zum Gefangenenpersonalakt genommen.

Es ist datenschutzrechtlich zu begrüßen, daß grundsätzlich vor einer Auskunftserteilung der Gefangene wegen seines Einverständnisses gefragt wird, daß bei entlassenen Gefangenen wegen der genauen Anschrift auf die zuständigen Meldebehörden verwiesen wird und daß die erteilte Auskunft durch Beinahme eines Doppels zur Akte dokumentiert bleibt. Ich gehe dabei davon aus, daß vor einer Übermittlung von Schuldnerdaten ohne Einverständnis des Schuldners geprüft wird, ob dieser kein schutzwürdiges Interesse an dem Ausschluß der Übermittlung hat (Art. 19 Abs. 1 Nr. 2 BayDSG). Soweit von einer der geprüften Anstalten bei entlassenen Gefangenen der neue Wohnort bekanntgegeben wird, habe ich um Prüfung und Stellungnahme gebeten, ob nicht auch insoweit auf die Meldebehörde verwiesen werden kann. Eine Antwort hierzu liegt mir noch nicht vor.

Eine stichprobenartige Überprüfung der erteilten Auskünfte ergab keinen Anlaß zur Beanstandung.

Nach Mitteilung des Leiters einer Anstalt gehen dort in unregelmäßigen Abständen Anfragen von in der Anstalt als Kind einer Strafgefangenen geborenen Personen ein, die nähere Einzelheiten zu ihrer Abstammung wissen wollen. Auf Vorlage von Personalausweis und Geburtsurkunde werde dem Abkömmling beispielsweise dahingehend Auskunft erteilt, wie alt die Mutter

zur Zeit der Geburt des Kindes gewesen sei, wann die Mutter geboren sei, ob das Kind selbst im Krankenhaus oder in der Anstalt geboren sei, ob es getauft sei und schließlich auch, weshalb die Mutter eingesessen sei. Soweit daneben nach dem Vater gefragt würde, sei beispielsweise mitgeteilt worden, daß es sich bei ihm nach Angaben der Mutter um einen amerikanischen Soldaten gehandelt habe.

Datenschutzrechtlich sind solche Vorgänge wie folgt zu bewerten:

Soweit nicht nur Daten des anfragenden Kindes, sondern auch personenbezogene Daten der Eltern, insbesondere der Mutter, übermittelt werden, richtet sich die Zulässigkeit der Datenübermittlung mangels spezialgesetzlicher Regelungen nach Art. 19 Abs. 1 BayDSG. Dabei wird eine Übermittlung nach Art. 19 Abs. 1 Nr. 2 BayDSG in der Regel nur zulässig sein, wenn (hier) die anfragende Person ein berechtigtes Interesse an der Kenntnis der zu übermittelnden Daten glaubhaft darlegt **und der Betroffene kein schutzwürdiges Interesse an dem Ausschluß der Übermittlung hat**.

Demnach kann die Übermittlung von Daten eines Elternteils mangels entgegenstehenden schutzwürdigen Interesses dann in Betracht kommen, wenn dieser Elternteil bereits gestorben ist. Lebt hingegen der von einer Datenübermittlung betroffene Elternteil noch, so wird man nicht ohne weiteres annehmen können, daß er kein schutzwürdiges Interesse an dem Ausschluß der Datenübermittlung hat. Insbesondere werden häufiger Fälle vorkommen, in denen der von einer Datenübermittlung Betroffene bewußt den Kontakt zu seinem Abkömmling abgebrochen hat oder seine Vergangenheit ihm gegenüber nicht offenbaren will. In solchen Fällen sollten daher ohne das Einverständnis des Betroffenen keine personenbezogenen Daten übermittelt werden.

7.3.2.7 Anstaltsführungen

Nach Mitteilung einer Anstalt werden Führungen im wesentlichen nur noch für beruflich interessierte Personen durchgeführt. Derzeit fänden ca. 15 solcher Führungen pro Jahr statt. Diese würden vorher angekündigt, die Gefangenen der von der Führung möglicherweise betroffenen Häuser bzw. Arbeitsstätten würden zuvor informiert und könnten sich dadurch der Führung entziehen. Es werde stets ein im voraus bestimmter Haftraum besichtigt und die betroffenen Gefangenen bereits vor der Führung gefragt, ob sie mit einer solchen Besichtigung einverstanden sind. Die Bitte um Entfernung des Haftraumschildes vor einer Anstaltsführung habe noch kein Gefangener vorgebracht. Es sollte den Gefangenen - jedenfalls auf Wunsch - die Möglichkeit eingeräumt werden, die Haftraumschilder bei Besuchen abzudecken oder abdecken zu lassen.

In der anderen Anstalt finden Führungen nach Mitteilung des Leiters vor allem für beruflich Interessierte wie z.B. Rechtsreferendare, Polizeianwärter, Staatsanwälte, Richter usw. statt. Darüber hinaus würden in Einzelfällen auch Schulklassen (vor allem im Zusammenhang mit dem Sozialkundeunterricht) zum Besuch zugelassen. Für Schulklassen werde allerdings in der Regel nur ein kurzer Gang durch eines der Häuser angeboten, daran schließe sich eine Diskussion im Vortragsraum der Anstalt an. Das Verfahren bei Anstaltsführungen gehe dahin, daß **Führungen nur während der Arbeitszeit** der Gefangenen durchgeführt werden, weil sich die Gefangenen in dieser Zeit entweder im Arbeitsbetrieb aufhalten oder eingeschlossen seien. Ein Kontakt zwischen Besuchern und Gefangenen sei daher nur im Arbeitsbereich oder bei einzelnen Gefangenen, die in der Anstalt unterwegs sind, möglich. Die Besucher dürften nicht in belegte Hafträume sehen. Mit Rücksicht auf diese Form der Führungen erfolge keine vorherige allgemeine Information über die anstehende Führung im Haus, zumal sich Begegnungen im Einzelfall ohnehin nicht vermeiden ließen. Bei Besichtigung eines Arbeitsbetriebs werde der dort Diensthabende bei Eintreffen der Besuchergruppe informiert.

Soweit die Führungen nur während der Arbeitszeit stattfinden, erscheint es aus Datenschutzsicht hinnehmbar, wenn die Gefangenen des betroffenen Hauses nicht vorab informiert werden. Anderes gilt jedoch hinsichtlich der Gefangenen in den Arbeitsbetrieben. Nach den Bekundungen einer dort Diensthabenden ist eine Vorab-Information bei Führungen in der Vergangenheit nicht immer erfolgt. Künftig sollten die in den Arbeitsbetrieben dieser Anstalt eingesetzten Strafge-

fangenen so **rechtzeitig vor Eintreffen einer Besuchergruppe** informiert werden, daß sie die Möglichkeit haben, sich den Blicken der Besucher zu entziehen bzw. sich zumindest abzuwenden.

7.3.2.8 Belehrung nach § 86 Abs. 3 Satz 2 Strafvollzugsgesetz

Nach § 86 Abs. 3 Satz 2 Strafvollzugsgesetz sind die Gefangenen spätestens bei der Entlassung über ihr Recht auf Vernichtung der erkennungsdienstlichen Unterlagen nach Vollstreckung der richterlichen Entscheidung zu belehren. Nachdem eine solche Belehrung bislang einheitlich nur beim Zugang der Gefangenen erfolgt ist, habe ich gegenüber dem Justizministerium zur Verbesserung des Datenschutzes vorgeschlagen, daß jedenfalls bei Gefangenen mit nicht nur kurzen Haftstrafen eine erneute Belehrung vor bzw. bei Entlassung aus dem Strafvollzug stattfinden sollte. Eine diesbezügliche Anweisung an die bayerischen Justizvollzugsanstalten hat mir das Justizministerium mit Schreiben vom 04.10.1995 mitgeteilt.

Gleichwohl mußte ich bei der Prüfung einer Anstalt feststellen, daß dort nur bei der Zugangsverhandlung über den Vernichtungsanspruch belehrt wird. Die Anstaltsleitung hat diesbezüglich Abhilfe zugesagt.

7.3.2.9 Nicht zeitgerechte Aktenaussonderung

Nach den Bestimmungen über die Aufbewahrungsfristen für das Schriftgut der ordentlichen Gerichtsbarkeit, der Staatsanwaltschaften und der Justizvollzugsbehörden sind Gefangenenbücher und Gefangenenkarteien 30 Jahre, Personalakten der Gefangenen über den Vollzug von Untersuchungshaft, Zivilhaft, Strafarrest, Erzwingungshaft sowie von Freiheitsstrafen von bis zu sechs Monaten 15 Jahre lang und Personalakten der Gefangenen im übrigen 30 Jahre lang aufzubewahren.

Daran gemessen bestanden in beiden geprüften Justizvollzugsanstalten erhebliche Rückstände bei der Aussonderung. Im einen Fall waren Gefangenenbücher bis ca. 1905/1906 und die Gefangenenkartei bis ins Jahr 1941 noch aufbewahrt, im anderen Falle wurden Gefangenenpersonalakten der Jahrgänge 1933 bis 1945 erst im Jahre 1993 dem Staatsarchiv angeboten. Beide Anstalten habe ich daher angehalten, künftig um eine zeitgerechte Aussonderung besorgt zu sein.

7.3.2.10 Besucherüberprüfung

Im 16. Tätigkeitsbericht (Nr. 7.9.5) habe ich darüber berichtet, daß eine polizeiliche Überprüfung der von Gefangenen auf die Besucherliste gesetzten Personen **ohne deren Wissen** nicht mehr stattfindet.

Mittlerweile verwenden die bayerischen Justizvollzugsanstalten ein Formblatt "Erklärung für die Zulassung zum Besuch", in dem die vom Gefangenen benannten Personen ihre Besuchsabsicht erklären können. Darüber hinaus ist die Angabe der Personalien mit evtl. ergänzenden Bemerkungen, wie beispielsweise die Art der Beziehung zum Gefangenen möglich. Schließlich kann in dem Formblatt das Einverständnis mit der Einholung von Auskünften über die Eignung als Besucher bei der zuständigen Polizeidienststelle/Staatsanwaltschaft/Verwaltungsbehörde und mit deren Verwertung im Rahmen des Verfahrens über die Genehmigung des Besuchsantrags erfolgen. Ziff. 4 des Formblatts endet mit den Worten: "Die Erteilung des Einverständnisses ist eine Voraussetzung für die Genehmigung eines Besuchsantrages."

Bei der Beurteilung dieses Verfahrens bin ich bisher davon ausgegangen, daß das Formblatt nur solchen Personen vorgelegt wird, bei denen **Anlaß zur Überprüfung** besteht und eine solche Überprüfung nur durchgeführt wird, sofern die benannte Person den Gefangenen auch besuchen will. Mittlerweile ist mir jedoch die Stellungnahme der betroffenen Justizvollzugsanstalt zur Eingabe eines Strafgefangenen zugegangen, aus der sich ergibt, daß das Formblatt grundsätzlich allen vom Gefangenen als Besucher benannten Personen zugeleitet wird. Eine Entscheidung darüber, ob der Besucher tatsächlich zu überprüfen ist, werde nach Rücklauf des Formblatts und Prüfung des konkreten Einzelfalles getroffen, wobei auch die Angaben auf dem Formblatt, wie z.B. die Art der Beziehung zum Gefangenen, berücksichtigt würden. Nahe Angehörige des Gefangenen und Personen, bei denen aufgrund sonstiger Erkenntnisse keine Zweifel an ihrer Eignung als Besucher bestehen, werden nach Mitteilung der Anstalt grundsätzlich nicht überprüft. Trotzdem wird auch ihnen das Formblatt zugeleitet.

Ich habe datenschutzrechtliche Bedenken, das Einverständnis mit der Erholung und Verwertung von Auskünften bei der Polizei/Staatsanwaltschaft/Verwaltungsbehörde zu verlangen und das Einverständnis als "Voraussetzung für die Genehmigung des Besuchsantrages" zu bezeichnen,

obwohl erst die spätere Prüfung durch die Justizvollzugsanstalt ergeben soll, ob eine Überprüfung des Besuchers tatsächlich notwendig ist.

- Ich halte daher bei Personen, bei denen nicht von vornherein die Notwendigkeit einer Überprüfung feststeht, ein "zweistufiges Verfahren" für geboten:
  Zunächst sollte lediglich erfragt werden, ob der Benannte beabsichtigt, den Gefangenen in der Justizvollzugsanstalt zu besuchen und ihm Gelegenheit zu ergänzenden Bemerkungen gegeben werden.
- Erst wenn diese Frage bejaht wird und wirklich Anlaß zu einer Überprüfung hinsichtlich der Eignung als Besucher besteht, sollte das Einverständnis mit der Erholung von Auskünften verlangt werden.

In diesem Sinne habe ich mich an das Bayerische Staatsministerium der Justiz und die Leitung der betroffenen Justizvollzugsanstalt gewandt.

7.3.2.11 Namensschilder im Arbeitsbetrieb einer Justizvollzugsanstalt

Ein Strafgefangener hat sich an mich gewandt und vorgetragen, daß sich für jeden sichtbar im Eingangsbereich des Arbeitsbetriebs seiner Anstalt Standtafeln mit den Namensschildern der dort eingesetzten Strafgefangenen befänden. Diese Tafeln würden auch vor Anstaltsführungen durch diesen Arbeitsbetrieb nicht entfernt, so daß auch "justizfremde" Personen die Namensschilder der Inhaftierten lesen könnten und ein "Mißbrauch" nicht auszuschließen sei. Hierdurch sieht sich der Strafgefangene in seinen Rechten verletzt und fordert Abhilfe durch Entfernung der Namensschilder vor einer Anstaltsführung.

Die Leitung der Justizvollzugsanstalt nahm zunächst dahingehend Stellung, daß die auf den Schildern angebrachten Namen einem konkreten Strafgefangenen nicht zugeordnet werden könnten und ein Abhängen der Schilder vor jeder Führung einen nicht unerheblichen Aufwand verursachen würde.

Daraufhin habe ich die Anstalt um Prüfung gebeten, ob dem datenschutzrechtlichen Anliegen dadurch entsprochen werden könnte, daß die Standtafeln vor einer Besichtigung des Arbeitsbetriebs - etwa durch Verhängen mit einem Tuch - abgedeckt werden.

Inzwischen hat mir der Leiter der Justizvollzugsanstalt mitgeteilt, daß entsprechend meiner Anregung künftig die Standtafeln vor einer Besichtigung des Arbeitsbetriebs abgedeckt werden.

7.3.2.12 Auskünfte einer Justizvollzugsanstalt über einen Strafgefangenen nach dessen Haftentlassung

Ein ehemaliger Strafgefangener einer Justizvollzugsanstalt bat mich um Überprüfung des folgenden Sachverhalts:

Ein Rechtsanwalt hatte sich im Jahre 1989 schriftlich an die Justizvollzugsanstalt gewandt und mitgeteilt, daß sein Mandant in Mietvertragsverhandlungen mit dem Petenten stehe. Der Petent habe erklärt, er sei gut situiert und im Ostblockhandel tätig, andererseits habe er jedoch die fällige Mietkaution und eine Monatsmiete nicht bezahlt. Darüber hinaus habe ein unbekannter Anrufer seinem Mandanten erklärt, daß es sich beim Petenten um einen "erst vor kurzem aus der Haftanstalt entlassenen Hochstapler" handele. Mit dieser Begründung hatte der Rechtsanwalt des Vermieters um Mitteilung gebeten, ob der Petent in der betreffenden Justizvollzugsanstalt in Haft gewesen sei, bzw. wann er entlassen worden sei. Die betreffende Justizvollzugsanstalt teilte dem Rechtsanwalt des Vermieters mit Kurznachricht mit, wann der Petent aus der Strafhaft entlassen worden war.

Die Erteilung der Auskunft widersprach dem Datenschutzrecht. Nach Art. 18 Abs. 1 BayDSG in der 1989 noch geltenden alten Fassung durfte die Justizvollzugsanstalt Auskunft nur erteilen, "soweit der Empfänger ein berechtigtes Interesse an der Kenntnis der zu übermittelnden Daten glaubhaft macht und dadurch schutzwürdige Belange des Betroffenen nicht beeinträchtigt werden". Auch die Neufassung des Bayerischen Datenschutzgesetzes enthält im wesentlichen die gleiche Regelung (vgl. Art. 19 Abs. 1 Nr. 2). Die Voraussetzungen für die hier vorgenommene Datenübermittlung waren nicht erfüllt. Zwar kann auch das Interesse eines Vermieters, seinen Mietzins pünktlich und vollständig zu erhalten, ein berechtigtes Interesse im Sinne der vorgenannten Bestimmung darstellen. Jedoch wurde durch die Mitteilung des Entlassungszeitpunkts und die damit verbundene Bestätigung, daß der Petent in Haft war, dessen Recht auf informationelle Selbstbestimmung beeinträchtigt. Bei Abwägung zwischen den Interessen des Vermieters an der Kenntnis, ob sich der Petent tatsächlich in Haft befunden hatte, und dem Interesse des Petenten an der Geheimhaltung des Haftaufenthalts durfte die Anstalt nicht ohne weiteres davon ausgehen, daß das Informationsinteresse des Vermieters überwog. Vielmehr hätte sich der Vermieter durch Vorlage von Einkommensnachweisen oder ähnlichen Unterlagen von der wirt-

schaftlichen Leistungsfähigkeit des Petenten ein Bild machen und die ihm aufgrund der konkreten Situation erforderlich erscheinenden Entscheidungen treffen können.

Diese Beurteilung habe ich der Justizvollzugsanstalt mitgeteilt, wegen der seit der Auskunft verstrichenen Zeit und der hier nicht einfach zu ziehenden Zulässigkeitsgrenze aber von einer Beanstandung abgesehen.

7.3.3 Informations- und Prüfungsbesuch bei der Industrie- und Handelskammer für München und Oberbayern

Die Neufassung der Vorschriften über das Schuldnerverzeichnis in der Zivilprozeßordnung (§§ 915 ff. ZPO) und das Inkrafttreten der Schuldnerverzeichnisverordnung (SchuVVO) vom 15. Dezember 1994 habe ich zum Anlaß genommen, im Berichtszeitraum der Industrie- und Handelskammer für München und Oberbayern als Vertreterin der Arbeitsgemeinschaft der bayerischen Industrie- und Handelskammern einen Informations- und Prüfungsbesuch abzustatten. Dieser sollte der Feststellung dienen, ob die Industrie- und Handelskammer für München und Oberbayern ihren datenschutzrechtlichen Verpflichtungen als Bezieherin von Abdrucken aus dem Schuldnerverzeichnis und verantwortliche Erstellerin von Schuldnerlisten nachkommt. Der Schwerpunkt lag dabei auf der Beurteilung der

7.3.3.1 Auftragsdatenverarbeitung durch den Verband der Vereine Creditreform e.V. in Neuss

Die Industrie- und Handelskammer für München und Oberbayern hat - auch in Vertretung der übrigen bayerischen Industrie- und Handelskammern - Erstellung und Vertrieb der sog. Schuldnerlisten vertraglich auf den Verband der Vereine Creditreform e.V. in Neuss übertragen.

Eine solche Übertragung der Erstellung von Schuldnerlisten auf Dritte wird in § 915 e Abs. 3 Satz 1, letzter Halbsatz ZPO für zulässig erklärt, die hier getroffene Auswahl des Auftragnehmers entspricht den Erfordernissen des Art. 6 Abs. 2 Satz 1 BayDSG.

7.3.3.2 Beurteilung des schriftlichen Vertrags über die Auftragsdatenverarbeitung

In dem von der Industrie- und Handelskammer vorgelegten schriftlichen Vertrag, der den datenschutzrechtlichen Anforderungen im übrigen entspricht, waren weder die zu treffenden technisch-organisatorischen Maßnahmen geregelt, noch Regelungen über eine Begründung bzw. den Ausschluß von Unterauftragsverhältnissen enthalten. Nach Art. 6 Abs. 2 Satz 2 BayDSG müssen jedoch solche Regelungen **im Vertrag** über die Auftragsdatenverarbeitung **selbst getroffen werden**.

Die Industrie- und Handelskammer hat das Fehlen von vorgeschriebenen Regelungsinhalten damit erklärt, daß die vorgenannten Fragen einvernehmlich bereits vor Vertragsabschluß besprochen worden seien und daher gleichsam als "Geschäftsgrundlage" vorausgesetzt worden seien. Mittlerweile hat die Industrie- und Handelskammer eine Ergänzung der vertraglichen Regelungen zugesagt und mir dazu den Entwurf einer "Ergänzungsvereinbarung" vorgelegt, der den datenschutzrechtlichen Anforderungen in vollem Umfang entspricht.

7.3.3.3 Kontrolle der Auftragsdatenverarbeitung

Nach § 915 e Abs. 3 Satz 2 ZPO hat im Falle der Erstellung der Schuldnerlisten durch Dritte der Auftraggeber den Dritten zu beaufsichtigen. Nach Auskunft der Industrie- und Handelskammer seien dazu Kontrollbesuche beim Verband der Vereine Creditreform e.V. in Neuss beabsichtigt.

Eine Überprüfung der vom Verband der Vereine Creditreform e.V. an die Industrie- und Handelskammer übersandten Listen bzw. Löschungsmitteilungen ist nach der derzeitigen Verfahrensgestaltung nur sehr eingeschränkt möglich, da die zuständige Mitarbeiterin alle eingehenden Abdrucke aus dem Schuldnerverzeichnis im Original sofort an den Auftragnehmer nach Neuss zur Bearbeitung übersendet. Ablichtungen werden nicht zurückbehalten. Die Sachbearbeiterin bei der Industrie- und Handelskammer kann daher nur eine Durchsicht der erstellten Listen und Löschungsmitteilungen nach formalen Kriterien vornehmen.
Im Interesse einer effektiven Beaufsichtigung des Auftragnehmers habe ich gefordert, daß neben Kontrollbesuchen beim Verband der Vereine Creditreform e.V. in Neuss die übersandten Listen bzw. Löschungsmitteilungen als Produkt der Auftragsdatenverarbeitung zumindest stichproben-

artig daraufhin überprüft werden sollten, ob die personenbezogenen Schuldnerdaten richtig verarbeitet wurden.

Die Industrie- und Handelskammer führt nunmehr entsprechend meinem Anliegen stichprobenartige Überprüfungen der übersandten Schuldnerlisten durch. Die Sachbearbeiterin kopiert dazu einige der von den Amtsgerichten übersandten Mitteilungen. Anhand dieser Kopien wird die richtige Bearbeitung der personenbezogenen Daten in der jeweiligen Schuldnerliste überprüft. Die von den Mitteilungen der Amtsgerichte gefertigten Kopien werden nach der Überprüfung vernichtet.

Hiermit wird den gesetzlichen Vorgaben entsprochen.

7.4 Zugriffe der Strafverfolgungsbehörden im Bereich der Telekommunikation

7.4.1 Staatliche Eingriffsbefugnisse in der modernen Informationsgesellschaft

Die tiefgreifende Entwicklung der modernen Telekommunikation (insbesondere durch Privatisierung der Netze, weite Verbreitung von Mobilfunkgeräten, Digitalisierung der Kommunikation), die rasche Fortentwicklung und weltweit vernetzte Nutzung der Informationstechnologie zu Kommunikationszwecken (z.B. Mailboxen, Internet) und Zwecken der Informations- und Güterbeschaffung (z.B. Online-Datenbanken, Tele-Shopping) sowie die neuen Medien lassen die traditionellen Grenzen zwischen Medien-, Kommunikations- und Informationstechnik verschwinden und führen - jedenfalls tendenziell - zu einem grundlegend veränderten Kommunikationsverhalten des Bürgers. Traditionelle Büroarbeiten werden über Tele-Working Gegenstand digitalisierter Übertragungen und damit überwachbar, Tele-Banking begründet die Überwachbarkeit von Banktransaktionen, Tele-Shopping kann zu einem transparenten Konsumverhalten führen, die Nutzung von Fernsehen mit Rückkanal oder der Informationsangebote von Rundfunk und Fernsehen im Internet führen zur Nachvollziehbarkeit der Mediennutzung.

Mit der Entwicklung hin zur "Informationsgesellschaft" gehen jedoch auch Gefahren durch die Nutzung der neuen Technik zu kriminellen Zwecken einher.

Es ist deshalb nicht nur legitim, sondern geboten, daß die Strafverfolgungsbehörden in die Lage versetzt werden, ihre gesetzlichen Überwachungs- und Zugriffsrechte wahrzunehmen.

Die dahingehenden gesetzgeberischen und technischen Anstrengungen dürfen jedoch aus datenschutzrechtlicher Sicht nicht zur Folge haben, daß in die Grundrechte der Bürger, insbesondere in ihr informationelles Selbstbestimmungsrecht, aber auch in das Fernmeldegeheimnis und das Recht auf unbeobachtete Kommunikation mehr eingegriffen wird, als unabdingbar erforderlich.

Die 52. Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat am 22./23. Oktober 1996 Thesen beschlossen, deren Beachtung notwendig ist, damit auch bei Nutzung der neuen Techniken die verfassungsrechtlich garantierten Freiräume des einzelnen erhalten bleiben. Dabei geht es im wesentlichen um folgende Forderungen:

---

1. Keine ungeprüfte Übertragung der herkömmlichen Eingriffsbefugnisse unter wesentlich veränderten Bedingungen auf die neuen Formen der Individual- und Massenkommunikation.

2. Vorrang der "spurenlosen Kommunikation", das heißt Wahl von Verfahren, die den Telekommunikationsteilnehmern ein Höchstmaß an Anonymität gegenüber Netzbetreibern und Dienstleistungsanbietern sichern.

3. Ersetzung des § 12 Fernmeldeanlagengesetz durch eine neue normenklare gesetzliche Regelung in der Strafprozeßordnung, die dem Verhältnismäßigkeitsgrundsatz auch unter den neuen Bedingungen, insbesondere der zunehmenden Bedeutung von Verbindungs- und Bestandsdaten für das Persönlichkeitsrecht des Betroffenen Rechnung trägt.

4. Dem Grundsatz der unbeobachteten Information kommt zur Sicherung eines demokratischen Gemeinwesens besondere Bedeutung zu. Ein Eingriff in dieses Grundrecht wäre nur im überwiegenden Allgemeininteresse unter besonderer Wahrung des Verhältnismäßigkeitsgrundsatzes zulässig. Seiner Bedeutung muß auch durch restriktive Anwendung der Eingriffsbefugnisnormen Rechnung getragen werden.

5. Strafprozessuale Zugriffsbeschränkungen zum Schutz besonderer Vertrauensverhältnisse (z.B. Arztgeheimnis, anwaltliches Vertrauensverhältnis usw.) dürfen - bei einer digitalisierten Informationsverarbeitung wie etwa bei "ausgelagerten" digitalisierten Speicherungen - nicht dadurch entwertet werden, daß die Anwendbarkeit der Beschlagnahme und Durchsuchungsverbote der Strafprozeßordnung vom traditionellen "Gewahrsam" des Zeugnisverweigerungsberechtigten abhängig gemacht wird.

6. Die Möglichkeit, Kommunikation durch geeignete Maßnahmen (z.B. Verschlüsselung) vor fremden Zugriffen zu schützen, ist ein herkömmliches Freiheitsrecht des Bürgers. Andererseits muß das Interesse des Staates anerkannt werden, sich rechtlich zulässige Zugriffsmöglichkeiten nicht dadurch versperren zu lassen, daß Verschlüsselungen zur Anwendung kommen, zu denen er keinen Zugriff hat. Ein umfassendes, den privaten Nutzer bindendes Verschlüsselungsverbot der digitalisierten Kommunikation ist aus Da-

tenschutzsicht nicht akzeptabel.

7. Die Kommunikation innerhalb von privat, nichtwirtschaftlich genutzten lokalen Netzen, die über öffentliche Leitungen zu erreichen sind (z.B. die familiäre häusliche Kommunikation zwischen Nebenstellen) ist wie bisher von Überwachungsmaßnahmen auszunehmen.

8. Aufzeichnung der sog. "Aktivmeldungen" von Mobiltelefonen nur, soweit dies zum Zwecke der Strafverfolgung unerläßlich sein sollte. Eine dem Verhältnismäßigkeitsgrundsatz entsprechende gesetzliche Regelung, die auch den besonders geregelten Vertrauensverhältnissen (Arztgeheimnis, Anwaltsgeheimnis usw.) Rechnung trägt, ist erforderlich (siehe dazu im einzelnen den folgenden Beitrag).

7.4.2 Erstellung sog. "Bewegungsprofile" auf der Grundlage von "Aktivmeldungen" der Funktelefone

Bei Mobilfunktelefonen ist es - entsprechende technische Ausgestaltung vorausgesetzt - wie oben angedeutet möglich, den Aufenthaltsbereich eines Mobilfunkteilnehmers nicht nur in den Fällen festzustellen, in denen ein Telefongespräch geführt wird, sondern bereits dann, wenn der Anschluß durch Einstecken der Chipkarte in den Mobilfunkapparat "aktiv gemeldet" ist. Aufgrund so gewonnener Aufenthaltsdaten läßt sich ein sog. "Bewegungsbild" erstellen.

Auf entsprechende Anfrage hat das Staatsministerium der Justiz die Auffassung vertreten, eine Erfassung und Auswertung der "Aktivmeldungen" zum Zwecke der Strafverfolgung sei - unbeschadet einer künftigen gesetzlichen Klarstellung - bereits jetzt durch § 100 c Abs. 1 Ziff. 1 b StPO (Einsatz technischer Mittel) gedeckt.

Im Gegensatz dazu besteht meiner Auffassung nach eine gesetzliche Grundlage für einen solchen strafprozessualen Eingriff in das Recht auf informationelle Selbstbestimmung nicht. Die Zulässigkeit ihres Einsatzes ist deshalb derzeit höchst fraglich. Sowohl § 100 a StPO als auch § 12 Fernmeldeanlagengesetz setzen voraus, daß "Fernmeldeverkehr" stattfindet. Demgegenüber findet bei bloßen Bereitschaftsmeldungen der Funktelefone gerade noch kein Fernmeldeverkehr statt. Die Aktivmeldungen dienen vielmehr lediglich der Aufrechterhaltung der Gesprächs**bereitschaft**. Auch von § 100 c Abs. 1 Ziff. 1 b StPO ist die Erfassung von Aufenthaltsdaten m.E. nicht gedeckt. Wie bereits der Wortlaut dieser Vorschrift zeigt, sind davon nur "besondere für Observationszwecke bestimmte technische Mittel" wie etwa Peilsender, Nachtsichtgeräte, Bewegungsmelder u.ä. erfaßt. Demgegenüber dienen die Aktivmeldungen der Mobilfunktelefone nicht Observationszwecken, sondern der Bereitstellung der Telekommunikationsdienstleistung.

Diese Auffassung habe ich dem Justizministerium mitgeteilt.

7.4.3 Verbesserung der Praxis der Telefonüberwachung

Im Berichtszeitraum habe ich mich durch einen mehrstündigen Informationsbesuch bei einem Großstadtpräsidium der Polizei über die Praxis der Überwachung des Fernmeldeverkehrs informiert. Nach eingehenden Beratungen mit Vertretern anderer Datenschutzbeauftragter habe ich mich mit den folgenden Möglichkeiten zu datenschutzrechtlichen Verbesserungen in diesem Bereich an das Staatsministerium der Justiz gewandt:

1. **Anordnung der Telefonüberwachung durch ein Kollegialgericht**

   Entscheidung über Anträge auf Telefonüberwachung statt - wie bisher - durch den Ermittlungsrichter beim Amtsgericht - durch ein Kollegialgericht. Dadurch würde eine gründlichere, vor allem aber kontroversere Prüfung der Eingriffsvoraussetzungen gewährleistet.

2. **Begründungszwang**

   Aufnahme von Vorgaben für die Begründung der Anordnung der Überwachung des Fernmeldeverkehrs in § 100 b StPO (Darstellung der Tatsachen, die den Verdacht nach § 100 a Abs. 1 StPO begründen; Darlegung, warum die Erforschung des Sachverhalts auf andere Weise aussichtslos oder wesentlich erschwert wäre; bei Verlängerungen: Darlegung, warum unter Berücksichtigung der gewonnenen Erkenntnisse eine Verlängerung weitere oder erstmalige Erfolge verspricht).

3. **Beginn und Ende der Aufzeichnung**

   Sicherstellung, daß die Aufzeichnung nicht schon beginnt, wenn der Hörer des überwachten Telefonanschlusses abgehoben wird (Abhören sog. Raumgespräche), sondern erst dann, wenn zwischen den Teilnehmern Telekommunikation stattfindet. Dies ist erst dann der Fall, wenn beide Gesprächsteilnehmer den Telefonhörer abgehoben haben.

4. **Dauer der Telefonüberwachung**

   Verkürzung der Höchstfrist des § 100 b Abs. 2 StPO von drei Monaten auf einen Monat. Dadurch würden Staatsanwaltschaft und Gericht gezwungen, öfter zu prüfen, ob die Fort-

führung der Maßnahme noch erforderlich ist. Nach meinen Erkenntnissen wird bisher regelmäßig die Höchstfrist angeordnet.

5. **Schutz von Verteidigergesprächen**

Gewährleistung eines ausreichenden Schutzes von sog. Verteidigergesprächen (§ 148 StPO) entweder durch elektronische Unterdrückung oder Kennzeichnung von Gesprächsbeginn und Gesprächsende und Sperrung dieser Gespräche.

6. **Benachrichtigung der Beteiligten**

Klarstellung in § 101 StPO, daß "Beteiligte" im Sinne des Abs. 1 nicht nur der Beschuldigte und die in § 100 a Abs. 2 genannten Personen sind, sondern auch diejenigen, die die überwachten Fernmeldegespräche geführt haben und deren Identität bekannt ist.

7. **Erfolgskontrolle**

Auswertung der Überwachungsmaßnahmen im Hinblick auf ihren Erfolg. In einen entsprechenden Bericht könnten insbesondere Angaben über den Anlaß der Telefonüberwachung, die Dauer der Maßnahme, die Anzahl der überwachten Anschlüsse, den betroffenen Personenkreis sowie die Anzahl der ermittelten, verurteilten, aber auch der entlasteten Personen einbezogen werden.

8. **Präventive Nutzung von Erkenntnissen aus der Telefonüberwachung**

Gesetzliche Regelung der Verwendung von Erkenntnissen aus der Überwachung des Fernmeldeverkehrs zu präventiven Zwecken in der Strafprozeßordnung.

Das Staatsministerium der Justiz sieht im wesentlichen keinen Anlaß für Änderungen der Praxis der Telefonüberwachung. Zu der von mir vorgeschlagenen Auswertung der Überwachungsmaßnahmen im Hinblick auf deren Erfolg vertritt das Justizministerium die Auffassung, daß eine solche Erfolgskontrolle mit den für die Strafverfolgung zur Verfügung stehenden Ressourcen keinesfalls zu leisten sei und verweist darüber hinaus auf "methodische Probleme" (u.a.: Schwie-

rigkeiten bei der Zuordnung des Erfolgs zu einer bestimmten Ermittlungsmaßnahme). Zwischenzeitlich wurden die vom Strafrechtsausschuß der Justizministerkonferenz erarbeiteten statistischen Erhebungsformulare für Telefonüberwachungsmaßnahmen von den Landesjustizverwaltungen ohne die unterbreiteten datenschutzrechtlichen Vorschläge zur Ergänzung in Kraft gesetzt. Darüber hinaus sieht das Telekommunikationsgesetz nunmehr vor, daß die nach den §§ 100 a, 100 b der Strafprozeßordnung verpflichteten Betreiber von Telekommunikationsanlagen eine **Jahresstatistik** über die nach diesen Vorschriften durchgeführten Überwachungsmaßnahmen zu erstellen und der Regulierungsbehörde unentgeltlich zur Verfügung zu stellen haben.

Ich würde eine Umsetzung meiner weitergehenden Vorschläge aus Gründen der Verbesserung des Schutzes des Rechts auf Privatheit nach wie vor begrüßen.

Bezüglich einer gesetzlichen Regelung der präventiv-polizeilichen Nutzung von Erkenntnissen aus der Überwachung des Fernmeldeverkehrs verweist das Justizministerium darauf, daß diese "sehr komplexe Angelegenheit" im Zusammenhang mit dem Bundesratsentwurf eines Strafverfahrensänderungsgesetzes 1994 erörtert werde.

7.4.4 Mitteilung von weiteren Betroffenen einer Telefonüberwachungsmaßnahme

Ein Petent hat sich an mich gewandt mit der Bitte um Überprüfung einer gegen ihn durchgeführten Telefonüberwachungsmaßnahme. U.a. hat mir der Petent eine an ihn gerichtete Benachrichtigung der Staatsanwaltschaft über die getroffene Maßnahme in Ablichtung übersandt. In diesem Schreiben sind die Nachnamen und Telefonnummern von zwei weiteren Personen aufgeführt, gegen die eine Überwachung des Fernmeldeverkehrs stattgefunden hatte.

Die betroffene Staatsanwaltschaft hat eingeräumt, daß es fehlerhaft war, in der Benachrichtigung die Daten weiterer von der Telefonüberwachung betroffener Personen aufzuführen und dies mit einem Versehen der Geschäftsstelle begründet.

Meine Überprüfung ergab, daß offensichtlich die Verfügung des sachbearbeitenden Staatsanwalts (getrennte Mitteilungen an die von der Telefonüberwachung betroffenen Personen) dahingehend mißverstanden worden war, daß in den Mitteilungen jeweils alle drei betroffenen Telefonanschlüsse aufgeführt werden sollten. Ich habe die Staatsanwaltschaft auf diesen Fehler hingewiesen und sie aufgefordert, darum besorgt zu sein, daß künftig solche überschießenden Datenübermittlungen unterbleiben. Einen Abdruck dieses Schreibens habe ich dem Staatsministerium der Justiz übersandt.

7.5 Ordnungswidrigkeitenverfahren

7.5.1 Keine Erkennung von Mehrfachtätern in Verkehrsordnungswidrigkeitenverfahren durch "Verkehrssünderdateien bzw. -karteien" der Gemeinden

Ein Bürger hat vorgetragen, in einer kreisfreien Stadt würden vom gemeindlichen Verkehrsüberwachungsdienst "Parksünder" zur Erkennung von Mehrfachtätern in Dateien bzw. Karteien gespeichert.

Nach einer von mir angeforderten Stellungnahme der betroffenen kreisfreien Stadt besteht dort keine sog. "Verkehrssünderkartei". Zur Verfolgung von Ordnungswidrigkeiten werden dort nur die für die Verfahrensabwicklung unabdingbar notwendigen Daten erfaßt. Zugriff auf diese Daten haben nur die mit der Sachbearbeitung beauftragten Personen.

Nach dem Abschluß des Verfahrens bei der städtischen Verkehrsüberwachung werden die vorhandenen Daten für weitere Arbeiten noch vier Monate lang gespeichert. Dies geschieht, um Nachermittlungen in Zahlungsangelegenheiten und die Bearbeitung von Einsprüchen nach Erlaß von Bußgeldbescheiden durch die Zentrale Bußgeldstelle zu ermöglichen. Nach Ablauf dieser vier-monatigen Frist haben die Mitarbeiter der Fachdienststelle keinen Datenzugriff mehr.

Diese Verfahrensweise entspricht den datenschutzrechtlichen Anforderungen. Die Unzulässigkeit örtlicher "Verkehrssünderkarteien" bzw. sonstiger Listen oder Dateien zur Erkennung von Mehrfachtätern ergibt sich bereits daraus, daß die Speicherung von Sanktionen auf dem Gebiet des Straßenverkehrsrechts bereichsspezifisch und abschließend in den Vorschriften des Straßenverkehrsgesetzes über das Verkehrszentralregister geregelt ist. Eine Speicherung der Personen- und Verfahrensdaten bis zu vier Monate nach Abschluß des Ordnungswidrigkeitenvorgangs halte ich aber im Hinblick auf die Notwendigkeit einer Beantwortung evtl. Nach- bzw. Rückfragen oder um verspätet eingehende Verwarnungsgeldüberweisungen zuordnen zu können für noch hinnehmbar.

Ich habe das Staatsministerium des Innern gebeten, allgemein sicherzustellen, daß eine gezielte Auswertung der personenbezogenen Daten zum Zweck der Erkennung von Mehrfachtätern bei abgeschlossenen Verfahren während der kurzfristigen Weiterspeicherung unterbleibt.

7.5.2 Einbeziehung von privaten Unternehmen in die kommunale Verkehrsüberwachung

Die Problematik der Beteiligung Privater bei der Erfüllung hoheitlicher Aufgaben stellt sich gleichermaßen im Bereich der Parkraumüberwachung wie auch im Bereich der Überwachung des fließenden Verkehrs.

7.5.2.1 Gemeindliche Geschwindigkeitskontrollen

Aufgrund einer entsprechenden Änderung der Verordnung über Zuständigkeiten im Ordnungswidrigkeitenrecht vom 05. Juli 1994 haben zahlreiche Städte und Gemeinden in Bayern auf Antrag die Befugnis erhalten, selbst Geschwindigkeitskontrollen durchzuführen und Verstöße zu verfolgen. Dabei sollen bestimmte Tätigkeiten, wie beispielsweise die technische Abwicklung der Geschwindigkeitsmessung und Entwicklung der aufgenommenen Filme unter Einschaltung privater Unternehmen erfolgen. Dazu wurde vom Staatsministerium des Innern eine Verwaltungsvorschrift über die "Verfolgung und Ahndung von Geschwindigkeitsverstößen durch Gemeinden" erlassen.

Meinen Standpunkt zur Einbeziehung privater Unternehmen in die kommunale Geschwindigkeitsüberwachung habe ich gegenüber dem Staatsministerium des Innern im wesentlichen wie folgt dargelegt:

- Auch bei Einbeziehung privater Unternehmen bei der Geschwindigkeitsmessung muß die Gemeinde "Herrin" des Meßvorgangs bleiben. Dies bedeutet, daß insbesondere Ort, Zeit und Umfang der Kontrollmaßnahmen stets und in jedem Einzelfall von der Gemeinde selbst festzulegen sind. Darüber hinaus muß sichergestellt sein, daß der Meßvorgang selbst (insbesondere: Verwendung geeichter Geräte, Anwendung zugelassener Verfahren, Durchführung vorgeschriebener Tests, Einsatz geschulten Bedienungspersonals) von einem mit den technischen Abläufen und der Bedienung des Geräts vertrauten und besonders geschulten Bediensteten der Gemeinde überwacht wird.

  Ausgangspunkt für diese Forderungen ist der Rechtscharakter der Geschwindigkeitsüberwachung. Dabei handelt es sich nämlich um eine hoheitliche Tätigkeit, die von den Gemeinden selbst zu erledigen ist und nicht auf Private übertragen werden darf. Lediglich unselbständige Hilfstätigkeiten dürfen in diesem Zusammenhang im Auftrag der

Gemeinden von Privaten zur Entlastung der Gemeinden wahrgenommen werden. Eine sog. Funktionsübertragung auf Private wäre unzulässig.

Dabei halte ich bis zu einer grundsätzlichen Klärung durch die Rechtsprechung die Auffassung für vertretbar, daß zum Ausschluß einer solchen Funktionsübertragung auf Private nicht eine **ständige** Überwachung des Meßvorgangs durch einen qualifizierten gemeindlichen Bediensteten notwendig ist, sondern **häufige Stichproben** hierfür genügen.

Nach Presseberichten hat mittlerweile ein bayerisches Amtsgericht einen Betroffenen vom Vorwurf der Überschreitung der zulässigen Höchstgeschwindigkeit freigesprochen mit der Begründung, daß die Geschwindigkeitsmessung im zu entscheidenden Fall allein von einem Mitarbeiter einer Privatfirma im Auftrag der Gemeinde durchgeführt worden sei. Gegen das Urteil hat nach dem Bericht die Staatsanwaltschaft Rechtsbeschwerde eingelegt, über die nun das Bayerische Oberste Landesgericht zu befinden hat.

- Gegen eine Übertragung der **Entwicklung von Filmen** auf Private erhebe ich keine Einwendungen, wenn ein ausreichender Datenschutz gewährleistet ist. Da es sich hierbei um eine sog. Auftragsdatenverarbeitung handelt, sind die Maßgaben des Art. 6 Abs. 2 BayDSG zu beachten. In der vom Gesetz geforderten schriftlichen Auftragserteilung sollten insbesondere Regelungen über die Art der Anlieferung bzw. Abholung der Filme, den Zugriffsschutz im Entwicklungslabor und den Ausschluß von Unterauftragsverhältnissen getroffen werden. Vertragsstrafen sowie die Verpflichtung der eingesetzten Mitarbeiter nach dem Verpflichtungsgesetz sollten vorgesehen werden.

- Eine Übertragung der Auswertung der entwickelten Filme auf Privatunternehmen begegnet im Hinblick auf Art. 33 Abs. 4 Grundgesetz verfassungsrechtlichen Bedenken. Da die Auswertung der entwickelten Filme bereits Bestandteil des Entscheidungsprozesses ist, ob ein Ordnungswidrigkeitenverfahren eingeleitet wird, halte ich eine Übertragung auf Private nicht für zulässig. Anderes gilt, sofern das Privatunternehmen lediglich überprüft, ob die Aufnahmen rein fototechnisch so gelungen sind, daß sie als Beweismittel verwertbar sind, und der Gemeinde einen entsprechenden Vorschlag macht. Gegen eine solche Beurteilung der foto-

technischen Qualität der einzelnen Aufnahme erhebe ich keine Einwendungen, sofern sichergestellt ist, daß letztlich die Gemeinde über die Beweiseignung einer Aufnahme und die Frage, ob ein Ordnungswidrigkeitenverfahren einzuleiten ist, allein entscheidet. Dies erfordert jedoch insbesondere, daß der Gemeinde auch Aufnahmen, bei denen nach Auffassung des Privaten eine Beweiseignung fehlt, zur Entscheidung vorgelegt werden. Nur so ist gewährleistet, daß der Private lediglich tatsächliche Feststellungen und nicht verfahrensrechtliche (Vor-)Entscheidungen trifft.

Mittlerweile hat das Staatsministerium des Innern in einer Neufassung der Verwaltungsvorschrift über die "Verfolgung und Ahndung von Geschwindigkeitsverstößen durch Gemeinden" meinen datenschutzrechtlichen Hinweisen Rechnung getragen.

7.5.2.2 Einbeziehung Privater bei der gemeindlichen Parkraumüberwachung

Diese Thematik ist bereits seit geraumer Zeit Gegenstand von Erörterungen verschiedener Gremien auf Bund-Länder-Ebene im Bereich der Innenminister- und Verkehrsministerkonferenz, wobei bislang eine Entscheidung nicht getroffen wurde.

Nach meinen Feststellungen werden in vier bayerischen Städten bereits seit mehreren Jahren im Rahmen der Überwachung des ruhenden Verkehrs private Überwachungsunternehmen eingesetzt.

Dazu wurde von drei Städten der sog. Außendienst (Feststellung des Verkehrsverstoßes) auf Mitarbeiter eines privaten Überwachungsunternehmens übertragen, in einem Falle zusätzlich auch die "Innendienstabwicklung" "in Abstimmung und unter Verantwortung der Stadt". Die Mitarbeiter der privaten Überwachungsfirma verpflichten sich in Nebenabreden zum jeweiligen Arbeitsvertrag, eine Erklärung nach dem Verpflichtungs- und Datenschutzgesetz gegenüber der Stadt abzugeben und unterwerfen sich ausdrücklich im Rahmen ihrer Überwachungstätigkeit den Weisungen der jeweiligen Stadt.

Diesen Sachverhalt bewerte ich vorläufig wie folgt:

Ich habe erhebliche Bedenken, sofern den "Außendienstmitarbeitern" hoheitliche Tätigkeiten wie insbesondere die Verwarnung eines Verkehrsteilnehmers zur selbständigen Erledigung übertragen werden.

Die Nutzung der personenbezogenen Daten über den Verkehrsverstoß zum Zwecke der Verwarnung setzt als hoheitliche Ordnungsmaßnahme aus verfassungsrechtlichen Gründen das Tätigwerden eines **Angehörigen der Verwaltungsbehörde** voraus. Auch aus dem Wortlaut des § 56 Abs. 1 Ordnungswidrigkeitengesetz ergibt sich, daß eine Verwarnung nur durch "die Verwaltungsbehörde" erfolgen darf. Diese handelt im Einzelfall durch ihre Verwaltungsangehörigen (Beamten oder Angestellten), die nach der innerdienstlichen Behördenorganisation dazu befugt sind. Da die Mitarbeiter einer privaten Überwachungsfirma nicht dadurch Verwaltungsangehörige der Stadt werden, daß sie sich deren Weisungen unterwerfen, liegen die Voraussetzungen für die Erteilung von Verwarnungen durch die Mitarbeiter der privaten Überwachungsfirma nicht vor.

Problematisch erscheint die Mitwirkung von Privaten auch, soweit sie über die Sachverhaltsschilderung hinaus bereits eine rechtliche Beurteilung des Verkehrsverstoßes abgeben. Dies könnte etwa dann der Fall sein, wenn die Art der Verkehrsordnungswidrigkeit bereits vom Außendienstmitarbeiter durch Eingabe in ein Datenerfassungsgerät rechtlich qualifiziert würde (z.B. Parken/Halten **mit Verkehrsbehinderung**).

Ich habe das Staatsministerium des Innern um Stellungnahme gebeten. Eine Antwort des Innenministeriums steht noch aus.

Zwischenzeitlich liegt mir ein Urteil des Amtsgerichts Tiergarten vom 24. April 1996 vor, in dem bereits der systematische Einsatz von Privatpersonen zur Tatsachenfeststellung bei der Parkraumüberwachung für unzulässig erklärt und mit einem Beweisverwertungsverbot für das nachfolgende Bußgeldverfahren sanktioniert wird. Das Gericht verwirft darin nachdrücklich einen Vergleich mit Anzeigen durch sonstige "private" Zeugen, da der "private" Anzeigeerstatter oder Zeuge "**nicht systematisch und in eigener Kompetenz**" Ordnungswidrigkeiten verfolge.

7.5.3 Beinahme von Geschwindigkeitsmeßlisten zum Ordnungswidrigkeitenakt

Ein Petent sah sich durch die folgende Verfahrensweise in seinen Rechten verletzt:

In der Akte eines gegen ihn gerichteten Bußgeldverfahrens wegen einer Verkehrsordnungswidrigkeit war eine zweiseitige Liste abgelegt, in der mindestens Verkehrsverstöße durch Überschreitung der zulässigen Höchstgeschwindigkeit von zwanzig anderen Personen mit Angabe der amtlichen Kennzeichen, Fahrzeugart und Marke der Fahrzeuge sowie der festgestellten Geschwindigkeit aufgeführt waren. Er (der Petent) gehe davon aus, daß sich dieselbe Liste in sämtlichen anderen Ordnungswidrigkeitenakten, die wegen der in der Liste aufgeführten Geschwindigkeitsverstöße angelegt wurden, befinde und damit seine Daten auch in anderen Verfahren gespeichert seien.

Das zuständige Polizeipräsidium hat auf Anfrage die Beinahme der Meßlisten zu den jeweiligen Verfahrensakten damit gerechtfertigt, daß bei Geschwindigkeitskontrollen mit LaserHandgeschwindigkeitsmeßgeräten und Kleinradargeräten die Meßlisten zum Zwecke der Nachvollziehbarkeit und Plausibilität der Meßergebnisse mit allen bei einem Einsatz durchgeführten "ahndungsrelevanten" Messungen aufbewahrt und ggf. dem Gericht oder Sachverständigen komplett vorgelegt werden müßten, weil sich auch aus der Gesamtheit der Messungen ein Indiz für die Fehlerfreiheit der Messung ergebe.

Ich beurteile diese Praxis wie folgt:

Gegen eine Beinahme der Liste aller festgestellten Verkehrsverstöße, die bei demselben Meßeinsatz festgestellt wurden, zum jeweiligen Ordnungswidrigkeitenvorgang - sofern zur Sachbehandlung erforderlich - erhebe ich dem Grunde nach keine Einwendungen. Insbesondere erkenne ich an, daß der Verteidiger eines Betroffenen bei Akteneinsicht ein legitimes Interesse daran haben kann, sich durch Einsicht in alle Meßergebnisse ein Bild von der Plausibilität der Messung machen zu können.

Allerdings halte ich es für unerläßlich, daß die Daten der nicht den konkreten Ordnungswidrigkeitenvorgang betreffenden anderen Messungen soweit wie möglich anonymisiert werden. In diesem Zusammenhang vermag ich keine Gesichtspunkte zu ersehen, weshalb die Kfz-

Kennzeichen der übrigen Fahrzeuge im Ordnungswidrigkeitenvorgang gegen einen bestimmten Betroffenen gespeichert werden müssen. Mögen Fahrzeugtyp und Fahrzeugfarbe noch für die Plausibilitätsüberprüfung der gesamten Messung von Bedeutung sein, so ist mir jedenfalls nicht einsichtig, weshalb die Kraftfahrzeugkennzeichen der anderen Fahrzeuge bei der Frage der Plausibilität der Meßergebnisse von Bedeutung sein könnten. Da die Kfz-Kennzeichen der übrigen gemessenen Fahrzeuge als Einzelangaben über die jeweiligen Fahrzeughalter personenbezogene Daten im Sinne des Art. 4 Abs. 1 BayDSG darstellen und die Speicherung dieser Daten im Rahmen des jeweiligen Ordnungswidrigkeitenvorgangs zur Sachbearbeitung nicht erforderlich ist, habe ich das Polizeipräsidium gebeten, künftig die Kennzeichen der jeweils anderen gemessenen Fahrzeuge unkenntlich zu machen. Da die Originalliste ohnehin für die Beinahme zu den jeweiligen Einzelvorgängen abgelichtet werden muß, kann dies ohne großen Verwaltungsaufwand unschwer mit einer Schablone bewerkstelligt werden, die jeweils nur das Kennzeichen des konkret betroffenen Fahrzeugs offenläßt.

Mittlerweile hat mir das Polizeipräsidium mitgeteilt, daß künftig entsprechend meinen Forderungen verfahren wird.

7.5.4 Nutzung von Paßbildern der Meldebehörden in Ordnungswidrigkeitenverfahren

Es haben sich mehrere Bürger an mich gewandt mit der Frage, ob die Übermittlung von Paß- bzw. Personalausweisfotos aus dem Melderegister an die Polizei zum Zwecke der Verfolgung von Verkehrsordnungswidrigkeiten (in der Regel Überschreitung der zulässigen Höchstgeschwindigkeit) zulässig war.

Dazu ist folgendes anzumerken:

Nach § 53 Abs. 1 Ordnungswidrigkeitengesetz haben die Behörden und Beamten des Polizeidienstes die Aufgabe, nach pflichtgemäßem Ermessen Ordnungswidrigkeiten zu erforschen und dabei alle unaufschiebbaren Anordnungen zu treffen, um die Verdunkelungen der Sache zu verhüten. Zur Erforschung der Ordnungswidrigkeit kann die Beiziehung eines Lichtbilds des Betroffenen erforderlich sein, denn durch den Vergleich eines anläßlich des Verkehrsverstoßes gefertigten Lichtbilds des Fahrers mit dem Lichtbild aus dem Personalausweis oder Reisepaß des Betroffenen kann die Behörde die Identität des Betroffenen mit dem Fahrer des Kraftfahrzeugs überprüfen.

Paßausweisdaten dürfen nach § 22 Abs. 2 Paßgesetz unter der Voraussetzung übermittelt werden, daß

1. die ersuchende Behörde aufgrund von Gesetzen oder Rechtsverordnungen berechtigt ist, solche Daten zu erhalten,
2. die ersuchende Behörde ohne Kenntnis der Daten nicht in der Lage wäre, eine ihr obliegende Aufgabe zu erfüllen und
3. die Daten beim Betroffenen nicht oder nur mit unverhältnismäßig hohen Aufwand erhoben werden können oder nach der Art der Aufgabe, zu deren Erfüllung die Daten erforderlich sind, von einer solchen Datenerhebung abgesehen werden muß.

Entsprechendes gilt für die Übermittlung des Lichtbildes aus einem Personalausweis (§ 2 b Personalausweisgesetz).

Hinsichtlich der Voraussetzungen des § 22 Abs. 2 Nr. 3 Paßgesetz dürfen allzu hohe Anforde-

rungen an den Grundsatz der Direkterhebung der Daten nicht gestellt werden. Ein unverhältnismäßig hoher Aufwand kann auch bereits dann angenommen werden, wenn nach Anhörung des Fahrzeughalters mehrere Betroffene abgeklärt werden müßten. Kommt jedoch nach den Erkenntnissen der Polizei nur eine bestimmte andere Person als Fahrer in Betracht, so ist diese zunächst anzuhören und ein Lichtbildvergleich erst hernach zulässig.

Insgesamt ist festzustellen, daß der Vergleich eines Lichtbilds aus dem Reisepaß bzw. Personalausweis mit dem gelegentlich des Verkehrsverstoßes gefertigten Frontfoto des Fahrers häufig im Vergleich mit den ansonsten erforderlichen Ermittlungen (etwa: Bildbefragung von Nachbarn, Arbeitskollegen usw.) zur Feststellung der für den Verkehrsverstoß in Betracht kommenden Personen als geringerer Eingriff anzusehen ist.

