**Bayerischer Landtag** · 9. Wahlperiode

DRUCKSACHE 9 / **11712**

04. 05. 82

**Der Landesbeauftragte für den Datenschutz**
Nr. DSB/1 – 510 – 5

München, den 4. Mai 1982

An den
Herrn Präsidenten
des Bayerischen Landtags
München

Betreff: **Vierter Bericht über die Tätigkeit des Landesbeauftragten für den Datenschutz**

Sehr geehrter Herr Landtagspräsident!

Anliegend übersende ich gemäß Art. 28 Abs. 4 des Bayerischen Gesetzes zum Schutz vor Mißbrauch personenbezogener Daten bei der Datenverarbeitung vom 28. April 1978 den vierten Tätigkeitsbericht für den Zeitraum vom 1. Januar bis 31. Dezember 1981.

Der Beirat hat den Entwurf in seiner Sitzung am 20. April 1982 vorberaten.

Mit vorzüglicher Hochachtung

**Dr. Stollreither**

# Vierter Tätigkeitsbericht des Landesbeauftragten für den Datenschutz

Berichtszeitraum: 1. Januar bis 31. Dezember 1981

Inhaltsübersicht

## 1. Vorbemerkungen

### 1.1 Zur Lage

Der nach Art. 28 Abs. 4 BayDSG alljährlich dem Landtag und der Staatsregierung vom Landesbeauftragten für den Datenschutz zu erstattende Bericht über seine Tätigkeit zwingt nicht nur dazu, über die im abgelaufenen Jahr geleistete Arbeit Rechenschaft abzulegen, sondern auch die eigene Position zu überdenken. Dies ist um so bedeutsamer, als der Datenschutz noch immer eine relativ „neue Einrichtung" ist, also weder im Bewußtsein der Öffentlichkeit noch in der Verwaltung zur Selbstverständlichkeit geworden ist. Immerhin ist er – das stelle ich gerne fest – keine Modeerscheinung mehr, im Gegenteil, manche Kritik der Presse, der Verwaltung und in einigen Bundesländern auch der Parlamente hat deutlichere Formen angenommen. Dies ist, wie ich glaube, bei einer nüchternen Betrachtung der Aufgabe und Stellung des Datenschutzes im Staate auch verständlich, legt aber dennoch die Frage nahe, ob das Verhalten von „Datenschützern" immer sachgerecht genug und für „Nichtdatenschützer" auch verständlich war.

Wie wenig der Bürger noch immer mit den Datenschutzgesetzen „zurechtkommt", erlebe ich täglich. Doch wird aus diesen Anfragen und Beschwerden ein wachsendes Datenschutzbewußtsein deutlich. Ein Teil unserer Mitbürger vermag dem Datenschutz allerdings nach wie vor keine nützliche Seite abzugewinnen. Mancher meint, daß er ja „nichts zu verbergen" habe und „seine Daten jeder kennen" dürfe. Ein Verständnis für den Sinn des Datenschutzes entwickelt der Einzelne vielfach erst dann, wenn er sich zum Beispiel im Zuge einer Rasterfahndung in den Datensammlungen der Polizei gespeichert weiß, weil er etwa einen Pkw eines bestimmten Fabrikats und einer bestimmten Farbe fährt und in einer Gegend wohnt, in der ein Kapitalverbrechen aufzuklären ist. Unbehagen überkommt den Bürger aber auch dann, wenn er eine Flut von Werbesendungen erhält und sich nicht erklären kann, „woher die Firmen seine Adresse haben". Hier fällt der Verdacht einer unzulässigen Datenweitergabe meist zunächst auf eine öffentliche Stelle, die aber in der Regel nicht die Quelle ist.

Mißmut der Verwaltung rührt wohl gelegentlich daher, daß sie sich in Datenschutzfragen zu Unrecht verdächtigt fühlt. Datenschutz erscheint ihr oftmals überflüssig, da mit Akten von jeher ordnungsgemäß umgegangen werde und der Zugriff zu automatisiert gespeicherten Daten schon rein technisch nur einem begrenzten und dienstlich verpflichteten Personenkreis möglich sei.

Im Berichtsjahr festgestellte Verstöße gegen Bestimmungen des Datenschutzes beruhten durchwegs auf Unbedachtheit, Gutgläubigkeit oder Unkenntnis. Es ist auch darauf hinzuweisen, daß in aller Regel nicht bekannt ist, an welchen Stellen, aus welchen Gründen und mit welchen Mitteln irgend jemand rechtswidrig von öffentlichen Dienststellen gespeicherte Daten in Erfahrung bringen will. Die mögliche Einbruchstelle ist nicht vorherzusehen. Daher müssen Schutzmaßnahmen „rundum" wirksam sein, um jeder Möglichkeit eines rechtswidrigen Eingriffs begegnen zu können.

Daraus ergeben sich als vereinfachte Grundregeln:

- Nur was für die Arbeit der Verwaltung wirklich erforderlich ist, darf sie erfassen, speichern und übermitteln.
- Zugang zu Daten darf nur erhalten, wer diese Daten zu seiner rechtmäßigen Arbeit braucht.
- Für den Bürger muß erkennbar sein, was mit seinen Daten geschieht.

Die Presse ist sicher ein wichtiger Verbündeter des Datenschutzes, da sie auf Probleme und Gefahren hinweist, freilich mit dem Ergebnis, daß ihre Veröffentlichungen sich häufig nur mit den aufgetretenen Fehlern und Mißständen befassen, was zu Veralgemeinerungen führen kann. So entsteht nicht selten in der Öffentlichkeit ein schiefes Bild.

Häufig überschätzt die Öffentlichkeit auch die Gefahren, die sich aus der Automatisierung von Datensammlungen ergeben. Es ist daher auch Aufgabe des Datenschutzes, übertriebenen Ängsten entgegenzutreten.

Ein weiterer Faktor, der für den Datenschutz zunehmend spürbar wird, ist der in der Öffentlichkeit hervorgerufene Eindruck, Datenschutz behindere die Arbeit der für die öffentliche Sicherheit verantwortlichen Organe. Dem trete ich entschieden entgegen. Auch die Sicherheitsbehörden haben die Grundsätze der Verfassung, alle übrigen Gesetze, und nicht zuletzt die Strafprozeßordnung zu beachten. Gerade die Strafprozeßordnung setzt hier hinsichtlich der Sammlung und Verwertung von Daten durch die Strafverfolgungsbehörden deutliche Grenzen. Eine wesentliche Änderung dieses in seinen Kernbestimmungen aus dem letzten Jahrhundert stammenden, also vom modernen Datenschutz noch unberührten Gesetzes, werden auch die Kritiker des Datenschutzes in Sicherheitsfragen nicht ernsthaft wünschen.

Ich habe, und das ist auch an dieser Stelle zu betonen, von den Sicherheitsorganen bisher Unterstützung und auch Verständnis erfahren. Zu den Begrenzungen, die sich die Sicherheitsorgane in Bayern bezüglich ihrer Sammlungen auferlegt haben, verweise ich auf Abschnitt 3.2.

Datenschutz, wie er sich mir heute darstellt, steht inmitten von Spannungsfeldern und damit Bewährungsproben, die sich nur durch intensiven Dialog mit Bürgern und Verwaltung bewältigen lassen.

### 1.2 Behandlung des 3. Tätigkeitsberichts in Parlament, Presse und Öffentlichkeit

Der von mir für das Jahr 1980 erstattete Tätigkeitsbericht wurde im Ausschuß für Verfassungs-, Rechts- und Kommunalfragen des Landtags und im Rechts- und Verfassungsausschuß des Senats eingehend und zustimmend erörtert. Auch die Aufnahme in der Presse war durchwegs positiv, wenngleich sich hier auch kritische Stimmen fanden. Von Bürgern erhielt ich eine Reihe von Zuschriften. Die Aufnahme des Tätigkeitsberichts – wie alle Kritik am Datenschutz – ist Anlaß zu ernster Prüfung und Überlegungen, ist doch der eigene Lernprozeß ein wesentlicher Faktor bei der Weiterentwicklung des Datenschutzes.

### 1.3 Aufbau des vierten Tätigkeitsberichts

Der vorliegende Tätigkeitsbericht hebt als besonderen Schwerpunkt „Technische und organisatorische Datenschutzfragen" hervor, denen für die Verwaltungspraxis große, bei den Datenschutzdiskussionen häufig nicht genügend gewürdigte Bedeutung zukommt. Daneben wird auch über die „Neuen Medien" verhältnismäßig ausführlich berichtet.

Im dritten Abschnitt des Tätigkeitsberichts werden in großem Umfang Einzelfälle erörtert. Ihre Behandlung in dieser Form rechtfertigt sich m. E. dadurch, daß aus ihnen Rückschlüsse für die Verwaltung aus den praktischen datenschutzrechtlichen Problemstellungen möglich sind und die Verwaltung gerade die einzelnen Lösungsfälle heranziehen kann, um ähnliche Probleme zu lösen. Aus der Gesamtschau ergibt sich, wie ich glaube, ein anschauliches Bild über die aktuellen Fragen und die Reaktion der Verwaltung auf meine Vorstellungen zum Datenschutz.

### 1.4 Die Geschäftsstelle

#### Unterbringung

Im Berichtsjahr befand sich die Geschäftsstelle noch in den gleichen Räumen, die sie bei der Aufnahme ihrer Tätigkeit im Sommer 1978 bezogen hatte. Wenn sich auch der Personalstand nur in bescheidenem Maße erweiterte – siehe unten – so ergab sich doch 1981 eine immer spürbarer werdende bedrängende Enge, die die Arbeitsbedingungen der Mitarbeiter zunehmend in Mitleidenschaft zog. So mußten Geräte und Maschinen, z.B. der Drucker zum Schreibautomaten, in Arbeitsräumen untergebracht werden. Gegen Ende des Jahres mußte daher der Umzug in andere Räume vorbereitet werden, da sich im Gebäude Königinstraße 11 keine Erweiterungsmöglichkeit bot. Die Verlegung in die Wagmüllerstraße 18, die eine geschlossene Unterbringung in einem Stockwerk ermöglichte, erfolgte gleich zu Beginn des Jahres 1982.

Haushalt – Personal

Der Staatshaushalt 1981/82 sah für die Geschäftsstelle des Landesbeauftragten für das Haushaltsjahr 1981 eine Erweiterung um 3 Stellen des höheren Dienstes, 2 Stellen des gehobenen Dienstes, 1 Stelle des mittleren Dienstes und 1 Angestelltenstelle vor, von denen jedoch zwei Stellen meiner Dienststelle bereits leihweise zur Verfügung gestellt und besetzt worden waren (siehe Tätigkeitsbericht 1980 unter 1.2.2).

Da die für das Haushaltsjahr 1981 ausgebrachten neuen Stellen aufgrund des Haushaltsgesetzes erst ab Mitte 1982 besetzbar sind, konnte die Geschäftsstelle im Jahre 1981 nur durch einen Beamten des gehobenen Dienstes verstärkt werden. Auch bei der Besetzung dieser Stelle war ich darauf bedacht, einen Mitarbeiter zu gewinnen, der die Gegebenheiten und Erfordernisse der Verwaltungspraxis durch Tätigkeit in der bayerischen Verwaltung kennt. Auch nach Besetzung der im Haushalt 1981/82 neu ausgebrachten Stellen wird die Personalausstattung meiner Dienststelle vergleichsweise bescheiden sein. Eine weitere Personalvermehrung wird, sofern sich die Arbeitsanforderungen nicht wesentlich ändern, zunächst nicht angestrebt.

Insgesamt ergab sich auch 1981 wie in den Vorjahren eine über das normale Maß erheblich hinausgehende Belastung meiner Mitarbeiter, die zudem – wie dargelegt – unter teilweise räumlich ungünstigen Verhältnissen erbracht wurde. Sie konnte dank der Einsatzbereitschaft meiner Mitarbeiter durch dauernde Leistung erheblicher Überstunden und Wochenendarbeit durchgestanden werden. Die Besetzung der noch offenen Stellen durch qualifiziertes, praxiserfahrenes Personal ist dringend geboten. Die für das Haushaltsjahr 1981 veranschlagten Sachmittel entsprechen dank der weitgehenden gegenseitigen Deckungsfähigkeit den Anforderungen.

An Informationsmaterial wurden 1981 über 2600 Broschüren „Der Bürger und seine Daten", über 500 Übersichten über das Datenschutzregister, fast 4000 Tätigkeitsberichte von 1979 und 1980 und über 2200 Textsammlungen „Bayerisches Datenschutzgesetz, Datenschutzregisterverordnung und Bundesdatenschutzgesetz" versandt.

Datenschutzregister

Im Berichtszeitraum wurde der Aufbau des Datenschutzregisters weitergeführt. Bei Redaktionsschluß der als Beilage zum Bayerischen Staatsanzeiger Nr. 47/1981 am 20. November 1981 erschienenen „Übersicht" waren zum Datenschutzregister 11318 Dateien von insgesamt 3383 speichernden Stellen gemeldet. Gegenüber der Veröffentlichung des Vorjahrs bedeutet dies eine Zunahme bei den Dateien um 12 Prozent und bei den speichernden Stellen um 11 Prozent. Beim Vergleich mit den Zahlen für 1979 ist eine Zunahme der gemeldeten Dateien um insgesamt 36 Prozent festzustellen. Besonders auffallend war die Zunahme der Dateien und speichernden Stellen im kommunalen Bereich. Auch aus dem Bereich der nichtstaatlichen öffentlichen Stellen, insbesondere der Allgemeinen Ortskrankenkassen und der Industrie- und Handelskammern, gingen zahlreiche Meldungen ein. Weniger zahlreich waren die Zugänge aus dem staatlichen Bereich.

Bei den im Berichtszeitraum erstmals gemeldeten automatisierten Verfahren war wieder eine beträchtliche Anzahl von Verfahren, die bereits seit einigen Jahren eingesetzt sind und schon früher hätten gemeldet werden müssen. Die Zunahme der Meldungen kann deshalb nicht einer Zunahme des Automatisierungsgrades gleichgesetzt werden.

1.5 Der Beirat

In der Besetzung des Beirats beim Landesbeauftragten für den Datenschutz trat folgende Änderung ein:

Der Bayerische Senat wählte anstelle des aus dem Senat ausgeschiedenene Senators Dr. Friedrich Wilhelm zum Mitglied des Beirats beim Landesbeauftragten für den Datenschutz Senator Wolfgang Burnhauser und als dessen Stellvertreter Senator Otto Neukum.

Da der bisherige Vertreter der Staatsregierung im Beirat beim Landesbeauftragten für den Datenschutz, Ministerialdirigent Dr. Hubert Mennacher aus dem Beirat ausschied, hat die Bayerische Staatsregierung Ministerialdirigent Hubert Kranz vom Bayerischen Staatsministerium der Finanzen als Mitglied des Beirats bestellt.

Danach sind gegenwärtig Mitglieder des Beirats und deren Stellvertreter:

Die Landtagsabgeordneten:

| | |
|---|---|
| Hermann Regensburger | Dr. Paul Wilhelm |
| Hans Spitzner | Manfred Humbs |
| Hermann Leeb | Johann Böhm |
| Eduard Hartmann | Alfred Sommer |
| Klaus Warnecke | Rolf Langenberger |
| Dr. Gerhard Zech | Peter Hürner |

Die Senatoren:

| | |
|---|---|
| Wolfgang Burnhauser | Otto Neukum |

Für die Staatsregierung:

| | |
|---|---|
| Ministerialdirigent<br>Hubert Kranz<br>Bayer. Staatsministerium<br>der Finanzen | Ministerialdirigent<br>Joachim Schweinoch<br>Bayer. Staatsministerium<br>des Innern |

Für die kommunalen Spitzenverbände:

| | |
|---|---|
| Dr. Georg Wilhelm<br>Geschäftsleitender Direktor<br>der Anstalt für Kommunale<br>Datenverarbeitung<br>in Bayern | Klaus Eichhorn<br>Ltd. Verwaltungsdirektor<br>Anstalt für Kommunale<br>Datenverarbeitung<br>in Bayern |

Für die Sozialversicherungsträger:

| | |
|---|---|
| Erster Direktor<br>Franz-Martin Fehn<br>Landesversicherungsanstalt<br>Oberfranken und Mittelfranken | Verwaltungsdirektor<br>Herbert Schmaus<br>Landesverband der Orts-<br>krankenkassen in Bayern |

Für den Verband der Freien Berufe in Bayern e.V.:

| | |
|---|---|
| Dr. med. H. Braun<br>Präsident des Verbandes<br>Freier Berufe in Bayern e.V. | Winfried Wachter<br>Präsidiumsmitglied des<br>Verbandes Freier Berufe<br>in Bayern e.V. |

Der Beirat tagte im Berichtsjahr fünfmal am 27. Januar, 10. März, 19. Mai, 14. Juli und 3. November 1981. Dabei befaßte er sich im wesentlichen mit folgenden Fragen:

- Unterrichtung über Beanstandungen unzureichender technisch-organisatorischer Datensicherungsmaßnahmen,
- Unterrichtung über Wirkungsweise und Anwendungsfälle neuer Medien, wie Videotext, Bildschirmtext, Kabeltext, Kabelfernsehen, Satellitenfernsehen, Rückkanal und die Forderungen, die aus der Sicht des Datenschutzes in Anbetracht der neuen Möglichkeiten, beispielsweise Interessenprofile über die Benutzer zu speichern und zu verwerten, aufgestellt werden müssen,
- Personalhaushalt der Geschäftsstelle, vor allem Forderungen zum Haushaltsplan 1981/82,
- Überarbeitung der Vorschriften über die „Mitteilung in Strafsachen – MiStra –" und der Richtlinien über Kriminalpolizeiliche Sammlungen (KpS),
- Unterrichtung durch den Technischen Überwachungsverein Bayern e.V. (TÜV), über dessen Vorgehensweise und bisherige Erfahrungen bei der Prüfung von Datensicherungsmaßnahmen im Auftrag der Datenschutzaufsichtsbehörden für den nichtöffentlichen Bereich, sowie zu Überlegungen über die Typ-Prüfung von DV-Systemen aus der Sicht des BDSG,
- Vorberatung des 3. Tätigkeitsberichts des Landesbeauftragten für den Datenschutz gemäß Art. 28 Abs. 4 und 6 BayDSG,
- Unterrichtung über datenschutzrechtliche Prüfungen im Krankenhausbereich, bei Polizei und Staatsanwaltschaften sowie bei Gemeinden und Landratsämtern,
- Unterrichtung zur Handhabung der „Schülergesundheitsbogen" in einigen Gymnasien,
- Unterrichtung durch das Bayerische Staatsministerium des Innern zur internen Überprüfung der Sammlung personenbezogener Daten bei der bayerischen Polizei,
- Überprüfung der Praxis der Datenübermittlung aus polizeilichen Unterlagen an die Staatsanwaltschaft und aus Akten der Staatsanwaltschaft an Rechtsanwälte, Versicherungen u.ä. (Auftrag des Beirats an den Landesbeauftragten),
- Unterrichtung über Fernwartung von DV-Anlagen aus der Sicht des Datenschutzes,
- Vorstellung der Grundzüge des künftigen Melderechts durch das Bayerische Staatsministerium des Innern,
- Bekanntgabe von Angaben über Prüflinge der Akademie der bildenden Künste an einen Ausschuß des Bayerischen Landtags,
- neutrale Gestaltung von Schulausweisen für Sonderschüler,
- Unterrichtung zur Übergangsfrist gemäß Art. 37 Abs. 3 Satz 1 BayDSG.

In seiner Sitzung am 10. März 1981 beschloß der Beirat auf Antrag des Vertreters der Staatsregierung, daß jeweils nach Erstellung des Beiratsprotokolls der Vorsitzende zusammen mit dem Landesbeauftragten für den Datenschutz festlegt und kenntlich macht, welche Teile des Beiratsprotokolls von den Beiratsmitgliedern an die verschiedenen Bereiche ihrer entsendenden Stellen weitergegeben werden dürfen, und über welche gem. Art. 29 Abs. 6 BayDSG Verschwiegenheit zu bewahren ist.

Zum Beirat siehe im übrigen in den Tätigkeitsberichten I unter 1.4, II unter 1.3 und III unter 1.2.1.

### 1.6 Zusammenarbeit mit anderen Stellen, Teilnahme an Kongressen und Seminaren

#### Konferenz der Datenschutzbeauftragten

Die Konferenz der Datenschutzbeauftragten der Länder und des Bundes, die im Jahre 1980 in München getagt hat, beriet im Berichtsjahr in Berlin. In den Tagungen am 2. April, 28./29. September und 14. Dezember 1981 wurden alle wesentlichen gemeinsam interessierenden Fragen erörtert. Beispielhaft zu nennen sind die gemeinsam erarbeiteten Stellungnahmen zum „Formulierungsvorschlag für ein Landesmeldegesetz", zum Musterentwurf für ein Krebsregister sowie zur Auslegung des SGB X und zu technischen und organisatorischen Fragen.

Die Landesbeauftragten haben sich auch mit dem Problem befaßt, daß die zum Teil schon seit Jahren bestehenden On-line-Anschlüsse anderer Behörden an automatisierte Einwohnermelderegister oder Kfz-Zulassungsdateien mit Regelungen der Datenschutzgesetze formal schwer zu vereinbaren sind. Sie haben einen Vorschlag zur Neufassung der entsprechenden Vorschriften des Datenschutzrechts entwickelt, der die Notwendigkeit solcher Anschlüsse im Grundsatz anerkennt und andere materielle und verfahrensmäßige Kriterien für ihre Zulassung enthält (s. Anhang 1).

#### Kongresse und Seminare

Die Teilnahme an allgemeinen Kongressen über den Datenschutz wurde auf die wesentlichsten Veranstaltungen begrenzt, an denen, je nach Themenstellung ich selbst und Mitarbeiter meiner Dienststelle teilnahmen. Wie in den letzten Jahren wurden dabei auch Fragen des Datenschutzes im nichtöffentlichen Bereich berücksichtigt, da die Probleme da wie dort sehr ähnlich sind.

Besonderes Augenmerk legte ich auf die Beteiligung an den Arbeitsgruppen „Datenschutz" in den Anwendervereinigungen SCOUT (Siemens Computer User Team) und GUIDE (Guidance for Users Integrated Dataprocessing Equipment, hauptsächlich IBM-Anwender) und an Veranstaltungen von Computer-Herstellern. Wirksamer Datenschutz und Datensicherung setzen bezüglich technischer und organisatorischer Maßnahmen umfassende Kenntnisse von Hardware und Software der EDV-Produzenten voraus. Zuverlässiges Wissen meiner Mitarbeiter auf diesem Gebiet scheint mir daher unabdingbare Voraussetzung für

sinnvolle Beratungs- und Kontrolltätigkeit im technischen und organisatorischen Bereich.

**2. Grundsätzliche Fragen**

2.1 Entwicklung des Datenschutzrechts

Eine Änderung des Bayerischen Datenschutzgesetzes erfolgte im Berichtsjahr ebensowenig wie die seit Jahren diskutierte Novellierung des Bundesdatenschutzgesetzes. Wenn auch bezüglich des Bayerischen Datenschutzgesetzes Vorstellungen bestehen, in welchen Fragen eine Änderung des geltenden Gesetzeswortlauts erwogen werden könnte, so besteht doch kein Zweifel, daß an eine solche erst nach einer Novellierung des Bundesdatenschutzgesetzes gedacht werden kann.

An der Diskussion über eine Änderung und Ergänzung des Bundesdatenschutzgesetzes habe ich mich bisher wenig beteiligt, einige Gedanken finden sich in meinem letzten Tätigkeitsbericht (S. 5ff.). Nach wie vor halte ich es für geboten, die Novellierung ohne Zeitdruck und nach reiflichen Überlegungen zu diskutieren; ich halte sie nicht für vordringlich und glaube, daß der Vollzug der bisherigen Gesetzesfassung noch nicht genügend zufriedenstellt und noch nicht genügend Erfahrungen gebracht hat, um eine grundlegende Überarbeitung in Angriff nehmen zu können. Auch sollte die Verwaltung, in die das geltende Datenschutzrecht (BDSG und BayDSG) noch nicht genügend Eingang gefunden hat, nicht allzubald mit einer neuen Rechtslage konfrontiert werden. Ein warnendes Beispiel sind meines Erachtens die neuen dem Datenschutz gewidmeten Abschnitte des Sozialgesetzbuches X, die zwar eine an sich durchaus begrüßenswerte bereichsspezifische Regelung gebracht haben, in denen andererseits die Eile des Gesetzgebungsverfahrens doch deutliche Spuren hinterlassen hat.

Als recht bedenklich empfinde ich es, wenn der Bundesgesetzgeber im Gesetz zur Bekämpfung der illegalen Beschäftigung (BillBG) eine datenschutzrelevante Bestimmung des Sozialgesetzbuches (§ 71 Nr. 3 SGB X) in der Weise abgeändert hat, daß über die Bekämpfung der illegalen Beschäftigung hinaus die Offenbarung von Sozialdaten gegenüber Finanzämtern auch in anderen Fällen erweitert wird, ohne daß diese Auswirkung in der Entstehungsphase des Änderungsgesetzes deutlich gemacht worden wäre (siehe dazu unter 3.4.1). Sicher ist Datenschutz kein Tabu, aber der Gesetzgeber sollte sich offen zu einer solchen Einschränkung des Datenschutzes bekennen.

2.2 Zur Tätigkeit des Bayerischen Landesbeauftragten für den Datenschutz

2.2.1 Beratung und Informationen

Grundsätzlich läßt sich zu meiner und meiner Geschäftsstelle Tätigkeit wenig Neues sagen. Den hohen Stellenwert der Beratungs- und Informationsarbeit habe ich oben „zur Lage" bereits betont. Um mein Ziel zu erreichen, Datenschutz zum Allgemeingut und zur Selbstverständlichkeit in allen Teilen des öffentlichen Dienstes werden zu lassen, und nicht zuletzt dem Bürger die Aufgaben, Möglichkeiten (und Grenzen) des Datenschutzes erkennbar zu machen – er ist ein entscheidender Helfer bei meiner Kontrolltätigkeit – sehe ich ein unermüdliches Wirken als Berater und Helfer als überzeugendstes Mittel an. Datenschutz kann, das steht außer Zweifel, nicht selten zu einem Abgehen von altgewohnten Verfahren führen und verlangt neue Überlegungen; in der Regel ist es aber vermeidbar, daß die Anpassung der Verwaltungspraxis an Datenschutzbestimmungen den Verwaltungsablauf erschwert. Gleichwohl vermag der Datenschutzgedanke nur dann Verwaltung und Öffentlichkeit zu durchdringen, wenn der Sinn des Datenschutzes verständlich wird. Hier machte sich auch im Jahre 1981 bemerkbar, wie kurz noch die Erfahrungen auch der Datenschutzbeauftragten und ihrer Mitarbeiter sind und wie wenig sie selbst in allen Fällen mit fertigen Rezepten aufwarten können. So setzt ein nützliches Handeln des Datenschutzbeauftragten das positive Mitwirken aller beteiligten Behörden voraus. Die Bereitschaft der bayerischen Verwaltung zu einem solchen Verhalten kann ich auch für das Berichtsjahr nur bestätigen.

2.2.2 Kontrollzuständigkeit des Landesbeauftragten für den Datenschutz

Ein Streit über den Umfang der Kontrollzuständigkeit des Datenschutzbeauftragten in einigen anderen Bundesländern gibt Anlaß festzustellen, daß die Datenschutzkontrollpraxis in Bayern bisher nicht zu derartigen Schwierigkeiten geführt hat. Meinen rechtlichen Standpunkt hierzu habe ich im dritten Tätigkeitsbericht (Nr. 2.2, Seite 7) dargelegt. Er hat sich seitdem nicht geändert. Meine Kontrollzuständigkeit umfaßt danach auch die Kontrolle der Einhaltung spezialrechtlicher Datenschutzvorschriften. Solche sind in der Regel Vorschriften über die Zulässigkeit der Weitergabe von personenbezogenen Angaben wie z. B. das Sozialgeheimnis (§ 35 SGB I), die ärztliche und sonstige Schweigepflichten nach § 203 StGB, oder das Steuergeheimnis (§ 30 der Abgabenordnung).

In anderen Bundesländern ist die Frage erörtert worden, inwieweit die Einhaltung solcher außerhalb der eigentlichen Datenschutzgesetze festgelegten spezialrechtlichen Datenschutzbestimmungen auch bei der Verarbeitung von personenbezogenen Angaben in Aktenunterlagen zu kontrollieren sei. Ich halte diese Erörterung schon deshalb für wenig fruchtbar, weil dem Datenschutzbeauftragten in seiner Geschäftsstelle ohnehin nur eine beschränkte Kontrollkapazität zur Verfügung steht, so daß neben der Kontrolle automatisierter und nicht automatisierter Dateien keine umfangreiche Prüfungstätigkeit im Bereich der Verarbeitung personenbezogener Angaben in Akten entfaltet werden kann.

Im übrigen finden in der Praxis wegen dieser beschränkten Kapazität immer wieder Abstimmungen über Kontrollen zwischen der Geschäftsstelle des Landesbeauftragten für den Datenschutz und allgemeinen Aufsichtsbehörden statt, um zu vermeiden,

daß Aufsichtsbehörden und Datenschutzbeauftragter ohne besonderen Grund unmittelbar nacheinander dasselbe prüfen (z.B. mit dem Landesprüfungsamt für Sozialversicherung im Bayer. Staatsministerium für Arbeit und Sozialordnung oder mit dem Staatsministerium des Innern oder Regierungen im Bereich der Kommunalaufsicht).

Andererseits ist aber, wie ich meine, auch ein öffentliches Interesse daran festzustellen, daß der Landesbeauftragte für den Datenschutz beispielsweise die Zulässigkeit einer Datenweitergabe auch aus Akten überprüfen kann (s.a. den in meinem zweiten Tätigkeitsbericht unter Nr. 2.2 geschilderten Fall). Weitere Beispielsfälle ließen sich anführen.

Aber auch im Interesse der betroffenen Bürger ist es zu begrüßen, daß der Datenschutzbeauftragte – immer im Rahmen seiner beschränkten Kontrollkapazität – grundsätzlich z.B. auch

- die Einhaltung der ärztlichen Schweigepflicht an einer Klinik überprüfen kann, unabhängig davon ob die betreffenden hochsensiblen Daten (z.B. Verdachtsdiagnosen, deren Bekanntwerden oft eine berufliche Existenz ungerechtfertigterweise vernichten kann) zufällig in einer Akte registriert waren,
- die Einhaltung des Steuergeheimnisses bei Angaben zur Grund- oder Gewerbesteuer in Gemeinden überprüfen kann, unabhängig davon ob die Gemeinde die Angaben aus ökonomischen Gründen in manuellen oder automatisierten Dateien, oder noch ausschließlich in Akten führt,
- die Einhaltung des Sozialgeheimnisses z.B. bei Krankheitsdaten oder Angaben über Suchtmittelabhängigkeit kontrollieren kann, die bei Sozialleistungsträgern, wie z.B. Krankenkassen oder Sozialhilfeverwaltungen teils in Dateien, teils in Akten registriert sein können,
- die Einhaltung der Amtsverschwiegenheit bei Verfassungsschutz oder Polizeibehörden prüfen kann, unabhängig davon, ob bei der Kontrolle festgestellt wird, daß die Daten, deren Weitergabe zu kontrollieren ist, nicht in sortierbarer (Datei-)Form vorliegen.

Meines Erachtens würde es der Bürger nicht verstehen, wenn die Kontrolltätigkeit des Datenschutzbeauftragten am Aktenschrank enden würde. In vielen Fällen wäre überdies ohne Einsicht auch in die Akten eine sachgerechte Nachprüfung nicht möglich.

Eine irgendwie fühlbare Belastung der zu prüfenden Behörden kann sich aus der Kontrolle der Weitergabe sensibler personenbezogener Daten aus Akten angesichts der beschränkten Kontrollkapazität des Landesbeauftragten für den Datenschutz nicht ergeben.

### 2.2.3 Kontrolltätigkeit

Art. 28 Abs. 1 Satz 1 Bayer. Datenschutzgesetz weist dem Landesbeauftragten für den Datenschutz die Überwachung der Einhaltung des Datenschutzes bei allen öffentlichen Stellen als wesentliche Aufgabe zu. Im Rahmen meiner diesbezüglichen Kontrolltätigkeit haben meine Mitarbeiter geprüft, inwieweit die notwendigen technischen und organisatorischen Maßnahmen beachtet werden, die erforderlich sind, um den Datenschutz zu gewährleisten. Außerdem wurde überwacht, ob die Bestimmungen eingehalten sind, die die Zulässigkeit der Verarbeitung von personenbezogenen Daten regeln.

Die Vorgehensweise im technisch-organisatorischen Bereich unterscheidet sich von den rechtlichen Überprüfungen. Während die Kontrolle der Einhaltung der technischen und organisatorischen Maßnahmen im Wege der umfassenden Überprüfung einer Reihe von öffentlichen Stellen vorgenommen worden ist, war für die Überprüfung der Beachtung der rechtlichen Voraussetzungen zulässiger Datenverarbeitung wegen der Vielzahl der Anfragen von Bürgern und Behörden regelmäßig ein Einzelfall Anlaß für das Tätigwerden. Meist wurde allerdings über die Einzelfallprüfung hinaus die Einhaltung der Rechtsvorschriften des Datenschutzes bei der aufgesuchten Stelle geprüft. Inzwischen war es möglich, auch im rechtlichen Bereich bei Behörden generell und ohne besonderen Anlaß die Einhaltung der Datenschutzvorschriften zu prüfen.

## 2.3 Technische und organisatorische Grundfragen

### 2.3.1 Datensicherung bei zentralen und dezentralen Systemen

In den vergangenen Jahren wurde wiederholt die Ansicht vertreten, daß zentrale Rechner zunehmend von dezentralen Rechnern abgelöst würden. Andere sahen und sehen den zentralen Rechner nach wie vor als die beste Lösung an, automatisiert Daten zu verarbeiten. Häufig war auch das Argument zu hören, daß Datenschutz am dezentralen Rechner leichter zu gewährleisten sei als am zentralen Rechner, in dem viele Aufgaben parallel ablaufen.