7.5.5 Datenschutz für Beifahrer bei Vorhalt von Lichtbildern an Dritte in Ordnungswidrigkeitenverfahren

Zur Feststellung, ob in Bayern bei der Vorlage von Lichtbildern (Beweisfotos) an Dritte in Verkehrsordnungswidrigkeitenverfahren der Datenschutz für den neben dem Fahrer abgelichteten Beifahrer gewährleistet ist, habe ich mich an das Staatsministerium des Innern gewandt.

Das Ministerium hat nunmehr - entsprechend einer bereits verbreiteten Verfahrensweise - angeordnet, daß Lichtbilder unbeteiligten Dritten im Rahmen der Fahrerermittlung zur Verfolgung und Ahndung von Verkehrsordnungswidrigkeiten in der Form vorzulegen sind, daß unbeteiligte Personen (Beifahrer, ggf. sonstige Mitfahrer) grundsätzlich abgedeckt werden. Nur soweit es im Interesse der Fahrerermittlung im Einzelfall erforderlich sei, (zunächst) den Beifahrer zu identifizieren, dürfte das Beweisfoto unbeteiligten Dritten vollständig zur Ansicht vorgelegt werden.

Das nunmehr angeordnete Verfahren berücksichtigt in angemessener Weise das Datenschutzrecht von Mitfahrern.

7.5.6 Nicht datenschutzkonforme Ausgestaltung eines Anhörungsformblatts im Ordnungswidrigkeitenverfahren

Ein Bürger hat sich an mich gewandt und vorgetragen, er sei im Rahmen eines Verfahrens wegen Verdachts einer Ordnungswidrigkeit nach dem Bayerischen Straßen- und Wegegesetz von einer Polizeiinspektion angehört worden, wobei im Anhörungsschreiben hinsichtlich der Angaben zur Person nicht nach Pflichtangaben und freiwilligen Angaben unterschieden worden sei.

Das zuständige Polizeipräsidium hat auf meine Anfragen hin den Mangel der Sache nach eingeräumt und mitgeteilt, daß die Formblätter für die Anhörung im Ordnungswidrigkeitenverfahren nunmehr so geändert wurden, daß zwischen den Pflichtangaben zur Person und freiwilligen Angaben deutlich unterschieden wird. Der Stellungnahme war das neu gestaltete Formblatt beigefügt. Dieses entspricht nunmehr den datenschutzrechtlichen Anforderungen. Insbesondere sind als Pflichtangaben nur die in § 111 Ordnungswidrigkeitengesetz enthaltenen Daten aufgeführt, im übrigen wird auf die Freiwilligkeit weiterer Angaben hingewiesen.

7.6 Einzelfragen

7.6.1 Eingaben wegen des Verhaltens bayerischer Justizbehörden

Aufgrund von Bürgereingaben wurden mir verschiedene Sachverhalte bekannt, denen zwar nicht Fehler im System, wohl aber Unaufmerksamkeit oder Fehlverhalten im Einzelfall zugrundelag:

7.6.1.1 Datenübermittlung durch die Hinterlegungsstelle eines Amtsgerichts

Nach Ehescheidung des Petenten und Versteigerung des gemeinsamen Wohnanwesens wurde der Versteigerungserlös beim zuständigen Amtsgericht hinterlegt. Nach Befriedigung verschiedener Gläubiger wurde der überschießende Betrag an den Petenten ausbezahlt. Hernach rief ein Dritter bei der zuständigen Rechtspflegerin der Hinterlegungsstelle des Amtsgerichts an und teilte mit, daß er neuer Eigentümer des versteigerten Grundstücks sei. Der Petent wolle von ihm das Grundstück zurückkaufen und habe ihm (dem Dritten) per Telefax die Auszahlungsmitteilung der Hinterlegungsstelle des Amtsgerichts übersandt, um seine Liquidität nachzuweisen. Im Telefax sei nur der auszuzahlende Betrag unkenntlich gemacht worden. Der Anrufer - der im übrigen vollständig über das Hinterlegungsverfahren informiert war - wollte wissen, ob die vom Petenten angegebene Höhe des Auszahlungsbetrages zutreffend war. Die Rechtspflegerin teilte dem Dritten den tatsächlich ausgekehrten Betrag mit.

Ich bin der Auffassung, daß von dieser fernmündlichen Datenübermittlung an einen - nicht identifizierten - Dritten aus folgenden Gründen hätte abgesehen werden sollen:

Mangels Regelung in der Hinterlegungsordnung galten für die Auskunftsgewährung durch Hinterlegungsstellen die Bestimmungen des Bayerischen Datenschutzgesetzes. Nach Art. 19 Abs. 1 Ziff. 2 BayDSG dürfen personenbezogene Daten an nicht-öffentliche Stellen nur übermittelt werden, wenn die nicht-öffentliche Stelle ein berechtigtes Interesse an der Kenntnis der zu übermittelnden Daten **glaubhaft darlegt** und der Betroffene kein schutzwürdiges Interesse an dem Ausschluß der Übermittlung hat. Demnach hätte der Anrufer sein berechtigtes Interesse an der Kenntnis der zu übermittelnden Daten glaubhaft darlegen müssen. Bei telefonischen Auskünften an unbekannte Dritte sind an eine solche Glaubhaftmachung besondere Anforderungen zu stellen. Allein die Kenntnis über Einzelheiten des Hinterlegungsverfahrens rechtfertigt in die-

sem Fall noch nicht die Annahme, die Eigentümerstellung des Anrufers, die Absicht des Petenten, das Grundstück zurückzukaufen und die Angaben des Petenten über die Höhe des Auszahlungsbetrags seien glaubhaft gemacht.

Gleichwohl handelt es sich hier um einen Grenzfall, dessen abweichender Beurteilung durch das Amtsgericht sachliche Gesichtspunkte zugrundelagen. Ich habe deshalb von einer förmlichen Beanstandung der Datenübermittlung abgesehen.

7.6.1.2 Unzutreffende Eintragung und Auskunft aus dem Schuldnerverzeichnis eines Amtsgerichts

Der Petent beschwerte sich darüber, daß er durch eine fehlerhafte Mitteilung eines bayerischen Amtsgerichts an die "Schufa" in seinen Rechten verletzt worden sei. Es sei fälschlich mitgeteilt worden, daß gegen ihn (den Petenten) ein Haftbefehl zur Abgabe der eidesstattlichen Versicherung ergangen sei. Daraufhin seien ihm Schwierigkeiten bei der Fremdfinanzierung eines Bauvorhabens entstanden.

Die Ermittlungen ergaben, daß die unzutreffende Eintragung in die Schuldnerkartei des Amtsgerichts ihre Ursache darin hatte, daß die zuständige Bedienstete im Zuge des Verfahrens zur Abnahme der eidesstattlichen Versicherung gegen einen Dritten mit gleichem Familiennamen fehlerhaft den Vornamen abgeändert hatte.

Der Leiter des Amtsgerichts hat dazu mitgeteilt, daß auf entsprechende Beschwerde des anwaltlichen Vertreters des Petenten sofort der Fehler korrigiert, die auf den Namen des Petenten lautende Karteikartei vernichtet und Industrie- und Handelskammer, Gerichtsvollzieher und "Schufa" telefonisch benachrichtigt worden seien. Überdies sei die Mitarbeiterin der Geschäftsstelle ermahnt worden.

Im Hinblick darauf habe ich zwar den Direktor des Amtsgerichts ausdrücklich auf den Datenschutzverstoß hingewiesen, jedoch von einer förmlichen Beanstandung der fehlerhaften Datenspeicherung und -übermittlung abgesehen.

7.6.1.3 Hinweis auf Verfahrensgegenstand bei Adressierung eines Schreibens im Konkursverfahren

Der Eingabe lag die Adressierung eines durch die Post versandten Schreibens eines Amtsgerichts zugrunde. Daraus war ersichtlich, daß gegen die Empfängerin des Schreibens ein Konkursverfahren anhängig war.

Der Präsident des betroffenen Amtsgerichts hat mitgeteilt, er werde die mit Kostensachen beauftragten Rechtspfleger bitten, in Zukunft personenbezogene Daten, die über die reine Postanschrift des Kostenschuldners hinausgehen, mittels einer Fußnote in einem Bereich anzubringen, der durch das Fensterkuvert für Dritte nicht einsehbar ist. Ich habe den Vorgang auch dem Staatsministerium der Justiz zur Kenntnis gegeben.

7.6.1.4 Zusatz "Justizvollzugsanstalt" bei Schreiben an Strafgefangene

Im Anschriftenfeld eines Schreibens eines Amtsgerichts an einen Strafgefangenen war neben der Postanschrift der Zusatz "JVA" aufgenommen.

Das Staatsministerium der Justiz hat veranlaßt, daß die zuständige Rechtspflegerin in allgemeiner Weise darauf hingewiesen wird, "daß die Aufnahme des Zusatzes "JVA" neben der Zustellanschrift des Adressaten dessen Persönlichkeitsrecht tangieren kann" und daher unterbleiben sollte, wenn auch ohne diesen Zusatz mit einer ordnungsgemäßen Zustellung gerechnet werden kann.

7.6.1.5 Versendung eines Erbscheins im offenen Umschlag

Einer Petentin war der Erbschein von einem Amtsgericht in einem offenen Briefkuvert durch die Post übersandt worden.

Der Präsident des betroffenen Amtsgerichts hat dazu angemerkt, daß dort arbeitstäglich ca. 3000 ausgehende Briefe mit Hilfe von zwei hierzu eingesetzten Maschinen versandfertig gemacht und frankiert würden. Bei einer dieser Maschinen komme es immer wieder einmal vor, daß einzelne Briefe nicht zugeklebt würden. Die Wachtmeister der Poststelle prüften deshalb regelmäßig, ob auch alle Kuverts verschlossen seien, indem sie die versandfertigen Briefe durchblätterten. Im Falle der Petentin sei gleichwohl offenbar ein nicht verschlossenes Kuvert übersehen worden. Der Vorfall sei zum Anlaß genommen worden, an der in Frage stehenden Maschine als "Sofortmaßnahme" eine Generalwartung und Teilerneuerung durchführen zu lassen. Darüber hinaus würden die Mitarbeiter der Poststelle künftig auslaufende Post noch genauer kontrollieren.

Da der hier vorliegende Verstoß gegen datenschutzrechtliche Grundsätze lediglich auf einem Versehen eines Mitarbeiters des Amtsgerichts beruhen dürfte und nicht etwa Ausfluß einer behördlichen Praxis ist und da der Präsident des Amtsgerichts sofortige Maßnahmen in Angriff genommen hat, um künftig solche Vorkommnisse zu vermeiden, habe ich von einer förmlichen Beanstandung abgesehen.

7.6.2 Übermittlung personenbezogener Daten durch die Strafverfolgungsbehörden an die Medien

Die Strafverfolgungsbehörden erheben aufgrund der gesetzlichen Befugnisnormen der Strafprozeßordnung im Rahmen ihrer Aufgabenerfüllung eine Vielzahl sensibler personenbezogener Daten. Die Medien, deren tägliche Berichterstattung in erheblichem Umfang laufende Ermittlungs- und Strafverfahren umfaßt, haben - nicht selten auch zur Befriedigung bloßer Sensationslust und Neugier der Öffentlichkeit - ein erhebliches Interesse an möglichst detaillierten Informationen über Täter und Opfer von Straftaten. Demgegenüber hat der Betroffene regelmäßig ein grundlegendes Interesse daran, daß personenbezogene Informationen über ihn nicht an die Öffentlichkeit gelangen.

Jede Bekanntgabe personenbezogener Daten an die Medien durch die Strafverfolgungsbehörden ist eine Datenübermittlung an Stellen außerhalb des öffentlichen Bereichs. Eine bereichsspezifische Rechtsgrundlage im Pressegesetz oder in der Strafprozeßordnung, die dem Spannungsverhältnis zwischen dem Recht auf informationelle Selbstbestimmung des betroffenen Bürgers und der freien Berichterstattung der Presse, die grundsätzlich auch das Recht auf Auskünfte durch die Behörden einschließt, angemessen Rechnung trägt, existiert bislang nicht.

Die Datenschutzbeauftragten des Bundes und der Länder haben in einer Entschließung den Gesetzgeber aufgefordert, bereichsspezifische Regelungen für die Übermittlung personenbezogener Daten durch die Strafverfolgungsbehörden an die Medien (außerhalb der Öffentlichkeitsfahndung) zu schaffen (vgl. Anlage 5). Diese Regelungen sollten für den betroffenen Bürger den Umfang des Eingriffs in sein Recht auf informationelle Selbstbestimmung erkennbar machen.

Ich habe gegenüber den Staatsministerien des Innern und der Justiz auf diese Entschließung hingewiesen und angeregt, die darin enthaltenen Grundsätze bei der Auslegung der bestehenden allgemeinen Regelungen heranzuziehen. Beim Polizeipräsidium München habe ich die Presseberichte für einen bestimmten Zeitraum anhand der Grundsätze der Entschließung überprüft (vgl. dazu Nr. 5.4.5).

7.6.3 Bereitstellung von Anklagesätzen und Sitzungslisten für Pressevertreter vor der Hauptverhandlung

Aus gegebenem Anlaß habe ich die Frage der Zulässigkeit der Bereitstellung von Anklagesätzen und Sitzungslisten vor Beginn der Hauptverhandlung für Pressevertreter nochmals aufgegriffen.

Nach Ziff. 3.2 der Bekanntmachung des Staatsministeriums der Justiz vom 26. Oktober 1978 über das Justizpressewesen kann in Schwurgerichtssachen und in Strafsachen, von denen anzunehmen ist, daß sie in der Öffentlichkeit eine besondere Beachtung finden werden, den Gerichtsberichterstattern der Presse nach Eröffnung des Hauptverfahrens und schon **vor Beginn der Hauptverhandlung** die Anklageschrift (ohne das wesentliche Ergebnis der Ermittlungen) zur Einsichtnahme zugänglich gemacht bzw. eine Abschrift der Anklageschrift überlassen werden. Darüber hinaus werden die Sitzungslisten der Strafverhandlungen vor den Landgerichten jeweils für eine Woche am Ende der vorausgehenden Woche zur Einsichtnahme durch die Gerichtsberichterstatter der Presse ausgelegt.

Ich habe mich dazu mit folgenden Überlegungen an das Justizministerium gewandt:

Durch eine Übermittlung des Anklagesatzes nach Zulassung der Anklage, aber noch vor Beginn der Hauptverhandlung werden zwar dem Umfang nach nicht mehr Daten übermittelt als in öffentlicher Sitzung bekannt werden; die Daten werden aber den Pressevertretern bereits vor Verlesung der Anklage in der Hauptverhandlung zur Verfügung gestellt.

Die Weitergabe personenbezogener Daten durch Staatsanwaltschaften bzw. Strafgerichte ist als Datenübermittlung an nicht-öffentliche Stellen zu qualifizieren. Sie steht im Spannungsfeld zwischen der Informationsfreiheit der Presse (Art. 5 Grundgesetz, Art. 111 Bayerische Verfassung) einerseits und dem Grundrecht auf informationelle Selbstbestimmung (Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 Grundgesetz) des von einer Datenübermittlung an die Presse Betroffenen andererseits. Da sich eine spezialgesetzliche Regelung für solche Datenübermittlungen in der Strafprozeßordnung (noch) nicht findet, kann die Rechtsgrundlage hierfür nur in Art. 19 Abs. 1 Satz 2 BayDSG i.V.m. dem Auskunftsrecht der Presse nach § 4 Abs. 1 des Bayerischen Pressegesetzes gesehen werden. Danach bedarf es in jedem Einzelfall einer umfassenden und konkreten Güterabwägung. Das Informationsinteresse der Öffentlichkeit einerseits und die Intensität des Eingriffs in das

Persönlichkeitsrecht des Betroffenen andererseits sind bestmöglich zum Ausgleich zu bringen.

In Übereinstimmung mit der Entschließung der 50. Konferenz der Datenschutzbeauftragten des Bundes und der Länder (siehe dazu Anlage 5) erscheint mir die Übermittlung personenbezogener Daten an die Medien (jedenfalls vor strafgerichtlicher Verurteilung) **nur ausnahmsweise** gerechtfertigt, wenn das Verfahren gerade im Hinblick auf die Person des Betroffenen oder die besonderen Umstände der Tat für die Öffentlichkeit von überwiegendem Interesse ist. Bei der - abwägenden - Entscheidung, ob und in welchem Umfang personenbezogene Daten an die Medien übermittelt werden, sind die schutzwürdigen Belange der Betroffenen (private und berufliche Folgen für das Opfer, den Angeklagten und deren Angehörige sowie die Schwere, die Umstände und die Folgen der Tat) zu berücksichtigen. Sollen personenbezogene Daten über Beschuldigte/Angeklagte übermittelt werden, so sind auch der Grad des Tatverdachts und der Verfahrensstand zu berücksichtigen. Vor Beginn der öffentlichen Hauptverhandlung ist ein besonders strenger Maßstab an das Vorliegen eines "überwiegenden Interesses" der Öffentlichkeit anzulegen. Eine Übermittlung personenbezogener Daten von **Opfern**, Zeugen und Familienangehörigen an die Presse kommt regelmäßig nicht in Betracht.

Ich habe erhebliche Zweifel, ob eine "routinemäßige" Bereitstellung und ggf. Übermittlung **aller** Anklagesätze in Schwurgerichtssachen und öffentlichkeitsträchtigen Strafverfahren an die Presse den o.g. Voraussetzungen genügt. Das gilt auch dann, wenn - wie in der Praxis - auf den für die Presse bestimmten Exemplaren des Anklagesatzes die personenbezogenen Daten anderer Beteiligter mit Ausnahme der Personalien des Angeklagten geschwärzt werden. Es bedarf vielmehr **in jedem Einzelfall** einer umfassenden Abwägung des Informationsinteresses der Presse mit den Belangen der von der Datenübermittlung Betroffenen.

Der Gedankenaustausch mit dem Justizministerium in diesen Fragen ist derzeit noch nicht abgeschlossen.

Hinsichtlich der Möglichkeit zur Einsichtnahme in die Sitzungsliste der Strafverhandlungen der Folgewoche durch die Pressevertreter habe ich das Justizministerium um Mitteilung gebeten, ob dem - grundsätzlich anzuerkennenden - Informationsinteresse der Presse nicht dadurch genügt werden könnte, daß die Sitzungslisten mit geschwärztem Namen der Angeklagten bzw. nur unter

Angabe des Vornamens und des Anfangsbuchstabens des Nachnamens bereitgestellt werden. Eine Antwort des Justizministeriums hierzu steht noch aus.

7.6.4 Mißbräuchliche Verwendung von durch Akteneinsicht erlangten personenbezogenen Erkenntnissen

Bereits in meinem 15. Tätigkeitsbericht (Nr. 6.8.2) habe ich mich eingehend mit der Problematik auseinandergesetzt. Zwei neuerliche Eingaben bestätigen mich in meiner Auffassung, daß dringender gesetzgeberischer Handlungsbedarf besteht:

Im einem Fall lag der Eingabe folgender Sachverhalt zugrunde:

In einem Zivilrechtsstreit vor einem Amtsgericht, in dem der Petent Beklagter war, wurde auf Anordnung des Gerichts vom Landgerichtsarzt ein Gutachten zur Frage der Geschäftsfähigkeit des Beklagten erstattet. Das schriftliche Sachverständigengutachten wurde zu den Gerichtsakten genommen. Der anwaltliche Vertreter der Klageparteien fertigte eine Fotokopie des Sachverständigengutachtens und übergab diese der Klägerin. Die Klägerin wiederum brachte das Sachverständigengutachten ihren Nachbarn zur Kenntnis.

Soweit es um die Gewährung von Akteneinsicht bzw. die Übersendung einer Ablichtung des Gutachtens an den anwaltlichen Vertreter der Klägerin während des laufenden Zivilrechtsstreits ging, mußte ich dem Petenten mitteilen, daß mir nach Art. 2 Abs. 6 BayDSG insoweit eine Prüfungszuständigkeit fehlt. Lediglich ergänzend habe ich auf § 299 Abs. 1 ZPO (Akteneinsicht der Parteien, Abschriften) hingewiesen. Soweit es um das Verhalten der Klägerin ging, mußte ich dem Petenten mitteilen, daß ich gemäß Art. 30 Abs. 1 Satz 1 BayDSG nur für die Kontrolle bei öffentlichen Stellen zuständig bin. Weiterhin habe ich den Petenten darauf hingewiesen, daß in Fällen, in denen Privatpersonen Daten, die nicht in oder aus Dateien geschäftsmäßig oder für berufliche oder gewerbliche Zwecke verarbeitet oder genutzt werden, im privaten Rechtsverkehr an Dritte übermitteln, weder die Bestimmungen des Bayerischen Datenschutzgesetzes noch diejenigen des Bundesdatenschutzgesetzes anwendbar sind. Es liege daher bei demjenigen, dessen Daten übermittelt wurden, etwaige Verletzungen seines Persönlichkeitsrechts selbst - ggf. unter Zuhilfenahme der Gerichte - geltend zu machen.

Im anderen Falle wurde der Petent, ein ehemaliger Beamter, im Zusammenhang mit einer vorzeitigen Ruhestandsversetzung von einem Dritten wegen Betrugs angezeigt und erstattete seiner-

seits Gegenanzeige wegen falscher Verdächtigung, übler Nachrede und Beleidigung. Im Zuge der beiden Ermittlungsverfahren wurde in Bezug auf den Petenten als ärztlicher Befund "Schizophrenie mit depressiver Prägung" in den Akten vermerkt. Durch Akteneinsicht in die wegen der Gegenanzeige geführten Ermittlungsakten erlangte der Anzeigeerstatter hiervon Kenntnis und verwandte diese im Zuge eines gegen ihn geführten Zivilrechtsstreits zur Beurteilung der Glaubwürdigkeit der dort gemachten Zeugenaussagen des Petenten.

Ich habe mich im Hinblick auf diese neuerlichen Eingaben unabhängig von meiner fehlenden Prüfungszuständigkeit im Einzelfall nochmals an das Staatsministerium der Justiz gewandt und dargelegt, daß ein wirksamer Schutz vor zweckwidriger Verwendung der durch Akteneinsicht oder Auskünfte des Gerichts erlangten personenbezogenen Daten nicht nur im Bereich des Strafverfahrens notwendig ist, sondern ein gleiches Schutzbedürfnis auch für personenbezogene Daten in Zivilrechtsstreitigkeiten oder anderen gerichtlichen Verfahren besteht. Angesichts des Spannungsfeldes zwischen dem Grundsatz rechtlichen Gehörs für die gegnerische Partei und dem Geheimhaltungsinteresse des Betroffenen halte ich es weiterhin für erforderlich, die Verwendung der erlangten personenbezogenen Daten einer Zweckbindung zu unterstellen und die Einhaltung der Zweckbindungsregelung durch eine Strafbewehrung abzusichern. Ich habe um Unterstützung dieses Anliegens, zunächst im Gesetzgebungsverfahren zu einem Strafverfahrensänderungsgesetz, gebeten.

7.6.5 Übermittlung von Entscheidungen an den Hohen Flüchtlingskommissar der Vereinten Nationen (UNHCR)

Im Berichtszeitraum hat sich ein Verwaltungsgericht mit folgender Anfrage an mich gewandt:

Der Hohe Flüchtlingskommissar der Vereinten Nationen (UNHCR) habe das Verwaltungsgericht gebeten, ihm künftig alle ausländer- und asylrechtlichen Entscheidungen des Gerichts in Abdruck zu übermitteln. Ziel des UNHCR sei es, die asyl- und ausländerrechtlichen Entscheidungen aller bayerischen Verwaltungsgerichte auszuwerten, um einen Überblick über die Entscheidungspraxis der bayerischen Verwaltungsgerichtsbarkeit zu erhalten. Das Verwaltungsgericht hat bei mir angefragt, ob und ggf. in welcher Form unter Berücksichtigung der datenschutzrechtlichen Belange der Bitte des UNHCR entsprochen werden kann.

Ich habe gegenüber dem Gericht folgende Stellungnahme abgegeben:

Für die Übersendung von Urteilsabschriften an Nichtverfahrensbeteiligte durch das Gericht fehlt bislang eine spezialgesetzliche Regelung. Heranzuziehen sind daher die allgemeinen Regelungen des Bayerischen Datenschutzgesetzes zur Übermittlung personenbezogener Daten durch öffentliche Stellen. Bei dem UNHCR handelt es sich um ein Organ der Vereinten Nationen und damit um eine überstaatliche Stelle im Sinne von Art. 21 BayDSG. Nach Art. 21 Abs. 1 BayDSG sind bei der Übermittlung personenbezogener Daten an überstaatliche Stellen die Vorschriften für die Datenübermittlung an nicht-öffentliche Stellen entsprechend anwendbar. Maßgeblich für die Rechtmäßigkeit einer Datenübermittlung ist daher Art. 19 BayDSG. Danach ist eine Datenübermittlung an nicht-öffentliche Stellen zulässig, wenn die nicht-öffentliche Stelle ein berechtigtes Interesse an der Kenntnis der zu übermittelnden Daten glaubhaft darlegt und der Betroffene kein schutzwürdiges Interesse an dem Ausschluß der Übermittlung hat.

Im vorliegenden Falle hat der UNHCR aufgrund seiner Aufgabenstellung und seiner Funktion erkennbar ein berechtigtes Interesse an aktuellen ausländerrechtlichen und asylrechtlichen Entscheidungen der bayerischen Verwaltungsgerichte. Für den vom UNHCR dargelegten Zweck erscheint mir jedoch eine Kenntnis der Namen der Verfahrensbeteiligten nicht erforderlich. In diesem Sinne hat der UNHCR selbst darauf hingewiesen, daß ein anderes außerbayerisches

Verwaltungsgericht Entscheidungen nur in anonymisierter Form übersendet. Ich habe daher gegen eine Übermittlung von Entscheidungen des anfragenden Verwaltungsgerichts an den UNHCR **in anonymisierter Form** aus datenschutzrechtlicher Sicht keine Bedenken.

Da ich davon ausgehe, daß entsprechende Anfragen auch an weitere bayerische Verwaltungsgerichte erfolgt sind bzw. erfolgen werden, habe ich meine Auffassung dem Staatsministerium des Innern mitgeteilt mit der Bitte, die anderen Verwaltungsgerichte in Bayern davon zu unterrichten.

7.6.6 Überwachung des Zahlungseingangs bei Verfahrenseinstellung gemäß § 153 a Strafprozeßordnung

Im 15. Tätigkeitsbericht (Nr. 6.8.4) und im 16. Tätigkeitsbericht (Nr. 7.5) habe ich den Umstand, daß bei Einstellung eines Verfahrens bei Erfüllung einer Geldauflage zugunsten einer gemeinnützigen Einrichtung diese nicht nur vom Strafverfahren, sondern auch von der Person des Beschuldigten in Kenntnis gesetzt wird, eingehend gewürdigt. Wegen der Eingabe eines Bürgers habe ich mich an das Staatsministerium der Justiz gewandt.

Dieses hält an seiner Auffassung fest, daß die Übermittlung der Daten des Beschuldigten an die gemeinnützige Einrichtung angesichts des Einverständnisses des Beschuldigten mit einer Verfahrenseinstellung nach § 153 a Abs. 1 Nr. 2 StPO gerechtfertigt sei. Im übrigen beruft sich das Justizministerium auf praktische Erfordernisse: Es reiche nicht aus, daß sich nur der Beschuldigte selbst mit dem Bußgeldempfänger dadurch in Verbindung setze, daß er bei seiner Zahlung das staatsanwaltschaftliche Aktenzeichen angibt. Die Erfahrung zeige nämlich, daß eine Vielzahl von Beschuldigten ohne Hilfestellung seitens des Bußgeldempfängers Schwierigkeiten damit habe, ordnungsgemäß und fristgerecht die Zahlungsauflage zu erfüllen. Es komme immer wieder zu Unstimmigkeiten bezüglich des Aktenzeichens der Staatsanwaltschaft, der Bankverbindung des Bußgeldempfängers oder zu reinen Fristversäumnissen. Sofern dem Bußgeldempfänger lediglich das Aktenzeichen der Staatsanwaltschaft mitgeteilt werde, führten schon geringfügige Unrichtigkeiten dazu, daß eine Zahlung nicht oder nur mit unverhältnismäßigem Aufwand zugeordnet werden könne. Unterbleibe eine Mitteilung der Staatsanwaltschaft an den Bußgeldempfänger, so laufe der Beschuldigte Gefahr, trotz Bezahlung der Geldauflage mit einem Strafbefehlsverfahren oder einer Anklage überzogen zu werden. In der Praxis komme es sogar vor, daß hernach erlassene Strafbefehle rechtskräftig würden, weil die Betroffenen offenbar irrtümlich meinten, ihre Zahlung mache einen Einspruch überflüssig.

Auch wenn die vorgetragenen Argumente nicht von der Hand zu weisen sind, gelten meine Bedenken grundsätzlicher Art fort, daß nämlich die Zustimmung zur Verfahrenserledigung nach § 153 a Abs. 1 Nr. 2 StPO nicht automatisch als Einverständnis mit der Übermittlung personenbezogener Daten an den Geldbußenempfänger angesehen werden kann.

Im Interesse eines akzeptablen Ausgleichs zwischen den Beschuldigten und den Erfordernissen der Praxis habe ich das Justizministerium nunmehr um Überprüfung gebeten, ob bei Erholung der Zustimmung des Beschuldigten mit einer Sachbehandlung nach § 153 a StPO gleichzeitig dessen Einverständnis mit der Übermittlung seiner Daten an den Bußgeldempfänger erfragt werden könnte. Ich gehe davon aus, daß in der überwiegenden Mehrzahl der Fälle der Beschuldigte mit einer solchen Sachbehandlung einverstanden ist. In den übrigen Fällen erscheint es sachgerecht, wenn der Beschuldigte das Risiko einer rechtzeitigen und zuordenbaren Zahlung selbst trägt.

Das Justizministerium hat zugesagt, meinen Vorschlag auf der nächsten Dienstbesprechung mit den Leiterinnen und Leitern der Staatsanwaltschaften zu erörtern.

7.6.7 Registermäßige Behandlung der Anzeigen nach dem Geldwäschegesetz durch die Staatsanwaltschaften

Nach § 11 Abs. 1 Satz 1 Geldwäschegesetz haben Kreditinstitute, Finanzinstitute, die Deutsche Bundespost und Spielbanken bei der Feststellung von Tatsachen, die darauf schließen lassen, daß eine Finanztransaktion einer Geldwäsche nach § 261 Strafgesetzbuch dient oder im Falle ihrer Durchführung dienen würde, diese unverzüglich den zuständigen Strafverfolgungsbehörden anzuzeigen. Auf entsprechende Anfrage hat mir das Staatsministerium der Justiz unter Berufung auf das Ergebnis eines bundesweiten Erfahrungsaustausches der Generalstaatsanwälte zu Fragen der Geldwäsche mitgeteilt, daß solche Verdachtsanzeigen nach dem Geldwäschegesetz bundesweit (mit Ausnahme der Freien und Hansestadt Hamburg) als Strafanzeigen im Sinne des § 158 Abs. 1 Strafprozeßordnung angesehen und in das Js-Register (Register für Verfahren gegen namentlich bekannte Personen) eingetragen werden.

Meiner Auffassung nach unterscheiden sich Verdachtsanzeigen im Sinne des Geldwäschegesetzes grundsätzlich von den in § 47 Abs. 1 b Aktenordnung angesprochenen Anzeigen, die sich gegen eine bestimmte Person richten.

Während Strafanzeigen nach § 47 Aktenordnung vom Willen des Anzeigeerstatters getragen sind, daß der von ihm Beschuldigte für ein bestimmtes Verhalten strafrechtlich zur Verantwortung gezogen wird, sind Institute und Spielbanken von Gesetzes wegen verpflichtet, ihnen verdächtig erscheinende Finanztransaktionen den zuständigen Strafverfolgungsbehörden unverzüglich anzuzeigen.

Diesem Umstand ist meines Erachtens durch eine differenzierte registermäßige Behandlung Rechnung zu tragen: Leitet die Staatsanwaltschaft aufgrund einer Verdachtsanzeige nach dem Geldwäschegesetz wegen bestehenden Anfangsverdachts einer Straftat ein Ermittlungsverfahren ein und ist der Beschuldigte bekannt, so steht einer Eintragung in das Js-Register nichts entgegen. Besteht jedoch gegen den Beschuldigten kein Anfangsverdacht einer Straftat, so sollte das Verfahren entweder in ein neu zu errichtendes besonderes Register für Verdachtsanzeigen oder nach dem Geldwäschegesetz in das allgemeine (AR-)Register eingetragen werden. Ich habe dem Justizministerium mitgeteilt, daß ich die derzeitige Verfahrensweise - nicht zuletzt im Hinblick

auf eine künftige **bundesweite** Speicherung solcher Anzeigen im zentralen staatsanwaltschaftlichen Verfahrensregister - aus datenschutzrechtlicher Sicht für nicht unbedenklich erachte. Das Justizministerium hat sich dieser Auffassung nicht angeschlossen, so daß Verdachtsanzeigen weiterhin in Strafakten gespeichert und die entsprechenden personenbezogenen Daten in Zukunft bundesweit von jedem Staatsanwalt für einen bestimmten Zeitraum abgerufen werden können.

7.6.8 Eintragung der Schuldunfähigkeit in das Bundeszentralregister

Bereits im 15. Tätigkeitsbericht 1993 (Nr. 6.8.5) habe ich ausführlich auf die Problematik hingewiesen, daß **Verfügungen der Staatsanwaltschaft**, mit denen ein Strafverfahren **wegen erwiesener oder nicht auszuschließender Schuldunfähigkeit** oder auf Geisteskrankheit beruhender Verhandlungsunfähigkeit ohne Verurteilung **eingestellt wird**, **in das Bundeszentralregister einzutragen sind**, dieser Umstand jedoch häufig dem Betroffenen nicht bekannt wird.

Das Staatsministerium der Justiz hat mir in der Zwischenzeit mitgeteilt, daß das Problem der Information des Beschuldigten bei Verfahrenseinstellungen wegen Schuldunfähigkeit bei der jährlichen Dienstbesprechung mit den Leiterinnen und Leitern der bayerischen Staatsanwaltschaften erörtert worden sei. Dabei sei dargelegt worden, daß die Eintragung in das Bundeszentralregister wegen ihrer Auswirkungen für den Betroffenen ein besonderes Interesse an seiner Unterrichtung über den Verfahrensausgang im Sinne des § 170 Abs. 2 Satz 2, 2. Halbsatz Strafprozeßordnung (StPO) begründen könne. Ferner sei geraten worden, bei einer Einstellung wegen Schuldunfähigkeit in der Mitteilung an den Betroffenen auf diesen Umstand hinzuweisen.

Darüber hinaus sei meine Auffassung erläutert worden, daß der Betroffene im Rahmen der Mitteilung zusätzlich über die Eintragung in das Bundeszentralregister und deren Folgen unterrichtet werden sollte. Da der Gesetzgeber dieses Problem jedoch im Rahmen der beabsichtigten Änderung des Bundeszentralregistergesetzes aufgreifen wolle, sei davon abgesehen worden, die Staatsanwaltschaften anzuweisen, in jedem Fall den Beschuldigten über die Eintragung in das Bundeszentralregister und deren Folgen zu informieren. Das Bundesjustizministerium beabsichtige, in der derzeitigen Legislaturperiode einen konsensfähigen Gesetzentwurf vorzulegen, der einem sachgerechten Ausgleich zwischen den berechtigten Schutzinteressen der Betroffenen und den Informationsinteressen von Rechtspflege und Verwaltung Rechnung trage.

Von einem Kollegen wurde mir mitgeteilt, daß ein außerbayerisches Justizministerium im Erlaßwege eine Übergangsregelung getroffen habe. Diese geht dahin, daß bis zu einer bundesgesetzlichen Regelung durch die in Vorbereitung befindliche Novellierung des Bundeszentralregistergesetzes in Fällen einer Einstellung wegen Schuldunfähigkeit um Prüfung gebeten wird, ob der Beschuldigte über die Bestimmungen in § 170 Abs. 2 Satz 2 StPO und Nr. 88 der Richtlinien

für das Straf- und Bußgeldverfahren hinaus ohne Gefährdung schutzwürdiger Interessen über den Grund der Einstellung des gegen ihn gerichteten Verfahrens in Kenntnis gesetzt werden kann. Eine Unterrichtung werde regelmäßig dann erfolgen können, wenn die Schuldunfähigkeit zur Zeit der Tat nur von vorübergehender Natur gewesen ist oder sonst Anhaltspunkte dafür bestehen, daß in absehbarer Zeit ein Antrag auf Entfernung der Eintragung nach § 25 des Bundeszentralregistergesetzes gestellt werden kann. **Es werde sich empfehlen, in solchen Fällen in der Einstellungsnachricht auf dieses Antragsrecht hinzuweisen**.

Da der vom Bundesministerium der Justiz angekündigte Entwurf zur Novellierung des Bundeszentralregistergesetzes weiter auf sich warten läßt, bin ich nochmals an das Staatsministerium der Justiz herangetreten: Für die Übergangszeit bis zur Novellierung des Bundeszentralregistergesetzes würde ich es begrüßen, wenn der Betroffene in geeigneten Fällen auf das Recht, einen Antrag auf Entfernung der Eintragung nach § 25 Bundeszentralregistergesetz zu stellen, hingewiesen würde.

7.6.9 Protokollierung der Einsichtnahme in das Grundbuch

Zuletzt in meinem 16. Tätigkeitsbericht (Nr. 7.2.4) habe ich zum sog. Registerverfahrenbeschleunigungsgesetz und zum EDV-System "SOLUM-STAR" ausführlich Stellung genommen. Nachdem eine Neuregelung der Grundbucheinsicht aus dem Registerverfahrenbeschleunigungsgesetz ausgeklammert worden war und im Zuge einer nachfolgenden Überarbeitung der Grundbuchverfügung vorgenommen werden sollte, ging ich davon aus, daß Forderungen nach einer Protokollierung der Einsichtnahme in das maschinell geführte Grundbuch im Verfahren zur Änderung der Grundbuchverfügung zeitnah weiterverfolgt werden könnten.

Zwischenzeitlich wurde zwar die Befristung für die Vorschriften über das maschinell geführte Grundbuch aufgehoben, an eine Neuregelung der Grundbucheinsicht ist offenbar jedoch nicht mehr gedacht. Aus dem Bereich des Bundesministeriums der Justiz war zu erfahren, daß nicht absehbar sei, wann mit einem Entwurf zur Änderung der Vorschriften über die Grundbucheinsicht zu rechnen sei. Damit wird die Berücksichtigung wichtiger Belange des Datenschutzes auf unbestimmte Zeit verschoben.

Das Staatsministerium der Justiz stellt sich auf den Standpunkt, daß selbst für eine Auswahl-Protokollierung eine bundesgesetzliche Regelung erforderlich sei. Folglich stünden die Vorschriften der Grundbuchordnung als abschließende gesetzliche Regelung einer Protokollierung der Einsichtnahme im Grundbuchamt entgegen.

Demgegenüber vertrete ich die Auffassung, daß die derzeit bestehenden gesetzlichen Regelungen der Grundbuchordnung bezüglich des Datenschutzes gerade nicht als abschließend angesehen werden können. Dies zeigt die Entstehungsgeschichte des Registerverfahrenbeschleunigungsgesetzes deutlich. So waren zunächst im Diskussionsentwurf eines Registerverfahrenbeschleunigungsgesetzes (Stand: 17.02.1993) konkrete Neuregelungen zu § 12 Grundbuchordnung, insbesondere zur Frage einer Protokollierung der Einsichtnahme, zum Auskunftsanspruch des Eingetragenen sowie zur Zweckbindung der Daten enthalten. Lediglich aufgrund des Wunsches der Mehrheit der Landesjustizverwaltungen wurde in der Folge die Neuregelung der Einsichtnahme in das Grundbuch - im Hinblick auf die Eilbedürftigkeit des Registerverfahrenbeschleunigungsgesetzes - aus dem Gesetz ausgeklammert und (wie sich aus einem Schreiben des Bun-

desministeriums der Justiz vom 15.07.1994 ergibt) einer "Verordnung zur Änderung des Grundbucheinsichtsrechts" vorbehalten, deren Erlaß für Herbst 1994 geplant war. Überdies war vom Bundesministerium der Justiz bei Ergänzung der Grundbuchverfügung um den Abschnitt VIII "Vorläufige Vorschriften über das maschinell geführte Grundbuch" wegen der **nicht ausreichenden Berücksichtigung von Belangen des Datenschutzes** (insbesondere Protokollierung der Grundbucheinsicht) eine Befristung vorgesehen und darauf verwiesen worden, daß diese Lücke bis zum Erlaß endgültiger Bestimmungen über das maschinell geführte Grundbuch geschlossen werden solle. Im Gegensatz dazu wurde mit der Dritten Verordnung zur Änderung der Verordnung zur Durchführung der Schiffsregisterordnung und zur Regelung anderer Fragen des Registerrechts die Befristung des EDV-Teils der Grundbuchverfügung ab 01.12.1994 aufgehoben, obwohl die erforderlichen datenschutzrechtlichen Ergänzungen nicht vorgenommen worden waren.

Da mithin der Bundesgesetzgeber gerade keine abschließende Regelung über den Datenschutz in der Grundbuchordnung bzw. Grundbuchverfügung getroffen hat, sind ergänzend die Bestimmungen des Bayerischen Datenschutzgesetzes anwendbar. Das bedeutet, daß die personenbezogenen Daten des Einsichtnehmenden nach Identitätsprüfung nach Art. 16 Abs. 1 BayDSG erhoben und diese Daten nach Art. 17 Abs. 1 BayDSG im Rahmen einer (Auswahl-)Protokollierung auch gespeichert werden dürfen, da die Erhebung und zeitlich begrenzte Speicherung zur Erfüllung der in der Zuständigkeit des Grundbuchamts liegenden Aufgaben erforderlich ist. Die Erforderlichkeit ergibt sich aus der Aufgabe des Grundbuchamts, unberechtigten Einsichtnahmen in das Grundbuch entgegenzuwirken. Dem dient die von einer Protokollierung ausgehende Präventivwirkung.

Ich habe daher gegenüber dem Justizministerium nochmals zumindest eine Auswahlprotokollierung gefordert und gebeten, die technischen Voraussetzungen hierfür im EDV-System SOLUM-STAR vorzusehen. Das Justizministerium steht dieser Forderung nach wie vor ablehnend gegenüber.

7.6.10 Datenschutzrechtliche Beurteilung von Forschungsvorhaben im Justizbereich

In jüngerer Zeit wurden mir wiederholt Forschungsvorhaben vor allem aus dem Bereich des Strafvollzugs vom Justizministerium zur datenschutzrechtlichen Beurteilung mitgeteilt. Ich habe dies zum Anlaß genommen, die mir für die datenschutzrechtliche Beurteilung solcher Vorhaben besonders wichtig erscheinenden Gesichtspunkte in einem Papier zusammenzufassen, das ich dem Justizministerium übersandt habe. Danach sind vor allem folgende Forderungen als Konkretisierungen des Rechts auf informationelle Selbstbestimmung und des verfassungsrechtlichen Grundsatzes der Verhältnismäßigkeit zu berücksichtigen:

1. Die Übermittlung **personenbezogener** Daten muß für die Durchführung des Forschungsvorhabens **erforderlich** sein. Der Zweck des Forschungsvorhabens darf nicht unter Verwendung anonymisierter Daten oder von Pseudonymen erreicht werden können.

2. Die Übermittlung personenbezogener Daten zu Forschungszwecken setzt grundsätzlich die **Einwilligung des Betroffenen** voraus. Vor seiner Entscheidung, ob er mit der Datenübermittlung einverstanden ist, ist der Betroffene dahingehend aufzuklären, daß seine Teilnahme freiwillig ist, wer Träger und Leiter des Forschungsprojekts ist, welchem Zweck das Forschungsvorhaben dient, daß die erhobenen Daten ausschließlich zu Zwekken wissenschaftlicher Forschung im Rahmen des konkreten Forschungsvorhabens verarbeitet werden, auf welche Art die Daten verarbeitet werden, welcher Personenkreis Kenntnis von den erhobenen Daten erhält und zu welchem Zeitpunkt die Daten anonymisiert bzw. gelöscht werden.

3. Eine Ausnahme vom Erfordernis der vorherigen Einwilligung des Betroffenen ist nur zulässig, wenn der Forschungszweck ansonsten nicht oder nur mit unverhältnismäßigem Aufwand erreicht werden könnte. In diesem Falle ist jedoch die Übermittlung personenbezogener Daten etwa durch Gewährung von Akteneinsicht nur dann gerechtfertigt, wenn ein **öffentliches Interesse an dem Forschungsvorhaben** das Geheimhaltungsinteresse des Betroffenen **erheblich überwiegt** (vgl. Art. 17 Abs. 2 Nr. 11 BayDSG) und nicht eine Verpflichtung zur Wahrung gesetzlicher Geheimhaltungspflichten oder von Berufs- oder besonderen Amtsgeheimnissen, die nicht auf gesetzlichen Vorschriften beruhen,

entgegensteht.

4. Zur Gewährleistung einer einheitlichen Entscheidungspraxis und hoher **Entscheidungskompetenz** sollte die Genehmigung der Datenübermittlung zu Forschungszwecken der **zuständigen obersten Landesbehörde** vorbehalten bleiben (siehe zum Inhalt einer solchen Genehmigung z.B. § 75 Abs. 2 SGB X).

5. Die **Gewährung von Akteneinsicht** ist gegenüber der Erteilung von Auskünften aus den Akten **nachrangig**. Kann der Forschungszweck ebensogut durch Auskünfte aus den Akten - falls möglich in anonymisierter Form - erreicht werden, so hat Akteneinsicht zu unterbleiben.

6. **Akteneinsicht ist grundsätzlich bei der speichernden Stelle** zu gewähren. Lediglich wenn dies nicht möglich oder mit einem unzumutbaren Aufwand verbunden ist, können die Akten zur Einsichtnahme an die forschende Stelle übersandt werden.

7. Wirken bei einem von einer öffentlichen Stelle durchgeführten Forschungsvorhaben Personen mit, die nicht Amtsträger oder für den öffentlichen Dienst besonders Verpflichtete sind, so sind diese entsprechend § 1 des Verpflichtungsgesetzes **zur Geheimhaltung zu verpflichten**. Bei privaten Forschungsvorhaben sollten die Mitarbeiter auf das Datengeheimnis verpflichtet werden (§ 5 BDSG).

8. Die übermittelten personenbezogenen Daten dürfen **nur im Rahmen des konkreten Forschungsvorhabens** verarbeitet und genutzt werden, für das sie übermittelt wurden. Die an die forschende Stelle übermittelten personenbezogenen Daten sind gegen unbefugte Kenntnisnahme durch Dritte zu schützen. Nicht-öffentliche Stellen sind durch geeignete Auflagen zur Einhaltung dieser Grundsätze zu verpflichten.

9. Die übermittelten personenbezogenen Daten sind, sobald der Forschungszweck dies erlaubt, zu **anonymisieren**.

10. Ohne Einwilligung des Betroffenen dürfen personenbezogene Daten nur veröffentlicht

werden, wenn dies für die Darstellung von Forschungsergebnissen über Ereignisse der Zeitgeschichte unerläßlich ist und überwiegende schutzwürdige Interessen des Betroffenen nicht entgegenstehen.

11. Ist der Datenempfänger eine nicht-öffentliche Stelle, so ist sicherzustellen, daß der zuständige Landesbeauftragte für den Datenschutz die Beachtung des Datenschutzes bei Durchführung des Forschungsvorhabens anlaßunabhängig kontrollieren darf. Dies gilt auch, wenn die personenbezogenen Daten nicht in Dateien verarbeitet werden.

12. Es ist sicherzustellen, daß der Schutz personenbezogener Daten, die zuvor durch ein besonderes Berufs- oder Amtsgeheimnis geschützt waren, bei Forschungseinrichtungen vor Zugriffen staatlicher Stellen - insbesondere durch Strafverfolgungsbehörden - gewährleistet ist.

Im Berichtszeitraum wurde mir ein Forschungsvorhaben zur Fortschreibung der therapeutischen Konzeption einer Justizvollzugsanstalt mitgeteilt. Die bei der Datenerhebung in Betracht kommenden Strafgefangenen konnten über ihre Teilnahme frei entscheiden, für ihre Einwilligungserklärung war ein Formblatt entworfen worden.

Zur Verbesserung des Datenschutzes habe ich vor allem folgende Anregungen gegeben, die vom Staatsministerium der Justiz aufgegriffen wurden:

- Im Interesse einer "informierten" Einwilligung des Gefangenen sollte sich dieser zuvor in groben Zügen über das Programm der Datenerhebung informieren können. Darüber hinaus sollte ausdrücklich darauf hingewiesen werden, daß die Mitwirkung am Forschungsprojekt freiwillig ist und der Gefangene bei Verweigerung der Mitwirkung keinerlei Nachteile zu befürchten hat.
- Im Zuge des Forschungsvorhabens eingesetzte Personen, die nicht bereits aufgrund eines öffentlich-rechtlichen Dienstverhältnisses zur Amtsverschwiegenheit verpflichtet sind, sollten nach den Vorschriften des Verpflichtungsgesetzes hierauf verpflichtet werden.
- Es muß sichergestellt sein, daß personenbezogene Daten nur den mit dem Forschungsvorhaben betrauten Mitarbeitern zur Kenntnis gelangen und ausschließlich für das Forschungsvor-

haben verwendet werden.

- Hinsichtlich der Erhebung von personenbezogenen Daten Dritter beim Strafgefangenen sind die Voraussetzungen des Art. 16 Abs. 2 Nr. 2 BayDSG zu beachten.

  Wegen überwiegender schutzwürdiger Interessen wurde eine Reihe von Daten von der Erhebung ausgenommen.

7.6.11 Versendung von Übersichten über die Diensteinnahmen der Gerichtsvollzieher

Ein Gerichtsvollzieher eines Amtsgerichts hat sich an mich gewandt und vorgetragen, mit Schreiben des Staatsministeriums der Justiz vom 18. Juli 1995 seien an die Präsidenten der Oberlandesgerichte München, Nürnberg und Bamberg Übersichten über die Diensteinnahmen der Gerichtsvollzieher für das Jahr 1994 übersandt worden. Dabei seien mehrere Gerichtsvollzieher - darunter auch der Petent - namentlich und unter Nennung des jeweiligen Amtsgerichts und des erzielten Einnahmebetrags aufgeführt worden. Dieses Schreiben sei mittlerweile an die Amtsgerichte weitergeleitet worden.

Der Petent hält eine namentliche Nennung der aufgeführten Gerichtsvollzieher für nicht erforderlich und sieht sich dadurch in seinen Rechten verletzt.

Die von mir erbetene Stellungnahme des Staatsministeriums der Justiz bestätigte im wesentlichen den vorgetragenen Sachverhalt, wobei die Daten im Zuge der Auswertung der für das Jahr 1994 vorgelegten Übersichten über die Diensteinnahmen der Gerichtsvollzieher mit Schreiben des Staatsministeriums der Justiz an die Präsidenten der Oberlandesgerichte sowie Amtsgerichtsdirektoren in Einzelfällen von diesen an Gerichtsvollzieher gelangt waren.

Das Justizministerium ist der Auffassung, daß es sich bei den Gebühren, Wegegeldern und Schreibauslagen einzelner Gerichtsvollzieher nicht um persönliche Daten des jeweiligen Gerichtsvollziehers handele, da die im Zusammenhang mit der beruflichen Tätigkeit anfallenden Kosten vom Gerichtsvollzieher für die Staatskasse eingezogen werden. Dessen ungeachtet sei veranlaßt worden, daß in künftigen Fällen Gerichtsvollzieher über die Diensteinnahmen anderer Gerichtsvollzieher nur ohne Namensangabe unterrichtet werden.

Zwar kann ich die mit dem genannten Schreiben des Staatsministeriums der Justiz vorgenommene Datenübermittlung nicht beanstanden, da keine Daten an die Präsidenten der Oberlandesgerichte übermittelt wurden, die dort nicht ohnehin bereits aufgrund der vorgelegten Übersichten bekannt gewesen wären.

Soweit jedoch die Direktoren einzelner Amtsgerichte im Zuge ihrer Überprüfungen das vorge-

nannte Schreiben des Justizministeriums mit personenbezogenen Daten einzelner Gerichtsvollzieher (Zahlen über bestimmte Diensteinnahmen) **auch anderen Gerichtsvollziehern** zur Kenntnis gebracht haben, halte ich diese Datenübermittlung nicht für erforderlich und damit nicht für zulässig. Das Staatsministerium der Justiz räumt selbst ein, daß für die Überprüfungen auch eine Unterrichtung der betroffenen Gerichtsvollzieher über die Diensteinnahmen anderer Gerichtsvollzieher **ohne Namensangabe** ausgereicht hätte. Das Justizministerium hat daher die Präsidentin und Präsidenten der Oberlandesgerichte gebeten, in künftigen Fällen entsprechend zu verfahren.

Da das Justizministerium das zur künftigen Beachtung des Datenschutzes Erforderliche veranlaßt hat, habe ich von einer förmlichen Beanstandung des Vorgangs abgesehen.

7.6.12 Zustellung eines Pfändungs- und Überweisungsbeschlusses durch Gerichtsvollzieher

Im Berichtszeitraum hat sich eine Petentin an mich gewandt mit dem Vorbringen, zwei gegen sie erlassene Pfändungs- und Überweisungsbeschlüsse seien in ihrer Arbeitsstelle an eine Aushilfskraft **offen** zugestellt worden.

Ich habe den zuständigen Amtsgerichtspräsidenten um Stellungnahme gebeten und auf die Neufassung des § 36 Nr. 3 Abs. 3 der Geschäftsanweisung für Gerichtsvollzieher gemäß Bekanntmachung des Staatsministeriums der Justiz vom 24.11.1994 hingewiesen. Danach braucht bei der Ersatzzustellung mit der Aufforderung zur Abgabe der Drittschuldnererklärung das zuzustellende Schriftstück nur dann nicht verschlossen zu werden, **wenn der Ersatzempfänger zur Abgabe der Drittschuldnererklärung befugt ist**. Ansonsten verbleibt es bei der Regelung des § 36 Nr. 3 Abs. 1 der Geschäftsanweisung für Gerichtsvollzieher, wonach der Gerichtsvollzieher das zu übergebende Schriftstück vor der Übergabe oder Niederlegung zu verschließen hat.

Das Justizministerium hat eingeräumt, daß das Verhalten des Gerichtsvollziehers nicht dem vorgeschriebenen Verfahren entsprochen hat. Nicht nur der betroffene Gerichtsvollzieher, sondern auch die anderen bei diesem Amtsgericht tätigen Gerichtsvollzieher seien auf die Bedeutung der besonderen Vorschriften über die Ersatzzustellung hingewiesen worden.

8. Gemeinden, Städte und Landkreise

8.1 Prüfung von Landratsämtern

Bei der Prüfung von Landratsämtern mußte ich folgende Mängel feststellen, die - soweit nichts anderes ausgeführt - von den Landratsämtern selbst behoben wurden:

Telefondatenerfassung

In einem Landratsamt wurden die Verbindungsdaten von ausgehenden Telefongesprächen erfaßt. Wurde das Telefonat als Privatgespräch gekennzeichnet, wurden zu Abrechnungszwecken in regelmäßigen Abständen Ausdrucke der erfaßten Daten (Nummer der rufenden Nebenstelle, Datum, Uhrzeit und Dauer des Gesprächs, verbrauchte Gebühreneinheiten, Kosten des Gesprächs) erstellt. Bei dienstlichen Gesprächen erfolgte eine Auswertung zu Abrechnungszwecken nur bei den Stellen, für die im Rahmen des Kreishaushalts ein getrennter Sachaufwand festgestellt wird. Dabei wurden alle Nebenstellen der jeweiligen Verwaltungseinheit zusammengefaßt, unabhängig davon, wer telefoniert hatte, und die verbrauchten Einheiten als Summe ausgedruckt. Der **Personalrat** wurde zu dieser Telefondatenerfassung **nicht beteiligt**.

Anlagen zur Telefondatenerfassung sind technische Einrichtungen zur Überwachung des Verhaltens oder der Leistung der Beschäftigten und unterliegen daher der Mitbestimmung des Personalrats (Art. 75 a Abs. 1 Nr. 1 Bayer. Personalvertretungsgesetz - BayPVG). Die Unterrichtung des Personalrats bedarf der Schriftform (Art. 70 Abs. 2 BayPVG). Eine Telefondatenerfassung ohne eine ordnungsgemäße Beteiligung des Personalrats ist unzulässig. Das Mitbestimmungserfordernis gilt bei Dienst- und Privatgesprächen und zwar auch dann, wenn die Bediensteten freiwillig am Verfahren zur Abrechnung von Privatgesprächen teilnehmen.