Ohne für eine bestimmte Meinung Partei zu ergreifen, seien an dieser Stelle einige Anmerkungen gemacht, die erkennen lassen sollen, daß der Datenschutz hier wie dort gewährleistet werden kann:

Für zentrale Rechner sprechen in erster Linie wirtschaftliche Gesichtspunkte: Das Preis-Leistungs-Verhältnis bei Hardware verbesserte sich ständig zugunsten des Anwenders und auch bei der Software spielen Kostengesichtspunkte zunehmend eine bedeutende Rolle, da am Großrechner für die Abwicklung vieler gleichartiger Verfahren kostenaufwendige Programme nur einmal beschafft oder erstellt werden müssen. Schließlich bringt das Angebot leistungsfähiger Datenkommunikations-Software auch bei Einsatz eines zentralen Rechners die Rechnerleistung direkt an den Arbeitsplatz in der Fachabteilung. Im Bereich der Datensicherung (Recovery) und des Datenschutzes wird gegenwärtig vermehrt Software angeboten, die durch ihre Automatik die Rechnersysteme sicherer gegenüber Ausfall und Mißbrauch macht. Auf der anderen Seite erfordert das Arbeiten in einem Rechenzentrum, das viele Benutzer bedient, die strikte Einhaltung von vorgegebenen Organisationsrichtlinien. Durch den Umfang und die Komplexität der Auf-

gaben steigt – wie die Erfahrung immer wieder zeigt – die Fehleranfälligkeit des Systems. Bei zentralen Systemen wiegt ein Ausfall oder eine Katastrophe schwerer als bei sogenannten autonom arbeitenden dezentralen Systemen, die nur für die maschinelle Abwicklung eines engbegrenzten Bereiches zuständig sind.

Dezentrale Systeme bringen – über die Gesamtheit aller Systeme gesehen – eine höhere Einzelverfügbarkeit. Automatische Datensicherungsfunktionen (wie eine Protokollierung der Dateibenützung) gehören jedoch nur in den seltensten Fällen zum angebotenen Standard. Für den Anwender ist es bei dezentralen Systemen häufig unmöglich für Zwecke des Datenschutzes eigene Software zu erstellen, weil dezentrale Systeme aus Kostengründen ohne eigenes Fachpersonal (Programmierer) betrieben werden. Aus der Sicht des Datenschutzes kann man auf der einen Seite in einem dezentralen System ein geringeres Gefährdungspotential vermuten, auf der anderen Seite könnte aber gerade die fest umrissene, häufig bei allen Bediensteten bekannte gespeicherte Datenmenge die Begehrlichkeit in Bezug auf Datenmißbrauch durch Insider steigern. Ein weiterer Gesichtspunkt, der für dezentrale Systeme sprechen könnte, ist, wie die Erfahrung zeigt, daß dort organisatorische Datensicherungsmaßnahmen schneller und wirksamer einzuführen sind als bei Stellen, die Großrechner betreiben.

2.3.2 Wirkung der technischen Prüfungen

Entwicklung von datenschutzunterstützender Software durch den Anwender:

Bei einer überprüften Behörde, die im Rechenzentrum ein umfangreiches Magnetbandarchiv unterhält, wurden Maßnahmen zur Abgangskontrolle gefordert. Am geeignetsten erscheint hier der Einsatz eines automatisierten Magnetbandverwaltungssystems. Nachdem die Hersteller für diese Zwecke keine geeignete Software anbieten, beabsichtigt nun die betreffende Behörde ein eigenes automatisiertes Verfahren zu entwickeln. Das System wird bildschirmunterstützt arbeiten. Es soll den Anwender bei der Entscheidung über Aufbewahrungsort und -dauer, Verarbeitungstermin und Versand von Datenträgern unterstützen; zusätzlich sollen Angaben über den Dateiinhalt samt Versionsnummer und Generation der Datenträger gespeichert werden.

Häufig lassen sich Testdatenbestände, die alle denkbaren Fälle abdecken, nur unter großem Aufwand erstellen. Eine überprüfte Behörde hat für diesen Zweck ein sogenanntes Verfremdungsprogramm entwickelt, das es gestattet, aus dem echten Produktionsdatenbestand über einen Algorithmus die identifizierenden personenbezogenen Merkmale in der Datei irreversibel zu verschlüsseln. Auf diese Weise kann mit „echten Daten" getestet werden, ohne daß einem Programmierer Merkmale offenbart werden, die einen direkten Bezug zu einer bestimmbaren Person zulassen. Die dort geleisteten Vorarbeiten lassen sich möglicherweise auch von anderen Stellen übernehmen.

Bauliche Datensicherungsmaßnahmen:

Werden in Rechenzentren wirksame Maßnahmen zur Zugangskontrolle gefordert, so handelt es sich dabei meist um Rechenzentren, die zu einer Zeit geplant wurden, als der Closed-Shop-Betrieb noch unüblich war und die Benutzer hautnah an der Anlage arbeiten mußten. Diese Zeiten gehören aber nicht erst seit Inkrafttreten der Datenschutzgesetze der Vergangenheit an. Vielmehr machte der zunehmende Komfort bei den Betriebssystemen und die enorme Steigerung der Verarbeitungsgeschwindigkeiten heutiger Anlagen eine Anwesenheit von Programmierern an der Konsole überflüssig.

Der datenschutzgerechte Umbau solcher Rechenzentren wirft häufig finanzielle Probleme auf. Sie hätten aber vermieden werden können, wenn schon bei Einrichtung dieser Rechenzentren Datensicherungsmaßnahmen berücksichtigt worden wären. Sie sind bei rechtzeitiger Planung stets kostengünstiger zu realisieren. Im Berichtszeitraum waren meine Mitarbeiter deshalb bei einer Reihe von Neubaumaßnahmen beratend tätig. Grundsätzlich ist zu diesem Fragenkomplex zu sagen, daß es zwar allgemeine Leitsätze etwa für Maßnahmen der Zugangskontrolle geben mag (vergleiche „Datensicherungskatalog" des Koordinierungsausschusses Datenverarbeitung vom 30. Juli 1980), die optimale und angemessene Lösung allerdings immer erst am konkreten Einzelfall zu finden ist. Bei rechtzeitiger Einschaltung meiner Dienststelle lassen sich daher aufwendige Nacharbeiten ersparen.

Dieses Angebot gilt selbstverständlich auch für solche Behörden, die keine Großrechenanlagen einzusetzen beabsichtigen, sondern nur ein dezentrales System betreiben oder überhaupt keine personenbezogenen Daten automatisiert verarbeiten, da auch für kleinere Einheiten und bei manueller Datenverarbeitung Datensicherungsmaßnahmen zu beachten sind. Der Besuch einer Behörde, die kurz zuvor einen Neubau bezogen hatte, zeigte, welche Mängel baulicher Art bezüglich der Datensicherung bei rechtzeitiger Inanspruchnahme meiner Dienststelle hätten vermieden werden können.

Übertragbarkeit von Datensicherungsmaßnahmen:

In einer Zuschrift wurde die Befürchtung ausgesprochen, daß die anläßlich der Prüfung einer Verwaltungsbehörde gemachten Vorschläge bei ihrer Übertragung auf eine andere Stelle zu Schwierigkeiten im Geschäftsablauf führen könnten.

Hierzu darf ich bemerken, daß ich stets darauf bedacht bin, keine den Verwaltungsablauf hemmenden Forderungen zu stellen. Die jeweilige Problemlösung baut stets auf den konkreten Gegebenheiten des Verwaltungsablaufes auf. Was für die eine Behörde praktikabel erscheint, kann für die andere unzweckmäßig sein, wenn dort andere Grundvoraussetzungen vorherrschen.

Trotz dieser beschränkten Übertragbarkeit von Erfahrungen halte ich es aber für sinnvoll, über konkrete

Kontrollen und Verbesserungsmaßnahmen auch an dieser Stelle zu berichten, um einen Anstoß zu eigenständigen Überprüfungen zu geben.

2.4 Neue Medien

Die beabsichtigte Einführung neuer Medientechnologien rückt zunehmend in das Bewußtsein der breiteren Öffentlichkeit. Zwar werden hierbei in erster Linie Fragen einer Reizüberflutung durch zuviel Angebote diskutiert, doch hoffe ich, daß wachsende Bereitschaft besteht, auch Datenschutzfragen zu erörtern.

Im Hinblick auf die anstehenden Termine in diesem Bereich dürfte dies auch dringend geboten sein.

2.4.1 Einführung der Neuen Medien

2.4.1.1 Bildschirmtext

Ab Herbst 1983 wird schrittweise die bundesweite Einführung des Dienstes „Bildschirmtext" beginnen. Voraussichtlich im Februar 1984 wird die Bildschirmtextzentrale München (als sog. A-Zentrale) errichtet. Im darauffolgenden Monat soll Nürnberg eine entsprechende Einrichtung erhalten. Derzeit wird davon ausgegangen, daß bis Ende 1985 etwa 78% aller Fernsprechteilnehmer so an eine Bildschirmtextzentrale angeschlossen sein werden, daß sie Bildschirmtext über die Fernsprechleitungen zu Nahbereichsgebühren nutzen können. Ich habe den Eindruck, daß die Dt. Bundespost über den Aufbau der technischen Einrichtungen auch für deren Nutzung – ein Bereich der für den Datenschutz wesentlich ist – Fakten schafft, die eine Ausnützung der Landeskompetenz einschränken können.

2.4.1.2 Kabelpilotprojekt

Der Start des Kabelpilotprojektes München steht nun ebenfalls kurz bevor. Die hierzu eingesetzte Projektkommission geht davon aus, daß Anfang 1983 mit dem gleitenden Start des Pilotprojekts begonnen werden kann. Ein Jahr später sollen voraussichtlich die neu errichteten Teile des umfassenden Breitbandkabelnetzes und damit auch der Rückkanal ihren vollen Ausbauzustand erreicht haben. Um die technischen Möglichkeiten der Neuen Medien umfassend zu testen, soll die zu errichtende „Technische Zentrale" sowohl zur Einspeisung von Hörfunk- und Fernsehprogrammen geeignet sein, als auch die Abonnement- und Abrufdienste sowie die Zweiwegkommunikation technisch bewältigen. Bei dem vorgesehenen gleitenden Start des Pilotprojektes wurde zunächst mit der Nutzung der vorhandenen und zusammenzuschließenden Inselnetze begonnen; im vorgesehenen Stadtgebiet München existieren bereits jetzt Großgemeinschaftsanlagen, die zu einem Verteilnetz für ca. 11000 Wohnungen zusammengeschlossen werden könnten. Da in dieser Phase des Projekts ein Rückkanal fehlt, können zunächst lediglich Verteildienste mit einer Verteilkapazität bis zu maximal 12 Kanälen verwirklicht werden. Das Angebot soll neben den üblichen empfangbaren Programmen (ARD, ZDF, Bayer. Regional-Fernsehen sowie ORF 1 und ORF 2) aus weiteren, allerdings mit zusätzlichen Kosten verbundenen Hörfunk- und Fernsehprogrammen bestehen. Daneben wird noch an die Heranführung weiterer Fernsehprogramme und unter anderem an die Einbeziehung des von der Deutschen Bundespost angebotenen Dienstes „Bildschirmtext" gedacht.

Sobald die vorgesehenen zwei Koaxialkabel zur Verfügung stehen und damit auch der Rückkanal nutzbar ist, soll das volle Spektrum des Nutzungsangebots im Pilotprojekt verwirklicht werden. Bei diesem Vollausbau werden neben den bereits für die Startphase genannten 12 Kanälen noch weitere 20 Kanäle belegt. Der weiteste Ausbauschritt des Pilotprojekts soll den Abruf von Spielfilmen und ähnlichem erlauben. Damit würde der Teilnehmer in die Lage versetzt, über den Rückkanal die von ihm gewünschte Abrufung zu bestimmen.

2.4.1.3 Datenschutzprobleme

Wie ich bereits in meinem 3. Tätigkeitsbericht (S. 25ff.) aufgeführt habe, sehe ich datenschutzrechtliche Probleme in erster Linie in der technisch grundsätzlich möglichen umfassenden Sammlung personenbezogener Daten in den Betriebszentralen. Über die Betriebszentralen wird die vollständige Kommunikation zwischen den Anbietern und den Anwendern der Neuen Medien abgewickelt. Über die Betriebszentralen werden also alle Programmanforderungen gehen, werden alle ausgetauschten Daten fließen und wird die Gebührenabrechnung abgewickelt. Damit ist jedenfalls theoretisch möglich, daß aus den bei den Betriebszentralen angefallenen Daten Rückschlüsse auf das Lebensverhalten des einzelnen gezogen werden: Seine Anwesenheitszeiten zu Hause, die bevorzugt abgerufenen Bildschirmtextseiten, Konsumgewohnheiten, Geldgeschäfte, Absender und Empfänger von BTX-Briefen, besondere Hobbys und vieles mehr.

Wenn Ziele der Einführung der Neuen Medien hauptsächlich ein erweitertes Programmangebot und mehr Komfort für den Bürger sind, vermag ich nicht einzusehen, weshalb die Anforderungen des Datenschutzes nicht umgesetzt werden können; zumal durch den Datenschutz nur den Gefahren begegnet werden soll.

2.4.2 Regelungsbedarf

Das Bundesverfassungsgericht hat in seiner jüngsten Rundfunkentscheidung (16. Juni 1981) auch Rechtsfragen der neuen Medienentwicklung erörtert. Das Gericht fordert, daß zur Gewährleistung der Rundfunkfreiheit gesetzlich sichergestellt werde, daß die Vielfalt der bestehenden Meinungen im Rundfunk in möglichster Breite und Vollständigkeit Ausdruck finden und daß auf diese Weise umfassende Information geboten wird. Dabei habe der Gesetzgeber insbesondere Vorkehrungen zu treffen, die sicherstellen, daß der Rundfunk nicht einer oder einzelnen gesellschaftlichen Gruppen ausgeliefert wird, daß die in Betracht kommenden gesellschaftlichen Kräfte im Gesamtprogramm zu Wort kommen und daß die Freiheit der Berichterstattung unangetastet bleibt. Im Hinblick auf die neue Medientechnologie führt das Bundesverfassungsgericht aus, daß diese Notwendigkeit ausge-

staltender gesetzlicher Regelung auch dann besteht, wenn die durch Knappheit der Sendefrequenzen und den hohen finanziellen Aufwand für die Veranstaltung von Rundfunkdarbietungen bedingte Sondersituation des Rundfunks im Zuge der modernen Entwicklung entfällt. Von dieser Sondersituation des Rundfunks – nämlich insbesondere der Knappheit der Frequenzen – war das Bundesverfassungsgericht in seinen früheren Rundfunkentscheidungen ausgegangen (E 12, S. 205/261; E 31, S. 314/326). Auch bei Wegfall dieser Sondersituation bleibe es bei der Notwendigkeit, durch gesetzliche Vorkehrungen für die Gewährleistung der Freiheit des Rundfunks Sorge zu tragen. Denn auch bei einem Fortfall der bisherigen Beschränkungen könne nicht mit hinreichender Sicherheit erwartet werden, daß das Programmangebot in seiner Gesamtheit kraft der Eigengesetzlichkeit des Wettbewerbs den Anforderungen der Rundfunkfreiheit entsprechen werde.

Zur Einführung privaten Rundfunks bedürfe es einer gesetzlichen Grundlage. Dies gelte – das ist für die Projekte im Bereich der Neuen Medien von besonderem Interesse – auch für zeitlich und örtlich begrenzte Versuche, weil diese den gleichen Grundrechtsbezug haben wie eine endgültige Regelung. Allerdings komme dem Gesetzgeber insoweit eine erhebliche größere Gestaltungsfreiheit zu, weil solche Versuche gerade der Aufgabe dienten, Erfahrungen zu gewinnen. Das Bundesverfassungsgericht hat im übrigen wiederholt ausgesprochen, daß dem Gesetzgeber bei komplexen, in der Entwicklung begriffenen Sachverhalten ein zeitlicher Anpassungsspielraum gebührt und daß seine Regelungen erst dann verfassungsrechtlich zu beanstanden sind, wenn der Gesetzgeber trotz ausreichender Erfahrungen und Erkenntnisse eine sachgerechte Lösung unterläßt (E 54/S. 173/202).

2.4.3 Datenschutzforderungen

Aus den eingangs und bereits im 3. Tätigkeitsbericht dargelegten Gefahren für den Datenschutz aus dem Einsatz Neuer Medien lassen sich die generellen Datenschutzanforderungen ableiten. Weil die größten Gefahren von der Möglichkeit der Erstellung von Persönlichkeitsprofilen ausgehen, gilt es diese zu verhindern. Dies kann nicht allein durch ein Verbot erreicht werden. Wünschenswert wäre es, bereits die Voraussetzungen zu der Anlegung derartiger Profile – nämlich die Speicherung großer personenbezogener Datenmengen in den Betriebszentralen oder bei den Anbietern – möglichst zu verhindern. Das Bundesverfassungsgericht hat frühzeitig festgestellt, daß es verboten sei, den Menschen in seiner ganzen Persönlichkeit zu registrieren und zu katalogisieren (E 27, S. 1/6). Auch dürfen seine persönlichen Verhältnisse nicht schrankenlos durchleuchtet werden (Bundesverwaltungsgericht NJW 1956, S. 393). Aber gerade dies würde mit der Bildung von solchen Profilen geschehen. Soweit öffentliche Stellen an derartigen Maßnahmen beteiligt wären, müßte sich dieses Verarbeiten von umfassenden Datenmengen auch am Verhältnismäßigkeitsgrundsatz messen lassen. Weiterhin müßte das Übermaßverbot beachtet werden.

Zwischenzeitlich steht, wie oben bemerkt, die bundesweite Einführung von Bildschirmtext bevor. Den Auftrag für die technische Ausgestaltung der Betriebszentralen – je nach Funktion Leit-, A- oder B-Zentrale genannt – hat die Bundespost bereits vergeben. Nach meinen Informationen wird in den Zentralen der Abruf von kostenlosen Seiten ohne Zuordnung auf den einzelnen Teilnehmer, also anonym gezählt. Beim Abruf einer kostenpflichtigen Seite hingegen ist vorgesehen, auf dem in der Zentrale befindlichen dem einzelnen Teilnehmer zugeordneten Zähler aufzulisten, an wen der Teilnehmer Gebühren zu zahlen hat. Damit erfolgt die Speicherung des gezielten Abrufs der einzelnen Bildschirmtextseiten und gegebenenfalls des Anschlusses an bestimmte Anbieterdatenverarbeitungsanlagen in der Zentrale, jedoch nicht beim Anbieter. Diese gespeicherten Informationen können Rückschlüsse auf die Interessengebiete der einzelnen Teilnehmer zulassen. Die Notwendigkeit der Speicherung der einzelnen Abrufe wird mit der verbraucherfreundlichen Offenlegung der Gebührenabrechnung begründet, die von der Zentrale erstellt und für den Anbieter eingezogen wird.

Unter Bezugnahme auf die im 3. Tätigkeitsbericht veröffentlichten Datenschutzgrundsätze bei den Neuen Medien fordere ich grundsätzlich, daß die Erhebung und die Speicherung von personenbezogenen Daten bei den Betriebszentralen und durch die Anbieter nur im unbedingt notwendigen Umfang erfolgen dürfen. Die notwendige Abrechnung für den Abruf kostenpflichtiger Informationen darf nicht als Begründung herangezogen werden, bei den Betriebszentralen die einzelnen Abrufvorgänge auf den Teilnehmer bezogen zu speichern. Die angefallenen Benutzerdaten sind im übrigen weitestgehend zu anonymisieren. Die rechtmäßig gespeicherten personenbezogenen Teilnehmerdaten sind frühzeitig zu löschen. Die Betriebszentralen sollen grundsätzlich keine personenbezogenen Daten der Teilnehmer an die Anbieter weitergeben. Daten, die Rückschlüsse auf ein bestimmtes Benutzerverhalten zulassen, dürfen den Anbietern nicht zugänglich werden, auch wenn diese Daten für Werbezwecke von Interesse sein könnten.

Eine Speicherung der bei Benützung des Rückkanals angefallenen personenbezogenen Daten, insbesondere soweit sie eine Meinungsäußerung darstellen oder Rückschlüsse auf persönliche Gegebenheiten zulassen, muß ausdrücklich eingeschränkt werden.

Auch wissenschaftliche Begleituntersuchungen dürfen nicht zu einer Aufweichung des Datenschutzes führen.

2.4.4 Durchsetzung der datenschutzrechtlichen Forderungen

Bei der Frage nach der möglichen Durchsetzung der datenschutzrechtlichen Forderungen ist zu prüfen, inwieweit bestehende Datenschutzvorschriften oder andere Gesetze den Datenschutzanforderungen genügen. Sofern diese Frage verneint wird, ist für die Schaffung neuer gesetzlicher Regelungen die Kompetenz festzustellen. Diese Klärung ist auch aus der Sicht des Datenschutzes dringend erforderlich, weil von der Kompetenz für die Gesetzgebung bei den

Neuen Medien insgesamt auch die Annexkompetenz für Regelungen zum Datenschutz abhängt.

Für diese Prüfung ist zwischen Netz- und Nutzungsbereich zu unterscheiden.

2.4.4.1 Netzbereich

Für das Fernmeldenetz ist grundsätzlich die ausschließliche Zuständigkeit des Bundes nach Art. 73 Nr. 7 GG gegeben. Allerdings ist für die Neuen Medien noch nicht abschließend geklärt, wer Träger des künftigen Kabelnetzes sein soll und ob das Fernmeldemonopol der Dt. Bundespost insoweit eingeschränkt werden müßte.

Entscheidend für die Kompetenz ist die Frage, ob die aus datenschutzrechtlicher Sicht bedeutsamen „Betriebszentralen" dem Netzbereich und damit eventuell der Kompetenz des Bundes zuzuordnen sind. Hiervon hängt im übrigen auch ab, wie weit das Fernmeldeanlagengesetz i.V.m Art. 10 Grundgesetz die Funktion eines bereits bestehenden bereichsspezifischen Datenschutzes erfüllen kann.

Entscheidend ist, ob die Betriebszentrale als Fernmeldeanlage im Sinne des § 1 Fernmeldeanlagengesetzes gesehen werden kann. Unter Fernmeldeanlage wird herkömmlich eine Anlage für die Fernübermittlung verstanden, die der Übermittlung durch Nachbildung der Übermittlungszeichen ohne körperliche Übersendung des Trägers des zu Übermittelnden dient (BVerfGE 46, S. 120/140). Das Bundesverfassungsgericht geht somit davon aus, daß Fernmeldeanlagen nur solche Anlagen sind, die ausschließlich der Übermittlung dienen. Das bedeutet, daß Anlagen zur Speicherung von Nachrichten nicht dem Begriff der Fernmeldeanlagen untergeordnet werden können. Da aber gerade eine nicht unwesentliche Aufgabe der Betriebszentralen bei den Neuen Medien, insbesondere aber bei Bildschirmtext, die Speicherung der über diese Medien abrufbaren Informationen und der angefallenen Teilnehmerdaten ist, können die Betriebszentralen nicht als Fernmeldeanlagen im Sinne des Fernmeldeanlagengesetzes angesehen werden. Jedenfalls soweit die Betriebszentralen über die reine Vermittlungsfunktion hinaus Aufgaben wahrnehmen, unterliegen sie nicht der Gesetzgebungszuständigkeit des Bundes; insoweit ist auch das Fernmeldeanlagengesetz nicht anwendbar.

Generell kann festgestellt werden, daß die Datenschutzgesetze die bei den Neuen Medien anfallende Datenverarbeitung nur bedingt regeln. So dürfte es zweifelhaft sein, ob die bei den Betriebszentralen anfallenden Prozeßdaten uneingeschränkt den Dateibegriff erfüllen. Außerdem ist auch die Verantwortung für die Speicherung, die die Datenschutzgesetze der speichernden Stelle zuweisen, bei den Neuen Medien nicht eindeutig, da zwischen Anbietern und Betriebszentrale eine Gemengelage besteht. Regelungen zur Auftragsdatenverarbeitung versagen jedenfalls, wenn wie künftig bei Bildschirmtext Tausende von Anbietern als Auftraggeber gegenüber den Betriebszentralen auftreten. Deshalb kann meines Erachtens den insoweit anfallenden Problemen nur durch spezialgesetzliche Datenschutzregelungen begegnet werden.

2.4.4.2 Nutzungsbereich

Die Nutzung der Neuen Medien ist als Rundfunk zu werten, soweit über die neuen Einrichtungen Rundfunk- und Fernsehprogramme verteilt werden (z.B. Kabelfernsehen). Sofern Zeitschriften- und Zeitungsverleger ihre Informationen auf einem der Neuen Medien verbreiten, ist diese Nutzung der „Presse" zuzuordnen. Der beispielsweise bei Bildschirmtext mögliche Einzelabruf von Informationen durch einzelne Teilnehmer und der unter Ausnützung des Rückkanals geführte Dialog sind kein dem Rundfunk vergleichbarer Verteildienst, sondern als Individualkommunikation zu werten. Während Rundfunk und Presse (bei letzterer hat der Bund nur Rahmenkompetenz) der ausdrücklichen Gesetzgebungskompetenz der Länder unterliegen, fehlt es an einer besonderen Regelung für die neu eröffnete Individualkommunikation. Damit fällt nach Art. 30 und Art. 70 Grundgesetz die Regelung auch dieser Individualkommunikation den Ländern zu.

Aus der Sicht des Datenschutzes würde ich es begrüßen, wenn der Landesgesetzgeber in Ausübung seiner Kompetenz eine öffentlich-rechtlich verfaßte Landesanstalt mit der Verantwortung für die Nutzung der Neuen Medien betrauen würde. Dies sollte insbesondere für die in Kürze bevorstehende Einführung von Bildschirmtext erwogen werden. Die Datenschutzkontrolle könnte dann entsprechend der derzeitigen Regelung im Bayer. Datenschutzgesetz vom Datenschutzbeauftragten beim Bayer. Rundfunk und vom Landesbeauftragten für den Datenschutz wahrgenommen werden.

Sofern statt einer der öffentlichen Aufsicht unterliegenden Anstalt mit der Verteilung der über die Neuen Medien verbreiteten Dienste eine privatrechtlich organisierte Einrichtung betraut wird, sollte zumindest die Datenschutzkontrolle eindeutig und ausdrücklich geregelt werden. Letzteres gilt insbesondere, wenn außer dem Rundfunk zuzuordnenden Sendungen noch andere Nutzungsinhalte über die Medien verbreitet werden sollen.

Soweit die geltenden Datenschutzgesetze auf den Nutzungsbereich der Neuen Medien angewendet werden könnten, würden deren Regelungen den speziellen Gefahren der Neuen Medien vielfach nicht gerecht. So enthalten sie beispielsweise kein Verbot der Erhebung personenbezogener Daten durch den Anbieter. Die aus der Sicht des Datenschutzes unerwünschte Datenspeicherung bei den Anbietern könnte vielfach als im Rahmen vertraglicher Verhältnisse gelegen und somit als zulässig angesehen werden. Auch die Übermittlung von Daten, die hier wegen der möglichen Rückschlüsse auf das Lebensverhalten des einzelnen problematisch sein kann, wird durch die Datenschutzgesetze nicht generell ausgeschlossen. Schließlich wäre auch die Überwachung der privatwirtschaftlichen Anbieter vielfach nur im Rahmen der sogenannten Anlaßaufsicht möglich.

Das bedeutet, daß auch für den Nutzungsbereich spezielle Datenschutzregelungen notwendig sind.

### 3. Einzelfragen

3.1 Allgemeine Innere Verwaltung, Kommunalbereich

3.1.1 Entwurf eines Bayerischen Landesmeldegesetzes

Im Berichtszeitraum lag ein Regierungsentwurf für ein neues Bayerisches Landesmeldegesetz noch nicht vor. Der Bayerische Landesbeauftragte für den Datenschutz war jedoch vom Bayerischen Staatsministerium des Innern in Vorüberlegungen eingeschaltet und hatte einen von einer Arbeitsgruppe der Innenministerien der Länder vorgelegten „Formulierungsvorschlag für ein Landesmeldegesetz" erhalten.

Die Datenschutzbeauftragten der Länder und des Bundes und die Datenschutzkommission in Rheinland-Pfalz haben zu dem vorgelegten „Formulierungsvorschlag für ein Landesmeldegesetz" am 2. April 1981 eine Stellungnahme beschlossen. Sie behielten sich dabei vor, zu den jeweiligen Landesmeldegesetzentwürfen, die in Ausfüllung des Bundes-Melderechts-Rahmengesetzes (MRRG) ergehen, im einzelnen Stellung zu nehmen.

Es ist anzuerkennen, daß der genannte „Formulierungsvorschlag" aus der Sicht des Datenschutzes einige erhebliche Verbesserungen enthält (z.B. gebührenfreie Auskunft aus dem Melderegister).

Die Datenschutzbeauftragten und die Datenschutzkommission haben aber grundsätzlich ihrer Sorge darüber Ausdruck gegeben, daß in Landesmeldegesetzen von datenschutzgerechten Begrenzungen im Melderechtsrahmengesetz zugunsten umfassender Erhebungen und Datenflüsse abgegangen werden könnte. Sie haben dazu aufgefordert, bei Novellierung des Melderechts in den Ländern an der Entscheidung des Melderechtsrahmengesetzes für ein begrenztes Einwohnermeldewesen i.S. des bereichsspezifischen Datenschutzes und gegen ein umfassendes Einwohnerinformationssystem festzuhalten.

Aus der Stellungnahme zum Formulierungsentwurf sei hervorgehoben:

- Die Datenschutzbeauftragten und die Datenschutzkommission unterstrichen, daß die Meldebehörden unabhängig von ihrer organisatorischen Einbindung, funktional eigene Stellen sind (s. auch § 18 Abs. 6 MRRG).
- Die Datenschutzbeauftragten und die Datenschutzkommission gehen davon aus, daß die in § 1 Abs. 1 MRRG genannten Aufgaben der Meldebehörden, die Identität der Einwohner und ihre Wohnungen festzustellen und nachzuweisen, eine bewußte Beschränkung darstellen und eine Abkehr von dem in früheren Entwürfen zu einem Bundesmeldegesetz vorgesehenen umfassenden Einwohnerinformationssystem festlegen. Sie gehen davon aus, daß eine Erhebung von Daten nur in dem gesetzlich zugelassenen Rahmen zulässig ist und eine Erweiterung dieses Rahmens durch gemeindliche Satzung nicht möglich ist.
- Die Aufgaben, an denen die Meldebehörden mitzuwirken haben, sind im Landesmeldegesetz abschließend festzulegen. Es darf sich dabei nur um solche Aufgaben handeln, die im engen Zusammenhang mit dem gesetzlich festgelegten Meldezweck stehen.
- Es bestehen Zweifel an der Erforderlichkeit der Speicherung von Angaben über Aufenthaltsanfragen anderer Behörden. Die Datenschutzbeauftragten regen an, die Erforderlichkeit dieser Datenspeicherungen zu überprüfen und ggf. die Zwecke darzulegen, für deren Erfüllung die Angaben bestimmt wären. Die Speicherung der Seriennummer des Passes oder Personalausweises ist im Melderechtsrahmengesetz zum Zwecke der Feststellung der Identität nicht vorgesehen worden. Sollte die Speicherung der Seriennummer für andere Zwecke als die Feststellung der Identität für erforderlich gehalten werden, so sollte dieser andere Zweck offengelegt werden.
- Zur Einführung eines Ordnungsmerkmals siehe unter Nr. 3.1.2.
- Solange noch keine Archivgesetze erlassen worden sind, halten es die Datenschutzbeauftragten und die Datenschutzkommission für erforderlich, im Landesmeldegesetz festzulegen, daß Daten, die dem Archiv übergeben wurden, dort nicht mehr verarbeitet oder sonst genutzt werden, es sei denn, daß dies zu wissenschaftlichen Zwecken oder zur Behebung einer bestehenden Beweisnot unerläßlich ist, oder der Betroffene schriftlich eingewilligt hat. Der Schutz der Meldedaten darf durch die Übergabe ans Archiv nicht gegenüber dem Schutz der Daten im Meldeamt selbst verschlechtert werden. Ein ausreichender Schutz der Meldedaten muß daher durch das Meldegesetz selbst sichergestellt werden.
- Die Datenschutzbeauftragten bezweifeln die Erforderlichkeit der Nebenmeldepflicht des Wohnungsgebers, denn eine wirksame Verbesserung der Qualität des Melderegisters ist durch die Einführung der Nebenmeldepflicht kaum zu erwarten. Sie führt aber dazu, daß der Wohnungsgeber Meldedaten des Wohnungsnehmers zur Kenntnis nehmen und prüfen muß. Aus der Sicht des Datenschutzes müßte daher zumindest sichergestellt werden, daß der Wohnungsgeber möglichst wenig Daten des Wohnungsnehmers erfährt.
- Bei Datenübermittlungen an Sicherheitsbehörden, die nach dem Bundes-Melderechtsrahmengesetz unter erleichterten Voraussetzungen zulässig sind, sollte, um eine Überprüfung durch den Datenschutzbeauftragten auch bei den Meldebehörden und nicht nur bei den Sicherheitsbehörden ansetzen zu können, bei der Meldebehörde die Abfrage der Sicherheitsbehörde registriert werden. Es ist im Einzelfall sonst nicht offenbar, welche Behörde bei der Meldebehörde angerufen oder vorgesprochen hat. Die Registrierung sollte allerdings nicht personenbezogen vorgenommen werden.
- Die Datenschutzbeauftragten gehen davon aus, daß On-line-Anschlüsse von Terminals dritter Stellen an das Melderegister wie regelmäßige Daten-

übermittlungen nur durch Rechtsvorschrift zugelassen werden dürfen.

- Nachdem fast kein Jahr ohne eine Wahl vergeht, für deren Zwecke nach dem Formulierungsvorschlag Wähleranschriften übermittelt werden dürfen, besteht zumindest theoretisch die Möglichkeit, daß Parteien, Träger von Wahlvorschlägen oder Wählergruppen für sich Anschriftenverzeichnisse, die praktisch Duplikate der Melderegister darstellen würden, anlegen könnten – obwohl dies dem Zweck der jeweiligen Datenübermittlung widersprechen würde. Die Datenschutzbeauftragten und die Datenschutzkommission fordern deshalb, auch für die Übermittlung von Wähleranschriften wenigstens ein gleiches Widerspruchsrecht des Betroffenen einzuführen, wie es für die Bekanntgabe von Jubiläumsdaten und die Übermittlung von Daten an Adreßbuchverlage bereits vorgesehen ist.

  Der Beirat beim Landesbeauftragten für den Datenschutz hat vorgesehen, den Regierungsentwurf für ein Bayerisches Landesmeldegesetz, sobald er vorliegt, mit dem Landesbeauftragten für den Datenschutz und dem Bayerischen Staatsministerium des Innern zu erörtern.