In einem anderen Landratsamt wurde zur **Abrechnung der Privatgespräche** ca. alle 4 - 6 Wochen ein Ausdruck erstellt, der u.a. die **vollständige Zielnummer** enthielt. Die angerufenen Nummern dürfen ohne Antrag des Betroffenen jedoch nur verkürzt um wenigstens die letzten beiden Ziffern ausgedruckt werden (vgl. Nr. 9.3 des 8. Tätigkeitsberichts, Nr. 12.3 des 13. Tätigkeitsberichts, Nr. 19.4 des 14. Tätigkeitsberichts).

Immissionsschutzrecht - Planauslegung

Bei **öffentlich ausliegenden Planunterlagen** in immissionsschutzrechtlichen Verfahren wurde der Name der Einsicht nehmenden Bürger notiert. Die immissionsschutzrechtlichen Verfahrensbestimmungen sehen keine Namensfeststellung der Personen vor, die in **öffentlich** ausliegende Planunterlagen Einsicht nehmen. Durch das unzulässige Notieren von Namen bei einer öffentlichen Auslegung können sich möglicherweise Bürger von einer Einsichtnahme abschrecken lassen. Auch das Ziel der öffentlichen Auslegung wird dadurch beeinträchtigt. Dabei ist es unerheblich, ob die Namen zur Akte genommen werden oder nach dem Ende der Einwendungsfrist vernichtet werden (vgl. 14. Tätigkeitsbericht Nr. 17.3). Die unzulässige Namensaufzeichnung habe ich beanstandet.

Datenübermittlung von der Kfz-Zulassungsstelle an die Sozialhilfeverwaltung

Die Sozialhilfeverwaltung überprüfte im Einzelfall bei konkretem Anlaß, ob Sozialhilfeempfänger Halter eines Kraftfahrzeuges waren. Wurde bei dieser Überprüfung festgestellt, daß ein Leistungsempfänger **Halter eines oder mehrerer Kraftfahrzeuge** war, ließ sich die Sozialhilfeverwaltung von der Zulassungsstelle **weitere Daten zum Fahrzeug** (z. B. Baujahr, Fahrzeugtyp) übermitteln. Für die Übermittlung dieser Fahrzeugdaten besteht weder in § 117 Bundessozialhilfegesetz (BSHG) noch in den straßenverkehrsrechtlichen Vorschriften eine Rechtsgrundlage. Benötigt die Sozialhilfeverwaltung weitere Daten zum Fahrzeug, muß sie diese bei dem als Halter eines Kfz ermittelten Hilfeempfänger selbst erheben oder sich von ihm das Einverständnis zur Datenübermittlung durch die Zulassungsstelle geben lassen. Der Sozialhilfeempfänger hat dabei die Pflicht zur Mitwirkung gem. §§ 60 ff. Sozialgesetzbuch I.

Auskünfte aus dem örtlichen Fahrzeugregister

Bei der einfachen Registerauskunft aus dem örtlichen Fahrzeugregister gem. § 39 Abs. 1 Straßenverkehrsgesetz (StVG) ist zu beachten, daß der Auskunftsuchende darlegen muß, daß er die Daten zur Geltendmachung, Sicherung oder Vollstreckung oder zur Befriedigung oder Abwehr von Rechtsansprüchen im Zusammenhang mit der **Teilnahme am Straßenverkehr** oder zur Erhebung einer Privatklage wegen **im Straßenverkehr begangener Verstöße** benötigt.

Für die Geltendmachung, Sicherung oder Vollstreckung von **nicht** mit der **Teilnahme am Straßenverkehr** im Zusammenhang stehenden Rechtsansprüchen besteht **kein Anspruch auf Auskunft**. Die Behörde kann aber aufgrund einer Ermessensentscheidung Halterdaten (Familienname, Vornamen bzw. Name der juristischen Person, Anschrift) einem Anfragenden übermitteln, wenn dieser **glaubhaft** macht, daß die Voraussetzungen des § 39 Abs. 3 StVG in seinem konkreten Einzelfall erfüllt sind. Die Daten müssen danach zur Geltendmachung, Sicherung oder Vollstreckung von **öffentlichrechtlichen** Ansprüchen in Höhe von mindestens eintausend DM benötigt werden, der Empfänger muß ohne die Kenntnis der Daten zur Geltendmachung, Sicherung oder Vollstreckung nicht in der Lage sein, und er muß die Daten auf andere Weise nicht oder nur mit unverhältnismäßigem Aufwand erlangen können.

Möchte jemand Auskunft aus dem örtlichen Fahrzeugregister, muß er daher entweder den Zusammenhang mit der Teilnahme am Straßenverkehr darlegen (z. B. durch die Angabe eines Unfallortes und -zeitpunktes) oder im Ersuchen muß dargelegt sein, daß die Voraussetzungen des § 39 Abs. 3 StVG vorliegen. Allgemeine Formulierungen wie "in einer zivilrechtlichen Angelegenheit" genügen diesen Anforderungen nicht (vgl. dazu das Merkblatt für Anfragen und Auskünfte aus den Fahrzeugregistern des Bayer. Staatsministeriums für Wirtschaft, Verkehr und Technologie, mit Schreiben vom 03.08.1993 an die nachgeordneten Behörden versandt).

8.2 Datenschutz bei Wahlen

8.2.1 Änderung wahlrechtlicher Vorschriften

Im Berichtszeitraum wurden das Gemeindewahlgesetz und das Landkreiswahlgesetz zu einem Gesetz zusammengefaßt (Gemeinde- und Landkreiswahlgesetz - GLKrWG) und die Gemeinde- und Landkreiswahlordnung (GLKrWO) neu erlassen. Dabei konnte ich erreichen, **daß die Daten der Wahlberechtigten, für die eine Auskunftssperre nach Art. 34 Abs. 5 MeldeG besteht, einschließlich der dazugehörenden fortlaufenden Nummer von der öffentlichen Auslegung der Wählerverzeichnisse ausgenommen werden und auf die Veröffentlichung des Tages der Geburt im Wählerverzeichnis verzichtet wird** (§ 22 Abs. 2 GLKrWO).

Darüber hinaus bin ich der Auffassung, **daß der Gesetzgeber auf die öffentliche Auslegung der Wählerverzeichnisse vollständig verzichten sollte.** Die Erfahrungen aus den vergangenen Wahlen und eine Umfrage, die ich bei verschiedenen Gemeinden durchgeführt habe, haben gezeigt, daß die Bürger die Möglichkeit der Einsichtnahme in das Wählerverzeichnis nicht wahrnehmen. Eine demokratische Kontrolle der Wahlberechtigung **durch interessierte Bürger**, mit der die öffentliche Auslegung der Wählerverzeichnisse begründet wird, findet somit in der Praxis nicht statt. Eine öffentliche Auslegung der Wählerverzeichnisse ist zur demokratischen Kontrolle der Wahlberechtigung auch nicht erforderlich.

8.2.2 Auskünfte an politische Parteien zur Wahlwerbung

Im Vorfeld der Kommunalwahlen 1995 bin ich gefragt worden, ob politischen Parteien zur Wahlwerbung Auskünfte aus den Wählerverzeichnissen und aus Verzeichnissen über Haus- und Grundbesitzer erteilt werden dürfen.

Auskünfte aus dem **Wählerverzeichnis** an politische Parteien zur Wahlwerbung sind nicht zulässig. Nach § 22 Abs. 3 der Wahlordnung für die Gemeinde- und Landkreiswahlen vom 28. August 1995, GVBl S. 605, dürfen **Wahlberechtigte im Zusammenhang mit der Prüfung des Stimmrechts einzelner bestimmter Personen** Auszüge aus den Wählerverzeichnissen fertigen. Die Auszüge dürfen **nur zur Prüfung des Stimmrechts verwendet und Dritten nicht zugänglich gemacht werden**.

Parteien, Wählergruppen und anderen Trägern von Wahlvorschlägen darf jedoch nach Art. 35 Abs. 1 Satz 1 des Meldegesetzes im Zusammenhang mit allgemeinen Wahlen und mit Abstimmungen in den sechs der Stimmabgabe vorangehenden Monaten **Auskunft aus dem Melderegister** über Namen, Doktorgrade und Anschriften von Gruppen von Wahlberechtigten erteilt werden, für deren Zusammensetzung das **Lebensalter** der Betroffenen bestimmend ist (vgl. dazu auch meine Ausführungen unter Nr. 9.1).

Name und Anschrift eines Grundsteuerpflichtigen unterliegen dem Steuergeheimnis nach § 30 der Abgabenordnung (AO). Die Gemeinde darf diese Daten nach § 31 Abs. 3 AO zur Verwaltung anderer **Abgaben** sowie zur Erfüllung sonstiger öffentlicher Aufgaben verwenden und den hierfür zuständigen Gerichten, Behörden oder juristischen Personen des öffentlichen Rechts auf Ersuchen mitteilen, soweit nicht überwiegende schutzwürdige Interessen des Betroffenen entgegenstehen. Eine Übermittlung der grundsätzlich dem Steuergeheimnis unterliegenden Daten an politische Parteien zur Wahlwerbung ist danach nicht zulässig.

8.2.3 Datenverarbeitung im Zusammenhang mit der Bestellung von Wahlvorstandsmitgliedern bzw. Wahlhelfern

Ein Bürger wandte sich mit folgendem Sachvortrag an mich:

Eine Stadt versende die Bescheide, mit denen Wahlberechtigte, die im öffentlichen Dienst beschäftigt sind, als Mitglieder des Wahlvorstandes verpflichtet werden, offen ohne Kuvert in der Dienstpost an die jeweiligen Dienststellen. Die Bescheide würden den Bediensteten der Stadt jeweils an ihrem Arbeitsplatz ausgehändigt. An andere Behörden in der Stadt würden die Bescheide ebenfalls offen ohne Kuvert mit der Dienstpost übermittelt.

Außerdem übermittele die Stadt dem Wahlvorsteher zu den Namen der Mitglieder des Wahlvorstandes noch zusätzliche Daten. Bei Personen die von ihrem Dienstherrn gemeldet worden sind, werde der Name des Dienstherrn übermittelt; bei Personen, die von einer Partei gemeldet worden sind, werde der Name der Partei genannt. . Ich habe zu dem Vorgehen der Stadt folgende Auffassung vertreten:

Offener Versand der Bescheide

Die Stadt leitete den Wahlvorstandsmitgliedern, die einer Behörde angehören, die Bescheide offen, nicht einzeln einkuvertiert, mit der Dienstpost über den Amts- bzw. Behördenleiter zu. Es handelte sich hierbei um eine formlose Aushändigung (eine förmliche Zustellung gem. Art. 5 VwZVG sollte nach dem erklärten Willen der Stadt nicht stattfinden).

Der Inhalt von Bescheiden, mit denen Beschäftigte verschiedener Dienststellen der Stadt und sonstiger öffentlicher Stellen in der Stadt zur Ausübung des Ehrenamtes verpflichtet werden, richtet sich an die jeweils Betroffenen in ihrer Eigenschaft als wahlberechtigte Bürger. Mit der Funktion, die der Einzelne an seiner Dienststelle innehat, stehen diese Schreiben in keinem Zusammenhang.

Bei der offenen Versendung mit der Dienstpost konnten jeweils die mit dem Versendevorgang Betrauten oder diejenigen, über deren Tisch der Vorgang lief, von den in den Bescheiden ent-

haltenen personenbezogenen Daten Kenntnis nehmen. Für diese Kenntnisnahme gibt es keine Rechtsgrundlage, da die in der Kenntnisnahme liegende Datenverarbeitung bzw. -nutzung für die Aufgabenerfüllung der Dienststellen nicht erforderlich war.

Das Einkuvertieren stellt auch keinen unverhältnismäßigen Verwaltungsaufwand im Sinne von Art. 7 Abs. 1 Satz 2 BayDSG dar. Gegen die Übersendung der - einkuvertierten - Schreiben an die Dienstanschrift und damit die Einsparung der Portogebühren bestehen keine Bedenken, so daß sich der finanzielle Aufwand auf die Briefumschläge reduziert, die im Pfennigbereich liegen. Diese Kosten stellen aber keine unzumutbare Ausgabe dar. Sie sind aus Gründen des Datenschutzes zur Vermeidung unzulässiger Datennutzungen und -übermittlungen gerechtfertigt.

Übermittlung des Namens des Dienstherrn und der Partei

Die **Angabe des Dienstherrn** der Wahlvorstandsmitglieder ist - wie überhaupt die Tatsache der Beschäftigung im öffentlichen Dienst - als Qualifikationsmerkmal einer Person, z. B. für die Tätigkeit als Schriftführer, ungeeignet. Die Stadt hat keinen Einfluß auf die Personen, die ihr ein anderer Dienstherr benennt. Soweit aus den Unterlagen im vorliegenden Fall ersichtlich, wird der Dienstherr offenbar auch nur bei den Personen genannt, die sich nicht freiwillig gemeldet haben bzw. nicht über eine Partei gemeldet worden sind, sondern deren Name von ihrem Dienstherrn an die Stadt übermittelt wurde. Der Wahlvorsteher hat damit keine vollständigen Angaben und muß ggf. die Mitglieder des Wahlvorstandes nach ihrer Eignung für bestimmte Tätigkeiten befragen. Im übrigen ist bei der Berufung der Schriftführer zwischen den unterschiedlichen Wahlen zu unterscheiden. § 6 Abs. 4 EuWO und § 6 Abs. 4 BWO sehen jeweils die Berufung des Schriftführers durch den Wahlvorsteher vor, während § 5 Abs. 3 LWO die Bestellung durch die Gemeinde vorsieht.

Auch die Kenntnis des Wahlvorstehers derjenigen Personen, die von einer **Partei** gemeldet worden sind, sowie die Bezeichnung der meldenden Partei, ist für die Aufgabenerfüllung des Wahlvorstehers offensichtlich nicht erforderlich.

8.2.4 Datenerhebung zur Überprüfung des Wählerverzeichnisses

Eine Gemeinde hatte bei Personen mit mehreren Wohnsitzen Zweifel, ob diese noch in der Gemeinde wahlberechtigt sind, weil sie eventuell nicht mehr den Schwerpunkt ihrer Lebensbeziehungen in der Gemeinde haben. Dies ist aber eine der Voraussetzungen für die Wahlberechtigung (Art. 1 Abs. 1 Nr. 2 Gemeinde- und Landkreiswahlgesetz).

Um das Wählerverzeichnis zu bereinigen, versandte die Gemeinde an eine größere Zahl von Einwohnern mit weiteren Wohnsitzen einen Fragenkatalog, mit dem geklärt werden sollte, wo die Betroffenen den Schwerpunkt ihrer Lebensbeziehungen haben. Dieser Katalog enthielt ohne Rücksichten auf den Einzelfall und auf die individuelle Erforderlichkeit der Beantwortung detaillierte Fragen. So wurde z.B. nach der Häufigkeit des Aufenthalts, des Aufenthalts des "Lebenspartners/der Familie" sowie der Belegenheit des "Großteils der persönlichen Habe" befragt.

Fragen in diese Richtung können zwar im Einzelfall zur Feststellung der für das Wahlrecht wesentlichen Frage nach dem Schwerpunkt der Lebensbeziehungen notwendig sein. Voraussetzung wäre zunächst, daß Anhaltspunkte dafür bestehen, daß die Vermutung in Art. 1 Abs. 1 Nr. 2 Satz 3 Gemeinde- und Landkreiswahlgesetz, wonach bei mehreren Wohnsitzen der Schwerpunkt der Lebensbeziehungen dort ist, wo die betroffene Person mit der Hauptwohnung gemeldet ist, nicht zutrifft. Liegen solche Anhaltspunkte vor, dann darf auch danach gefragt werden, nicht aber pauschal und ohne Rücksicht auf die Erforderlichkeit im Einzelfall. Für die Betroffenen muß zudem klar erkennbar sein, welchem Zweck die Fragen dienen, und die Fragen müssen klar und unmißverständlich formuliert sein. Das Schreiben der Gemeinde enthielt im übrigen nicht den nach dem Datenschutzgesetz erforderlichen Hinweis auf die Freiwilligkeit der Beantwortung (Art. 16 Abs. 3 Satz 2 BayDSG).

Die Gemeinde habe ich auf den fehlenden Hinweis auf die Freiwilligkeit hingewiesen und gefordert, eine derartige Erhebung auf die im Einzelfall wirklich erforderlichen Daten zu beschränken sowie schon erhobene nicht erforderliche Daten zu löschen bzw. zu sperren.

8.3 Datenschutz bei Volksbegehren

Im Berichtszeitraum war ich mit datenschutzrechtlichen Fragen im Zusammenhang mit den Eintragungslisten für das Volksbegehren "Mehr Demokratie in Bayern" befaßt.

- Ein Bürger trug vor, er habe mit der Eintragung zum o.b. Volksbegehren in die **gesamte** Eintragungsliste Einblick nehmen können. Dieser Vortrag hat sich im nachhinein nicht bestätigt. Ich möchte ihn jedoch zum Anlaß nehmen, nochmals ausdrücklich auf § 80 Abs. 7 Satz 2 Landeswahlordnung (LWO) hinzuweisen, wonach den Eintragenden **jeweils nur die laufende Liste** (d.h. das laufende Listen**blatt**) vorgelegt werden darf.

- In einem gemeindlichen Mitteilungsblatt wurden außer der Gesamtzahl der Wahlberechtigten und der Gesamtzahl der Eintragungen zum o.b. Volksbegehren noch Aussagen über das **Alter** der an der Eintragung beteiligten Bürger getroffen **und** ein **Vergleich** zwischen der **Beteiligung am Volksbegehren und an den Wahlen** 1994 angestellt. Mehr als die Hälfte der eingetragenen Bürger sei jünger als 35 Jahre gewesen und 2/3 der Eingetragenen hätten sich nicht an den demokratischen Wahlen 1994 beteiligt.

  Die in der Auswertung nach dem Alter und in dem Vergleich bezüglich des Wahlverhaltens liegenden Datennutzungen waren unzulässig und wurden von mir beanstandet.

1. Auskunft über die Zahl der Eintragungen

   Gemäß § 80 Abs. 7 LWO kann die Gemeinde Auskünfte über die Zahl der Eintragungen in die Eintragungslisten zu einem Volksbegehren erteilen. Diese Auskunft kann bereits vor Abschluß der Eintragungslisten erteilt werden.

2. Aussage über das Alter der eintragenden Bürger

   Die Aussage, daß mehr als die Hälfte der sich eintragenden Bürger jünger als 35 Jahre waren, stellt eine statistische Auswertung dar. Für eine derartige Auswertung gibt es keine Rechtsgrundlage im Wahlrecht. Statistische Bearbeitungen sind nur bei Wahlen, also nicht nicht bei Volksbegehren oder -entscheiden, unter den Voraussetzungen des Art. 92 LWG, § 86 LWO durch das Landesamt für Statistik

und Datenverarbeitung vorgesehen. Im übrigen gilt der Grundsatz, daß - mit Ausnahme der Angabe unter 1. - aus den Eintragungslisten keine Auskünfte erteilt werden dürfen.

Auf diese Rechtslage hat das Innenministerium in einer Vollzugsbekanntmachung hingewiesen (Nrn. 8.2 und 8.3 der IMBek vom 06.12.1994, Staatsanzeiger Nr. 50).

3. Vergleich der Beteiligung am Volksbegehren und der Wahlen 1994

Eine Auswertung der Wählerverzeichnisse und Eintragungslisten für einen Vergleich der Teilnahme an Wahlen und Volksbegehren ist ebenfalls unzulässig. Dafür gibt es im Wahlrecht keine Rechtsgrundlage. Das Abstimmungsgeheimnis erfaßt auch die Frage der Teilnahme an der Abstimmung, soweit diese durch die Öffentlichkeit der Wahlhandlung nicht zwangsläufig bekannt ist. Die Wahlgesetze enthalten entsprechende Schutzvorschriften (vgl. z.B. § 88 Abs. 1, 2, § 89 Abs. 2 LWO).

8.4 Einführung des kommunalen Bürgerentscheids

8.4.1 Gesetzliche Regelung

Mit dem Gesetz zur Einführung des kommunalen Bürgerentscheids vom 27.10.95 (GVBl S. 730) wurde in Bayern die Möglichkeit geschaffen, auf kommunaler Ebene Bürgerbegehren einzubringen und Bürgerentscheide durchzuführen. Dazu wurden mit diesem Gesetz u. a. in die Gemeindeordnung der Art. 18a und in die Landkreisordnung der Art. 25a eingefügt.

Meine praktischen Erfahrungen aus Beschwerden sowie aus Anfragen von Bürgern und Kommunen in der kurzen Zeit seit Einführung des kommunalen Bürgerentscheids haben gezeigt, daß die Rechtsvorschriften in folgenden Punkten aus der Sicht des Datenschutzes ergänzungsbedürftig sind:

- Werden die Unterschriften wie bisher auf der Straße, an der Haustür usw. - wie auch in anderen Ländern Deutschlands und in der ersten Stufe zur Zulassung eines Volksbegehrens - gesammelt, unterliegen die dabei erhobenen personenbezogenen Daten bis zu dem Zeitpunkt, an dem die Listen der Gemeinde übergeben werden, nicht den Bestimmungen des Bayerischen Datenschutzgesetzes und nur unter den eingeschränkten Voraussetzungen des § 1 Abs. 2 Nr. 3 BDSG den Vorschriften des Bundesdatenschutzgesetzes, das zudem zur Zweckbestimmung für die Datenverarbeitung nicht-öffentlicher Stellen auch weiter gefaßte Regelungen als das Bayerische Datenschutzgesetz enthält (vgl. § 28 BDSG). Nach geltendem Recht ist es deshalb nicht ausgeschlossen, daß die auf diese Weise erhobenen Daten bis zur Übergabe der Listen an die Gemeinde auch für andere Zwecke als die Durchführung des Bürgerbegehrens Verwendung finden können.

  Bei einer Auflage der Eintragungslisten **nur** in der Gemeinde (vergleichbare Regelung zum Volksbegehren, Art. 68 Abs. 2 Landeswahlgesetz - LWG -, §§ 79, 80 Landeswahlordnung - LWO) würden die Daten der Bürger, die sich eintragen, bereits ab dem Zeitpunkt der Eintragung den weitergehenden Schutzregelungen über die Zweckbestimmung nach dem Bayerischen Datenschutzgesetz unterliegen.

- Abschließende Festlegung der in die Listen einzutragenden personenbezogenen Daten (vergleichbare Regelung zum Volksbegehren, Art. 69 Abs. 2 LWG, § 78 Abs. 1 LWO).

- Der jeweils Eintragende darf von der Gemeinde nur Einsicht in die laufende Liste erhalten (kein Umblättern, vergleichbare Regelung zum Volksbegehren, § 80 Abs. 7 Satz 2 LWO).

- Auskunft aus den Listen darf nur über die Gesamtzahl der Eintragungen gegeben werden (vergleichbare Regelung zum Volksbegehren, § 80 Abs. 7 Satz 1 LWO).

- Es sind Regelungen zur Aufbewahrung und Vernichtung der Listen erforderlich.

8.4.2 Unzulässige Datennutzung bei der Auswertung von Unterschriftenlisten bei Bürgerbegehren

Die Gemeinden und Landkreise müssen bei der Auswertung der für ein Bürgerbegehren abgegebenen Unterschriftenlisten den Grundsatz der Zweckbindung (Art. 17 Abs. 1 Nr. 2 BayDSG) beachten. Die Unterschriften dürfen daher nur hinsichtlich der Frage ausgewertet werden, ob das Bürgerbegehren von einer ausreichenden Zahl antragsberechtigter Gemeinde- bzw. Kreisbürger (Art. 18 a Abs. 6 GO; Art. 25 a Abs. 6 LKrO) unterschrieben worden ist.

Nicht zulässig ist hingegen eine darüber hinausgehende Datenauswertung. So hat z.B. eine Gemeinde in ihrem Mitteilungsblatt bekanntgegeben, bei Prüfung der Unterschriftenlisten sei aufgefallen, daß sich Neubürger, die zum Teil erst wenige Wochen ihren Wohnsitz in der Gemeinde hätten, gegen eine geplante Ersatzanbindung einer Straße ausgesprochen hätten. Hier "darf angenommen" werden, daß die Neubürger "entweder überfordert" gewesen seien oder sog. "Gefälligkeitsunterschriften" geleistet haben.

In einer anderen Gemeinde wurde den Gemeindebediensteten vom ersten Bürgermeister nach Überprüfung der Unterschriftenlisten in einem Rundschreiben empfohlen, sich zukünftig "im eigenen Interesse" bei ähnlichen Fällen "vorab in der Hauptverwaltung zu informieren", damit sie nicht "in eine völlig falsche Richtung" liefen bzw. sich "für eine populistisch ausgerichtete Sache benutzen" ließen. In beiden Fällen habe ich die wegen Verstoßes gegen die Zweckbindung unzulässigen Datennutzungen gemäß Art. 31 Abs. 1 BayDSG beanstandet. Auf meine Anregung hin hat das Innenministerium die Gemeinden und die Landkreise auf die Beachtung des Grundsatzes der Zweckbindung bei der kommunalrechtlichen Überprüfung der Unterschriftenlisten für Bürgerbegehren hingewiesen.

8.5 Weitergabe von Daten zu einem Grundstücksverkauf an eine politische Partei

In einer Gemeinde hatte der zweite Bürgermeister Daten zu einem Grundstücksverkauf, die ihm in seiner **dienstlichen Eigenschaft bekannt geworden** waren, an eine politische Partei weitergegeben. Die Daten wurden anschließend in einer Parteibroschüre zu Wahlkampfzwecken veröffentlicht.

Die Weitergabe dieser Daten war unzulässig, da dafür keine Rechtsgrundlage vorlag und die Betroffenen auch nicht eingewilligt hatten (Art. 15 Abs. 1 BayDSG). Ich habe die Weitergabe deshalb beanstandet.

Die Datenübermittlung beurteilte sich, da ein Einverständnis der Betroffenen nicht vorlag, nach Art. 19 Abs. 1 Nr. 2 BayDSG, der neben der Vorschrift des Art. 40 des Gesetzes über die kommunalen Wahlbeamten (KWBG), die allgemein die Verschwiegenheitspflicht der kommunalen Wahlbeamten regelt, in diesem Fall anwendbar war. Danach ist die Übermittlung personenbezogener Daten an nicht-öffentliche Stellen zulässig, wenn die nicht-öffentliche Stelle ein berechtigtes Interesse an der Kenntnis der zu übermittelnden Daten glaubhaft darlegt und der Betroffene kein schutzwürdiges Interesse an dem Ausschluß der Übermittlung hat.

Diese Voraussetzungen lagen hier nicht vor. Zum einen bestand kein berechtigtes Interesse der Datenempfänger an den der Gemeinde vorliegenden personenbezogenen Angaben. Außerdem hatten die Betroffenen ein schutzwürdiges Interesse daran, daß nicht Angaben, die der Gemeindeverwaltung im Rahmen ihrer Aufgabenerfüllung bekannt geworden sind, Dritten zugänglich gemacht werden. Ein Bürger darf darauf vertrauen, daß Schreiben, Verträge usw., die sich auf ihn beziehen und der Gemeinde vorliegen, **entsprechend den Bestimmungen des Verwaltungsverfahrensrechts, der Gemeindeordnung und sonstiger spezialgesetzlicher Regelungen behandelt** und Daten daraus nicht ohne seine Einwilligung, auch nicht auszugsweise, an Dritte weitergegeben werden.

8.6 Veröffentlichung eines Schriftvergleichs

Ein Bürgermeister ließ ein Schreiben verteilen, in dem er Handschriftproben einer namentlich bezeichneten Bürgerin mit der Schrift eines anonymen öffentlichen Aushangs, in dem die Gemeindeführung verunglimpft worden war, verglich. Die Handschriftproben der Bürgerin waren gemeindlichen Akten entnommen worden. Der Bürgermeister verdächtigte die Bürgerin der Urheberschaft des anonymen Aushangs.

Die Veröffentlichung personenbezogener Daten der Bürgerin aus gemeindlichen Unterlagen in dem Flugblatt war rechtswidrig. Die Voraussetzungen des Art. 19 Abs. 1 Nr. 2 BayDSG für eine Datenübermittlung lagen ersichtlich nicht vor. Ich habe die Unterschriftsveröffentlichung deshalb beanstandet.

8.7 Veröffentlichung personenbezogener Daten von Widerspruchsführern

Der Bürgermeister einer Gemeinde hat in einer Beilage zum amtlichen Mitteilungsblatt im Zusammenhang mit einem geplanten Turnhallenneubau einen Lageplan mit den **Grundstücken der Widerspruchsführer** gegen das Vorhaben, die **Namen** der Widerspruchsführer sowie die Beurteilung der Widersprüche durch den Bürgermeister veröffentlicht. Die Öffentlichkeit und die Widerspruchsführer sollten dadurch auf die Verzögerung des Turnhallenbaus und die dadurch zu erwartende Kostensteigerung aufmerksam gemacht werden. Die Veröffentlichung war unzulässig:

Einwendungen gegen Bauvorhaben sind zwar grundsätzlich in öffentlicher Sitzung des Gemeinderats zu behandeln (Art. 52 Abs. 2 GO). Soweit es zur Beratung und Beschlußfassung im Gemeinderat erforderlich ist, können die Einwendungen in öffentlicher Gemeinderatssitzung auch verlesen werden oder den Gemeinderatsmitgliedern in Ablichtung übergeben werden. Dritte können sich aus der Tagesordnung und in der öffentlichen Sitzung über die Angelegenheit informieren. Sie haben jedoch kein berechtigtes Interesse an darüber hinausgehenden Informationen.

Die Veröffentlichung personenbezogener Daten der Widerspruchsführer in einem Informationsblatt, das mit dem gemeindlichen Mitteilungsblatt verbreitet wurde, verletzte deren schutzwürdige Belange. Sie durften darauf vertrauen, daß ihre Einwendungen entsprechend den Bestimmungen der Gemeindeordnung und des Verwaltungsverfahrensrechts behandelt werden und im Bereich der Verwaltung und des zuständigen Entscheidungsgremiums verbleiben würden. Im gemeindlichen Amtsblatt dürfen zwar die Niederschriften öffentlicher Sitzungen veröffentlicht werden, wenn der Gemeinderat einen entsprechenden Beschluß faßt, jedoch nur mit dem in Art. 54 Abs. 1 GO vorgeschriebenen Mindestinhalt. Dies gilt auch dann, wenn die Widerspruchsführer zum Teil in der Gemeinde bekannt waren. Eine mehr oder weniger auf dem Vernehmen beruhende teilweise Bekanntheit einzelner Betroffener als Widerspruchsführer in der Gemeinde rechtfertigt es nicht, die Widerspruchsführer, die Lage ihrer Grundstücke usw. in dieser Weise in einer zusammen mit dem amtlichen Mitteilungsblatt der Gemeinde verbreiteten Informationsschrift des Bürgermeisters offiziell quasi an den Pranger zu stellen.

8.8 Herausgabe der Niederschriften über öffentliche Sitzungen des Stadtrats in Form von Disketten an die Stadtratsmitglieder

Eine Stadt bat mich zu prüfen, ob es aus datenschutzrechtlicher Sicht zulässig ist, den Stadtratsmitgliedern die Niederschriften zu öffentlichen Sitzungen des Stadtrats abgespeichert auf Disketten zu überlassen.

Die Gemeindeordnung enthält keine Vorschrift, aus der sich eine Pflicht zur Herausgabe von Niederschriften der Sitzungen des Gemeinderats und seiner Ausschüsse an die Gemeinderatsmitglieder ergibt. Art. 54 Abs. 3 Satz 1 GO sieht neben dem Einsichtsrecht lediglich vor, daß sich die Gemeinderatsmitglieder Abschriften der in **öffentlicher** Sitzung gefaßten **Beschlüsse** erteilen lassen können. Diese Vorschrift legt allerdings nur einen Mindeststandard fest. Der Gemeinderat ist nicht gehindert, in der Geschäftsordnung zu regeln, daß den Gemeinderatsmitgliedern Abschriften der jeweiligen Niederschriften öffentlicher Sitzungen zur Verfügung gestellt werden. Von einer Überlassung der Niederschriften auf Disketten möchte ich allerdings aus den folgenden Gründen abraten:

Bei einer Übermittlung auf Disketten ist eine automatisierte Auswertung der Niederschriften nach vielen verschiedenen Suchkriterien möglich. Die Suchkriterien können beliebig logisch verknüpft werden.

Durch die Möglichkeit der umfassenden, schnellen und problemlosen gezielten personenbezogenen Abfrage bei einer elektronischen Speicherung ergeben sich für die Gemeinderatsmitglieder und die Bürger, deren Angelegenheiten im Gemeinderat behandelt werden, Gefahren für deren Recht auf informationelle Selbstbestimmung, die bei einer Übermittlung der Niederschriften in Papierform, die nur mit einem wesentlich größeren zeitlichen und technischen Aufwand ausgewertet werden können, nicht bestehen. So können z.B. bei der elektronischen Auswertung von Wortprotokollen, möglicherweise über einen Zeitraum von mehreren Jahren, in kürzester Zeit Verhaltensprofile einzelner Gemeinderatsmitglieder angefertigt werden (z.B. Abfrage nach Äußerungen eines Gemeinderatsmitglieds zu bestimmten Themen, Abfrage nach bestimmten Wor-

ten und Suche nach widersprüchlichen Aussagen etc.). Die Mitglieder des Gemeinderats könnten sich angesichts dieser Möglichkeiten in ihrem Recht auf freie und ungezwungene Rede beeinträchtigt fühlen.

In gleicher Weise sind Auswertungen zu Bürgern möglich, deren Anliegen im Gemeinderat behandelt worden sind.

Es kann auch problemlos die Teilnahme der einzelnen Gemeinderatsmitglieder an den Gemeinderatssitzungen über einen längeren Zeitraum, bzw. bei Abwesenheit der Grund hierfür festgestellt und eine vergleichende Aufstellung ausgedruckt werden.

Im Ergebnis befürchte ich, daß bei einer Überlassung der Niederschriften auf Diskette von den damit gegebenen vielfältigen schnellen und problemlosen Auswertungsmöglichkeiten Gebrauch gemacht und letztlich auch in unzulässiger Weise personenbezogene Daten genutzt werden. Diese mit der Speicherung auf Disketten verbundenen Gefahren sprechen ebenfalls gegen die Anlegung "privater Akten" und Dateien durch Mandatsträger, die ich nicht für erforderlich und in höchstem Maße für bedenklich halte (vgl. dazu die Ausführungen im 14. Tätigkeitsbericht, Nr. 7.4. und im 15. Tätigkeitsbericht, Nr. 7.3, 2. Spiegelstrich).

8.9 Datenerhebungen mittels Fragebögen zur Überprüfung der Kurbeitragspflicht und zur Vergabe von Bauland

- Eine Stadt versandte im Rahmen der **Überprüfung der Kurbeitragspflicht** an Zweitwohnungsinhaber Erhebungsbögen mit Fragen zu familiären Bindungen in der Kommune, zu einer Schwerbeschädigteneigenschaft und zu besuchsweisen, unentgeltlichen Übernachtungen.

  Derartige Angaben waren aber zum Vollzug der Kurbeitragssatzung nicht erforderlich. Diese sah keine Ausnahme von der Kurbeitragspflicht oder eine Ermäßigung bei der Höhe des Kurbeitrags für Schwerbeschädigte und Personen mit familiären Bindungen zu Bürgern der Kommune vor. Die Kurbeitragspflicht war auch nicht von einem Übernachtungsentgelt abhängig.

  Einem anderen Zweck als dem unmittelbaren Vollzug der Kurbeitragssatzung diente die Fragebogenaktion nicht. Es sollten also nicht etwa damit Erkenntnisse für eine Überarbeitung der Satzung gewonnen werden. Dazu dürfen die Bürger durchaus um entsprechende, für die Überarbeitung erforderliche Angaben gebeten werden. Sie sind dann aber gemäß BayDSG deutlich auf den Erhebungszweck und die Freiwilligkeit ihrer Angaben hinzuweisen. Außerdem müssen die Fragebögen anonym zurückgegeben werden können.

  Im vorliegenden Fall waren die bezeichneten Angaben zum Vollzug der Kurbeitragssatzung und damit zur Aufgabenerfüllung der Stadt nach Art. 16 Abs. 1 BayDSG nicht erforderlich. Hinzu kommt, daß die Betroffenen nicht auf die Freiwilligkeit ihrer Angaben hingewiesen wurden. Die unzulässige Datenerhebung habe ich beanstandet.

- In einer Gemeinde mußten **Bürger, die günstiges Bauland von der Kommune erwerben wollten**, einen Fragebogen ausfüllen, in dem u.a. nach Beruf und Familienstand der Bewerber und nach dem Verwandtschaftsverhältnis der in ihrem Haushalt lebenden Personen gefragt wurde. Diese Angaben waren aber zum Vollzug der gemeindlichen Vergaberichtlinien nicht erforderlich. Diese stellten auf Merkmale wie "alleinerziehend" (gleichgültig, ob ledig, geschieden oder verwitwet), "junge Familie" und "im Haus lebende, unterhaltsberechtigte Kinder" ab.

Die von den Vergaberichtlinien nicht gedeckte Datenerhebung habe ich ebenfalls beanstandet, weil sie nach Art. 16 Abs. 1 BayDSG zur Aufgabenerfüllung nicht erforderlich war.

8.10 Behandlung der Anträge auf Erteilung einer Abgeschlossenheitsbescheinigung durch die Baubehörden

Zur Begründung von Wohnungseigentum ist dem Grundbuchamt u.a. eine Bescheinigung der Baubehörde vorzulegen, daß die Wohnung in sich abgeschlossen ist (sog. Abgeschlossenheitsbescheinigung). Baubehörden sind auch die kreisfreien Städte und die großen Kreisstädte, die im übertragenen Wirkungskreis die Aufgaben erfüllen, die sonst von den Landratsämtern als den unteren staatlichen Bauaufsichtsbehörden wahrzunehmen sind.

Eine kreisfreie Stadt hat mir nun mitgeteilt, daß sie beabsichtige, künftig den vom Stadtrat gebildeten Ausschuß für Stadtplanung, Verkehr- und Wohnungsfragen von Anträgen auf Erteilung einer Abgeschlossenheitsbescheinigung für vermietete Wohnungen in öffentlicher Sitzung zu informieren. Die Namen der Antragsteller sollten dabei nicht genannt werden. Über die Anträge und die sich daraus ergebenden Rechtsfolgen wollte die Stadt die betroffenen Mieter durch ein Schreiben unterrichten.

Die datenschutzrechtliche Überprüfung hat folgendes ergeben:

1. **Keine Unterrichtung der betroffenen Mieter durch die Baubehörde von Amts wegen über Anträge auf Erteilung einer Abgeschlossenheitsbescheinigung**

   Der Bundesgesetzgeber hat den Schutz des Wohnraummieters bei Veräußerung der Mietsache eingehend geregelt. Die gesetzlichen Bestimmungen zeigen, daß er genau vorgeschrieben hat, in welchen Fällen und zu welchen Zeitpunkten bei tatsächlichen oder rechtlichen Veränderungen in Bezug auf den Wohnraum eine Beteiligung oder Unterrichtung des Mieters geboten ist. Die Regelungen sind abschließend.

   Der Gesetzgeber hat bei der Begründung von Wohnungseigentum an vermietetem, nicht öffentlich gefördertem Wohnraum im Gegensatz zur Regelung im öffentlich geförderten Mietwohnungsbau (§ 2 a Abs. 2 Wohnungsbindungsgesetz) eine Unterrichtung des Mieters nicht vorgesehen.

   Die Vorschrift des § 2 a Abs. 2 Wohnungsbindungsgesetz, wonach die Umwandlung in eine Eigentumswohnung dem Mieter mitzuteilen ist, ist auf frei finanzierten oder

nicht mehr öffentlich geförderten Mietwohnraum nicht entsprechend anwendbar. Die Vorschrift läßt nur den Umkehrschluß zu, daß bei frei finanziertem oder nicht mehr öffentlich gefördertem Mietwohnraum eine Unterrichtung des Mieters über die Umwandlung der Mietwohnung in eine Eigentumswohnung nicht zulässig ist.

Eine Unterrichtung der Mieter von frei finanziertem oder nicht mehr öffentlich gefördertem Mietwohnraum von Amts wegen, ohne daß dies aus behördlicher Sicht erforderlich wäre, über Anträge auf Erteilung einer Abgeschlossenheitsbescheinigung und die sich daraus ergebenden Rechtsfolgen ist danach unzulässig, solange der Gesetzgeber keine Rechtsgrundlage dafür geschaffen hat. Als datenschutzgerechter Weg besteht die Möglichkeit, Mieter allgemein, z.B. durch das Verteilen von Informationsbroschüren, in größeren Bereichen über die Rechtsfolgen der Schaffung von Wohnungseigentum zu informieren. Eine Unterrichtung der betroffenen Mieter wäre nur mit Einwilligung der Hauseigentümer zulässig (vgl. Art. 15 Abs. 1 Nr. 2 BayDSG).

2. **Keine Bekanntgabe von Anträgen auf Erteilung einer Abgeschlossenheitsbescheinigung in öffentlicher Ausschußsitzung**

   Zwar sollte auf eine Namensnennung der Antragsteller bei der Behandlung in öffentlicher Ausschußsitzung verzichtet werden, diese sind jedoch über die Bezeichnung des Objekts im Sinn von Art. 4 Abs. 1 BayDSG bestimmbar.

   Die Behandlung in öffentlicher Ausschußsitzung bedeutet deshalb eine Verarbeitung personenbezogener Daten. Eine Unterrichtung des Ausschusses für Stadtplanung, Verkehr- und Wohnungsfragen über die von Anträgen auf Erteilung einer Abgeschlossenheitsbescheinigung betroffenen Objekte als solches halte ich für zulässig, soweit die Begründung von Wohnungseigentum Auswirkungen auf die Bevölkerungsstruktur des Stadtviertels haben kann und die Kenntnis der betroffenen Objekte für den Ausschuß zu Planungszwecken erforderlich ist.

   Für unzulässig halte ich jedoch eine Bekanntgabe der betroffenen Objekte in öffentlicher Ausschußsitzung. Nach der bestehenden Rechtslage ist bei der Begründung von Wohnungseigentum an frei finanziertem oder nicht mehr öffentlich gefördertem Wohnraum eine Unterrichtung der Mieter durch die Baubehörde von Amts wegen

über Anträge auf Erteilung einer Abgeschlossenheitsbescheinigung, ohne daß dies aus behördlicher Sicht erforderlich wäre - wie vorher bemerkt - nicht vorgesehen und deshalb mangels Rechtsgrundlage unzulässig. Bei einer Unterrichtung des Gemeinderats in öffentlicher Sitzung würde somit der Wille des Gesetzgebers unterlaufen und das vom ihm als schutzwürdig anerkannte Interesse des Eigentümers an der Vertraulichkeit der Behandlung seines Antrags in der Verwaltung verletzt.

In der Folge wurde mir ein Fall bekannt, in dem eine Stadt die betroffenen Mieter von Amts wegen über Anträge auf Erteilung einer Abgeschlossenheitsbescheinigung informiert hat und die Anträge in öffentlicher Ausschußsitzung behandelt hat. Beides habe ich beanstandet.

8.11 Auskunft aus dem Paß- oder Personalausweisregister an Banken und Sparkassen

Mehrere Gemeinden haben sich bei mir erkundigt, ob es zulässig sei, den Banken und Sparkassen Auskunft aus dem Paß- oder Personalausweisregister zu erteilen. Die Banken und Sparkassen würden entsprechende Auskunftsersuchen mit dem Geldwäschegesetz begründen.

Sowohl das Paß- als auch das Personalausweisregister sind **keine öffentlichen**, sondern ausschließlich für **behördliche Zwecke** bestimmte Register (vgl. Nr. 21.7 PaßVwV, Nr. 12.1 VollzBekPAuswG). Die Zwecke, denen diese Register dienen, sind in § 21 Abs. 3 Paßgesetz (PaßG) bzw. § 2 a Gesetz über Personalausweise (PAuswG) **abschließend** aufgezählt. Nach § 22 Abs. 2 PaßG dürfen Paßbehörden anderen **Behörden** auf deren Ersuchen Daten aus dem Paßregister übermitteln, wenn die dort genannten Voraussetzungen erfüllt sind. Für das Personalausweisregister gibt es in § 2 b Abs. 2 PAuswG eine vergleichbare Regelung. Von der Möglichkeit des Art. 16 Abs. 2 AGPersPaßG, Datenübermittlung an nicht-öffentliche Stellen durch Rechtsverordnung zuzulassen, wurde bislang noch kein Gebrauch gemacht.

Banken sind keine Behörden; Sparkassen sind zwar öffentlichrechtliche Kreditinstitute, jedoch erfüllen auch sie nicht den Behördenbegriff des Art. 1 Abs. 2 Bayer. Verwaltungsverfahrensgesetz. Im übrigen ergibt sich aus Art. 3 Abs. 2 Satz 2 BayDSG, daß öffentlich-rechtliche Kreditinstitute keine Sonderstellung gegenüber privatrechtlichen Kreditinstituten eingeräumt werden kann. Für öffentlich-rechtliche Kreditinstitute sowie für ihre Zusammenschlüsse und Verbände gelten die Vorschriften des Bundesdatenschutzgesetzes, die auf private Kreditinstitute anzuwenden sind. Eine Auskunftserteilung z. B. über Art, Nummer und ausstellende Behörde von Personalausweisen und Pässen an Banken und Sparkassen ist also nicht möglich.

Das Geldwäschegesetz schreibt in Art. 1 §§ 2 bis 6 vor, daß die Identifizierung vor bzw. zum Zeitpunkt des Geldgeschäfts durch das Kreditinstitut erfolgt. Nach Art. 1 § 1 Abs. 5 Geldwäschegesetz ist Identifizieren das Feststellen des Namens aufgrund eines Personalausweises oder Reisepasses sowie des Geburtsdatums und der Anschrift, soweit sie darin enthalten sind, und das Feststellen der Art, Nummer und ausstellenden Behörde des amtlichen Ausweises.

8.12 Weitergabe eines Briefes mit personenbezogenen Angaben durch eine Regierung an Dritte

Zwei Bürger hatten sich in einem Schreiben an eine Regierung nach den Bestandteilen und der Zusammensetzung eines in einer Asylbewerberunterkunft verwendeten Schädlingsbekämpfungsmittels erkundigt und die Durchführung von Schadstoffmessungen gefordert. Das Schreiben enthielt die Anschriften der beiden Bürger und endete mit dem Zusatz: "PS: Kopien dieses Schreibens gehen an die Presse und an den Rundfunk."

Dieses Schreiben war von der Regierung in Kopie und damit mit den Namen und Anschriften der beiden Bürger an die betroffene Schädlingsbekämpfungsfirma zur Stellungnahme weitergeleitet worden. Die Bürger waren daraufhin von der Firma zur Abgabe einer Verpflichtungerklärung, daß sie keinen Zusammenhang mehr zwischen den Symptomen bei den Asylbewerbern und dem Einsatz der Schädlingsbekämpfungsmittel herstellen werden, und zum Ersatz von entstandenen Anwaltskosten aufgefordert worden.

Die Weitergabe des Briefes mit den Namen und den Anschriften der Eingabeführer durch die Regierung an die private Schädlingsbekämpfungsfirma war eine Übermittlung personenbezogener Daten an Dritte (Art. 4 Abs. 1, Abs. 6 Nr. 3 BayDSG). Da weder eine Einwilligung der Betroffenen noch eine spezialgesetzliche Rechtsvorschrift für die Datenübermittlung vorlag, beurteilte sich die Datenübermittlung nach Art. 19 Abs. 1 BayDSG. Die Weitergabe des Briefes war danach weder nach Art. 19 Abs. 1 Nr. 1 BayDSG (Erforderlichkeit zur Aufgabenerfüllung) noch nach Art. 19 Abs. 1 Nr. 2 BayDSG (berechtigtes Interesse des Empfängers) zulässig.

Ich habe die Weitergabe des Briefes deshalb beanstandet.

- Die Weitergabe des Briefes war nicht nach Art. 19 Abs. 1 Nr. 1 BayDSG zulässig, weil es zur Feststellung des Sachverhalts und zur Beantwortung der Frage der Petenten nicht erforderlich war, die Tatsache der Anfrage und damit verbunden die Namen und Anschriften der Eingabeführer der Firma mitzuteilen. Es hätte genügt, wenn sich die Regierung bei der Firma unter Hinweis auf eine Anfrage (ohne diese näher zu bezeichnen) nach den Bestandteilen und der Zusammensetzung des Mittels erkundigt hätte.

- Die Datenübermittlung war auch nicht nach Art. 19 Abs. 1 Nr. 2 BayDSG zulässig:

  Zum einen ist ein **berechtigtes** Interesse der Firma an der Kenntnis der Namen und Adressen der Eingabeführer nicht erkennbar. Art. 19 Abs. 1 Nr. 2 BayDSG geht im übrigen davon aus, daß der Datenübermittlung ein entsprechender Antrag des potentiellen Empfängers zugrundeliegt ("glaubhaft darlegt"). Art. 19 Abs. 1 Nr. 2 BayDSG kommt bei der Übermittlung personenbezogener Daten, die die öffentliche Stelle **von sich aus** herausgibt, wie dies im vorliegenden Fall geschehen ist, daher nur dann als Rechtsgrundlage in Betracht, wenn eine Glaubhaftmachung entbehrlich ist, weil das berechtigte Interesse des Empfängers an der Kenntnis der Daten der übermittelnden Stelle bekannt oder für sie offenkundig ist. Beide Voraussetzungen lagen nicht vor.

  Die Bürger, die sich mit der Anfrage nach den Bestandteilen und der Zusammensetzung der verwendeten Insektizide an die Regierung gewandt hatten, hatten außerdem ein schutzwürdiges Interesse, daß ihnen durch die Anfrage keine Nachteile entstehen. Das schutzwürdige Interesse ist nicht dadurch entfallen, daß das Schreiben an die Regierung den Zusatz "PS: Kopien dieses Schreibens gehen an die Presse und an den Rundfunk" enthielt. Im Zeitpunkt der Weitergabe des Briefes durch die Regierung war die Anfrage in keiner Weise veröffentlicht. Die Regierung konnte nicht sicher davon ausgehen, daß Presse und Rundfunk das Schreiben im Original veröffentlichen würden. Desweiteren durfte die Regierung auch nicht davon ausgehen, daß die Medien bei einem Aufgreifen des Vorgangs die Namen und insbesondere die vollständige Anschrift der Eingabeführer im Hinblick auf den Informantenschutz ohne deren ausdrückliches Einverständnis veröffentlichen würden. Insbesondere die Veröffentlichung der vollständigen Anschrift durch die Presse in einem Bericht widerspricht praktischer Erfahrung. Schließlich ist es ein erheblicher qualitativer Unterschied, ob die Firma den Vorgang einer Anfrage mittelbar aus den Medien erfahren hätte oder ob ihr das Originalschreiben mit Namen und Anschrift der Anfragenden vorliegt.

8.13 Datenübermittlungen vom bzw. an das Finanzamt im Rahmen eines Wohngeldverfahrens

Ein Landratsamt hatte Zweifel, ob die Angaben über die Höhe der tatsächlich geleisteten Mietzahlungen einer Wohngeldempfängerin korrekt waren, weil die Wohngeldempfängerin die einzige (erwachsene) Tochter des Vermieters war. Als Mietnachweis lag ein selbstgeführtes Mietenbuch vor, in dem die Vermieter (Eltern) den Erhalt der Mietzahlungen bestätigten. Das Landratsamt wollte nun wissen, ob es Auskunft beim zuständigen Finanzamt über die Höhe der von den Eltern (Vermietern) versteuerten Mieteinnahmen erhalten kann und ob es ggf. dem Finanzamt Auskunft aus dem Wohngeldverfahren erteilen darf.

Die Tatsache, daß die Betroffene Wohngeld erhält und die Höhe der im Wohngeldantrag angegebenen Mietzahlungen stellen **Sozialdaten** (§ 67 Abs. 1 SGB X) dar, für deren Erhebung, Verarbeitung und Nutzung die §§ 67 a ff. SGB X gelten. Die Angaben der Eltern/Vermieter gegenüber dem Finanzamt unterliegen dem **Steuergeheimnis** nach § 30 AO. Die Offenbarung dieser Angaben durch das Finanzamt ist nach § 30 Abs. 4 Nr. 2 AO nur zulässig, wenn sie durch Gesetz ausdrücklich zugelassen ist.

1. Auskunft vom Finanzamt

   Als Rechtsgrundlage für die o. g. Durchbrechung des Steuergeheimnisses kommt § 21 Abs. 4 SGB X in Betracht, wonach die Finanzbehörden, soweit es in einem Verfahren nach dem SGB X erforderlich ist, Auskunft über die ihnen bekannten Einkommens- und Vermögensverhältnisse des Antragstellers, Leistungsempfängers, Erstattungspflichtigen, Unterhaltsverpflichteten, Unterhaltsberechtigten oder der sonst zum Haushalt rechnenden Familienmitglieder zu erteilen haben. Im vorliegenden Fall würde aber nicht auf die Eigenschaft der Eltern als Unterhaltsverpflichtete oder andere Berechtigte oder Verpflichtete nach dieser Bestimmung abgestellt, sondern auf deren Vermietereigenschaft. § 21 Abs. 4 SGB X scheidet damit als Rechtsgrundlage für die erbetene Datenübermittlung aus, sie wäre unzulässig.

   Zur Verifizierung der Angaben der Betroffenen kann die Wohngeldstelle - unter Hinweis auf die gesetzlichen Folgen von Falschangaben - von den Beteiligten, je nach Einzelfall, Quittungen, Überweisungsbelege, Mietenbücher u. ä. verlangen.

2. Auskunft an das Finanzamt

Sofern das Finanzamt ein entsprechendes Auskunftsersuchen an die Wohngeldstelle richtet, ist eine Übermittlung von Sozialdaten, wie beispielsweise die dem Wohngeld zugrundeliegende Miethöhe, zur Sicherung des Steueraufkommens nach § 71 Abs. 1 Nr. 3 SGB X zulässig.

8.14 Schutz personenbezogener Daten in Planfeststellungsverfahren

Im Berichtszeitraum war ich mit Fragen der Behandlung personenbezogener Daten in Planfeststellungsverfahren befaßt. Datenschutzrechtliche Fragen stellen sich hier insbesondere im Zusammenhang mit der öffentlichen Auslegung der Planunterlagen im Verfahren, der öffentlichen Bekanntmachung des Planfeststellungsbeschlusses und der Unterrichtung des Vorhabensträgers über Einwendungen.

1. Das Bundesverfassungsgericht hat in seinen Beschlüssen vom 24. Juli 1990 (CR 1990, S. 798 = NVwZ 1990, S. 1162) und vom 14. Oktober 1987 (BVerfGE 77, S. 121 = NJW 1988, S. 403) **die Veröffentlichung von personenbezogenen Daten, die ein Einwendungsführer der Planfeststellungsbehörde preisgibt**, um ihr eine sachgerechte Beurteilung der geltend gemachten Einwendungen zu ermöglichen, **für verfassungswidrig erklärt**. Das Bundesverfassungsgericht ging in diesen Beschlüssen davon aus, daß der Bürger der Behörde seine personenbezogenen Daten nur zu einem bestimmten Zweck offenbart. Dieser Zweck ist die sachgerechte Entscheidung im Planfeststellungsverfahren. Durch die öffentliche Bekanntmachung der nichtanonymisierten Daten sah das Bundesverfassungsgericht diese Zweckbindung als unterlaufen und im Ergebnis aufgehoben an. Das Bundesverfassungsgericht hat darauf hingewiesen, daß keine Gründe ersichtlich sind, warum eine ordnungsgemäße Begründung des Planfeststellungsbeschlusses notwendig voraussetzt, daß sachbezogene Erwägungen zur Beurteilung und Gewichtung der geltend gemachten Einwendungen personenbezogen in die Begründung aufgenommen und mit dieser veröffentlicht werden müssen. Die sachliche Zuordnung kann hier auch durch die Vergabe von Betriebsnummern erfolgen.

   Unter Bezugnahme auf die Rechtsprechung des Bundesverfassungsgerichts hat der Bundesbeauftragte für den Datenschutz die Veröffentlichung von Einwendungen mit Name und Adresse der Einwender und von personenbezogenen Daten der Grundstückseigentümer in den Anlagen zum Entwurf eines Gesetzes über den Bau der "Südumfahrung Stendal" der Eisenbahnstrecke Berlin-Oebisfelde - BR-Drs. 513/92 - als rechtswidrigen Eingriff in das Recht der betroffenen Bürger auf informationelle Selbstbestimmung betrachtet. Laut dpa-Meldung vom 07.09.1992 hat daraufhin das

Bundesverkehrsministerium erklärt, die Bundesregierung werde im weiteren Gesetzgebungsverfahren die personenbezogenen Daten von Grundstückseigentümern verschlüsseln und damit dafür sorgen, "daß nur datenschutzrechtlich unanfechtbare Angaben der Öffentlichkeit zugänglich gemacht werden".

2. Die Entscheidungen des Bundesverfassungsgerichts bezogen sich auf die öffentliche Bekanntmachung von personenbezogenen Daten der Einwendungsführer im Planfeststellungsbeschluß. In gleicher Weise wäre aber auch eine **Veröffentlichung der Grunderwerbsverzeichnisse mit den Namen und Anschriften der Grundstückseigentümer im Rahmen der Auslegung** nach Art. 73 Abs. 3 BayVwVfG ein unzulässiger Eingriff in das informationelle Selbstbestimmungsrecht der betroffenen Grundstückseigentümer.

   Die Veröffentlichung der Eigentümerverhältnisse im Rahmen der Planauslegung bedeutet eine Preisgabe an eine unübersehbare Vielzahl unbekannter Dritter, die nach Sinn und Zweck des Anhörungsverfahrens nicht erforderlich ist. Aus den nach Art. 73 Abs. 1 Satz 2 BayVwVfG vom Vorhabensträger bei der Anhörungsbehörde einzureichenden Planunterlagen muß zwar u.a. erkennbar sein, welche Grundstücke von dem Vorhaben betroffen sind. Die öffentliche Auslegung der Planunterlagen zur Einsichtnahme soll es potentiell Betroffenen ermöglichen, sich über das Vorhaben zu informieren und ggf. Einwendungen gegen den Plan zu erheben. Dazu reicht aber die Angabe der Flurstücksnummern aus. Aus den ausgelegten Lageplänen und den Flurstücksnummern können interessierte Bürger bei der Einsichtnahme durchaus erkennen, ob ihr Grundstück betroffen ist. Mit der darüber hinausgehenden Angabe der jeweiligen Eigentümer in den auszulegenden Unterlagen würden auch zahlreichen Nichtbetroffenen wesentliche Angaben zu Vermögensverhältnissen der Eigentümer zugänglich gemacht werden. Damit würde mangels Erforderlichkeit in unzulässiger Weise in die Rechte der Grundstückseigentümer eingegriffen werden. Soweit in Einzelfällen Unklarheiten bestehen, können diese jederzeit durch eine Anfrage bei der Behörde bereinigt werden. Darauf kann die Behörde bei der Auslegung hinweisen.

   Aus den genannten Gründen ist auch eine Veröffentlichung der Namen und Anschriften der Grundstückseigentümer im **Planfeststellungsbeschluß** unzulässig.

3. Von einer öffentlichen Bekanntgabe des Planfeststellungsbeschlusses mit den personenbezogenen Angaben der Einwendungsführer oder Grundstückseigentümer und einer Veröffentlichung der Grundstückseigentümer im Wege der Planauslegung nach Art. 73 Abs. 3 BayVwVfG ist die **Übermittlung der personenbezogenen Daten der Einwendungsführer an den Träger des Vorhabens** zu unterscheiden. Diese Datenübermittlung halte ich grundsätzlich für zulässig, soweit der Träger des Vorhabens zur fachgerechten Vorbereitung auf die Behandlung von Einwendungen im Erörterungstermin die konkret betroffenen individuellen Belange des Einwenders kennen muß. Zu berücksichtigen ist dabei, daß mit der form- und fristgerechten Erhebung einer Einwendung der Einwender sich förmlich am Verwaltungsverfahren beteiligt und damit die Rechtsstellung eines Beteiligten im Sinne des Art. 13 BayVwVfG mit den daraus sich ergebenden verfahrensrechtlichen Rechtspositionen erhält. Dies bringt mit sich, daß der Einwender gegenüber dem Projektträger aus dem Kreis der Anonymität heraustritt und den übrigen **am Verfahren Beteiligten**, soweit erforderlich, bekanntgegeben wird, ebenso wie umgekehrt der Einwender deren Identität kennt.

   Eine Kenntnisnahme der personenbezogenen Daten der Einwender durch den Vorhabensträger ist dagegen nicht erforderlich, wenn diese erkennbar keinen Beteiligtenstatus anstreben, z.B. weil sie nicht die Verletzung eigener Rechte geltend machen, sondern nur allgemein z.B. für die Belange des Naturschutzes eintreten.

---

9. Einwohnermeldewesen

9.1 Melderegisterauskünfte zur Wahlwerbung

Auch in diesem Berichtszeitraum haben sich wieder zahlreiche Bürger und Gemeinden mit Anfragen zu Auskünften aus dem Melderegister an politische Parteien, Wählergruppen und anderen Trägern von Wahlvorschlägen zur Wahlwerbung an mich gewandt. Aufgrund von Bürgerbeschwerden und Presseberichten wurden mir in diesem Zusammenhang auch Datenschutzverstöße bekannt. So haben Kommunen in einigen Fällen die Namen und Anschriften von Neubürgern und von EU-Ausländern sowie von Bürgern, obwohl sie nach Art. 35 Abs. 1 Satz 3 MeldeG Widerspruch eingelegt hatten, an politische Parteien zu Wahlzwecken übermittelt.

Zu Auskünften aus dem Melderegister zur Wahlwerbung habe ich mich regelmäßig in meinen Tätigkeitsberichten, zuletzt im 16. Tätigkeitsbericht unter Nr. 9.3, geäußert. Auch in diesem Tätigkeitsbericht möchte ich nochmals darauf hinweisen, daß Art. 35 Abs. 1 MeldeG bei der Zusammensetzung der Gruppen von Wahlberechtigten, über die Auskunft erteilt werden kann, allein auf das **Lebensalter** abstellt. Ein **anderes** Auswahlkriterium, z.B. "Neubürger" oder "EU-Ausländer" ist **nicht zulässig**.

Darauf hat auch das Innenministerium nochmals in Nr. 24.2 seiner Vollzugsbekanntmachung zum Gemeinde- und Landkreiswahlgesetz und zur Gemeinde- und Landkreiswahlordnung (GLKrWBeK vom 12.10.1995, AllMBl S. 801, ber. S. 867) hingewiesen.

9.2 Übermittlung der An- und Abmeldungen an örtliche Banken

Eine Stadt übermittelte regelmäßig an die örtlichen Banken Listen über **alle Zu- und Wegzüge** von Bürgern.

Bei der Weitergabe der Listen an die örtlichen Banken mit Daten einer Vielzahl von Einwohnern, die nicht von den Banken namentlich benannt worden sind, handelte es sich um Gruppenauskünfte nach Art. 34 Abs. 3 MeldeG. Eine Gruppenauskunft darf nur erteilt werden, soweit sie im öffentlichen Interesse liegt (Art. 34 Abs. 3 Satz 1 MeldeG) und die Zustimmung der Regierung vorliegt (Nr. 34.6 Abs. 2 VollzBekMeldeG). Ein öffentliches Interesse liegt nur vor, wenn die Auskünfte Belange der Allgemeinheit betreffen und nicht nur im Interesse von einzelnen liegen. Rein kommerzielle Interessen, z.B. von Kreditinstituten, können die Annahme eines öffentlichen Interesses nicht rechtfertigen (vgl. Nr. 34.6 ff. der Vollzugsbekanntmachung zum Meldegesetz - VollzBekMeldeG). Es ist daher nicht im öffentlichen Interesse, Bankinstitute über Adreßänderungen ihrer Kunden zu unterrichten. Im vorliegenden Fall kommt hinzu, daß bei einer Mitteilung aller Zu- und Wegzüge an alle örtlichen Banken diese die Daten einer Vielzahl von Personen erhalten haben, die nicht ihre Kunden waren.

Diese regelmäßige Weitergabe von Listen über die Zu- und Wegzüge an die örtlichen Banken habe ich beanstandet. Aus den o.g. Gründen wäre aber auch eine Weitergabe von Listen über die Zu- und Wegzüge von Bürgern im Einzelfall auf Anfrage, ohne daß die Personen, über die Auskunft ersucht wird, namentlich bezeichnet werden, mangels eines öffentlichen Interesses unzulässig gewesen und hätte von mir beanstandet werden müssen.

9.3 Weitergabe von Melderegisterdaten durch Verwaltungsgemeinschaften an Mitgliedsgemeinden

Im Berichtszeitraum haben mich verschiedentlich Anfragen dazu erreicht, inwieweit den einzelnen Mitgliedsgemeinden, z.B. bei der Neuinstallierung von EDV-Programmen, bzw. den Bürgermeistern, z.B. für die Ehrung von Altersjubilaren oder die Jugendarbeit, ein Zugriff auf die Melderegisterdaten der eigenen Gemeinden eingeräumt werden darf.

Die Verwaltungsgemeinschaft nimmt die Aufgaben der Meldebehörde anstelle der Mitgliedsgemeinden wahr, da es sich beim Vollzug des Melderechts um eine Aufgabe des übertragenen Wirkungskreises handelt (Art. 1 Satz 2 Meldegesetz in Verbindung mit Art. 4 Abs. 1 Satz 1 Verwaltungsgemeinschaftsordnung). Das Melderegister wird bei einer Verwaltungsgemeinschaft **getrennt nach den einzelnen Mitgliedsgemeinden** geführt (vgl. Nr. 3.1 Vollzugsbekanntmachung zum Meldegesetz -VollzBekMeldeG- vom 28. April 1984, MABl Seite 177, zuletzt geändert durch Bekanntmachung vom 23.08.1995 , AllBMl Seite 711). EDV-Programme zum Melderegister dürfen bei der Verwaltungsgemeinschaft nur eingesetzt werden, wenn eine Trennung nach den einzelnen Mitgliedsgemeinden gewährleistet ist.

Eine Datenweitergabe von Verwaltungsgemeinschaften an Mitgliedsgemeinden bezüglich der Daten der Einwohner der jeweiligen Gemeinde richtet sich nach Art. 31 Abs. 7 in Verbindung mit Art. 31 Abs. 1 Meldegesetz (MeldeG). Durch diese Bestimmung bietet das Melderecht die Möglichkeit, sämtliche der Art.3 **Abs. 1** MeldeG (Grunddaten) aufgeführten Daten und Hinweise von der Verwaltungsgemeinschaft an die Mitgliedsgemeinden weiterzugeben, wenn dies zur rechtmäßigen **Aufgabenerfüllung erforderlich** ist. Es können daher nicht die Namen, Anschriften und Geburtstage **aller** Gemeindeeinwohner an einen Bürgermeister weitergegeben werden, wenn dieser nur bestimmte Altersjubilare ehren will. Für die in Art. 3 **Abs. 2** MeldeG (Daten für besondere Zwecke) genannten Daten und Hinweise gelten für die Weitergabe zwischen einer Verwaltungsgemeinschaft und ihren Mitgliedsgemeinden nach Art. 31 Abs. 7 Satz 3 MeldeG die strengeren Anforderungen aus Art. 31 Abs. 2 und 6 MeldeG entsprechend. Die Weitergabe ist hier nur dann zulässig, wenn der Empfänger ohne Kenntnis der Daten zur Erfüllung einer ihm durch Rechtsvorschrift übertragenen Aufgabe nicht in der Lage wäre, und er die Daten beim betroffenen Einwohner nur mit unverhältnismäßig hohem Aufwand erheben könnte

oder von einer Datenerhebung nach der Art der Aufgabe, zu der die Daten erforderlich sind, abgesehen werden muß (Art. 31 Abs. 2 MeldeG). Bei der Verwendung dieser Daten unterliegen die Mitgliedsgemeinden dem Zweckbindungsgebot nach Art. 31 Abs. 6 MeldeG.

Die von der Verwaltungsgemeinschaft weitergegebenen Daten dürfen bei den Mitgliedsgemeinden im übrigen nur solange gespeichert bleiben, solange sie zur Aufgabenerfüllung erforderlich sind, so daß nicht sukzessive bei den Mitgliedsgemeinden ein weiteres Melderegister entsteht. Zusätzliche Melderegister, auch in verkürztem Umfang, bei den Mitgliedsgemeinden sieht das Melderecht nicht vor. Sie sind daher nicht zulässig. **Ausgeschlossen** ist auch die Weitergabe und Einsichtnahme von **Wahlausschlußdaten** (Art. 3 Abs. 2 Nr. 1 MeldeG) nach Art. 5 Satz 4 MeldeG, soweit dies nicht zur amtlichen Vorbereitung und Durchführung von Wahlen erforderlich ist.

9.4 Adreßbücher auf CD-ROM

Nach Art. 35 Abs. 3 MeldeG darf aus dem Melderegister **Adreßbuchverlagen** Auskunft über Vor- und Familiennamen, den Doktorgrad und Adressen sämtlicher Einwohner, die das 18. Lebensjahr vollendet haben, erteilt werden, soweit die Betroffenen der Weitergabe ihrer Daten nicht widersprochen haben.

Mit der immer weiteren Verbreitung von PCs mit CD-ROM-Laufwerken wird es für gewerbliche Unternehmen zunehmend interessant, solche **Adreßbücher auf CD-ROM** herauszubringen. Diese elektronischen Verzeichnisse bieten - je nach Gestaltung - gegenüber herkömmlichen Adreßbüchern auf Papier vielfältige Auswertungsmöglichkeiten nach vielen verschiedenen Suchkriterien.

Mehrere Länder haben ihren Meldebehörden inzwischen empfohlen, Auskünfte an Adreßbuchverlage nur dann zu erteilen, wenn Adreßbücher in Buchform hergestellt werden, da die Verwendung der Daten für ein "Adreßbuch" auf CD-ROM mit der gesetzlichen Regelung nicht vereinbar sei. Der Gesetzgeber habe die Übermittlung von Meldedaten auf die Herausgabe von Adreßverzeichnissen in Buchform beschränkt und von der Möglichkeit, diese Zweckbindung der Daten wegen neuer Techniken der Datenverarbeitung zu erweitern, bisher keinen Gebrauch gemacht.

Das Landgericht Mannheim hat mit Urteil vom 8.3.1996 (Aktenzeichen 7-O-77/96) in einem Rechtsstreit betreffend die Herausgabe eines Verzeichnisses von Fernsprechteilnehmern auf CD-ROM u.a. festgestellt, daß die Zustimmung eines Betroffenen, seine Daten in eine (öffentlich zugängliche) Datei aufnehmen zu lassen (hier in das Telefonbuch), keineswegs die Annahme rechtfertigt, der Betroffene sei mit der Übernahme seiner Daten in weitere Dateien einverstanden. Ich habe diese Entscheidung begrüßt. Andererseits ist nach § 28 Abs. 1 Nrn. 3 BDSG das Speichern, Veränderung oder Übermitteln personenbezogener Daten oder ihre Nutzung als Mittel für die Erfüllung eigener Geschäftszwecke zulässig, wenn die Daten aus allgemein zugänglichen Quellen entnommen werden können oder die speichernde Stelle sie veröffentlichen dürfte, es sei denn, daß das schutzwürdige Interesse des Betroffenen an dem Ausschluß der Verarbeitung oder Nutzung offensichtlich überwiegt. Ich meine es spricht viel dafür, daß ein überwiegen-

des Schutzinteresse hier anzunehmen ist. Die Frage ist aber umstritten.

Der Unterausschuß "Melde-, Paß- und Personalausweiswesen" der Arbeitsgemeinschaft der Innenministerien der Bundesländer hat in seiner Sitzung am 07./08.05.1996 einvernehmlich festgestellt, daß bis zu einer datenschutzrechtlichen Klärung der Problematik durch den Bund von Auskunftserteilungen der Meldebehörden an solche Unternehmen abgesehen werden soll, die nicht zumindest auch Adreßbücher im herkömmlichen Sinn herstellen.

Solange ein wirksamer Schutz der nach Art. 35 Abs. 3 MeldeG übermittelten Melderegisterdaten gegenüber den Gefahren einer elektronischen Übernahme und Verknüpfung mit anderen personenbezogenen Daten durch Dritte nicht besteht, ist es umso wichtiger, die Bürger darauf hinzuweisen, daß die Gefahr besteht, daß die übermittelten Daten nicht nur in gedruckten, sondern auch in elektronischen Verzeichnissen mit den damit verbundenen vielfältigen Auswertungsmöglichkeiten erscheinen können. Nur wenn sie darüber informiert sind, können sie eine sachgerechte Entscheidung über die Ausübung ihres Widerspruchsrechts gegen die Aufnahme ihrer Daten in Adreßbücher treffen.

Auf ihr Widerspruchsrecht sind die Bürger nach Art. 35 Abs. 3 Satz 3 MeldeG bei der Anmeldung hinzuweisen. Darüber hinaus soll die Meldebehörde nach Nr. 35.4 VollzBekMeldeG vor einer Auskunftserteilung an Adreßbuchverlage das beabsichtigte Erscheinen des Adreßbuchs in geeigneter Form bekanntgeben (z.B. Amtsblatt, Amtstafel, örtliche Presse) und auf das Widerspruchsrecht hinweisen. Das Innenministerium hat die Meldebehörden durch Rundschreiben gebeten, dabei auch auf die Möglichkeit der Aufnahme der Daten in elektronische Verzeichnisse durch die Adreßbuchverlage und die damit verbundenen vielfältigen Auswertungsmöglichkeiten hinzuweisen. In meinen Tätigkeitsberichten habe ich wiederholt angeregt, die Bürger in geeigneter Weise über ihre Widerspruchsrechte aufzuklären, da vielen Bürgern diese trotz der nach dem Meldegesetz und der VollzBekMeldeG vorgeschriebenen Hinweise offenbar noch nicht hinreichend bekannt zu sein scheinen. Im übrigen halte ich ein abgestuftes Widerspruchsrecht (Aufnahme nur in schriftliche Verzeichnisse, nicht aber in elektronisch auswertbare) entsprechend der jetzigen Regelung im Telekommunikationsrecht für erforderlich.

9.5 Erteilung von Melderegisterauskünften über das Internet

Der Datenschutzbeauftragte eines anderen deutschen Landes hat mitgeteilt, daß sich eine dortige Gemeinde bei ihm erkundigt hat, ob zur Erteilung einfacher Melderegisterauskünfte die dafür im Melderegister gespeicherten Daten über das Internet zum Abruf bereitgehalten werden dürfen. Der Service-Provider würde Gebühren für die Auskunftserteilung erheben und an die Meldebehörde weiterleiten.

Ein solches Vorhaben wäre aus den folgenden Gründen unzulässig:

Das Melderegister ist kein öffentliches Register. Es ist vielmehr ein für behördliche Zwecke bestimmtes Register, das **die Meldebehörden** zur Erfüllung ihrer Aufgaben führen (Art. 2 Abs. 1 Meldegesetz).

Im Internet wären die eingestellten Meldedaten ohne Einschränkung für die Öffentlichkeit verfügbar. Zwar sieht Art. 34 Abs. 1 Meldegesetz für die Erteilung einer einfachen Melderegisterauskunft keine besonderen Voraussetzungen vor, jedoch regelt diese Vorschrift eindeutig, daß die Auskunft **durch die Meldebehörde** erteilt wird und es sich um eine Auskunft über **einzelne bestimmte Einwohner** handeln muß. Die Meldebehörde hat deshalb z.B. zu prüfen, ob die Angaben des Auskunftssuchenden ausreichen, um Personenverwechslungen auszuschließen. Dies wäre bei einer Einstellung von Meldedaten ins internationale, frei zugängliche Internet nicht mehr möglich.

Regelmäßige Auskünfte an Private oder Online-Abrufe durch Private sind im Meldegesetz nicht vorgesehen und damit unzulässig.

9.6 Mißbräuchliche Anfragen über personenbezogene Daten

Im April 1995 berichtete die Presse über mißbräuchliche Abfragepraktiken einer Berliner Auskunftei, die bundesweit bei Behörden und sonstigen öffentlichen Dienststellen personenbezogene Daten abgefragt hat. Durch falsche Angaben und Täuschung über die Identität der Anfragenden, über falsche Rückrufnummern und durch Vorgabe von schon teilweiser Informiertheit über bestimmte Sachverhalte konnten die Behörden zur Preisgabe personenbezogener Daten verleitet werden. U.a. wurde über Abfragen bei Einwohnermeldeämtern, Staatsanwaltschaften, Polizeidienststellen und Krankenkassen berichtet.

Mißbräuchliche Abfragen erfolgten auch beim Einwohnermeldeamt einer bayerischen Stadt. Dort ist es einem Mitarbeiter der Berliner Auskunftei, der sich als ein "Herr Köpke" vom Bundeszentralregister ausgab, gelungen, durch Vorspiegelung von Insiderwissen Daten aus dem Melderegister zu bekommen. Die unzulässigen Datenübermittlungen wurden durch ein fahrlässiges Verhalten der Bediensteten der Einwohnerbehörde ermöglicht. Diese haben die Identität des Anrufers nicht nachgeprüft, sondern seinen Angaben, er sei Mitarbeiter beim Bundeszentralregister, geglaubt. Diese Fehleinschätzung beruhte allerdings auf einem erheblichen kriminellen Verhalten des Anrufers, der über einschlägige Fachkenntnisse verfügte und sich - wie oben bereits erwähnt - die Auskünfte aus dem Melderegister durch Vorspiegelung von Insiderwissen erschlichen hat. Wegen dieses Umstandes habe ich nach Art. 31 Abs. 3 des Bayerischen Datenschutzgesetzes von einer förmlichen Beanstandung abgesehen.

Auf meine Bitte hin haben die Ministerien die nachgeordneten Behörden auf die notwendige Sorgfalt beim Umgang mit personenbezogenen Daten hingewiesen. Bei fernmündlichen Anfragen ist insbesondere im Hinblick auf die damit verbundene erhöhte Gefahr der Datenübermittlung an nicht berechtigte Dritte äußerste Vorsicht geboten. Läßt sich eine fernmündliche Auskunft im Einzelfall nicht umgehen, sind die erforderlichen Schutzmaßnahmen durchzuführen, wie z.B. Rückruf an eine eindeutig zuordenbare Telefonnummer, die Vereinbarung von Paßworten o.ä.

10. Ausländerwesen

10.1 Deutsch-vietnamesisches Rückübernahmeabkommen

Durch Hinweise eines Mitglieds des Landtags wurde ich auf folgenden Sachverhalt aufmerksam: Am 21. September 1995 trat das zwischen der Bundesrepublik Deutschland und der Regierung von Vietnam geschlossene Abkommen über die Rücknahme von vietnamesischen Staatsangehörigen in Kraft. Als Anlage 1 des Durchführungsprotokolls zu dem Abkommen wurde ein Fragebogen (Muster H 03) für die vietnamesischen Staatsangehörigen in Deutschland, die nach Vietnam zurückkehren, beigefügt. Der Fragebogen ist nach Mitteilung des Bundesinnenministeriums auf Wunsch der Republik Vietnam in das Durchführungsprotokoll aufgenommen worden, da ein entsprechendes Formular auch bei der Rückführung von Vietnamesen aus anderen Staaten verwendet werde und durch die Verwendung eines standardisierten Fragebogens die Bearbeitung durch die vietnamesischen Behörden erleichtert werde.

Für die vietnamesischen Staatsangehörigen besteht keine Verpflichtung, den Fragebogen auszufüllen. Das hat das Bundesinnenministerium im August 1995 gegenüber dem Bundesbeauftragten für den Datenschutz bestätigt.

Rückübernahmeabkommen und Durchführungsprotokoll lassen insoweit eine klare Regelung vermissen. Die Formulierungen "... weisen die zuständigen deutschen Behörden die rückzuführenden vietnamesischen Staatsangehörigen zur Ausfüllung des als Anlage 1 beigefügten Fragebogens (Muster H 03) an" und "Jede Person hat zwei Exemplare des Fragebogens auszufüllen" suggerieren vielmehr eine Pflicht des Ausländers zur vollständigen Ausfüllung des Fragebogens.

Auch das Selbstangabe-Formular erweckt den Eindruck, daß es sich nicht um eine freiwillige Datenerhebung handelt. Der Hinweis in Ziff. 13 des Vordruckes ("Zusätzliche freiwillige Angaben") läßt auf eine Verpflichtung zum Ausfüllen der Ziffern 1 - 12 schließen. Dies wird durch die Gestaltung der Unterschrift verstärkt, mit der der Betroffene bestätigen soll, die Fragen "wahrheitsgemäß beantwortet" zu haben.

Ich habe den Sachverhalt wie folgt beurteilt:

Werden personenbezogene Daten beim Betroffenen mit seiner Kenntnis erhoben, ohne daß eine Pflicht zur Auskunftserteilung besteht, so muß der Betroffene nach Art. 16 Abs. 3 Satz 2 BayDSG auf die Freiwilligkeit seiner Angaben hingewiesen werden. Der Betroffene muß wissen, daß er zum Ausfüllen des Fragebogens nicht verpflichtet ist und bei einer Weigerung keine Nachteile befürchten muß. Der Hinweis auf die Freiwilligkeit hat so rechtzeitig und klar zu erfolgen, daß Mißverständnisse ausgeschlossen sind und dem Betroffenen eine freie, auf der Grundlage zutreffender Informationen beruhende Entscheidung ermöglicht wird. Dazu habe ich gefordert, die vietnamesischen Staatsangehörigen **in einem Merkblatt in ihrer Landessprache** auf die Freiwilligkeit ihrer Angaben hinzuweisen.

Die Überprüfung der Praxis von Ausländerbehörden im Zusammenhang mit der Durchführung des deutsch-vietnamesischen Rückübernahmeabkommens aufgrund mehrerer Eingaben hat die Notwendigkeit bestätigt, die Betroffenen auf die Freiwilligkeit der Angaben in ihrer Heimatsprache hinzuweisen. So hat ein Landratsamt eingeräumt, daß es aufgrund erheblicher Sprachprobleme in Einzelfällen zu Mißverständnissen hinsichtlich eines Zusammenhanges zwischen dem Ausfüllen der Fragebögen und der Erneuerung der Duldung gekommen sein kann. In mir übermittelten Anschreiben von Ausländerbehörden an vietnamesische Staatsangehörige werden diese aufgefordert, die Fragebögen auszufüllen. Dabei fehlt in den Anschreiben nicht nur ein Hinweis auf die Freiwilligkeit, es wird darüber hinaus auch ein Sachzusammenhang zwischen dem Ausfüllen der Fragebögen und einer möglichen Abschiebung hergestellt. Die Betroffenen mußten in diesen Fällen jedenfalls zunächst annehmen, sie seien zum Ausfüllen der Fragebögen verpflichtet und bei einem Nichtausfüllen gehe die Ausländerbehörde davon aus, sie seien an einer freiwilligen Rückkehr in ihr Heimatland nicht interessiert und die Behörde sei gezwungen, Abschiebungsmaßnahmen einzuleiten. Auch wenn sie dann im weiteren Verfahren bei Vorsprachen im Ausländeramt darauf hingewiesen wurden, daß keine Verpflichtung zum Ausfüllen der Fragebögen bestehe, wird damit im Hinblick auf die zunächst hervorgerufenen falschen Vorstellungen doch nur in unzureichender Weise den Anforderungen des Art. 16 Abs. 3 Satz 2 BayDSG (ausdrücklicher Hinweis auf die Freiwilligkeit) entsprochen. Eine überprüfte Behörde geht nach eigener Darstellung davon aus, daß die Datenerhebungen ohne Hinweis auf die Freiwilligkeit erfolgt sind, da die Behörde das Schreiben des Innenministeriums vom 18.10.1995, in dem aus-

drücklich darauf hingewiesen wurde, daß die Ausfüllung des Vordruckes H 03 durch die vietnamesischen Staatsangehörigen nur auf freiwilliger Basis erfolgt, erst erhalten habe, als die Datenerhebungen bereits abgeschlossen gewesen seien.

Die Datenerhebungen ohne Hinweis auf die Freiwilligkeit und die nicht rechtzeitige und eindeutige Aufklärung der Betroffenen verstießen gegen Art. 16 Abs. 3 Satz 2 BayDSG. Da sie letztlich auf das zwar vom Bundesministerium des Innern herausgegebene, aber wegen des Landesvollzugs der Gesetze vom Bayerischen Innenministerium zu verantwortende, mißverständliche Formblatt ohne deutlichen Hinweis auf die Freiwilligkeit der Angaben zurückgingen, habe ich das Staatsministerium des Innern beanstandet. Ich habe gefordert, klar und nachweisbar, in einem schriftlichen Hinweis in der Landessprache auf die Freiwilligkeit derartiger personenbezogener Angaben hinzuweisen.

Das Bayerische Innenministerium hat zunächst einen solchen Hinweis aus Präzedenzgründen abgelehnt. In ausländerrechtlichen Situationen würden sich vielfach Notwendigkeiten ergeben, Ausländer auf bestimmte Dinge hinzuweisen. Wenn dies in der jeweiligen Landessprache erfolgen müßte, müßten die Ausländerbehörden aus Gleichbehandlungsgründen in allen Sprachen der Erde entsprechende Hinweise geben. Im übrigen verwies das Innenministerium auf Art. 23 Abs. 1 Bayer. Verwaltungsverfahrensgesetz (BayVwVfG), der festlegt, daß die Amtssprache deutsch ist.

Dem ist entgegenzuhalten, daß die hier vorliegende Problematik mit den vom Staatsministerium des Innern angesprochenen "vielfachen Notwendigkeiten" von "Hinweisen an die Ausländer" nicht vergleichbar ist. Der in Art. 16 Abs. 3 Satz 2 BayDSG gesetzlich vorgeschriebene Hinweis auf die Freiwilligkeit kann nur dann wirksam erteilt werden, wenn er in einer für den Betroffenen **verständlichen Weise** erfolgt. Der gesetzlich normierten Hinweispflicht in dieser Vorschrift kann deshalb ungeachtet der ebenfalls gesetzlichen Regelung in Art. 23 Abs. 1 BayVwVfG für Verwaltungsverfahren, daß die Amtssprache deutsch ist, nur dann Rechnung getragen werden, wenn **in den Fällen des Art. 16 Abs. 3 Satz 2** BayDSG bei Ausländern der Hinweis **auch** in deren Landessprache erfolgt (jedenfalls wenn - wie hier - auch der Fragebogen in vietnamesisch vorlag), soweit nicht im Einzelfall darauf verzichtet werden kann, z.B. weil ein Ausländer die deutsche Sprache ausreichend beherrscht oder ein Dolmetscher anwesend ist. Jedenfalls bei bun-

desweiten Fragebogenaktionen, die in der Landessprache durchgeführt werden, wie im vorliegenden Fall halte ich einen Hinweis ebenfalls in der Landessprache auf dem Fragebogen selbst oder einem diesem beigefügten Merkblatt für erforderlich. Auch der Grundsatz des fairen Verfahrens gebietet es meines Erachtens, daß die von einem Gesetz geforderten Hinweise den Betroffenen klar und rechtzeitig gegeben werden und diese deshalb bei Ausländern grundsätzlich auch in deren Landessprache vorzunehmen sind. Die Betroffenen müssen in die Lage versetzt werden, die vom Gesetz vorgesehenen Hinweise auch zu verstehen. Der Hinweis des Innenministeriums auf Art. 23 BayVwVfG - Landessprache ist deutsch - greift hier nach meiner Auffassung schon deshalb nicht, weil der Fragebogen H 03 den Ausländerbehörden vom Staatsministerium des Innern außer in deutsch auch in vietnamesisch zur Verfügung gestellt wurde. Es leuchtet mir nicht ein, warum zwar dieses möglich ist, nicht aber die Übermittlung des gesetzlich vorgeschriebenen Hinweises auf die Freiwilligkeit ebenfalls in der Landessprache. In anderen Ländern können die Betroffenen auch in ihrer Landessprache auf die Freiwilligkeit der Angaben hingewiesen werden, wie sich aus dem in der Anlage 8 beigefügten Merkblatt in deutscher und vietnamesischer Sprache ergibt, das in Brandenburg und Mecklenburg-Vorpommern verwendet wird.

Inzwischen hat das Staatsministerium des Innern die Aufnahme eines Hinweises in der Landessprache auf Formulare (Fragebogen), die zwei- oder fremdsprachig sind, "im Rahmen des rechtlich und tatsächlich Möglichen" zugesagt.

10.2 Ehefähigkeitszeugnisse für Asylbewerber

Ein Landratsamt fragte, ob aus datenschutzrechtlicher Sicht Bedenken dagegen bestehen, daß bei Anträgen auf Befreiung von der Beibringung des Ehefähigkeitszeugnisses durch Asylbewerber grundsätzlich die Ausländerakten **über die Standesämter** dem Präsidenten des zuständigen Oberlandesgerichts übersandt werden.

Die Ausländerakte enthält personenbezogene Daten im Sinne von Art. 4 Abs. 1 BayDSG über den Betroffenen und ggf. über dritte Personen. Wird die Ausländerakte an das Standesamt übersandt, handelt es sich um eine Datenübermittlung (Art. 4 Abs. 6 Nr. 3 BayDSG) an eine andere öffentliche Stelle. Diese Datenübermittlung ist nach Art. 18 Abs. 1 BayDSG zulässig, wenn sie zur Erfüllung der in der Zuständigkeit der übermittelnden oder der empfangenden Stelle liegenden Aufgaben erforderlich ist und für Zwecke erfolgt, für die eine Nutzung nach Art. 17 Abs. 1 Nr. 2, Abs. 2 bis 4 BayDSG zulässig wäre.

Nach § 10 Abs. 2 Ehegesetz (EheG) ist für die Entscheidung über die Befreiung der Beibringung des Ehefähigkeitszeugnisses der Präsident des Oberlandesgerichts zuständig. Dem Standesbeamten obliegt nach § 5a Abs. 2 Personenstandsgesetz (PStG), § 171 Dienstanweisung für Standesbeamte (DA) die Pflicht, den Antrag entgegenzunehmen und die Entscheidung **vorzubereiten**; hierbei hat er alle Nachweise zu fordern, die vor der Anordnung des Aufgebots erbracht werden müssen. Der Standesbeamte ist also nicht nur für die Aufnahme des Antrags zuständig, er hat auch alle erforderlichen Unterlagen beizufügen (vgl. § 171 Abs. 2, 3 DA).

Ist es für die Entscheidung des Präsidenten des Oberlandesgerichts erforderlich, daß die Ausländerakte beigezogen wird (z.B. zur Identitätsprüfung, Überprüfung der Angaben zum Familienstand, zu Kindern), so ist das Standesamt berechtigt, die Ausländerakte beizuziehen und mit den übrigen Unterlagen dem Präsidenten des Oberlandesgerichtes vorzulegen, da der Standesbeamte - wie ausgeführt - die Aufgabe hat, die Entscheidung vorzubereiten.

Die Datenübermittlung erfolgt auch für Zwecke, für die eine Nutzung nach Art. 17 Abs. 2 BayDSG zulässig ist. § 5 a Abs. 2 PStG, § 171 DA setzen zwingend voraus, daß der Standesbeamte alle erforderlichen Daten erhebt und sich Nachweise darüber vorlegen läßt (Art. 17 Abs. 2

Nr. 1 BayDSG). Die Datenübermittlung kann außerdem je nach Umständen des Einzelfalls im Interesse des Betroffenen liegen (vgl. Art. 17 Abs. 2 Nr. 3 BayDSG), der die Befreiung vom Ehefähigkeitszeugnis beantragt hat, unter Umständen müssen Angaben des Betroffenen überprüft werden, weil tatsächliche Anhaltspunkte für deren Unrichtigkeit bestehen (vgl. Art. 17 Abs. 2 Nr. 5 BayDSG) oder die Datennutzung kann zur Abwehr einer schwerwiegenden Beeinträchtigung der Rechte einer anderen Person erforderlich sein (vgl. Art. 17 Abs. 2 Nr. 9 BayDSG), z. B. bei falschen Angaben zum Familienstand oder zu Kindern.

Sind in der Akte die personenbezogenen Daten des Betroffenen mit den Daten dritter Personen verbunden, die zur Aufgabenerfüllung nicht erforderlich sind, so ist die Übermittlung dieser Daten gem. Art. 17 Abs. 5 BayDSG zulässig, wenn eine Trennung nicht oder nur mit unvertretbarem Aufwand möglich ist, soweit nicht offensichtlich überwiegende schutzwürdige Interessen des Betroffenen oder Dritter entgegenstehen.

Es ist daher datenschutzrechtlich zulässig, daß die Ausländerakte über das Standesamt dem Präsidenten des Oberlandesgerichts zugeleitet wird. Zur Sicherstellung des Datenschutzes auf dem Postlauf müssen geeignete Maßnahmen getrofffen werden (z.B. Versand der Akte im verschlossenen Umschlag, der nur vom sachbearbeitenden Standesbeamten geöffnet wird).

11. Steuerverwaltung

11.1 AO-Änderungsgesetz

Die Arbeiten am Gesetz zur Änderung der Abgabenordnung wurden bisher nicht wieder aufgenommen.

In meinem sechzehnten Tätigkeitsbericht habe ich mitgeteilt, daß der Bundesbeauftragte für den Datenschutz die Erstellung einer Bestandsaufnahme von wünschenswerten Änderungen der Abgabenordnung aus datenschutzrechtlicher Sicht beabsichtigt.
Diese Bestandsaufnahme wurde - auch unter meiner Beteiligung - inzwischen vorgenommen.
Das Bundesministerium der Finanzen beabsichtigt in Kürze eine Erörterung dieser Vorschläge mit den obersten Finanzbehörden der Länder, an der außer dem Bundesbeauftragten für den Datenschutz auch ein Vertreter der Landesbeauftragten für den Datenschutz teilnehmen wird.
Ich habe das Staatsministerium der Finanzen um Unterstützung der Vorschläge gebeten. Ich sehe bei der Novellierung der datenschutzrechtlichen Bestimmungen in der Abgabenordnung unverändert Handlungsbedarf. Als Beispiel dafür mag der nachfolgende Beitrag dienen.

11.2 Outsourcing von Aufgaben der Steuerverwaltung

Die Steuerhoheit umfaßt neben der Steuergesetzgebung die Steuerertragshoheit und die Steuerverwaltungshoheit. Letztere findet ihre Grundlage in Art. 108 GG. Die Verwaltung von Steuern wird damit den Steuerbehörden zugewiesen.

In der Praxis wird gegenwärtig in verstärktem Maße dazu übergegangen, Steuerdaten durch private Dritte verarbeiten zu lassen.

So hatte ich im Berichtszeitraum zum Versand von Steuerformularen durch eine Privatfirma sowie zur Kuvertierung und zum Versand von Lohnsteuerkarten durch eine private MailingService-Firma Stellung zu nehmen.

Eine mir vorliegende Stellungnahme des Staatsministeriums der Finanzen ordnet die genannten Tätigkeiten im weitesten Sinn der Durchführung eines Steuerverfahrens zu.

Das Staatsministerium hält deshalb die Offenbarung von steuerlichen Daten (hier: Anschrift von Steuerpflichtigen; Steuerklasse) nach § 30 Abs. 4 Nr. 1 der Abgabenordnung für zulässig. Einschränkungen dergestalt, daß dies nicht gegenüber Privatfirmen zulässig sei, träfe die Abgabenordnung nicht.

Die Rechtsauffassung des Staatsministeriums der Finanzen kann bei Hilfstätigkeiten, welche letztendlich den Kern der eigentlichen Verwaltungstätigkeit nicht berühren, geteilt werden.

Datenschutzrechtlich handelt es sich bei dem gewählten Verfahren - bezogen auf den Auftragnehmer - um Datenverarbeitung im Auftrag. Hierbei sind die Regelungen des Art. 6 Bayer. Datenschutzgesetz zu beachten. Danach bleibt der Auftraggeber für die Einhaltung datenschutzrechtlicher Vorschriften (und somit des § 30 AO) verantwortlich. Er hat den Auftragnehmer hinsichtlich dessen Eignung sorgfältig auszuwählen.

Der Schutz des Steuergeheimnisses durch § 30 AO, § 355 StGB muß bei einer Vergabe von Aufträgen außerhalb der Finanzverwaltung allerdings sichergestellt bleiben.

Die Beschäftigten eines Privatunternehmens sind deshalb nach § 1 des Verpflichtungsgesetzes zur gewissenhaften Erfüllung der Obliegenheiten zu verpflichten und auf die strafrechtlichen Konsequenzen von Pflichtverletzungen hinzuweisen. Dadurch werden sie Amtsträgern i.S.v. § 30 Abs. 1 i.V.m. § 7 AO gleichgestellt.

Im übrigen halte ich es für zweckdienlich, den ordnungsgemäßen Ablauf der durchzuführenden Arbeiten durch einen Bediensteten der auftraggebenden Behörde überwachen zu lassen und im Fall der Versendung von Lohnsteuerkarten den zwischen Gemeinden und Mailing-Service-Firma abzuschließenden Vertrag hinsichtlich der erforderlichen Bestimmungen durch das zuständige Finanzamt überprüfen zu lassen. Die Nutzung der übergebenen Adressen der Steuerpflichtigen für andere Zwecke ist auszuschließen.

Soweit diese Voraussetzungen erfüllt sind, werde ich bei der beabsichtigten Auslagerung von Tätigkeiten, welche den eingangs erwähnten Sachverhalten ähnlich sind, keine Einwendungen erheben.

Unklar bleibt, wo die Grenze zu Tätigkeiten liegt, deren die Finanzverwaltung sich durch Outsourcing nicht entledigen kann.

Angesichts der Bedeutung, welche die Privatisierung von öffentlichen Aufgaben bereits jetzt erlangt hat und mehr noch in der Zukunft erlangen wird, halte ich eine eindeutige Regelung zu diesem Komplex in der Abgabenordnung für erforderlich. In diesem Zusammenhang ist auch die Frage zu klären, ob die allgemeinen datenschutzrechtlichen Bestimmungen über die Datenverarbeitung im Auftrag für Fälle des Outsourcing ausreichen oder ob ergänzende Bestimmungen (bspw. zur Kontrollbefugnis) geschaffen werden müssen.

11.3 Steuerdatenabruf-Verordnung

In § 30 der Abgabenordnung, der sich mit dem Steuergeheimnis befaßt, werden in Absatz 6 auch Aussagen zum automatisierten Abruf von steuerlichen Daten getroffen. Danach ist ein Abruf zulässig, soweit er der Durchführung eines Verwaltungsverfahrens in Steuersachen, eines gerichtlichen Verfahrens in Steuersachen, eines Strafverfahrens wegen einer Steuerstraftat, eines Bußgeldverfahrens wegen einer Steuerordnungswidrigkeit oder - als weitere Alternative - der zulässigen Weitergabe von Daten dient.

Zur Wahrung des Steuergeheimnisses kann durch Rechtsverordnung bestimmt werden, welche technischen und organisatorischen Maßnahmen gegen den unbefugten Abruf von Daten zu treffen sind, die Art der Daten, deren Abruf zulässig ist, sowie der Kreis der Amtsträger, die zum Abruf von Daten berechtigt sind.

Aufgrund dieser Ermächtigungsnorm hat die Bundesregierung in der Vergangenheit den Entwurf einer Steuerdatenabruf-Verordnung vorgelegt. Ich habe darüber in meinem zehnten Tätigkeitsbericht informiert.

Im Berichtszeitraum sind die Bemühungen zum Erlaß der Verordnung wohl endgültig gescheitert. Nach übereinstimmender Feststellung der obersten Finanzbehörden der Länder war eine einvernehmliche Regelung über die Einbeziehung der Gemeinden (der kommunalen Steuerbehörden) in die Verordnung nicht möglich.

In der Gegenargumentation wird darauf hingewiesen, daß die im Verordnungsentwurf vorgesehenen Verfahren der Zugriffssicherung und Protokollierung auf kleineren EDV-Anlagen nur mit schwer abschätzbarem Kostenaufwand realisierbar seien, auch würden bei kleineren Gemeinden mit nur wenigen Sachbearbeitern wegen der gegenseitigen Vertretung ein Teil der vorgesehenen Kontrollmechanismen leer laufen. Diese Argumente sind nicht völlig von der Hand zu weisen.

Ich habe aber darauf hingewiesen, daß bei einer pauschalen Nichteinbeziehung aller Gemeinden auch Datenabrufe in und aus den Steuerämtern von Großstädten ungeregelt bleiben. Angesichts des durch eine größere Anzahl von Sachbearbeitern und beteiligten Stellen erhöhten Miß-

brauchsrisikos ergeben sich meines Erachtens gleichartige Regelungsbedürfnisse wie bei den Finanzämtern. Ich habe weiter bemerkt, daß alternativ eine Anwendung des Art. 8 Bayer. Datenschutzgesetz (Einrichtung automatischer Verfahren) nicht in Betracht kommt, da Online-Zugriffe innerhalb unterschiedlicher Ämter einer Gemeinde nicht als Übermittlung im Sinne des Art. 4 Abs. 6 Nr. 3 BayDSG, sondern lediglich als Nutzung im Sinne des Art. 4 Abs. 7 BayDSG anzusehen sind.

Auch sind die übrigen Bestimmungen des Bayer. Datenschutzgesetzes über Datensicherungsmaßnahmen (Art. 7) nicht ausreichend präzise, so daß die anzustrebende gleichartige Verfahrensweise bei Finanzämtern und Steuerämtern großer Gemeinden allein über die vorhandenen gesetzlichen Regelungen nicht erreicht werden kann.

Eine entsprechende Regelung im Wege der Verwaltungsanweisung an die Gemeinden scheidet wegen fehlender Weisungskompetenz der Aufsichtsbehörden aus.

Nach dem Scheitern der Bemühungen ist nunmehr beabsichtigt, an Stelle der ursprünglich vorgesehenen Rechtsverordnung eine zwischen dem Bundesfinanzministerium und den obersten Finanzbehörden der Länder einvernehmliche bundeseinheitliche Steuerdatenabruf-Verwaltungsregelung zu schaffen (ohne Einbeziehung der Gemeinden).

Zu der geplanten Regelung habe ich hinsichtlich einzelner technisch-organisatorischer Maßnahmen gegenüber dem Staatsministerium der Finanzen Stellung genommen.

Aus rechtlicher Sicht erscheint mir wesentlich, daß die Verwaltungsregelung insbesondere hinsichtlich der vorgesehenen Protokollierungsmaßnahmen nicht hinter dem Verordnungsentwurf zurückbleibt.

Wegen der in **Art. 7 Abs. 1** BayDSG normierten Verpflichtung zur Gewährleistung des Datenschutzes durch technische und organisatorische Maßnahmen erwarte ich von großen kommunalen Steuerämtern eine der Steuerdatenabruf-Verwaltungsregelung entsprechende Verhaltensweise. Ich werde diesem Bereich bei meinen Kontrollen in den kommenden Jahren besonderes Augenmerk schenken.

11.4 Prüfung von kommunalen Steuerämtern

Im Berichtszeitraum habe ich zwei kommunale Steuerämter datenschutzrechtlich überprüft. Dabei wurden folgende Feststellungen getroffen:

Verwendung von Melderegisterdaten

Die Stadtsteuerämter nutzen - bspw. für die Bescheidversendung - die im Melderegister gespeicherten Adressen der Steuerpflichtigen (Art. 31 Abs. 7 MeldeG).

Art. 34 Abs. 5 MeldeG sieht vor, daß jede Melderegisterauskunft unzulässig ist, wenn dadurch im Gesetz genannte schutzwürdige Belange der Betroffenen verletzt werden. Diese Auskunftssperre wirkt für alle Arten der Melderegisterauskünfte, also auch für die einfache Melderegisterauskunft. Die Auskunftssperre wirkt allerdings nur gegenüber privaten Dritten. Sie zeigt keine Auswirkungen auf Datenübermittlungen für den öffentlichen Bereich nach den Art. 30 - 32 MeldeG. Den Datenempfängern im öffentlichen Bereich ist jedoch die Tatsache einer eingerichteten Auskunftssperre mitzuteilen, damit sich diese bei der Verwendung der übermittelten Daten entsprechend beschränken. Dies gilt auch für eine Datenweitergabe innerhalb der Stadt.

Bei einer Überprüfung eines entsprechenden Falles wurde festgestellt, daß das Steueramt einer Stadt bei Übernahme der Adresse eines Bürgers und Steuerpflichtigen keinen Hinweis auf eine bestehende Auskunftssperre erhielt.

Ich habe eine entsprechende Ergänzung des Verfahrens gefordert, was inzwischen geschehen ist.

Aufbewahrung/Archivierung

Bei einem Stadtsteueramt wurden die Datensätze und Aktenunterlagen 30 Jahre gespeichert bzw. aufbewahrt.

Ich habe eine derart lange Aufbewahrungsdauer für nicht sachgerecht gehalten. Nach Art. 12 Abs. 1 Nr. 2 BayDSG sind personenbezogene Daten in Dateien zu löschen, wenn ihre Kenntnis

für die speichernde Stelle zur Erfüllung der in ihrer Zuständigkeit liegenden Aufgaben nicht mehr erforderlich ist.

Das Bayerische Archivgesetz (BayArchivG) bestimmt, daß öffentliche Stellen dem zuständigen Archiv jene Unterlagen zur Übernahme anzubieten haben, die sie zur Erfüllung ihrer Aufgaben nicht mehr benötigen. Für die öffentlichen Stellen des Freistaates Bayern wird dies in der Regel 30 Jahre nach Entstehung der Unterlagen angenommen, soweit durch Rechtsvorschriften oder Verwaltungsvorschriften der obersten Staatsbehörden nichts anderes bestimmt ist (Art. 6 Abs. 1 Satz 2 BayArchivG).

Für die staatlichen Stellen hat die Bayerische Staatsregierung mit Bekanntmachung vom 19.11.1991 (AllMBl S. 884) Aussonderungsbestimmungen erlassen. Nach Nr. 5.1 der Bekanntmachung ist die Aussonderung von Unterlagen in regelmäßigen Zeitabständen, spätestens alle 10 Jahre vorzunehmen.

Soweit das zuständige Archiv eine Übernahme ablehnt, sind die Unterlagen zu vernichten.

Art. 6 Abs. 1 Satz 2 BayArchivG gilt für Kommunen nicht unmittelbar. Diese regeln die Archivierung der bei ihnen erwachsenen Unterlagen vielmehr in eigener Zuständigkeit (Art. 13 BayArchivG).

In der Gemeinsamen Bekanntmachung der Bayer. Staatsministerien des Innern und für Kultus, Wissenschaft und Kunst vom 22.1.1992 (AllMBl S. 139) wird unter Nr. 1.4 den Kommunen aber empfohlen, die angesprochene Aussonderungsbekanntmachung der Staatsregierung sinngemäß anzuwenden.

Einen Anhaltspunkt für die Aufbewahrungsdauer bspw. der Gewerbesteuerunterlagen des Steueramts können auch die Bestimmungen zur Aufbewahrung und Aussonderung von Schriftgut bei den Finanzämtern darstellen.

Nach den genannten Bestimmungen sind Unterlagen zur Durchführung der Besteuerung bei Fällen mit Gewinneinkünften grundsätzlich 10 Jahre aufzubewahren.

Ich habe aus diesen Gründen eine Löschung der automatisiert gespeicherten Gewerbesteuerdaten für rechtskräftige Veranlagungsjahre bzw. eine Anbietung und ggf. Löschung der für diese Jahre entstandenen Unterlagen nach 10 Jahren für sachgerecht gehalten.

Für andere Steuerarten habe ich das Stadtsteueramt um eine praxisnahe Festlegung der Aufbewahrungsfristen gebeten.

Das betreffende Stadtsteueramt hat sich entschieden, die Aufbewahrungsfristen für rechtskräftige Gewerbesteuerveranlagungsjahre auf 10 Jahre, für abgeschlossene Grundsteuerfälle auf 5 Jahre und für nicht mehr existierende Hundesteuertatbestände auf 2 Jahre festzusetzen.

Dagegen habe ich keine Einwendungen erhoben.

11.5 Datenschutzrechtliche Prüfung des Landesentschädigungsamtes

Mitarbeiter meiner Geschäftsstelle haben im Berichtszeitraum das Landesentschädigungsamt datenschutzrechtlich überprüft.

Aus den Prüfungsfeststellungen möchte ich folgende Punkte herausgreifen:

Weitergabe von Entschädigungsakten an Gutachter.

Bei Anträgen zur Feststellung einer Leidensverschlimmerung von Betroffenen mit Wohnsitz im Inland entscheidet der Ärztliche Dienst des Landesentschädigungsamtes über die Erforderlichkeit der Einschaltung eines medizinischen Gutachters. Dieser wird ggf. direkt vom Ärztlichen Dienst beauftragt. Dem Gutachter wurden bisher die gesamten Entschädigungsakten übermittelt. Der Antragsteller wurde von der Beauftragung informiert.

Ich habe aus datenschutzrechtlicher Sicht die Übergabe der gesamten Entschädigungsakte - also bspw. einschließlich der Erklärung über die Einkommensverhältnisse usw. - für nicht erforderlich gehalten. Ich habe verlangt, nur die für das Gutachten benötigten medizinischen Unterlagen zur Verfügung zu stellen.

Das Landesentschädigungsamt hat aufgrund dieser Prüfungsfeststellung seine diesbezügliche Praxis geändert. Es holt nunmehr vor einer Datenübermittlung die ausdrückliche Einwilligung des Betroffenen zu einer Weitergabe der gesamten Entschädigungsakte ein. Wird diese nicht erteilt, werden nur die medizinisch relevanten Aktenteile an den Gutachter übersandt.

Zentralkartei

Bei der Prüfung wurden regelmäßige Datenweitergaben an eine und von einer der Bezirksregierung Düsseldorf Abt. Wiedergutmachung (vormals Landesrentenbehörde Nordrhein-Westfalen) zugeordneten Bundeszentralkartei festgestellt.

In dieser Kartei sind alle Antragsteller auf Leistungen nach dem Bundesentschädigungsgesetz

enthalten. Gespeichert sind Name, Vorname, Geburtsdatum, Geburtsort, Familienstand, Wohnort, ggf. Namen der Erben sowie die aktenführenden Stellen.

Das Land Nordrhein-Westfalen ist seit 1.2.1954 mit der Einrichtung und Unterhaltung der Kartei betraut. Es besteht eine Ländervereinbarung, die in der Hauptsache die Verteilung der Kosten regelt.

In meinem Prüfbericht habe ich dargelegt, daß ich für die genannte Kartei normenklare Regelungen für erforderlich halte.

In Verhandlungen mit dem Staatsministerium der Finanzen habe ich deutlich gemacht, daß ich mich auch der Interpretation, wonach die Bezirksregierung Düsseldorf hinsichtlich der Bundeszentralkartei Datenverarbeitung im Auftrag betreibt, nicht verschließen würde. Die Landesentschädigungsbehörden blieben danach Herr der an die Bundeszentralkartei jeweils gemeldeten Daten.

In diesem Fall wäre aber gem. Art. 6 Abs. 2 BayDSG die Auftragsvergabe zu konkretisieren, was im Rahmen einer Ergänzung der Ländervereinbarung erfolgen könnte.

In dieser Ergänzung wären insbesondere Festlegungen zum Umfang der gespeicherten Daten, zur Datenverarbeitung und -nutzung (also bspw. zur Auskunftserteilung), zur Löschung bzw. Aufbewahrungsdauer und zu technischen und organisatorischen Maßnahmen zu treffen.

Das Staatsministerium wird die Angelegenheit auf der nächsten Konferenz der Entschädigungsreferenten der Länder behandeln.

11.6 Auskünfte aus den Steuerkarteien von Gemeinden

In meinem fünfzehnten Tätigkeitsbericht habe ich zur Nutzung von Grundsteuer-Adreßdaten von Gemeinden für andere öffentliche Aufgaben Stellung genommen.

Zu diesem Themenkomplex erreichen mich immer wieder Anfragen.

Ich weise darauf hin, daß es sich bei den Grundsteueradreßdaten im Grundsatz um dem Steuergeheimnis unterliegende Daten handelt. Die Durchbrechung des Steuergeheimnisses wurde durch § 31 Abs. 3 der Abgabenordnung (AO) für bestimmte Zwecke zwar erlaubt, aber zugleich durch Benennung nur bestimmter Datenempfänger wieder eingeschränkt. § 31 Abs. 3 AO ermöglicht den für die Verwaltung der Grundsteuer zuständigen Behörden, die Namen und Anschriften von Grundstückseigentümern zur Erfüllung sonstiger öffentlicher Aufgaben zu verwenden oder den hierfür zuständigen Gerichten, Behörden oder juristischen Personen des öffentlichen (nicht privaten!) Rechts auf Ersuchen mitzuteilen, soweit nicht überwiegende schutzwürdige Interessen des Betroffenen entgegenstehen.

Aufgrund dieser Bestimmung war bspw. die Frage einer Gemeinde, ob es zulässig sei, dem Auskunftsersuchen einer Rechtsanwaltskanzlei nach Grundbesitz eines Gemeindebürgers zu entsprechen, zu verneinen.

Positiv beantworten konnte ich die Anfrage zur Zulässigkeit der Überlassung der gemeindlichen Grundsteueradreßdaten an den Landkreis zur Erfüllung der öffentlichen Aufgabe Müllbeseitigung.

Ebenfalls positiv war meine Stellungnahme zur Nutzung der Anschriften von Grundstückseigentümern aus den Grundsteuerdateien für Zwecke der Vermessungsämter.