3.1.2 Einführung eines Ordnungsmerkmals (OM)

Der „Formulierungsvorschlag für ein Landesmeldegesetz" (s. 3.1.1) sieht die Einführung eines Ordnungsmerkmals (OM) für die Verwaltung von Datenbeständen der Meldebehörden vor. Gegenwärtig verwendet in Bayern die AKDB ein solches OM für die mit dem Aufgabengebiet Meldewesen bei ihr angeschlossenen Gemeinden. Das OM dient für den Bereich der Meldebehörden innerhalb des jeweiligen Regierungsbezirks als eindeutiges Merkmal für die einzelnen Bürger. Damit wird beispielsweise zu einer Person, die zwei Wohnsitze innerhalb eines Regierungsbezirks hat, nur ein OM geführt. Nach dem Entwurf zum Landesmeldegesetz soll nun zugelassen werden, die Verwendung eines eindeutigen Merkmals auf den gesamten AKDB-Bereich und damit grundsätzlich auf das ganze Land auszudehnen.

Für die Behörden und öffentlichen Religionsgesellschaften, die das OM nach dem Entwurf übermittelt erhalten sollen, ist eine beschränkte Nutzung vorgesehen: Sie sollen zwar das OM erhalten, jedoch nur für den Datenaustausch mit der Meldebehörde. Sie dürfen es anderen Stellen nicht weiterübermitteln. Von dieser Beschränkung bleibt die Offenbarung des OM durch die verschiedenen Behörden gegenüber dem Betroffenen selbst unberührt. Es ist daher nicht ausgeschlossen, daß das OM über den Betroffenen allgemein in Verkehr gebracht werden wird.

Somit besteht Anlaß zur Sorge, daß der Betroffene sein OM auch im Privatrechtsverkehr nicht wird für sich behalten können. Private Stellen, wie Banken, Versicherungen, Versandhäuser und andere Vertragspartner des Betroffenen könnten vom einzelnen Bürger die Mitteilung seines OM verlangen und es im Laufe der Zeit auch im privaten Bereich zur Identifizierung des Betroffenen verwenden. Auf diese Weise könnte auch in nichtöffentlichen Dateien das OM als Identifizierungs- und Erschließungsmerkmal Eingang finden. Bisher erforderlicher technischer und organisatorischer Aufwand beim Abgleich von Dateien aus den verschiedenen Bereichen von Wirtschaft und Verwaltung und für deren Verknüpfung würde damit entfallen. Noch etwa bestehende rechtliche Hürden gegenüber der tatsächlichen Zusammenfassung von Angaben verschiedener privater Stellen ließen sich möglicherweise im Laufe der Zeit durch entsprechende „Vertragsgestaltung" mit dem Betroffenen überwinden. Ein gesetzliches Verbot, das vom Betroffenen erhaltene OM zu nutzen – wie etwa das Verbot in § 4 des Bundespersonalausweisgesetzes, die Seriennummer des Personalausweises im nichtöffentlichen Bereich zur Einrichtung oder Erschließung von Dateien zu nutzen – fehlt.

Es wird aufmerksam zu beobachten sein, ob später eine Änderung des Landesmelderechts angeregt werden wird, um die bisher im öffentlichen Bereich noch vorgesehenen Hemmnisse für die Nutzung des OM zu Verknüpfungen zwischen verschiedenen öffentlichen Stellen zu beseitigen.

Es ist zu befürchten, daß eine allgemeine Verbreitung eines landesweit eindeutigen OM im öffentlichen wie im privatwirtschaftlichen Bereich – neben dem Vorteil der Vermeidung von Verwechslungen – folgende aus der Sicht des Datenschutzes bedenkliche Wirkung hätte:

Die Herstellung der eindeutigen Verknüpfungsmöglichkeit der im privaten und öffentlichen Bereich verstreut gespeicherten Daten würde deren Zusammenführung (ohne Mitwirkung und Kenntnis des Betroffenen) technisch bzw. organisatorisch stark erleichtern. Die Infrastruktur für ein bedenkliches Entstehen von Persönlichkeitsprofilen würde im Laufe der Zeit geschaffen.

Die allgemeinen Datenschutzgesetze des Bundes und der Länder setzen zwar bisher in erheblichem Maße auch auf die Selbstverantwortung des Betroffenen: Nach Art. 16 Abs. 2 BayDSG bzw. § 9 Abs. 2 BDSG muß sich jede Behörde, die beim Betroffenen Daten erhebt, ihm gegenüber rechtfertigen, zu welchem Zweck die Daten erhoben werden, und klarstellen ob zur Angabe der Daten eine Verpflichtung besteht oder ob diese im freien Belieben des Betroffenen liegt. Der Betroffene kann sich bei der Angabe von Daten daran orientieren.

Diese Sachlage, von der die Datenschutzgesetze ausgehen, könnte sich durch die Verbreitung des OM jedoch erheblich ändern, denn die Anforderungen der Datenschutzgesetze an Datenübermittlungen zwischen Behörden oder auch zwischen privaten Stellen, die dann in erheblichem Maße anstelle von Datenerhebungen beim Betroffenen treten könnten, sind im Ergebnis weitaus geringer als die Einwirkungsmöglichkeit des Betroffenen, wenn er selbst als Datenlieferant in Anspruch genommen wird. Zwar findet auch bei der Datenübermittlung zwischen Behörden eine gewisse Rechtfertigung des Übermittlungsersuchens statt, doch genügt eine generelle Prüfung der abgebenden Stelle

(siehe z.B. Nr. 14.4 VollzBek BayDSG), während der Betroffene, bei dem Daten erhoben werden, aus der konkreten Sicht seines Falles heraus beurteilt, klärende Fragen stellt und notfalls zu Recht Angaben verweigert.

In dem Maße, in dem nun künftig mehr Daten übermittelt und weniger Daten beim Betroffenen erhoben würden, wird außerdem dem Einzelnen die Kontrolle darüber entzogen, bei welchen Stellen sich Angaben über ihn konzentrieren, wo er seine Datenschutzrechte geltend machen kann, von welchen Stellen besondere Mißbrauchsgefahren ausgehen. Diese Aussage gilt für den öffentlichen wie den privaten Bereich. Im öffentlichen Bereich würde die Transparenz durch die bei den Datenschutzbeauftragten geführten Datenschutzregister noch bis zu einem gewissen Grade gewahrt. Die Aussagekraft von Datenschutzregistern würde jedoch in gleichem Maße sinken, da sie nur Datenspeicherungen und regelmäßige Datenübermittlungen ausweisen, die denkbare Verknüpfungsmöglichkeit dem Einsichtnehmenden aber nicht bewußt machen.

Die Datenschutzbeauftragten der Länder und des Bundes und die Datenschutzkommission Rheinland-Pfalz haben in ihrer Stellungnahme zum Formulierungsvorschlag für ein Landesmeldegesetz vom 2. April 1981 zur Einführung eines Ordnungsmerkmals folgenden Beschluß gefaßt:

„Um die Entstehung eines allgemeinen Personenkennzeichens zu vermeiden, fordern die Datenschutzbeauftragten und die Datenschutzkommission, daß Ordnungsmerkmale, die zur Führung der Melderegister, insbesondere in automatisierten Verfahren eingeführt werden, nicht übermittelt oder sonst weitergegeben werden. Ein entsprechendes Verbot muß im Landesmeldegesetz vorgesehen werden. Ausnahmen von diesem Grundsatz sind allenfalls beim Rückmeldeverfahren gerechtfertigt. Dabei muß jedoch sichergestellt sein, daß übermittelte Ordnungsmerkmale nach Abschluß des Rückmeldeverfahrens beim Empfänger nicht mehr gespeichert werden. Bei Wohnungswechsel über die Gemeinde hinaus muß ein neues Ordnungsmerkmal vergeben werden."

Es wäre bedauerlich, wenn das neue Landesmelderecht den Vorstellungen der Datenschutzbeauftragten zu einer auf Meldebehörden beschränkten Nutzung des OM nicht folgen würde. Es wäre dann zunächst die zuverlässige Einhaltung der Nutzungsbeschränkungen des OM bei den Behörden, die es gegen den Rat der Datenschutzbeauftragten erhalten würden zu beobachten. Ob eine weitere Verbreitung des OM aufgrund dessen Erfassung beim Betroffenen so frühzeitig erkannt würde, daß noch wirksame Maßnahmen dagegen ergriffen werden könnten, kann bezweifelt werden, da die nichtöffentlichen Stellen, die das OM als Erschließungsmerkmal in ihre Dateien übernehmen könnten, außer der Aufsicht auf einzelne Beschwerden hin, keiner externen Datenschutzkontrolle unterliegen.

3.1.3 Adressenübermittlung für eine Befragung von Jugendlichen

Einem Markt- und Meinungsforschungsinstitut waren in einer nicht zu beanstandenden Weise durch Meldeämter stichprobenweise ausgesuchte Adressen von Jugendlichen für eine Befragung übermittelt worden. Dabei war durch das Meldeamt – entsprechend einer Weisung des Bayerischen Staatsministeriums des Innern – die Auflage erteilt worden, die Betroffenen auf die Freiwilligkeit ihrer Teilnahme an der Befragung hinzuweisen.

Der Hinweis auf die Freiwilligkeit war jedoch getrennt von dem Fragebogen auf der Rückseite eines dem Anschreiben beiliegenden Merkblatts angebracht worden. Angesichts einiger sehr in den persönlichen Bereich gehender Fragen des Fragebogens habe ich diesen Hinweis nicht als ausreichenden Hinweis auf die Freiwilligkeit und damit nicht als Erfüllung der Auflage der Meldebehörde angesehen. Das Merkblatt kann verloren gehen, oder unachtsam beiseite gelegt werden. Ein Hinweis auf die Freiwilligkeit, insbesondere bei sehr sensiblen Fragen, sollte unmittelbar im Anschreiben an den Betroffenen untergebracht werden, damit kein Zweifel darüber besteht, daß die Fragen nicht beantwortet zu werden brauchen.

Ich habe die Datenschutzaufsichtsbehörde, die für die Datenschutzkontrolle bei dem befragten Institut zuständig ist und das Bayerische Staatsministerium des Innern als oberste Aufsichtsbehörde über die Meldeämter von diesem Vorgang unterrichtet und die Ansicht vertreten, daß der Hinweis auf die Freiwilligkeit in klar erkennbarer Weise erfolgen müßte. Andernfalls hätte ich die Datenübermittlung durch Meldebehörden an das Befragungsinstitut zu beanstanden.

3.1.4 Einwohnermeldewesen, Datensperrung:

Aufgrund des zur Zeit noch geltenden Melderechts müssen auch Personen, die freiwillig in einer Heil- und Pflegeanstalt längere Zeit zur Behandlung waren, im Melderegister der Gemeinde, in der sich die Heil- und Pflegeanstalt befindet, registriert werden. Dies gilt unabhängig davon, ob die Betroffenen einen gemeldeten Wohnsitz in der Bundesrepublik haben. Das kann zu erheblicher Beeinträchtigung schutzwürdiger Belange führen.

Soweit bekannt, ist beabsichtigt, in dem auf Grund des Melderechtsrahmengesetzes des Bundes zu erlassenden neuen Landesmeldegesetz eine differenziertere Lösung zu finden, die den unterschiedlichen Sachverhalt des freiwilligen oder angeordneten Aufenthalts in einer Heil- und Pflegeanstalt berücksichtigt.

Um diskriminierende Auswirkungen einer Meldung nach bisherigem Recht zu verhindern, habe ich im Falle einer Eingabe angeregt, die Daten über den Aufenthalt in der Gemeinde der Heil- und Pflegeanstalt im Melderegister gemäß Art. 10 Nr. 1 in Verbindung mit Art. 20 BayDSG sperren zu lassen. Eine solche Sperre wirkt auch gegenüber öffentlichen Stellen. Gesperrte Daten dürfen nicht mehr verarbeitet und

sonst genutzt werden. Erlaubt ist die Verarbeitung gesperrter Daten nur in den Fällen des Art. 20 Abs. 2 BayDSG, nämlich wenn sie zu wissenschaftlichen Zwecken, zur Behebung einer bestehenden Beweisnot oder aus sonstigen im überwiegenden Interesse der speichernden Stelle oder eines Dritten liegenden Gründen unerläßlich ist, oder der Betroffene in die Nutzung eingewilligt hat. Dabei sind grundsätzlich schutzwürdige Belange des Betroffenen zu berücksichtigen (Art. 1 Abs. 1, 18, 24 BayDSG, letzteres ist allerdings nicht unumstritten; siehe im übrigen auch Schweinoch/Geiger Kommentar zum BayDSG, Deutscher Gemeindeverlag 1978 zu Art. 10 Anm. 4). Voraussetzung einer solchen Sperrung ist ein „berechtigtes Interesse an der Sperrung". Dies war im Fall der Eingabe anzuerkennen.

Hilfsweise könnte für die genannten Angaben auch eine Sperre nach Abschnitt II Nr. 1 Buchst. ee der Vollzugsbekanntmachung zum Bayerischen Meldegesetz i.d.F. vom 14. Juli 1978 (MABl S. 553) in Frage kommen. Diese Sperre wirkt gegen alle, ausgenommen öffentliche Stellen und den Betroffenen selbst, ist jedoch grundsätzlich schwieriger zu erlangen.

Eine Löschung der Daten gemäß Art. 9 Abs. 2 oder Art. 11 BayDSG kommt nur dann in Betracht, wenn die Unrichtigkeit der Daten feststeht und richtige Daten nicht ermittelt werden können (beides ist nicht der Fall), wenn die Speicherung unzulässig war (dies trifft ebenfalls nicht zu, da sie durch das gegenwärtige Melderecht sogar vorgesehen ist), oder wenn die Kenntnis für die speichernde Stelle (Meldeamt) zur rechtmäßigen Erfüllung der hier durch Rechtsnorm zugewiesenen Aufgabe nicht mehr erforderlich ist. Auch dies kann nach der gegenwärtigen Rechtslage kaum angenommen werden.

3.1.5 Kuvertierung von Lohnsteuerkarten und anderen Mitteilungen

Eine Eingabe führte darüber Beschwerde, daß die Lohnsteuerkarte offen, ohne Briefumschlag, von einem gemeindlichen Boten an eine völlig fremde Person ausgehändigt worden war, obwohl ein Briefkasten mit eindeutiger Namensangabe vorhanden war.

In einem anderen Fall wurde die Lohnsteuerkarte des volljährigen Sohnes ohne Umschlag dem im gleichen Haus lebenden Vater übergeben. Der Vater erfuhr aus der Lohnsteuerkarte erstmals von dem unehelichen Kind seines Sohnes.

Beide Eingaben veranlassen mich, darauf hinzuweisen, daß das Bayerische Staatsministerium der Finanzen im Einvernehmen mit dem Bayerischen Staatsministerium des Innern angeordnet hat, daß die Lohnsteuerkarten nur noch in verschlossenem Umschlag zugestellt werden dürfen. Diese Anordnung wurde den Gemeinden im Frühjahr 1980 von den Oberfinanzdirektionen mitgeteilt. Die Gemeinden sind gemäß § 39 Abs. 6 EStG als örtliche Finanzbehörden den Weisungen der Finanzverwaltung unterworfen. Die Unzulässigkeit der offenen Zustellung der Lohnsteuerkarten geht auch aus Nr. 11 des Merkblattes für die Gemeinden über die Personenstandsaufnahme 1980 und die Ausstellung der Lohnsteuerkarten 1981 hervor.

Mit einer anderen Eingabe wurde mir das Original einer Postkarte übersandt, mit der der Beschwerdeführer von einer Gemeinde gebeten worden war, u.a. ein rechtskräftiges Scheidungsurteil vorzulegen.

Da bei der Versendung von offenen Postkarten an Private erfahrungsgemäß nicht ausgeschlossen werden kann, daß unbefugte Dritte vom Inhalt der Postkarte Kenntnis nehmen, ist aus der Sicht des Datenschutzes grundsätzlich zu fordern, daß zumindest Angaben sensibleren Charakters nur in verschlossenem Kuvert an Betroffene versandt werden. Mit der Gemeinde, die ich um Stellungnahme gebeten hatte, wurde hierüber Einverständnis für die künftige Handhabung erzielt.

3.1.6 Nachforschungen über den Sachverhalt zur Erhebung von Kommunalabgaben bei Dritten anstatt beim Betroffenen

In einer Eingabe wurde darüber Beschwerde geführt, eine Gemeinde habe bei der Erhebung von Kommunalabgaben Sachverhaltsaufklärung statt beim Betroffenen bei dritten Stellen betrieben. Unabhängig von den nicht allgemein interessierenden Besonderheiten des Eingabefalles sei daher kurz auf die Problemstellung hingewiesen:

Nach Art. 13 Abs. 1 Nr. 3a des Bayerischen Kommunalabgabengesetzes findet bei der Erhebung von Kommunalabgaben auch der Verfahrensgrundsatz des § 93 der Abgabenordnung Anwendung. In § 93 Abs. 1 AO ist bestimmt, daß die Beteiligten, aber auch andere Personen zur Feststellung eines für die Besteuerung erheblichen Sachverhaltes die erforderlichen Auskünfte zu erteilen haben. In § 93 Abs. 1 Satz 3 AO wird dies jedoch wie folgt eingeschränkt: „Andere Personen als die Beteiligten sollen erst dann zur Auskunft angehalten werden, wenn die Sachverhaltsaufklärung durch die Beteiligten nicht zum Ziele führt oder keinen Erfolg verspricht". Die Vorschrift schützt das Interesse der Beteiligten daran, daß Dritten keine steuer- oder abgabenrechtlichen Sachverhalte bekannt werden, solange die Sachverhaltsaufklärung durch den Beteiligten selbst möglich ist. Daraus ergibt sich, daß die Erhebungsstellen die Sachverhaltsaufklärung zunächst bei dem Beteiligten selbst versuchen müssen (s. auch Tipke/Kruse, Kommentar zur AO § 93 Anm. 4 b).

Auch eine Gemeinde muß sich daher bei der Erhebung von Abgaben zunächst an die Beteiligten selbst wenden. Es würde § 93 Abs. 1 Satz 3 AO und damit Art. 13 Abs. 1 Nr. 3a des Kommunalabgabengesetzes widersprechen, wenn statt dessen zunächst die Unterlagen dritter Personen oder anderer privater oder öffentlicher Stellen auf Anhaltspunkte für abgabenrelevante Sachverhalte abgefragt würden.

Auch eine Übermittlung aus Dateien durch Dritte oder andere Stellen an eine Gemeinde würde nach den Vorschriften des BDSG für nichtöffentliche Stellen (§ 24 Abs. 1 Satz 1 BDSG) bzw. den Vorschriften des BayDSG für bayerische öffentliche Stellen (Art. 17 Abs. 1 BayDSG) unzulässig sein, soweit die Anfor-

derung der Daten mit § 93 Abs. 1 Satz 3 AO i.V. mit Art. 13 Nr. 3a Kommunalabgabengesetz nicht vereinbar ist. Die Gemeinde muß daher, soweit die Sachverhaltsaufklärung durch einzelne Betroffene nicht zum Ziele führt, für diese Fälle darlegen, daß eine andere Art der Aufklärung, die für den Betroffenen einen geringeren Eingriff darstellen würde als die Offenbarung des Steuer- oder Abgabensachverhalts an Dritte, nicht (mehr) zur Verfügung stehen. Die Darlegung der Gemeinde muß einer etwaigen um Auskunft ersuchten Stelle die Möglichkeit einräumen, das mit § 93 Abs. 1 AO in Einklang stehende Interesse an der Datenübermittlung zu erkennen.

3.1.7 Personenstands- und Betriebsaufnahme durch Gemeinden gemäß § 134 Abs. 1 der Abgabenordnung

In einer Eingabe wurde die Kopie einer Haushaltsliste zur Personenstandsaufnahme einer Gemeinde vorgelegt. Der Betroffene vermißte einen Hinweis auf den Verwendungszweck der geforderten Angaben und die Rechtsgrundlagen für ihre Erhebung und teilte mit, daß ihm auf Rückfrage erklärt worden sei, die erhobenen Daten würden für die Ausstellung von Lohnsteuerkarten benötigt. Er kritisierte, daß hierzu Angaben über Stellung im Beruf, Arbeitgeber, Miethöhe und Lage der Wohnung, An- oder Abwesenheit und deren Gründe am Stichtag der Erhebung nicht erforderlich seien.

Nach § 134 Abs. 1 AO können die Gemeinden für die Finanzbehörden zur Erfassung von Personen und Unternehmen, die der Besteuerung unterliegen, eine Personenstands- und Betriebsaufnahme durchführen. Dies setzt jedoch voraus, daß die Landesregierung bzw. die obersten Finanzbehörden den Zeitpunkt der Erhebung festlegen (§ 134 Abs. 3 AO). Zusätzlich zur Erhebung von Daten für die Finanzbehörden können die Gemeinden mit einer solchen Personenstands- und Betriebsaufnahme für ihre Zwecke besondere Erhebungen verbinden. Solche Erhebungen setzen allerdings eine besondere Rechtsgrundlage außerhalb der AO voraus (§ 134 Abs. 4 AO).

Ist eine Personenstands- und Betriebsaufnahme von der Landesregierung bzw. den obersten Finanzbehörden nicht angeordnet, so handelt es sich nicht um eine Personenstands- und Betriebsaufnahme i.S. der §§ 134ff. AO. Nach Art. 16 Abs. 2 BayDSG muß hierauf im Erhebungsbogen hingewiesen werden. Die von Erhebungsbogen und -listen der Oberfinanzdirektionen, die für angeordnete Personenstands- und Betriebsaufnahmen vorgesehen sind, können ohne einen klarstellenden Hinweis nach Art. 16 Abs. 2 BayDSG nicht verwendet werden. Fehlt die Anordnung, so ist auf die Freiwilligkeit von Angaben hinzuweisen.

3.1.8 Kommunale Grundstückskartei

Im Berichtszeitraum bin ich mehrmals gefragt worden, inwieweit die Einrichtung kommunaler Grundstückskarteien zulässig ist und inwieweit daraus Übermittlungen insbesondere an Private vorgenommen werden dürften. Hierzu habe ich grundsätzlich folgendes festgestellt:

Die Eigentumsverhältnise an Grundstücken darzustellen und darüber Auskünfte zu erteilen, ist in erster Linie Aufgabe des Grundbuchamtes, das hierbei § 12 Grundbuchordnung zu beachten hat. Grundsätzlich ist nur bei Auskünften aus dem Grundbuch sichergestellt, daß die regelmäßigen Veränderungen im Eigentümerbestand vollständig und richtig wiedergegeben werden.

Die Einrichtung kommunaler Grundstückskarteien ist grundsätzlich zulässig, wenn die darin enthaltenen Daten aus gemeindlichen Akten und Unterlagen herrühren. Voraussetzung ist, daß die Daten zulässigerweise von den Gemeinden erhoben wurden. Allerdings sind bereits bei Erstellung einer derartigen Kartei die Grundsätze des Art. 17 BayDSG, insbesondere Art. 17 Abs. 3 BayDSG, zu beachten. Sollten nämlich die in die Grundstückskartei aufgenommenen Daten von verschiedenen Ämtern der Gemeinde herrühren, so wäre die Zusammenführung der Daten nur zulässig, wenn die Übermittlung dieser Daten zwischen den einzelnen Ämtern der Gemeinde zulässig ist. Soweit ein Teil der Daten aus Unterlagen der gemeindlichen Steuerverwaltung stammt, ist im übrigen zu prüfen, inwieweit § 30 Abgabenordnung (Steuergeheimnis) anzuwenden ist.

Die Zulässigkeit einer Auskunft aus einer derartigen Grundstückskartei bemißt sich ihrerseits nach Art. 17 BayDSG, wenn die Auskunft an andere öffentliche Stellen erteilt wird, und nach Art. 18 BayDSG, sofern die Auskunft privaten Dritten gegeben werden soll. Dabei muß die Zulässigkeit der Übermittlung im jeweiligen Einzelfall festgestellt werden. Diese Prüfungspflicht trifft die Stelle, die die Grundstückskartei führt. Sofern in der Grundstückskartei auch Daten enthalten sind, die von der gemeindlichen Steuerverwaltung stammen, sind Art. 17 Abs. 2 bzw. 18 Abs. 2 BayDSG zu beachten, sofern für diese Daten § 30 Abgabenordnung gilt. Da im Einzelfall wohl nicht mehr unterschieden werden kann, woher die in der Grundstückskartei enthaltenen Daten herrühren, dürften, sofern überhaupt dem § 30 Abgabenordnung unterliegende Daten in der Kartei enthalten sind, Auskünfte nur nach den strengen Bestimmungen des Art. 17 Abs. 2, 18 Abs. 2 BayDSG erteilt werden. Das bedeutet, daß Auskünfte an private Personen oder an Firmen generell unzulässig sind.

Für eine Auskunft über eine Mehrheit von Grundstückseigentümern ist über die vorgenannten Voraussetzungen hinaus noch Nr. 18.2.4 VollzBek-BayDSG zu beachten. Hiernach soll eine Auskunft im Regelfall nur erteilt werden, wenn die Gruppenauskunft im öffentlichen Interesse liegt. Abschließend kann somit festgestellt werden, daß derartige kommunale Grundstückskarteien grundsätzlich nur für Zwecke der Kommune selbst verwendet werden sollten und im übrigen Auskunftsersuchende an das dafür vom Gesetz vorgesehene Grundbuchamt verwiesen werden.

3.1.9 Überprüfung von Landratsämtern, Städten, Gemeinden und Verwaltungsgemeinschaften

Im Berichtsjahr wurden eine Reihe von Landratsämtern, Städten, Gemeinden und Verwaltungsgemein-

schaften datenschutzrechtlich überprüft. Daneben fanden auch Prüfungen der technischen und organisatorischen Datenschutzmaßnahmen statt (s. u. 3.11). Gegenstand der Prüfung waren im wesentlichen:

1. die verwendeten Erhebungsvordrucke,
2. die Führung von manuellen Dateien bzw. Karteien und Datenübermittlungen daraus,
3. die Form, der Inhalt der Verpflichtung auf das Datengeheimnis gemäß Art. 14 BayDSG,
4. Auftragsdatenverarbeitung,
5. Einzelfälle.

Hinsichtlich der verwendeten Vordrucke für die Erhebung von Daten beim Bürger bzw. über den Bürger wurde in der Regel folgendes vereinbart:

Soweit Vordrucke von Vordruckverlagen Verwendung finden, wurden die überprüften Behörden gebeten, auf eine Anpassung der Formulare an Art. 16 Abs. 2 BayDSG zu drängen. Nach dieser Vorschrift muß bei der Erhebung von Daten stets darauf hingewiesen werden, ob der Betroffene zur Angabe verpflichtet ist oder die Daten freiwillig angibt. Bei Formularen, die gleichzeitig als Karteiblätter verwendet werden, müssen besonders die Voraussetzungen für die Zulässigkeit der Datenspeicherung (Art. 4 und Art. 16 Abs. 1 BayDSG) geprüft und in die Formulargestaltung einbezogen werden.

Soweit von den öffentlichen Stellen selbst hergestellte Formulare verwendet werden, sind diese anhand von Art. 16 Abs. 2 BayDSG und der Vollzugsbekanntmachung zu Art. 16 BayDSG zu überprüfen. Zu beachten ist dabei, daß auch der Umfang der Daten für die rechtmäßige Aufgabenerfüllung der Behörde erforderlich sein muß (Art. 4 und 16 BayDSG). Beispiele für überprüfte Erhebungsvordrucke waren der Anhörungsbogen zur Einleitung eines Ordnungswidrigkeitenverfahrens, der Erhebungsbogen zur Feststellung der Unterhaltsrente nach dem Nichtehelichenrecht, der Antrag auf Erteilung bzw. Verlängerung eines Jagdscheines, der Antrag auf Erteilung eines „Blanco"-Fahrzeugbriefes und der Erlaubnisantrag zur Abwasserbeseitigung.

Die Speicherung von Daten in Dateien bzw. Karteien wurde stichprobenweise überprüft. Für die Zulässigkeit der Speicherung jeder einzelnen Angabe sind die Artikel 4 und 16 Abs. 1 BayDSG maßgeblich. Stichprobenweise überprüft wurde auch die Übermittlung von Daten aus den geführten Karteien.

Bei den Gemeinden wurden beispielsweise folgende selbst hergestellten Erhebungsvordrucke überprüft: Verschiedene Anträge und Fragebogen der Personalverwaltung, Erhebungsbogen für Stundung oder Erlaß von Gebühren, Bauantrag, Antrag auf Zuschuß für Familienerholung auf dem Bauernhof, Antrag auf Kostenübernahme beim Jugendamt, Anzeige einer Geburt, Anzeige eines Sterbefalles.

Die Gemeinden wurden über den gem. Art. 16 Abs. 2 BayDSG notwendigen Hinweis auf Freiwilligkeit der Angabe von Daten bzw. den Hinweis auf die Rechtsnorm, die zur Angabe verpflichtet, beraten. Beispielsweise bei Formularen zur Anzeige einer Geburt und zur Anzeige eines Sterbefalles wurde festgestellt, daß die Daten teilweise zur Erfüllung von Aufgaben nach dem Personenstandsgesetz erforderlich waren, ein konkreter Hinweis auf die die Datenerhebung rechtfertigende Norm jedoch fehlte. Darüber hinaus wurden in diesen Formularen auch Daten aufgrund des Gesetzes über die Statistik der Bevölkerungsbewegung und die Fortschreibung des Bevölkerungsstandes erfragt. Der Hinweis hierauf fehlte ebenso. Außerdem enthielt das Formular Angaben, zu denen die Betroffenen nicht verpflichtet waren. Hier hätte der Hinweis auf die Freiwilligkeit der Angaben angebracht werden müssen.

Die Überprüfung der manuell geführten Karteien und Dateien ergab, daß „Rundfunkgebührenbefreiungs-Karteien" geführt werden. Die Antragsformulare waren entweder alphabetisch oder zusätzlich in Karteiform abgelegt. Die Rechtsgrundlage für diese Karteiführung ist zweifelhaft (s.a. 3.9.6). Ich bin um Klärung bemüht.

In weiteren Fällen wurde festgestellt, daß in einem Ordner Ablichtungen der ausgefüllten und an das Statistische Landesamt im Original weitergeleiteten Erhebungsbogen für die Bodennutzungserhebung aufbewahrt wurden. Die Sammlung der Formblätter stellt eine Datei im Sinne des Art. 5 Abs. 3 Nr. 3 BayDSG dar. Die Aufbewahrung, d.h. Speicherung und Nutzung der Daten außerhalb des im Statistikgesetz vorgesehenen Verfahrens kann nicht gebilligt werden.

In einer Lohnsteuerkarten-Kartei wurde die Speicherung von Angaben festgestellt, die zur Ausstellung der Lohnsteuerkarten nicht erforderlich sind. Auf die Unzulässigkeit dieser Art der Karteiführung wurde hingewiesen.

In einem anderen Fall wurde festgestellt, daß Meldeamtsdaten über den durch Art. 24 Abs. 3 BayDSG und Nr. 2.4 der Vollzugsbekanntmachung zum Meldegesetz festgelegten Rahmen hinaus an Religionsgesellschaften übermittelt wurden. Dies betraf insbesondere Daten von dem jeweiligen Bekenntnis nicht angehörigen Familienmitgliedern. Die Übermittlung wurde insofern beanstandet.

In einem Fall wurde festgestellt, daß eine Stadt alljährlich die Lohnsteuerkarten von Personen kuvertieren und austragen läßt, die dem städtischen Personal nicht angehören. Diese Handhabung widerspricht dem Steuergeheimnis (§ 30 AO) jedenfalls dann, wenn das für die Verteilung eingesetzte Personal nicht nach dem Verflichtungsgesetz vom 2. März 1974 (BGBl. I, S. 547) verpflichtet ist. Das Bayerische Staatsministerium der Finanzen hatte dementsprechend angeordnet, daß die Lohnsteuerkarten ausnahmslos in einem verschlossenen Umschlag entweder durch Gemeindeangestellte auszuhändigen oder durch die Post zu übersenden sind. Die Anordnungen, an die die Stadt gemäß § 39 Abs. 6 des Einkommensteuergesetzes gebunden ist, waren im Frühjahr 1980 durch die Oberfinanzdirektion bekanntgegeben worden. Die nicht korrekte Handhabung war zu beanstanden.

Aus der Art der Aufbewahrung von Steuerunterlagen ergab sich in einem anderen Fall die Frage, ob das Steuergeheimnis hinreichend gewahrt ist. Es handelte sich dabei, zumindest teilweise, nicht um zur Archivierung bereits ausgesonderte Akten mit Karteien, sondern um Unterlagen des Steueramts, die aus Platzgründen außerhalb des Steueramts untergebracht werden mußten. Ich habe mich daher mit den Bayerischen Staatsministerien des Innern und der Finanzen in Verbindung gesetzt, um für eine dem Steuergeheimnis Rechnung tragende befriedigende Lösung zu sorgen. Bis dahin muß sichergestellt werden, daß ausschließlich Steueramtspersonal zu diesem Aktenbestand Zutritt hat.

Die Verpflichtung der in automatisierten Verfahren beschäftigten Mitarbeiter auf das Datengeheimnis war überwiegend durchgeführt worden. In den übrigen Fällen wurde auf schnellen Vollzug des Art. 14 BayDSG gedrängt.

Bei der Überprüfung von Fällen einer Auftragsdatenerfassung ergab sich, daß die hierüber abgeschlossenen Verträge häufig unvollständig waren. Sie enthielten in der Regel keine Verpflichtung des Auftragnehmers, die erforderlichen Datenschutzmaßnahmen nach Art. 14 und 15 BayDSG zu treffen. Eine entsprechende Vertragsergänzung wurde gefordert.

3.2 Sicherheitsbereich

3.2.1 Kriminalpolizeiliche Sammlungen (KpS)

In Bayern traten mit Wirkung vom 1. Januar 1982 die Richtlinien für die Führung kriminalpolizeilicher personenbezogener Sammlungen (KpS) in Kraft. Sie lösen die bisherigen Bayer. Richtlinien über kriminalpolizeiliche Sammlungen ab. Mit Genugtuung habe ich festgestellt, daß gegenüber der Fassung der KpS, der die Innenminister-/Senatoren des Bundes und der Länder zugestimmt hatten und die in einer Reihe von Ländern nahezu unverändert eingeführt worden sind, in der bayerischen Fassung einige zusätzliche Regelungen enthalten sind, die die Anforderungen des Datenschutzes und der Datensicherung besonders berücksichtigen. Zu erwähnen sind hier die Vorschriften über die Errichtung und Führung kriminalpolizeilicher Unterlagen in der Form von Karteien und Dateien, die Regelungen über den Abgleich von Datenbeständen und über die Behandlung archivwürdiger Unterlagen.