11.7 Datenübermittlungen der Finanzämter an die Industrie- und Handelskammern

Im Berichtszeitraum haben mehrere Gewerbetreibende um datenschutzrechtliche Bewertung der Mitteilung ihres Gewerbeertrags durch das für sie zuständige Finanzamt an die jeweilige Industrie- und Handelskammer für Zwecke der Beitragsfestsetzung gebeten.

Dazu ist folgendes zu bemerken:

Die Industrie- und Handelskammern sind Körperschaften des öffentlichen Rechts. Durch § 3 Abs. 3 des Gesetzes zur vorläufigen Regelung des Rechts der Industrie- und Handelskammern (IHKG) wird ihnen das Recht eingeräumt, Beiträge gestaffelt nach der Leistungskraft der Kammerzugehörigen zu erheben. Bemessungsgrundlage ist dafür im Regelfall der Gewerbeertrag.

Nach § 9 Abs. 2 IHKG sind die Kammern berechtigt, die o.g. Bemessungsgrundlage bei den Finanzbehörden zu erheben.

Damit korrespondierend erlaubt es § 31 Abs. 1 der Abgabenordnung den Finanzbehörden, Besteuerungsgrundlagen an Körperschaften des öffentlichen Rechts zur Festsetzung von solchen Abgaben mitzuteilen, die an diese Besteuerungsgrundlagen anknüpfen.

Nach herrschender Meinung sind unter dem Begriff Abgaben nicht nur Steuern, sondern auch Gebühren und Beiträge zu verstehen.

Ich vermag aus den genannten Gründen keine datenschutzrechtlichen Einwendungen gegen die geschilderten Datenübermittlungen zu erheben.

11.8 Unzulässige Anforderung von Führungszeugnissen und Verweigerung der Akteneinsicht im Bereich der Staatlichen Lotterieverwaltung und des Staatsministeriums der Finanzen

Einer Beschwerde lag folgender Sachverhalt zugrunde:

Im Rahmen der Nichterteilung eines Geschäftsauftrags zur Führung einer Lotto- und Totoannahmestelle durch die Staatl. Lotterieverwaltung kam es zu Streitigkeiten.

In der Folgezeit beschwerte sich der Eingabeführer bei verschiedenen Stellen, u.a. bei der Staatl. Lotterieverwaltung, dem Bayer. Staatsministerium der Finanzen, einem Landtagsabgeordneten und dem Petitionsausschuß des Bayer. Landtags.

In Stellungnahmen der Staatl. Lotterieverwaltung bzw. des Staatsministerium der Finanzen gegenüber dem Landtagsabgeordneten bzw. dem Petitionsausschuß des Bayer. Landtags wurden als Gründe für die Nichterteilung des Geschäftsauftrags neben technischen Hindernissen und fehlendem Bedarf auch nicht näher erläuterte Gründe in der Person des Antragstellers erwähnt.

Der Eingabeführer versuchte mehrmals, Auskunft über die Gründe seiner persönlichen Nichteignung zu erhalten. Diese Auskunft wurde ihm ohne Angabe von Gründen nicht gewährt.

Meine Ermittlungen ergaben folgendes:

Seit vielen Jahren holt die Staatliche Lotterieverwaltung beim Bundeszentralregister Führungszeugnisse für Behörden nach § 31 Bundeszentralregistergesetz (BZRG) für alle Bewerber für eine Lotto- und Totoannahmestelle ein. In den früher dabei verwendeten Formularen versicherte die Staatliche Lotterieverwaltung in jedem Einzelfall, daß eine Aufforderung an den Betroffenen, ein Führungszeugnis vorzulegen, nicht sachgemäß sei. Diese Erklärung war unrichtig. § 31 BZRG sieht als Regelfall vor, daß die Behörde den Betroffenen selbst auffordert, ein Führungszeugnis nach § 30 Abs. 5 BZRG vorzulegen. Mit dieser Aufforderung erfüllt die Behörde am ehesten den Grundgedanken des informationellen Selbstbestimmungsrechts. Der Betroffene kann verlangen, daß das Führungszeugnis, wenn es Eintragungen enthält, zunächst an ein von ihm

benanntes Amtsgericht zur Einsichtnahme durch ihn übersandt wird (§ 30 Abs. 5 Satz 3 BZRG). Dies eröffnet dem Betroffenen die Möglichkeit, nach Einsichtnahme zu entscheiden, ob das Führungszeugnis an die Behörde weitergeleitet oder vom Amtsgericht vernichtet wird, wobei im letzteren Fall rechtliche Nachteile billigend in Kauf zu nehmen sind. Die Staatliche Lotterieverwaltung konnte auf Befragen keine Gründe darlegen, die eine entsprechende Aufforderung an den Betroffenen als nicht sachgemäß erscheinen ließen.

Ich habe die Verfahrensweise der Staatlichen Lotterieverwaltung beanstandet und die Herstellung eines rechtlich einwandfreien Zustandes in den Vertragsunterlagen mit den Lotto- und Totoannahmestellen gefordert. Zwar hatte die Staatliche Lotterieverwaltung das Verfahren kurz vor meiner Intervention selbst der Rechtslage angepasst; die Beschwer der Betroffenen dauert jedoch noch an, da die Vertragsunterlagen immer noch die Auszüge aus dem Bundeszentralregister enthalten und die Betroffenen von dieser Tatsache nichts wissen. Aufgrund meiner Beanstandung hat die Staatliche Lotterieverwaltung alle früheren Auszüge aus dem Bundeszentralregister inzwischen gem. Art. 12 Abs. 3 BayDSG gesperrt.

Auch für den Beschwerdeführer war ein Auszug aus dem Bundeszentralregister eingeholt worden, der eine Eintragung aufwies. Es handelte sich dabei um ein Delikt, daß nach Angaben der Staatlichen Lotterieverwaltung der Erteilung eines Geschäftsauftrages normalerweise nicht im Wege steht.

Das Staatsministerium der Finanzen fügte den Auszug aus dem Bundeszentralregister den eigenen Akten zu, um eine Dienstaufsichtsbeschwerde gegen einen Beamten des Ministeriums bearbeiten zu können. In einem Antwortschreiben an einen Landtagsabgeordneten und in einer Stellungnahme an den Petitionsausschuß des Landtags wies das Ministerium auf Bedenken gegen die persönliche Eignung des Beschwerdeführers hin, ohne dies näher auszuführen. Im gleichen Zusammenhang erklärte das Ministerium aber auch, daß der Bewerbung allein aus sachlichen Gründen nicht hätte entsprochen werden können. Der Beschwerdeführer versuchte daraufhin mehrfach, Auskunft über die Gründe seiner persönlichen Nichteignung zu erhalten. Diese Auskunft wurde ihm ohne Angabe von Gründen nicht gewährt.

Ich habe die Aufnahme des Führungszeugnisses für Behörden in die Aktenunterlagen des Mini-

steriums, sowie die Datenweitergabe aufgrund der Erkenntnisse aus diesem Führungszeugnis an den Bayerischen Landtag beanstandet. Ebenfalls beanstandet habe ich die Weigerung des Ministeriums, dem Beschwerdeführer Auskunft über die zu seiner Person in Akten gespeicherten Daten, sowie Einsicht in das Führungszeugnis zu gewähren.

Das Ministerium konnte nicht darlegen, inwieweit die Anforderung des Führungszeugnisses zur Entscheidung über eine Dienstaufsichtsbeschwerde notwendig gewesen sein sollte. Die Länge des Vorstrafenregisters eines Beschwerdeführers kann im allgemeinen kein Bewertungskriterium für die Prüfung einer Dienstaufsichtsbeschwerde sein. Auch im konkreten Fall konnte das Ministerium eine Begründung nicht nachweisen. Für die Beantwortung der Anfrage des Landtagsabgeordneten und für die Stellungnahme an den Petitionsausschuß des Landtags waren abwertende Andeutungen zur Person des Beschwerdeführers nicht sachdienlich, da als Gründe für die Nichterteilung des Geschäftsauftrages fehlender Bedarf angegeben wurde. Nach Art. 10 Abs. 1 BayDSG hat die speichernde Stelle dem Betroffenen auf Antrag Auskunft zu erteilen über die zu seiner Person gespeicherten Daten, den Zweck der Speicherung, sowie die Herkunft der Daten und deren Empfänger, soweit diese Angaben gespeichert sind. Ferner hat die Behörde gem. § 31 Satz 2 BZRG dem Betroffenen auf Verlangen Einsicht in das Führungszeugnis zu gewähren.

Aufgrund meiner Beanstandung hat das Ministerium dem Beschwerdeführer inzwischen Auskunft und Einsichtnahme angeboten.

12. Personalwesen

12.1 Zulässigkeit von Personalnebenakten

Bei der datenschutzrechtlichen Prüfung von Dienststellen stelle ich immer wieder Unklarheiten über die Zulässigkeit der Führung von Personalnebenakten fest.

Ausführliche Regelungen zur Führung von Personal(neben)akten enthält das Bayer. Beamtengesetz. Ihre Anwendung beschränkt sich damit zunächst nur auf die Personalunterlagen von Beamten.

Eine Vielzahl der aufgestellten Grundsätze ist nach meiner Ansicht aber auf die Personalaktenführung aller öffentlichen Bediensteten anzuwenden.

Gemäß Art. 100 a Abs. 2 BayBG können Nebenakten (Unterlagen, die auch im Grundakt oder in Teilakten vorhanden sind) geführt werden, wenn die personalverwaltende Behörde nicht zugleich Beschäftigungsbehörde ist. Ich interpretiere den Gesetzestext so, daß Behörde dabei jede Stelle ist, die Aufgaben der öffentlichen Verwaltung wahrnimmt. Personalnebenakten dürfen nur solche Unterlagen enthalten, deren Kenntnis zur rechtmäßigen Aufgabenerledigung der betreffenden Behörde (Stelle) erforderlich ist (Art. 100 a Abs. 2 Satz 3 BayBG).

Bei der Beurteilung, welche Unterlagen bei nachgeordneten Dienstbehörden zur rechtmäßigen Aufgabenerledigung erforderlich sind, kann die jeweilige Zuständigkeit in personalrechtlichen Entscheidungen nur ein Teilaspekt sein. Zwar ist vielfach die personalrechtliche Zuständigkeit des unmittelbaren Dienstvorgesetzten beschränkt; jedoch darf die dem Dienststellenleiter vor Ort zukommende Organisationsgewalt und das ihm gegenüber den Beschäftigten im Amt zustehende Direktionsrecht nicht außer Betracht bleiben. Die Ausübung der Organisationsgewalt und des Direktionsrechts machen die Information über die durch die vorgeordneten Dienstbehörden getroffenen personalrechtlichen Entscheidungen (mit Aufnahme in den Personalnebenakt) in vielen Fällen erforderlich.

Personalnebenakten liegen bereits vor, wenn beispielsweise Abdrucke von Versetzungs- und Abordnungsverfügungen sowie Unterlagen über Beförderungen und Ernennungen bei der Be-

schäftigungsbehörde vorgehalten werden.

Dies gilt auch, wenn dem Dienststellenleiter dabei lediglich ein Abdruck der abschließenden Entscheidung, nicht jedoch Abdrucke der Vorgänge, die im Rahmen der Entscheidungsvorbereitung innerhalb der personalverwaltenden Stelle(n) angefallen sind, zur Verfügung gestellt werden.

Ich verweise in diesem Zusammenhang auf die Gesetzesbegründung zum "Zwölften Gesetz zur Änderung beamtenrechtlicher Vorschriften" vom 23. Juli 1994. Danach sind in einen Personalakt insbesondere aufzunehmen: Nachweise über Vor-, Aus- und Weiterbildung, Prüfungszeugnisse, Unterlagen über Ernennungen, Abordnungen, Versetzungen usw.

Personalnebenakten können auch bei automatisierter Verarbeitung von Personalaktendaten entstehen.

Gemäß Art. 100 a Abs. 2 Satz 4 BayBG ist in den Grundakt ein vollständiges Verzeichnis aller Teil- und Nebenakten aufzunehmen. Diese Bestimmung soll das in Art. 100 d Abs. 1 Satz 1 BayBG vorgesehene Einsichtsrecht des Beamten in seinen vollständigen Personalakt sicherstellen. Kein Kriterium kann in diesem Zusammenhang sein, daß der Inhalt der Personalunterlagen bei der Beschäftigungsbehörde den Bediensteten oftmals vollinhaltlich bekannt ist.

Nebenakten sind zu vernichten, sobald sie zur rechtmäßigen Aufgabenerfüllung bei der Beschäftigungsbehörde nicht mehr erforderlich sind, also beispielsweise bei der Versetzung des Beschäftigten an eine andere Dienststelle. Nachdem Nebenakten nur Vorgänge enthalten dürfen, die sich bereits im Grundakt oder in Teilakten befinden, besteht für eine Weitergabe an den neuen Dienstvorgesetzten, der bei einer Versetzung ohnehin in der Regel den gesamten Personalakt erhält, grundsätzlich keine Veranlassung. Anders kann jedoch der Fall liegen, wenn bei einem entsprechend gegliederten Verwaltungsaufbau durch Organisationsanordnung bestimmt ist, daß die Personalakten nicht beim neuen direkten Dienstvorgesetzten, sondern bei einer vorgesetzten Behörde geführt werden.

12.2 Organisatorische Trennung der Beihilfestelle von der Personalverwaltung

Im Rahmen der datenschutzrechtlichen Prüfung der Personalverwaltung einer Stadt habe ich mich auch mit der organisatorischen Trennung der Beihilfestelle von der Personalverwaltung befaßt.

Die Beihilfestelle war organisatorisch in das Personalamt integriert. Die Beihilfeunterlagen wurden zwar in Beihilfe(teil)akten, aber in einer gemeinsamen Registratur mit den Personalakten im Personalamt geführt. Eingehende Beihilfeunterlagen wurden vom Registrator geöffnet und zusammen mit der Beihilfeakte auf dem üblichen Dienstweg (Bote) der Beihilfestelle zugeleitet. Weiterhin waren die Beihilfesachbearbeiter nur bis zu einer bestimmten Grenze beihilfefähiger Aufwendungen zeichnungsbefugt. Darüber hinausgehende Beihilfeverfügungen wurden vom stellvertretenden Leiter des Personalamts unterzeichnet.

Ich habe in meinem Prüfbericht gegenüber der Stadt gegen die dargestellte Verfahrensweise erhebliche datenschutzrechtliche Bedenken erhoben.

Im Zuge der weiteren Erörterung hat die Stadt das von ihr praktizierte Verfahren als bei einer Vielzahl von Kommunen übliche Sachbearbeitung dargestellt. Meine weiteren Ermittlungen und Eingaben im Berichtszeitraum haben diese Aussage bestätigt. Ich möchte diese Fälle deshalb zum Anlaß nehmen, grundsätzliche Ausführungen zur organisatorischen Trennung von Beihilfestelle und Personalverwaltung zu treffen:

Das novellierte Bayerische Beamtengesetz (BayBG) enthält in Art. 100 b Vorschriften zur Führung von Beihilfeakten. Danach sind Unterlagen über Beihilfen stets als Teilakt zu führen. Dieser Teilakt ist vom übrigen Personalakt getrennt aufzubewahren. Er soll in einer von der übrigen Personalverwaltung getrennten Organisationseinheit bearbeitet werden. Zugang sollen nur Beschäftigte dieser Organisation haben.

Art 100 b BayBG gilt zunächst nur für Beamte. Die darin aufgestellten Grundsätze sind nach meiner Ansicht aber auf alle öffentlichen Bediensteten anzuwenden.

Die Fassung als Sollvorschrift erfolgte - ausweislich der Gesetzesbegründung - mit Rücksicht

auf sehr kleine personalverwaltende Dienststellen, insbesondere im kommunalen Bereich, bei denen ein Sachbearbeiter mit der Bearbeitung von Beihilfevorgängen nicht ausgelastet ist und ihm zwangsläufig noch andere Aufgaben übertragen werden müssen.

Bei der eingangs geschilderten vor Ort festgestellten Verfahrensweise ergeben sich vielfältige Berührungspunkte zur Personalsachbearbeitung. So übernimmt der stellvertretende Leiter des Personalamts durch die für bestimmte Fälle vorgesehene Unterschriftsleistung die Verantwortung für die sachliche und inhaltliche Richtigkeit der Beihilfebescheide. Die beihilfebegründenden Unterlagen sind den Bescheiden zu diesem Zeitpunkt noch beigeheftet, so daß eine Kenntnisnahme zwangsläufig ist.

Diese Unterlagen und zum Teil auch die Beihilfeakten selbst enthalten regelmäßig höchstpersönliche Daten über Krankheiten, Diagnosen, Behandlungen und Medikationen des Bediensteten (und seiner Angehörigen), die bei zweckwidrigem Gebrauch zu spürbaren Nachteilen für den Betroffenen führen können.

Der Abschottung und damit der strikten organisatorischen Trennung der Beihilfeakten und -bearbeitung von den sonstigen Personalakten und der sonstigen Personalverwaltung kommt damit erhöhte Aufmerksamkeit zu.

Diese Abschottung läßt sich zum einen durch Ausgliederung der Beihilfestelle aus dem Personalamt bzw. der Personalverwaltung erzielen. Es sind jedoch auch andere Verfahren denkbar, soweit diese gewährleisten, daß mit Personalangelegenheiten befaßte Entscheidungsträger bei normalem Geschäftsgang weder Einblick in die Beihilfeunterlagen und -bescheide nehmen können, noch Beihilfebescheide unterzeichnen.

Die von mir hinsichtlich der Personalverwaltung geprüfte Stadt hat in diesem Zusammenhang folgende Vorschläge unterbreitet:

Räumliche Trennung

Der Beihilfestelle werden neue Räume, getrennt von der Personalverwaltung, zugewiesen.

Die gesonderten Beihilfeakten werden in einem eigenen Aktenraum der Beihilfestelle mit verschärften Sicherungsmaßnahmen und Zugangsmöglichkeiten nur für die Beschäftigten der Beihilfestelle untergebracht.

Sachliche Trennung

Die Beihilfestelle erhält einen eigenen Posteinlauf und Postauslauf in den neuen Räumen der Beihilfestelle.

Den Beihilfeberechtigten wird ein eigenes Kuvert mit dem Aufdruck "Beihilfeunterlagen" zur Verfügung gestellt, das diese zur Übersendung des Beihilfeantrages sowie der Belege verwenden können. Dadurch wird sichergestellt, daß dieses Kuvert weder bei der zentralen Posteinlaufstelle noch bei der Registratur des Personalamtes geöffnet werden.

Organisatorische Trennung

Die Beschäftigten der Beihilfestelle handeln in Beihilfeangelegenheiten nur nach Weisung des Leiters der Beihilfestelle.

Die Beihilfestelle ist keiner Abteilung des Personalamtes eingegliedert, sondern der Amtsleitung des Personalamtes als Stabsstelle unmittelbar zugeordnet.

Der Amtsleiter des Personalamtes wird gegenüber dem Leiter der Beihilfestelle und den Mitarbeitern nur noch als Dienstvorgesetzter tätig.

Der Leiter der Beihilfestelle entscheidet in Widerspruchsverfahren in eigener Zuständigkeit selbständig.

Dem Leiter der Beihilfestelle wird die uneingeschränkte Anordnungs- und Bewirtschaftungsbefugnis sowie Unterschriftsbefugnis in Beihilfeangelegenheiten übertragen. Bei Verhinderung des Leiters der Beihilfestelle gilt die Anordnungs- und Bewirtschaftungsbefugnis für die Stellvertre-

ter.

Personelle Trennung

Die Beschäftigten in der Beihilfestelle werden nicht mit Personalangelegenheiten befaßt. Dies gilt auch für eine mögliche Vertretungsregelung.

Ich habe gegen diese Vorschläge keine datenschutzrechtlichen Bedenken erhoben, da sie die vom Gesetz vorgesehene und aus datenschutzrechtlicher Sicht auch unabdingbare organisatorische Trennung der Beihilfeakten und -bearbeitung von den sonstigen Personalakten und der sonstigen Personalverwaltung gewährleisten.

---

12. 3 Telefondatenerfassung

Die Mehrzahl der heute eingesetzten Telefonanlagen erlaubt eine automatische Gesprächsdatenerfassung und -auswertung.

Bei Telefonanlagen in Behörden sind deshalb Regelungen erforderlich, die sowohl den schutzwürdigen Belangen der Bediensteten als auch den berechtigten Interessen des Dienstherrn Rechnung tragen.

Bei Prüfungen mußte ich immer wieder Unsicherheiten im Vollzug feststellen. Ich fasse den gegenwärtigen Diskussionsstand daher wie folgt zusammen:

Anlagen zur Telefondatenerfassung und -auswertung sind regelmäßig technische Einrichtungen auch zur Überwachung des Verhaltens oder der Leistung der Bediensteten. Ihr Einsatz ist daher nach Art. 75 a des Bayerischen Personalvertretungsgesetzes (BayPVG) mitbestimmungspflichtig. Über die getroffenen Modalitäten wird in der Regel eine schriftliche Dienstvereinbarung (Art. 73 BayPVG) abgeschlossen.

Die Speicherung von Telefonverbindungsdaten dient der Erfüllung haushaltsrechtlicher Vorschriften (Sparsamkeit, Wirtschaftlichkeit) und ist deshalb insoweit als erforderlich im Sinne des Bayerischen Datenschutzgesetzes anzusehen.

Die verwendeten Telefoncomputer ermöglichen in der Regel die Erfassung folgender Daten:

- Nummer der rufenden Nebenstelle (einschließlich des zugelassenen Benutzers dieser Nebenstelle)

- Datum und Uhrzeit des geführten Gesprächs

- Zielnummer (Vorwahl / Rufnummer)

- aufgelaufene Gebühreneinheiten für das Gespräch (Kosten)

- Kennzeichnung als Privat- oder Dienstgespräch (soweit Privatgespräche generell zugelassen sind)

- ggf. weitere technische Merkmale (Nummer der belegten Amtsleitung u.ä.)

Bei privaten Orts- und Nahgesprächen ist vielfach Kostenerstattung nicht vorgesehen, wenn die Gesprächsgebühren keinen unvertretbaren Umfang annehmen. Die Speicherung der Zielnummer, sowohl für dienstliche als auch private Orts- und Nahgespräche ist in diesen Fällen nicht erforderlich.

Bei dienstlichen und privaten Ferngesprächen (soweit letztere gegen Kostenerstattung überhaupt zugelassen sind) werden im Regelfall alle oben aufgeführten Merkmale gespeichert.

Die Auswertung der gespeicherten Daten dienstlicher Telefongespräche hat sich am Grundsatz der Erforderlichkeit zu orientieren.

Zulässig sind beispielsweise

- ein Ausdruck der Summe der Gebühreneinheiten pro Nebenstelle

- ein Ausdruck aller gespeicherten Daten pro Nebenstelle

- ein Ausdruck aller gespeicherten Daten von Gesprächen, deren Kosten einen festgelegten Grenzwert überschritten haben.

Soweit die Führung von Privatgesprächen gegen Erstattung der Gesprächsgebühren erlaubt ist, sind diese Gespräche schon bei der Speicherung besonders zu kennzeichnen. Die gespeicherten Daten dürfen in diesen Fällen ausschließlich für Abrechnungszwecke verwendet werden. Beim Ausdruck der Daten ist die Zielnummer zu unterdrücken oder zu verkürzen, um eine unbefugte Kenntnisnahme der angerufenen Gesprächsteilnehmer durch Dritte zu vermeiden. Ausdrucke mit (auch verkürzten) Zielnummern dürfen nur den betroffenen Bediensteten zugänglich gemacht werden. Eine Versendung sollte nur im verschlossenen Umschlag erfolgen. Ein vollständiger

Ausdruck der angewählten Zielnummer zur eindeutigen Identifizierung des Gesprächspartners ist nur bei strittigen Abrechnungsfällen zulässig.

Sonderregelungen sind für die Gespräche der Personalvertretung und von Bediensteten, die einer besonderen Schweigepflicht unterliegen, vorzusehen. Zu letzteren sind Behördenbedienstete zu rechnen, die im Rahmen der freiwilligen Beratung tätig sind, so z.B. in der Drogenberatung oder Ehe- und Familienberatung.

Alle Bediensteten sind bei der Neuinstallation eines Telefoncomputers bzw. bei der Einstellung auf den Umfang der Speicherung und Auswertung von Gesprächsdaten in der Dienststelle hinzuweisen.

Staatliche Behörden haben auch die vom Bayerischen Staatsministerium der Finanzen erlassenen Dienstanschlußvorschriften zu beachten.

Die automatisierte Speicherung und Auswertung von Telefongesprächen ist nach Art. 26 BayDSG vor dem erstmaligen Einsatz oder einer wesentlichen Änderung des Verfahrens von der dafür zuständigen Stelle datenschutzrechtlich freizugeben.

12.4 Veröffentlichung von Behördenfernsprechverzeichnissen

Immer wieder erreichen mich Anfragen von Behörden, die um datenschutzrechtliche Stellungnahme zum beabsichtigten Verkauf behördeneigener Telefonverzeichnisse in der Öffentlichkeit bitten.

Durch den Verkauf sollen - auch mit Hilfe von Werbeinseraten - die Herstellungskosten finanziert werden.

Zu diesem Sachverhalt habe ich bereits in meinem vierzehnten Tätigkeitsbericht kurz Stellung genommen. Wegen der Aktualität des Themas möchte ich die mir in diesem Zusammenhang wesentlichen Punkte nochmals zusammenfassen.

Ein berechtigtes Interesse an der Kenntnis der in einem behördlichen Telefonverzeichnis aufgeführten personenbezogenen Daten sämtlicher Mitarbeiter kann in der Öffentlichkeit nur dann bestehen, wenn diese Kenntnis für den Erwerber des Verzeichnisses im telefonischen Verkehr mit der Behörde notwendig und damit erforderlich ist. Diese Erforderlichkeit ist im Regelfall jedoch nicht gegeben. Es ist z.B. nicht einzusehen, welchen anerkennenswerten Nutzen die Öffentlichkeit aus der Kenntnis der konkreten personellen Zusammensetzung von Dienststellen ziehen sollte, soweit die Mitarbeiter im Parteiverkehr nicht in Erscheinung treten. Der Persönlichkeitsschutz der Bediensteten steht hier einer generellen Weitergabe entgegen.

Mitarbeiterdaten können allerdings in Form eines Behördenwegweisers veröffentlicht werden, wenn es darum geht, in allgemeiner Form darüber zu informieren, wer konkret für den Bürger Ansprechpartner bei einschlägigen Themenkomplexen ist.

Die behördlichen Telefonverzeichnisse sind im übrigen vom Grundsatz her für den dienstlichen Gebrauch bestimmt. Sie sind daher nicht als allgemein zugängliche Quelle im Sinne des Datenschutzgesetzes anzusehen.

Ein Verkauf bzw. eine Veröffentlichung eines vollständigen behördlichen Fernsprechverzeichnisses scheidet damit aus.

12.5 Aufnahme von Unterlagen mit negativem Inhalt in den Personalakt

Im Rahmen einer Eingabe habe ich von folgendem Sachverhalt Kennntnis erlangt:

Die Eingabeführerin hatte sich um eine freie Funktionsstelle an einer Schule beworben, an der sie bereits tätig war. In einem Schreiben hatte daraufhin der Leiter der Schule die zuständige Regierung gebeten, diese Bewerbung nicht weiter zu behandeln. In diesem Schreiben waren z.T. sehr negative Äußerungen über die Bewerberin enthalten. Abschließend verwies der Schulleiter auf einen bereits von ihm erstellten "Dreiervorschlag" für die Funktionsstelle.

Die Regierung hat im weiteren Verlauf den Schulleiter um Abgabe eines neuen "Dreiervorschlags" gebeten. In diesem Vorschlag war die Eingabeführerin aufgeführt, wobei der Schulleiter in Form einer ergänzenden Bemerkung seine negativen Äußerungen über die Petentin wiederholte. Zugleich hat der Schulleiter gebeten, einen namentlich genannten anderen Bewerber auf der Vorschlagsliste zu berücksichtigen. Diesem Antrag wurde durch das Staatsministerium für Unterricht, Kultus, Wissenschaft und Kunst entsprochen.

Die genannten Schriftstücke wurden von der Regierung nicht in den Personalakt der Eingabeführerin aufgenommen, sondern in einem Sachakt zusammengefaßt.

Die Beamtin wurde über die negativen Äußerungen ihres Vorgesetzten nicht informiert.

Bei einer gelegentlichen Einsichtnahme in ihren Personalakt fand die Eingabeführerin dementsprechend keinen Hinweis auf die Schriftstücke.

Nach einer Versetzung nahm die Beamtin beim Leiter der neuen Dienststelle in den bei diesem vorliegenden Personalnebenakt Einsicht und entdeckte das eingangs erwähnte Schreiben.

Im Zuge eines aus anderen dienstrechtlichen Gründen angestrengten Verwaltungsverfahrens wurde vom Verwaltungsgericht der Personalakt der Eingabeführerin angefordert.

Bei Übergabe des Personalakts an das zuständige Verwaltungsgericht war nunmehr eine Kopie des Schreibens dem Akt beigefügt.

Zu Umfang und Inhalt von Personal- und Sachakten habe ich, ohne auf den konkreten Fall Bezug zu nehmen, eine Stellungnahme des hierfür federführenden Staatsministeriums der Finanzen eingeholt.

Das Staatsministerium führt aus, daß bei einer erfolglosen Bewerbung eines Beamten für einen anderen Dienstposten seine Bewerbungsunterlagen zum Personalakt zu nehmen sind, wenn es sich um ein Amt beim gleichen Dienstherrn handelt.

Besetzungsberichte ("Dreiervorschläge") sollen vorwiegend Organisationsentscheidungen vorbereiten. Der prägende Zweck dieser Unterlagen greift nach Darstellung des Ministeriums über die Person und das Dienstverhältnis der jeweiligen Kandidaten hinaus. Vorgänge der genannten Art haben nach Auskunft des Ministeriums deshalb Sachaktencharakter.

Bei dieser Bewertung ist das Staatsministerium allerdings davon ausgegangen, daß der Besetzungsbericht für die einzelnen Bewerber nur eine Zusammenstellung ausgewählter Daten aus dem jeweiligen Personalakt enthält und nicht grundlegend neue Gesichtspunkte in das Bewerbungsverfahren eingeführt werden.

Zulässigerweise geführte Personal-Nebenakten dürfen nur Vorgänge enthalten, die sich bereits im Grundakt oder in Teilakten befinden.

Ich bewerte den geschilderten Sachverhalt wie folgt:

Personalakten sollen ein möglichst vollständiges Bild von der Persönlichkeit eines Beamten geben. Sie sollen ein lükkenloses Bild der Entstehung und Entwicklung eines Dienstverhältnisses als historischen Geschehensablauf vermitteln. Daraus folgt, daß auch eine fehlgeschlagene Bewerbung darin dokumentiert werden muß. Dies jedenfalls, soweit es sich um eine Bewerbung für ein Amt beim gleichen Dienstherrn handelt. Dies ist im vorliegenden Fall nicht geschehen.

Zu den Personalaktendaten zählen auch Beurteilungen und Bewertungen des Beamten durch den Vorgesetzten. Es entspricht allgemeiner Lebenserfahrung, daß solche Einschätzungen vom Betroffenen selbst nicht immer geteilt werden, dies um so weniger, wenn negative Werturteile ge-

troffen werden. Die genannten Einschätzungen beeinflussen den beruflichen Werdegang eines Beamten in wichtiger Weise.

Das Beamtenrecht sieht daher vor, daß der Beamte zu Beschwerden, Behauptungen und Bewertungen, die für ihn ungünstig sind oder ihm nachteilig werden können, vor deren Aufnahme in den Personalakt zu hören ist. Die Äußerung des Beamten ist zum Personalakt zu nehmen (Art. 100 c BayBG).

Eine Verfahrensweise, nach der für das berufliche Fortkommen wichtige Bewertungen eines Beamten nur im Rahmen eines Besetzungsberichtes gemacht werden und damit nur in Sachakten erscheinen, widerspricht dem informationellen Selbstbestimmungsrecht und dem Grundgedanken auf rechtliches Gehör. Der Beamte muß darauf vertrauen können, daß außerhalb seines Personalaktes keine ungünstigen dienstlichen schriftlichen Werturteile über ihn existieren.

Ich trete daher der Auffassung des Bayer. Staatsministeriums der Finanzen bei, wonach ein Besetzungsbericht (im Sachakt) nur Zusammenfassungen und Auszüge aus den jeweiligen Personalakten und keine grundlegenden neuen Gesichtspunkte enthalten darf. Dies entspricht auch dem Verbot der Führung "geheimer" Personalakten.

Für den vorliegenden Fall bedeutet dies, daß das bereits mehrfach erwähnte Schreiben als eine für die Beamtin ungünstige Bewertung nicht ohne Kenntnis der Betroffenen verwendet werden durfte und ebenso wie die später abgelehnte Bewerbung dem Personalakt beizufügen war. Nach Anhörung hätte der Inhalt des Briefes im "Dreiervorschlag" unter Berücksichtigung eventueller Gegenäußerungen der Beamtin bei der Auswahl eines geeigneten Bewerbers allerdings ggf. Verwendung finden können.

Von einer formellen Beanstandung habe ich im vorliegenden Fall deshalb abgesehen, weil das Personalaktenrecht zum Zeitpunkt der beschriebenen Vorgänge nicht in der ab 1.8.1994 durch Art. 100 - 100 h BayBG beschriebenen Ausführlichkeit geregelt war und weil ich vor Inkrafttreten der Novellierung des Bayer. Datenschutzgesetzes zum 1.4.1994 für die Kontrolle datenschutzrechtlicher Probleme in Akten nicht zuständig war.

12.6 Herausgabe personenbezogener Daten an das Kreisrevisionsamt

Bereits in meinem fünfzehnten Tätigkeitsbericht habe ich zur regelmäßigen Herausgabe von Lohnkonten an das Kreisrevisionsamt Stellung genommen.

Ich wurde in diesem Zusammenhang gefragt, ob sich durch die Novellierung des Bayer. Datenschutzgesetzes eine Änderung meiner rechtlichen Beurteilung ergeben hätte.

Durch Art. 17 Abs. 1 Nr. 2 des Bayer. Datenschutzgesetzes (BayDSG) i.d.F. vom 23. Juli 1993 wurde der Zweckbindungsgrundsatz ausdrücklich in den Gesetzestext aufgenommen. Danach ist die Speicherung, Veränderung und Nutzung von Daten nur zulässig für den Zweck, für den sie erhoben worden sind.

Die Absätze 2 und 3 der genannten Bestimmung führen jene Sachverhalte auf, die Voraussetzungen für eine zulässige Zweckänderung sind. Ferner wird festgelegt, daß die Wahrnehmung von Aufsichts- und Kontrollbefugnissen und die Rechnungsprüfung nicht als Zweckänderung gilt.

Art. 17 Abs. 3 BayDSG legt also eine Zweckidentität zwischen den dort aufgeführten Verarbeitungs- und Nutzungszwecken und den Zwecken fest, zu denen die Daten ursprünglich erhoben worden sind. Diese Fiktion bzw. Klarstellung wurde deshalb erforderlich, weil auch für den Bereich des Nutzens, also bspw. der Verwendung von Daten innerhalb einer speichernden Stelle (etwa zwischen zwei Sachgebieten eines Landratsamtes) der Zweckbindungsgrundsatz gilt.

Neben der Beachtung der Zweckbindung ist weitere Voraussetzung für ein zulässiges Speichern, Verändern und Nutzen von personenbezogenen Daten, daß dies zur Erfüllung der in der Zuständigkeit der speichernden Stelle liegenden Aufgaben erforderlich ist (Art. 17 Abs. 1 Nr. 1 BayDSG). Auch eine Nutzung innerhalb der speichernden Stelle muß sich am Grundsatz der Erforderlichkeit und damit auch der Angemessenheit orientieren.

Ich habe in meinem 15. Tätigkeitsbericht unter Nr. 11.10 die Auffassung vertreten, daß eine regelmäßige Übergabe sämtlicher Lohnkonten des jeweils abgelaufenen Kalendermonats an ein Kreisrevisionsamt für eine ordnungsgemäße und ausreichende Rechnungsprüfung nicht erfor-

derlich ist.

Die Neufassung des Bayer. Datenschutzgesetzes erfordert keine Änderung dieser Auffassung.

Die Neufassung hat auch hinsichtlich der Stellung der Rechnungsprüfungsbehörden keine Änderung gebracht. Deren Rechte bestimmen sich ausschließlich nach dem jeweiligen Spezialgesetz. Die Aufgabe des Kreisrevisionsamtes, eine umfassende Prüfung durchzuführen, wird durch meine Auffassung zur Herausgabe von Unterlagen nicht eingeschränkt, da es dem Kreisrevisionsamt unbenommen ist, stichprobenartig sämtliche Lohnkonten eines oder mehrerer Monate zu überprüfen.

Zur Frage, wo Rechnungsprüfungen stattzufinden haben, trifft das Datenschutzgesetz keine Aussage. In vielen Fällen dürfte einer Prüfung vor Ort, d.h. in den Räumen der geprüften Stelle, der Vorzug zu geben sein. Es sind aber auch durchaus Sachverhalte denkbar, in denen der Rechnungsprüfer Unterlagen in den Räumen der Rechnungsprüfungsstelle sichten und bearbeiten will, bspw. um die Möglichkeiten einer hier vorhandenen EDV-Ausstattung zu nutzen. Soweit die Rechnungsprüfungsstelle durch geeignete technische und organisatorische Maßnahmen den Schutz der ihr für Zwecke der Prüfung in den eigenen Räumen übergebenen Prüfungsunterlagen gewährleisten kann, erhebe ich dagegen keine Einwendungen. Ich gehe dabei davon aus, daß beim Sichten und Prüfen der Unterlagen nur für die Begründung von Prüfungsfeststellungen erforderliche Auszüge gefertigt werden.

13. Gewerbe und Handwerk

13.1 Änderung der Gewerbeordnung

13.1.1 Gruppenauskünfte aus den Gewerbeanzeigen

Bis zum Inkrafttreten des neugefaßten § 14 GewO am 01.12.95 (vgl. Gesetz zur Änderung der Gewerbeordnung und sonstiger gewerberechtlicher Vorschriften vom 23. November 1994, BGBl I S. 3475 ff) konnten die Gewerbebehörden Gruppenauskünfte, also Auskünfte über eine Vielzahl namentlich nicht genannten Gewerbetreibenden, für **Zwecke der Werbung oder Meinungsforschung** nur erteilen, falls die betroffenen Gewerbetreibenden ausdrücklich zugestimmt hatten. Eine Zustimmungserklärung war entweder auf dem Anzeigenvordruck oder einem Beiblatt vorzusehen.

Nach dem jetzt geltenden § 14 Abs. 4 GewO sind für die Gewerbeanzeigen Vordrucke nach den Mustern der Anlagen 1 bis 3 zu verwenden. Diese Muster sehen **keine** Felder mehr für die Zustimmung zu einer Datenübermittlung an Dritte zum Zwecke der Werbung oder Meinungsforschung (z. B. Adreßbuchverlage, Versicherungen, Marktforschungsinstitute) vor.

Derartige Auskünfte richten sich nach der neuen Rechtslage nach § 14 Abs. 8 GewO. Die drei Grunddaten (Name, betriebliche Anschrift, angezeigte Tätigkeit) dürfen bei Vorliegen eines berechtigten Interesses sowohl fallweise als auch regelmäßig in Form einer Gruppenauskunft, z. B. an Berufsverbände, Markt- und Meinungsforschungsinstitute, Versicherungen, Adreßbuchverlage usw. gegeben werden. Gruppenauskünfte über die drei Grunddaten zum Zwecke der Werbung und der Meinungsforschung sind demnach auch ohne die ausdrückliche Zustimmung der Betroffen zulässig.

In diesem Zusammenhang ist darauf hinzuweisen, daß ein Rechtsanspruch auf Auskünfte aus den Gewerbeanzeigen nicht besteht. Die Gewerbeanzeigen bilden kein öffentliches Register. Die Entscheidung über Auskunftsersuchen steht im **pflichtgemäßen Ermessen** der Gewerbebehörden.

13.1.2 Datenübermittlungen aus den Gewerbeanzeigen und über Gewerbeuntersagungsverfahren

Die Übermittlung von Daten zu einem **abgeschlossenen Gewerbeuntersagungsverfahren** richtet sich nach § 11 Abs. 5 Gewerbeordnung (GewO). Danach kann z. B. an nichtöffentliche Stellen eine Datenübermittlung nur noch vorgenommen werden, soweit die Kenntnis der zu übermittelnden Daten zur Verfolgung von Straftaten erforderlich ist oder eine besondere Rechtsvorschrift dies vorsieht.

Auskünfte über ein Gewerbeuntersagungsverfahren an private Dritte, beispielsweise Gläubiger, zur Verfolgung privatrechtlicher Ansprüche sind daher **unzulässig**.

§ 11 Abs. 5 und § 14 Abs. 5 ff. GewO enthalten getrennte Übermittlungsvorschriften. Eine auskunftssuchende Privatperson kann daher unter den Voraussetzungen des § 14 Abs. 8 GewO **Auskunft aus den Gewerbeanzeigen** darüber erhalten, daß ein Gewerbe abgemeldet wurde. Wurde also gegen einen Gewerbetreibenden eine rechtskräftige Untersagung ausgesprochen und kommt dieser seinen Rechtspflichten daraus nach, indem er das Gewerbe abmeldet, kann gem. § 14 Abs. 8 GewO an nichtöffentliche Stellen Auskunft **über die Abmeldung** erteilt werden.

Dies führt zu dem unbefriedigenden Ergebnis, daß derjenige, der einer bestands- bzw. rechtskräftigen Gewerbeuntersagung zuwiderhandelt und sein Gewerbe nicht abmeldet, ein ordnungsgemäß angemeldetes Gewerbe vortäuschen kann. Eine Auskunft an private Gläubiger zur Verfolgung von privatrechtlichen Ansprüchen über die Gewerbeuntersagung ist - wie oben ausgeführt - nicht zulässig, über eine Gewerbeabmeldung - mangels Anzeige - nicht möglich. Die Gewerberechtsreferenten von Bund und Ländern diskutieren derzeit eine Ergänzung des § 14 Abs. 1 Satz 2 Nr. 3 GewO. Demnach soll in der Gewerbeordnung festgelegt werden, daß für den Fall der eindeutigen Aufgabe eines Betriebs und gleichzeitiger Nichtabmeldung innerhalb eines angemessenen Zeitraums die Behörde eine Abmeldung auch von Amts wegen vornehmen kann.

13.2 Neufassung der Bewachungsverordnung

Zum 01. April 1996 trat die neugefaßte Bewachungsverordnung (BewachV vom 07. Dezember 1995, BGBl I S. 1602 ff) in Kraft. Darin hat das Bundesministerium für Wirtschaft auf der Grundlage des § 34 a Abs. 2 Gewerbeordnung Anforderungen an den Unterrichtungsnachweis festgelegt und Vorschriften über die Pflichten des Gewerbetreibenden bei der Einstellung und Entlassung der im Bewachungsgewerbe beschäftigten Personen, über die Aufzeichnung von Daten dieser Personen und ihre Übermittlung an die Gewerbebehörde erlassen.

Personen, die das Bewachungsgewerbe selbständig ausüben wollen, gesetzliche Vertreter von juristischen Personen, soweit sie mit der Durchführung von Bewachungsaufgaben direkt befaßt sind und Personen, die mit der Leitung eines Bewachungsunternehmens beauftragt sind, müssen mindestens 40 Unterrichtsstunden mit den für die Ausübung des Gewerbes notwendigen rechtlichen Vorschriften und spezifischen Pflichten und Befugnissen sowie deren praktischer Anwendung in einem Umfang vertraut gemacht werden, der ihnen die eigenverantwortliche Wahrnehmung von Bewachungsaufgaben ermöglicht (§§ 1, 3 BewachV). Zu den Sachgebieten der **Unterrichtung** (vgl. Anlage 2 der BewachV) gehören auch die Pflichten der Unternehmer nach dem **Bundesdatenschutzgesetz**.

Nach § 9 BewachV hat der Gewerbetreibende die **Wachpersonen, die er beschäftigen will, der zuständigen Behörde** durch Übersendung je einer Kopie eines **Führungszeugnisses** und in der Regel der Kopie des Unterrichtungsnachweises **vorher zu melden.** Das Führungszeugnis darf nicht älter als drei Monate sein. Diese Regelung entspricht der in Bayern bisher schon praktizierten Verfahrensweise aus Nr. 3.4.1 der allgemeinen Verwaltungsvorschrift zu § 34 a der Gewerbeordnung und der Bewachungsverordnung (BewachVwV, Bek. des Bayer. Staatsministeriums für Wirtschaft und Verkehr vom 31. August 1992, AllMBl S. 849, geändert durch Bek. vom 11. Februar 1993, AllMBl S. 513). Der Gewerbetreibende hat nach § 9 BewachV außerdem für jedes Kalenderjahr Namen und Vornamen der **Personen** unter Angabe des Beschäftigungsbeginns bis zum 31. März des darauffolgenden Jahres **zu melden**, die aus dem Unternehmen **ausgeschieden** sind. Die zuständige Gewerbebehörde muß dann die bei ihr vorhanden Unterlagen (Kopie des Führungszeugnisses usw.), zu den ausgeschiedenen Personen vernichten bzw. die gespeicherten Daten löschen, soweit diese nicht mehr zur Aufgabenerfüllung benötigt werden.

Überflüssige Datenspeicherungen zu Personen, die schon lange nicht mehr für das Bewachungsunternehmen tätig sind, werden so vermieden.

Durch Art. 5 des Gesetzes zur Änderung der Gewerbeordnung und sonstiger gewerberechtlicher Vorschriften vom 23. November 1994 (BGBl I S. 3475 ff) wurde § 41 Abs. 1 Nr. 9 des Bundeszentralregistergesetzes geändert, so daß es für die Gewerbebehörde seit dem 01. Februar 1995 im übrigen möglich ist, für die Erteilung von Erlaubnissen für das Bewachungsgewerbe und die Überprüfung des Bewachungspersonals eine **unbeschränkte Auskunft aus dem Bundeszentralregister einzuholen**.

13.3 Übermittlung von Gesellenprüfungsnoten durch die Handwerkskammer

Im Berichtszeitraum war ich mit der Frage befaßt, ob die Handwerkskammer dem Ausbildungsbetrieb eines Lehrlings, dem Landesinnungsverband und den Innungen die **Prüfungsnoten der bestandenen Gesellenprüfung** mitteilen darf.

Bei den Prüfungsergebnissen handelt es sich um personenbezogene Daten im Sinne von Art. 4 Abs. 1 BayDSG. Die Verarbeitung personenbezogener Daten, zu der auch die Übermittlung gehört, ist nach Art. 15 BayDSG nur zulässig, wenn der Betroffene eingewilligt hat oder wenn das Bayerische Datenschutzgesetz oder eine andere Rechtsvorschrift sie erlaubt oder angeordnet hat.

Eine bereichsspezifische gesetzliche Regelung, z.B. in der Handwerksordnung, über die Weitergabe der Prüfungsergebnisse durch den Gesellenprüfungsausschuß bzw. die Handwerkskammer an die Landesinnungsverbände oder an die Lehrherren besteht nicht.

Die Zulässigkeit der Datenübermittlung an die Landesinnungsverbände und die Lehrherren, beides nicht-öffentliche Stellen im Sinne des Bayerischen Datenschutzgesetzes, richtet sich daher nach Art. 19 BayDSG. Danach können personenbezogene Daten an nicht-öffentliche Stellen übermittelt werden, wenn die nicht-öffentliche Stelle ein berechtigtes Interesse an der Kenntnis der zu übermittelnden Daten glaubhaft darlegt und der Betroffene kein schutzwürdiges Interesse an dem Ausschluß der Übermittlung hat (Art. 19 Abs. 1 Nr. 2 BayDSG).

1. Für die Weitergabe der Prüfungsergebnisse an die **Landesinnungsverbände** kann ein berechtigtes Interesse nicht anerkannt werden. Allein der Wunsch, gute Prüflinge auszuzeichnen und mit guten Prüfungsergebnissen für den Beruf zu werben, kann die Annahme eines berechtigten Interesses nicht rechtfertigen. Die Werbung für den Beruf kann im übrigen, wenn sicherlich auch eingeschränkt, mit den übermittelten Prüfungsergebnissen in anonymisierter Form erfolgen.

2. Der **Lehrherr** hat insbesondere zur Erfolgskontrolle der Ausbildung grundsätzlich ein berechtigtes Interesse an der Übermittlung der Prüfungsergebnisse, das im jeweiligen Einzelfall mit dem schutzwürdigen Interesse des Prüflings am Ausschluß der Übermitt-

lung abgewogen werden muß. Dabei wird das Interesse des Prüflings an der Geheimhaltung seiner Prüfungsergebnisse, bei denen es sich um sensible Daten handelt, im Regelfall das Interesse des Lehrherrn an einer Erfolgskontrolle der zwischenzeitlich abgeschlossenen Ausbildung übersteigen.

Das berechtigte Interesse des Lehrherren überwiegt jedoch in einzelnen Fällen, wenn der Lehrling die Abschlußprüfung **nicht bestanden** hat, sich das Berufsausbildungsverhältnis auf Verlangen gemäß § 14 Abs. 3 Berufsbildungsgesetz (BBiG) verlängert, der Lehrherr die Prüfungsergebnisse für die weitere Ausbildung benötigt und der betroffene Lehrling die Ergebnisse nicht selbst zur Verfügung stellt.

Ein überwiegend berechtigtes Interesse des Lehrherren an der Weitergabe der Prüfungsergebnisse kann auch für den Fall der Begründung eines Arbeitsverhältnisses auf unbestimmte Zeit durch die Weiterbeschäftigung nach Beendigung des Ausbildungsverhältnisses bestehen (§ 17 BBiG). Da die Rechtsfolge beim Bestehen der Prüfung allein durch die Mitteilung des Bestehens **und** die Weiterbeschäftigung eintritt, kann für den Arbeitgeber ein Bedürfnis bestehen, das Prüfungsergebnis zu erfahren, da die konkrete Ausgestaltung des Arbeitsverhältnisses hiervon wesentlich abhängig sein kann. Eine Übermittlung der Prüfungsergebnisse wird hier aber nur in Frage kommen, wenn der Arbeitgeber nicht auf andere Weise Auskunft erlangen kann. Im Regelfall dürfte es wohl möglich sein, die Weiterbeschäftigung von der Vorlage des Prüfungszeugnisses abhängig zu machen.

Eine generelle Übermittlung der Prüfungsergebnisse an alle Lehrherren scheidet daher aus, da - wie oben dargestellt - eine Abwägung der Interessen im Einzelfall erforderlich ist.

3. Eine generelle Weitergabe der Prüfungsergebnisse an die **Innungen** als Körperschaften des öffentlichen Rechts ist ebenfalls nicht zulässig. § 5 a Abs. 2 der Handwerksordnung enthält hierfür keine ausreichende Ermächtigungsgrundlage, soweit die Innungen nicht im konkreten Einzelfall mit der Ausbildung von Lehrlingen befaßt sind und deshalb die Prüfungsergebnisse zur Erfüllung eines gesetzlichen Auftrags benötigen. Der allgemeine gesetzliche Auftrag der Innungen, die Ausbildung der Lehrlinge zu fördern, erfordert nicht die Kenntnis der einzelnen Prüfungsergebnisse.

Von der Mitteilung über die Prüfungsnoten der bestandenen Gesellenprüfung sind z.B. Übermittlungen von **Beurteilungsdaten aus einer überbetrieblichen Ausbildung** an den Ausbildungsbetrieb zu unterscheiden. Die überbetriebliche Ausbildung, also die Berufsausbildung in geeigneten Einrichtungen außerhalb der Ausbildungsstätte, findet **während der Ausbildungszeit** statt und ist ein Bestandteil der betrieblichen Ausbildung. Der Ausbildende im Sinne von § 3 Abs. 1 BBiG ist Gesamtverantwortlicher für die Ausbildung. Er hat gemäß § 6 Abs. 1 Nr. 1 BBiG dafür zu sorgen, daß dem Auszubildenden die Fertigkeiten und Kenntnisse vermittelt werden, die zum Erreichen des Ausbildungsziels erforderlich sind, und die Berufsausbildung in einer durch ihren Zweck gebotenen Form planmäßig, zeitlich und sachlich gegliedert so durchzuführen, daß das Ausbildungsziel in der vorgesehenen Ausbildungszeit erreicht werden kann. Eine derartige Gesamtverantwortung kann der Ausbildende aber nur erfolgreich wahrnehmen, wenn er über den Werdegang des Auszubildenden und den Stand der Ausbildung, also bei einer überbetrieblichen Maßnahme auch über deren individuellen Verlauf und das Ergebnis der Maßnahme, unterrichtet ist.

14. Statistik

14.1 Mikrozensusgesetz

Die Neufassung des Mikrozensusgesetzes ab 1996 wurde vom Gesetzgeber am 17.1.1996 beschlossen.

Der Fragenkatalog wurde gegenüber manchem Vorentwurf - nicht zuletzt aufgrund von Einwendungen der Datenschutzbeauftragten des Bundes und der Länder - erheblich reduziert. Er entspricht im wesentlichen jenem des bisherigen Mikrozensus.

Das Mikrozensusgesetz 1996 belegt, wie auch die bisherigen Befragungen, verschiedene Fragen mit einer Auskunftspflicht, andere stellt sie von der Pflicht zur Beantwortung frei.

Die Kennzeichnung von Pflicht- und freiwilligen Fragen war in den bisherigen Erhebungsvordrucken wenig auffällig.

Ich habe deshalb angeregt, zu prüfen, ob die Fragenkategorien mittels getrennter Erhebungsbögen abgefragt werden können bzw. die freiwilligen Fragen optisch stärker herausgestellt werden können.

Gegen eine Trennung wurden von Seiten der Fachbehörden gute Argumente vorgebracht. Es wurde insbesondere darauf hingewiesen, daß dies eine höhere Belastung des Bürgers mit sich bringe, da er sich mit bereits abgeschlossenen Themenbereichen erneut beschäftigten müsse.

Das von einer Arbeitsgruppe des Statistischen Bundesamtes neugestaltete Muster für den Erhebungsbogen für die Mikrozensuserhebungen ab 1996 enthält dafür einen wesentlich deutlicheren Hinweis auf die Freiwilligkeit bestimmter Fragen.

Dies wird dadurch sichergestellt, daß am linken Rand der betreffenden Fragen die Kennzeichnung durch das Wort freiwillig erfolgt, die Kennzeichnung in einer anderen Farbe als der ansonsten im Erhebungsbogen benutzten Farbe unterlegt wird und bei allen Fragen mit freiwilliger Auskunftserteilung eine eigene Antwortkategorie "keine Angabe" aufgenommen wurde.

Ich habe mich mit diesem Verfahren einverstanden erklärt.

In der Zusatzerhebung nach § 4 Abs. 5 Nr. 2 Mikrozensusgesetz wird ab 1999 in vierjährigem Turnus u.a. nach der Dauer von Krankheiten, Krankheitsrisiken, Behinderteneigenschaft usw. auf freiwilliger Basis gefragt. Nachdem diese Fragen den Kernbereich des Persönlichkeitsrechts tangieren, aber einen in sich abgeschlossenen Themenbereich darstellen, sollte dieser Komplex auf einem getrennten Erhebungsbogen abgefragt werden.

Das Gesetz enthält in § 11 Abs. 2 eine Regelung zur Nutzung der Bautätigkeitsstatistik für Zwecke der Ermittlung von Auswahlbezirken. Ich habe eine vergleichbare Nutzung im Zusammenhang mit einer datenschutzrechtlichen Kontrolle der Gebäude- und Wohnungstichprobe 1993 in meinem 16. Tätigkeitsbericht angesprochen und darauf hingewiesen, daß weder das 2. Gesetz über die Durchführung von Statistiken der Bautätigkeit und die Fortschreibung des Gebäudestandes noch das Gesetz über gebäude- und wohnungsstatistische Erhebungen eine derartige Nutzung vorsehen. Die normenklare Regelung ist deshalb zu begrüßen.

Das Gesetz bringt weiterhin eine Änderung des Bundesstatistikgesetzes (BStatG) insoweit mit sich, als computergestützte Erhebungsverfahren bei Bundesstatistiken ausdrücklich zugelassen werden. Daneben können die Antworten auch schriftlich erteilt werden, soweit in einer besonderen Regelung in einer eine Bundesstatistik anordnenden Rechtsvorschrift nicht anderes bestimmt ist.

§ 15 Abs. 4 und Abs. 5 BStatG schreibt vor, daß beim Einsatz von Erhebungsbeauftragten die in den Erhebungsvordrucken enthaltenen Fragen auch schriftlich beantwortet werden können und in diesem Fall die ausgefüllten Vordrucke u.a. in verschlossenem Umschlag der Erhebungsstelle direkt übersandt werden können. Weiterhin bestimmt § 17 BStatG, daß die zu Befragenden schriftlich u.a. über Zweck, Art und Umfang der Erhebung, die Auskunftspflicht oder die Freiwilligkeit der Erhebung und die Rechte und Pflichten der Erhebungsbeauftragten zu unterrichten sind.

Ich gehe davon aus, daß aufgrund der genannten Bestimmungen der Verfahrensablauf einer Befragung durch einen Interviewer unter Verwendung eines Laptops nicht anders ist, als bei den

bisherigen Verfahren.

Bedenken hätte ich allerdings bei ausschließlichen Datenerhebungen aufgrund computergestützter fernmündlicher Befragungen. Ich weise insbesondere auf die letztendlich nicht zuverlässige Identifizierung sowohl des Anrufers als auch des Angerufenen hin.

14.2 Nutzung von Daten der Landwirtschaftsverwaltung für statistische Zwecke

Das Bayer. Landesamt für Statistik und Datenverarbeitung hat mich um Äußerung zu einer geplanten Datenübernahme von Daten der Landwirtschaftsverwaltung für statistische Zwecke gebeten.

Dem liegt folgender Sachverhalt zugrunde:

Mit der Verordnung (EWG) Nr. 3508/92 des Rates vom 27.11.1992 wurde ein integriertes Verwaltungs- und Kontrollsystem für bestimmte gemeinschaftliche Beihilferegelungen geschaffen (InVekoS). Die dazu erlassenen Durchführungsbestimmungen sehen auch die Möglichkeit vor, die im Rahmen des integrierten Systems erhobenen Daten für statistische Zwecke zu verwenden.

Die in InVekoS erhobenen Daten umfassen auch Angaben zur Flächennutzung der land- und forstwirtschaftlichen Betriebe sowie zur Tierhaltung (Mehrfachantrag). Das Agrarstatistikgesetz schreibt ebenfalls die Erhebung von Flächennutzungs- und Tierbestandsdaten im Rahmen der Bodennutzungserhebungen sowie der Viehzählungen vor.

Zur Vermeidung von Doppelbefragungen der Betroffenen und zur Reduzierung des Erhebungsaufwands bei den Gemeinden - diese sind aufgrund der Verordnung zur Durchführung des Agrarstatistikgesetzes mit der Erhebung beauftragt - strebt das Landesamt eine Datenübernahme der bereits vorliegenden Datenbestände bei der Landwirtschaftsverwaltung an.

Ich habe die Auffassung vertreten, daß die in der genannten Verordnung (EWG) enthaltene Bestimmung zur statistischen Nutzung von InVekoS-Daten allein nicht ausreicht, das vom Landesamt angestrebte Verfahren zu ermöglichen. Ich habe vielmehr eine Einwilligungslösung gefordert. Der nach dem Agrarstatistikgesetz Auskunftspflichtige muß dabei seine Einwilligung jährlich (für das Folgejahr im Mehrfachantrag der Landwirtschaftsverwaltung) freiwillig abgeben können, ohne daß ihm bei einer Weigerung ein Nachteil entstehen darf. Er muß weiterhin im üblichen Rahmen und Ausmaß über das Verfahren der Datenübernahme und den Verwendungszweck aufgeklärt werden. Soweit ausschließlich für die Statistik benötigte Merkmale erhoben werden, sollen diese nicht im Mehrfachantrag abgefragt werden. Diese Daten sind vielmehr so

zu erheben, daß die Landwirtschaftsverwaltung davon nicht Kenntnis erhält. Dies kann beispielsweise durch einen gesonderten Vordruck geschehen, der zwar zusammen mit den Formularen für den Mehrfachantrag an den Betriebsinhaber verschickt wird, dessen Rücklauf aber direkt an das Landesamt bzw. im verschlossenen Kuvert über das Amt für Landwirtschaft an das Landesamt erfolgt.

Das Landesamt hat diesen Verfahrensgrundsätzen zugestimmt.

15. Schulwesen

15.1 Datenschutz an Schulen

Das Staatsministerium für Unterricht, Kultus, Wissenschaft und Kunst hatte bereits in der Vergangenheit zum Vollzug des Bayerischen Datenschutzgesetzes an Schulen umfangreiche "Erläuternde Hinweise" in Form einer Bekanntmachung herausgegeben.

Aufgrund der Novellierung des Bayerischen Datenschutzgesetzes hat das Staatsministerium die "Hinweise" neu gefaßt und mit Datum vom 19.03.1996 im Amtsblatt des Staatsministeriums bekanntgemacht.

Ich wurde an dem Verfahren beteiligt und konnte Änderungswünsche einbringen.

Die Neufassung war für mich Anlaß, meine bisherige Rechtsauffassung zur Frage der Anwendbarkeit des Bayerischen Datenschutzgesetzes und des Bundesdatenschutzgesetzes bzw. kirchlicher Vorschriften über den Datenschutz auf privatrechtlich-organisierte Schulen in kirchlicher Trägerschaft zu überdenken.

Ich war bisher mit dem Staatsministerium für Unterricht und Kultus, Wissenschaft und Kunst davon ausgegangen, daß für die genannten Schulen stets kirchliches Datenschutzrecht anzuwenden sei.

Ich bin zu dem Ergebnis gekommen, daß für privatrechtlich organisierte kirchliche Schulen als staatlich anerkannte Ersatzschulen für den Umgang mit personenbezogenen Daten der Schüler und Erziehungsberechtigten das Bayerische Datenschutzgesetz anzuwenden ist. Die verfassungsrechtlich gesicherte Autonomie des Trägers, die gewährleistet, daß die eigenen Angelegenheiten innerhalb der Schranken der für alle geltenden Gesetze selbständig geordnet und verwaltet werden können, endet meines Erachtens dort, wo eine öffentlich-rechtliche Religionsgesellschaft eine ihr vom Staat durch Gesetz übertragene hoheitliche Aufgabe wahrnimmt und damit ein Über-/Unterordnungsverhältnis zwischen Bürger und Staat entsteht. Bei staatlich anerkannten Ersatzschulen nach Art. 100 BayEUG und noch deutlicher bei Ersatzschulen mit dem Charakter öffentlicher Schulen nach Art. 101 BayEUG sind diese Bedingungen erfüllt. Verfügungen bei

der Aufnahme, beim Vorrücken und beim Schulwechsel von Schülern sowie bei der Abhaltung von Prüfungen und Erteilung von Zeugnissen sind Verwaltungsakte. Bei der Wahrnehmung solcher hoheitlicher Aufgaben als Beliehener gegenüber Schülern und Erziehungsberechtigten - aber auch nur insoweit - sind in Bayern die öffentlich-rechtlichen Religionsgesellschaften öffentliche Stellen i.S. des Bayerischen Datenschutzgesetzes.

Das Staatsministerium für Unterricht, Kultus, Wissenschaft und Kunst hat sich dieser Argumentation angeschlossen. Ziff.3.3. der Neufassung der "Erläuternden Hinweise" gibt insoweit meine geänderte Rechtsauffassung wieder.

15.2 Aushang von Klassenlisten

Im Rahmen einer Eingabe haben sich Eltern an mich gewandt.

Sie haben mitgeteilt, daß bei der Einschulung ihres Kindes Klassenlisten vor dem Haupteingang der Schule ausgehängt waren, die neben dem Namen und Geburtsdatum auch die Religionszugehörigkeit der Schüler enthielten.

Das Aushängen von Klassenlisten ist durchaus sinnvoll, um am ersten Schultag des neuen Schuljahrs die Schüler zu informieren, welcher Klasse sie zugeteilt sind, in welchem Klassenzimmer und bei welchem Klassenleiter sie sich einzufinden haben.

Nicht akzeptabel ist allerdings die Angabe der Religionszugehörigkeit.

Art. 85 Abs. 2 BayEUG erlaubt die Weitergabe von Daten und Unterlagen über Schüler und Erziehungsberechtigte an außerschulische Stellen nur bei Vorliegen eines rechtlichen Anspruchs.

Außerschulische Stellen (Dritte) sind alle Personen oder Stellen außerhalb der speichernden Stelle (Schule), aber auch Erziehungsberechtigte und Mitschüler in anderen Klassen. Bei einem öffentlichen Aushang von Klassenlisten an Tafeln im Schulhof oder in der Eingangshalle handelt es sich deshalb um eine Datenübermittlung an außerschulische Stellen. Diese Datenübermittlung kann in analoger Anwendung der für Zwecke der Herausgabe von Jahresberichten bestehenden Vorschrift in Art. 85 Abs. 3 BayEUG zulässig sein, wenn der in dieser Vorschrift aufgeführte Datenrahmen nicht überschritten wird.

Das Merkmal Religionszugehörigkeit - dabei kann es sich um ein äußerst sensibles Datum handeln - ist in Art. 85 Abs. 3 BayEUG nicht genannt. Eine Bekanntgabe an Dritte ohne Vorliegen eines rechtlichen Anspruchs ist deshalb nicht zulässig.

Das Merkmal Religionszugehörigkeit kann auch nicht aufgrund der Teilnahme eines Schülers am jeweiligen Religions- bzw. Ethikunterricht als offenkundig angesehen werden. Zum einen ist eine Teilnahme am Ethikunterricht auch bei Zugehörigkeit zu einer der großen Religionsgemein-

schaften möglich. Zum anderen mag die jeweilige Religionszugehörigkeit den Mitschülern in derselben Klasse ggf. bekannt sein, sie ist es sicherlich nicht allen Mitschülern anderer Klassen und deren Erziehungsberechtigten. Diese konnten das Merkmal gleichwohl dem Aushang entnehmen.

Ich habe in der Veröffentlichung des Merkmals Religionszugehörigkeit einen Verstoß gegen die datenschutzrechtliche Vorschrift des Art. 85 BayEUG gesehen und diesen Verstoß gemäß Art. 31 BayDSG wegen seiner grundsätzlichen Bedeutung auch für andere Schulen beanstandet.

Das Staatsministerium für Unterricht, Kultus, Wissenschaft und Kunst wurde entsprechend unterrichtet.

Das Staatsministerium hat zugesagt, die Schulleiter und Schulaufsichtsbeamten anläßlich von Dienstbesprechungen darauf hinzuweisen, daß der öffentliche Aushang von Klassenlisten nur ohne das Merkmal Bekenntniszugehörigkeit erfolgt.

15.3 Erfassung stark verhaltensgestörter Schüler

Ein Landtagsabgeordneter hat mich darüber in Kenntnis gesetzt, daß ein Staatliches Schulamt Erhebungsbögen an Schulleiter von Hauptschulen verteilt hatte, die der namentlichen Erfassung stark verhaltensgestörter Schüler dienen sollten.

Nach der von mir erbetenen Stellungnahme des angesprochenen Schulamts waren in der Vergangenheit mehrere Hauptschulen und auch Elternbeiräte an das Staatliche Schulamt mit der Bitte herangetreten, die sonderpädagogischen Förderungsmaßnahmen für stark verhaltensgestörte Schüler bis hin zu einer Schule zur Erziehungshilfe auszubauen. Die an die Schulleiter der Hauptschulen versandten Erhebungsbogen sollten der Feststellung dienen, ob den verhaltensauffälligen Schülern mit dem vorhandenen pädagogischen Instrumentarium geholfen werden kann.

Ich habe das Schulamt darauf hingewiesen, daß nach Art. 16 Abs. 1 Bayerisches Datenschutzgesetz (BayDSG) das Erheben personenbezogener Daten nur zulässig ist, wenn ihre Kenntnis zur Erfüllung der in der Zuständigkeit der erhebenden Stelle liegenden Aufgabe erforderlich ist. Personenbezogene Daten dürfen bei Dritten (hier: bei den Schulen) nur erhoben werden, wenn die zu erfüllende Verwaltungsaufgabe ihrer Art nach oder im Einzelfall eine solche Erhebung erforderlich macht (Art. 16 Abs. 2 Nr. 2a BayDSG). Da die Meldung stark verhaltensgestörter Schüler nur der Feststellung des Bedarfes für die Errichtung einer Schule zur Erziehungshilfe dienen sollte, habe ich bei einer derartigen planerischen Zielsetzung eine namentliche Bekanntgabe der betroffenen Schüler für nicht erforderlich gehalten. Die namentliche Erfassung war nicht zulässig. Nicht ausgeschlossen ist damit die Meldung von statistischen Einzelmerkmalen zu den Schülern, wenn dadurch ein Personenbezug nicht hergestellt werden kann.

Anders ist der Sachverhalt zu bewerten, wenn der sonderpädagogische Förderungsbedarf der betroffenen Schüler im Einzelfall ermittelt und eine Entscheidung über den weiteren Bildungsgang des Schülers und den Förderort getroffen werden soll. Ein solches Verfahren zur Feststellung des individuellen sonderpädagogischen Förderungsbedarfes ist von den Erziehungsberechtigten, der Schule oder ggf. von anderen zuständigen Diensten aufgrund von Empfehlungen der Kultusministerkonferenz zu beantragen. Danach entscheidet die Schulaufsicht im Einzelfall, ob der betroffene Schüler in der allgemeinen Schule verbleibt oder Unterricht und Förderung in

einer Sonderschule erhält. Mit einem solchen Antrag wird in die Rechte des betroffenen Schülers erheblich eingegriffen. Die Empfehlungen der Kultusministerkonferenz sehen daher die Einbeziehung der Erziehungsberechtigten in das Verfahren und die Beteiligung des schulpsychologischen Dienstes vor.

Das Staatliche Schulamt hat auf meine Bedenken hin mitgeteilt, daß es "vorerst" auf die Erhebung von Schülernamen verzichtet hat. Ich werde die Angelegenheit im Auge behalten und gegebenenfalls eine nicht erforderliche namentliche Erfassung beanstanden.

15.4 Speicherungsdauer von Angaben über Kursteilnehmer an Volkshochschulen

Im Rahmen einer Eingabe hatte ich mich mit der Speicherungsdauer von Angaben über Kursteilnehmer an Volkshochschulen zu befassen.

Der Petent wollte sich bei einer Volkshochschule für einen Kurs einschreiben. Dabei stellte er fest, daß seine persönlichen Angaben (u.a. die Bankverbindung) über einen mehrere Jahre zurückliegenden Kursbesuch von der Volkshochschule noch gespeichert waren.

Ich habe in diesem Zusammenhang eine gutachterliche Stellungnahme des Bayer. Volkshochschulverbands zu Umfang und Dauer der Datenspeicherung eingeholt.

Der Volkshochschulverband führt aus, daß es im Sinne einer guten Teilnehmerbetreuung unerläßlich sei, ein Minimum an Daten des einzelnen Kursteilnehmers zu speichern.

Dies geschehe, um beispielsweise auf weiterführende oder neu ins Programm genommene Kurse aufmerksam zu machen, um im nachhinein Teilnahmebescheinigungen (berufsbildende Kurse) ausstellen zu können und nicht zuletzt, um bei einer erneuten Anmeldung den Anmeldevorgang wesentlich beschleunigen zu können, da die persönlichen Daten nicht erneut eingegeben werden müßten.

Ich habe darauf hingewiesen, daß das Bayer. Datenschutzgesetz u.a. eine Datenspeicherung erlaubt, soweit diese zur Aufgabenerfüllung erforderlich ist. Diese Erforderlichkeit sehe ich für die Merkmale Namen, Anschrift und Art des besuchten Kurses als gegeben an.

Anders verhält es sich mit dem Merkmal Bankverbindung. Die Vorhaltung dieses Datums kann bei einer wiederholten Anmeldung eine Verkürzung des Anmeldevorgangs bewirken, für eine effektive Teilnehmerbetreuung nach erfolgtem Kursbesuch ist es nicht erforderlich.

Ich habe deshalb vorgeschlagen, dem Teilnehmer bei Anmeldung eine Widerspruchsmöglichkeit gegen die Datenvorhaltung einzuräumen und diese aus Praktikabilitätsgründen auch auf die übrigen Teilnehmerdaten auszudehnen. Dies könnte bspw. in Form einer Bemerkung im Kursver-

zeichnis bzw. in den Anmeldeunterlagen mit folgendem Inhalt geschehen:

"Zum Zweck einer effektiven Teilnehmerbetreuung und zur Verkürzung des Anmeldevorgangs bei künftigen Anmeldungen speichert die Volkshochschule für die Dauer von ... Jahren folgende Teilnehmerdaten:

1. Name, Anschrift
2. Bankverbindung
3. .....
4. .....

Eine Speicherung der Bankverbindung entfällt bei Barzahlung bzw. Hingabe eines Schecks.

Wenn Sie es wünschen, kann die Datenspeicherung nach Abschluß des besuchten Kurses beendet werden. Eine nachträgliche Ausstellung von Teilnahmebescheinigungen ist dann allerdings nicht mehr möglich."

Der Volkshochschulverband hat diesem Vorschlag zugestimmt und hat ihn als Empfehlung an seine Mitgliedseinrichtungen weitergeben.

16. Verkehrswesen

16.1 Eignungsgutachten bei Busfahrern über 50 Jahren

Das Bundesverwaltungsgericht hatte darüber zu befinden, welchen Nachweis die Straßenverkehrsbehörden für die geistige und körperliche Eignung von Busfahrern im Alter ab 50 Jahren verlangen dürfen, wenn diese eine Verlängerung ihrer Fahrerlaubnis zur Fahrgastbeförderung beantragen. Nach § 15 f Abs. 1 der Straßenverkehrs-Zulassungs-Ordnung (StVZO) wird die Fahrerlaubnis zur Fahrgastbeförderung für eine Dauer von nicht mehr als drei Jahren erteilt. Nach § 15 f Abs. 2 Nr. 2 StVZO setzt die Verlängerung der Fahrerlaubnis zur Fahrgastbeförderung voraus, daß der Inhaber seine geistige und körperliche Eignung im übrigen nachweist a) durch das Zeugnis bestimmter Ärzte, z.B. eines Arztes mit der Gebietsbezeichnung "Arbeitsmedizin", oder c) auf Verlangen der Behörde durch ein fachärztliches Gutachten oder das Gutachten einer amtlich anerkannten medizinisch-psychologischen Untersuchungsstelle (MPU). Die bayerischen Straßenverkehrsbehörden hatten aufgrund der Eignungsrichtlinien (Richtlinien für die Prüfung der körperlichen und geistigen Eignung von Fahrerlaubnisbewerbern und -inhabern, Bekanntmachung des Bayerischen Staatsministeriums des Innern vom 19. März 1983, MABl S. 213) bei der Verlängerung von Fahrgastfahrerlaubnissen für Kraftomnibusse bei Inhabern ab dem 50. Lebensjahr generell ein medizinisch-psychologisches Gutachten gefordert. Hiergegen wandte sich ein 1941 geborener Busfahrer, der lediglich das Zeugnis eines Arztes mit der Gebietsbezeichnung "Arbeitsmedizin" vorgelegt hat, in dem seine geistige und körperliche Eignung ohne nähere Ausführungen festgestellt wird.

Das Bundesverwaltungsgericht stellte in seinem Urteil vom 17.05.1995 (BVerwG 11 C 2.94) dazu fest, daß es sich zwar im Rahmen vertretbarer Ermessensausübung hält, wenn die Behörde von über 50-jährigen Bewerbern um die Erneuerung der Fahrerlaubnis zur Fahrgastbeförderung als Nachweis ihrer geistigen und körperlichen Eignung nicht nur ein unsubstantiiertes Eignungszeugnis, sondern das Eignungsgutachten eines Facharztes oder einer medizinisch-psychologischen Untersuchungsstelle verlangt. Wird jedoch dieses Gutachten lediglich aus Anlaß des fortgeschrittenen Alters des Antragstellers verlangt, so darf die Behörde keine umfassende medizinisch-psychologische Durchleuchtung und Beurteilung der Gesamtpersönlichkeit verlangen. Das Untersuchungsprogramm ist aus Gründen der Bestimmtheit und Verhältnismäßigkeit **vielmehr anlaßbezogen auf diejenigen verkehrsrelevanten Fähigkeiten zu beschränken,**

die mit zunehmenden Alter abzunehmen pflegen. Außerdem hat das Bundesverwaltungsgericht festgestellt, daß das Verlangen, sich einer Untersuchung durch eine anerkannte medizinisch-psychologische Untersuchungsstelle zu unterziehen dann zu weit geht, wenn damit jedes andere fachärztliche Gutachten - etwa eines Arbeitsmediziners - von vornherein ausgeschlossen wird.

Das Bayerische Staatsministerium des Innern hat den nachgeordneten Behörden die Entscheidung des Bundesverwaltungsgerichts mit Rundschreiben vom 13.07.1995 mitgeteilt und die Eignungsrichtlinien entsprechend überarbeitet (Bekanntmachung vom 13.10.1995, AllMBl 1995, S. 868).

16.2 Vorlage von Gutachten bei der Fahrerlaubnisbehörde

Ein Petent trug vor, daß an Psychose erkrankte Patienten von der Führerscheinstelle aufgefordert werden, zur Wiedererteilung der Fahrerlaubnis ein nervenärztliches Gutachten und danach ein medizinisch-psychologisches Gutachten vorzulegen. Erst nach der Vorlage des nervenärztlichen Gutachtens würde die medizinisch-psychologische Begutachtung eingeleitet. Da in diesen Gutachten medizinische Detailerkenntnisse enthalten seien, bat mich der Petent zu prüfen, ob diese Gutachten der Führerscheinstelle im Wortlaut zur Verfügung gestellt werden müßten oder ob es nicht ausreichend wäre, das nervenärztliche Gutachten nur der Gutachtenstelle für die medizinisch-psychologische Untersuchung vorzulegen, so daß die Führerscheinstelle nur das Gesamtergebnis dieser Gutachterstelle erfahre. Dem Petenten habe ich folgendes mitgeteilt:

Die zuständige Verwaltungsbehörde kann unter bestimmten Voraussetzungen aufgrund der Straßenverkehrs-Zulassungsordnung (StVZO) anordnen, daß der Inhaber einer Erlaubnis zum Führen von Kraftfahrzeugen (§ 15 b StVZO) oder der Bewerber um eine solche Erlaubnis (§ 12 StVZO) je nach den Umständen des Einzelfalles das Gutachten eines Amts- oder eines Facharztes, einer amtlich anerkannten medizinisch-psychologischen Untersuchungsstelle (MPU) oder eines amtlich anerkannten Sachverständigen oder Prüfers für den Kraftfahrzeugverkehr über die körperliche oder geistige Eignung zum Führen von Kraftfahrzeugen beizubringen hat. Untersuchung und Gutachten haben sich auf die Fragen zu beschränken, die zur Aufklärung von Zweifeln an der Eignung des Betroffenen oder zur Feststellung besonderer Eignungsvoraussetzungen beantwortet werden müssen. Die Verwaltungsbehörde hat die Fragestellung entsprechend festzulegen.

Die bei Bedenken gegen die Kraftfahreignung wegen des körperlichen oder geistigen Zustands des Betroffenen im Regelfall erforderlichen Untersuchungen ergeben sich aus Anlage 1 der Eignungsrichtlinien (Richtlinien für die Prüfung der körperlichen und geistigen Eignung von Fahrerlaubnisbewerbern und -inhabern - Eignungsrichtlinien - Bekanntmachung des Bayerischen Staatsministerium des Innern vom 19.03.1983, MABl S. 213, zuletzt geändert durch Bekanntmachung vom 13.10.1995, AllMBl S. 868). Diese Anlage sieht unter Nr. 4.1 bei Geisteskrankheiten (Schizophrenie, zirkuläre Psychosen) und exogenen Psychosen das Gutachten eines Facharztes und das Gutachten einer medizinisch-psychologischen Untersuchungsstelle vor.

Von der Verwaltungsbehörde sind daher bei Psychosen beide Untersuchungen anzuordnen. Die medizinisch-psychologische Untersuchung baut dabei dabei auf dem fachärztlichen Gutachten auf und kann nur entfallen, wenn bereits der Facharzt die Nichteignung zweifelsfrei festgestellt hat und die Verwaltungsbehörde diese Feststellung akzeptiert.

Die Gutachten haben dabei die Funktion eines **Hilfsmittels** für eine eigene Urteilsbildung der Verwaltungsbehörde. Die **Entscheidung trifft die Verwaltungsbehörde** in eigener Verantwortung. Es genügt für diese Entscheidung nicht, daß sich die Verwaltungsbehörde den Gutachten summarisch anschließt, sie muß selbst prüfen, welche einzelnen Eigenschaften der Gutachter festgestellt hat und ob diese Feststellungen der Beurteilung zugrunde gelegt werden können. Nach Art. 39 Abs. 1 Bayer. Verwaltungsverfahrensgesetz ist ein schriftlicher Verwaltungsakt schriftlich zu begründen. In der Begründung sind die wesentlichen tatsächlichen und rechtlichen Gründe mitzuteilen, die die Behörde zu ihrer Entscheidung bewogen haben. In ihrer Begründung muß die Verwaltungsbehörde also erkennen lassen, daß sie das Gutachten den Besonderheiten des Einzelfalls entsprechend verarbeitet hat. Die Verwaltungsbehörde hat ggf. auch darauf hinzuwirken, daß die Gutachten in allgemein verständlicher Sprache abgefaßt sowie nachvollziehbar und nachprüfbar sind.

Die Verwaltungsbehörde muß, um eine eigene Entscheidung treffen zu können, daher die Gutachten kennen. Eine Mitteilung der Ergebnisse an die Verwaltungsbehörde allein reicht hierzu nicht aus. Die Kenntnis der Gutachten ist zur Aufgabenerfüllung der Verwaltungsbehörde erforderlich. Es bestehen daher keine datenschutzrechtlichen Bedenken, die Gutachten an die Verwaltungsbehörde zu übersenden. Voraussetzung ist allerdings, daß die Gutachten nur solche personenbezogenen Angaben und Bewertungen enthalten, die für die Entscheidung der Verwaltungsbehörde erforderlich sind.

17. Medien

17.1 Telekommunikationsgesetz

Der Berichtszeitraum war geprägt von umfassenden gesetzgeberischen Aktivitäten zur Neuordnung der Telekommunikation, insbesondere im Zusammenhang mit der Privatisierung der Deutschen Telekom und der Liberalisierung des Telekommunikationsmarktes.

Die derzeit stattfindende Digitalisierung im Fernmeldewesen schafft für den Benutzer eine Reihe von Vorteilen, sie erzeugt aber auch, insbesondere durch die softwaregesteuerte Vermittlung, zahlreiche Datenspuren, wer wann mit wem wie lange telefoniert hat bzw. in Verbindung gestanden ist. Diese Information über den einzelnen, aus denen sich ein getreuliches Bild seines Telekommunikationsverhaltens ableiten läßt, können die werbende Wirtschaft, den Adressenhandel, den Arbeitgeber, aber auch Staatsorgane oder die Presse interessieren. Zum Schutz der Privatheit ist eine klare und eindeutige Beschränkung der Datenverarbeitung auf das zur Herstellung und Abrechnung der Verbindung Notwendige erforderlich, sowie eine zuverlässige Gewährleistung der Zweckbindung.

Es ist zu begrüßen, daß in dem nunmehr verabschiedeten Telekommunikationsgesetz den Belangen des Datenschutzes weitgehend Rechnung getragen wurde. Im Zuge des Gesetzgebungsverfahrens hatte ich die Gelegenheit, zu verschiedenen Entwurfsfassungen des Gesetzes Stellung zu nehmen. Meine Hinweise galten vorrangig Verbesserungsvorschlägen zum Umfang des Fernmeldegeheimnisses und zur Datenschutzkontrolle.

Das Fernmeldegeheimnis ist inzwischen in die Regulierungsziele des Telekommunikationsgesetzes aufgenommen worden. Mit dieser ausdrücklichen Festlegung als Zielvorgabe für die Regulierung des Fernmeldeverkehrs hat der Gesetzgeber die Bedeutung des Fernmeldegeheimnisses besonders hervorgehoben und damit wenigstens einen gewissen Ausgleich dafür geschaffen, daß Art. 10 GG für die privaten Betreiber von Fernmeldeanlagen, wozu auch die Deutsche Telekom AG gehört, jedenfalls nicht unmittelbar gilt. Das Fernmeldegeheimnis wurde auch auf interne Netze, sogenannte Corporate Networks ausgedehnt; damit wird eine erhebliche Schutzlücke geschlossen.

Auch die Regelungen über die Datenschutzkontrolle wurden verbessert. Im Gegensatz zu früheren Entwürfen wird die Datenschutzkontrolle im Telekommunikationsbereich nicht mehr von der sogenannten Regulierungsbehörde, bei der sich Zielkonflikte mit ihren sonstigen Aufgaben ergeben könnten, sondern vom Bundesbeauftragten für den Datenschutz wahrgenommen. Die Abgrenzung der Kontrollaufgaben zwischen dem Bundesbeauftragten für den Datenschutz und den Landesaufsichtsbehörden für den Datenschutz im nichtöffentlichen Bereich muß allerdings noch geklärt werden.

Ich hatte im Gesetzgebungsverfahren darauf hingewiesen, daß ein Verstoß gegen das Fernmeldegeheimnis nahezu ohne Sanktionen bleibt. Ich habe eine umfassende Strafbewehrung zur Durchsetzung der entsprechenden Verbote für erforderlich gehalten. Diese Vorschläge wurden aber im weiteren Gesetzgebungsverfahren leider nicht berücksichtigt.

Nach einer Ausschußempfehlung des Bundesrates sollten neben Höchstfristen für die aus betrieblichen Gründen erforderliche Datenspeicherung auch Mindestfristen für die Speicherung von Verbindungsdaten im Interesse einer effektiven Strafverfolgung festgelegt werden. Dieser Änderungsvorschlag hätte eine völlig neue Qualität der Vorschrift bewirkt. Der Vorschlag lief auf ein über den eigentlichen Erhebungszweck hinausgehendes Datensammeln auf Vorrat hinaus. Von dieser vorsorglichen Datenspeicherung wäre jeder betroffen gewesen, der Telekommunikationsdienstleistungen in Anspruch nimmt. Damit läge der erste Fall vor, im dem eine mit einer alltäglichen Verhaltensweise verbundene Datenspeicherung für eine eventuelle Nutzung zur Strafverfolgung über das für die Betriebsabwicklung Erforderliche hinaus weiter vorgehalten werden sollte.

Wegen dieser grundsätzlichen Bedeutung haben die Datenschutzbeauftragten von Bund und Ländern einmütig gegen diese Forderung des Bundesrates protestiert. Der Vorschlag wurde in der weiteren Folge nicht mit in das Gesetz aufgenommen.

In meinen Augen stellt das am 1. August 1996 in Kraft getretene Telekommunikationsgesetz einen gelungenen regulatorischen Rahmen zur Gewährleistung des Schutzes personenbezogener Daten in einem sich schnell ändernden technischen Umfeld dar.

17.2 Telekommunikationsunternehmen - Datenschutzverordnung (TDSV)

Nahezu zeitgleich mit der Verabschiedung des Telekommunikationsgesetzes hat die Bundesregierung eine Verordnung über den Datenschutz für Unternehmen, die Telekommunikationsdienstleistungen erbringen (TDSV), erlassen. Die Verordnung regelt den Schutz personenbezogener Daten der am Fernmeldeverkehr Beteiligten. Sie enthält nähere Vorschriften zum Umfang der zulässigen Datenerhebung, -verarbeitung und -nutzung durch die Anbieter von Telekommunikationsleistungen und setzt Fristen für die Löschung von Verbindungsdaten nach erfolgter Abrechnung bzw. von Bestandsdaten nach Beendigung des Vertragsverhältnisses.

Auch hier hatte ich Gelegenheit, zum Entwurf der Verordnung Stellung zu nehmen. Meine Hinweise bezogen sich auf den Geltungsumfang der Verordnung, auf Beschränkungen bei der Auswertung von Verbindungsdaten, auf die Verkürzung der Löschfristen, auf Regelungen über die öffentlichen Kundenverzeichnisse und die Telefonauskunft und auf Regelungskonflikte mit bestehenden Vorschriften über Bildschirmtextdienste sowie Fernwirk- und Fernmeßdienste.

Die nunmehr erlassene Verordnung kommt datenschutzrechtlichen Forderungen weit entgegen. Die Verordnung ist jedoch noch auf die Ermächtigungsgrundlage nach § 10 Abs. 1 des Gesetzes über die Regulierung der Telekommunikation und des Postwesens (PTRegG) gestützt, die durch eine vergleichbare Verordnungsermächtigung im Telekommunikationsgesetz inzwischen überholt ist. Wesentliche Schwäche der alten Verordnungsermächtigung und damit der TDSV ist die fehlende Möglichkeit, die genannten Datenschutzregelungen auf geschlossene Telekommunikationsnetze (Corporate Network) auszudehnen. Das PTRegG bezog sich ausschließlich auf Unternehmen, die der Öffentlichkeit angebotene Telekommunikationsdienstleistungen erbringen.

Wegen der zunehmenden Bedeutung der geschlossenen Telekommunikationsnetze ist der baldige Erlaß einer neuen Verordnung auf der Basis der Ermächtigung in § 89 Telekommunikationsgesetz dringlich.

17.3 Teledienstegesetz und Mediendienste-Staatsvertrag

Die rasch fortschreitende Entwicklung im Bereich der Telekommunikationsdienste, die gerade in Bayern besonders gefördert wird - Bayern-Online -, läßt die Grenzen zwischen Rundfunk und Individualkommunikation, zwischen Information und Unterhaltung, zwischen kultureller Darbietung, journalistischer Aufbereitung und kommerzieller Nutzung verschwimmen. Genau diese Merkmale waren aber bisher entscheidend für die datenschutzrechtliche Einordnung der vorhandenen Medienangebote.

Kennzeichnend für die neuen multimedialen Dienste ist die Möglichkeit der digitalisierten Übertragung von Daten, Sprache und Tönen, sowie bewegten und unbewegten Bildern bei gleichzeitiger Verwendung eines Rückkanals, der eine interaktive Steuerung des Geschehens erlaubt. Begriffe wie Internet, Elektronic-Mailing, Voice-Mailbox, News-Groups, OnlineKonferenzen, Telebanking, elektronische Buchungssysteme, Telearbeit, Telemedizin, Teleunterricht, Fernmeß- und Fernwirkdienste, Fernseheinkauf, Videotext, Video on demand sowie Abrufdienste für Presseveröffentlichungen und Informationen aller Art prägen die Diskussion.

Durch die multimediale Nutzung der Telekommunikationsnetze werden in erheblichen Umfang personenbezogene Daten anfallen. Für den Aufbau der Verbindungen, die Auswahl und die Abrechnung der Leistungen werden personenbezogene Daten über die Teilnehmer erhoben und verarbeitet. Sie werden zur Abrechnung der Entgelte gespeichert und könnten auch anderweitig genutzt werden. Die Anbieter solcher Leistungen sind technisch in der Lage, über den einzelnen Teilnehmer umfassende Erkenntnisse bezüglich seines Umgangs mit Geld, seiner Unterhaltungsinteressen, seines Weiterbildungsverhaltens, seiner Kaufinteressen und seines Geschicks mit dem Umgang mit Kommunikationstechnologien zu gewinnen. Die Persönlichkeitsphäre des einzelnen könnte damit im hohen Maße gefährdet werden.

Auf dem Weg in die neue Informationsgesellschaft existieren Datenschutzvorschriften bislang in Gestalt der Telekom-Datenschutzverordnung, im Rahmen des Btx-Staatsvertrages, der Landesmediengesetze, des Rundfunkstaatsvertrages und der allgemeinen Bestimmungen im Bundesdatenschutzgesetz (BDSG). Nunmehr sind übergreifende Datenschutzregelungen erforderlich, die den neuen Datenverarbeitungsqualitäten und den mit ihnen verbundenen Mißbrauchsmöglich-

keiten gerecht werden. Diese Datenschutzvorschriften müssen vor allem folgende Rechte gewährleisten:

Die Bürger sollen die Möglichkeit haben, die MultimediaDienste weitestgehend unter Wahrung der Anonymität zu nutzen. Soweit personenbezogene Verbindungs- und Abrechnungsdaten unvermeidbar sind, sollen sie nur im unbedingt notwendigen Umfang verarbeitet und nur für die unbedingt erforderliche Zeit gespeichert werden. Eine Löschung ist unverzüglich vorzunehmen, sobald die Informationen zur Abwicklung des Vertrages und die eventuelle Erfüllung von Gewährleistungsansprüchen nicht mehr erforderlich sind. In keinem Fall dürfen Mediennutzungsprofile erstellt werden darüber, wer wann wie lange und wie oft welche Dienste in Anspruch genommen hat. Die Nutzung von Angeboten darf nicht von der Einwilligung in hierfür nicht erforderliche Datenverarbeitung abhängig gemacht werden. Jederzeitiger Zugriff der Betroffenen auf Nutzungsbedingungen auch in schriftlicher Form muß möglich sein. Eine effektive und nicht anlaßgebundene Datenschutzaufsicht ist zu gewährleisten. Schließlich ist auch ein angemessenes Datenschutzniveau bei ausländischen Anbietern anzustreben. Dazu ist eine Fortentwicklung in der europäischen und internationalen Rechtsordnung notwendig.

Sowohl die Bundesregierung als auch die Landesregierungen sind in Erkenntnis der Dringlichkeit des Regulierungsbedarfes nicht untätig geblieben. Zum gegenwärtigen Zeitpunkt liegt sowohl der Entwurf eines Teledienste-Gesetzes des Bundes als auch der Entwurf eines Mediendienste-Staatsvertrages der Länder vor. Beide Entwürfe versuchen, den beschriebenen datenschutzrechtlichen Anforderungen gerecht zu werden.

Leider konnte bisher bezüglich der Gesetzgebungszuständigkeit Einigkeit zwischen dem Bund und den Ländern nicht erreicht werden. Ich möchte mich aus der Sicht des Datenschutzes nicht zu den sicherlich schwierigen Abgrenzungsfragen zur Gesetzgebungkompetenz äußern. Entscheidend ist für mich vielmehr, daß baldmöglichst ausreichende und den oben genannten datenschutzrechtlichen Anforderungen entsprechende Regeln zustande kommen. Dies läge sicher auch im Sinn der Akzeptanz der neuen Dienste und damit auch im Interesse der Diensteanbieter. Auch das scheint mir ein Beispiel, wo Datenschutz gleichzeitig Verbraucher- und Anbieterinteressen dient.

17.4 Vermittlung und Abrechnung digitaler Fernsehsendungen

Aktuellen Bezug erhält die oben aufgestellte Forderung auf Datenminimierung durch die gegenwärtig stattfindende Markteinführung des digitalen Fernsehens. Hier ist u.a. vorgesehen, daß der Kunde einzelne empfangene Sendungen gesondert bezahlen muß. Damit entsteht die Gefahr, daß individuelle Interessen und Sehgewohnheiten des Zuschauers registriert werden und damit ein Mediennutzungsprofil des einzelnen Kunden entsteht. Der vorliegende Entwurf eines MediendiensteStaatsvertrages sieht vor, daß die Gestaltung und Auswahl technischer Einrichtungen für Mediendienste sich am Ziel, keine oder so wenige personenbezogene Daten wie möglich zu erheben und zu verarbeiten, auszurichten hat. Die technischen Voraussetzungen für derartige Lösungen sind gegeben. Zusammen mit den anderen Datenschutzbeauftragten des Bundes und der Länder habe ich die Anbieter und Programmlieferanten aufgefordert, den Nutzern zumindest alternativ auch solche Lösungen anzubieten, bei denen die Nutzung der einzelnen Programmangebote nicht personenbezogen registriert werden kann.

Bei der Entwicklung datenschutzfreundlicher technischer Lösungen kann auf die Erfahrungen bei den elektronischen Geldbörsen und anderen kartengestützten Zahlungssystemen zurückgegriffen werden, die teilweise schon im Einsatz sind oder demnächst im Großversuch erprobt worden. Vor allem ist hier an im voraus bezahlte Wertkarten - ähnlich wie Telefonkarten - zu denken. Für die Akzeptanz dieser Bezahlungsart wird es wichtig sein, einfache Verfahren zu finden, mit deren Hilfe die Guthabenkarten aufgeladen werden können. Auch setzt eine vollständig anonyme Nutzung voraus, daß beim Zuschauer gespeicherte Informationen über die gesehenen Sendungen nicht durch den Anbieter abgerufen werden können.

Ich werde die weitere Entwicklung in diesem Bereich mit nachdrücklichem Interesse verfolgen.

17.5 Inkasso des Teilnehmerentgeltes bei Kabelanschluß für Fernsehen und Rundfunk

Aufgrund einer Beschwerde habe ich zusammen mit dem Beauftragten für den Datenschutz bei der Bayer. Landeszentrale für neue Medien eine Kontrolle bei der Bayer. Medien-Servicegesellschaft durchgeführt.

Dabei wurde folgender Sachverhalt festgestellt:

Nach Art. 38 Abs. 2 des Bayer. Mediengesetzes (BayMG) ist in Bayern eine Vereinbarung zwischen der zuständigen Medienbetriebsgesellschaft und dem Inhaber eines Kabelanschlusses Voraussetzung für den Bezug von Rundfunk- und Fernsehprogrammen, die über das Kabel eingespeist werden. Die Medienbetriebsgesellschaft ist nach Art. 38 Abs. 3 BayMG befugt, vom Inhaber eines Kabelanschlusses aufgrund dieser Vereinbarung ein Teilnehmerentgelt zu erheben und dieses in ihrem Namen von Dritten einziehen zu lassen. Auch kann die Medienbetriebsgesellschaft den Betreiber von Kabelanlagen beauftragen, in ihren Namen die Vereinbarung abzuschließen.

Aufgrund dieser Rechtslage wurde und wird auch zum gegenwärtigen Zeitpunkt in Bayern mit der Unterschrift des Kunden unter den Auftrag an die Telekom AG (früher: Deutsche Bundespost) zur Bereitstellung eines Kabelanschlusses neben dem zivilrechtlichen Vertragsverhältnis zur Telekom gleichzeitig auch ein rundfunkrechtliches Teilnehmerverhältnis mit der örtlich zuständigen Medienbetriebsgesellschaft abgeschlossen. Diese Medienbetriebsgesellschaft erhebt von den Kabelanschlußnehmern auf der Grundlage des rundfunkrechtlichen Teilnehmerverhältnisses ein Teilnehmerentgelt. Aufgrund von internen Vereinbarungen mit den örtlich zuständigen Medienbetriebsgesellschaften hat die Deutsche Bundespost Telekom bis Ende 1993 die den Medienbetriebgesellschaften zustehen den Medienentgelte - neben den Telekom-Entgelten für die Nutzung des Kabelanschlusses - namens und im Auftrag dieser Gesellschaften von den Teilnehmern eingezogen.

Nachdem diese Inkassovereinbarung aufgehoben wurde, ziehen nun die Medienbetriebsgesellschaften selbst die ihnen zustehenden Gebühren ein. Die meisten bayerischen Medienbetriebsgesellschaften und die Bayer. Landeszentrale für neue Medien haben deswegen die Bayer. Medien-

Servicegesellschaft gegründet, die als wesentlichen Gesellschaftszweck das Inkasso des Teilnehmerentgelts für die Gesellschaft vornehmen soll. Im Zusammenhang mit der Aufhebung der Inkassovereinbarung hat die Deutsche Bundespost Telekom ab Beginn 1994 die Vertragsunterlagen für alle Kabelkunden an die Bayer. Medien-Servicegesellschaft übergeben. Gleichzeitig übergeben wurde ein bis zu diesem Zeitpunkt bei der Deutschen Bundespost Telekom in maschinenlesbarer Form geführter Datenbestand über die genannten Kabelkunden. Etwa die Hälfte dieser Kunden hatte gegenüber der Deutschen Bundespost Telekom eine Einzugsermächtigung für die bis dorthin gemeinsam eingezogenen Kabelgebühren und Teilnehmerentgelte erteilt. Die entsprechenden Angaben zur Bankverbindung hat die Deutsche Bundespost Telekom im maschinenlesbaren Datenbestand an die Medien-Servicegesellschaft übermittelt.

Die Bayer. Medien-Servicegesellschaft sah sich zum Zeitpunkt der Übergabe der Unterlagen außerstande, eine ins einzelne gehende Überprüfung des übergebenen Materials vorzunehmen. Die Papierunterlagen wurden vielmehr in Ordnern abgelegt; die maschinell lesbaren Daten dienten als Grundlage für den Aufbau eines eigenen automatisierten Inkasso-Verfahrens.

Meine stichprobenhafte Überprüfung der Papierunterlagen hat ergeben, daß diese nicht vollständig sind. Ferner habe ich auch Mängel bei der Rechtsverbindlichkeit vorhandener Vertragsunterlagen festgestellt. Im Laufe der Jahre wurden für den "Auftrag für einen Kabelanschluß" des Kunden mindestens 8 verschiedene Formulare verwendet, deren Inhalt eine Abbuchungserlaubnis der Medienbetriebsgesellschaften häufig nicht begründet. In ca. 1/3 der Fälle wird eine Abbuchungserlaubnis lediglich unterstellt.

Mit Beginn des Jahres 1996 wurde bei der Bayerischen MedienServicegesellschaft ein neues EDV-Verfahren für den Lastschrifteinzug eingeführt. Durch einen Programmfehler wurden dabei in ca. 150 Fällen Abbuchungen bei Teilnehmern vorgenommen, die ihre Abbuchungsermächtigung zu einem vorangegangenen Zeitpunkt widerrufen hatten. Unter diesen Fällen war auch der Beschwerdeführer.

Die Bayerische Medien-Servicegesellschaft handelt gegenüber den Teilnehmern namens und im Auftrag der jeweiligen Medienbetriebsgesellschaft. Entsprechende schriftliche Aufträge im Sinne des Art. 6 BayDSG existieren jedoch nicht; demzufolge fehlen auch entsprechende schriftli-

che Vorgaben der auftraggebenden Medienbetriebsgesellschaften zum Umfang der Datenerhebung, der Datenverarbeitung und zur Nutzung der vorhandenen Daten.

Ich habe diese Verfahrensweise beanstandet und die Bayer. Medien-Servicegesellschaft aufgefordert, umgehend entsprechende schriftliche Weisungen von den Auftraggebern einzuholen. Auf die Pflicht zur Vervollständigung der Vertragsunterlagen und auf die Notwendigkeit, gültige Abbuchungsermächtigungen beizubringen, habe ich hingewiesen.

Ich habe ferner den Verstoß gegen die Löschvorschriften des § 28 Abs. 5 Rundfunkstaatsvertrag beanstandet. Die Bankverbindung der betroffenen Teilnehmer war nach dieser Vorschrift zu löschen, sobald die Abbuchungsermächtigung widerrufen wurde. Nur als Folge dieser Unterlassung konnte der Programmfehler bei Umstellung des automatisierten Inkassoverfahrens auftreten. Die Bayer. Medien-Servicegesellschaft hat mir eine zügige Vervollständigung der fehlenden Unterlagen und die künftige Beachtung der Löschvorschrift zugesichert.

18. Technischer und organisatorischer Bereich

18.1 Grundsatzfragen

18.1.1 Voraussetzungen für die Nutzung von Internet-Diensten

Die Bayerische Staatsregierung fördert aus den Privatisierungserlösen seit 1995 im Rahmen des Projektes "Bayern Online" eine Reihe von Telekommunikationsprojekten. Grundlage für die meisten Teilprojekte - auf manche wird im einzelnen noch einzugehen sein - ist das Vorhandensein einer flächendeckenden, leistungsfähigen Kommunikationsinfrastruktur, auf der eine multimediale Kommunikation abgewickelt werden kann. Da ein solches Netz auch für **jedermann** zur Verfügung stehen und selbstverständlich auch Anschlußstellen zum Internet haben soll, sind als Grundversorgung bestimmte **Basissicherheitsmaßnahmen** zur Verfügung zu stellen. Im einzelnen handelt es sich um folgende Maßnahmenbündel:

- Verschlüsselungsroutinen zur Sicherung der Vertraulichkeit von übertragenen Informationen

- Sicherung der Integrität und Authentität der übertragenen Informationen durch elektronische Signaturverfahren

- Einrichtungen zur Abschottung von internen Netzen gegen Zugriffe Unbefugter von außen (Installation geeigneter Firewall-Systeme)

- Führung von revisionsfähigen Nachweisen für die Beweissicherung

- Maßnahmen zur ständigen Verfügbarkeit der Netzinfrastruktur

Ich bin von der Staatsregierung über den Führungskreis an der Umsetzung des Projektes Bayern Online beteiligt und habe auf die Notwendigkeit dieser Maßnahmen hingewiesen. Es liegen einige Projekte in dieser Richtung vor. Ich werde die Maßnahmen weiter begleiten.

Aus der Sicht des Datenschutzes sind weiter folgende Hinweise im Zusammenhang mit der Internetschulung wichtig, deren Nichtbeachtung entweder zu einer zweckentfremdeten Nutzung von Benutzerdaten führen oder ungewollt Benutzer- und Benutzungsdaten an Dritte offenbaren

kann:

- Bei der Paßwortwahl sind gewisse Grundregeln zu beachten:
    - Keine Worte oder Wortteile verwenden, da diese mit Hilfe elektronischer Wörterbücher sehr schnell geknackt werden können.
    - Das Paßwort mindestens alle 3 Monate wechseln.
    - Das Paßwort sollte mindestens 6 Zeichen und ein Sonderzeichen enthalten.
    - Für verschiedene Rechner sind verschiedene Paßworte zu verwenden.
- Service-Provider speichern zu Abrechnungszwecken Zugangs- und Verbindungsdaten. Bei einer Speicherung im Ausland gibt es meist keine eindeutigen gesetzlichen Regelungen über die Verwendung dieser Daten.
- In den Log-Files wird aufgezeichnet, welcher Rechner auf welche Informationsangebote zugegriffen hat. Kann ein Rechner einem ganz bestimmten Benutzer zugeordnet werden, sind diese Daten personenbezogen und unterfallen somit dem Datenschutzrecht.
- Internet-Zusatzprogramme können manchmal unbemerkt Identifikationsdaten zum Internet-Rechner übertragen, wenn der Benutzer keine Sicherheitsmaßnahmen (Setzen des Schreibschutzes für sog. "Cookie-Dateien") vorsieht.
- Der Benutzer muß bezüglich der Sicherheitslücken und Schwächen von Internetprogrammen, etwa von Browsern, am laufenden bleiben. (So empfiehlt es sich beispielsweise, Javascript von Netscape zu deaktivieren, weil damit ganze Dateien, auch Paßwortdateien, vom lokalen Rechner ausgelesen werden können.)
- Als weitere Vorsorgemaßnahme empfiehlt es sich, nicht immer mit den neuesten Versionen solcher Programme zu arbeiten, da erst eine weltweite Nutzung deren Schwächen offenbart.

18.1.2 Bayerisches Gesundheitsnetz

Zu den rechtlichen Fragen im Zusammenhang mit der Telemedizin, die sich auch im Rahmen des Bayerisches Gesundheitsnetzes - Bayern Online stellen, wird zunächst auf den Beitrag unter Nr. 3.1.2 verwiesen. Aus der technisch organisatorischen Sicht muß nachstehendes sichergestellt werden.

Wegen der besonderen Geheimhaltungspflicht medizinischer Daten muß beim Austausch von Patientendaten im Rahmen einer Telekonsultation ausgeschlossen werden, daß diese Daten auf dem Übertragungswege Dritten zugänglich werden, unabhängig davon, ob der Zugang mißbräuchlich geschieht. Eine vertrauliche Kommunikation wird nur dann sichergestellt, wenn die Daten durch zuverlässige Algorithmen verschlüsselt werden, bevor sie auf das Transportmedium gebracht werden.

Dabei können Kompatibilitätsprobleme auftreten, wenn die in Kommunikation tretenden Stellen unterschiedliche Hard- und Betriebs-Software einsetzen, auf denen die vereinbarten Verschlüsselungsverfahren nicht ablauffähig sind. Auch die Modalitäten der Schlüsselerzeugung und -verteilung sind rechtzeitig abzuklären. Aus diesem Grunde ist dringend geboten, daß bereits vor dem Beginn der Pilotversuche im Rahmen von Bayern Online Spezifikationen für diese unverzichtbaren Sicherheitsmaßnahmen entwickelt sind. Inzwischen liegt auch ein Projekt mit diesen Zielvorstellungen vor. Eines muß allen Beteiligten dabei klar sein: der Einsatz dieser Sicherheitskomponenten ist nicht zum Nulltarif zu haben. Die Akzeptanz dieser Verfahren wird jedoch von der Gesamtsicherheit des Systems abhängen.

Mit der Verwendung des preiswerten Internets handelt man sich im übrigen nicht zu unterschätzende weitere Sicherheitsrisiken ein: Um Angriffe von Hackern aus dem Internet abzuwehren, benötigt man sowohl an zentraler Stelle als auch bei den Abfragestationen (also bei jedem Arztsystem) geeignete Schutzmechanismen (Firewall-Konzepte), die Eindringversuchen in interne Netze oder Rechner wirksam begegnen.

Ich habe meine Vorstellungen über die zu realisierenden Sicherheitsmaßnahmen in den Arbeitskreis "Telemedizin" eingebracht und werde die Entwicklung aufmerksam beobachten.

Zu einem Projekt ist noch folgendes zu bemerken:

Im Projekt ByMedCard wird eine Patientenkarte für Diabetiker entwickelt, die als Kommunikationsinstrument zwischen niedergelassenem Arzt und dem Krankenhaus (dem Diabeteszentrum) sowie innerhalb des Krankenhauses zwischen den einzelnen Fachabteilungen dienen soll. Darüberhinaus soll noch eine professionelle Arztkarte zur Steuerung der Zugriffsberechtigungen, Signierung von Nachrichten und Verschlüsselung von Nutzdaten entwickelt werden. Auf der Patientenkarte müssen neben der Speicherung von Daten (eine Art Krankengeschichte) auch Autorisierungs- und Verschlüsselungsalgorithmen implementiert sein. Bei Einsatz von Public-Key-Systemen sind schließlich Vorgaben über die Einrichtung eines sog. Trust Centers (Trusted Third Party) zu machen, das als Aufgaben die Schlüsselgenerierung, -verwaltung und -verteilung sowie die Personalisierung der Karten hat. Auch über diese Arbeitsschritte sollen im ByMedCard Erfahrungen gesammelt werden.

18.1.3 Sicherheit von Chipkarten

Chipkarten haben Eingang ins tägliche Leben gefunden und gewinnen zunehmend an gesellschaftlicher und wirtschaftlicher Bedeutung. Aufgrund ihrer mannigfachen Ausprägungsformen und vielfältigen Anwendungsmöglichkeiten bedürfen sie zur Wahrung der informationellen Selbstbestimmung und der informationstechnischen Sicherheit größter Aufmerksamkeit.

Chipkarten sind miniaturisierte Computer im Scheckkartenformat, die über keine eigenen Ein- und Ausgabegeräte als Schnittstelle zum Menschen verfügen.

Heutzutage sind im wesentlichen zwei Varianten von Chipkarten auf dem Markt verfügbar:

- Speicherchipkarten
    - mit nicht-flüchtigem Speicher (z.B. Krankenversichertenkarten und sonstige Identifikationskarten)
    - intelligente Speicherchipkarten (z.B. Telefonkarten)
- Prozessorchipkarten
    - mit Speichereinrichtungen und einem Prozessor
    - mit Speichereinrichtungen und Co-Prozessoren (für kryptographische Verfahren)

Die Sicherheit einer Chipkarte stützt sich auf vier Komponenten:

- Kartenkörper
- Chip (Prozessor und Speicher)
- Betriebssystem-Software

- Anwendungs-Software

Chipkarten können jedoch nicht nur für sich gesehen als sicher oder unsicher bewertet werden, sondern müssen hierzu immer in ihrem gesamten Umfeld betrachtet werden.

Zu diesem Umfeld gehören insbesondere Kartenterminals, die als Schnittstelle zwischen dem Kartenbenutzer und der Chipkarte verwendet werden, da Chipkarten über keine eigenen Ein- und Ausgabegeräte (wie ein "richtiger" Computer) zur Kommunikation mit dem Menschen verfügen. Aber auch die hinter den Kartenterminals liegenden Datenverarbeitungssysteme müssen in die Betrachtung mit einbezogen werden.

Durch die rasant fortschreitende Entwicklung der Halbleitertechnologie kann davon ausgegangen werden, daß sowohl die Leistungsfähigkeit der Mikroprozessoren als auch die Speicherkapazität von Chipkarten in wenigen Jahren der von heutigen Personal Computern entspricht.

Der technologische Fortschritt und der Anwendungstrend gehen eindeutig in Richtung **multi-funktionale Chipkarte**, d.h. Vereinigung mehrerer, unterschiedlichster Anwendungen auf einer einzigen Chipkarte.

Um zukünftig einen möglichst hohen Sicherheits- und Zuverlässigkeitsstandard zu gewährleisten, ist es erforderlich, daß bereits beim Design von Kartenbetriebssystemen und Kartenanwendungen Standards und Regeln eingehalten werden.

Der Arbeitskreis "Technische und organisatorische Datenschutzfragen der Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat sich ausführlich mit diesem Thema befaßt und ein Papier mit "Anforderungen zur informationstechnischen Sicherheit bei Chipkarten" erstellt (Anlage 4).