Allerdings sind meine darüberhinausgehenden Änderungsvorschläge weitgehend unberücksichtigt geblieben:

So bin ich der Ansicht, daß Einzelangaben über Geschädigte nur mit deren Einwilligung gespeichert werden sollten, sofern über den Namen des Geschädigten ein Zugang zu dessen Daten eröffnet ist. Denn grundsätzlich besteht ein gewisses Risiko, daß durch einen Fehler bei einer späteren polizeilichen Sachbearbeitung der Name des Geschädigten in falsche Beziehung zu einer Straftat gesetzt und der Geschädigte immerhin kurzzeitig als Verdächtiger angesehen wird – zumindest ein derartiger Fall ist mir bekannt geworden.

Meines Erachtens muß auch die Übermittlung von Angaben aus den Kriminalakten an Ausländerbehörden noch näher eingegrenzt werden. Auch sollte der Verwendungszweck, zu dem die Ausländerbehörden derartige Daten erhalten dürfen, näher beschrieben werden.

Die Übermittlung von Angaben aus Kriminalakten an ausländische Stellen sollte in der Weise eingeschränkt werden, daß Daten zum einen nur an Polizeidienststellen übermittelt werden dürfen und zum anderen die Übermittlung nur zum Zweck der Aufklärung schwerwiegender Straftaten zulässig ist. Außerdem muß eine Übermittlung selbst an ausländische Polizeidienststellen unterbleiben, wenn keine Gewähr dafür besteht, daß die übermittelten Daten ausschließlich für den aus der Anforderung ersichtlichen Zweck verwendet werden oder wenn zu befürchten ist, daß schutzwürdige Belange des Betroffenen durch die Übermittlung über das vom Verwendungszweck her bereits gegebene Maß hinaus beeinträchtigt werden.

Die KpS erlauben den Polizeidienststellen, über im Bundeszentralregister bereits getilgte und zu tilgende Verurteilungen und die diesen Verurteilungen zugrundeliegende Straftaten an andere Polizeidienststellen grundsätzlich Mitteilung zu machen. Darüber hinaus dürfen Mitteilungen über derartige getilgte Veurteilungen und die ihnen zugrundeliegenden Straftaten an andere Behörden zumindest dann vorgenommen werden, wenn die in § 50 Bundeszentralregistergesetz vorgesehenen Ausnahmen vom Verwertungsverbot vorliegen.

Erscheint es schon nicht unbedenklich, wenn Polizeidienststellen sich gegenseitig Mitteilungen über Verurteilungen geben, die bereits dem Verwertungsverbot des Bundeszentralregisters unterliegen, ist es meines Erachtens besonders bedenklich, wenn die Polizeidienststellen auch anderen Behörden derartige Mitteilungen geben. Selbst wenn letzteres nur dann geschieht, wenn die Voraussetzungen einer Ausnahme vom Verwertungsverbot vorliegen, wird damit doch den Polizeidienststellen die Anwendung der Bestimmung des § 50 BZRG zugemutet, mit deren Auslegung diese im Regelfall wenig vertraut sein dürften. Fehlinterpretationen dürften daher grundsätzlich nicht ausgeschlossen sein.

In diesem Zusammenhang stellt sich noch ein weiteres Problem. Der einzelnen Polizeidienststelle kann möglicherweise die Tatsache einer bereits vollzogenen Tilgung unbekannt sein. Sollte beispielsweise aus Resozialisierungsgründen eine vorzeitige Tilgung (vgl. § 23 BZRG) angeordnet worden sein und die Polizeidienststelle in Unkenntnis dieser Tatsachen die entsprechenden Angaben an eine andere Behörde übermitteln, kann die Behörde, die von der früheren Eintragung aus den vorgenannten Resozialisierungsgründen gerade nichts erfahren sollte, Kenntnis erlangen. Es muß daher zumindest sichergestellt sein, daß sich Polizeidienststellen vor Übermittlungen an andere Behörden und Stellen vom Eintragungsstand des Bundeszentralregisters unterrichten.

Zur Rasterfahndung habe ich zwar gemeinsam mit anderen Landesbeauftragten für den Datenschutz (vgl. 3. Tätigkeitsbericht, S. 12) die Einführung entsprechender Vorschriften gefordert, die eine ausreichende Rechtsgrundlage für diese Maßnahme darstellen. Allerdings sind die im Zusammenhang mit der Rasterfahndung im polizeilichen Bereich auftretenden Probleme zu komplex und derzeit noch zu wenig geklärt, als daß sie in den KpS hinreichend geregelt werden könnten. Es besteht aber bei der derzeitigen Regelung in den KpS meines Erachtens die Gefahr, daß die vor Durchführung einer Rasterfahndung notwendige rechtliche 1rüfung weniger sorgfältig durchgeführt wird. Außerdem ist die Regelung über den Datenabgleich bei der Rasterfahndung in kriminalpolizeilichen Sammlungen insgesamt sehr weit gefaßt. Insbesondere müßten die schwerwiegenden Straftaten, die eine Rasterfahndung rechtfertigen können, in der Vorschrift bezeichnet werden. Dabei könnte sich die Abgrenzung etwa an § 100a StPO orientieren. Darüber hinaus kann die „Ergreifung von zur Festnahme gesuchten Personen" wohl nur in begründeten Einzelfällen eine Rasterfahndung rechtfertigen, soll diese nicht unverhältnismäßig sein. Daher wird eine Rasterfahndung zur Festnahme gesuchter Personen im Regelfall nur dann zulässig sein, wenn die Gesuchten einer schwerwiegenden Straftat beschuldigt werden. Im übrigen muß noch festgelegt werden, daß die Ergebnisse der Rasterfahndung nur für Zwecke verwendet werden dürfen, die selbst eine Rasterfahndung rechtfertigen würden.

Die Richtlinien für die Führung kriminalpolizeilicher personenbezogener Sammlungen sehen seit 1. 1. 1982 die Möglichkeit vor, dem Betroffenen Auskunft aus den ihn betreffenden kriminalpolizeilichen Unterlagen zu geben. Wegen der zum Teil hohen Sensibilität der im Bereich der Kriminalpolizei gespeicherten Daten muß im Interesse des Betroffenen die Identität eines um Auskunft ersuchenden Bürgers sicher festgestellt und darüber hinaus gewährleistet sein, daß Auskünfte nicht an Unberechtigte gelangen. Hierbei muß jedoch verhindert werden, daß der Aufwand für den Nachweis der Identität so hoch wird, daß dadurch faktisch eine Ausschlußwirkung entsteht und der Betroffene auf sein Auskunftsrecht verzichtet.

Ich habe daher folgende Verfahrensweise vorgeschlagen:

Teilen die Polizeibehörden lediglich die Tatsache mit, daß über den Anfragenden keine Daten gespeichert sind, genügt hierzu die Versendung der Auskunft in einem einfachen, verschlossenen Brief. Selbst wenn diese Auskunft dadurch an einen Unberechtigten gelangen würde, dürften im Falle der bloßen Negativauskunft schutzwürdige Belange in der Regel nicht beeinträchtigt sein.

Erteilt die Polizei hingegen Positivauskünfte oder verweigert sie die Auskunft wegen vorrangiger Sicherheitsinteressen, sollten derartige Auskünfte entweder als „Einschreiben eigenhändig" versandt werden oder aber über die örtlich zuständige Polizeidienststelle im verschlossenen Brief an den Betroffenen gelangen. Im letzteren Falle könnte der Betroffene die Auskunft unter Vorlage eines Personalausweises abholen. Damit wäre auch die Frage der Identität des Auskunftsersuchenden geklärt.

Sofern die Versendung als „Einschreiben eigenhändig" gewählt wird, dürfte ebenfalls sichergestellt sein, daß nur der Berechtigte die Sendung erhält, denn derartige Schreiben werden nach Auskunft der Bundespost nur dem Empfänger persönlich ausgehändigt, der sich, wenn er dem Zustellungsbeamten nicht persönlich bekannt sein sollte, ausweisen muß.

### 3.2.2 Aktenführung im Bereich bayerischer Polizeien

Im Berichtszeitraum habe ich über die Kontrollen aufgrund von Eingaben hinaus mehrere bayerische Polizeidienststellen einer Überprüfung unterzogen und neben einem Präsidium und zwei Direktionen auch einige Inspektionen und Stationen aufgesucht. Die Schwerpunkte meiner Maßnahmen lagen in der Überprüfung des Datenverkehrs mit den jeweiligen Einwohnermeldebehörden und mit der örtlich zuständigen Allgemeinen Ortskrankenkasse, in der Erörterung der generellen Probleme des Datenschutzes im Polizeibereich sowie in der Kontrolle von Zugang, Führung und Aussonderung der Kriminalakten.

Wie meine Feststellungen ergaben, ist die Führung der polizeilichen Akten im allgemeinen sachgerecht und den Richtlinien für die Führung kriminalpolizeilicher personenbezogener Sammlungen (KpS) entsprechend. Schwerwiegende Mängel oder erhebliche Verletzungen datenschutzrechtlicher Vorschriften hatte ich nicht zu beanstanden.

Bei einigen Dienststellen habe ich jedoch festgestellt, daß ein Nachweis fehlt, aus dem der polizeiliche Sachbearbeiter zu ersehen ist, der einen Kriminalakt aus der Aktensammlung entnommen hat. Auch war die fristgerechte, den Bayer. Richtlinien über die Führung kriminalpolizeilicher Sammlungen entsprechende Aussonderung von Kriminalakten und der zugehörigen Suchkarten nicht in allen Fällen gewährleistet. Überdies war in einem Fall eine Schreibkraft mit der Festlegung der Aussonderungsfristen betraut.

Ich habe daher angeregt, die Entnahme von Kriminalakten entweder auf der entsprechenden Suchkarte einzutragen oder durch die Führung eines dem jeweiligen Kriminalakt zuzuordnenden Fehlblattes nachzuweisen. Außerdem habe ich darauf hingewiesen, daß die Eintragung des voraussichtlichen Aussonderungsdatums auf den entsprechenden Suchkarten für die Kriminalakten grundsätzlich durch Fachkräfte und keinesfalls durch Schreibkräfte vorgenommen werden darf. Dabei ist entsprechend den einschlägigen Richtlinien zu verfahren und nicht für alle Fälle eine einheitliche Aussonderungsfrist vorzusehen. Der jeweilige Dienstvorgesetzte sollte die auf den Karteikarten eingetragenen voraussichtlichen Aussonderungstermine zumindest stichprobenartig überprüfen.

Die von mir verlangte Einsicht in Dateien und Unterlagen wurde mir in allen aufgesuchten Polizeidienststellen gewährt. Es erfolgte auch in keinem Fall eine Berufung auf Art. 28 Abs. 3 Satz 2 Bayerisches Datenschutzgesetz, wonach die Einsicht verweigert werden

könnte, wenn dies die Sicherheit des Bundes oder eines Landes gefährden würde.

3.2.3 Aktenaussonderung beim Bayer. Landeskriminalamt

Das Bayer. Landeskriminalamt hat am 1. November 1979 mit einer Sonderaktion zur Bereinigung der kriminalpolizeilichen Aktensammlung begonnen. Mit dieser Aufgabe waren durchschnittlich 11 Beamte betraut. Von dem Bestand zu Beginn der Aktion von über 700000 Kriminalakten sind derzeit ca. 450000 überprüft worden. Über 170000 Kriminalakten sind vernichtet worden. Ich begrüße es außerordentlich, daß das Bayer. Landeskriminalamt sich mit Nachdruck der Aktenbereinigung widmet und zu diesem Zweck Beamte abgestellt hat. Ich hoffe, daß der in Aussicht genommene Termin von etwa Mitte 1983 für den Abschluß der Sonderaktion „Aktenbereinigung" eingehalten werden kann.

Um Befürchtungen entgegenzutreten, daß durch diese Aktenbereinigung möglicherweise die Einsatzfähigkeit des Landeskriminalamtes leiden könnte, weise ich darauf hin, daß das Bayer. Landeskriminalamt nicht nur aus Gründen des Datenschutzes ein besonderes Interesse hat, die inaktuellen Datensätze zu löschen, sondern daß auch wirtschaftliche und haushaltsrechtliche Zwänge bestehen, den Lagerraum von inaktuellem Material freizuhalten. Schließlich dürfte auch die Effektivität polizeilicher Arbeit gewinnen, wenn die vorhandenen Aktensammlungen aktualisiert sind.

3.2.4 Erkennungsdienstliche Unterlagen

Nach meinen Erfahrungen, die auf Bürgereingaben und einzelnen Stichproben beruhen, werden die Voraussetzungen von erkennungsdienstlichen Maßnahmen durch Polizeibeamte teilweise zu großzügig ausgelegt. Ich habe den Eindruck, daß erkennungsdienstliche Maßnahmen vielfach schematisch durchgeführt werden. So werden in einem Polizeipräsidium grundsätzlich alle vorläufig Festgenommenen erkennungsdienstlich behandelt. Da beispielsweise die abgenommenen Fingerabdrücke über das Bayer. Landeskriminalamt an das Bundeskriminalamt weitergeleitet und dort zentral gespeichert werden, können diese Maßnahmen für den Einzelnen von erheblicher Auswirkung sein.

So wurde ein Bürger, der eine Geldstrafe nicht bezahlt hatte und zum Antritt der Ersatzfreiheitsstrafe von der Polizei abgeholt worden war, erkennungsdienstlich behandelt, obwohl zum Zeitpunkt des Antritts der Ersatzfreiheitsstrafe keine neuen Erkenntnisse zu dieser Person vorlagen. Diese ed-Behandlung war weder zum Zwecke der Durchführung eines Strafverfahrens – dieses war ja bereits abgeschlossen – noch für die Zwecke des Erkennungsdienstes notwendig. Für diese Auffassung spricht insbesondere die Tatsache, daß der Betroffene bei Durchführung des Ermittlungsverfahrens nicht ed-behandelt worden war. Aus dem Umstand, daß der Betroffene die ihm auferlegte Geldstrafe nicht bezahlt hatte, konnte eine andere Bewertung nicht auf § 81b Strafprozeßordnung gestützt werden. Ebensowenig konnte der Umstand des Antritts der Verbüßung der Ersatzfreiheitsstrafe erkennungsdienstliche Maßnahmen nach Art. 13 Polizeiaufgabengesetz rechtfertigen. Anhaltspunkte dafür, daß die erkennungsdienstliche Behandlung nach § 86 Strafvollzugsgesetz im Auftrag der Justizvollzugsanstalt vorgenommen worden sei, lagen ebenfalls nicht vor. Im übrigen wären diese erkennungsdienstlichen Unterlagen von der Justizvollzugsanstalt selbst zu verwahren gewesen. Überdies hätte der Betroffene im letzteren Falle nach § 86 Abs. 3 Strafvollzugsgesetz verlangen können, daß diese Unterlagen nach Verbüßung seiner kurzen Ersatzfreiheitsstrafe vernichtet werden.

Auf meine entsprechenden Vorstellungen wurden die den Bürger betreffenden ed-Unterlagen vernichtet.

Zwischenzeitlich sind neue „Vorläufige Richtlinien für erkennungsdienstliche Maßnahmen" von den Bund-/Länder-Gremien beschlossen worden. Diese stellen zweifelsohne gegenüber den bisherigen Richtlinien eine Verbesserung dar, weil sie konkreter sind. Allerdings sollten auch diese vorläufigen Richtlinien vor ihrer endgültigen Einführung in einigen Punkten weiter präzisiert werden. Ich habe hierzu Vorschläge unterbreitet. So sollte beispielsweise der Grundsatz der Verhältnismäßigkeit, den es selbstverständlich auch bei der ed-Behandlung zu beachten gilt, ausdrücklich in den Richtlinien berücksichtigt werden. Außerdem müßten zum einfachen Vollzug der Richtlinien für erkennungsdienstliche Maßnahmen die für die ed-Behandlung sowie die Speicherung und Löschung maßgeblichen Rechtsvorschriften im einzelnen so deutlich interpretiert werden, daß sie zweifelsfrei vollzogen werden können.

3.2.5 Vorfälle in Nürnberg

Aufgrund der Ermittlungsverfahren, die nach den Vorfällen in Nürnberg am 5./6. 3. 1981 eingeleitet worden waren, habe ich im Polizeipräsidium Mittelfranken in Nürnberg eine datenschutzrechtliche Überprüfung vorgenommen. Dabei habe ich festgestellt, daß die in diesem Zusammenhang angelegten kriminalpolizeilichen Akten nicht anders als die sonstigen kriminalpolizeilichen Akten behandelt worden waren. Insbesondere wurde für diese Akten kein zusätzliches Merkmal in die Karteien eingeführt, das einen gesonderten Zugriff auf diese Akten gestattet hätte. Im übrigen war zu erkennen, daß die überwiegende Anzahl der von der Polizei in Nürnberg festgenommenen jungen Leute ed-behandelt worden war. Die ed-Unterlagen wurden der allgemeinen Praxis folgend und entsprechend den damals geltenden „Vorläufigen Richtlinien für erkennungsdienstliche Maßnahmen" über das Bayer. Landeskriminalamt an das Bundeskriminalamt gesandt. Als Rechtsgrundlage für die ed-Behandlung war § 81b StPO genannt worden. Ohne die Frage nach der Zulässigkeit der ed-Behandlung zu prüfen, die sich nach einschlägigen Bestimmungen der Strafprozeßordnung und nicht nach Datenschutzrecht bemißt, habe ich frühzeitig angeregt, zu prüfen, inwieweit zumindest in den Fällen, in denen gegen die erkennungsdienstlich behandelten Personen das Ermittlungsverfahren zwischenzeitlich eingestellt wor-

den ist, die entsprechenden ed-Unterlagen ausgesondert werden könnten. Sofern sich einzelne Betroffene in dieser Angelegenheit unmittelbar mit der Bitte um Löschung an mich gewandt haben, habe ich die Anträge an das Bayer. Landeskriminalamt weitergeleitet. Dort ist den Anträgen entsprochen worden.

Die ed-Behandlungen in Nürnberg haben mich in meiner Auffassung bestärkt, daß die entsprechenden Vorschriften möglichst präzise gefaßt werden sollten.

3.2.6 Rasterfahndung

Das Bayer. Staatsministerium des Innern hat mich im Berichtszeitraum von einem Fall der Rasterfahndung in Kenntnis gesetzt. Im Hinblick auf die Schwere der aufzuklärenden Straftat und die Notwendigkeit in diesem Falle über die konventionellen Ermittlungsmethoden hinaus die Möglichkeiten einer Rasterung auszunützen, habe ich keine Bedenken geltend gemacht. Zudem hat das Bayer. Staatsministerium des Innern ausdrücklich erklärt, daß die gewonnenen Daten nur den Ermittlungen im vorliegenden Falle dienen und eine Übernahme in andere polizeilichen Dateien ausgeschlossen sei. Ich habe darüber hinaus gebeten, daß die im Rahmen der Rasterung gewonnenen Daten nach ihrer zweckbezogenen Auswertung umgehend zu löschen seien, um die Gefährdung für unschuldig Betroffene so gering wie möglich zu halten.

3.2.7 Fragebogen zur Beurteilung der Glaubwürdigkeit kindlicher Zeugen

Bereits in meinem 3. Tätigkeitsbericht habe ich darauf hingewiesen, daß einzelne Polizeidienststellen im Rahmen von Ermittlungsverfahren an Schulen Fragebogen zur Beurteilung der Glaubwürdigkeit kindlicher Zeugen versenden. Offensichtlich ist diese Praxis auch im Berichtsjahr fortgeführt worden.

So ist mir folgender Fall bekannt geworden: Zur Aufklärung einer Straftat, bei der der Wert des Tatgegenstandes lediglich 20,– DM betrug, hat die zuständige Polizeidienststelle an die Schulleitung einen Fragebogen versandt, in dem unter anderem nach der Schullaufbahn (Versetzungen, Sonderbeschulung), nach der körperlichen Entwicklung und deren Besonderheiten (z. B. Stottern, Schwerhöriger, Bettnässer), nach der geistigen Konstitution, der charakterlichen Beurteilung durch den Lehrer (Selbstbewußtsein, Beeinflußbarkeit, Aufrichtigkeit, Zuverlässigkeit, Kontaktfähigkeit, Gemeinschaftsfähigkeit), den Auffälligkeiten in sexueller Hinsicht, den häuslichen Einflüssen (soziale Lage, erzieherische Verhältnisse in der Familie) und zu etwaigen psychischen Entwicklungsstörungen, Verwahrlosungserscheinungen und Abartigkeiten gefragt wurde.

Im diesem Fall stieß die Verwendung des Fragebogens auf erhebliche datenschutzrechtliche Bedenken. So standen die einzelnen, eingehenden Fragestellungen zum großen Teil in keinerlei Zusammenhang mit der zugrundeliegenden Straftat. Damit blieb also unberücksichtigt, daß von Zeugen grundsätzlich nur solche Angaben verlangt werden sollen, die im Zusammenhang mit der Straftat stehen. Werturteile und Meinungen eines Zeugen sollen im Regelfall nicht in Betracht gezogen werden. Davon abgesehen sind der Grundsatz der Verhältnismäßigkeit und das Übermaßverbot, die ebenfalls bei der Zeugenbefragung zu beachten sind, im vorliegenden Fall grob mißachtet worden. Schließlich fehlte in dem Fragebogen eine Zeugenbelehrung.

Bei der Bewertung der Verwendung derartiger Fragebogen scheinen mir folgende Gesichtspunkte besonders gewichtig:

Selbst eine im Einzelfall angebrachte Verwendung derartiger Fragebögen zur Beurteilung der Glaubwürdigkeit kindlicher Zeugen durch die Polizei darf nicht dazu führen, daß die Schulverwaltung Kenntnis von den Antworten des Lehrers erhält, die teilweise den Intimbereich des betroffenen Schülers berühren; auch dürfte es fraglich sein, ob die Schulverwaltung überhaupt in allen Fällen von der Tatsache Kenntnis erlangen sollte, daß ein Schüler in einem polizeilichen Ermittlungsverfahren als Zeuge auftritt. Der befragte Lehrer selbst muß darüber aufgeklärt werden, daß er seinerseits Auskünfte als Zeuge gibt und ihn nicht nur die Zeugenpflichten treffen, sondern ihm auch die entsprechenden Rechte zustehen. Der befragte Lehrer darf nicht den Eindruck haben, daß er aufgrund einer Amtspflicht zur umfassenden Auskunft über den betroffenen Schüler der Polizei gegenüber verpflichtet sei. Ich sehe bei Verwendung derartiger Fragebogen die Gefahr, daß der Grundsatz der Verhältnismäßigkeit nicht in allen Fällen ausreichend beachtet und die Beantwortung von Fragen verlangt wird, die im konkreten Einzelfall zur Aufklärung einer Straftat nicht erforderlich sind. Überhaupt muß vermieden werden, daß Formblätter mit umfangreichen Fragestellungen bei der Ermittlung von weniger schwerwiegenden Straftaten benützt werden. Für unbedenklich halte ich es hingegen, wenn den ermittelnden Polizeibeamten schriftliche Fragezusammenstellungen als Anhaltspunkt für Zeugenvernehmungen in Sachen der Glaubwürdigkeit kindlicher Zeugen zur Verfügung gestellt werden, sofern diese einzelfallbezogen benützt werden.

Auf meine entsprechenden Anfragen zur grundsätzlichen Problematik hat das Bayer. Staatsministerium des Innern mitgeteilt, daß der Arbeitskreis „Öffentliche Sicherheit und Ordnung" der Innenministerkonferenz hierzu einen Beschluß gefaßt habe, wonach keine Notwendigkeit bestehe, einheitliche Verfahren für die Glaubwürdigkeitsprüfung kindlicher Zeugen festzulegen. Das Staatsministerium des Innern beabsichtige aber, die Polizeipräsidien in einem Rundschreiben aufzufordern, Fragebogen dieser Art nur bei schwerwiegenden Straftaten einzuholen und auch nur individuell abgestimmte Fragen zu stellen, auf deren Beantwortung es für das jeweilige Ermittlungsverfahren ankomme. Meines Wissens steht die Versendung dieses Rundschreibens jedoch noch aus.

3.2.8 Anfrage von Haftpflichtversicherern wegen Einsicht in Ermittlungsunterlagen

Einzelne Versicherungsgesellschaften erbitten wiederholt von den Staatsanwaltschaften und von Polizeibehörden Auskünfte aus Ermittlungsverfahren.

Teilweise werden den Anfragen sogenannte Rückantwortkarten beigefügt.

Auf meine entsprechenden Erkundigungen hat mir das Bayer. Staatsministerium der Justiz mitgeteilt, daß die Staatsanwaltschaften entsprechend den Richtlinien für das Strafverfahren und das Bußgeldverfahren (Nr. 185, 296) Akteneinsicht an private Versicherungsgesellschaften regelmäßig nur über einen Rechtsanwalt oder Rechtsbeistand gewähren. Das Bayer. Staatsministerium des Innern hat vorgetragen, daß die Bayer. Polizei Anfragen von Versicherungsunternehmen grundsätzlich unter Verwendung von Rückantwortkarten beantworte. Dabei würden die Polizeibehörden überwiegend nur mitteilen, ob eine Anzeigenaufnahme erfolgt sei und darüber hinaus die Tagebuchnummer, die sachbearbeitende Dienststelle sowie ggf. das Aktenzeichen der Staatsanwaltschaft bzw. der zentralen Bußgeldstelle angeben, soweit der Vorgang dorthin abgegeben sei.

Gegen diese Verfahrensweise sind aus der Sicht des Datenschutzes keine Bedenken zu erheben, wenn die Versicherungsgesellschaften wegen des zugrundeliegenden strafrechtlich relevanten Vorgangs Ansprüche abzuwickeln haben und sichergestellt ist, daß im Einzelfall etwa vorliegende besonders schutzwürdige Belange berücksichtigt werden.

3.2.9 Grenzkontrolle

Im Berichtszeitraum haben sich mehrmals Bürger mit der Befürchtung an mich gewandt, daß ihre Personaldokumente anläßlich eines Grenzübertrittes fotografiert worden seien mit der Folge, daß die Tatsache des Grenzübertrittes besonders registriert und eventuell noch an weitere Stellen übermittelt worden sei.

Meine Ermittlungen haben jeweils ergeben, daß die Betroffenen einer routinemäßigen Fahndungsüberprüfung unterzogen worden sind. Die Reisedokumente sind dabei auf ein Paßlesegerät gelegt worden, das aufgrund seiner technischen Konstruktion zum Anfertigen von Ablichtungen oder Fotografien nicht geeignet ist. Im Zusammenhang mit dieser Überprüfung wurden über die Betroffenen keine Daten gespeichert, noch wurden Daten an andere Stellen übermittelt. Die Rechtsgrundlagen für die Überprüfung der Personaldokumente und für das Verlangen nach Aushändigung der mitgeführten Papiere sind Art. 5 Abs. 1 Ziff. 1, 2 Polizeiorganisationsgesetz, § 1 Paßgesetz, §§ 4 Abs. 2, 24 Satz 2 Straßenverkehrszulassungsordnung und Art. 12 Abs. 2 Polizeiaufgabengesetz.

3.2.10 Speicherung von Daten beim Verfassungsschutz

Im Berichtszeitraum habe ich im Landesamt für Verfassungsschutz aufgrund von Bürgereingaben eine Reihe von Prüfungen durchgeführt. Diese blieben im wesentlichen ohne Beanstandungen. Teilweise hat das Landesamt für Verfassungsschutz von sich aus die Löschung gespeicherter Daten aus Anlaß meiner Überprüfung durchgeführt. In einigen Fällen von jedoch geringerer Bedeutung sind die Auffassungen über den zulässigen Umfang der gespeicherten Daten und deren Übermittlung unterschiedlich geblieben. Aus Gründen der in diesem Bereich notwendigen Geheimhaltung kann ich hier nicht auf Einzelheiten eingehen.

Ganz generell bin ich der Ansicht, daß Informationen über eine Person grundsätzlich nur dann gespeichert werden dürfen, wenn sich aus diesen Informationen für die dem Landesamt für Verfassungsschutz gesetzlich zugewiesene Tätigkeit verwertbare Schlüsse ziehen lassen. Nur wenn diese Voraussetzung gegeben ist, ist die Speicherung der Daten zur rechtmäßigen Erfüllung einer durch Rechtsnorm zugewiesenen oder öffentlichen Aufgabe erforderlich. Nimmt eine Person, zu der Informationen im Landesamt für Verfassungsschutz gespeichert sind, von der Verfassung zugelassene Rechte wahr, ohne dabei den Verdacht einer verfassungsfeindlichen Zielrichtung zu erregen, so ist die Speicherung derartiger Tatsachen im Regelfall nicht zur Aufgabenerfüllung erforderlich und damit unzulässig. Nicht jede zulässige Wahrnehmung rechtfertigt die Speicherung aller beobachteten Lebensäußerungen. Dies gilt erst recht für Beobachtungen zu nicht gespeicherten Personen. Die Tatsache einer Speicherung sollte nur von der Bewertung eines Vorgangs durch Bedienstete des Landesamts für Verfassungsschutz oder andere als zuverlässig bekannte Personen abhängen. Problematisch erschiene es gerade im Bereich des Verfassungsschutzes, wenn die Speicherung allein aufgrund einer Bewertung durch sonstige Personen ausgelöst würde. Vor einer Speicherung zumindest solcher Vorgänge in NADIS, deren Relevanz für die Tätigkeit des Landesamtes für Verfassungsschutz nicht zweifelsfrei ist, sollten noch weitere Anhaltspunkte vorliegen, die die Speicherung rechtfertigen. Eine Speicherung von Tatsachen kann beim Landesamt für Verfassungsschutz auch dann unzulässig sein, wenn ein Verhalten beobachtet wird, das zwar strafrechtlich relevant ist, jedoch nicht den Aufgabenbereich des Landesamtes für Verfassungsschutz berührt.

Meines Erachtens stellt eine Speicherung beim Landesamt für Verfassungsschutz im Regelfall einen Eingriff im datenschutzrechtlichen Sinne für den hiervon Betroffenen dar. Derzeit müssen aus Art. 2 des Gesetzes über die Errichtung eines Landesamtes für Verfassungsschutz neben der Aufgabenzuweisung auch die erforderlichen Befugnisse für die Verarbeitung personenbezogener Daten entnommen werden. Das erklärt sich aus dem Zeitpunkt, zu dem die Grundkonzeption dieses Gesetzes geschaffen worden ist. Damals war die Vorstellung, daß für Eingriffe durch die Datenverarbeitung Befugnisse vorhanden sein müssen, noch nicht geläufig. Um Zweifelsfragen über die Reichweite des Art. 2 des vorgenannten Gesetzes zu begegnen, sollte eine möglichst deutliche Zuweisung von Befugnisnormen für das Landesamt für Verfassungsschutz angestrebt werden.

Klärungsbedürftig erscheint mir in diesem Zusammenhang der zulässige Umfang der Zusammenarbeit zwischen Verfassungsschutz und anderen Behörden, insbesondere der Polizei. Die Grenzen dieser Zusammenarbeit sollten verdeutlicht werden. Sofern dies

nicht durch gesetzliche Regelungen möglich ist, müßten zumindest entsprechende Verwaltungsvorschriften erlassen werden.

3.2.11 Zusammenarbeit zwischen der Bayerischen Grenzpolizei und dem Bayerischen Landesamt für Verfassungsschutz

Die Zusammenarbeit des Bundesgrenzschutzes mit dem Bundesamt für Verfassungsschutz ist in den letzten Jahren häufig Gegenstand heftiger öffentlicher Diskussionen gewesen. Die bisherige Praxis der Amtshilfe zwischen diesen Behörden war teilweise als rechtswidrig bezeichnet worden.

Wie bereits aus der Presse zu erfahren war, hat der Bundesminister des Innern die bisherige Regelung der Zusammenarbeit zwischen Grenzschutzbehörden und Behörden des Verfassungsschutzes durch neue Weisungen ersetzt. Mit diesen soll die Amtshilfe neu bestimmt werden. Für den bayerischen Bereich gelten die vom Bundesminister des Innern herausgegebenen Weisungen nicht unmittelbar; derzeit sind sie jedenfalls noch nicht übernommen worden.

Gegen eine unveränderte Übernahme dieser Regelung für die Zusammenarbeit der bayerischen Grenzpolizei mit dem Bayerischen Landesamt für Verfassungsschutz entsprechend § 3 des Verwaltungsabkommens zwischen dem Bundesminister des Innern und der Bayer. Staatsregierung über die Wahrnehmung von Aufgaben des grenzpolizeilichen Einzeldienstes in Bayern bestünden aus der Sicht des Datenschutzes Bedenken. Denn in einer Reihe von Punkten sind diese Weisungen zu unbestimmt und lassen den Grenzpolizeibehörden einen zu weiten Handlungsspielraum. Dadurch bestünde die Gefahr, daß ohne die erforderlichen Konkretisierungen Daten von Grenzbehörden an Verfassungsschutzbehörden in größerem als dem wirklich erforderlichen Umfang übersandt werden. Eine spätere Konkretisierung dieser Übermittlungsbestimmungen würde möglicherweise eine einmal eingeführte Praxis nicht vollständig ändern können.

Für den bayerischen Bereich sind daher Richtlinien für die Zusammenarbeit zwischen der Grenzpolizei und dem Landesamt für Verfassungsschutz zu fordern, die den Beamten an der Grenze nicht Auslegungen abverlangen, durch die diese im Drange der Geschäfte überfordert wären.

Generell ist zur Zusammenarbeit zwischen Grenzpolizei und den Ämtern für Verfassungsschutz folgendes zu bemerken:

Sofern die Grenzpolizei im Rahmen der Amtshilfe für Ämter des Verfassungsschutzes tätig wird, ist zu beachten, daß durch die Tatsache der Amtshilfegewährung eine Befugnisverschiebung zwischen ersuchender und ersuchter Behörde nicht stattfindet. Das bedeutet, daß die ersuchte Behörde nur solche Maßnahmen treffen darf, zu deren Ausübung sie befugt ist. Etwa vorhandene Befugnisse der Ämter für Verfassungsschutz gehen insoweit nicht auf die Grenzpolizei über. Dies hat zur Folge, daß die Grenzpolizei grundsätzlich nur solche Informationen an Ämter für Verfassungsschutz weitergeben darf, die sie bei Gelegenheit der grenzpolizeilichen Tätigkeit erlangt hat. Nachrichtendienstliche Mittel, zu deren Anwendung die Ämter für Verfassungsschutz befugt wären, darf die Grenzpolizei im Rahmen der Amtshilfe nicht anwenden. Ebenso wenig dürfen die Ämter für Verfassungsschutz im Wege der Amtshilfe polizeiliche Befugnisse in Anspruch nehmen. Daher dürfen auch die Ämter für Verfassungsschutz nur um solche Informationen ersuchen, die im Rahmen der Grenzkontrolle angefallen sind. Die Anwendung nachrichtendienstlicher Mittel durch die Grenzpolizei kommt dabei nicht in Betracht.

3.3 Justiz

3.3.1 Kriminologische Zentralstelle

Der Bund und die Länder haben, vertreten jeweils durch die Justizminister, eine Vereinbarung unterzeichnet, wonach zur Förderung der kriminologischen Forschung in der Bundesrepublik Deutschland ein Verein mit dem Namen „Kriminologische Zentralstelle" gegründet wird. Die Kriminologische Zentralstelle soll nach ihrer Satzung insbesondere

- kriminologisch bedeutsame Unterlagen erfassen und auswerten,
- Methoden der Erfassung, Sammlung und Auswertung kriminologisch bedeutsamer Unterlagen und Daten entwickeln,
- kriminologische Forschungsvorhaben und Forschungsarbeiten registrieren,
- in der kriminologischen Forschung tätige Stellen und Personen bei der Koordinierung von Forschungsvorhaben beraten und in ihrer Forschung unterstützen,
- Stellen und Personen, die Probleme der Verbrechensverhütung und Verbrechensbekämpfung einschließlich des Strafvollzugs durch kriminologische Forschung klären wollen, bei der Fassung und Vergabe von Forschungsaufträgen beraten und unterstützen,
- mit dem kriminologischen Dienst im Strafvollzug (§ 166 Strafvollzugsgesetz) zusammenarbeiten.

Zur Erfüllung seiner Aufgaben wird der Verein eng mit allen Einrichtungen zusammenarbeiten, die kriminologische Forschung betreiben und fördern, insbesondere mit den Universitäten, dem Bundeskriminalamt, der Polizeiführungsakademie Münster und der Deutschen Forschungsgemeinschaft. Forschungsvorhaben und sonstige Vorhaben gemeinsamen Interesses wird die „Kriminologische Zentralstelle" mit dem Bundeskriminalamt abzustimmen haben.

Inwieweit die „Kriminologische Zentralstelle" bei ihrer Aufgabenerfüllung personenbezogene Daten übermittelt oder speichert, kann nach Auskunft des Bayer. Staatsministeriums der Justiz gegenwärtig noch nicht gesagt werden. Dies wird von dem jeweiligen Forschungsvorhaben abhängen. Eine besondere Datenschutzregelung für die „Kriminologische Zentralstelle" wurde nicht getroffen.

Die Problematik der Errichtung einer „Kriminologischen Zentralstelle" wurde auch von den Landes- und dem Bundesbeauftragten für den Datenschutz erörtert. Dabei haben sich insbesondere Bedenken ergeben, weil die „Kriminologische Zentralstelle" als eingetragener Verein errichtet wird. Dadurch wird diese Zentralstelle den Kontrollinstanzen des Datenschutzes entzogen, die für die Justizbehörden zuständig sind. Dies befremdet insbesondere deshalb, weil die in diesem Zusammenhang etwa verarbeiteten personenbezogenen Daten im Regelfall wegen des Bezugs zu Straftaten besonders sensibel sind. Bei der datenschutzrechtlichen Beurteilung der Zulässigkeit von Speicherung und Übermittlung derartiger personenbezogener Daten ist zu bedenken, daß die Grundsätze des Bayer. Datenschutzgesetzes auch dann zu beachten sind, wenn dieses Gesetz mangels Dateibezug nicht unmittelbar zur Anwendung gelangt. Danach dürfte eine Datenübermittlung durch die Justizbehörden an die privatrechtlich organisierte „Kriminologische Zentralstelle" nur zulässig sein, wenn die Daten zur rechtmäßigen Erfüllung einer öffentlichen Aufgabe der übermittelnden Stelle erforderlich sind oder soweit der Empfänger ein berechtigtes Interesse an der Kenntnis der zu übermittelnden Daten glaubhaft macht und dadurch schutzwürdige Belange des Betroffenen nicht beeinträchtigt werden. Bei der Bewertung der schutzwürdigen Belange ist zu berücksichtigen, daß wohl in erster Linie Daten von Straftätern zur Übermittlung in Frage kommen. Daher ist das Interesse an der Wiedereingliederung des Straftäters in die Gesellschaft, also an seiner Resozialisierung, zu beachten. Das Ziel der Resozialisierung hat sich in den letzten Jahrzehnten im Strafrecht zunehmend durchgesetzt. Verfassungsrechtlich entspricht diese Forderung im übrigen dem Selbstverständnis einer Gemeinschaft, die die Menschenwürde in den Mittelpunkt ihrer Wertordnung stellt und dem Sozialstaatsprinzip verpflichtet ist (BVerfGE 35, 202/235).

Zur Vermeidung der Beeinträchtigung schutzwürdiger Belange sollte regelmäßig geprüft werden, inwieweit die „Kriminologische Zentralstelle" ihren Auftrag auch mit anonymisierten Daten erfüllen kann. Sofern im Einzelfall anonymisierte Daten genügen, sollte unter Berücksichtigung der besonderen Schutzbedürftigkeit dieser Daten auf die Übermittlung personenbezogener Daten verzichtet werden.

Ich habe diese Bedenken dem Bayer. Staatsministerium der Justiz mitgeteilt und gebeten zu prüfen, inwieweit sichergestellt werden kann, daß die „Kriminologische Zentralstelle" einer ausreichenden Datenschutzkontrolle unterzogen wird. Gegebenenfalls wäre zu erwägen, die Zentralstelle zu verpflichten, sich der Kontrolle eines Datenschutzbeauftragten zu unterziehen.

3.3.2 Mitteilungen in Strafsachen

In meinem letzten Tätigkeitsbericht hatte ich die Bedenken der Landesbeauftragten und des Bundesbeauftragten für den Datenschutz vorgetragen, die gegen die „Anordnung über Mitteilungen in Strafsachen (MiStra)" bestehen. Zwischenzeitlich hat die Justizministerkonferenz diese Thematik aufgegriffen und einen Unterausschuß der Justizministerkonferenz mit deren Erörterung beauftragt. Dieser Unterausschuß hat sich mehrheitlich für eine spezielle gesetzliche Grundlage für den Bereich der Anordnung über Mitteilungen in Strafsachen ausgesprochen und damit ein wesentliches Anliegen der Datenschutzbeauftragten übernommen. Darüber hinaus beabsichtigt dieser Unterausschuß, den Umfang der Mitteilungspflichten mit dem Ziel einer generellen Verringerung erneut zu überprüfen. Dabei soll gemeinsam mit den Behörden, die derzeit Mitteilungen in Strafsachen erhalten, geklärt werden, inwieweit bei Abwägung der Interessen der betroffenen Bürger und der zur Aufgabenerfüllung der Behörden notwendigen Kenntnis bestimmter Vorgänge einzelne Mitteilungspflichten entfallen oder sich auf weniger Angaben beschränken können.

Diese Überlegungen der Justizministerkonferenz begrüße ich.

Inzwischen hat der Bayer. Landtag betreffend die verfassungsgemäße und gesetzentsprechende Fassung der Anordnung über Mitteilungen in Strafsachen am 4. März 1982 folgenden Beschluß gefaßt, der mein Anliegen nachhaltig unterstützt:

„Die Staatsregierung wird aufgefordert, die Anordnung über Mitteilungen in Strafsachen MiStra (Bayerisches Justizministerialblatt vom 1. Dezember 1977, Seiten 279/80) im Hinblick auf die Bedenken der Datenschutzbeauftragten des Bundes und der Länder im Zusammenwirken mit dem Bund und den anderen Ländern zu überprüfen.

Insbesondere sind bei der Neuformulierung der ‚Anordnung über Mitteilungen in Strafsachen' folgende Gesichtspunkte zu berücksichtigen:

1. Die Mitteilungspflicht der Staatsanwaltschaften bzw. Gerichte ist auf die Bereiche zu reduzieren, bei denen die Mitteilung zur gesetzlichen Aufgabenerfüllung des Empfängers unumgänglich ist.
2. Die künftige Regelung der Mitteilungspflicht in Strafsachen hat die Wahrung des Persönlichkeitsrechtes, dem Grundsatz der Verhältnismäßigkeit und der Verwaltungsvereinfachung Rechnung zu tragen.
3. Es ist Sorge zu tragen, daß Mitteilungen in Strafsachen nach Ablauf bestimmter Fristen aus den Akten des Empfängers entfernt werden."

3.3.3 Zentraldateien der Staatsanwaltschaften

Wie ich bereits in meinem 3. Tätigkeitsbericht dargelegt habe, sind bei den Staatsanwaltschaften zentrale Namensverzeichnisse, genannt „Zentralnamenskarteien" eingerichtet, die dem gezielten Zugriff auf einzelne Strafakten dienen.

Die Zentralnamenskarteien enthalten personenbezogene Daten und sind Dateien im Sinne des Bayer. Datenschutzgesetzes. Dieses Gesetz ist somit auf die Zentralnamenskarteien anwendbar. Wegen des in der Natur der Sache liegenden Bezugs zu Strafsachen

zählen die in den Zentralnamenskarteien geführten Angaben zu den besonders sensiblen Daten, die die schutzwürdigen Belange der Betroffenen nachhaltig berühren können. Das gilt vor allem, wenn die Daten Unschuldiger gespeichert sind, weil bereits der Ort der Speicherung einen belastenden Bezug vermitteln kann.

Wegen dieser bereits in der Speicherung in den Zentralnamenskarteien liegenden Gefährdung für den Betroffenen sollten diese Karteien möglichst auf ihre ursprüngliche Funktion eines Hilfsmittels zur Aktenführung beschränkt werden. Auf dieser Grundlage hat die von den Landesbeauftragten und dem Bundesbeauftragten für den Datenschutz eingesetzte Arbeitsgruppe unter bayerischer Federführung „Mindestanforderungen für den Datenschutz bei den Zentralnamenskarteien der Staatsanwaltschaften" (siehe Anhang) festgelegt. Die Konferenz der Datenschutzbeauftragten hat diese Mindestanforderungen zustimmend zur Kenntnis genommen. Unter deren Berücksichtigung stelle ich aus datenschutzrechtlicher Sicht folgende Forderungen:

Gespeichert dürfen in den Zentralnamenskarteien nur solche Daten werden, die zur rechtmäßigen Aufgabenerfüllung der Staatsanwaltschaft erforderlich sind. Auch hierbei ist der Grundsatz der Verhältnismäßigkeit zu beachten. Eine Verkartung des maßgeblichen Inhalts der Strafakten wäre unzulässig.

Aus der Funktion der zentralen Namenskartei, als Hilfsmittel der Aktenführung bei der Staatsanwaltschaft zu dienen, ergibt sich eine weitgehende Beschränkung der Übermittlung. Für die Beurteilung von Datenübermittlungen an Behörden gilt, daß den Zentralnamenskarteien nicht die Aufgabe eines Ersatzzentralregisters zukommen darf.

Anläßlich einiger Einzelüberprüfungen bei Staatsanwaltschaften habe ich festgestellt, daß bei Erteilung fernmündlicher Auskünfte aus Zentralnamenskarteien nicht immer eindeutige Klarheit über die Identität des Anrufers besteht. Um zu verhindern, daß Unberechtigte Kenntnisse aus Zentralnamenskarteien erlangen, sollten telefonische Auskünfte daher nach Möglichkeit unterbleiben oder allenfalls dann erteilt werden, wenn die Identität des Gesprächspartners eindeutig feststeht.

Teilweise liegen den Strafakten, die an andere Behörden versandt werden, Auszüge aus Zentralnamenskarteien bei. Auf diese Weise erlangen diese Behörden möglicherweise von Vorgängen Kenntnis, die sie zur Aufgabenerfüllung nicht benötigen. Im Hinblick auf die vorgenannten Mindestanforderungen müssen derartige Auszüge vor Versendung der Strafakten aus diesen entfernt werden.

Die Richtigkeit der Daten ist ein wesentliches Anliegen des Datenschutzes. Dies gilt selbstverständlich auch bei der Speicherung sensibler Daten in den zentralen Namenskarteien. Wird ein Verfahren nach § 170 Abs. 2 StPO eingestellt oder erfolgt Freispruch, ist zu prüfen, inwieweit diese Tatsachen entweder ausdrücklich in den Zentralnamenskarteien vermerkt oder aber die entsprechenden Eintragungen gelöscht werden. Je belastender die Eintragungen für den Betroffenen sind, desto mehr muß darauf geachtet werden, daß die Eintragungen richtig sind. Wird beispielsweise neben dem Tatvorwurf die Tatsache der Anklageerhebung niedergelegt, muß der Freispruch eingetragen werden. Dies gilt zumal dann, wenn die Zentralnamenskarteien nicht ausschließlich internen Zwecken der Staatsanwaltschaft dienen.

Weil belastende Daten nicht über den unbedingt erforderlichen Zeitraum hinaus gespeichert werden dürfen, ist die Frist erheblich zu verkürzen, innerhalb der die Zentralnamenskarteien zur gewöhnlichen Sachbearbeitung zur Verfügung stehen. Eventuell sind für Sperrung und Löschung dieser Daten unter Berücksichtigung des Grundsatzes der Verhältnismäßigkeit zeitlich abgestufte Fristen entsprechend der Schwere der im Einzelfall zur Last gelegten Straftat und des weiteren strafrechtlich relevanten Verhaltens des Einzelnen zu erwägen. Die technischen und organisatorischen Maßnahmen bei den Staatsanwaltschaften München I und Nürnberg-Fürth beispielsweise erlauben durch abgestufte Aussonderungsfristen die Berücksichtigung der individuellen Besonderheiten der einzelnen Betroffenen. Die Lösungen sind der begrüßenswerte Beweis dafür, daß mit einem sinnvollen Automatisierungskonzept den schutzwürdigen Belangen der Betroffenen manchmal besser entsprochen werden kann, als durch wenig flexible manuelle Verfahren.

Ich habe das Bayer. Staatsministerium der Justiz gebeten, die in den Mindestanforderungen für den Datenschutz bei den Zentralnamenskarteien der Staatsanwaltschaften enthaltenen Grundsätze bei der Führung dieser Karteien künftig zu berücksichtigen.

3.3.4 Pressemitteilungen der Staatsanwaltschaften bei Verfahren gegen Abgeordnete und Senatoren

In jüngster Zeit wurde mehrfach Beschwerde darüber geführt, daß die Staatsanwaltschaften bei Verfahren gegen Abgeordnete oder gegen Regierungsmitglieder den Namen der betroffenen Abgeordneten öffentlich nennen, wenn sie bei Verdacht einer Straftat die Aufhebung der Immunität beantragen. Dadurch würden schutzwürdige Belange beeinträchtigt.

Auf derartige Vorgänge ist das Bayer. Datenschutzgesetz grundsätzlich nicht unmittelbar anwendbar, weil die in Rede stehenden Angaben im Regelfall aus den Strafakten selbst stammen. Allerdings bestimmen die Richtlinien für das Strafverfahren und das Bußgeldverfahren folgendes:

„Der Staatsanwalt vermeidet alles, was zu einer nicht durch den Zweck des Ermittlungsverfahrens bedingten Bloßstellung des Beschuldigten führen kann."

Mit dem Bundesbeauftragten für den Datenschutz, der von der Vizepräsidentin des Deutschen Bundestages auf diese Thematik angesprochen worden war, bin ich der Ansicht, daß diese Bestimmung in den Richtlinien grundsätzlich ausreicht, um auch Abgeordnete und Regierungsmitglieder angemessen zu schützen. Allerdings ist aber zu berücksichtigen, daß Personen der Zeitgeschichte – als solche sind Abge-

ordnete und Regierungsmitglieder grundsätzlich anzusehen – bei der Abwägung zwischen ihrem Persönlichkeitsrecht und dem durch Art. 5 Grundgesetz abgestützten Interesse der Öffentlichkeit an Information von der Rechtsprechung nur ein eingeschränkter Schutz eingeräumt wird.

Das Bayer. Staatsministerium der Justiz hat mir auf eine entsprechende Anfrage mitgeteilt, daß die Staatsanwaltschaften in Bayern von sich aus keine Pressemitteilungen herausgeben, wenn sie eine Vorlage an den Bayer. Landtag oder an den Bayer. Senat zum Zwecke der Herbeiführung einer Entscheidung über die Aufhebung der Immunität leiten. In der Vergangenheit seien derartige Verfahren allerdings häufig deshalb öffentlich bekannt geworden, weil die Medien aus dem Parlament entsprechende Informationen erhalten hätten – dies erscheint mir nicht unbedenklich. Im übrigen würden die bayerischen Staatsanwaltschaften auch bei der Beantwortung diesbezüglicher Anfragen durch Mitarbeiter von Presse und Rundfunk selbstverständlich die Richtlinien für das Strafverfahren und das Bußgeldverfahren beachten.

3.3.5 Schuldnerverzeichnis

Zu dem nach § 915 Zivilprozeßordnung (ZPO) vom Amtsgericht – Vollstreckungsgericht zu führenden Schuldnerverzeichnis habe ich aus datenschutzrechtlicher Sicht bereits kurz in meinem 3. Tätigkeitsbericht Stellung genommen. Darin habe ich darauf hingewiesen, daß der Bundesminister der Justiz den Entwurf einer Verordnung über Abschriften aus dem Schuldnerverzeichnis erarbeitet hat. Bislang ist die Verordnung noch nicht in Kraft getreten.

Wiewohl ich den Entwurf aus der Sicht des Datenschutzes als Verbesserung gegenüber der bisherigen Rechtslage grundsätzlich begrüße, erscheint es mir notwendig, nochmals auf die Probleme der Erteilung von Abschriften und Auszügen aus dem Schuldnerverzeichnis hinzuweisen, denen meines Erachtens im Verordnungsentwurf nicht ausreichend Rechnung getragen ist:

Die bisherigen Erfahrungen aus Überprüfungen bei Zweitempfängern von Daten aus dem Schuldnerverzeichnis zeigen, daß Abschriften und Auszüge aus dem Schuldnerverzeichnis über die Löschungsfrist hinaus aufbewahrt werden, die für das Schuldnerverzeichnis selbst gilt. Wegen dieser Tatsache erscheint es mir sehr bedenklich, wenn die öffentlich-rechtlichen Berufsvertretungen, die Abschriften aus den Schuldnerverzeichnissen erhalten, ihren Mitgliedern und den Mitgliedern einer gleichen öffentlich-rechtlichen Berufsvertretung Abschriften zugänglich machen dürfen. Bei einer derart breiten Streuung auf einen großen Empfängerkreis wird die Gefahr des Mißbrauchs dieser sensiblen Daten erhöht und ist die Beachtung der Löschungsfrist des § 915 Abs. 2 ZPO trotz der im Verordnungsentwurf vorgesehenen Maßnahme nicht gewährleistet.

Im übrigen läßt die Regelung dieses Entwurfs nicht erkennen, daß eine Art. 18 Abs. 1 BayDSG für die Datenübermittlung an Stellen außerhalb des öffentlichen Bereichs vergleichbare Pflicht zur Interessenabwägung berücksichtigt ist. Die Beachtung der schutzwürdigen Belange der Betroffenen beispielsweise ist aber ein über das Datenschutzrecht hinausreichender Grundsatz. Meines Erachtens kann weder unterstellt werden, daß alle Mitglieder von Berufsvertretungen, die eine entsprechende schriftliche Anforderung auf Erteilung von Abschriften stellen, ein berechtigtes Interesse an der Kenntnis aller im Schuldnerverzeichnis eingetragener Personen haben, noch daß in allen Fällen trotz einer derart umfassenden Übermittlung schutzwürdige Belange der Betroffenen unbeeinträchtigt bleiben. Bei diesen Erwägungen ist zu beachten, daß selbst die berufliche und geschäftliche Tätigkeit des Einzelnen – auch mit deren Folgen, die zu einer Eintragung in das Schuldnerverzeichnis führen können – grundsätzlich seiner persönlichen Sphäre zuzuordnen ist (BGH 24, S. 200/208). Aus der Tatsache, daß der Persönlichkeitsschutz der gewerblichen Tätigkeit nicht so weit reicht wie der Schutz des privaten Bereichs im engeren Sinne (BGH 36, S. 77/80) kann der Schluß gezogen werden, daß die Übermittlung von Abschriften an Mitglieder von Berufsvertretungen, sofern diese nicht gänzlich untersagt wird, zumindest auf gewerblich Tätige beschränkt werden sollte.

Eine weitere gravierende Schwachstelle des vorliegenden Verordnungsentwurfes scheint mir noch der Erwähnung wert:

Während § 915 Abs. 4 Satz 1 Zivilprozeßordnung die Erteilung von Abschriften aus dem Schuldnerverzeichnis unter dem Vorbehalt der gesicherten Einhaltung der Löschungsfrist gestattet, ist im Verordnungsentwurf (§ 1 Abs. 1 Satz 1) die generelle Verpflichtung zur Erteilung von Abschriften enthalten. Damit könnte die Erteilung von Abschriften an möglicherweise amtsbekannt unzuverlässige Personen erst dann verweigert werden, wenn ausdrücklich der Widerruf der diesbezüglichen Genehmigung ausgesprochen worden ist. Dann kann aber im Einzelfall bereits ein Mißbrauch dieser besonders sensiblen Daten eingetreten sein. Meines Erachtens sollte daher dem, der für die Entscheidung über den entsprechenden Antrag auf Erteilung von Abschriften zuständig ist, ein Ermessensspielraum bei der Erteilung von Abschriften eingeräumt werden.

3.3.6 Auskunftsersuchen des Amtsgerichts über wirtschaftliche Verhältnisse von Bürgern

Einzelne Amtsgerichte ersuchen Gemeinden um Auskünfte darüber, ob zu einer bestimmten Person Nachteiliges über deren wirtschaftliche Verhältnisse bekannt sei. Sofern derartige Anfragen dann erfolgen, wenn minderjährige Kinder durch eine letztwillige Verfügung von der Erbfolge nach einem verstorbenen Elternteil ausgeschlossen sind und eine dingliche Sicherung der ihnen zustehenden Pflichtteilsforderung nicht vereinbart worden ist, ist zur Rechtslage folgendes festzustellen:

Allgemein gilt, daß das Amtsgericht – Vormundschaftsgericht entsprechend dem das Vormundschaftsrecht beherrschenden Offizialprinzip von

Amts wegen tätig wird und die erforderlichen Ermittlungen anzustellen hat (§ 12 FGG). Sofern der Pflichtteilsanspruch eines Kindes gegenüber einem verstorbenen Elternteil gefährdet ist, hat das Vormundschaftsgericht ein Verfahren zur Bestellung eines Pflegers für die Geltendmachung des Pflichtteils einzuleiten. Zunächst muß das Vormundschaftsgericht jedoch prüfen, ob der überlebende Ehegatte das durch das Testament in ihn gesetze Vertrauen nach Charakter, Wirtschafts- und Lebensführung verdient oder ob die Besorgnis besteht, daß eine etwaige später angezeigte Geltendmachung der Pflichtteilsansprüche, z.B. im Falle einer Wiederverheiratung, gefährdet sein würde, wenn diese Ansprüche nicht schon jetzt erhoben werden. Außerdem stellt das Vormundschaftsgericht fest, ob sonst irgendwelche wichtigen Umstände erkennbar sind, die zur Verhinderung dauernder Nachteile die vorzeitige Erhebung der Pflichtteilsansprüche als angezeigt erscheinen lassen (KG JW 36 S. 2748). Eine Gefährdung des Pflichtteilsanspruchs eines minderjährigen Kindes kann schon darin liegen, daß der überlebende Ehegatte in Vermögensverfall gerät oder hinsichtlich der Vermögensverwaltung sich Pflichtverletzungen hat zuschulden kommen lassen. In derartigen Fällen hätte der Vormundschaftsrichter zumindest auf eine Sicherstellung des Pflichtteilsanspruchs hinzuwirken oder die Pflegschaft zur Geltendmachung des Pflichtteils einzuleiten.

Soweit das Vormundschaftsgericht mögliche Gefährdungen für den Pflichtteilsanspruch des Kindes prüft, hat es nach dem obengenannten § 12 FGG alle Ermittlungen anzustellen, die zur Aufklärung des Sachverhalts notwendig sind. Zu diesen Ermittlungen gehören grundsätzlich auch Anfragen bei anderen Behörden, die über die Vermögenssituation des überlebenden Elternteils Auskunft geben können. Neben dem Vollstreckungsgericht kann im Einzelfall grundsätzlich auch die Gemeinde Angaben über die Vermögensverhältnisse eines überlebenden Elternteils machen. Sofern die der Gemeinde bekannten Angaben zu den Vermögensverhältnissen des überlebenden Elternteils nicht einem besonderen Geheimnis (z.B. Steuergeheimnis, Sozialgeheimnis) unterliegen, darf sie derartige gerichtliche Anfragen grundsätzlich beantworten.

Das Gericht hat hierbei den Verhältnismäßigkeitsgrundsatz zu beachten. Dem überlebenden Elternteil, der von einer solchen Anfrage betroffen wird, dürfen dadurch möglichst keine Nachteile entstehen. Daher sollten solche Anfragen nur dann an die Gemeinde gerichtet werden, wenn nicht bereits aus anderen Quellen – beispielsweise durch Anfrage beim Vollstreckungsgericht – eindeutige Aussagen über die Vermögensverhältnisse des Betroffenen gewonnen werden können und außerdem im konkreten Einzelfall zu erwarten ist, daß die ersuchte Gemeinde tatsächlich über die wirtschaftlichen Verhältnisse des Betroffenen Auskünfte erteilen kann. Letzteres dürfte im Regelfall dann ausgeschlossen sein, wenn wegen der Größe der Gemeinde Kenntnisse über Einzelpersonen nicht mehr erwartet werden können.

Schließlich erscheint es mir sinnvoll, wenn zur Vermeidung möglicherweise unrichtiger Vermutungen über den Grund der Anfrage im jeweiligen Ersuchen hinreichend deutlich gemacht werden könnte, daß die Anfrage rein vorsorglich gestellt und kein Verfahren zu Lasten des Betroffenen geführt wird.

3.3.7 Benachrichtigungen in Nachlaßsachen

Ein Bürger hat mir mitgeteilt, daß er vom Amtsgericht eine Mitteilung in Nachlaßsachen auf offener Postkarte erhalten habe. Auf dieser Postkarte waren Name, Geburtsdatum und Sterbedatum des Erblassers vermerkt (zur Datenübermittlung auf Postkarten siehe auch 3.10.2).

Auf meine entsprechende Anfrage hat das Bayer. Staatsministerium der Justiz mitgeteilt, daß Ladungen und Benachrichtigungen in Nachlaßsachen weitgehend als Briefe versandt würden. Nur gelegentlich würden einige Gerichte dafür auch Postkarten verwenden, sofern nicht gleichzeitig weitere Schriftstücke zu versenden seien. Eine Änderung der bestehenden Praxis sei nicht veranlaßt. Die Benachrichtigung enthielte nur Geburts- und Sterbedaten des Erblassers, die auf jedem Grabstein, Friedhofsaushang und in jeder Todesanzeige zu finden seien.

Der dieser Begründung offensichtlich zugrundeliegenden Ansicht, daß schutzwürdige Belange durch die Versendung derartiger Daten auf offener Postkarte nicht berührt würden, konnte ich in dieser Form nicht folgen.

Es mag dahin stehen, ob das Persönlichkeitsrecht nach dem Tode erlischt oder nur eine Einschränkung erleidet. In Nachlaßangelegenheiten können jedoch Rechte Lebender, nämlich der Angehörigen eines Verstorbenen berührt sein. Durch die Übermittlung der Daten über einen Verstorbenen werden konkludent die Tatsache eines Todesfalles im näheren Lebenskreis des Empfängers der Postkarte – im konkreten Fall war dies die Mutter des Beschwerdeführers –, die Möglichkeit der Erlangung einer Erbschaft und in Einzelfällen der Grad der Verwandtschaft oder der sonstigen Beziehungen zwischen Verstorbenen und Empfänger der Postkarte mitgeteilt. Die Angaben zu Vor- und Nachname, einschließlich des Geburtsnamens des Verstorbenen und dessen Todeszeitpunkt gewinnen durch diesen Bezug zu einer lebenden Person ein anderes Gewicht, als vergleichbare Angaben auf einem Grabstein, einem Friedhofsaushang oder in einer Todesanzeige. Ganz abgesehen davon, dürften die letztgenannten Veröffentlichungen grundsätzlich auf dem Willen der Angehörigen beruhen. Die auf diese Weise auf einer offenen Postkarte mitgeteilten Daten betreffen dagegen den privaten Lebensbereich eines Betroffenen und könnten durchaus dessen schutzwürdige Belange berühren. Im übrigen hat gerade die hierzu eingegangene Eingabe gezeigt, daß in diesem Bereich durchaus eine Sensibilität unter den Bürgern besteht.

In diesem Zusammenhang habe ich festgestellt, daß zwischenzeitlich die Übermittlung von Daten von öffentlichen Stellen an Private in vielen Fällen entgegen der früheren Übung nicht mehr auf offenen Postkar-

ten erfolgt. Selbst bei Verwendung von Briefen wird nun von Aufdrucken auf den Briefumschlägen abgesehen, die einen Hinweis auf den Inhalt der Sendung enthalten. Auch bei der Verwendung von sogenannten Fensterkuverts wird dafür Sorge getragen, daß durch entsprechendes Einlegen des Schreibens Unberechtigte nicht von dessen Inhalt Kenntnis erlangen können. Diese Änderung der Sachbehandlung bei Versendung von Daten aus dem öffentlichen Bereich an Private macht einen zwischenzeitlich eingetretenen Bewußtseinswandel in der Wahrung schutzwürdiger Belange Betroffener deutlich. Diese Änderung wurde unabhängig von der unmittelbaren Anwendbarkeit des Bayer. Datenschutzgesetzes im Einzelfall erreicht.

In der oben angesprochenen Nachlaßsache hat aufgrund meiner nochmaligen Vorstellungen das Bayer. Staatsministerium der Justiz die Angelegenheit erneut überprüft und zwischenzeitlich die nachgeordneten Behörden angewiesen, Ladungen und Benachrichtigungen in Nachlaßsachen künftig einheitlich im verschlossenen Briefumschlag zu versenden. Dies begrüße ich.

3.3.8 Hauptverhandlung

Die nachfolgenden Fragen gehören nicht zum Datenschutzbereich im engeren Sinne. Insoweit mache ich von meinem mir durch Art. 28 Abs. 4 Satz 2 BayDSG eingeräumten Recht Gebrauch, Verbesserungen des Datenschutzes anzuregen.

Mehrfach haben sich Bürger an mich gewandt und haben Klage geführt, daß sie vor Gericht als Zeugen Auskunft über Geburtstag, Wohnung und Familienstand geben mußten, obwohl erkennbar diese Angaben für die Beurteilung der Zeugenaussage keine Rolle gespielt hätten. Nach § 68 Satz 1 StPO und § 395 Abs. 2 ZPO beginnt die Vernehmung des Zeugen damit, daß er über Vor- und Zunamen, Alter, Stand oder Gewerbe und Wohnung befragt wird. Obwohl die Frage nach dem Familienstand in diesen Vorschriften nicht ausdrücklich genannt wird, scheint sie doch in Gerichtsverhandlungen üblicherweise gestellt zu werden. Wenn ich auch grundsätzlich gegen eine Überspitzung des Begriffs „schutzwürdige Belange" bin, gebe ich zu erwägen, ob die Richter darauf hingewiesen werden könnten, daß die Frage nach Familienstand und Alter nur in den Fällen gestellt werden sollte, wo sie entscheidungserheblich ist. De lege ferenda ist zu prüfen, inwieweit auf die Frage nach dem Alter dann verzichtet werden kann, wenn der Zeuge ersichtlich einer Altersgruppe angehört, für die sich aus der Kenntnis des genauen Alters keine gesetzlich bestimmten Rechtsfolgen ableiten lassen und das Alter auch ansonsten keine Bedeutung für das Verfahren besitzt.

Neben der Frage nach der Zulässigkeit der Erhebung dieser Personalangaben bin ich auch mit den Problemen der Öffentlichkeit der Hauptverhandlungen vor Gericht konfrontiert worden. Es wurde verschiedentlich vorgetragen, daß durch die Vernehmung von Angeklagten oder von Zeugen sowie die Verlesung medizinischer Gutachten in öffentlicher Sitzung schutzwürdige Belange der Bürger wesentlich beeinträchtigt würden. Ich habe die Bürger jeweils darauf hingewiesen, daß das Bayer. Datenschutzgesetz auf die Durchführung einer gerichtlichen Verhandlung grundsätzlich nicht anwendbar ist.

Ich bin jedoch der Ansicht, daß auch diese Fragen einer Diskussion unterzogen werden sollten. Denn der in § 169 Satz 1 Gerichtsverfassungsgesetz (GVG) niedergelegte Grundsatz der Öffentlichkeit der Verhandlungen vor Gericht dient in erster Linie dem Informationsinteresse der Allgemeinheit. Dagegen haben die ursprünglichen Gründe für die Verfahrensöffentlichkeit, nämlich die öffentliche Kontrolle der Rechtsprechung und der Schutz vor Willkür, ihre Bedeutung heute weitgehend eingebüßt. Auch im Hinblick auf diesen Bedeutungswandel des Öffentlichkeitsgrundsatzes muß dieser gegenüber dem verfassungsrechtlich garantierten Schutz der Persönlichkeit des Angeklagten und der anderen Verfahrensbeteiligten im Einzelfall eingeschränkt werden. Die Möglichkeit des Ausschlusses der Öffentlichkeit – wenn Umstände aus dem persönlichen Lebensbereich eines Verfahrensbeteiligten zur Sprache kommen, durch deren öffentliche Erörterung überwiegend schutzwürdige Interessen verletzt würden – ist in § 172 Nr. 2 GVG gesetzlich niedergelegt. Dem Gericht wächst nun aus seiner prozessualen Fürsorgepflicht die Aufgabe zu, das Verfahren so zu gestalten, daß der Persönlichkeitsschutz möglichst gewahrt wird. Dies kann im Einzelfall den Ausschluß der Öffentlichkeit bedeuten. In diesem Zusammenhang ist zu beachten, daß selbst der Straftäter grundsätzlich ein Recht auf Achtung seiner Persönlichkeit hat, wie das Bundesverfassungsgericht (E 35, 202/233) festgestellt hat.