18.1.4 Verschlüsselungstechniken

Im Zusammenhang mit der ständig zunehmenden Benutzung von offenen Computer-Netzwerken, wie z.B. dem Internet, kommt der Sicherung der Daten bei der Übertragung vor unbefugter Kenntnisnahme und unbefugter Veränderung größte Bedeutung zu. Vor diesem Hintergrund haben die Datenschutzbeauftragten des Bundes und der Länder im Frühjahr 1996 die "Entschließung zur sicheren Übertragung elektronisch gespeicherter personenbezogener Daten" gefaßt (siehe Anlage 7).

Mit der Anwendung zuverlässiger und geeigneter kryptographischer Verfahren können die o.a. Schutzziele, für deren Einhaltung stets der Absender einer Nachricht verantwortlich ist, erreicht werden.

Durch Verschlüsselung (Kryptierung, Chiffrierung) wird eine lesbare Nachricht in eine Nachricht aus scheinbar sinnlos aufeinanderfolgenden Zeichen (Chiffrat) verändert. Die Rückumformung des Chiffrats in die ursprüngliche Nachricht (Klartext) wird als Entschlüsselung (Dekryptierung, Dechiffrierung) bezeichnet. Die Vorgänge der Ver- und Entschlüsselung können durch Software und/oder Hardware durchgeführt werden.

Im wesentlichen gibt es drei Verschlüsselungstechniken:

- symmetrische Verschlüsselung
- asymmetrische Verschlüsselung
- hybride Verschlüsselung

Die **symmetrischen Verschlüsselungsverfahren** sind dadurch charaktierisiert, daß für die Verschlüsselung und für die Entschlüsselung jeweils der gleiche Schlüssel verwendet wird. Dies bedeutet, daß sowohl der Absender als auch der Empfänger einer verschlüsselten Nachricht über den gleichen Schlüssel verfügen müssen. Die bekanntesten Verfahren sind der Data Encryption Standard (DES), Triple DES und der International Data Encryption Algorithm (IDEA).

Die **asymmetrischen Verschlüsselungsverfahren** sind dadurch charaktierisiert, daß für die Verschlüsselung und für die Entschlüsselung von Nachrichten jeweils unterschiedliche Schlüssel verwendet werden. Dies bedeutet, daß jedem Kommunikationsteilnehmer nicht ein Schlüssel, sondern ein Schlüsselpaar zugeordnet sein muß, nämlich ein sog. öffentlicher Schlüssel (public key) und ein privater Schlüssel (private key). Aus den Bezeichnungen für diese beiden Schlüsselteile rührt auch der Name Public-Key-Verfahren. Das bekannteste Verfahren ist das RSA-Verfahren, welches von Rivest, Shamir und Adleman entwickelt wurde. Der RSA-Algorithmus ermöglicht grundsätzlich zwei verschiedene Anwendungen, nämlich das Verschlüsseln einer Nachricht und das Authentifizieren einer Nachricht mit Hilfe einer sog. digitalen Signatur. Mit einer digitalen Signatur werden "Unterschriften" elektronisch nachgebildet. Da die elektronische Unterschrift auf Basis der Nachricht ermittelt wird, wird diese Nachricht gleichzeitig quasi versiegelt.

Hybride Verschlüsselungsverfahren vereinen die Vorteile der symmetrischen mit den Vorteilen der asymmetrischen Verfahren, ohne jeweils die Nachteile der einen oder anderen mit zu übernehmen. Sie bestehen überwiegend aus einer Kombination des RSA- mit dem DES-Algorithmus sowie einer Kombination des RSA- mit dem IDEA-Algorithmus. Mit hybriden Verfahren können Nachrichten i.d.R.

- nur verschlüsselt,
- nur digital signiert oder
- verschlüsselt und digital signiert

werden. Bei den hybriden Verfahren werden die symmetrischen Verfahren zur Verschlüsselung der Nachricht an sich verwendet. Das asymmetrische Verfahren dient zur digitalen Signatur und zur Verschlüsselung des benutzten symmetrischen Schlüssels, der mit der Nachricht übertragen wird.

Ein Hauptproblem bei allen Verfahren ist das Schlüsselmanagement, d.h.

- die Erzeugung sicherer Schlüssel,

- die sichere Verwaltung der Schlüssel sowie

- die Sicherstellung der Authentizität der öffentlichen Schlüssel der Teilnehmer bei den asymmetrischen Verfahren.

Um dieses Problem zu lösen, gibt es mittlerweile vielfältige Ansätze in Industrie, Forschung und Verwaltung.

18.1.5 Firewall-Techniken

Firewall-Systeme (aus dem Englischen: Brandschutzmauern) sind Lösungen und Konzepte, die ein eigenes sicheres Netzwerk vor der Außenwelt schützen sollen. Sie bestehen aus einer oder mehreren Hard- und/oder Softwarekomponenten oder nur aus Software, die einen kontrollierten zentralen Übergang zwischen zwei Netzen darstellen.

Ein Firewall-System kann im wesentlichen mit zwei Grundtechniken realisiert werden:

- Paketfilterung (Packet filtering)

- Gateway auf Anwendungsebene (Application Gateway)

Bei der Paketfilterung unterscheidet ein Router anhand der IP-Pakete zwischen erlaubten und unerlaubten Diensten. Paketfilter können nach Quell- und Zieladresse sowie nach Quell- und Zielort filtern. Damit sind sowohl die für eine Kommunikation zugelassenen Rechner von den nicht zugelassenen Rechnern als auch die zugelassenen Dienste von den nicht zugelassenen Diensten zu unterscheiden. Eine benutzerbezogene Authentisierung ist nicht möglich.

Ein Gateway auf Anwendungsebene ist ein speziell konfigurierter Rechner, der als Übergangstelle vom eigenen zum offenen Netz dient. Da es auf Anwendungsebene greift, besteht hier z.B. die Möglichkeit, ausführliche Protokolle zu führen und eine benutzerbezogene Authentisierung für die einzelnen Dienste durchzuführen.

Durch Kombination der Grundtechniken sowie deren unterschiedlicher Anordnung werden die klassischen Firewall-Architekturen realisiert:

- Screening Router

- Screened Gateway

- Dual Homed Gateway

- Screened Subnet

Damit sind individuelle Realisierungen von zentralen FirewallSystemen für unterschiedlichste Kommunikations- und Sicherheitsbedürfnisse in einem homogenen Netzwerk möglich.

Für komplexe Netzwerke und insbesondere für Netze mit heterogenen Schutzbedürfnissen von Teilnetz zu Teilnetz oder gar von Rechner zu Rechner sind diese o.a. Architekturen in ihrer reinen Ausprägung nicht angemessen und nicht ausreichend. In diesen Fällen kann eine Kaskadierung von Firewall-Systemen erforderlich sein, d.h. einzelne oder alle Teilnetze schützen sich ihrerseits nochmals selbst durch ein geeignetes Firewall-System gegenüber den anderen Teilnetzen. Dadurch ist eine feinere Abstimmung auf die spezifischen Schutzbedürfnisse in jedem einzelnen Teilnetz möglich, der finanzielle, administrative und organisatorische Aufwand steigt allerdings entsprechend an. Auch hier gilt der Satz, daß Sicherheit nicht umsonst zu haben ist.

Mittlerweile sind auch Firewall-Systeme auf dem Markt verfügbar, die über die sog. Tunnelling-Funktion verfügen. Mit diesen Systemen können über verschiedene Standorte verteilte lokale Netze über ein offenes unsicheres Netz sicher miteinander kommunizieren, wobei die zu übertragenden Daten vom absendenden Firewall-System verschlüsselt und vom empfangenden Firewall-System wieder entschlüsselt werden.

Darüberhinaus sind derzeit auch Firewall-Systeme verfügbar, die für Remote-Anmeldungen berechtigter Benutzer die Verwendung starker Authentifizierungshilfsmittel, wie z.B. Chipkarten, unterstützen.

Wie jede Brandschutzmauer in einem Gebäude kann aber auch ein Firewall-System keinen hundertprozentigen Schutz gegen alle Risiken bieten. Die Schutzwirkung von Firewall-Systemen kann sich nur unter wohl definierten Umständen und Konfigurationen und nur gegenüber bestimmten, d.h. bekannten, Risiken und Angriffsversuchen entfalten. Die Stärke eines Firewall-Systems hängt wesentlich von der eingesetzten Technik und ihrer korrekten Konfiguration und Administration ab.

Da

- sich die EDV-Technologie permanent fortentwickelt,
- die Angriffsmethoden und -techniken immer raffinierter und gleichzeitig leichter anwendbar werden und
- auch in bereits langjährig eingesetzten Betriebssystemen und Anwendungen immer wieder neue Mängel entdeckt werden,

sind eine permanente Pflege, Wartung und Fortentwicklung eines eingesetzten Firewall-Systems unbedingt notwendig.

Es sei deutlich nochmals darauf hingewiesen, daß

- Firewall-Systeme nur gegen derzeit bekannte Angriffsformen schützen können,
- kein Firewall-System evtl. vorhandene Sicherheitslücken im eigenen "sicheren" Netz schließen kann,
- Firewall-Systeme grundsätzlich keinen Schutz vor Computer-Viren bieten,
- Firewall-Systeme i.d.R. keine Mechanismen zum Schutz der Daten vor unberechtigter Kenntnisnahme oder Veränderung während ihrer Übertragung über das offene Netz bieten (Ausnahme: Systeme mit sog. "Tunnelling-Funktion"),
- Firewall-Systeme einer permanenten Überwachung, Anpassung und Pflege bedürfen,
- mit Firewall-Systemen derzeit nur Teilbereiche der gesamten Sicherheitsproblematik bei Anbindung an und Nutzung von offenen Netzen abgedeckt werden können und
- keine Technik oder Firewall-Architektur das Sicherheitsproblem umfassend lösen kann.

Zu Firewall-Techniken und Datenschutzfragen des Anschlusses von Netzen der öffentlichen Verwaltung an das Internet hat der Arbeitskreis "Technische und organisatorische Datenschutzfragen" der Datenschutzbeauftragten des Bundes und der Länder eine Orientierungshilfe erarbeitet, die bei meiner Geschäftsstelle angefordert werden kann.

18.1.6 Datenschutzfreundliche Technik

Durch die Fortentwicklung und zunehmende Verbreitung moderner Informations- und Kommunikationstechnik (IuK-Technik) wird z. B. über die Speicherung von Nutzerdaten die Privatsphäre des Bürgers mehr und mehr gefährdet. Die Technologie, die dafür gesorgt hat, daß personenbezogene Daten gespeichert, genutzt und weitergegeben werden können, läßt sich aber auch zum Schutz der Privatsphäre nutzen. Diese Möglichkeiten der modernen Datenschutztechnologie, die mit dem Begriff "Privacy enhancing technology (PET)" eine Philosophie der Datensparsamkeit beschreibt und ein ganzes System technischer Maßnahmen umfaßt, sollten hierfür genutzt werden.

Die zunehmende Verbreitung, Nutzung und Verknüpfbarkeit von IuK-Technik führt dazu, daß jeder der Benutzer in zunehmendem Maße elektronische Spuren hinterläßt. In der Regel hat der Benutzer über Art, Umfang, Speicherort, Speicherungsdauer und Verwendungszweck der über ihn gespeicherten Daten keine Kontrolle.

Der Schutz der Privatsphäre des Benutzers wird bisher i.d.R. dadurch erreicht, daß der Zugang und der Zugriff zu bereits gespeicherten personenbezogenen Daten mittels rechtlicher, technischer und organisatorischer Maßnahmen beschränkt wird.

Der Schutz der Privatsphäre hängt somit lediglich von der Wirksamkeit der ergriffenen Maßnahmen und der Gewissenhaftigkeit ab, mit der diese vollzogen werden. Und je mehr personenbezogene Daten erhoben und gespeichert werden, desto größer wird die Gefahr für die Privatsphäre.

Mit den technischen Sicherheitsmaßnahmen werden die klassischen Schutzziele

- Integrität,
- Vertraulichkeit und
- Verfügbarkeit

der gespeicherten Daten verfolgt.

Das Erreichen dieser Schutzziele reicht in Anbetracht der Entwicklungen in der IuK-Technik heutzutage jedoch nicht mehr aus. Nur durch eine weitgehende Reduzierung der Menge der gespeicherten Daten kann der Gefährdung der Privatsphäre auch zukünftig wirksam begegnet werden. Der Grundsatz der **Datensparsamkeit** muß zu einem vierten, klassischen Schutzziel werden.

Bereits bei der Konzeption von Verfahren und Systemen der IuK-Technik ist daher nach Lösungsformen und -wegen zu suchen, die vollständig auf die Erhebung und Verarbeitung personenbezogener Daten verzichten, d.h. **Datenvermeidung** als zunächst anzustrebende Form der Datensparsamkeit.

Gelungene Beispiele für solche, bereits eingesetzten bzw. projektierten Systeme sind das bargeldlose Telefonieren mit der vorausbezahlten, anonymen Telefonkarte, das bargeldlose Parken mit der vorausbezahlten, anonymen Münchener Parkkarte oder die beabsichtigte Geldkarte der bayerischen Raiffeisen- und Volksbanken.

Wo solche Lösungen nicht machbar sind, sollte zum Schutz der Privatsphäre von der schwächeren Form der Datensparsamkeit, der **Anonymisierung** Gebrauch gemacht werden. In der Praxis bedeutet dies, daß zum frühest möglichen Zeitpunkt eine Anonymisierung der erhobenen, personenbezogenen Daten erfolgt. Dabei ist darauf zu achten, daß eine Rekonstruktion des Personenbezugs nicht bzw. nur mit unverhältnismäßig hohem Aufwand möglich sein kann und darf.

Diese Methodik wird beispielsweise im Bereich der Statistik bereits seit langem praktiziert. Die Daten einer repräsentativen Personengruppe werden zunächst mit Personenbezug erhoben. Für die statistische Auswertung erfolgt dann aber die sofortige Anonymisierung.

Dieses Verfahren ist aber dann nicht anwendbar, wenn nachträglich Daten einer bestimmten Person zugeordnet werden müssen und die bereits vorhandenen Daten ohne Personenbezug gespeichert wurden. Hier kann die schwächste Form der Datensparsamkeit, die **Pseudonymisierung**, angewendet werden.

Pseudonyme werden anstelle unmittelbar personenbezogener Identifikationsdaten verwendet. Aus sich heraus ermöglichen sie keinen unmittelbaren Rückschluß auf die tatsächliche Identität des Betroffenen. Nur bei Bedarf und unter Einhaltung vorher zu definierender Rahmenbedingungen ist es möglich, den Personenbezug wieder herzustellen. Es sind grundsätzlich drei Klassen von Pseudonymen möglich, die sich nach ihrer Schutzwirkung hinsichtlich der Zusammenführbarkeit des Pseudonyms mit der wahren Identität des Betroffenen unterscheiden:

- vom Betroffenen selbst generierte Pseudonyme,

- von Dritten vergebene und nur über eine Referenzliste rückbeziehbare Pseudonyme (Referenz-Pseudonyme),

- Einweg-Pseudonyme, die nicht oder nur mit unverhältnismäßigem Aufwand rückgeführt werden können.

Als ein Beispiel sei hier auf die medizinische Forschung verwiesen, wo nachträglich erhobene Daten zu einem Patientenstammdatensatz zugewiesen werden müssen, ohne daß in diesem Stammdatensatz personenbezogene Daten gespeichert wären (z.B. Krebsregister).

Ein in Entwicklung befindliches System, das Datensparsamkeit durch Datenvermeidung zusammen mit einer Variante der Pseudonymisierung realisiert, ist das derzeitige Pilotprojekt für eine Multifunktionale Universitäts-Chipkarte (MUCK) an der Universität Würzburg. Die Chipkarte soll dabei einerseits als eine wiederaufladbare anonyme elektronische Geldbörse (ZKA-genormte Geldkarte; zentraler Kreditausschuß) und andererseits als starkes Authentifizierungshilfsmittel für Zugangs- und Zugriffskontrollsysteme (unter Verwendung des freien Speichers der Geldkarte) dienen. Dabei kommt diese Karte ohne direkten Personenbezug aus, indem lediglich eine eindeutige Identifikationsnummer benutzt wird.

Der Arbeitskreis "Technische und organisatorische Datenschutzfragen" der Datenschutzbeauftragten des Bundes und der Länder ist derzeit mit diesen Aspekten der datenschutzfreundlichen Technologien befaßt und erstellt ein entsprechendes Grundsatz- und Arbeitspapier.

18.1.7 Makroviren

Nachdem sich bislang Computerviren ausschließlich über bootfähige Disketten und ausführbare Programmdateien ausbreiteten, kann seit Mitte 1995 ein neuer Typ von Computerviren beobachtet werden, der sich dadruch auszeichnet, daß er Textverarbeitungs- oder Tabellenkalkulations-Dokumente befällt und diese Dateien als Wirt zur Vermehrung benutzt, indem er sich mittels eines Makros (Folge von Befehlen, die sich wiederholt ausführen lassen (z. B. Formatierung von Texten)) an einen gewöhnlichen Text anhängt. Wenn dann z. B. das Textverarbeitungsprogramm den Text lädt, führt es den Makrocode aus, der dann weitere Dateien verseucht und irgendwann beginnt, die definierten Funktionen auszuführen. Dieser Virustyp wird dementsprechend als Makrovirus bezeichnet. Makroviren stellten Mitte 1996 nach den Ermittlungen des Virus Bulletins mit ca. 20 % nach den Bootsektorviren bereits die zweithäufigste Virenart dar.

Ein Makrovirus ist eine in der Makrosprache (z. B. WordBasic von WinWord) eines Anwendungsprogrammes geschriebene Routine. Diese Makroroutinen sind in den zu bearbeitendem Text, einer Tabelle oder ähnlichem eingebettet. Damit sind sie an ihr Objekt gebunden. Der Anwender aktiviert diese Routinen automatisch, wenn er das Objekt mit einem Anwendungsprogramm bearbeitet.

Über Makrosprachen verfügen so gut wie alle Textverarbeitungen (z. B. WinWord, Wordperfect, Starwriter und Wordpro), Tabellenkalkulationen (z. B. Excel oder Lotus 1-2-3), Datenbanken (Access u. a.), aber auch Programme wie Powerpoint und Autocad.

Ein Makrovirus kann auch als Trojanisches Pferd fungieren. Zum Beispiel könnte ein Hacker einen unauffälligen Makrovirus in ein Behördennetz einschleußen, um alle von einem Anwender geladenen Dateien einer Textverarbeitung oder Tabellenkalkulation zu kopieren und über das Netz an sich selbst zu schicken, um sich so unerlaubt Informationen zu verschaffen.

Neu an dem Makrovirus ist auch seine Betriebssystemunabhängigkeit. Der Makrovirus kann gleichermaßen Windows-, OS/2- und DOS-PC als auch Macintosh-Computer befallen.

Bisher sind die Schäden durch Makroviren zwar noch gering (so sind vor allem Veränderungen

des Druckergebnisses, der Bildschirmdarstellung und Manipulationen beim Speichern verursacht worden), doch steckt in ihnen ein großes Gefahrenpotential. Es ist abzusehen, daß sich die Klasse der systemübergreifenden Makroviren sowohl zahlenmäßig als auch qualitativ sehr bald vermehren werden. Auch größere, komplizierte Makros mit Tarnkappenfunktionen oder polymorphen Eigenschaften scheinen durch die Mächtigkeit der Makrosprachen in absehbarer Zeit realisierbar. Um Makroviren zu programmieren, sind keine Kenntnisse der Maschinensprache und der Systemarchitektur nötig. War es bislang ohne tiefgehende Kenntnisse der C- oder Assembler-Sprache praktisch unmöglich, einen Virus zu erzeugen (mit Ausnahme der Viren-Toolkits), kann mit den Hilfedateien der Makrosprachen auch ein Laie in wenigen Stunden einen Virus programmieren. So ist es beispielsweise für einen durchschnittlich begabten Word-Anwender kein Problem, den Inhalt der Festplatte aus einem Makro heraus zu löschen. Ein entsprechendes WordBasic-Makro, das gleich die ganze Festplatte formatiert, existiert bereits. Aber auch bereits durch veränderte Werte in einer Tabelle können sich verhängnisvolle Fehlentscheidungen ergeben. Ein Makrovirus, der in einer großen Datenbank Datensätze durcheinanderwürfelt, macht den gesamten Datenbestand in kürzester Zeit völlig wertlos. Solche Schäden können fatale Folgen für eine Behörde haben.

Ein Makrovirus verbreitet sich durch das Laden der infizierten Datei mit dem vorgesehenen Programm, z. B. durch das Lesen des verseuchten Dokumentes mit Hilfe einer Textverarbeitung und durch das damit verbundene Abarbeiten der eingebetteten Makros. Die Herkunft des Dokumentes (ob von Diskette, als E-Mail über LAN oder WAN (Internet) oder über Mailbox-Download) und die jeweilige Landessprache des Programms spielen keine Rolle. Risikobehaftet sind vor allem Textdateien unbekannter Herkunft - egal, ob sie über Diskette oder über Online-Dienste in das System eingespeist werden. Auch beim Anklicken von Internet Seiten, die z. B. mit WinWord geschriebene Texte enthalten, besteht bereits ein Infektionsrisiko.

Durch den Aufruf des verseuchten Dokumentes ist der Virus aktiviert, infiziert als erstes die globale Dokumentenvorlage NORMAL.DOT, indem er z. B. neue Makros mit den Namen "AAAZ...", "AutoOpen", "FileSaveAs" und "PayLoad" einfügt, beziehungsweise, falls diese bereits vorhanden sind, modifiziert und kopiert sich danach unbemerkt in jedes neues Dokument, das der Benutzer in seine Textverarbeitung lädt. Über diese Dokumente können natürlich auch alle eingesetzten Server befallen werden.

Bisher können die Makroviren auch ohne Virenscanner noch relativ leicht erkannt werden. Zum Beispiel erscheint bei der Infizierung der globalen Dokumentenvorlage NORMAL.DOT durch den Concept-Virus auf dem Bildschirm ein kleines Dialog- oder Nachrichten-Fenster, in welchem eine einzelne Zahl - normalerweise die 1 (damit wird festgelegt, daß Word jedes Dokument als Vorlage speichert) - zu sehen ist. Dieses Fenster läßt sich nur durch ein Klicken auf "OK" schließen, um weiterarbeiten zu können. Allerdings erscheint diese verdächtige Meldung in allen Folgeoperationen (also auch bei der Weiterverbreitung des Virus) nicht mehr.

Eine weitere Erkennungsmöglichkeit ist das Überprüfen der globalen Makros (Menüpunkt Extras-Makro im WinWord). Existieren hier Makros mit den Anfangsbuchstaben "AAAZ" oder ein Makro namens "Payload", so ist der Computer vermutlich verseucht. Auch der Eintrag WW6I=1 in der WINWORD6.INI deutet auf einen etwaigen Virenbefall hin.

Gute Virenschutzprogramme können die Makroviren erkennen und beseitigen. Eine weitere Entfernungsmöglichkeit besteht zumindest beim Concept-Virus darin, alle Makros, welche mit den Anfangsbuchstaben "AAAZ" beginnen, sowie die Makros "AutoOpen", "FileSaveAs" und - soweit vorhanden - "Payload" in der NORMAL.DOT und in den einzelnen infizierten Dokumenten zu löschen. Wichtig dabei ist, daß die gesäuberten Dokumente **nur** mit "Speichern" und nicht mit "Speichern unter" gesichert werden. Sonst bleibt der Schädling virulent.

Zur Vorsorge vor einem Virenbefall der NORMAL.DOT sollte die Sicherheitsabfrage bei Veränderungen der Dokumentenvorlage (Optionsmenü-Speichern, Automatische Abfrage bei Speicherung der NORMAL.DOT) aktiviert werden. Außerdem kann die Datei NORMAL.DOT mittels DOS-Attributen geschützt werden. (Die Eingabe des Befehls **ATTRIB +R NORMAL.DOT** im entsprechenden Verzeichnis bewirkt, daß die Datei nur gelesen und nicht verändert werden kann.)

Eine weitere Möglichkeit zum Schutz vor dem Makrovirus ist das Drücken der Shift- (Hoch-) Taste beim Öffnen eines Dokumentes. Dadurch wird die Ausführung von AutoMakros beim Öffnen unterbunden.

Da diese Aktion aber leicht vergessen werden kann, sollte - zum Erreichen des gleichen Zweckes

- folgendes AutoExec-Makro in der NORMAL.DOT integriert werden:

```
Sub MAIN
DisableAutoMacros          zw. AutoMakroUnterdrücken für die deutsche Version)
End Sub
```

Der Nachteil dieser Lösung ist allerdings, daß auch eigene Makros nicht mehr automatisch ausgeführt werden können.

Ein weiterer Virenschutz besteht darin, keine fremden/unbekannten Dokumente mit Textverarbeitungs- bzw. Tabellenkalkulationsprogramme zu laden, ohne sie vorher mit einem bekanntermaßen guten Virenschutzprogramm geprüft zu haben.

18.2 Prüfungstätigkeit

18.2.1 Kontrolle und Beratung

Die Kontrolle der technischen und organisatorischen Datensicherheitsmaßnahmen war wiederum ein Schwerpunkt im Berichtszeitraum.

Bei folgenden **Dienststellen** habe ich Datenverarbeitungseinrichtungen nach Art. 7 BayDSG (z.T. i.V.m. § 9 BDSG und Anlage) kontrolliert:

- Amt für Landwirtschaft Passau
- Amtsgericht München (Verfahren SOLUM-STAR)
- AOK-Direktion Wunsiedel
- Bayerische Verwaltungsschule
- Bayerischer Oberster Rechnungshof
- Betriebskrankenkasse (BKK) Hutschenreuther, Selb
- Fachhochschule München
- Gemeinde Hausen
- Klinikum Nürnberg
- Landbauamt München
- Landesamt für Statistik und Datenverarbeitung
- Landeshauptstadt München (Inkassostelle der wahlärztl. Leistungen)
- Landeskriminalamt (Dokumentation des ADOK-Verfahrens)
- Landratsamt Augsburg
- Landratsamt Hof
- Landratsamt Landsberg
- Landratsamt Oberallgäu
- Polizeiverwaltungsamt, Viechtach
- Rechenzentrum der Staatsforstverwaltung
- Staatliches Hochbauamt Passau
- Stadt Aschaffenburg
- Stadt Fürstenfeldbruck
- Stadt Immenstadt

- Stadt Lindau
- Stadt Memmingen
- Stadt Passau
- Stadt Schrobenhausen
- Stadt Schwabach
- Stadt Weilheim
- Stadtwerke Wunsiedel
- Tumorregister, Klinikum Großhadern
- Universität Bayreuth, Verwaltung
- Universitätsklinikum Würzburg (SAP-Verfahren)

Einige Prüfungsverfahren sind bei Drucklegung dieses Tätigkeitsberichtes hinsichtlich der Berichtserstellung allerdings noch nicht abgeschlossen.

Die Prüfung beim Bayerischen Landeskriminalamt betraf die Dokumentation und Abschottung der ADOK-Verfahren Bayern und Baden-Württemberg (Einzelheiten dazu unter 18.2.3).

Beim Amtsgericht München habe ich die Datensicherheitsmaßnahmen des auch im Rahmen von Bayern Online geförderten Verfahrens SOLUM-STAR geprüft (Ergebnisse siehe 18.2.4).

Bei der Prüfung im Landesamt für Statistik und Datenverarbeitung war die Abschottung der Auftragsdatenverarbeitung für bayer. Behörden von den eigenen Statistikanwendungen Gegenstand der Prüfung. Die Abschottung ist gewährleistet.

Dazu habe ich wieder zahlreiche Dienststellen beraten. Die Zahl der Dienststellen steigt ständig, die im Vorfeld von Um- oder Neubauaktivitäten oder vor Einführung neuer EDV-Verfahren Anregungen hinsichtlich der gebotenen Datenschutz- und Datensicherheitsmaßnahmen (Objektschutz, DV-Organisation, Notfallvorsorge) erhalten. Wegen der ständig steigenden DV-Vernetzung, vor allem aber wegen des Anschlusses an Internet, haben auch die Beratungen auf diesem Gebiet zugenommen. Schließlich werde ich den technischen Einsatz von SAP im Klinikbereich begleiten.

18.2.2 Ergebnisse der Kontrolltätigkeit

Auch für diesen Berichtszeitraum konnte bei den Kontrollen festgestellt werden, daß der Stand der technischen und organisatorischen Maßnahmen zur Datensicherheit recht unterschiedlich ist. Zum Teil wurden Datensicherheitsmaßnahmen von hoher Qualität angetroffen, aber ich mußte auch immer wieder teilweise erhebliche Mängel feststellen.

Wegen ihrer generellen Bedeutung möchte ich auf einige Mängel nachfolgend ausführlicher eingehen:

Absicherung von Server- und Netzverteilungsräumen

Auch Server- und Netzverteilungsräume sind gegen unbefugtes Betreten abzusichern. Dazu müssen als Mindestmaßnahmen alle zu diesen Räumen führenden Türen mit mechanischen Türschließern und Türknaufe (statt Türgriffe) ausgestattet sein. In diesen Räumen dürfen auch keine größeren Papiervorräte oder Putzmittel gelagert werden, da dies eine vermeidbare Brandlast darstellt.

Revisionsfähige Dokumentation der Zugriffsberechtigungen

Trotz wiederholter Hinweise in den letzten Tätigkeitsberichten ist es leider bei vielen Dienststellen immer noch üblich, daß Zugriffsrechte auf telefonische Anweisung eingerichtet werden. Eine revisionsfähige Dokumentation der Vergabe von Benutzerberechtigungen ist jedoch nur möglich, wenn eine **schriftliche** Beantragung der Zugriffsrechte durch die Fachdienststellen vorliegt.

Paßwortänderung

Die Paßwortvergabe und -änderung muß bei allen Rechnern, auf denen personenbezogene Daten verarbeitet werden, durch den Anwender selbst erfolgen können. Die Gültigkeit der Paßworte sollte ca. 90 Tage betragen. Nähere Hinweise zur Paßwortvergabe, -wahl und -verwaltung können einer Orientierungshilfe entnommen werden, die bei meiner Geschäftsstelle kostenlos er-

hältlich ist.

Protokollauswertung

Alle anomalen Betriebszustände und Sicherheitsverletzungen an den DV-Anlagen sind durch Auswertung der entsprechenden Log-Dateien in einem täglichen Sicherheitsbericht aufzuzeigen und zu überprüfen, damit Sicherheitsverletzungen und vor allem Versuchen von unzulässigen Aktionen rechtzeitig nachgegangen werden kann.

Datenfernverarbeitung

Die Modems von Wählleitungsanschlüssen sind außerhalb der Zeiten der Datenfernverarbeitung inaktiv zu schalten, damit ein Verbindungsaufbau nur mit Wissen der EDV-Stelle stattfinden kann und ein mißbräuchlicher Anschluß ausgeschlossen wird, soweit nicht anderweitige technische Einrichtungen vorhanden sind, die unbekannte Verbindungsaufbauversuche unterbinden.

Bestellung und Einbindung eines Datenschutzbeauftragten

Gemäß Nr. 3.1 der "Gemeinsamen Bekanntmachung der Bayerischen Staatskanzlei und der Bayerischen Staatsministerien vom 01.07.1994 zum Vollzug des Bayerischen Datenschutzgesetzes" haben Gerichte, Behörden und sonstige öffentliche Stellen des Freistaates Bayern zur Sicherstellung des Datenschutzes bei Vorliegen folgender Voraussetzungen behördliche Datenschutzbeauftragte zu bestellen:

- wenn in der Regel mindestens fünf Beschäftigte ständig in automatisierten Dateien personenbezogene Daten verarbeiten, oder

- wenn in der Regel mindestens 20 Beschäftigte ständig in nicht-automatisierten Dateien personenbezogene Daten verarbeiten, oder

- wenn die öffentliche Stelle Daten im Auftrag anderer Stellen verarbeitet, oder

- in Krankenhäusern, die über mehr als 100 Betten verfügen.

Den Gemeinden, den Gemeindeverbänden und den sonstigen der Aufsicht des Freistaates Bayern unterstehenden juristischen Personen des öffentlichen Rechtes und den privatrechtlichen Vereinigungen, auf die das BayDSG nach Art. 2 Abs. 2 anwendbar ist, wird empfohlen, bei Vorliegen dieser Voraussetzungen ebenfalls behördliche Datenschutzbeauftragte zu bestellen. Dieser Datenschutzbeauftragte sollte besonders in alle EDV-Verfahrensabläufe aber auch in sonstige Datenverarbeitungsvorgänge mit grundsätzlicher Bedeutung eingebunden werden. So sollte er bei der Vergabe von Benutzerberechtigungen beteiligt werden und eine entsprechende Dokumentation führen. Diese Tätigkeiten können von einem Bediensteten außerhalb der EDV meistens miterledigt werden. Nähere Informationen zu den Aufgaben eines behördlichen Datenschutzbeauftragten sind bei meiner Geschäftsstelle erhältlich.

Anlagen- und Verfahrensverzeichnis

Ich möchte an dieser Stelle noch einmal darauf hinweisen, daß gemäß Art. 27 Bayer. Datenschutzgesetz jede öffentliche Stelle ein Anlagen und Verfahrensverzeichnis führen muß. Mustervordrucke liegen bei meiner Geschäftsstelle auf.

18.2.3 Prüfung des ADOK-Verfahrens beim Bayerischen Landeskriminalamt

Die Auftragsdatenverarbeitung des bayerischen Landeskriminalamtes für das baden-württembergische Landeskriminalamt gibt keinen Anlaß zu einer Beanstandung.

In ihrem 15. Tätigkeitsbericht hat meine baden-württembergische Kollegin die Fragen der Abschottung der bayerischen von den baden-württembergischen ADOK-Daten sowie der Zugriffsberechtigungen bayerischer Beamter auf baden-württembergische ADOK-Daten angesprochen.

Ich habe daher im Frühjahr 1995 im Bayerischen Landeskriminalamt die Maßnahmen überprüft, die zur Abschottung und zum Schutze der für das Landeskriminalamt Baden-Württemberg gespeicherten Daten getroffen wurden.

Das Bayerische Landeskriminalamt nutzt die selbstentwickelte "Arbeitsdatei Organisierte Kriminalität (ADOK)" einerseits selbst für eigene Zwecke und hat diese andererseits dem Landeskriminalamt Baden-Württemberg in Kopie (ADOK-BW) zur Nutzung überlassen. ADOK-BW läuft im Auftrag auf dem Rechnersystem des Bayerischen LKA ab. Die software-technische Wartung und Pflege obliegen dem Bayerischen Landeskriminalamt.

Eine Trennung des bayerischen vom baden-württembergischen ADOK ist sowohl bzgl. der Programme als auch der Daten gegeben.

Die Zugriffskontrolle für das Verfahren wird auf der Ebene der Bildschirmberechtigung und auf der Ebene der Benutzerberechtigung durchgeführt wird. Alle Eintragungen in den entsprechenden Berechtigungsdateien werden von den Mitarbeitern des Bayerischen LKA ausschließlich auf schriftlichen Auftrag des LKA Baden-Württemberg vorgenommen. Diese Benutzerverwaltung geschieht in revisionsfähiger Form.

Die Verfahrensdokumentation liegt als Kurzbeschreibung in Papierform vor. Eine ausführliche Programmdokumentation steht auf der EDV-Anlage online zur Verfügung. Darüberhinaus ist ein ausführliches Benutzerhandbuch verfügbar.

Pflege und Wartung der Programme des ADOK-BW erfolgen revisionsfähig aufgrund eines formalen, schriftlichen Auftrags.

Alle Zugriffe auf die Dateien werden automatisch protokolliert. Die Protokolldatei wird regelmäßig gesichert und der jeweilige Datenträger wird für die Dauer von einem Jahr aufbewahrt. Die Protokolldaten stehen dem behördlichen Datenschutzbeauftragten auf Anforderung zur Auswertung zur Verfügung. Vorbereitete Auswerteprogramme gibt es nicht.

Ein selektiver Zugriff des Bayerischen LKA auf die im Rahmen der technischen Datensicherung auf externen Datenträgern gespeicherten Daten des ADOK-BW (sowohl in der Gesamtheit als auch auf einzelne Datensätze) ist aufgrund des eingesetzten Datenbanksystems und der gewählten Sicherungstechnik nicht möglich.

Zum Prüfzeitpunkt lagen die für eine derartige Auftragsdatenverarbeitung erforderlichen, schriftlichen Vorgaben des LKA Baden-Württemberg zu Datenschutz- und Datensicherungsmaßnahmen an das LKA Bayern nicht vor. Dies ist zwischenzeitlich erfolgt und auch meine sonstigen, gemachten Anregungen zur Verbesserung des Datenschutzes und der Datensicherheit wurden umgehend umgesetzt.

Die Prüfung ergab, daß zu Beanstandungen meinerseits kein Anlaß gegeben war.

18.2.4 Das Verfahren SOLUM-STAR im Grundbuchamt München

Das elektronische Grundbuchamt SOLUM-STAR erreicht durch geschickte Organisation und durch Einsatz kryptographischer Verfahren ein hohes Maß an Datenintegrität und -vertraulichkeit auch bei der Kommunikation über offene und öffentliche Netze.

Im Rahmen des von der Bayerischen Staatsregierung initiierten Programms "Bayern Online" soll mit dem Projekt SOLUM-STAR die Umstellung und die Führung von Grundbüchern in München und zunächst in Nürnberg auf elektronische Verarbeitung pilothaft erprobt werden. Das Projekt umfaßt auch ein automatisiertes Abrufverfahren aus dem zentral geführten Grundbuch sowie die Kommunikation mit externen Nutzern wie Notaren und Banken im Rahmen der gesetzlichen Vorschriften.

Insbesondere den Aspekten der Benutzerverwaltung, der Zugriffskontrolle, der Unverfälschbarkeit gespeicherter Dokumente sowie der Datensicherheit bei ihrer Übertragung über offene und öffentliche Netze kommt hier besondere Bedeutung zu.

Im Frühjahr 1996 besuchten daher meine Mitarbeiter das Grundbuchamt München, um sich über die ergriffenen technischen und organisatorischen Maßnahmen zu Datenschutz und Datensicherheit zu informieren. Sie stellten dabei fest, daß die ergriffenen Maßnahmen der Benutzerverwaltung, der Zugriffssicherung - u.a. durch Paßwort mit Zeitsperre nach drei Fehlversuchen -, der Protokollierung der externen Recherchen, der digitalen Signatur zum Nachweis der Änderungsberechtigung und der Verschlüsselung der Daten während der Übertragung über Netze ein hohes Maß an Datenintegrität und Vertraulichkeit gewährleisten.

18.3 Technische Einzelfragen

18.3.1 Datenaustausch zwischen Leistungserbringern und Krankenkassen

Ursprünglich war vorgesehen, daß der Datenaustausch zwischen Leistungserbringern und Krankenkassen bzw. den Kassenärztlichen Vereinigungen in maschinenlesbarer Form ab 1.1.1996 beginnen sollte. Da sich der Aufbau der DV-Infrastruktur verzögerte, ist damit erst 1997 zu rechnen.

Aus Gründen der Datensicherung gegen unbefugte Kenntnisnahme auf dem Transportweg wurden für diesen Datenaustausch folgende Sicherheitsmaßnahmen gefordert:

- **Bei der Übermittlung auf dem Leitungsweg (Online-Übermittlung) sind die Nutzdaten (Patientendaten) zu verschlüsseln.**

  Gründe dafür sind: Abhörrisiko, Ungewißheit über welche Leitungswege die Datenübermittlung führen bzw. denkbare Zwischenspeicherung in den Vermittlungsstellen.

- Bei der Übermittlung der Daten auf Diskette oder Magnetband lassen sich folgende zwei Fälle unterschieden:

  a) Direkte Übermittlung an die Krankenkassen oder kassenärztliche Vereinigung auf dem Postwege.

  b) Einschaltung von Auftragnehmern (z.B. nach § 80 SBG X bzw. Vermittlungsstellen nach § 69d Abs. 4 SGB X), die die Weiterleitung an die zuständige Krankenkasse oder kassenärztliche Vereinigung steuern und nicht Teil der empfangenden Stelle sind.

  - Fall a): Die Daten sind wegen des hohen Vertraulichkeitsgrades zu verschlüsseln, falls nur eine normale Versandart (Brief, Paket) gewählt wird. **Übergangsweise und nur solange und soweit** keine technische Möglichkeiten zur Verschlüsselung bestehen, ist eine unverschlüsselte Speicherung der personenbezogenen zulässig, **wenn eine höherwertige Versandart** (z. B. Wertbrief, -paket) **gewählt wird**.

  - Fall b): Die Daten sind zu verschlüsseln, wenn sie zur Weiterleitung an die Krankenkassen von Diskette auf Leitung etwa durch Dritte umgesetzt werden müssen (eine

Kenntnisnahme der Inhalte kann sonst nicht ausgeschlossen werden, diese wäre aber durch durch den Umfang des Vermittlungsauftrags nicht gedeckt).

- Werden die Abrechnungsdaten vom Leistungserbringer auf Papier zur Verfügung gestellt, müssen sie ohne Umweg direkt an die Krankenkasse gesandt werden. Der Versand erfolgt über Wertbrief oder -paket.

Die Datenübermittlung vom Leistungserbringer zur Krankenkasse mittels maschinenlesbaren Datenträger und auf dem Leitungswege muß also grundsätzlich verschlüsselt erfolgen. Als **Übergangsregelung** wird lediglich die folgende Ausnahme akzeptiert: Diskettenversand direkt zur Krankenkasse mit höherwertiger Versandart, wenn und solange die Hard- und Software des Leistungserbringers den Einsatz des von der Krankenkasse gewählten Verschlüsselungsverfahrens nicht zulassen.

Trotz rechtzeitiger Bekanntgabe meiner Forderungen, die mit den Datenschutzbeauftragten des Bundes und der Länder abgestimmt wurden, und in Anbetracht der Vertraulichkeit und Integrität der zu übertragenden Daten war es für einige Institutionen, die von Leistungserbringern patientenbezogene Abrechnungsdaten erhalten, bisher nicht möglich, mir den Einsatz eines geeigneten Sicherungssystems zu melden.

Einige Krankenkassen richten für diesen Datenaustausch eigene Vermittlungsstellen (sog. Clearingstellen) ein. Sofern diese Stellen nicht zur Krankenkasse oder kassen(zahn)ärztlichen Vereinigung gehören, dürfen ihnen keine Inhaltsdaten (patientenbezogene Abrechnungsdaten) offenbart werden. Ihre Aufgaben beschränken sich lediglich auf die Annahme und formale Überprüfung von Absender und Empfänger sowie auf die Weiterleitung der Daten an die Krankenkasse. Für den Fall, daß diesen Vermittlungsstellen eine Einsicht in die Inhaltsdaten möglich ist, werde ich dies bei den unter meine Zuständigkeit fallenden Stellen wegen eines Verstoßes gegen Art. 22 BayDSG und § 81 Abs. 2 SGB X gemäß Art. 31 BayDSG beanstanden.

18.3.2 Sicherheitsmaßnahmen im Behördennetz

Ein Ziel von Bayern Online ist es, daß alle bayerischen Behörden zukünftig ihre gesamte Daten-

kommunikation auf einem gemeinsamen Netz, dem sog. Behördennetz abwickeln. Das kann aus Datensicherheitsgründen aber nur dann akzeptiert werden, wenn das Behördennetz die gleichen Sicherheiten bietet, wie es bisher bei den geschlossenen Netzen der Fall war. Bei der Einbindung bereits bestehender Rechnernetze in das Behördennetz ist also darauf zu achten, daß die bereits heute verfügbare Datensicherheit keinesfalls gemindert wird.

Im bayerischen Behördennetz werden eine Vielzahl von vertraulichen Informationen, sei es im Rahmen von Datenabrufen aus zentralen Datenbeständen, sei es als elektronische Mitteilungen (E-Mails) zwischen zwei oder mehreren Partnern übertragen. Schließlich wird es vorkommen, daß umfangreiche Dokumente, ganze Datenbestände und Bilder über das Netz gehen werden. Um die Vertraulichkeit dieser Informationen und die Unverletzlichkeit der angeschlossenen internen Netze sicherzustellen, sind von allen Betroffenen geeignete Sicherheitsmaßnahmen zu ergreifen. Im einzelnen handelt es sich dabei um folgende, im Zusammenhang mit der Nutzung des Internets erwähnte Maßnahmen:

- Verschlüsselungsverfahren zum Schutze der Vertraulichkeit der übertragenen Informationen

- Sicherung der Integrität und Authentität der übertragenen Daten durch deren Signierung (elektronische Unterschrift)

- Sicherung der internen Netze gegen Eingriffe unbefugter Dritter durch Abschottung mit geeigneten Firewall-Systemen

- Führung von revisionsfähigen Nachweisen zur Beweissicherung der Datenkommunikation. Maßnahmen der Verschlüsselung und der Signierung von übertragenen Informationen hängen selbstverständlich von der Sensibilität der übertragenen Informationen ab.

Die Datenschutzbeauftragten des Bundes und der Länder haben sich am 9.5.1996 unter meiner Mitwirkung angesichts der Zunahme der elektronischen Datenkommunikation in einer Entschließung zu "Forderungen einer sicheren Übertragung elektronisch gespeicherter personenbezogener Daten" geäußert und gefordert, daß "sichere kryptografische Verfahren beim Transport elektronisch gespeicherter personenbezogener Daten unter Berücksichtigung ihrer Schutzwür-

digkeit anzuwenden" sind (siehe Anlage 7).

In einem Netz, wie es das Bayer. Behördennetz darstellen wird, das von einer Vielzahl unterschiedlicher Benutzer genutzt werden wird, gilt schließlich die Faustregel: Alles was in herkömmlicher Art in einem umschlossenen Umschlag versandt wird, muß bei der Übertragung im Netz verschlüsselt werden. Eine unverschlüsselte Informationsübertragung entspräche der herkömmlichen Versandart auf einer Postkarte.

18.3.3 Sicherheitsanforderungen an Telearbeitsplätze

Die Telearbeit wird eine immer größere Bedeutung erlangen. Bereits heute gibt es in der öffentlichen Verwaltung dafür Ansätze. So erkundigte sich im Berichtszeitraum eine Behörde aus dem Sozialbereich unbeschadet der rechtlichen Rahmenbedingungen darüber, welche Anforderungen an technische und organisatorische Sicherungsmaßnahmen für Telearbeitsplätze im häuslichen Bereich zu stellen sind.

Im einzelnen war dazu folgendes zu bemerken:

- Die Telearbeiter bleiben Bedienstete des Amtes; es findet keine Auftragsdatenverarbeitung statt.

- Der Dienstherr bleibt weisungsbefugt, er bestimmt die Art und Weise, wie die Aufgaben zu erledigen sind.

- In einer Dienstanweisung sind die Telearbeiter auf die Einhaltung aller vorgebenen Sicherheitsmaßnahmen schriftlich zu verpflichten.

- Sicherheitsvorgaben, die in einer solchen Dienstanweisung vorgegeben werden sollten, sind:

- Der Aktentransport erfolgt in verschlossenen Behältnissen, die der Dienstherr zur Verfügung stellt. Soweit beim Transport öffentliche Verkehrmittel benützt werden, ist darauf zu achten, daß die Behältnisse dort nicht unbeaufsichtigt abgestellt oder ganz vergessen werden.

- Für die Aufbewahrung der dienstlichen Unterlagen im häuslichen Bereich muß ein verschließbarer Schrank oder Teil eines Schrankes vorhanden sein; unter Umständen lassen sich auch die verschließbaren Transportbehältnisse zur Aufbewahrung heranziehen. Die Unterlagen dürfen in der Wohnung nicht offen herumliegen, Familienangehörige dürfen keinen Zugang zu den Unterlagen erhalten.

- Werden für die Bearbeitung elektronische Rechner eingesetzt, sind diese einschließlich der

benötigten Datenträger vom Dienstherrn zur Verfügung zu stellen. Rechner und Datenträger sind gegen den Zugriff Unberechtigter zu schützen.

- Auf dem Rechner dürfen keine anderen, als dienstlichen Aufgaben zum Ablauf kommen.

- Der Rechner ist mit einer Sicherheitskomponente gegen die Inbetriebnahme Unbefugter abzusichern. Gegebenenfalls sollte täglich ein Virenerkennungsprogramm ablaufen.

- Das DV-System zeichnet Inbetriebnahme, Benutzungen und Sicherheitsverstöße in einem Protokoll auf. Die Protokolle sind dem Dienstherrn monatlich zur Verfügung zu stellen. Da diese Protokolle zur Verhaltenskontrolle geeignet sind, ist eine Mitbestimmung durch den Personalrat nach Art. 75 a Abs.1 Nr.1 BayPVG zwingend. Unabhängig davon empfiehlt es sich, für die Verarbeitung dieser Protokolle eine strikte Zweckbindung zu vereinbaren.

- Wenn Datenbestände länger als einen Tag gespeichert werden, ist täglich eine Datensicherung auf Diskette oder ähnlichen Datenträger zu ziehen. Diese Sicherungsdatenträger sind unter Verschluß zu halten.

- Der elektronisch gespeicherte Datenbestand ist so gering wie möglich zu halten.

- Ein Online-Anschluß des Rechners an das Rechnersystem des Dienstherrn setzt Sicherheitsmaßnahmen auf dem Übertragungswege und Abschottungsmaßnahmen sowohl beim zentralen, wie beim dezentralen System voraus. Da die Kosten für diese Sicherheitsmaßnahmen doch beträchtlich sein dürften, wird man zweckmäßigerweise vor deren Einführung eine Kosten-Nutzen-Analyse durchführen.

- Da es sich um keine Auftragsdatenverarbeitung handelt, sind die Vorgaben des SGB an diese Art der Verarbeitung gegenstandslos.

- Auf die Bearbeitung von sensitiven Daten, insbesondere von Personaldaten im häuslichen Bereich sollte verzichtet werden. Einige Geschäftsbereiche haben dies durch entsprechende Weisungen bereits ausgeschlossen (vgl. 16. TB Nr. 12.3).

18.3.4 96-Stunden-Stromzähler (LZ96)

Der Konflikt zwischen Kundenservice und berechtigtem Anspruch eines Leistungserbringers einerseits und der Wahrung der Privatsphäre sowie der Vermeidung der Bildung von Persönlichkeitsprofilen andererseits wird am Beispiel des von einem Energieversorger verwendeten Stromzählers deutlich.

Gem. §§ 4 und 5 der Bundestarifordnung Elektrizität 1990 (BTO Elt 1990) vom 18. Dezember 1989, setzt sich der von einem Kunden eines Energieversorgungsunternehmens zu entrichtende Pflichttarif aus den Bestandteilen Arbeitspreis, Leistungspreis und Verrechnungspreis zusammen.

Der Arbeitspreis wird für jede abgenommene Kilowattstunde berechnet, der Leistungspreis ist ein Entgelt für die Bereitstellung von elektrischer Leistung. Der Verrechnungspreis ist das Entgelt für die Kosten der Verrechnung, des Inkassos sowie der technisch notwendigen Meß- und Steuereinrichtungen.

Der Leistungspreis kann entweder durch Messung der in Anspruch genommenen Leistung (§ 5 BTO Elt 1990) oder nach (Jahres)Durchschnittswerten bzw. nach Mengenzonen (§ 6 BTO Elt 1990) berechnet werden.

Auf der Grundlage des § 5 BTO Elt 1990 "Berechnung des Leistungspreises durch Messung" i.V.m. dem jeweiligen Allgemeinen Tarif haben einige bayerische Energieversorgungsunternehmen bei ihren Kunden mit einem Jahresstromverbrauch von mehr als 10.000 kWh die sog. 96-Stunden-Messung mittels eines dafür vorgesehenen Meßgerätes (LZ96) eingeführt, das anstelle des üblichen Stromzählers beim Kunden eingebaut wird.

Dazu hat jeder betroffene Kunde vom Energieversorgungsunternehmen vorab ein Schreiben erhalten, in dem ihm der Umfang und der Grund der mit dem LZ96 durchgeführten Datenspeicherungen erläutert werden. Dabei geht das EVU davon aus, daß ein Kunde, solange er nicht explizit widerspricht, mit der umfassenden Aufzeichnung und Speicherung der vom LZ 96 erhebbaren Verbrauchsdaten einverstanden ist.

Der LZ96 ermittelt stündlich die in diesem Zeitraum verbrauchten Kilowattstunden, bestimmt aus den Meßwerten der zurückliegenden 96 Stunden den Höchstwert und speichert diesen mit einer Tagesnummer ab. Außerdem wird für jedes 30-Tage-Intervall ein solches Wertepaar als "Monatsmaximum" im Meßgerät abgespeichert. Auf der Basis des höchsten dieser Maximalwerte bestimmt sich dann der vom Kunden zu entrichtende Tarif.

Mit

- diesen zwölf Monatsmaxima,
- den Einzelwerten der unmittelbar zurückliegenden 96 Stunden und
- dem aktuellen Höchstwert aus diesen sowie mit
- den erforderlichen zähleridentifizierenden Angaben

werden somit ca. 140 Werte im LZ96 festgehalten.

Die Ablesung dieser gespeicherten Werte ist durch den Kunden jederzeit selbst möglich. So soll ihm die Gelegenheit gegeben werden, sein Verbrauchsverhalten selbst kontrollieren und ggf. beeinflussen zu können. Auf ausdrücklichen Wunsch des Kunden wird die Ausleseeinrichtung am LZ96 verplombt, wodurch aber er nicht mehr in der Lage ist, die gespeicherten Werte jederzeit selbst abzurufen.

Das Energieversorgungsunternehmen liest die gespeicherten Werte zur Zeit über eine mobile Datenerfassungseinheit (MDE) vor Ort beim Kunden aus. Ein Fernabruf der gespeicherten Daten über das Stromversorgungsnetz ist u.a. aufgrund der Bauart des LZ96 nicht möglich. Es ist jedoch beabsichtigt in nicht allzu ferner Zukunft den Fernabruf der gespeicherten Daten mittels separater MODEM-Leitungen über das Telefonnetz abzuwickeln.

Beim Ablesevorgang werden alle im LZ96 gespeicherten Daten abgezogen. Von der mobilen Datenerfassungseinheit werden die Daten in einen PC und von dort in die zentrale EDV-Anlage übertragen. In der MDE werden die Daten mit dem nächsten Ablesevorgang überschrieben, auf

dem PC bleiben die Daten einen Tag gespeichert. Auf der zentralen EDV-Anlage werden die Daten etwa drei bis sechs Monate online vorgehalten und danach auf CD-ROM ausgelagert. Bei etwaigen Zweifeln des Kunden an der Richtigkeit der Rechnungsstellung kann auf diesen Datenbestand (für die vergangene Abrechnungsperiode) zurückgegriffen werden.

Vor diesem Hintergrund habe ich nachfolgende Hinweise für ein datenschutzgerechtes Vorgehen gegeben:

1. **Die Praxis der Widerspruchslösung soll auf eine Erklärungslösung umgestellt werden.**

   Bisher geht - wie ausgeführt - das Energieversorgungsunternehmen davon aus, daß ein Kunde, solange er nicht explizit widerspricht, mit der umfassenden Aufzeichnung und Speicherung der vom LZ 96 erhebbaren Verbrauchsdaten einverstanden ist.

   Statt dessen sollte dem Kunden bei Aufnahme der Geschäftsbeziehungen bzw. vor Einbau des LZ 96 ein Formblatt vorgelegt werden, in dem er über die beiden möglichen und bzgl. des erhobenen Datenumfangs unterschiedlichen Speicherungsformen samt jeweiligen Folgen ausführlich unterrichtet wird. Mit diesem Formblatt kann der Kunde sodann den von ihm gewünschten Aufzeichnungs- und Speicherumfang (d. h. Basisdaten oder erweiterter Datenumfang) wählen.

   In diesem Zusammenhang ist es jedoch erforderlich, daß auch Bauformen des LZ 96 auf dem Markt zur Verfügung stehen, die einen reduzierten Datenumfang erheben und speichern können. Die Energieversorgungsunternehmen sollten deshalb entsprechend auf die Gerätehersteller einwirken.

2. **Eine Fernablesung von Verbrauchsdaten darf nur mit Wissen und schriftlich erklärtem Willen des Kunden erfolgen.**

   Für Sonderkunden (Großkunden) des Energieversorgungsunternehmens ist die Einführung von Fernwirken und Fernablesen derzeit in Projektierung. Langfristig gesehen ist es

nur eine Frage der Zeit, daß derartige Techniken auch für Privathaushalte zur Verfügung stehen und dann auch genutzt werden.

Gemäß Art. 35 Abs. 1 Satz 1 Bayer. Mediengesetz ist in diesen Fällen eine schriftliche Einwilligung nach Information über Verwendungszweck und Wirkungsweise des Dienstes erforderlich.

Weiter sind in diesem Fall geeignete technische und organisatorische Maßnahmen und Geräte vorzusehen, die den Kunden in die Lage versetzen, sowohl die Tatsache als auch den Vorgang des Fernwirkens und der Fernablesung unter seiner unmittelbaren Kontrolle zu behalten.

3. **Die Abrechnung anderer Energieformen und Leistungen muß den gleichen Grundsätzen genügen.**

Derzeit stellt sich die unter 1. beschriebene Situation nur in Verbindung mit der Bereitstellung und Abrechnung von elektrischer Energie (abgesehen von o.a. Projekt für Sonderkunden).

Die vorstehenden Anregungen und Forderungen sind für evtl. zukünftige Anwendungen aus dem Bereich anderer Energieformen (z. B. Gas, Fernwärme) und Leistungsbereitstellungen (z. B. Wasser) jedoch analog anzuwenden und zu berücksichtigen.

18.3.5 Kostenrechnung von Protokollauswertungen

Auf einer DSB-Konferenz wurde das Problem der In-Rechnung-Stellung von Protokollauswertungen behandelt. Dabei wurde von spürbaren Erschwerungen der Datenschutzkontrolle bei Wegfall der Ablaufprotokolle als Folge von Einsparungsmaßnahmen in der Informationsverarbeitung, insbesondere beim Outsourcing, berichtet.

Die Ablaufprotokolle (Loggings) in der automatisierten Datenverarbeitung sind für die DV-Revision und die Datenschutzkontrolle ein unverzichtbares Instrument. Für die Gewährleistung eines ordnungsgemäßen DV-Betriebs sind diese Informationen wichtige Beweismittel für die Betriebssicherheit und die Ordnungsmäßigkeit der gesamten Datenverarbeitung, insbesonders dort, wo die Datenverarbeitung einen hohen Grad an Komplexität erreicht hat.

Für die DV-Sicherheit haben Protokolle deshalb einen hohen Stellenwert. Das spiegelt sich auch in den IT-Sicherheitskriterien (ITSEC) wider, die **Maßnahmen zur Beweissicherung** schon bei mittleren Sicherheitsanforderungen vorsehen. Bei einer komplexen DV-Struktur sorgen Protokolle letztlich für die notwendige Transparenz.

Schließlich haben Protokolle für eine effektive Datenschutzkontrolle eine zentrale Bedeutung: Fehlen Protokolle, existieren keine maschinellen Hilfsmittel für eine effektive Anlaßkontrolle. Für Routinekontrollen genügt es häufig, daß die Protokolloberfläche lediglich für einen gewissen Zeitraum aktiv geschaltet wird (sofern die notwendige Software dafür vorhanden ist), um die notwendigen Unterlagen für eine Überprüfung verfügbar zu haben.

Für den Betreiber wie für den Auftraggeber (im Falle des Outsourcings) gibt es bei Fehlen von aussagefähigen Ablaufprotokollen keinerlei Möglichkeiten, folgende Aktivitäten durchzuführen:

- Überprüfung des ordnungsgemäßen Ablaufs der DV-Programme
- Aufdecken von Sicherheitsverstößen
- Prüfung der Wirksamkeit des Sicherheitssystems
- Aufdecken von Lücken im Sicherheitssystem
- Schaffung einer Transparenz in der automatisierten Datenverarbeitung

Ablaufdaten, die von der Protokollebene der DV-Systeme erzeugt werden, und geeignete Auswertewerkzeuge sind also für die Transparenz und Kontrolle der automatisierten Datenverarbeitung sowie für die DV-Sicherheit unverzichtbar. In der Auftragsdatenverarbeitung (Outsourcing) wäre es geradezu absurd, auf Ablaufprotokolle zu verzichten, weil diese doch einen Anhaltspunkt dafür liefern, daß die Aufgaben ordnungs- und vertragsgemäß abgewickelt wurden. Sie sind somit als Nachweis der ordnungsgemäßen Abwicklung der DV-Programme notwendig, die dadurch entstehenden Kosten hat die datenverarbeitende Institution zu tragen.

Die Kosten für die Erzeugung und Auswertung von Ablaufdaten sind im übrigen wohl in erster Linie solche für die SoftwareBeschaffung und geringe zusätzliche Personalkosten, die bei der regelmäßigen Auswertung und Kontrolle dieser Informationen entstehen; Performance-Verluste bezüglich Rechnerleistung dürften in aller Regel vernachlässigbar sein.

18.3.6 Datensicherheit beim Versand schutzwürdiger Informationen mit dem Telefax

Der Telefax-Dienst der Deutschen Telekom AG hat sich zu einer beliebten und vor allem recht wirtschaftlichen Möglichkeit des Dokumententransports entwickelt. Er ist damit eine echte Alternative zur herkömmlichen Briefpost geworden.

Im Gegensatz zur Briefpost handelt es sich beim Telefax aber um eine Art offener Zustellung. In meinem 15. Tätigkeitsbericht (1993, Tz. 19.3.3, Seite 99) bin ich ausführlich auf die damit verbundenen Risiken und auf mögliche Sicherheitsmaßnahmen eingegangen.

Aus gegebenem Anlaß möchte ich erneut darauf hinweisen, daß trotz aller möglicher ergriffener technischer und organisatorischer Maßnahmen es immer wieder zu Fehlübertragungen kommen kann. Als häufigste Ursache dafür ist meist menschliches Versagen verantwortlich, etwa nicht erkannte Tippfehler bei der Eingabe der Zielnummer.

Insbesondere bei der Übertragung von Telefaxen mit besonders schutzwürdigem Inhalt (sensible personenbezogenen Daten) kann eine Fehlzustellung gravierende Folgen für den Absender, Empfänger und Betroffene haben.

Alle verantwortlichen Stellen möchte ich daher an ihre Pflicht erinnern, in ihrem unmittelbaren Bereich darauf hinzuwirken,

- daß vor Versand von schutzwürdigen Daten mit dem TelefaxDienst geprüft wird, ob diese Versandart wirklich erforderlich und nicht eine andere Versandart angemessener ist und

- daß bei Benutzung des Telefax-Dienstes die den zu übertragenden Informationen angemessene Sorgfalt bei der Eingabe der jeweiligen Zielnummer aufgebracht wird.

Soweit technische Hilfsmittel dafür vorhanden sind, ist von ihnen Gebrauch zu machen. Dazu einige Beispiele:

- Um Fehler bei der Zielnummerneingabe zu vermeiden, können die Zielnummern eingespei-

chert werden.

- Ist der Fax-Anschluß an eine Nebenstellenanlage angeschlossen, kann eine Nebenstellennummer verwendet werden, die möglichst wenig Spielraum für Fehleingaben durch den Absender zuläßt (Vermeidung ähnlicher Fax-Nummern bei anderen Stellen, soweit das bekannt ist).
- Zum Schutze gegen unbefugte Kenntnisnahme auf dem Übertragungsweg oder im Falle einer Fehlleitung kann das Fax durch den Einsatz von Zusatzkomponenten verschlüsselt werden. Eine Entschlüsselung ist dann nur dem rechtmäßigen Empfänger möglich. Hierzu sind jedoch entsprechende, nicht ganz billige Zusatzeinrichtungen bei Absender und Empfänger erforderlich. Da es sich hier um Einmalinvestitionen handelt, sollte das jedoch nicht zu stark ins Gewicht fallen.

Vorsicht ist überall dort geboten, wo ein Fax-Gerät mit einer eigenen Amtsnummer an einer ISDN-Nebenstellenanlage hängt. Hier muß, um ins Netz zu gelangen, eine "0" gewählt werden. Wird das unterlassen, kommt es in manchen Fällen zu Fehlleitungen, nämlich dann, wenn die verkürzte Nummer einen Fax-Anschluß darstellt.

18.3.7 Feldversuch: Automatische Gebührenerhebung auf Autobahnen

Im 16. Tätigkeitsbericht (Nr. 21.1.2, Seite 94) wurde über das Vorhaben des Bundesverkehrministeriums zur automatischen Gebührenerhebung auf Autobahnen ausführlich berichtet. Im Berichtszeitraum wurde auf der A 555 zwischen Köln und Bonn ein Feldversuch abgeschlossen, an dem sich 10 Privatfirmen mit unterschiedlichen Technologien beteiligten. Der mit der Durchführung beauftragte TÜV Rheinland stellte die Ergebnisse des Feldversuches in einem Abschlußbericht vor.

Zusammengefaßt stellen sich diese wie folgt dar:

- Die **Gebührenerhebung** ist mit der derzeit verfügbaren Technologie bereits mit hoher Erfolgsquote durchführbar. Bei geeigneter Weiterentwicklung wäre eine flächendeckende Einführung mit einsatzreifen Erhebungseinrichtungen aus technischer Sicht in wenigen Jahren möglich.

- Die **Kontrolle** (Verifikation) der Gebührenerhebung ist hinsichtlich der Anforderungen auf ausreichende Zuverlässigkeit, auch zu Beweissicherungszwecken, derzeit nicht zu gewährleisten.

- Die **datenschutzrechtlichen Forderungen** wie eindeutige Anonymisierung, Trennung von Zahlungs- und Nutzungsdaten sowie die Transparenz der Erhebungs- und Kontrollvorgänge konnten **von den eingesetzten Systemen** nicht vollständig erfüllt werden.

Wie bekannt, soll die bundesweite Einführung der automatisierten Gebührenerfassung auf Autobahnen vorerst nicht weiterverfolgt werden. Den Medien sind aber auch Informationen über anderweitige Bestrebungen zu entnehmen. Auch die Modellwirkung ähnlicher Vorhaben in Österreich verdient Beachtung. Aufmerksamkeit ist deshalb weiterhin geboten.

18.3.8 Nutzung eines Privatraums als Dienstzimmer (Amtsverschwiegenheit)

Ein Petent hatte sich mit der Bitte an mich gewandt, zu überprüfen und sicherzustellen, daß der Schutz personenbezogener Daten in seiner Gemeinde gewährleistet ist.

Er führte u. a. aus, daß das Arbeitszimmer des ersten Bürgermeisters grundsätzlich unversperrt sei und sich auch in Abwesenheit des Bürgermeisters Unberechtigte darin aufhielten, obwohl in diesem Zimmer sensible personenbezogene Daten aufbewahrt würden.

Mitarbeiter meiner Geschäftsstelle informierten sich daraufhin unangemeldet beim Bürgermeister dieser Gemeinde über die in dessen (privaten) Arbeitszimmer aufbewahrten personenbezogenen Unterlagen der Gemeinde.

Diese Überprüfung ergab, daß die entsprechende Gemeinde - als Teil einer Verwaltungsgemeinschaft - über keine eigenen Diensträume verfügt. Aus diesem Grunde benutzt der Bürgermeister sein privates Arbeitszimmer auch für die zwischenzeitliche Lagerung von dienstlichen Unterlagen der Gemeinde. Beim Besuch wurden zwar lediglich nichtpersonenbezogene Unterlagen (Statistiken) vorgefunden, es ist aber nicht auszuschließen, daß gelegentlich auch Unterlagen mit personenbezogenen Daten, etwa Bauanträge, dort aufbewahrt werden.

Desweiteren befand sich im Arbeitszimmer des Bürgermeisters ein Telefonapparat mit integrierten Faxgerät, das ausschließlich für dienstliche Zwecke benutzt wird. In der Abwesenheit des Bürgermeisters nahmen die Familienangehörigen die dort auflaufenden Gespräche entgegen.

Zur Absicherung des Arbeitszimmers gegen unbefugtes Betreten (auch durch Angehörige) und unbefugter Entnahme von dienstlichen Unterlagen wurde der Bürgermeister aufgefordert, diesen Raum stets verschlossen zu halten. Zur zukünftigen Vermeidung der Entgegennahme dienstlicher Gespräche durch Familienangehörige wurde ihm die Anschaffung eines Anrufbeantworters oder eines Mobiltelefons (Handy) angeraten.

Im übrigen sind Anrufbeantworter dort besonders zu schützen, wo Informationen von besonderem Geheimhaltungsgrad (z.B. Arztgeheimnis) auflaufen. Diese Geräte dürfen erst nach Eingabe

einer vierstelligen PIN-Nummer abgefragt werden können.

18.4 Orientierungshilfen

18.4.1 Gedanken zum Grundschutz

Bei jeder Verwendung eines EDV-Systems, mit dem personenbezogene Daten be- und verarbeitet werden, sind eine ganze Reihe von Maßnahmen zu ergreifen, um den gesetzlichen Forderungen nach Datenschutz gerecht zu werden.

Der Rahmen für diese zu ergreifenden Maßnahmen ist im Bayerischen Datenschutzgesetz in Art. 7 "Technische und organisatorische Maßnahmen" in Form der sog. "10 Gebote des Datenschutzes" umfassend abgesteckt.

In der Praxis herrscht häufig Unsicherheit darüber, welche Mindestmaßnahmen zu ergreifen sind. Aus diesem Grunde hat das Bundesamt für Sicherheit in der Informationstechnik (BSI) u.a. in Zusammenarbeit mit einigen Aufsichtsbehörden ein sog. IT-Grundschutzhandbuch entwickelt und in überarbeiteter Fassung im Jahre 1996 herausgegeben.

Ziel des Grundschutzes ist es, durch geeignete Anwendung von organisatorischen, personellen, infrastrukturellen und technischen Standardsicherheitsmaßnahmen ein grundlegendes Sicherheitsniveau für EDV-Systeme zu erreichen, das für einen mittleren Schutzbedarf angemessen und ausreichend ist. Für EDV-Systeme mit höherem Schutzbedarf kann der Grundschutz als Ausgangsbasis dienen.

Dazu werden im IT-Grundschutzhandbuch Maßnahmenbündel für typische EDV-Konfigurationen, Umfeld- und Organisationsbedingungen bereitgestellt und empfohlen.

Auf Basis dieses IT-Grundschutzhandbuches wurde in meiner Dienststelle eine Orientierungshilfe für "Erforderliche Maßnahmen der technischen und organisatorischen Sicherheit" erstellt. Diese Orientierungshilfe kann bei meiner Geschäftsstelle angefordert werden.

Für einzelne Maßnahmen oder Maßnahmenbündel liegen darüber hinaus spezielle und detaillierte Orientierungshilfen vor, die bei Bedarf angefordert werden können.

Im Einzelfall kann es sich durchaus herausstellen, daß die empfohlenen Maßnahmen zu weitgehend oder auch nicht weit genug gehend sind. Eine pauschale Beurteilung und Wertung, welche Maßnahme im einzelnen erforderlich ist oder nicht, kann meiner Meinung nach nicht getroffen, sondern nur am Einzelfall entschieden werden.

Gleichwohl können und sollen die Orientierungshilfen dazu dienen, zunächst Anregungen für die Erstellung eines eigenes Sicherheitskonzeptes zu geben. Die Verfeinerung des Sicherheitskonzeptes ergibt sich meist aus der Diskussion mit allen Beteiligten.

18.4.2 Zusammenstellung der neuen Orientierungshilfen

Im Berichtszeitraum wurden in meiner Dienststelle folgende Orientierungshilfen neu erstellt bzw. überarbeitet:

- Orientierungshilfe für erforderliche Maßnahmen der technischen und organisatorischen Sicherheit
- Datenschutzrechtliche Protokollierung beim Betrieb informationstechnischer Systeme (IT-Systeme) - (Grundlage war ein Papier des Arbeitskreises Technik der Datenschutzbeauftragten des Bundes und der Länder)
- Datensicherheit bei der Installation und beim Betrieb von Datenverarbeitungsanlagen - HP 3000 - der Hewlett Packard GmbH
- Regeln für den sicheren PC-Einsatz (im Stand-Alone-Betrieb)
- Orientierungshilfe für Paßwortvergabe, -wahl und -verwaltung
- Orientierungshilfe für Maßnahmen zur baulichen und organisatorischen Sicherheit von DV-Komponenten.

Im Rahmen meiner Beteiligung am Projekt Bayern Online, Anschluß von Behördennetzen an das Internet, habe ich "Grundsätze für Benutzerrichtlinien für die Nutzung des Internet" sowie die dazu notwendigen Benutzer-Musterrichtlinien erarbeitet.

Alle Unterlagen können bei meiner Geschäftstelle kostenlos angefordert werden.

19. Der Beirat

Dem Beirat gehörten an:

die Landtagsabgeordneten

Franz Brosch CSU	Prof. Dr. Hans Gerh. Stockinger
Rudolf Engelhard CSU	Johannes Neumeier
Alfred Reisinger	Dr. Helmut Müller
Markus Söder	Markus Sackmann
Dr. Klaus Hahnzog	Joachim Wahnschaffe
Franz Schindler	Dr. Thomas Jung

die Senatoren

Wolfgang Burnhauser	Hartwig Reimann

für die Staatsregierung

Hubert Kranz Ministerialrat im Bayer. Staatsministerium der Finanzen	Christian P. Wilde Ministerialrat im Bayer. Staatsministerium des Innern

für die Sozialversicherungsträger

Dr. Ludwig Bergner Erster Direktor der Landesversicherungsanstalt Oberbayern	Gerhard Wunderlich Direktor, Geschäftsführer des BKK Landesverband Bayern ab 26.03.96: Herr Dr. Helmut Platzer Stellv. Vorsitzender des Vorstandes der AOK Bayern

für die Kommunale Spitzenverbände

Klaus Eichhorn Geschäftsführender Direktor der Anstalt für kommunale Datenverarbeitung	Hanns Herrlitz Direktor bei der Anstalt für kommunale Datenverarbeitung

---

für den Verband Freier Berufe in Bayern e. V.

Erwin Stein	Winfried Wachter
Präsident der Steuerberaterkammer München	Präsidiumsmitglied des Verbandes freier Berufe e. V.
	ab 04.10.95:
	Dr. Wolf-Dieter Seeher
	Zahnarzt

Den Vorsitz im Beirat führt Franz Brosch, MdL; Stellvertreter ist Dr. Klaus Hahnzog.

Der Beirat befaßte sich in seinen Sitzungen im Berichtszeitraum insbesondere mit folgenden Themen:

- Beratung des 17. Tätigkeitsberichtes
- Berichte über Prüfungen und Beanstandungen
- Einschaltung von Privatunternehmen durch Gemeinden bzw. Zusammenschlüsse von Gemeinden bei der Verfolgung von Ordnungswidrigkeiten durch Verstöße gegen die Vorschriften über die zulässige Geschwindigkeit von Fahrzeugen
- datenschutzrechtliche Aspekte der Öffnung von Medienarchiven für jedermann
- Berichte von Arbeitskreisen und Datenschutzkonferenzen
- datenschutzrechtliche Fragen im Zusammenhang mit der Behördenreform
- Berichte zur Patientenkarte/Versichertenkarte

Anlagen

Anlage 1: Entschließung der 51. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 14./15. März 1996:

Modernisierung und europäische Harmonisierung des Datenschutzrechts

Die Datenschutzrichtlinie der Europäischen Union vom Oktober 1995 verpflichtet alle Mitgliedstaaten, ihr Datenschutzrecht binnen drei Jahren auf europäischer Ebene zu harmonisieren. Die Richtlinie geht zu Recht von einem hohen Datenschutzniveau aus und stellt fest: "Die Datenverarbeitungssysteme stehen im Dienste des Menschen".

Die Datenschutzbeauftragten begrüßen diesen wichtigen Schritt zu einem auch international wirksamen Datenschutz. Sie appellieren an den Gesetzgeber in Bund und Ländern, die Umsetzung der Richtlinie nicht nur als Beitrag zur europäischen Integration zu verstehen, sondern als Aufforderung und Chance, den Datenschutz fortzuentwickeln. Die Datenschutzbeauftragten sprechen sich für eine umfassende Modernisierung des deutschen Datenschutzrechts aus, damit der einzelne in der sich rapide verändernden Welt der Datenverarbeitung, der Medien und der Telekommunikation über den Umlauf und die Verwendung seiner persönlichen Daten soweit wie möglich selbst bestimmen kann.
Die wichtigsten Ziele sind:

1. Weitgehende Vereinheitlichung der Vorschriften für den öffentlichen und privaten Bereich mit dem Ziel eines hohen, gleichwertigen Schutzes der Betroffenen, beispielsweise bei der Datenerhebung und bei der Zweckbindung bis hin zur Verarbeitung in Akten

2. Erweiterung der Rechte der Betroffenen auf Information durch die datenverarbeitenden Stellen über die Verwendung der Daten, auf Auskunft, auf Widerspruch und im Bereich der Einwilligung

3. Verpflichtung zu Risikoanalyse, Vorabkontrolle, Technikfolgenabschätzung und zur Beteiligung der Datenschutzbeauftragten bei der Vorbereitung von Regelungen mit Auswir-

kungen auf den Datenschutz

4. Verbesserung der Organisation und Stärkung der Befugnisse der Datenschutzkontrolle unter den Gesichtspunkten der Unabhängigkeit und der Effektivität

5. Einrichtung und effiziente Ausgestaltung des Amtes eines internen Datenschutzbeauftragten in öffentlichen Stellen

6. Weiterentwicklung der Vorschriften zur Datensicherheit, insbesondere im Hinblick auf Miniaturisierung und Vernetzung

Darüber hinaus machen die Datenschutzbeauftragten folgende Vorschläge:

1. Erweiterung des Schutzbereichs bei Bild- und Tonaufzeichnungen und Regelung der Video-Überwachung

2. Stärkere Einbeziehung von Presse und Rundfunk in den Datenschutz; Aufrechterhaltung von Sonderregelungen nur, soweit dies für die Sicherung der Meinungsfreiheit notwendig ist

3. Sonderregelungen für besonders empfindliche Bereiche, wie den Umgang mit Arbeitnehmerdaten, Gesundheitsdaten und Informationen aus gerichtlichen Verfahren

4. Sicherstellung der informationellen Selbstbestimmung bei Multimedia-Diensten und anderen elektronischen Dienstleistungen durch die Pflicht, auch anonyme Nutzungs- und Zahlungsformen anzubieten, durch den Schutz vor übereilter Einwilligung, z.B. durch ein Widerrufsrecht, und durch strenge Zweckbindung für die bei Verbindung, Aufbau und Nutzung anfallenden Daten

5. Besondere Regelungen für Chipkarten-Anwendungen, um die datenschutzrechtliche Verantwortung aller Beteiligten festzulegen und den einzelnen vor unfreiwilliger Preisgabe seiner Daten zu schützen

---

6. Schutz bei Persönlichkeitsbewertungen durch den Computer, insbesondere durch Beteiligung des Betroffenen und Nachvollziehbarkeit der Computerentscheidung

7. Verstärkung des Schutzes gegenüber Adressenhandel und Direktmarketing

8. Verbesserung des Datenschutzes bei grenzüberschreitender Datenverarbeitung; Datenübermittlung ins Ausland nur bei angemessenem Datenschutzniveau

---

Anlage 2: Entschließung der 50. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 09./10. November 1995:

Weiterentwicklung des Datenschutzes in der Europäischen Union

Die Konferenz der Datenschutzbeauftragten der Europäischen Union hat am 08.09.1995 in Kopenhagen in einer Resolution im Hinblick auf die für 1996 geplante Regierungskonferenz dafür plädiert, anläßlich der Überarbeitung der Unions- und Gemeinschaftsverträge in einen verbindlichen Grundrechtskatalog ein einklagbares europäisches Grundrecht auf Datenschutz aufzunehmen. Die Schaffung rechtsverbindlicher Datenschutzregelungen für die Organe und Einrichtungen der Union sowie die Schaffung einer unabhängigen und effektiven Datenschutzkontrollinstanz der EU werden angemahnt. Dieser Resolution schließt sich die Konferenz der Datenschutzbeauftragten des Bundes und der Länder an. Sie hält angesichts der fortschreitenden Integration und des zunehmenden Einsatzes von Informations- und Kommunikationstechnologien in der EU eine Weiterentwicklung des Datenschutzes im Rahmen der EU für geboten.

Sie fordert die zuständigen Politiker und insbesondere die Bundesregierung auf, dafür einzutreten, daß im EU-Vertragsrecht ein Grundrecht auf Datenschutz aufgenommen wird, die materiellen Datenschutzregelungen in der EU verbessert werden, das Amt eines Europäischen Datenschutzbeauftragten geschaffen wird sowie eine parlamentarische und richterliche Kontrolle der Datenverarbeitung der im EU-Vertrag vorgesehen Instanzen sichergestellt wird.

Grundrecht auf Datenschutz

Bei einer Weiterentwicklung der Europäischen Union ist es unabdingbar, daß dem Grundrechtsschutz eine angemessene Bedeutung beigemessen wird. Dies sollte dadurch geschehen, daß die Verträge zur Europäischen Union mit einem Grundrechtskatalog ergänzt werden. Mit einer Entschließung vom 10.02.1994 hat das Europäische Parlament einen Entwurf zur Verfassung der Europäischen Union zur Erörterung gestellt, der u.a. folgende Aussagen enthält: "Jeder hat das Recht auf Achtung und Schutz seiner Identität. Die Achtung der Privatsphäre und des Familienlebens, des Ansehens (...) wird gewährleistet".

Die Konferenz der Datenschutzbeauftragten ist mit ihrer Entschließung vom 28.04.1992 dafür eingetreten, daß in das Grundgesetz nach dem Vorbild anderer europäischer Verfassungen ein Grundrecht auf Datenschutz aufgenommen wird. Sie hat hierfür einen Formulierungsvorschlag gemacht. Auf ihren Konferenzen am 16./17.02.1993 und 09./10.03.1994 bekräftigten die Datenschutzbeauftragten des Bundes und der Länder ihre Position. Diese Forderung wurde aber wegen des Nichterreichens der notwendigen qualifizierten Mehrheit durch den Gesetzgeber nicht umgesetzt.

In Wirtschaft, Verwaltung und Gesellschaft der Staaten der EU erhält der Dienstleistungs- und Informationssektor eine zunehmende Bedeutung. Dies hat zur Folge, daß mit hochentwickelten Informationstechnologien von privaten wie von öffentlichen Stellen verstärkt personenbezogene Daten verarbeitet und auch grenzüberschreitend ausgetauscht werden. Diese Entwicklung wird gefördert durch die Privatisierung und den rasanten Ausbau transeuropäischer elektronischer Telekommunikations-Netze. Dadurch gerät das Grundrecht auf informationelle Selbstbestimmung in besonderem Maße auf der überstaatlichen Ebene in Gefahr. Dieser Gefahr kann dadurch entgegengetreten werden, daß in einen in den überarbeiteten EU-Vertrag aufzunehmenden Grundrechtskatalog das Grundrecht auf Datenschutz und zu dessen Konkretisierung ein Recht auf unbeobachtete Telekommunikation aufgenommen werden. Dies hätte folgende positive Auswirkungen:

- Anhand einer ausdrücklichen gemeinsamen Rechtsnorm kann sich eine einheitliche Rechtsprechung zum Datenschutz entwickeln, an die sowohl die EU-Organe wie auch die nationalen Stellen gebunden werden.

- Ein solches Grundrecht wäre die Basis für eine Vereinheitlichung des derzeit noch sehr unterschiedlichen nationalen Datenschutzrechts auf einem hohen Niveau.

- Den Bürgerinnen und Bürgern wird deutlich erkennbar, daß ihnen in einklagbarer Form der Datenschutz in gleicher Weise garantiert wird wie die traditionellen Grundrechte.

- Das grundlegende rechtsstaatliche Prinzip des Datenschutzes wird dauerhaft, auch bei Erweiterung der EU, gesichert.

- Mit der rechtlichen Konkretisierung eines Rechts auf unbeobachtete Telekommunikation würde der zunehmenden Registrierung des Verhaltens der Bürgerinnen und Bürger in der multimedialen Informationsgesellschaft entgegengewirkt und der Schutz des Fernmeldegeheimnisses auch nach dem Abbau der staatlichen Monopole im Sprachtelefondienst sichergestellt.

Materielle Datenschutzregelungen

Mit der kürzlich verabschiedeten EU-Datenschutzrichtlinie wird ein großer Fortschritt für den Datenschutz auf europäischer Ebene erreicht. Dies darf aber nicht den Blick dafür verstellen, daß in einzelnen Bereichen spezifische, dringend nötige Datenschutzregelungen fehlen. Insbesondere sind folgende Bereiche regelungsbedürftig:

- Es bedarf eines für die EU-Institutionen verbindlichen eigenen Datenschutzrechts. Die datenschutzrechtliche Verantwortung der Mitgliedstaaten einschließlich ihrer Datenschutzkontrolle der Übermittlung von Daten an EU-Institutionen bleibt dabei unberührt.

- Die geplante ISDN-Datenschutzrichtlinie darf weder einer völlig falsch verstandenen Subsidiarität zum Opfer fallen noch in unzureichender Form verabschiedet werden.

- Die im Bereich der Statistik bestehenden datenschutzrechtlichen Defizite sind abzubauen.

- Es soll eine Technikfolgenabschätzung bei der Förderung und Einführung neuer Informationstechniken mit Personenbezug durch die EU obligatorisch eingeführt werden.

- In den Bereichen Inneres und Justiz sind aufeinander abgestimmte verbindliche Regelungen mit hohem Datenschutzstandard, die die Datenverarbeitung in Akten und die Sicherung der Datenschutzkontrolle mit umfassen, zu schaffen.

- Es bedarf der Harmonisierung des Arbeitnehmerdatenschutzes auf hohem Niveau

in den Staaten der EU.

- Für das Personal der EU-Organe ist der Arbeitnehmerdatenschutz sicherzustellen, was z.B. bei der Durchführung von Sicherheitsüberprüfungen insbesondere unter Beteiligung von Behörden der Heimatstaaten, von großer Bedeutung ist.

- Es ist zu prüfen, inwieweit Informationszugangsrechte in weiteren Bereichen eingeführt werden sollen.

Europäischer Datenschutzbeauftragter

Die Konferenz der EU-Datenschutzkontrollinstanzen (25./26.05.1994, 08.09.1995) und die Konferenz der Datenschutzbeauftragten des Bundes und der Länder (25.08.1994) haben darauf hingewiesen, daß es an einer unabhängigen und effektiven Datenschutzkontrollinstanz fehlt, an die sich jeder wenden kann, wenn er der Ansicht ist, bei der Verarbeitung seiner personenbezogenen Daten durch Stellen der EU in seinen Rechten verletzt zu sein. Aufgabe eines Europäischen Datenschutzbeauftragten sollte die Behandlung aller Datenschutzbelange der EU sein. Dazu gehört nicht nur die Bearbeitung von Betroffeneneingaben, sondern auch die datenschutzrechtliche Beratung der EUOrgane und -Einrichtungen sowie deren anlaßunabhängige Kontrolle, die Begleitung informationstechnischer EU-Projekte und der entsprechenden EU-Normsetzung sowie die Zusammenarbeit mit den nationalen Kontrollinstanzen. Wegen der teilweise anders gelagerten Aufgaben sollen die Funktionen des Europäischen Datenschutzbeauftragten und des Bürgerbeauftragten nach den EG-Verträgen nicht vermengt werden. Die Bundesregierung sollte im Rahmen der Vorbereitung der Regierungskonferenz 1996 darauf hinwirken, daß ein unabhängiger Europäischer Datenschutzbeauftragter in den Verträgen über die Europäische Union institutionell abgesichert wird.

Parlamentarische und richterliche Kontrolle

Bei der Zusammenarbeit der EU-Staaten in den Bereichen Justiz und Inneres muß mit Besorgnis festgestellt werden, daß eine ausreichende parlamentarische und richterliche Kontrolle im EUV derzeit nicht gewährleistet ist. Die geplante Europol-Konvention ist hierfür ein Beispiel. Mit unbestimmten Formulierungen werden einem fast völlig freischwebenden Europäischen Polizeiamt informationelle Befugnisse eingeräumt, einem Amt, das keiner parlamentarischen Ver-

antwortlichkeit und nur einer unzureichenden (teils nur nationalen) Rechtskontrolle unterworfen wird. Zur Wahrung des Datenschutzes bei der Umsetzung gemeinsamer Maßnahmen in den Bereichen Justiz und Inneres muß daher - unbeschadet der Kontrolle durch die nationalen Datenschutzbehörden - auch eine im Rahmen ihrer jeweiligen Zuständigkeiten lückenlose Kontrolle durch die nationalen Parlamente und Gerichte sowie durch das Europäische Parlament und den Europäischen Gerichtshof sichergestellt werden.

Anlage 3: Entschließung der 52. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 22./23. Oktober 1996:

Automatisierte Übermittlung von Abrechnungsdaten durch Kassenzahnärztliche Vereinigungen an gesetzliche Krankenkassen.

Der in dem Schiedsspruch vom 20. Februar 1995 für die Abrechnung festgelegte Umfang der Datenübermittlung zwischen Kassenzahnärztlichen Vereinigungen und gesetzlichen Krankenkassen erfüllt nicht die Anforderungen des Sozialgesetzbuches an diesen Datenaustausch. § 295 SGB V fordert, daß Daten nur **im erforderlichen Umfang** und **nicht versichertenbezogen** übermittelt werden dürfen.

Die Datenschutzbeauftragten begrüßen es deshalb, daß der größte Teil der gesetzlichen Krankenkassen in "Protokollnotizen" - Stand 22. März 1996 - den Umfang der zu übermittelnden Daten reduziert hat. Das Risiko der Identifizierbarkeit des Versicherten wurde dadurch deutlich verringert. Zum letztlich erforderlichen Umfang haben die Spitzenverbände der gesetzlichen Krankenkassen erklärt, daß genauere Begründungen für die Erforderlichkeit der Daten erst gegeben werden könnten, wenn das DV-Projekt für das Abrechnungsverfahren auf Kassenseite weit genug entwickelt sei.

Der Verband der Angestellten-Ersatzkassen (VdAK) hat bisher als einziger Spitzenverband der gesetzlichen Krankenkassen diese Datenreduzierungen nicht mitgetragen. Die Datenschutzbeauftragten fordern den VdAK auf, sich für die Frage der Datenübermittlung zwischen Kassenzahnärztlichen Vereinigungen und gesetzlichen Krankenkassen der einheitlichen Linie anzuschließen. Dies liegt im gesetzlich geschützten Interesse der Versicherten.

Die besonderen Vorgaben des Sozialgesetzbuches für die Prüfung der Wirtschaftlichkeit der ärztlichen Abrechnung werden dadurch nicht berührt.

Anlage 4: Entschließung der 50. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 09./10. November 1995:

Datenschutzrechtliche Anforderungen an den Einsatz von Chipkarten im Gesundheitswesen

Die Datenschutzbeauftragten des Bundes und der Länder haben auf ihrer 47. Konferenz am 09./10. März 1994 kritisch zum Einsatz von Chipkarten im Gesundheitswesen Stellung genommen. In dem Beschluß wird die Nutzung von Patientenkarten von mehreren Voraussetzungen zur Sicherung des Persönlichkeitsrechts abhängig gemacht.

Seitdem werden in mehreren Ländern Modellversuche und Pilotprojekte durchgeführt. Die Bandbreite reicht

- von allgemeinen Patientenkarten, die an möglichst viele Patienten/Versicherte ausgegeben werden, eine Vielzahl von Krankheitsdaten enthalten und von einem unbestimmten Kreis von Personen und Institutionen des Gesundheitswesens zu vielfältigen Zwecken verwendet werden können (z.B. VitalCard der AOK Leipzig, Persönliche Patientenkarte Neuwied, BKK-Patientenkarte Berlin)

- bis zu krankheitsspezifischen Karten für bestimmte Patientengruppen mit reduziertem Datensatz und einer Definition der Verwendung (z.B. Dialyse-Card, Diab-Card, Krebsnachsorgekarte, Defi-Card).

Datenschutzrechtlich stellen sich vor allem folgende Probleme:

- Die massenhafte Einführung der Karten erzeugt einen sozialen Druck auf die Betroffenen, sie mitzuführen und vorzulegen. Diesen Erwartungen wird sich der Betroffene vielfach nur unter Befremden des Arztes oder sogar der Gefahr, daß dieser die Behandlung ablehnt, verweigern können.

- Die Verwendung von allgemeinen Patientenkarten bringt die Gefahr einer pauschalen Offenbarung von medizinischen Daten mit sich.

- Dem Patienten wird die Last aufgebürdet, für die Sicherheit seiner medizinischen Daten selbst zu sorgen.

Die Datenschutzbeauftragten fordern alle für Kartenprojekte im Gesundheitswesen Verantwortlichen in Politik, Industrie, Ärzteschaft, Wissenschaft und in den Krankenversicherungen auf, das Recht auf informationelle Selbstbestimmung der betroffenen Patienten bzw. Versicherten zu gewährleisten. Die 50. Konferenz hält folgende Voraussetzungen für elementar:

1. Besondere Schutzwürdigkeit medizinischer Daten

Medizinische Daten sind besonders schutzwürdig, unabhängig davon, welche Technologien eingesetzt werden, ob die Patientendaten beim Arzt gespeichert und versandt oder über ein Netz abgerufen werden oder ob der Patient die Daten auf einer Chipkarte bei sich hat. Es handelt sich oftmals um belastende, schicksalshafte Daten. Zudem geht es nicht nur um Daten des Patienten, sondern auch um fremde Einblicke in die ärztliche Tätigkeit.

2. Wirksame Entscheidung der Betroffenen über die Verwendung einer Karte

Die freie Entscheidung der Betroffenen (Patienten/Versicherten), eine Chipkarte zu verwenden, muß gewährleistet sein. Dies umfaßt die Entscheidung,

- ob Daten auf einer Chipkarte gespeichert werden,
- welche der Gesundheitsdaten auf die Karte aufgenommen werden,
- welche Daten auf der Karte wieder gelöscht werden,
- ob die Karte bei einem Arztbesuch bzw. einem Apothekenbesuch vorgelegt wird und
- welche Daten im Einzelfall zugänglich gemacht werden.

Ein Widerruf der Entscheidung muß ohne Nachteile für die Betroffenen möglich sein. Die gleiche Freiheit der Entscheidung für oder gegen die Verwendung der Chipkarte muß für Ärzte und Apotheke gewährleistet sein. Eine wirksame Entscheidung für oder gegen die Verwendung einer Chipkarte setzt eine schriftliche, objektive, vollständige und nachvollziehbare Information über Zweck, Art, Umfang und Beteiligte der Chipkarten-Kommunikation voraus. Das Gesamtkonzept des Chipkarteneinsatzes und der damit verbundenen Datenverarbeitung muß für die Betroffenen überschaubar sein.

Auf der Karte darf nicht der Datensatz der Krankenversichertenkarte nach § 291 Abs. 2 SGB V, insbesondere nicht die Krankenversicherung und die Krankenversicherungsnummer, gespeichert werden, da andernfalls - zumal bei allgemeinen Patientenkarten mit hohem Verbreitungsgrad - die Krankenversichertenkarte verdrängt und deren Nutzungsbeschränkungen umgangen werden.

3. Freiheit der Entscheidung

Die uneingeschränkte Freiheit der Entscheidung der Betroffenen für oder gegen die Verwendung einer Chipkarte muß gewährleistet sein, denn der Einsatz von Chipkarten im Gesundheitswesen führt keineswegs zwangsläufig zu größerer Autonomie der Patienten. Neu Technologien können sich auch als Verführung erweisen, deren Preis erst langfristig erkennbar wird. Die individuelle Entscheidung des Bürgers über die Verarbeitung seiner Daten war und bleibt ein zentrales Recht gegenüber Eingriffen in seine Freiheitssphäre. Mit der Chipkarte können sich jedoch Situationen ergeben, in denen wirkliche Freiheit und tatsächliche Wahlmöglichkeit der Betroffenen nicht mehr gewährleistet sind und durch technische und organisatorische, rechtliche und soziale Rahmenbedingungen wiederhergestellt werden müssen.

Dem Staat kommt hier eine veränderte Rolle zu: Freiheitsrechte nicht einzuschränken, sondern sie zu sichern, wo Entwicklungen des Marktes und der Technologien sowie Gruppeninteressen die Entscheidungsfreiheit des Bürgers bedrohen. Die Technologie selbst kann für die Sicherung der Freiheitsrechte ein wertvolles Hilfsmittel sein. Darüber hinaus kommt der Informiertheit der Betroffenen ein zentraler Stellenwert zu. Ihre Kompetenz zur Entscheidung und zum praktischen Umgang mit der Karte muß gestärkt wer-

den, damit sie auch langfristig die größtmöglichen Chancen haben, ihre Interessen durchzusetzen.

Mit der Ausstellung der Karte dürfen nur die Vorteile verknüpft werden, die sich unmittelbar aus den Nutzungspraktiken der Karte selbst ergeben. Die freie Entscheidung der Betroffenen, eine Karte zu nutzen oder dies abzulehnen, darf nicht durch einen Nutzungszwang oder eine Bevorzugung von Karten-Nutzern (z.B. durch Bonuspunkte) bzw. von Karten-Verweigerern eingeschränkt werden.

4. Keine Verschlechterung der Situation der Betroffenen

Durch die Einführung von Kommunikationssystemen mit Chipkarten dürfen die Betroffenen nicht schlechter gestellt werden als im konventionellen Verfahren. Die medizinische Versorgung, der Schutz der Gesundheitsdaten und die Mitentscheidungsrechte der Betroffenen müssen in Umfang und Qualität erhalten bleiben.

Das therapeutische Verhältnis Arzt/Patient darf sich durch den Einsatz von Chipkarten nicht verschlechtern. Freiheit und Vertrauen innerhalb des Arzt-Patienten-Verhältnisses sowie der Grundsatz der Abschottung der dem Arzt anvertrauten Informationen und der ärztlichen Erkenntnisse nach außen, gegen die Kenntnisnahme durch Dritte, müssen erhalten bleiben. Insbesondere muß der Gesetzgeber sicherstellen, daß die auf der beim Patienten befindlichen Chipkarte gespeicherten medizinischen Daten ebenso gegen Beschlagnahme und unbefugte Kenntnisnahme geschützt sind wie die beim Arzt gespeicherten Daten. Eine Kommunikation unter Vorlage der Karte mit Personen oder Stellen außerhalb des Arzt-Patienten-Verhältnisses, z.B. Arbeitgebern oder Versicherungen, muß vom Gesetzgeber untersagt werden.

Das sich im Gespräch entwickelnde Vertrauensverhältnis zwischen Arzt und Patient darf nicht durch eine Chipkartenvermittelte Kommunikation verdrängt werden. Verkürzte Darstellungen medizinischer Sachverhalte auf der Chipkarte - z.B. mit Hilfe von Schlüsselbegriffen - dürfen nicht zu einer Minderung der Qualität des therapeutischen Verhältnisses führen; das liegt auch im Interesse des Arztes. Der Patient muß auch weiterhin die Möglichkeit des individuellen Dialogs wählen können. Dies schließt insbesondere die

Freiheit des Betroffenen ein, eine Chipkarte im Einzelfall nicht vorzulegen, auf der Chipkarte nur einen begrenzten Datensatz speichern zu lassen oder zu entscheiden, welchem Arzt welche Informationen oder Informationsbereiche offenbart werden. Der Patient darf durch die Ausgestaltung und den Verwendungszusammenhang der Chipkarte nicht zur pauschalen Offenbarung seiner Daten gezwungen sein. So sind Daten auf der Chipkarte so zu ordnen, daß z.B. beim Zahnarzt die gynäkologische Behandlung geheim bleiben kann.

Es darf keine "Einwilligung" in Chipkarten und Chipkartensysteme mit verminderter Datensicherheit geben. Der Gesetzgeber muß die Patienten vor "billigen Gesundheitskarten" ohne ausreichende Sicherung vor einer Nutzung durch Dritte schützen.

5. Sicherstellung der Integrität und Authentizität der Daten

Zur Sicherstellung der Vertraulichkeit, Integrität und Authentizität der Daten auf Chipkarten im Gesundheitswesen und zur Differenzierung der Zugriffsmöglichkeiten nach dem Grundsatz der Erforderlichkeit in unterschiedlichen Situationen sind kryptographische Verfahren sowie geeignete Betriebssysteme zur Abschottung unterschiedlicher Anwendungsbereiche nach dem Stand der Technik in Chipkarten und Schreib/Lese-Terminals zu implementieren. Eine Protokollierung der Lösch- und Schreibvorgänge auf der Karte ist unverzichtbar.

Darüber hinaus ist für das infrastrukturelle Kartenumfeld (Herstellung, Verteilung, Personalisierung, Rücknahme) sicherzustellen, daß ausreichende technische und organisatorische Maßnahmen Berücksichtigung finden. Für die zur Erstellung und Personalisierung von Gesundheits-Chipkarten dienenden Systeme sowie die informationstechnischen Systeme und Verfahren, mit denen Daten auf der Chipkarte gelesen, eingetragen, verändert, gelöscht oder verarbeitet werden, muß der gleiche hohe Sicherheitsstandard erreicht werden.

6. Keine neuen zentralen medizinischen Datensammlungen

Der Einsatz von Chipkarten im Gesundheitswesen darf nicht zur Entstehung neuer zentraler Dateien von Patientendaten bei Kassenärztlicher Vereinigung, Krankenkassen, Kartenherstellern oder sonstigen Stellen führen. Dies gilt auch für das Hinterlegen von Sicherungskopien der auf der Karte gespeicherten medizinischen Daten. Es steht in der freien Entscheidung der Betroffenen, ob sie dem Arzt ihres Vertrauens eine umfassende Pflege aller Chipkarten-Daten - einschließlich der Sicherungskopien - übertragen oder nicht.

7. Leserecht des Karteninhabers

Der Karteninhaber muß das Recht und die Möglichkeit haben, seine auf der Chipkarte gespeicherten Daten vollständig zu lesen.

8. Suche nach datenschutzfreundlichen Alternativen

Angesichts der aufgezeigten Gefährdungen der informationellen Selbstbestimmung im Gesundheitswesen muß die Suche nach datenschutzrechtlichen Alternativen zur Chipkarte fortgesetzt werden.

Vorstehende Kriterien sind der Maßstab für die datenschutzrechtliche Bewertung von Projekten für die Einführung von Chipkarten im Gesundheitswesen.

Die Datenschutzbeauftragten von Bund und Ländern fordern die Gesetzgeber auf, die dringend notwendigen Regelungen zur Sicherung der Rechte von Patienten und Ärzten zu schaffen. Ebenso ist durch die Gesetzgeber den Besonderheiten der Datenverarbeitung auf Chipkarten durch bereichsspezifische Regelungen Rechnung zu tragen.

Anlage 5: Entschließung der 50. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 09./10. November 1995:

Forderungen an den Gesetzgeber zur Regelung der Übermittlung personenbezogener Daten durch die Ermittlungsbehörden an die Medien (außerhalb der Öffentlichkeitsfahndung der Ermittlungsbehörden)

1. Für die Übermittlung von personenbezogenen Daten durch Justiz und Polizei an die Medien sollte eine bereichsspezifische Rechtsgrundlage geschaffen werden. Die Regelung sollte für den betroffenen Bürger den Umfang des Eingriffs in sein Recht auf informationelle Selbstbestimmung erkennbar machen.

2. Die Übermittlung personenbezogener Daten an die Medien ist nur ausnahmsweise gerechtfertigt, wenn das Verfahren gerade im Hinblick auf die Person des Betroffenen oder die besonderen Umstände der Tat für die Öffentlichkeit von überwiegendem Interesse ist.

3. Bei der Entscheidung, ob und in welchem Umfang personenbezogene Daten an die Medien übermittelt werden, sind die schutzwürdigen Belange der Betroffenen zu berücksichtigen. Dazu zählen insbesondere die privaten und beruflichen Folgen für das Opfer, den Beschuldigten/Angeklagten und deren Angehörige, die Schwere, die Umstände und die Folgen des Delikts.

Bei der Übermittlung von personenbezogenen Daten über Beschuldigte/Angeklagte sind auch der Grad des Tatverdachts und der Stand des Verfahrens zu berücksichtigen. Vor Beginn der öffentlichen Hauptverhandlung ist ein besonders strenger Maßstab an das Vorliegen eines "überwiegenden Interesses" der Öffentlichkeit anzulegen.

Bis zur rechtskräftigen Verurteilung ist die Unschuldsvermutung zugunsten des Beschuldigten oder Angeklagten zu beachten. Zu unterlassen sind alle Auskünfte oder Erklärungen, die geeignet sind, die Unbefangenheit der Verfahrensbeteiligten zu beeinträchtigen. Akteneinsicht durch Medienvertreter kommt nicht in Betracht.

4. Grundsätzlich sind in Auskünfte und Erklärungen über das Ermittlungs- und Strafverfahren keine Namen und sonstige personenbezogene Angaben, die Opfer von Straftaten, Zeugen, Beschuldigte und Angeklagte bestimmbar machen, aufzunehmen. Vor allem bei Hinweisen auf den Wohnort, das Alter, den Beruf und die familiären Verhältnisse oder sonstigen sozialen Bindungen (z.B. Partei- oder Vereinsmitgliedschaft) ist zu prüfen, inwieweit dadurch eine Identifizierung des Betroffenen möglich wird.

5. Personenbezogene Daten dürfen nicht übermittelt werden, wenn besondere bundesgesetzliche oder landesgesetzliche Verwendungsregelungen entgegenstehen.

6. Ist die Bekanntgabe der Person des Beschuldigten oder Angeklagten wegen des überwiegenden öffentlichen Interesses gerechtfertigt, muß auch bei der Übermittlung sonstiger personenbezogener Daten abgewogen werden, ob diese Informationen für die Berichterstattung über die Tat selbst oder die Hintergründe, die zu der Tat geführt haben, erforderlich sind, und in welchem Umfang der Betroffene dadurch in seinem Persönlichkeitsrecht beeinträchtigt wird.

7. Die Bekanntgabe von Vorstrafen ist nur ausnahmsweise zulässig. Sie setzt voraus, daß die frühere Verurteilung im Bundeszentralregister noch nicht getilgt und ihre Kenntnis für eine nachvollziehbare Berichterstattung über eine schwerwiegende Straftat - auch unter Berücksichtigung des Persönlichkeitsrechts des Betroffenen und des Resozialisierungsgedankens - erforderlich ist. Besondere Zurückhaltung ist bei Auskünften und Erklärungen über Sachverhalte geboten, die der früheren Verurteilung zugrunde liegen.

8. Wegen des überragenden Schutzes von Minderjährigen und Heranwachsenden ist bei Auskünften und Erklärungen über Verfahren gegen diesen Personenkreis besondere Zurückhaltung hinsichtlich der Bekanntgabe personenbezogener Daten zu wahren.

9. Opfer, Zeugen und Familienangehörige haben in der Regel keine Veranlassung gegeben, daß ihre persönlichen Lebensumstände in der Öffentlichkeit bekannt gemacht werden. Die Übermittlung personenbezogener Daten über diesen Personenkreis an die Medien kommt deshalb grundsätzlich nicht in Betracht.

---

10. Bildveröffentlichungen greifen wegen der damit verbundenen sozialen Prangerwirkung besonders tief in das Persönlichkeitsrecht des Betroffenen ein. Eine Bildherausgabe kommt daher für Zwecke der Medienberichterstattung nicht in Betracht.

Anlage 6: Entschließung der 49. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 09./10. März 1995:

Aufbewahrungsbestimmungen und Dateiregelungen im Justizbereich

Bisher ist der Gesetzgeber im Bereich der Justiz den verfassungsrechtlichen Forderungen nach ausreichenden normenklaren Regelungen über die Aufbewahrung von Akten und die Speicherung personenbezogener Daten in Dateien nicht nachgekommen. So enthalten z.B. die bislang bekannt gewordenen Entwürfe zu einem Strafverfahrensänderungsgesetz nur unzureichende Generalklauseln. Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder erklärt deshalb:

1. Aufbewahrung, Aussonderung und Vernichtung der Akten und die Speicherung personenbezogener Daten in Dateien im Bereich der Justiz müssen nach den Grundsätzen des Bundesverfassungsgerichts im Volkszählungsurteil für die Gerichte, Staatsanwaltschaften und Strafvollzugsbehörden gesetzlich geregelt werden, wobei sich die Aufbewahrungsdauer am Recht auf informationelle Selbstbestimmung und am Zweck der Speicherung zu orientieren hat.

   Hierbei hat der Gesetzgeber die grundlegenden Entscheidungen zur Aufbewahrungsdauer selbst zu treffen. Aufgrund einer hinreichend konkreten Verordnungsermächtigung können die Einzelheiten durch Rechtsverordnung bestimmt werden.

2. Die derzeit bestehenden Aufbewahrungsfristen sind konsequent zu vereinfachen und zu verkürzen. Soweit geboten, sind Verkürzungen vorzunehmen.

3. Die derzeit geltende generelle 30-jährige Aufbewahrungsfrist für Strafurteile und Strafbefehle mit der Folge der umfassenden Verfügbarkeit der darin enthaltenen Informationen ist nicht angemessen. Bei der Bemessung der Aufbewahrungsfrist von Strafurteilen und Strafbefehlen sowie für die Bestimmung des Zeitpunkts der Einschränkung der Verfügbarkeit ist vielmehr nach Art und Maß der verhängten Sanktionen zu differenzieren.

   Bei der Festlegung des Beginns der Aufbewahrungsfrist sollte - abweichend von der bis-

herigen Praxis, nach der es auf die Weglegung der Akte ankommt - regelmäßig auf den Zeitpunkt des Eintritts der Rechtskraft der ergangenen gerichtlichen Entscheidung abgestellt werden.

Ergeht keine rechtskräftige Entscheidung, so sollte die Aufbewahrungsfrist mit dem Erlaß der Abschlußverfügung beginnen.

4. Wird der Akteninhalt auf Bild- oder Datenträgern, die an die Stelle der Urschrift treten, aufbewahrt, so sind gleichwohl unterschiedliche Löschungsfristen für einzelne Aktenteile zu beachten. Aus datenschutzrechtlicher Sicht sind Datenträger zu wählen, die eine differenzierte Löschung gewährleisten. Ist bei Altbeständen eine teilweise Aussonderung technisch nicht möglich oder nur mit unverhältnismäßigem Aufwand zu bewerkstelligen, so hat eine Sperrung der an sich auszusondernden Teile zu erfolgen.

5. Sind in einer Akte Daten mehrerer beteiligter Personen gespeichert, so ist eine Sperre hinsichtlich solcher Aktenteile, die einzelne beteiligte Personen betreffen, vorzusehen, wenn diese Aktenteile eigentlich ausgesondert werden müßten, aus praktischen Gründen aber keine Vernichtung erfolgen kann.

6. Bei Freisprüchen und Einstellungen des Verfahrens wegen Wegfalls des Tatverdachts ist dafür Sorge zu tragen, daß ein Zugriff auf die automatisiert gespeicherten Daten nur noch zu Zwecken der Aktenverwaltung erfolgen kann.

7. Für die Daten von Nebenbeteiligten (z.B. Anzeigeerstatter, Geschädigte) ist eine vorzeitige Löschung vorzusehen. Hinsichtlich der Hauptbeteiligten sollte eine Teillöschung der Personen- und Verfahrensdaten stattfinden, sobald die vollständigen Daten zur Durchführung des Verfahrens nicht mehr erforderlich sind.

8. Soweit Daten verschiedener Gerichtszweige oder verschiedener speichernder Stellen in gemeinsamen Systemen verarbeitet werden, ist durch rechtliche, technische und organisatorische Maßnahmen sicherzustellen, daß die Zweckbindung der gespeicherten Daten beachtet wird.

Anlage 7: Entschließung der Datenschutzbeauftragten des Bundes und der Länder vom 9. Mai 1996:

Forderungen zur sicheren Übertragung elektronisch gespeicherter personenbezogener Daten

Der Schutz personenbezogener Daten ist während der Übertragung oder anderer Formen des Transportes nicht immer gewährleistet. Elektronisch gespeicherte, personenbezogene Daten können sowohl auf leitungsgebundenen oder drahtlosen Übertragungswegen als auch auf maschinell lesbaren Datenträgern weitergegeben werden. Oft sind die Eigenschaften des Transportweges dem Absender und dem Empfänger weder bekannt noch durch sie beeinflußbar. Vor allem die Vertraulichkeit, die Integrität (Unversehrtheit) und die Zurechenbarkeit der Daten (Authentizität) sind nicht sichergestellt, solange Manipulationen, unbefugte Kenntnisnahme und Fehler während des Transportes nicht ausgeschlossen werden können. Die Verletzung der Vertraulichkeit ist möglich, ohne daß Spuren hinterlassen werden.

Zahlreiche Rechtsvorschriften gebieten, das Grundrecht auf informationelle Selbstbestimmung auch während der automatisierten Verarbeitung personenbezogener Daten zu sichern (z.B. § 78a SGB X mit Anlage, § 10 Btx-Staatsvertrag, § 9 BDSG nebst Anlage und entsprechende landesgesetzliche Regelungen).

Kryptographische Verfahren (z.B. symmetrische und asymmetrische Verschlüsselungsverfahren, digitale Signatur) sind besonders geeignet, um Verletzungen des Datenschutzes beim Transport schutzwürdiger elektronisch gespeicherter Daten zu verhindern. Mit ihrer Hilfe lassen sich Manipulationen und Übertragungsfehler nachweisen und unberechtigte Kenntnisnahme verhindern. Derartige Verfahren sind heute Stand der Technik und können in vielen Anwendungsfällen mit vertretbarem Aufwand eingesetzt werden.

Angesichts der beschriebenen Situation und der vorhandenen technischen Möglichkeiten fordern die Datenschutzbeauftragten des Bundes und der Länder geeignete, sichere kryptographische Verfahren beim Transport elektronisch gespeicherter personenbezogener Daten unter Berücksichtigung ihrer Schutzwürdigkeit anzuwenden.