Die Entscheidung, wo konkret die Grenze für die grundsätzlich bedeutsame Öffentlichkeit der gerichtlichen Verhandlung zu ziehen ist, kommt allein dem Gericht zu. Es wird jedoch zu beobachten sein, inwieweit die Gerichte insbesondere im Hinblick auf die kürzlich zu dieser Thematik ergangene Entscheidung des Bundesgerichtshofs in Zukunft den Schutz der Persönlichkeit bei der Abwägung mit der Bedeutung der Öffentlichkeit der gerichtlichen Verhandlung stärker berücksichtigen. Gegebenenfalls könnte eine Gesetzesänderung zu erwägen sein.

3.4 Sozial- und Gesundheitsbereich

3.4.1 Änderung der Datenschutzbestimmungen des X. Buches zum SGB

Durch das Gesetz zur Bekämpfung der illegalen Beschäftigung (BillBG, BGBl I 1981, S. 1389ff, Art. 7) wird § 71 Nr. 3 SGB X geändert. Die Vorschrift eröffnet die Möglichkeit zur Offenbarung von Sozialdaten für die Erfüllung besonderer ausdrücklich genannter gesetzlicher Mitteilungspflichten. Das BillBG erweitert die Offenbarungsmöglichkeit gegenüber Steuerbehörden. Nach der amtlichen Begründung soll die Änderung klarstellen, „daß von dieser Regelung auch Auskünfte im Rahmen der Amtshilfe und Auskünfte zur Vollstreckung erfaßt werden sollen".

Die Begründung verschweigt jedoch, daß sich diese Änderung nicht wie das BillBG im übrigen auf die Bekämpfung der illegalen Beschäftigung beschränkt,

sondern die Offenbarung von Sozialdaten gegenüber Finanzämtern auch in anderen Fällen erweitert. Eine Diskussion darüber, die Offenbarungsmöglichkeit von Sozialdaten gegenüber Finanzämtern über den Bereich der Bekämpfung der Schwarzarbeit hinaus zu erweitern, hat meines Wissens nicht stattgefunden – jedenfalls wurde bei der Erörterung des Bundesgesetzentwurfs in Bayern der Landesbeauftragte für den Datenschutz in eine solche Erörterung nicht einbezogen. Dies bedauere ich.

Ich bin der Ansicht, daß der Landesbeauftragte für den Datenschutz in die Erörterung von Gesetz, Verordnungs- oder Richtlinienentwürfen, die den Datenschutz berühren, grundsätzlich eingeschaltet werden sollte – um so mehr, als er nach Inkrafttreten der Datenschutzregelungen deren korrekten Vollzug zu kontrollieren hat. Ich meine, daß Gesetze, Verordnungen oder Richtlinien, die Datenschutzrechte einräumen oder beschränken, die Stellung des Betroffenen oft tiefgreifender berühren können, als ein in einem Einzelfall unkorrekter Vollzug durch eine öffentliche Stelle.

3.4.2 Anwendung der Vorschriften über den Sozialdatenschutz im kommunalen Bereich (SGB X)

Die neuen Vorschriften über den Schutz der Sozialdaten im 10. Buch des Sozialgesetzbuches (SGB X) sind auch im kommunalen Bereich der Sozialleistungsträger anzuwenden. Hierbei hatten sich Unklarheiten vor allem auch in anderen Bundesländern ergeben, die die Offenbarung von Sozialdaten durch die jeweilige Sozialleistungsverwaltung gegenüber der sonstigen Verwaltung der Stadt oder des Kreises betraf.

Die Datenschutzbeauftragten der Länder und des Bundes haben sich damit befaßt und festgestellt:

1. Die Bestimmungen über das Sozialgeheimnis bzw. den Schutz der Sozialdaten sowie ergänzend die Vorschriften des Bundesdatenschutzgesetzes gelten innerhalb von Stadt- und Kreisverwaltungen für alle Ämter und Stellen insoweit, als sie Aufgaben nach dem SGB wahrnehmen.

2. Insbesondere finden die Regelungen über die Offenbarung von Sozialdaten (§§ 35 SGB I, 67 ff SGB X) auch gegenüber anderen Ämtern und Stellen der gleichen kommunalen Gebietskörperschaft Anwendung.

3. Bestrebungen, das Sozialgeheimnis in den Kommunen mit einer sog. „ganzheitlichen Interpretation des kommunalen Behördenbegriffs", über allgemeine Amtshilfegrundsätze oder ähnliche Konstruktionen einzuschränken, treten die Datenschutzbeauftragten entgegen. Die Bestrebungen widersprechen §§ 35 SGB I, 67 ff SGB X.

4. Der Geheimhaltungsanspruch nach § 35 Abs. 1 Satz 1 SGB I richtet sich zwar gegen den Leistungsträger, also gegen die jeweilige Körperschaft, Anstalt oder Behörde (§ 12 SGB I). Eine Offenbarung im Sinne dieser Vorschrift liegt jedoch auch dann vor, wenn personenbezogene Daten innerhalb eines Leistungsträgers weitergegeben werden. Dieser hat dafür zu sorgen, daß die ihm bekanntgewordenen Sozialdaten auch innerhalb des Leistungsträgers nicht unbefugt offenbart werden. Er hat dementsprechend sicherzustellen, daß diese Daten nur dem für die Bearbeitung und Entscheidung des einzelnen Falles zuständigen Personenkreis zugänglich sind (§ 69 Abs. 1 DNr. 1 SGB X).

5. Aus dem Verbot der unbefugten Offenbarung von Sozialdaten innerhalb des Leistungsträgers folgt, daß diese Daten erst recht gegenüber anderen Stellen innerhalb der Kommunalverwaltung geheimzuhalten sind und nur unter den Voraussetzungen der §§ 35 Abs. 2 SGB I, 67 bis 77 SGB X offenbart werden dürfen.

Zur Bestellung von internen Datenschutzbeauftragten nach dem SGB X § 79 Abs. 1, 2. Halbsatz sind die Datenschutzbeauftragten der Länder und des Bundes folgender Ansicht:

1. Aus § 27 Abs. 1, 2. Halbsatz SGB X i.V.m. §§ 28, 29 BDSG ergibt sich eine gesetzliche Verpflichtung auch für die Städte und Kreise, einen Bediensteten zum Verantwortlichen für die Sicherstellung der Ausführung der Bestimmungen über den Schutz der Sozialdaten zu bestellen. Auf die Bezeichnung „Datenschutzbeauftragter" kommt es dabei nicht an.

2. Anforderungsprofil, Stellung und Aufgabenbereich dieses Mitarbeiters ergeben sich grundsätzlich aus §§ 28, 29 BDSG. Abweichungen auf Grund der lediglich „entsprechenden" Anwendbarkeit dieser Normen sind nur da zulässig, wo Besonderheiten der kommunalen Verwaltungsstruktur dies zwingend erfordern. Dieser Bedienstete sollte daher
   - die erforderliche Fachkunde und Zuverlässigkeit besitzen
   - auf dem Gebiet des Sozialdatenschutzes weisungsfrei sein
   - der Behördenleitung für die Aufgabe des Sozialdatenschutzes unmittelbar unterstellt sein
   - die in § 29 aufgelisteten Aufgaben wahrnehmen.

3. Keine Bedenken bestehen, wenn Bedienstete, die wie in mehreren Bundesländern auf Grund von Erlassen, Richtlinien u.ä. bereits bisher die Aufgaben eines „kommunalen Datenschutzbeauftragten" wahrnehmen, auch diese Funktion nach § 79 SGB X mitübernehmen, sofern die unter 2. genannten Voraussetzungen erfüllt sind. Auch in diesem Fall ist eine entsprechende schriftliche Bestellung notwendig.

3.4.3 Verpflichtung auf das Datengeheimnis unter Berücksichtigung des Sozialdatenschutzes

Bei der Verpflichtung der bei der Datenverarbeitung beschäftigten Personen auf das Datengeheimnis ist seit Inkrafttreten der neuen Vorschriften des Sozialgesetzbuches (1. 1. 1981) § 5 des Bundesdatenschutzgesetzes zu berücksichtigen. Während nach

Art. 14 Absatz 2 des Bayerischen Datenschutzgesetzes nur die bei der automatisierten Datenverarbeitung beschäftigten Personen auf das Datengeheimnis nach Art. 14 Abs. 1 BayDSG zu verpflichten waren, verlangt § 5 BDSG (in Verbindung mit § 79 Abs. 1 SGB X) die Verpflichtung auch von Personal, das in nicht-automatisierten Verfahren Daten in Dateien verarbeitet, auf das Datengeheimnis.

Nachdem ab 1. 1. 1981 die bei der Datenverarbeitung beschäftigten Bediensteten von Sozialleistungsträgern gleichzeitig auch die Neufassung des § 35 SGB I und die Vorschriften der §§ 67–85 SGB X zu beachten haben, halte ich es für erforderlich, bei der Verpflichtung dafür zu sorgen, daß von diesen Sondervorschriften Kenntnis genommen wird. Ich habe auf Anfrage von kommunalen Sozialleistungsträgern daher vorgeschlagen, allen bereits gemäß Art. 14 Abs. 1 BayDSG verpflichteten Personen die Vorschriften des neuen Sozialdatenschutzes zur Kenntnis zu geben, sowie die entsprechend § 5 BDSG noch zusätzlich zu verpflichtenden Personen bei dieser Gelegenheit ebenfalls auf die neuen Vorschriften hinzuweisen.

3.4.4 Anwendbarkeit der Vorschrift über den Schutz der Sozialdaten auf Adoptionsvermittlungsstellen

Mit dem Inkrafttreten des X. Buches des SGB sind eine Reihe von Auslegungsfragen aufgetreten, die derzeit noch nicht abschließend geklärt sind. Zu diesen Problemen zählt auch die Frage nach dem Anwendungsbereich der Bestimmungen zum Schutz der Sozialdaten. Nach meinem gegenwärtigen Erkenntnisstand vertrete ich dazu die Auffassung, daß das in § 35 SGB I begründete Sozialgeheimnis für alle personenbezogenen Daten gilt, die einem Sozialleistungsträger für die Erfüllung seiner gesetzlichen Aufgaben nach dem SGB bekannt geworden sind. Nicht unter § 35 SGB I fallen demnach Daten, die der Leistungsträger als Arbeitgeber, für fiskalische Zwecke oder in Erfüllung einer gesetzlichen Aufgabe außerhalb des Sozialgesetzbuches speichert.

Das Landesjugendamt und die Jugendämter zählen gemäß § 27 Abs. 2 SGB I zwar zu den Leistungsträgern im Sinne des Sozialgesetzbuches. Die Adoptionsvermittlung wird diesen Stellen aber durch das Adoptionsvermittlungsgesetz als gesetzliche Aufgabe zugewiesen. Dieses Gesetz fehlt in der Aufzählung in Art. II § 1 SGB I und gilt daher nicht als besonderer Teil des Sozialgesetzbuches. § 78a Jugendwohlfahrtsgesetz (JWG) ist in diesem Zusammenhang meines Erachtens als Zulässigkeitsnorm für die Datenübermittlung an das Landesjugendamt, nicht aber als Aufgabenzuweisung für diese Stelle zu verstehen. Eine unmittelbare Anwendung der Bestimmungen zum Schutz der Sozialdaten nach SGB X kommt für die Adoptionsvermittlung daher nicht in Betracht.

Zu beachten ist jedoch das Zweckbindungsgebot des § 78 SGB X. Danach dürfen Adoptionsvermittlungsstellen und die Zentrale Adoptionsstelle des Landesjugendamtes personenbezogene Daten, die sie im Rahmen des JWG oder von anderen Sozialleistungsträgern befugt erfahren haben, nur zweckgebunden verwenden. Im übrigen sind diese Daten entsprechend der §§ 67 ff SGB X geheimzuhalten. Für die übrigen Daten gelten die Bestimmungen des Bayerischen Datenschutzgesetzes. § 1758 BGB ist dabei als vorrangige Rechtsvorschrift im Sinne des Art. 2 Abs. 2 BayDSG zusätzlich besonders zu beachten. Wegen der besonderen Geheimhaltungserfordernis der Adoptionsvermittlung ist eine mögliche Beeinträchtigung schutzwürdiger Belange der Betroffenen sorgfältig zu prüfen.

3.4.5 Meldungen über Krankenhausaufenthalt an das Sozialamt

Ein Stadtkrankenhaus hatte zur Wahrung der Anmeldefristen gemäß § 121 BSHG dem zuständigen Sozialhilfeträger die Krankenhausaufnahme jedes im Krankenhaus behandelten Patienten vorsorglich gemeldet. Diese Meldungen waren in der weit überwiegenden Mehrzahl der Fälle zur Klärung der Kostenübernahme durch das Sozialamt jedoch nicht erforderlich, da andere Kostenträger (z. B. Krankenkassen) zuständig waren und die Kosten auch übernommen haben.

Nach Art. 13 Abs. 4 des Bayerischen Krankenhausgesetzes darf die Krankenhausverwaltung gespeicherte Patientendaten nur weitergeben, soweit dies zur verwaltungsmäßigen Abwicklung der Behandlung des betroffenden Patienten erforderlich ist. Nach dem Wortlaut des Gesetzes muß die Erforderlichkeit der Weitergabe von Patientendaten im Einzelfall festgestellt werden. Eine vorsorgliche Meldung aller Patienten an das Sozialamt ist demzufolge unzulässig und war zu beanstanden.

Die Datenweitergabe war mit einer möglichen Fristversäumnis begründet worden. Die Frist für die Antragstellung auf Erstattung von Aufwendungen im Sinne des § 121 BSHG bestimmt sich nach den besonderen Verhältnissen des Einzelfalls. Ich habe daher empfohlen auf örtlicher Ebene entsprechende Absprachen zwischen Krankenhaus und Sozialhilfeträger zu treffen, um ein solches Fristversäumnis zu verhindern.

Das Bayerische Staatsministerium für Arbeit und Sozialordnung hat in einer Stellungnahme zum angegebenen Sachverhalt eine generelle Klärung des Verhältnisses Krankenhaus/Sozialhilfeverwaltung für notwendig erachtet und eine entsprechende Prüfung durch die für die Sozialhilfe zuständige Abteilung des Hauses eingeleitet.

3.4.6 Sozialbericht Suchtkranke

Die Problematik des „Sozialbericht Suchtkranke", der u. a. für Rentenversicherungsträger erstellt wird, ist im zweiten Tätigkeitsbericht (Nr. 4.1.4.3, S. 22) kurz dargestellt worden. Zusammen mit den Landesbeauftragten und dem Bundesbeauftragten für den Datenschutz wurden inzwischen die aus der Sicht des Datenschutzes an eine Datenerhebung über Suchtkranke für Zwecke der Rentenversicherung zu stellenden Forderungen definiert. Die Konferenz der Datenschutzbeauftragten der Länder und des Bundes hat in ihrer Sitzung am 28./29. 9. 1981 folgendes beschlossen:

„Für die nach § 1236 RVO und den sonstigen einschlägigen Bestimmungen (z.B. das Angestellten- und Knappschaftsversicherungsrechts) von den Leistungsträgern zu treffenden Entscheidungen wird ein Formular ‚Sozialbericht' verwendet, dessen bisherige Fassung nicht den datenschutzrechtlichen Anforderungen entspricht. Das Formular sollte klarer als bisher erkennbar machen, daß die Mitwirkung des Betroffenen durch § 60 SGB I begrenzt wird. Erheblichkeit und Erforderlichkeit sind danach im Einzelfall zu prüfen, insbesondere im Hinblick auf

- Zuständigkeit für die Leistungsgewährung,
- Erfolgsaussichten der Suchtbehandlung,
- Zeitpunkt des Therapiebeginns,
- Auswahl der Behandlungsstätte und
- Auswahl der Leistungen zur Rehabilitation in dem in den §§ 1237–1237b RVO bestimmten Umfang.

Daraus folgt, daß das Formular nicht in allen Fällen vollständig auszufüllen ist (‚Rahmenformular'). Dies sollte durch einen Hinweis in der ‚ergänzenden Information' zum Sozialbericht klargestellt werden.

Es wird vorgeschlagen, das Formular wie folgt neu zu strukturieren:

1. Das Formular wird in einen datenerhebenden und einen bewertenden Teil gegliedert. Der erhebende Teil hat sich auf Tatsachenfeststellungen beim Betroffenen zu beschränken. Der bewertende Teil enthält die Begutachtung des Sozialarbeiters und etwaige von diesem erhobene anderweitige Tatsachen. Für den erhebenden Teil kommen etwa die Fragen 1–3 und 5, für den bewertenden Teil die Fragen 4 und 6–10 des bisherigen Formulars in Betracht. Die zuständigen Leistungsträger wurden gebeten, in Zusammenarbeit mit den freien Wohlfahrtsverbänden das Formblatt auf dieser Grundlage neu zu gestalten.
2. In der ‚ergänzenden Information' zum Sozialbericht sollte auf folgende Punkte hingewiesen werden:
   a) Angaben zur Dosis des Rauschmittels werden nur bei Alkohol und ‚legalen' Medikamenten erhoben.
   b) auf die Tatsache, daß strafrechtlich relevante Hinweise nicht gegeben zu werden brauchen, sollte wegen der besonderen Bedeutung gerade bei den nach Ziffer 4 zu erhebenden Daten dort nochmals hingewiesen werden.
   c) Daten über laufende Strafverfahren und unverbüßte Haftstrafen sind nur zu erheben, soweit diese in den Zeitraum der Rehabilitationsmaßnahme fallen können.
   d) Daten, die nur für die Behandlung des Betroffenen relevant sind, dürfen nicht erhoben werden, da § 1236 RVO insoweit keine Rechtsgrundlage bietet. Sie können jedoch mit Einwilligung des Betroffenen erhoben und den Behandlungseinrichtungen direkt zugeleitet werden."

Im Beschluß der Konferenz werden außerdem Forderungen an die im Anschluß an den Sozialbericht abzugebende „Erklärung des Betreuten" erhoben. Im wesentlichen betreffen sie die Unterrichtung des Betreuten über die einschlägigen Vorschriften der RVO und über die Mitwirkung des Leistungsberechtigten und die Belehrung darüber, daß er zum Zwecke der Abfassung des Sozialberichts keine Hinweise zu geben braucht, die ihn oder nahestehende Personen der Gefahr strafrechtlicher Verfolgung oder eines Verfahrens nach dem Gesetz über Ordnungswidrigkeiten aussetzen.

Darauf hinzuweisen ist, daß in vielen Fällen eine vollständige Beantwortung der im Sozialbericht gestellten Fragen den Rahmen der Erforderlichkeit und damit der Mitwirkungspflicht des Leistungsberechtigten gemäß § 60 SGB I sprengt. Im Hinblick auf die besondere Sensibilität der erhobenen Daten kommt der Prüfung der Erforderlichkeit im Einzelfall besondere Bedeutung zu. Für erforderlich halte ich die Beantwortung der einzelnen Fragen nur, wenn dadurch erkennbar die Prüfung der Zuständigkeit für die Leistungsgewährung, die generellen Erfolgsaussichten der Suchtbehandlung, der Zeitpunkt des Therapiebeginns und die Auswahl der Behandlungsstätte beeinflußt wird. Angaben, die darüber hinaus für die Therapie von Bedeutung sind, sollten gegebenenfalls unmittelbar der Behandlungsstätte zugeleitet werden. In vielen Fällen wird in der Praxis bereits jetzt so verfahren. Die im Wesen eines Fragebogens liegende Schematisierung der Datenerhebung läßt möglicherweise die Neigung des Ausfüllenden aufkommen, die Angaben ohne nähere Prüfung der Erforderlichkeit zu machen. Die Erforderlichkeit zu prüfen, halte ich insbesondere bei der Erhebung von Daten über Wohnverhältnisse und finanzielle Verhältnisse, Vorgeschichte und derzeitiger Gesamtzustand und Sozialanamnese des Betreuten für erforderlich.

Die Datenschutzbeauftragten werden sich mit der Reaktion der Rentenversicherungsträger und freien Wohlfahrtsverbände auf ihre Forderung wieder befassen.

3.4.7 Weitergabe von Sozialdaten innerhalb einer „Zentralstelle für Strafentlassene"

In Bayern bestehen „Zentralstellen für Strafentlassene". Es handelt sich um Arbeitsgemeinschaften von Sozialleistungsträgern (Sozialamt, Arbeitsamt) und Verbänden der Freien Wohlfahrtspflege (Stadtmission, Caritasverband, Arbeitsamt, Arbeiterwohlfahrt, Arbeits-Resozialisierung, Bayerischer Landesverband für Gefangenenfürsorge und Bewährungshilfe), denen die Betreuung von Strafentlassenen im Gebiet der Städte obliegt. Im Rahmen ihrer Tätigkeit können Mitarbeiter der beteiligten Stellen auch Sozialdaten erfahren. Angesichts der neuen Vorschriften zum Schutz der Sozialdaten im X. Buch des SGB stellte sich daher die Frage der Zulässigkeit solcher Kenntnisnahmen durch andere Stellen als den jeweiligen Sozialleistungsträgern. Die rechtliche Stellung solcher Arbeitsgemeinschaften ist derzeit aus datenschutzrechtlicher Sicht noch nicht abschließend geregelt. Entsprechende Bestimmungen sind im 3. Kapitel zum X. Buch des Sozialgesetzbuches vorgesehen und befinden sich im Gesetzgebungsverfahren.

§ 28 Abs. 2 SGB I, § 10 Abs. 3 des Bundessozialhilfegesetzes (BSHG) und § 35 Abs. 1 BSHG dienen als Rechtsgrundlage für die Zusammenarbeit im Bereich der Sozialhilfe zwischen Sozialleistungsträgern und Trägern der Freien Wohlfahrtspflege. Eine Offenbarung von Sozialhilfedaten innerhalb der Arbeitsgemeinschaft ist deshalb im Rahmen des § 69 Abs. 1 Nr. 1 SGB X im erforderlichen Umfang als zulässig anzusehen.

Gleichartige Bestimmungen über eine Zusammenarbeit von Arbeitsämtern mit Trägern der Freien Wohlfahrtspflege im Rahmen der Leistung in der Arbeitsförderung (§ 19 SGB I) fehlen. Eine Offenbarung nach § 69 Abs. 1 Nr. 1 SGB X innerhalb der Zentralstelle für Strafentlassene durch die Mitarbeiter des Arbeitsamtes kommt daher nur gegenüber den Mitarbeitern des Sozialamts im erforderlichen Umfang in Betracht.

Die Mitarbeiter der Einrichtungen der Freien Wohlfahrtspflege haben als Träger von Berufsgeheimnissen vorrangig das in § 203 StGB strafbewehrte Schweigegebot zu beachten. Eine Offenbarung der ihnen anvertrauten persönlichen Daten an Dritte ist nur mit Zustimmung des Betroffenen zulässig; andere Offenbarungsbefugnisse, die sich aus der Rechtsprechung zu § 203 StGB ergeben haben, sind nicht erkennbar.

In einem Fall enthält die „Einheitsakte" der Zentralstelle für Strafentlassene alle Schriftstücke und Unterlagen über den Betroffenen von allen in der Arbeitsgemeinschaft tätigen Mitarbeitern. Bei der Weitergabe der Einheitsakte zwischen den Mitarbeitern werden persönliche Daten offenbart, die im Einzelfall zur Bearbeitung der im Zuständigkeitsbereich liegenden Aufgaben nicht erforderlich sind. Die Führung und Weitergabe der Einheitsakte setzt auch eine schriftliche Einwilligung des Betroffenen voraus (§ 67 SGB X bzw. 32 BG). Zur Sicherstellung des Verfassungsgrundsatzes der Verhältnismäßigkeit habe ich vorgeschlagen, die Einwilligung des Betroffenen auf die Datenweitergabe innerhalb der Zentralstelle für Strafentlassene zu beschränken. Von dieser Beschränkung müssen aber solche Offenbarungen an Stellen außerhalb der Zentralstelle ausgenommen bleiben, die zur Erfüllung einer gesetzlichen Aufgabe nach dem SGB durch das Sozialamt oder das Arbeitsamt zwingend erforderlich sind. Eine Weitergabe von Informationen, die durch Einsichtnahme in die Einheitsakte zufällig bekannt geworden sind, also von der betreffenden beteiligten Stelle nicht selbst erhoben wurden, wäre danach unzulässig.

### 3.5 Schul- und Hochschulbereich

#### 3.5.1 Novellierung des Gesetzes über das Erziehungs- und Unterrichtswesen

Zur Novellierung des Gesetzes über das Erziehungs- und Unterrichtswesen (EUG) habe ich aus datenschutzrechtlicher Sicht Stellung genommen. Dabei habe ich insbesondere darauf hingewiesen, daß die Gelegenheit der Neufassung des EUG zum Anlaß genommen werden sollte, die nach dem Bayer. Datenschutzgesetz ab 1. Januar 1983 für die Zulässigkeit von Speicherung und Übermittlung personenbezogener Daten notwendigen Rechtsnormen rechtzeitig zu schaffen. So habe ich die vorgesehene Regelung zur „Erhebung und Weitergabe von Daten" ausdrücklich begrüßt.

Zu einer Reihe von vorgesehenen Regelungen habe ich Bedenken vorgetragen und Änderungswünsche angemeldet. Zum Beispiel erschien es mir bedenklich, wenn eine vorgesehene Bestimmung zur Folge haben sollte, daß bei jedem Schüler, der das 14. Lebensjahr vollendet hat, vor Aufnahme an einer Schule eine Anfrage an das Bundeszentralregister gerichtet oder die Vorlage eines Führungszeugnisses verlangt würde. Die jeweils vorgesehene Verständigung des Jugendamtes, wenn dem Erziehungsberechtigten angedroht wird, daß die Lehrerkonferenz mit der Frage der Entlassung des Schülers befaßt werden kann, schien mir auch zu weitgehend zu sein. Meines Erachtens sollte das Jugendamt grundsätzlich nur dann von diesen belastenden Vorgängen unterrichtet werden, wenn die Entlassung des Schülers tatsächlich zu erwarten ist. Die Unterrichtung des Jugendamtes darf meines Erachtens nicht als zusätzliches Disziplinierungsmittel dienen. Zudem muß sich der Umfang der hierbei zu übermittelnden Informationen am Aufgabengebiet des Jugendamtes orientieren.

Aus meinen Erfahrungen zur Schulgesundheitpflege – insoweit verweise ich auf meinen 3. Tätigkeitsbericht – habe ich gefordert, daß eindeutig geregelt wird, wer für die im Rahmen der Schuluntersuchungen angefallenen Daten der Schüler verantwortlich ist. Um hier Mißverständnisse zu vermeiden und Verletzungen des Arztgeheimnisses zu verhindern, halte ich eine diesbezügliche eindeutige Regelung für erforderlich. Darüber hinaus sollte auch geregelt werden, inwieweit die Gesundheitsämter die im Rahmen der Schuluntersuchungen erkannten Erkrankungen und Leistungseinschränkungen der Schule mitteilen, sofern diese Tatsachen bei Gestaltung und Durchführung des Unterrichts von den Lehrern berücksichtigt werden müssen.

Nach meinem bisherigen Erkenntnisstand gehe ich davon aus, daß zumindest einige meiner Anregungen im EUG Berücksichtigung finden werden.

#### 3.5.2 Datenerhebung an Schulen für Zwecke der Bildungsforschung

Das Staatsinstitut für Bildungsforschung und Bildungsplanung führte im Sommer des letzten Jahres im Auftrag des Bayer. Staatsministeriums für Unterricht und Kultus eine Untersuchung zur Beschreibung von Bedingungen und Problemen der Übertrittsbeurteilung durch. Dabei wurden über zwei Fragebogen Daten über Schüler der 4. Jahrgangsstufe und mit einem Lehrerfragebogen Angaben über die jeweiligen Klassenlehrer erbeten.

Mit den beiden erstgenannten Fragebogen, die als „Klassenliste 1" und „Klassenliste 2" bezeichnet waren, wurden die schulischen Leistungen aller Schüler einer Klasse erfragt. Außerdem wurden noch sogenannte demographische Daten verlangt, wie Beruf des Vaters/der Mutter, Ausländerkind, Anzahl der

Geschwister, Geburtsmonat, Geburtsjahr, Geschlecht und „elterliche Unterstützung der Lernarbeit".

Die Fragebogen „Klassenliste 1" und „Klassenliste 2" sahen eine Spalte „Schülername" vor, die gleichzeitig mit einer Nummer versehen ist, die sich dann in einer weiteren Spalte wiederholt.

Es war vorgesehen, daß nach Eintragung der Daten in diese beiden Fragebogen die Rubrik „Schülername" von der Lehrkraft abgetrennt wird. Daraus habe ich geschlossen, daß für die Erhebung durch das Staatsinstitut für Bildungsforschung und Bildungsplanung lediglich anonymisierte Daten erforderlich waren. Dies bedeutete in Anwendung des in Art. 17 Abs. 1 BayDSG niedergelegten Grundsatzes, daß im Rahmen der diesbezüglichen Aufgabenerfüllung dem Staatsinstitut für Bildungsforschung und Bildungsplanung auch lediglich anonymisierte Daten übermittelt werden dürften. Nach der Gestaltung der Fragebogen „Klassenliste 1" und „Klassenliste 2" war diese Anonymisierung jedoch nicht vollständig sichergestellt. Wurden die Schülernamen nämlich entsprechend der Klassenliste eingetragen – so wurde in der Praxis wohl verfahren –, war auch nach Abtrennung der Schülernamen die Reidentifizierung der Schüler über die jeweilige Schule jederzeit möglich, weil auf diesen Fragebogen zusätzlich noch die Angabe der Schule und der Klasse verlangt war.

Leider habe ich von dieser Befragungsaktion zu spät Kenntnis erlangt, als daß ich noch rechtzeitig Hinweise für diese Aktion hätte geben können. Ich habe daher gebeten, wenigstens sicherzustellen, daß durch entsprechende Auflagen beim Staatsinstitut für Bildungsforschung und Bildungsplanung gewährleistet ist, daß dort eine Reidentifizierung unmöglich wird.

Sofern derartige Umfragen in gleicher oder ähnlicher Weise wiederholt werden sollten, müßte von vorneherein sichergestellt werden, daß eine Reidentifizierung verhindert wird. Dazu wären die Lehrkräfte darauf hinzuweisen, daß sie die Schülernamen nicht entsprechend der Schülerliste, sondern möglichst in einer gewillkürten Reihenfolge auf den Fragebogen eintragen sollten. Darüber hinaus müßte wohl auch auf die exakte Bezeichnung der befragten Klasse verzichtet werden, weil andernfalls zumindest in Einzelfällen über die Angaben zum Beruf des Vaters oder das Geburtsdatum und ähnliche Angaben eine Beziehung zu einem konkreten Schüler hergestellt werden könnte.

Da Forschung dann weitgehend unproblematisch ist, wenn sie mit anonymisierten Daten arbeitet, sollte der Weg der Anonymisierung wenn irgend möglich beschritten werden. Gleichzeitig gilt es jedoch in diesen Fällen sicherzustellen, daß durch ausreichende Anonymisierung eine Identifizierung der Betroffenen unmöglich wird.

### 3.5.3 Datenerhebung an Schulen

Wie mir aufgrund einer Beschwerde bekannt wurde, erbat ein Klassenlehrer an einer Münchner Volksschule mit einem selbstgefertigten „Erfassungsblatt" von den Eltern seiner Schüler neben Angaben zum Schüler (z. B. Geburtsdatum, Geburtsort, Bekenntnis) auch Name, Anschrift und Beruf der Erziehungsberechtigten. Der nach Art. 16 Abs. 2 BayDSG erforderliche Hinweis auf eine eventuelle Rechtsgrundlage oder die Freiwilligkeit der Beantwortung des Fragebogens fehlte. Die erbetenen Angaben hätten im wesentlichen aus den bereits vorhandenen Einschulungsunterlagen zur Ausfüllung des Schülerbogens entnommen werden können.

Über diese Datenerhebung wollte der Klassenlehrer wohl eine eigene Kartei über die Schüler seiner Klasse und deren Eltern anlegen. Wenn auch die erhobenen Daten nicht sehr sensibel waren, sind gegen derartige nicht offizielle Datenerhebungen durch öffentlich Bedienstete datenschutzrechtliche Bedenken geltend zu machen: Datenerhebungen sollen grundsätzlich auf das unbedingt erforderliche Maß begrenzt werden. Parallele Erhebungen neben den für die öffentliche Aufgabenerfüllung unbedingt erforderlichen können die betroffenen Bürger verunsichern. Außerdem ist die mögliche Verwendung solcher privater Karteien der Lehrer – eventuell über das einzelne Schuljahr hinaus – im Regelfall mangels Kenntnis von der Existenz solcher Karteien nicht zu überprüfen. Meines Erachtens sollten daher eigene Datenerhebungen und das Anlegen zusätzlicher Karteien durch die Lehrer nicht nur im Hinblick auf Art. 16 BayDSG, sondern auch zur Vermeidung von entsprechenden Befürchtungen der betroffenen Eltern weitgehend eingeschränkt werden.

Das Staatsministerium für Unterricht und Kultus hat in dieser Angelegenheit mitgeteilt, daß im konkreten Fall und allgemein in Dienstbesprechungen auf die Prüfung der Erforderlichkeit der Datenerhebungen im Schulbereich hingewiesen werde.

### 3.5.4 Übermittlung von Anschriften ehemaliger Mitschüler für ein Klassentreffen

Immer wieder erreichen mich Anfragen, ob die Schule einem ehemaligen Schüler die Namen seiner früheren Klassenkameraden mitteilen kann. Grund der Anfrage ist meistens die Einladung zu einem Klassentreffen.

Mit dem Bayer. Staatsministerium für Unterricht und Kultus bin ich der Auffassung, daß die Übermittlung der Namen seiner Klassenkameraden an einen ehemaligen Mitschüler durch die Schule oder das Staatliche Schulamt für den Zweck, ein Klassentreffen zu organisieren, grundsätzlich unbedenklich ist. Zwar bestimmt § 97a Abs. 2 der Allgemeinen Schulordnung (ASchO), der in seinem Wortlaut wohl im wesentlichen in das neugefaßte Gesetz über das Erziehungs- und Unterrichtswesen übernommen wird, daß die Weitergabe von Daten über Schüler an außerschulische Stellen untersagt ist, sofern nicht ein rechtlicher Anspruch auf die Herausgabe der Daten nachgewiesen wird. Allerdings dürfen nach § 97a Abs. 3 ASchO in den von den Schulen herausgegebenen Jahresberichten bestimmte personenbezogene Daten enthalten sein. Diese Daten in den Jahresberichten dienen unter anderem auch dem Zweck, Klassengemeinschaften über die Schulzeit hinaus

aufrechtzuerhalten. Daher kann § 97a Abs. 3 ASchO für die Mitteilung der Namen ehemaliger Schüler an einen früheren Mitschüler entsprechend angewandt werden.

3.5.5 Verwendung von Gesundheitskarten bzw. Gesundheitsbogen an den Schulen

Wie ich in meinem letzten Tätigkeitsbericht (S. 20) ausgeführt habe, hatte ich beanstandet, daß in einzelnen Gymnasien die im Rahmen der schulärztlichen Betreuung der Schüler angefallenen Gesundheitsunterlagen im allgemeinen Schülerakt geführt und nicht – wie vorgeschrieben – vom Schularzt aufbewahrt wurden.

Das Bayer. Staatsministerium für Unterricht und Kultus hat sich bemüht, bei den von mir überprüften Gymnasien eine datenschutzgerechte Lösung für die Aufbewahrung der Schülergesundheitskarten zu finden. Zudem wurden die Ministerialbeauftragten für die Gymnasien in Bayern auf die insoweit bestehende Rechtslage hingewiesen.

Diese Maßnahmen reichen jedoch meines Erachtens nicht voll aus. Wie mir nämlich mitgeteilt wurde, sollen im gesamten Schulbereich zweier größerer bayerischer Städte die Gesundheitskarten nach wie vor offen im Schülerakt geführt werden. Ich habe daher Anlaß zu befürchten, daß dieses Problem landesweit noch nicht erkannt ist und die entsprechenden Vorschriften des Bayer. Staatsministeriums für Unterricht und Kultus an einigen Schulen nach wie vor nicht vollzogen werden.

3.5.6 Verwendung des Wortes „Sonderschule" auf amtlichen Dokumenten

Im 3. Tätigkeitsbericht habe ich darauf hingewiesen, daß an Sonderschulen Schülerausweise ausgegeben werden, die den Inhaber als Schüler einer Sonderschule ausweisen. Meinen diesbezüglichen Bedenken hat das Bayer. Staatsministerium für Unterricht und Kultus leider nicht Rechnung getragen. Ich habe im Berichtszeitraum das Staatsministerium nochmals gebeten, seine Haltung zu überprüfen.

Ich bin nach wie vor der Ansicht, daß der Schülerausweis hauptsächlich im außerschulischen Bereich benutzt wird und neben der Feststellung der Schulzugehörigkeit einer Person insbesondere zur Erlangung von Vergünstigungen verschiedenster Art (z.B. verbilligter Eintrittskartenbezug, Fahrpreisermäßigung bei öffentlichen Verkehrsmitteln) dient. Diese Vergünstigungen werden dem Schüler aber ohne Rücksicht auf die Zugehörigkeit zu einem besonderen Schultyp gewährt. Die mit der Vorlage des Ausweises jeweils verbundene Bekanntgabe der Tatsache, daß der Schüler eine Sonderschule besucht, ist somit für den Schüler unnötig belastend. Vergünstigungen hingegen, auf die der Schüler unmittelbar aufgrund seiner Behinderung Anspruch hat (z.B. Sitzgelegenheiten in öffentlichen Verkehrsmitteln als Schwerbehinderter), werden dem Betroffenen im Regelfall aufgrund eines dafür vorgesehenen Schwerbeschädigtenausweises zuerkannt. Probleme eher organisatorischer Art, die gegen den Wegfall der Bezeichnung „Sonderschule" ins Feld geführt werden, müssen sich lösen lassen. So dürfte die Zugehörigkeit eines Schülers zu einer bestimmten Schule schulintern wohl nicht über die Vorlage des Schulausweises festgestellt werden. Schließlich bin ich auch der Ansicht, daß die Vergabe eines neutralen Schülerausweises nicht zur Umbenennung einer Schule oder zu Schwierigkeiten im amtlichen Schriftverkehr führen muß.

Gegen die Verwendung der Bezeichnung „Sonderschule" in Zeugnissen habe ich in Anbetracht der vom Bayer. Staatsministerium für Unterricht und Kultus gefundenen Lösung meine Bedenken zurückgestellt. Ein Zeugnis muß meines Erachtens zur richtigen Einordnung der auf ihm vermerkten Leistungen die Schule ausweisen, an der der Schüler die Leistungen erbracht hat. In diesem Zusammenhang habe ich es begrüßt, daß den Sonderschülern die Möglichkeit eröffnet ist, gegen Ende eines freiwillig besuchten 10. Schuljahres den einfachen Hauptschulabschluß zu erwerben. Weil in diesen Fällen die Schule das Zeugnis ausstellt, an der der Hauptschulabschluß erworben worden ist, wird somit eine Gleichstellung mit den übrigen Hauptschülern erreicht.

3.5.7 Aufbewahrung von personenbezogenen Unterlagen an Schulen

Zusammen mit dem Staatsministerium für Unterricht und Kultus habe ich Anforderungen an die sichere Unterbringung von personenbezogenen Unterlagen an den Schulen erarbeitet. Nach Art. 15 Abs. 1 BayDSG sind auch für die in herkömmlicher Weise in Karteien geführten Daten die technischen und organisatorischen Maßnahmen zu treffen, die erforderlich sind, um die Einhaltung des Bayer. Datenschutzgesetzes zu gewährleisten. Im Schulbereich fallen hierunter insbesondere die Schülerkarteien, die Schülergesundheitskarten – soweit der Schularzt diese nicht verwahrt –, Unterlagen mit personenbezogenen Daten über die Schüler einer Klasse, beispielsweise Notenbögen, Schülerbögen, und die Lehrerkarteien. Solche Daten dürfen nur den Personen zugänglich sein, die sie zu ihrer Aufgabenerfüllung benötigen (Art. 17 Abs. 1, Abs. 3 BayDSG); das sind grundsätzlich nur der Schulleiter, dessen Stellvertreter oder die mit der Sachbearbeitung besonders betrauten Personen. Auf die Schülergesundheitskarten darf selbstverständlich nur der Schularzt zugreifen. Um den Zugang Unbefugter auszuschließen, sind diese Karteien in verschließbaren und möglichst mit einem Sicherheitsschloß gesicherten Schränken zu verwahren.

Die sonstigen Personalunterlagen über Lehrer, Schüler, Verwaltungs- und Hauspersonal sind auf gleiche Weise zu sichern, auch wenn für derartige nicht in Karteien geführte Unterlagen das Bayer. Datenschutzgesetz nicht unmittelbar Anwendung findet.

Das Bayer. Staatsministerium für Unterricht und Kultus hat zwischenzeitlich den Regierungen, den Ministerialbeauftragten für Gymnasien, Fachoberschulen und Realschulen sowie allen staatlichen Schulen mit mir abgesprochene schriftliche Hinweise zugesandt, die praxisbezogene Anleitungen für eine vernünftige Datensicherung geben. Diese Hinweise sind im folgenden auszugsweise abgedruckt:

„1. Dies – Beachtung des Art. 15 Abs. 1 BayDSG (eingefügt von mir) – gilt auch für personenbezogene Daten, die nicht in automatisierten Dateien gespeichert werden.
Hierunter fallen insbesondere
- Schülerkarteien
- Schülergesundheitskarten, soweit der Schularzt diese nicht verwahrt
- Unterlagen mit personenbezogenen Daten über die Schüler einer Klasse (z. B. Schülerbögen, Notenbögen, soweit sie während des Schuljahres nicht in den einzelnen Schülerakten abgelegt, sondern klassenweise zusammengefaßt sind; vgl. dazu auch Abschnitt II Nr. 3 der Erläuternden Hinweise für die Schulen zum Vollzug des BayDSG vom 9. April 1979, KMBl I S. 187)
- Lehrerkarteien.

Solche Datensammlungen dürfen nur für die unmittelbar Zugangsberechtigten (Schulleiter, Schulleiterstellvertreter, Klassenleiter, mit der Sachbearbeitung beauftragte Verwaltungsangestellte; bei Schülergesundheitskarten nur der Schularzt und ggf. die mit der aktenmäßigen Vorbereitung der Untersuchungen beauftragte Schulsekretärin, die insoweit zum Hilfspersonal des Schularztes gehört), nicht aber für – unbefugte – Dritte zugänglich sein. Die Dateien sind daher sorgfältig zu verwahren, z. B. in einem Archivraum oder in einem verschließbaren Behältnis, das gegen unbefugte Öffnungsversuche gesichert ist (Wandschrank bzw. Blechschrank mit Sicherheitsschloß u. ä.). Sofern nur ein einfaches Schloß vorhanden ist, wird gebeten, nach Herstellung des Einvernehmens mit dem Sachaufwandsträger zusätzlich ein Sicherheitssteckschloß anzubringen, das mit geringem Kostenaufwand in einschlägigen Fachgeschäften erworben werden kann.

Die zur Aufbewahrung von Dateien bestimmten Behältnisse sind stets verschlossen zu halten. Die Schlüssel dürfen nur den Zugangsberechtigten zur Verfügung stehen. Die Räume, in denen sich die Schränke befinden, sind bei Verlassen sorgfältig abzusperren und – soweit vorhanden – durch zusätzliche Vorkehrungen zu sichern (z. B. Schließen vorhandener Fensterläden beim Verlassen der Räume nach Dienstschluß).

2. Die vorstehend genannten Sicherheitsvorkehrungen sind auch bei sonstigen Personalunterlagen über Lehrer, Schüler, Verwaltungs- und Hauspersonal usw., die nicht unter das Bayer. Datenschutzgesetz fallen (z. B. Schüler- oder Lehrerakten), zu beachten. Oft sind bereits einfache Maßnahmen, die keinen zusätzlichen Kostenaufwand erfordern, der Sicherheit dienlich (z. B. Unterlassen von Hinweisen auf dem Türschild, daß ein Raum das (Personal-)Archiv der Schule enthält).“

3.5.8 Weitergabe von Namenslisten an die Wehrerfassungsbehörden

Die Wehrbereichsverwaltung VI in Bayern hat wiederholt die Herausgabe von Schülerlisten mit Geburtsdatum von Endkläßlern gewünscht. Als Begründung hat sie angegeben, daß die Wehrerfassungsbehörden die einzelnen Schüler rechtzeitig über die Möglichkeiten einer vorgezogenen Musterung und einer vorzeitigen Ableistung des Grundwehrdienstes unterrichten wollten. Bei der Prüfung der Zulässigkeit einer solchen Übermittlung von Schülerlisten an die Wehrerfassungsbehörden kann zwar davon ausgegangen werden, daß es Aufgabe der Kreiswehrersatzämter ist, die Schüler über die Möglichkeit der vorzeitigen Musterung und Einberufung zu unterrichten. Jedoch ist meines Erachtens zur Erfüllung dieser Aufgabe der Kreiswehrersatzämter die Kenntnis der Daten dieser Schüler nicht erforderlich. Wie die Sachbehandlung in einer Reihe anderer Länder zeigt, ist es hierzu ausreichend, den betroffenen Schülern entsprechende Formblätter – gegebenenfalls über die Schule – auszuhändigen.

Sofern vermieden werden soll, daß über einen längeren Zeitraum hinweg immer wieder einzelne Schüler wegen ihrer Musterung dem Unterricht fernbleiben und statt dessen die Musterung aller dafür anstehenden männlichen Schüler zu einem einzigen Termin vorgenommen werden soll, können in diesem Falle mit Einverständnis der Schüler die notwendigen Daten zur Vereinbarung eines Termins den Kreiswehrersatzämtern mitgeteilt werden. Auf diese Weise ist eine unbürokratische Lösung der Probleme unter der Beachtung der Schülerinteressen möglich.

Das Bayer. Staatsministerium für Unterricht und Kultus hat die Ministerialbeauftragten für die Gymnasien und für die Fachoberschulen entsprechend angewiesen.

3.5.9 Fragen an Studentenwohnheimbewerber

Ein bayerisches Studentenwerk verlangte von den Studenten, die sich um Aufnahme in ein Studentenwohnheim bewarben, in einem Formblatt die Beantwortung der Frage nach der aktiven/passiven Mitgliedschaft in Organisationen und der darin ausgeübten Funktion. Um die Beantwortung der Frage zu erleichtern, war der Hinweis angebracht, daß hierbei Organisationen schulischer, sozialer, politischer, kultureller o. a. Art gemeint seien. Der Student, der sich an mich gewandt hat, hat zu Recht vorgetragen, daß es ihm unerfindlich sei, in welchem Zusammenhang sein kulturelles und politisches Engagement mit einer Aufnahme in ein Studentenwohnheim stehe. Die Frage ist meines Erachtens um so unverständlicher, weil nach den Richtlinien des Bundes und der Länder für die Studentenwohnheimförderung die Aufnahme eines Studierenden in ein Studentenwohnheim nicht wegen seiner Rasse, seiner Weltanschauung oder seiner politischen Überzeugung abgelehnt oder davon abhängig gemacht werden kann.

In den neuen Bewerbungsformularen des betroffenen Studentenwerkes wird die beanstandete Frage nicht mehr gestellt. Obwohl mir zugesagt worden war, daß das alte Formblatt nicht mehr verwendet werde, bedurfte es einer weiteren Mahnung zur Erreichung dieses Ziels.

Ich habe das betroffene Studentenwerk im übrigen noch gebeten, die insoweit datenschutzrechtlich

unzulässig erhobenen Daten nach Art. 20 Abs. 4 BayDSG zu löschen bzw. zumindest nach Art. 20 Abs. 1 BayDSG zu sperren. Die Sperrung dieser Daten wurde inzwischen veranlaßt.

3.6 Forschung

3.6.1 Wissenschaftsfreiheit vor Datenschutz?

Datenschutz und Forschung können in einem Spannungsverhältnis zueinander stehen. Vertreter von Wissenschaft und Forschung haben mehrfach die Befürchtung geäußert, daß ein zu weitgehender Datenschutz den notwendigen Zugang zu für die Forschung dringend erforderlichen Daten abschneiden könnte. Ich verstehe diese Sorgen grundsätzlich. Allerdings wird auf seiten der Forschung teilweise übersehen, daß die nun unter dem Stichwort „Datenschutz" erörterten Forderungen nach Beachtung der schutzwürdigen Belange Betroffener teilweise nicht neu sind. So handelte es sich beispielsweise bei den in jüngster Zeit erörterten Fragen zur Forschung im psychiatrischen Bereich vielfach um Probleme der ärztlichen Schweigepflicht, die grundsätzlich nicht neu sind.

Ich sehe meine Aufgabe auch darin, um Verständnis dafür zu werben, daß die Landesbeauftragten für den Datenschutz von Gesetzes wegen gefordert sind, die Belange des Datenschutzes nachhaltig zu vertreten. Wenn auch nicht auszuschließen ist, daß dadurch im Einzelfall eine gewisse Behinderung der Forschung nicht immer vermieden werden kann, meine ich jedoch, daß bei ruhiger Erörterung dieser die Forschung und den Datenschutz gemeinsam berührenden Fragen praxisgerechte Lösungen gefunden werden können. Dabei gilt es zu berücksichtigen, daß das Recht auf Achtung der Privatsphäre und der freien Entfaltung der Persönlichkeit einerseits und die Wissenschaftsfreiheit auf der anderen Seite gegensätzliche Grundrechtspositionen darstellen können. Zwischen diesen muß ein Ausgleich gefunden werden. Daß die Wissenschaftsfreiheit nach Art. 5 Abs. 3 Satz 1 Grundgesetz nicht durch Gesetz beschränkt werden kann, steht der Notwendigkeit einen Ausgleich zu finden nicht entgegen. Auch die Wissenschaftsfreiheit ist nicht gänzlich schrankenlos gewährt. In einem Spannungsverhältnis mit anderen Grund- und Verfassungsrechten kommt der Wissenschaftsfreiheit gegenüber solchen mit ihr kollidierenden gleichfalls verfassungsrechtlich geschützten Prinzipien nicht schlechthin Vorrang zu (BVerfGE 57, 70/99).

Ich bin gerne bereit, meinen Teil dazu beizutragen, einen vernünftigen Ausgleich zu finden.

3.6.2 Vorentwürfe für Krebsregistergesetze

Der Bundesminister für Jugend, Familie und Gesundheit hatte einen „Diskussionsentwurf, Muster eines Gesetzes über ein Krebsregister" durch eine Arbeitsgruppe ausarbeiten lassen. Die Landesbeauftragten und der Bundesbeauftragte für den Datenschutz haben sich mit dem Entwurf (Stand 28. August 1981) in einer Konferenz am 14. Dezember 1981 befaßt und folgende Stellungnahme verabschiedet:

„1. Die Datenschutzbeauftragten erkennen die gesundheitspolitische Bedeutung der medizinischen Forschung, insbesondere im Zusammenhang mit der Bekämpfung von Krebserkrankungen an. Es entspricht ihrer gesetzlichen Aufgabe, auch in diesem Bereich für die Wahrung der schutzwürdigen Belange der Patienten einzutreten. Ihre Bedenken und Vorschläge zielen daher ausschließlich darauf ab, die Freiheit der Forschung in ein ausgewogenes und rechtlich abgesichertes Verhältnis zu den grundrechtlich geschützten Belangen der Betroffenen zu bringen. Sie gehen davon aus, daß es möglich ist, Regelungen zu finden, die den Erfordernissen der Forschung wie auch des Schutzes der Individualsphäre gerecht werden. Die gelegentlich geäußerte pauschale Behauptung, der Datenschutz behindere die Krebsforschung, weisen sie als unbegründet zurück.

2. Es ist nicht Aufgabe der Datenschutzbeauftragten, Sinn und Nutzen von Krebsregistern zu beurteilen. Sie warnen aber nachdrücklich vor der Gefahr, daß die Gesetzgebung zum Krebsregister ein erster Schritt zur Errichtung einer Vielzahl anderer Epidemiologieregister werden könnte. In diesem Zusammenhang weisen sie darauf hin, daß auch aus Kreisen der Ärzteschaft erhebliche Zweifel am Nutzen medizinischer Register geäußert werden, woraus sich Zweifel an der Erforderlichkeit derartiger Register ableiten lassen. Sie appellieren an die medizinische Forschung, stärker als bisher den bereits vorhandenen Forschungsstand zur Anonymisierung personenbezogener Daten zu nutzen und sich vordringlich um die Weiterentwicklung von Anonymisierungs- und Aggregationsmethoden zu bemühen. Diese methodologischen Überlegungen können wesentlich dazu beitragen, Probleme, die sich durch die ärztliche Schweigepflicht und den Datenschutz ergeben, gar nicht erst aufkommen zu lassen.

3. Für den Fall der politischen Entscheidung in den Ländern zugunsten der Schaffung von Krebsregistern halten es die Datenschutzbeauftragten für notwendig, daß die Errichtung, Ausgestaltung und Nutzung von Krebsregistern in einem speziellen Gesetz geregelt werden. Der mit der Einrichtung eines Krebsregisters verbundene Eingriff in Grundrechtspositionen der Betroffenen ist nur durch ein Gesetz zu legitimieren, das die nachfolgenden Grundsätze beachtet (vergleiche unten 4). Dabei wird davon ausgegangen, daß es sich um ein Register zur Erfassung der Anzahl der Neuerkrankungen (Inzidenzregister) bzw. der Anzahl der erkrankten Personen (Privalenzregister) handeln wird.

Eine im Anwendungsbereich unbestimmte allgemeine Rahmenregelung für die medizinische Forschung in einem Landesdatenschutzgesetz, die derzeit im Vordergrund baden-württembergischer Überlegungen steht, lehnen die Datenschutzbeauftragten daher – auch aus verfassungsrechtlichen Bedenken – ab.

4. Nach Auffassung der Datenschutzbeauftragten muß ein Krebsregistergesetz zumindest die folgenden Prinzipien berücksichtigen:

4.1 Die Meldung von Patientendaten mit Personenbezug an das Krebsregister bedarf grundsätzlich der Einwilligung des Betroffenen (bzw. der Entbindung von der ärztlichen Schweigepflicht). Nur in wenigen Ausnahmefällen kann die Meldung auch ohne Einwilligung des Patienten erfolgen, und zwar wenn sie für die Zwecke des Krebsregisters nachweisbar notwendig ist und dem Patienten dadurch, daß ihm die Art seiner Krankheit bekannt wird, gesundheitliche Nachteile entstehen können. Soweit weder ein solcher Ausnahmefall noch eine Einwilligung vorliegt, unterbleiben Meldungen an das Register. Der zulässige Umfang der Einwilligung ist im Gesetz festzulegen.

4.2 Für die weitere Übermittlung durch das Krebsregister an andere Forschungseinrichtungen ist grundsätzlich eine besondere Einwilligung erforderlich, wenn die Daten nicht in aggregierter oder anonymisierter Form weitergegeben werden. Für diese Übermittlung ist entsprechend der Regelung über die Forschung mit Sozialdaten ein Genehmigungsverfahren vorzusehen. Eine nochmalige Übermittlung durch die Forschungseinrichtung an Dritte ist unzulässig.

4.3 Der Gesetzeszweck, die Aufgaben des Krebsregisters, seine Rechtsform und die institutionelle Ausgestaltung sind im Gesetz festzulegen. Im Interesse einer wirksamen Aufsicht sollte das Krebsregister in öffentlich-rechtlicher Trägerschaft geführt werden.

4.4 Der Kreis derjenigen Institutionen, die zu Forschungszwecken personenbezogene Daten des Krebsregisters erhalten können, sollte in der Weise beschränkt werden, daß die ausschließliche Verwendung zu Forschungszwecken gewährleistet ist.

Dies bedingt eine externe Kontrolle des Datenschutzes von Amts wegen.

4.5 Der in den Statistikgesetzen verankerte Grundsatz der Zweckbindung muß auch für die im Krebsregister gespeicherten Daten gelten.

Im übrigen sollte geprüft werden, ob ein gesetzliches Verbot eingeführt werden sollte, vom Betroffenen eine Bescheinigung über den Inhalt der im Krebsregister gespeicherten Daten zu verlangen. Ein solches Verbot könnte verhindern, daß potentielle Arbeitgeber oder sonstige Vertragspartner vom Betroffenen die Vorlage einer Art Negativattest des Krebsregisters fordern.

4.6 Eine Verknüpfung mit anderen Datenbanken ist unzulässig.

4.7 Die Aufbewahrung personenbezogener Daten beim Krebsregister ist zu befristen. Patientendaten sind außerdem zu löschen, wenn sie nicht mehr benötigt werden.

4.8 Jeder Betroffene hat Anspruch auf Auskunft über die zu seiner Person gespeicherten Daten aus dem Krebsregister. Dies gilt auch für Patienten, die über die Meldung nicht informiert worden sind. Entsprechend der Regelung für Sozialdaten in § 25 SGB X kann bei Gefahr für die Gesundheit des Patienten die Auskunft – vermittelt durch einen Arzt – erteilt werden."

Ich halte es für erforderlich, daß sich Planungen zur Einrichtung eines oder mehrerer zentraler Krebsregister, in denen die Betroffenen – wie bisher vorgesehen – mit vollem Namen und Anschrift geführt werden sollen, mit den vorstehenden Überlegungen der Datenschutzbeauftragten auseinandersetzen.

Ein wesentlicher Ausgangspunkt dieser Überlegungen war, daß der Diskussionsentwurf zum „Muster eines Gesetzes über ein Krebsregister" den Ärzten die Meldung an das Krebsregister völlig freistellen will und zur Hebung ihrer Motivation eine Vergütung für jede Meldung vorsieht, während dem Betroffenen selbst nicht freigestellt werden soll, ob er mit Namen und Anschrift im Register gespeichert wird, da seine Einwilligung nicht grundsätzlich zur Voraussetzung der Meldung gemacht werden soll.

Die Tatsache, daß es den Ärzten freigestellt sein soll, Patienten zu melden, bewirkt, daß der Entwurf nicht von einer lückenlosen Meldung aller Krebserkrankungsfälle ausgeht. Es muß daher zunächst gründlich geprüft werden, inwieweit die Einholung der Einwilligung der Patienten überhaupt noch eine relevante zusätzliche Beeinträchtigung des Registers verursacht, bevor den Betroffenen ein so erheblicher Eingriff in ihre Privatsphäre, wie eine zentrale personenbezogene Registrierung ihres Krankheitsfalles ohne Einwilligung zugemutet werden kann. Zu dieser Frage sind, soweit ersichtlich bisher lediglich dezidierte Meinungen veröffentlicht worden. Eine fundierte Studie über den Einfluß einer vorherigen Einholung der Einwilligung, d.h. also über die mögliche Quote der versagten Einwilligungen, ist nicht bekannt. Angesichts der Schwere des vorgesehenen Grundrechtseingriffs hielte ich eine fundierte Erforschung dieser Frage für notwendig – insbesondere, da mir aus der Prüfung von Krebsregistern in Kliniken, die teilweise auf Grund der Behandlung von Patienten in der Klinik entstanden sind, die jedoch auch Patienten aus anderen Kliniken enthalten, bekannt ist, daß in der überwiegenden Mehrzahl der Fälle die Einwilligung zu solchen Speicherungen erteilt wird.

Hinzuweisen ist auch darauf, daß das Register lediglich als Nachweisregister geplant ist. D.h. die eigentliche Forschungstätigkeit soll auf Grund von Daten durchgeführt werden, die von den Patienten, deren Adressen aus dem Register zu erfahren wären, nachträglich erst für den jeweiligen Forschungszweck erhoben würden. Voraussetzung für eine solche Patientenbefragung soll auch nach dem Konzept des Musterentwurfs die vorherige schriftliche Einwilligung des Patienten sein. Eine Darstellung derjenigen Forschungsergebnisse, die allein mit den wenigen in dem Nachweisregister zu speichernden Daten möglich wäre, fehlt bisher.

Die von den Datenschutzbeauftragten geäußerten Bedenken sind auch von anderen Stellen vorgetragen worden, sie werden dadurch bestätigt.

Der Bayerische Staatsminister des Innern bezeichnete gegenüber dem Bundesminister für Jugend, Familie und Gesundheit einen inzwischen vorgelegten weiterentwickelten Musterentwurf für ein Krebsregistergesetz als unausgewogen und betonte, der Entwurf orientiere sich vorrangig am epidemiologischen Forschungsinteresse, ohne dabei auch dem Interesse des einzelnen Krebskranken ausreichend Rechnung zu tragen. Der Entwurf begegne in dieser Form schwerwiegenden verfassungsrechtlichen Bedenken. Der Bayerische Staatsminister des Innern vermißte insbesondere ein Eingehen, geschweige denn eine Auseinandersetzung mit den erheblichen Einwendungen der Datenschutzbeauftragten. So wichtige Probleme wie die Frage von Zeugnisverweigerungsrechten der registerführenden Stellen oder die Frage eines Verbots, Negativatteste zu verlangen, seien unberücksichtigt geblieben. Zu denken sei schließlich auch noch an die Bezugsproblematik im Blick auf andere, mehr oder weniger umfassende Register, und zwar nicht nur im Bereich der Medizin. Voraussetzung für die Formulierung eines Gesetzentwurfs sei die wissenschaftlich exakte Definition der Ziele einer möglichst umfassenden Krebsregistrierung. Die Notwendigkeit, ob und welche Persönlichkeitsdaten zu erheben seien, ließe sich nur dann begründen, wenn die damit zu erreichenden Ziele klar und eindeutig definiert seien. Dies sei auch ein Gebot der Verfassung, die für jeden staatlichen Eingriff in grundrechtsgeschützte Positionen dessen „Eignung" zur Erreichung des gemeinschaftswichtigen Zieles zwingend erfordere. Es sei in diesem Zusammenhang auch nicht dargetan, daß nur der Verzicht auf die Einwilligung des Patienten zu einem brauchbaren Krebsregister führe. Die vorliegende Konzeption, die dem Arzt ein Melderecht ohne Einwilligung des Krebskranken nach freiem Ermessen einräume, liefe darauf hinaus, daß er über den Krebskranken verfüge und dieser somit zum Objekt des Handelns Dritter mit staatlicher Billigung gemacht würde. Dies sei auch im Hinblick auf Art. 1 Abs. 1 GG fragwürdig. Die Wissenschaftsfreiheit könne einen so weitgehenden Eingriff in die persönliche Entscheidungsautonomie und damit in den Eigenwert des einzelnen Menschen nicht rechtfertigen. Die obersten Landesgesundheitsbehörden in Bayern seien der Auffassung, daß ein Gesetzentwurf weiterer Beratungen bedürfe. Sie neigen dabei allerdings bereits jetzt der Auffassung zu, daß nach Abwägung aller Gesichtspunkte an der generellen Einwilligungsbedürftigkeit kein Weg vorbeiführe.

Der Hartmannbund hatte mir den Beschluß seiner Hauptversammlung 1981 übersandt in dem gefordert wird, die ärztliche Schweigepflicht auch bei Forschungsvorhaben zu beachten. Der Beschluß betont, daß auch das steigende Interesse an der Krankheitsursachenforschung das Verfügungsrecht des Patienten über seine persönlichen Daten nicht außer Kraft setzen könne. Patientendaten dürften nur mit Einwilligung des Patienten für Forschungszwecke weitergegeben werden, dies dürfe nicht durch spezialgesetzliche Regelungen eingeengt werden. Der Hartmannbund befürchtet, daß dem Krebsregister weitere personenbezogene Krankheitsregister folgen würden, da es außer Krebs noch eine Vielzahl ähnlich schwer beherrschbarer Krankheiten gebe.

In letzter Zeit wandten sich auch die Bayer. Landesärztekammer und die Kassenärztliche Vereinigung Bayerns gegen die Einführung eines Krebsregisters, wie es im März 1982 auf dem deutschen Krebskongreß in München gefordert worden war. Wesentlicher Kritikpunkt ist offenbar die fehlende Einwilligung des Patienten zur Speicherung im Register. Sie weisen darauf hin, daß ein solches Krebsregister die Forderung nach personenbezogenen Registern über andere Krankheiten nach sich ziehe (SZ. v. 30. März 1982).

Ich möchte betonen, daß ich jederzeit zu einer intensiven und konstruktiven Beratung bereit bin, um diese wichtige Forschung zu fördern. Der vorstehend wiedergegebene Beschluß der Landesbeauftragten und des Bundesbeauftragten für den Datenschutz hat diese Bereitschaft zur Grundlage. Mein Ziel wird dabei sein, darauf hinzuwirken, daß auf die Belange der betroffenen Patienten hinreichend Rücksicht genommen wird und daß bei den unvermeidbaren Grundrechtseinschränkungen der Grundsatz der Verhältnismäßigkeit berücksichtigt und außerdem zwischen Einschränkung des Persönlichkeitsrechts und nachweisbar erzielbarem Effekt abgewogen wird.

### 3.6.3 Gesundheitsbefragung durch ein Universitätsinstitut

Ein Institut einer bayerischen Universität beabsichtigte, bei der Bevölkerung mehrerer bayerischer Gemeinden eine ausführliche Gesundheitsbefragung, die sich über mehrere Jahre erstrecken sollte, durchzuführen. Neben die freiwillige Befragung der Betroffenen sollte eine ergänzende Durchsicht von Krankenunterlagen der für die Betroffenen zuständigen Sozialversicherungen treten.

Das Institut hatte von vorneherein vorgesehen, hierfür die Einwilligung der Betroffenen einzuholen. In Zusammenarbeit mit dem Landesbeauftragten für den Datenschutz wurde eine Einwilligungserklärung formuliert. In das Projekt sind mehrere tausend Betroffene einbezogen. Probleme oder auch nur Anfragen bei meiner Geschäftsstelle haben sich nicht ergeben. Ich führe dies vor allem auf die aufgeschlossene Haltung des Universitätsinstituts zurück, das im Rahmen des Projektes von Anfang an auch zeitlich eingeplant hatte, die Privatsphäre der Betroffenen und ihre freie Entscheidung darüber zu respektieren und einen gewissen Aufwand für die Aufklärung über die Freiwilligkeit der Angaben und die Einholung der Einwilligungen auf sich zu nehmen. Die Abklärung der Datenschutzfragen zwischen Institut und meiner Geschäftsstelle war in weniger als zwei Wochen abgewickelt.

3.6.4 Datenübermittlung durch Meldebehörden zu Forschungszwecken

Die sozialwissenschaftliche Forschungsstelle einer bayerischen Universität führte im Berichtszeitraum Forschungsprojekte über die Segregation alter Menschen und über das generative Verhalten von Gastarbeiterfamilien durch. Zu diesem Zweck sollten von verschiedenen ausgewählten bayerischen Kommunen über die Meldeämter die dazu benötigten Daten bereitgestellt werden. Die ursprüngliche Absicht, diese Informationen mit dem identifizierenden behördlichen Suchbegriff (Personenkennzeichen) oder mit dem in automatisierten Verfahren benützten Ordnungsmerkmal zu übermitteln, stieß, auch bei den betroffenen Kommunalbehörden, auf datenschutzrechtliche Bedenken.

Da gegen die Übermittlung anonymisierter Daten grundsätzlich keine datenschutzrechtlichen Vorbehalte bestehen, konnte erreicht werden, daß die zutreffende sozialwissenschaftliche Forschungsstelle auf die Übermittlung des Suchbegriffs oder des Ordnungsmerkmals verzichtete, so daß die Möglichkeit der Bestimmbarkeit einer natürlichen Person durch die Kenntnis behördeninterner Suchmerkmale durch Dritte ausgeschlossen werden konnte. Die solchermaßen anonymisierten Daten dürfen darüber hinaus nur für diese bestimmten Forschungsprojekte verwendet werden und sind durch die Forschungsstelle zu löschen, wenn die Durchführung der Forschungsvorhaben abgewickelt worden ist.

3.7 Statistik und Planung

3.7.1 Grundsätze

Im Rahmen des Forschungs- und Entwicklungsvorhabens „Entwicklung von Methoden und Verfahren für Planungs- und Entscheidungshilfen auf der Basis des automatisierten Einwohnerwesens (PENTA-Projekt)", mit dessen Durchführung das Institut DATUM e.V. beauftragt war, wurde der bayerische Landesbeauftragte für den Datenschutz mit den Datenschutzfragen dieses Projektes befaßt. Obwohl PENTA Ende 1981 ausgelaufen ist, erscheint es nicht zweckmäßig, ohne Abstimmung mit den übrigen Datenschutzbeauftragten zu diesem Problem abschließend Stellung zu nehmen, zumal nur Teile dieses Entwicklungsvorhabens realisiert wurden. Es erscheint jedoch nützlich, an dieser Stelle grundsätzliche Anmerkungen über den Datenschutz in Statistik und Planung zu machen. Beim Aufbau oder der Erweiterung eines Datenpools für die kommunale Statistik und Planung sind folgende Regeln zu beachten:

1. Werden Daten für statistische Datenbanken beim Betroffenen erhoben, so ist dieser stets davon zu unterrichten, ob und welche Daten für statistische Zwecke gespeichert werden.
2. Es ist grundsätzlich sicherzustellen, daß durch Verknüpfung von Individualdaten kein Persönlichkeitsbild eines einzelnen entstehen kann.
3. Individualdaten aus statistischen Datenbanken sind von der Offenbarungspflicht gegenüber anderen Behörden auszuschließen.
4. Bei der Speicherung von sensiblen personenbezogenen Daten, wie Straftaten, Gesundheitsdaten oder Angaben über wirtschaftliche Verhältnisse, ist grundsätzlich die Einwilligung des Betroffenen notwendig, sofern keine gesetzlichen Grundlagen für die Speicherung dieser Daten vorhanden sind.
5. Soweit Individualdaten nicht für Verlaufsstatistiken oder ähnliches benötigt werden, sollten personenbezogene Daten möglichst frühzeitig anonymisiert werden. Derartige Individualdaten dürfen dann keine identifizierenden Merkmale mehr enthalten, die einen direkten Personenbezug herstellen können.
6. Die speichernde Stelle muß durch geeignete Sicherungsmaßnahmen gewährleisten, daß eine unbefugte Kenntnisnahme oder Verknüpfung von Individualdaten verhindert wird, da nicht auszuschließen ist, daß im Einzelfall die Personenbezogenheit erhalten bleiben kann.
7. Eine Veröffentlichung bzw. Übermittlung von personenbezogenen Daten aus statistischen Datenbanken ist grundsätzlich zu unterlassen.
8. Bei der Verarbeitung und Auswertung von statistischen Datenbanken sollten – soweit möglich – folgende Grundsätze Beachtung finden: Bei der Erfassung von Grundgesamtheiten ist eine generelle Vorsicht geboten: Je kleiner die Stichprobe, um so weniger läßt sich ein konkreter Personenbezug herstellen. Schließlich ist bei der Kontrolle der Ergebnisse zu prüfen, inwieweit die Ergebnisse im Zuge der Anonymisierung modifiziert werden können, ohne daß dabei der Informationsgehalt des Ergebnisses darunter leidet.

3.7.2 Kommunale Statistik und Planung

Artikel 57 Bayerische Gemeindeordnung weist den Gemeinden im eigenen Wirkungskreis eine Reihe von Aufgaben zu, die, je größer die Gemeinde, um so wirkungsvoller bewältigt werden können, wenn fundiertes Datenmaterial zur Verfügung steht. Dieses Datenmaterial kann entweder aus dem Verwaltungsvollzug oder aus eigenen Erhebungen stammen. Häufig wird für derartige Querschnittsaufgaben ein eigenes Amt innerhalb der Gemeinde mit der Durchführung dieser Tätigkeiten betraut. Kommen die Daten aus dem Vollzug, handelt es sich um eine Datenübermittlung nach Art. 17 BayDSG. Eine Übermittlung von personenbezogenen Daten an andere öffentliche Stellen ist aber nur dann zulässig, wenn sie zur rechtmäßigen Erfüllung der durch Rechtsnorm der übermittelnden Stelle oder dem Empfänger zugewiesenen Aufgaben erforderlich ist. Die Erforderlichkeit ist zu prüfen, dabei in den meisten Fällen anzunehmen. Konkrete Rechtsgrundlagen für die Nutzung für statistische und planerische Zwecke fehlen jedoch im allgemeinen. Den Erhebungen beim Betroffenen liegen bis auf wenige Ausnahmen ebenfalls keine rechtlichen Verpflichtungen zugrunde. In solchen Fällen ist der Betroffene nach Art. 16 Abs. 2 BayDSG auf die Freiwilligkeit seiner Angaben hinzuweisen. Die Praxis hat gezeigt, daß Erhebungen auf Freiwilligenbasis sich häufig durch

eine schlechte Datenqualität auszeichnen. Dieses Problem ließe sich aber in den Griff bekommen, wenn der Betroffene über den Wert seiner Angaben aufgeklärt wird. Im allgemeinen wird der Bürger dann keine Datenabstinenz ausüben, wenn er erkennt, daß ihm oder der Allgemeinheit durch das Ergebnis der Datenerhebung ein Nutzen entsteht.

Kommunale Statistik, Stadtforschung und Planung sind, wie oben bereits bemerkt, besonders für größere Kommunen von Bedeutung. Besprechungen und Informationsbesuche im Berichtszeitraum führten hierbei zu folgenden Ergebnissen:

1. Bei freiwilligen Erhebungen ist der Hinweis auf die Freiwilligkeit der Angaben deutlich hervorzuheben. Bei einer Erhebung wurde festgestellt, daß die verwendete Darstellungsform geeignet war, beim Betroffenen Zweifel über die Freiwilligkeit seiner Angaben entstehen zu lassen.
2. Häufig wird bei freiwilligen Erhebungen auf die ausschließliche Verwendung der Daten ohne Namen – für Planungszwecke hingewiesen. Hierdurch wird bei dem Betroffenen der Eindruck erweckt, daß bei seinen Angaben, die rein statistischen Zwecken dienen sollen, ein Personenbezug wegen fehlenden Namens überhaupt nicht hergestellt werden könne. Dies kann im Einzelfall unrichtig sein – auch wenn der erhobene Name für die statistische Auswertung nicht verwendet wird. Auch hier sind daher eindeutige Formulierungen notwendig.
3. Bei freiwilligen Erhebungen sind die Betroffenen über die Folgen, welche die Datenerhebung und die Datenspeicherung nach sich ziehen könnten, nicht im unklaren zu lassen.

Um mit einem vertretbaren Aufwand wirksame Datensicherungsmaßnahmen in Fachämtern, die mit solchen Aufgaben betraut sind, festzulegen, wurden – soweit solche Maßnahmen nicht ohnehin schon praktiziert werden – folgende Maßnahmen vorgeschlagen:

1. Bei der Verknüpfung von Dateien mit personenbezogenen Daten aus unterschiedlichen Fachbereichen ist grundsätzlich die Erforderlichkeit und eine eventuelle Beeinträchtigung schutzwürdiger Belange zu überprüfen. Gegebenenfalls ist der interne behördliche Beauftragte für den Datenschutz einzuschalten. Bei Übernahme von neuen Datenbeständen sind im Hinblick auf die Freigabe nach Artikel 26 Abs. 2 BayDSG der interne Datenschutzbeauftragte und der Landesbeauftragte ohnehin zu beteiligen.
2. Alle Aufgaben, in denen personenbezogene Daten verarbeitet werden und die über den routinemäßigen Tagesbetrieb hinaus gehen, sind zu protokollieren. Aus diesen Aufzeichnungen sollte klar erkennbar sein, welche Daten zu welchem Zweck verarbeitet wurden, und ob das Ergebnis personenbezogene Daten enthält oder nicht.

3.7.3 Statistik-Geheimnis und zulässige Übermittlung und Nutzung statistischer Einzelangaben

§ 11 des Bundesstatistikgesetzes, der die Geheimhaltung von Einzelangaben regelt, die für eine Bundesstatistik erhoben wurden, bestimmt auch, daß statistische Einzelangaben an andere (öffentlichen) Stellen nur übermittelt werden dürfen, wenn und soweit die Übermittlung unter Angabe des Empfängerkreises und der Art des Verwendungszweckes in der die Statistik anordnenden Rechtsvorschrift zugelassen und in den Erhebungsvordrucken bekanntgegeben ist.

Die Überprüfung von statistischen Erhebungsbogen veranlaßt mich, auf die Notwendigkeit einer Bekanntgabe etwaiger Nutzungen oder Übermittlungen in der Rechtsvorschrift und in den Erhebungsvordrucken besonders hinzuweisen. Ich gehe daher bei der Überprüfung etwaiger Nutzungen von statistischen Einzelangaben, beispielsweise durch die Gemeinden, die an der Erhebung mitwirken, davon aus, daß der Hinweis auf diese Nutzung auf dem Erhebungsbogen so angebracht werden muß, daß der Betroffene bei normaler bzw. üblicher Art des Ausfüllens von dieser Nutzung Kenntnis erlangt.

Mit dem Bayerischen Statistischen Landesamt wurde daher bereits für die Bodennutzungserhebungen 1977 bis 1982 und für die Viehzählung eine Übereinkunft getroffen, nach der die Unterrichtung über zulässige Übermittlungen von Einzelangaben unter einer hervorgehobenen Überschrift „Geheimhaltung und zulässige Datenübermittlung" erfolgt (s. a. 3. TB Nr. 3.6.1, S. 21). Meiner Ansicht nach würden erhebliche Zweifel an der wirksamen Unterrichtung über Datenübermittlungen und damit an deren Zulässigkeitsvoraussetzungen nach § 11 Abs. 3 Bundesstatistikgesetz bestehen, wenn die Erläuterung der Übermittlung von Einzelangaben lediglich unter der beruhigenden Überschrift „Geheimhaltung" auf der Rückseite eines Erhebungsbogens abgedruckt wären. Dies gilt besonders wenn nicht vom Betroffenen, sondern vom Zähler ausgefüllt wird, so daß der Betroffene nur unterschreibt und wohl im Regelfall von der Rückseite des Formulars keine Kenntnis nimmt.

In diesem Zusammenhang wird vom Statistischen Landesamt stets zu Recht besonders hervorgehoben, daß auch Einzelangaben, die an andere Stellen übermittelt werden dürfen, nicht zu Maßnahmen gegen den Betroffenen verwendet werden dürfen (§ 11 Abs. 3 Satz 3 Bundesstatistikgesetz).

Behörden, denen durch Rechtsvorschrift die Möglichkeit eröffnet ist, statistische Einzelangaben (mit oder ohne Namensangabe) zu verwenden, wird durch diese Vorschrift auferlegt zu prüfen, ob die Art der Verwendung zu „Maßnahmen gegen den Betroffenen" führt. Daß das Bundesstatistikgesetz hier von Maßnahmen und nicht von Entscheidungen spricht, läßt darauf schließen, daß über das Verbot hinaus, die Angaben im Rahmen von Verwaltungsakten zu verwerten, auch ein Verbot besteht, die Angaben zu sonstigen gegenüber dem Betroffenen beschwerend wirkenden Maßnahmen zu verwenden.

Klargestellt ist damit, daß eine Berichtigung des Melderegisters aufgrund der Erhebungen zur Volks-, Berufs-, Wohnungs- und Arbeitsstättenzählung (Volkszählung) zu keinem Ordnungswidrigkeitenverfahren wegen fehlender Anmeldung führen darf. Dies wird in

§ 9 des Entwurfs eines Volkszählungsgesetzes 1982 nochmals ausdrücklich wiederholt (Abs. 1 Satz 2). Das Verbot gilt aber auch für Bundes- oder Landesbehörden, denen nach § 9 Abs. 2 des genannten Entwurfes Volkszählungs-Einzeldaten übermittelt werden sollen und für Gemeinden und Gemeindeverbände, die nach Abs. 3 des Entwurfs für Zwecke der Regionalplanung, des Vermessungswesens, der gemeindlichen Planung und des Umweltschutzes sowie für eigene statistische Aufbereitungen Einzelangaben erhalten sollen. Der Begriff der gemeindlichen Statistik und Planung muß also im Lichte des Verbots von Maßnahmen gegen den Betroffenen interpretiert werden. Eine Planung, die sich mittelbar oder unmittelbar gegen den Betroffenen auswirkt, dürfte unter Zuhilfenahme statistischer Einzeldaten, wie z. B. auch von Daten der Volkszählung, nicht betrieben werden (s. hierzu auch die Anmerkungen zur Planungsdatensammlung in meinem 2. Tätigkeitsbericht, Nr. 4.1.3.1, Seite 20/21).

3.8 Archivwesen

Zwischen Datenschutz und Archivwesen sind in jüngster Zeit einige Problemfelder deutlich geworden, die eine gesetzliche Regelung aus der Sicht des Datenschutzes wünschenswert erscheinen lassen:

- So sind seit Inkrafttreten des Bayer. Datenschutzgesetzes die seinem Schutzbereich unterfallenden personenbezogenen Daten nach Art. 20 Abs. 1 BayDSG zu sperren, wenn die Kenntnis der Daten für die speichernde Stelle zur rechtmäßigen Erfüllung der ihr durch Rechtsnorm zugewiesenen Aufgaben nicht mehr erforderlich ist. Sofern der Betroffene es verlangt, sind diese Daten nach Art. 20 Abs. 4 BayDSG sogar zu löschen. Während gesperrte Daten nach Art. 20 Abs. 2 BayDSG einer beschränkten Nutzung beispielsweise für wissenschaftliche Zwecke offenstehen, zu der möglicherweise die Archivtätigkeit gerechnet werden kann, gehen Daten, die nach Art. 20 Abs. 4 BayDSG zu löschen sind, den Archiven verloren. Wegen dieser Problematik enthalten einige Landesdatenschutzgesetze sogenannte Archivklauseln, wonach Daten vor ihrer Löschung den Archiven angeboten werden müssen. Die Praxis hat jedoch gezeigt, daß diese Bestimmungen nicht ausreichen und für diesen Problembereich wohl umfangreichere Regelungen erforderlich sind.
- Schwierigkeiten können auch dort auftreten, wo die Abgabe von Daten an Archive ansteht, die einem besonderen Geheimnisschutz unterliegen (zum Beispiel Gesundheits-, Sozial- oder Steuerdaten). Die entsprechenden Geheimhaltungsvorschriften könnten möglicherweise einer Abgabe dieser Daten an die Archive entgegenstehen. Dies mag am Beispiel von Sozialhilfeakten deutlich werden:

  Eine Abgabe von Sozialhilfeakten an das Staatsarchiv ist eine Offenbarung von Angaben über persönliche und sachliche Verhältnisse von Sozialhilfeempfängern. Eine solche Offenbarung ist nach § 35 Abs. 2 SGB I „nur unter den Voraussetzungen der §§ 67 bis 77 des 10. Buches" SGB zulässig. Nach keiner dieser Bestimmungen ist eine Offenbarung von Sozialdaten zu Archivzwecken erlaubt. Inwieweit der Gesetzgeber diese Fragestellung übersehen hat oder absichtlich nicht geregelt hat, kann dahinstehen. Jedenfalls hat diese Rechtslage zur Folge, daß Sozialhilfeakten, die lebende Personen betreffen, dem Staatsarchiv nur dann überlassen werden dürfen, wenn entweder die Betroffenen in die Aktenweitergabe eingewilligt haben, oder die Sozialhilfeakten durch Löschung der Identifizierungsangaben so aufbereitet wurden, daß Betroffene nicht mehr bestimmbar sind. Sozialhilfeakten können daher an das Staatsarchiv erst dann abgegeben werden, wenn die Betroffenen verstorben sind oder ihr Ableben mit hoher Wahrscheinlichkeit anzunehmen ist.

  Akten von Sozialleistungsträgern enthalten allerdings fast immer auch medizinische Daten. Nach § 76 Abs. 1 SGB X ist der Sozialleistungsträger gehalten, solche Daten nur unter den Voraussetzungen zu offenbaren, unter denen die in § 203 Abs. 1 und 3 StGB genannten Personen selbst zur Offenbarung befugt wären. Nach § 203 Abs. 4 StGB ist die unbefugte Offenbarung fremder Geheimnisse auch nach dem Tode des Betroffenen strafbar. Auch in diesen Fällen wird die Befugnis zur Offenbarung nur vorliegen, wenn eine ausdrückliche Zustimmung des Betroffenen – etwa ausgesprochen noch vor seinem Tode – oder seine mutmaßliche Einwilligung vorliegt oder aufgrund besonderer Gesetze oder eines Notstandes die Offenbarung erlaubt ist. Eine ausdrückliche gesetzliche Befugnis liegt meines Erachtens nicht vor. Inwieweit die mutmaßliche Einwilligung des Betroffenen angenommen werden kann, erscheint zweifelhaft.

  Im übrigen kann auch die Ausnahmeregelung des § 76 Abs. 2 SGB X über die Weitergabe von Gutachten und Bescheinigungen wegen der Erbringung von Sozialleistungen eine Abgabe an das Staatsarchiv nicht rechtfertigen, weil eine derartige Weitergabe nicht dem Vollzug einer gesetzlichen Aufgabe im Sinne des § 69 Abs. 1 Nr. 1 SGB X dienen würde.
- Teilweise wird Aktenmaterial an die Archive zur Zwischenlagerung abgegeben, noch bevor über die endgültige Archivwürdigkeit entschieden ist. In diesen Fällen verwaltet das Archiv die Materialien quasi im Auftrag für die an sich zuständige Stelle. Durch § 10 Abs. 5 Melderechtsrahmengesetz wird diese Möglichkeit im übrigen für die Meldedaten gesetzlich eröffnet. Derartige zwischengelagerte Daten dürfen der üblichen Nutzung durch die Archive grundsätzlich nicht offenstehen.
- Schließlich können Zweifelsfragen auftreten, weil die zeitgeschichtliche Forschung an archiviertem Material aus jüngerer Zeit interessiert ist. Es kann nicht ausgeschlossen werden, daß hiervon Daten noch lebender Personen betroffen werden.

– Aus dem Blickwinkel des Datenschutzes tritt noch ein weiteres Problem hinzu: Ab 1. Januar 1983 genügt es nicht mehr, daß Speichern, Verändern und Übermitteln personenbezogener Daten zur Erfüllung öffentlicher Aufgaben erforderlich sind (Art. 37 Abs. 3 Satz 1 BayDSG). Nach diesem Zeitpunkt ist die Verarbeitung geschützter personenbezogener Daten nur zulässig, wenn sie zur rechtmäßigen Erfüllung der durch Rechtsnorm zugewiesenen Aufgabe erforderlich ist (Art. 16 Abs. 1, 17 Abs. 1 BayDSG). Zwar ist derzeit die Menge der vom Bayer. Datenschutzgesetz erfaßten personenbezogenen Daten, also der Daten, die in Dateien oder Karteien geführt sind, die zur Abgabe an Archive heranstehen, noch gering, doch ist mit dem Anwachsen derartiger Daten in näherer Zukunft zu rechnen.

Derzeit regeln im wesentlichen nur Benutzungsordnungen das Archivwesen. Sofern künftig Rechtsvorschriften erforderlich sind, genügen diese Benutzungsregelungen den Anforderungen nicht.

Folgende Schwerpunkte einer Archivgesetzgebung sehe ich:

Die Aufgaben der Staatlichen Archive sollten möglichst deutlich beschrieben werden, weil sich nach Datenschutzrecht die Zulässigkeit einer Datenspeicherung nach der erforderlichen Aufgabenerfüllung bemißt. Meines Erachtens sollte hierbei auch eine deutliche Trennung gegenüber der Tätigkeit der öffentlichen Verwaltung zum Ausdruck gebracht werden.

Die Begriffe „Archivgut" und „archivwürdig" haben für die Datenübermittlung von den Verwaltungsbehörden zu den Archiven und für die Frage der Zulässigkeit der Aufbewahrung bei den Archiven eine Schlüsselbedeutung. Zur Vermeidung von Auslegungsschwierigkeiten sollten sie möglichst genau definiert werden.

Sofern Archiven die Einsicht in sämtliche bei staatlichen Behörden, Gerichten und sonstigen Dienststellen angefallenen und zur Erledigung laufender Geschäfte nicht mehr benötigten Unterlagen gestattet werden soll, damit die Archive selbst die Frage der Archivwürdigkeit entscheiden können, würde dies den Archiven – von Befugnissen des Obersten Rechnungshofes abgesehen – eine Sonderstellung zuweisen. Die Notwendigkeit eines solchen umfassenden Einsichtsrechts muß daher meines Erachtens sorgfältig geprüft werden. Aus der Sicht des Datenschutzes erscheint eine so weitgehende Einsichtnahme jedenfalls nicht unbedenklich.

Einer Lösung bedarf das Verhältnis von Sperrung und Löschung nach den Datenschutzgesetzen und den Erfordernissen der Archive nach Erfassung möglichst aller archivwürdigen Materialien.

Das Anlegen von Zwischenarchiven und der Zugriff der Archivare auf diese Materialien bedarf einer Regelung, die die originären Zuständigkeiten der abgebenden Verwaltung unberührt läßt. Sofern Daten einem besonderen Geheimnisschutz unterliegen, ist für deren Abgabe an Archive gegebenenfalls eine gesonderte Regelung notwendig.

Eine vollständige Übernahme des in einem Teilbereich der Verwaltung angefallenen Schriftgutes sollte nach Möglichkeit ausgeschlossen werden, um zu vermeiden, daß durch Einsatz künftiger Techniken beim Archiv die Daten zusammengeführt und ausgewertet werden, obwohl deren Zusammenführung bei den Verwaltungsstellen nach dem Datenschutzrecht untersagt war.

Generell sollte sichergestellt werden, daß eine Beeinträchtigung schutzwürdiger Belange der Betroffenen durch die Benutzung der Archive ausscheidet. Hierzu ist sicherzustellen, daß der Zugriff auf Archivalien möglichst erst nach Ableben der Betroffenen gestattet wird. Außerdem sollten die Betroffenen entsprechend den grundliegenden Datenschutzrechten ein Auskunftsrecht erhalten. Sofern der Betroffene hierbei Unrichtigkeiten feststellt, ist ihm zumindest eine Art Gegendarstellungsrecht zu gewähren. Bei der Sammlung umfassender Datenmengen bestimmter Bevölkerungsgruppen ist zu beachten, daß hierdurch für diese kein besonderes Gefährdungspotential eröffnet werden darf.

In einem Archivgesetz sollten möglichst schon jetzt künftige Entwicklungen auf dem Gebiet der Informationstechnologie mit deren umfassenden Speicherung- und Auswertungsmöglichkeiten berücksichtigt werden. Die Erstellung von Persönlichkeitsprofilen sollte auch den Archiven untersagt sein.

Schließlich empfiehlt sich eine Regelung zur Datensicherung vergleichbar der Bestimmung des Art. 15 BayDSG.

Ich habe es außerordentlich begrüßt, daß das Bayer. Staatsministerium für Unterricht und Kultus in seiner Antwort vom 15. Juni 1981 auf die schriftliche Anfrage eines Abgeordneten mitgeteilt hat, daß auch für Bayern der Erlaß eines Archivgesetzes angestrebt wird und eine gesetzliche Regelung des Archivwesens neben der Festlegung seiner Aufgaben die erforderlichen bereichsspezifischen Datenschutzbestimmungen enthalten könnte.

### 3.9 Verschiedenes

#### 3.9.1 Datenschutzrechtliche Freigabe nach Art. 26 Abs. 2 BayDSG

Im Berichtszeitraum habe ich festgestellt, daß die Mitteilungen über die datenschutzrechtliche Freigabe in der Planung befindlicher automatisierter Verfahren gegenüber dem Vorjahr zunahmen. In einigen Fällen wurden mir auch die Ergebnisse der Hauptuntersuchung zur datenschutzrechtlichen Stellungnahme übersandt. Grundsätzlich ist gegen ein derartiges Verfahren nichts einzuwenden. Es ist allerdings festzuhalten, daß die Hauptuntersuchung sich an andere Zieladressaten richtet und im allgemeinen für eine datenschutzrechtliche Stellungnahme weniger geeignet ist, weil – wie die Erfahrung zeigte – Aussagen über die Rechtsgrundlagen für die Speicherung und Übermittlung von personenbezogenen Daten fehlten.

Für die datenschutzrechtliche Freigabe nach Art. 26 Abs. 2 und 4 BayDSG sollten – wie bereits im 2. Tätigkeitsbericht unter der Ziffer 2.2.5 auf Seite 9 behandelt – folgende Angaben gemacht werden:

- Eine kurze Verfahrensbeschreibung mit Hinweis auf den betroffenen Personenkreis und ungefähre Abschätzung des Mengengerüsts;
- Beschreibung des Datensatzes auf Feldebene mit Angabe der Rechtsgrundlage für die Speicherung bzw. Verarbeitung;
- Beschreibung des Datensatzes auf Feldebene mit Angabe der Rechtsgrundlage für die Übermittlung von personenbezogenen Daten;
- Art des ADV-Verfahrens (z.B. Online- oder Batch-Verfahren);
- die Stelle, die für die Systementwicklung und Programmierung des Verfahrens zuständig ist;
- der Ort, an dem die Daten verarbeitet werden sollen;
- Beschreibung der vorgesehenen technischen und organisatorischen Maßnahmen zur Datensicherung.

Bei der Verarbeitung personenbezogener Daten im Auftrag ist stets darauf zu achten, daß eine schriftliche Regelung im Sinne von Nr. 3.4 ff. der Vollzugsbekanntmachung zum Bayer. Datenschutzgesetz abgeschlossen wird. Schließlich hat sich die auftraggebende Behörde davon zu überzeugen, daß beim Auftragnehmer ausreichende Datensicherungsmaßnahmen vorhanden sind. Das ist zum Beispiel auch dann notwendig, wenn im Hauptamt einer Kommune auf einem Textsystem Adressenmaterial aus Ämtern verarbeitet wird, die sensiblere Daten verarbeiten, wie etwa das Sozial- oder Gesundheitsamt.

Bei der Planung eines automatisierten Verfahrens sollte man an die automatisierte Speicherung der einzelnen Datenfelder eines Datensatzes einen strengen Maßstab anlegen. Häufig sind Datenfelder sensiblen Inhalts nicht sogenannte „Muß-", sondern lediglich „Kannfelder" oder sie haben im automatisierten Verfahren keine wesentliche Bedeutung. Hier ist zu überlegen, ob der zusätzliche technische und organisatorische Datensicherungsaufwand für diese sensiblen Daten in einem wirtschaftlichen Verhältnis zu dem Automatisierungseffekt steht. Beim Aufbau von Personalinformationssystemen können das insbesondere Angaben über Dienststrafverfahren oder Ergebnisse von Beurteilungen sein.

Schließen sich Behörden einem bereits überregional laufenden Verfahren, zum Beispiel einem Verfahren der AKDB, an, so ist auf eine Freigabemitteilung nach Art. 26 Abs. 4 zu verzichten, da der Landesbeauftragte für den Datenschutz durch die Meldung zum Datenschutzregister ohnehin vom Anschluß an das betreffende Verfahren in Kenntnis gesetzt wird und die AKDB ihrerseits das Verfahren nach Art. 26 Abs. 2 und Abs. 4 BayDSG beim Landesbeauftragten anzuzeigen hat.

3.9.2 Zum Datenschutzregister

Auch im Jahre 1981 mußte ich feststellen, daß bei vielen Stellen noch Unklarheit über die Art und den Umfang des Meldevorgangs herrscht. Eine formlose Anmeldung einer automatisiert geführten Datei zum Datenschutzregister ist nicht möglich. Für die Erst- sowie für die Änderungsmeldung sind die im Bayerischen Staatsanzeiger Nr. 48/1978 veröffentlichten Meldeformulare zu verwenden. Bei Abgabe einer Änderungsmeldung ist jedoch zu beachten, daß eine solche nur dann erforderlich ist, wenn sich das Verfahren geändert hat, z.B. durch zusätzliche Datenübermittlungen an Dritte oder durch die Erweiterung des Datensatzes. Eine Änderungsmeldung ist aber dann abzugeben, wenn eine bereits bestehende Datei für die maschinelle Abwicklung weiterer Aufgaben verwendet wird.

Bei manchen Meldungen mußte ich feststellen, daß die Datei nicht meldepflichtig ist, da keine personenbezogenen Daten gespeichert werden. In vielen Bereichen werden im übrigen für statistische Zwecke anonymisierte Daten automatisiert gespeichert und verarbeitet. Können aber die Daten einer solchen anonymisierten Datei durch die speichernde Stelle z.B. mit Hilfe einer manuell geführten Kartei über den Inhalt von Datenfeldern ohne unverhältnismäßigen Aufwand wieder auf bestimmte Personen bezogen werden, so wird eine derartige Datei meldepflichtig. In die Überlegungen sind auch Dateien anderer Stellen einzubeziehen, wenn ihre Nutzung für die speichernde Stelle ohne unverhältnismäßigen Aufwand möglich ist. Ist eine Reidentifizierung für die speichernde Stelle nicht oder nur sehr schwierig möglich, braucht diese automatisiert geführte anonymisierte Datei nicht zum Datenschutzregister gemeldet zu werden. Gleichwohl ist aber bei Datenübermittlungen aus solchen nicht meldepflichtigen Dateien zu prüfen, ob die empfangende Stelle einen Personenbezug herstellen kann. Zutreffendenfalls ist die Notwendigkeit einer Anzeige zum Datenschutzregister erneut zu prüfen.

Die Inanspruchnahme des Registers durch den Bürger war im Berichtszeitraum etwas geringer als im Vorjahr. Die Übersicht, deren Erstellung zugegebenermaßen etwas aufwendig ist, hat aber für den Bürger meines Erachtens einen hohen Informationswert, da er einen umfassenden Überblick über die automatisierten Datenspeicherungen im öffentlichen Bereich des Landes erhält. Als besonders wertvoll hat sich das Register wieder für die Kontrolltätigkeit des Landesbeauftragten für den Datenschutz erwiesen. Durch die Übernahme des Registers auf eine elektronische Rechenanlage erhoffe ich mir durch die gezielte Auswertbarkeit der Informationen eine weitere Steigerung des Informationsgehaltes.

Durch die zunehmende Büroautomation werden in naher Zukunft bei der Verbindung von Text- und Informationsverarbeitung weitere Dateien mit personenbezogenen Daten entstehen. Auch im Krankenhauswesen und bei der Kfz-Zulassung werden in den kommenden Jahren bisher manuell durchgeführte Verwaltungsaufgaben automatisiert abgewickelt wer-

den. Schließlich wird auch der Einzug der elektronischen Datenverarbeitung in die Parlamentsarbeit Meldungen zum Datenschutzregister zur Folge haben, nämlich dann, wenn Beschwerden und Petitionen in personenbezogener Form automatisiert geführt werden. Diese Gesichtspunkte lassen in absehbarer Zeit nicht auf einen Abschluß beim Aufbau des Datenschutzregisters hoffen.

3.9.3 Datenübermittlung auf Postkarten

Im Berichtszeitraum bin ich wieder mehrfach von Behörden befragt worden, inwieweit im Verkehr zwischen Behörden und bei Schriftwechsel mit Privaten Postkarten als Datenträger für personenbezogene Daten verwendet werden könnten. Hierzu stelle ich folgendes fest:

Gegen die Verwendung von Postkarten im Verkehr zwischen Behörden bestehen grundsätzlich keine Bedenken. Für den Übermittlungsweg der Postkarte gilt das Postgeheimnis, so daß außenstehende Dritte grundsätzlich vom Inhalt der Postkarte nicht Kenntnis erlangen. Zudem sind die Bediensteten der betroffenen Behörden zur Amtsverschwiegenheit verpflichtet. Die Verwendung von Briefumschlägen würde im übrigen, abgesehen von den erhöhten Portokosten, einen unverhältnismäßig hohen Arbeitsaufwand bedingen und bei anfragender wie auskunftserteilender Behörde erhöhte Arbeitsbelastung zur Folge haben. Daher habe ich keine Bedenken, wenn Anfragen der Polizei an das Meldeamt oder an die Zulassungsstellen nach den Namen der Kfz-Halter im Ordnungswidrigkeitenverfahren auf Postkarten gestellt und beantwortet werden. Selbstverständlich gehe ich davon aus, daß in begründeten Einzelfällen, in denen aufgrund besonderer Umstände eine Beeinträchtigung schutzwürdiger Belange eines Betroffenen zu befürchten sind, ausnahmsweise verschlossene Briefumschläge verwendet werden.

Allerdings muß durch organisatorische Maßnahmen sichergestellt werden, daß auch innerhalb der betroffenen Behörden nur die Bediensteten Kenntnis vom Inhalt der Postkarten nehmen können, die mit der Erledigung beauftragt sind. So habe ich in einem Fall vorgeschlagen, diese Antwortkarten nicht im allgemeinen Auslaufkorb abzulegen, sondern sie gesondert bis zu Abholung aufzubewahren.

Sofern die Behörden einen Schriftwechsel mit Privatpersonen führen, in dem personenbezogene Daten übermittelt werden, sind grundsätzlich verschlossene Briefumschläge zu verwenden. In diesem Falle kann nicht ausgeschlossen werden, daß die Mitteilungen der Behörde im Haushalt des Empfängers von Unberechtigten zur Kenntnis genommen werden können. Meines Wissens wird von bayerischen Behörden entsprechend verfahren (vgl. auch Justiz).

3.9.4 Veröffentlichung von Daten aus der Architektenliste

Die Bayerische Architektenkammer, eine Körperschaft des öffentlichen Rechts, führt aufgrund des Bayerischen Architektengesetzes die Architektenliste. Sie wird aufgrund von Neueintragungen, Änderungen und Löschungen fortgeschrieben. Jährlich einmal wurden bisher Name, Vorname, akademischer Grad, Anschrift, Fachrichtung und Mitgliedsnummer aller Kammermitglieder veröffentlicht, damit ohne zeitraubende Nachforschungen festgestellt werden kann, ob ein Entwurfsverfasser berechtigt ist, die Berufsbezeichnung „Architekt" zu führen. Diese Praxis dient dem Schutz der Berufsgruppe selbst, sowie Dritter, die Leistungen dieser Berufsgruppe in Anspruch nehmen oder Geschäftsbeziehungen mit Architekten aufnehmen wollen.

Nach Inkrafttreten der Datenschutzgesetze sind in einigen Bundesländern Bedenken gegen die Übermittlung oder Veröffentlichung aus der Architektenliste entstanden. Der Bayerische Landtag hat solchen Bedenken im Zuge der Novellierung des Bayerischen Architektengesetzes (GVBl. 1981 S. 498) durch folgende Neuregelung Rechnung getragen: „Aus der Architektenliste dürfen Auskünfte über Vornamen, Namen, akademische Grade, Fachrichtung und Tätigkeit der Architekten erteilt werden. Diese Angaben dürfen auch veröffentlicht werden. Art. 17 des Bayerischen Datenschutzgesetzes vom 28. April 1978 (GVBl. S. 165) bleibt unberührt."

3.9.5 Schülerfahrausweise des Münchner Verkehrsverbunds

Auf den Schülerfahrausweisen, die vom Münchner Verkehrsverbund ausgegeben wurden, waren neben Name, Vorname, Geburtsdatum und Anschrift des Schülers auch Name und Anschrift der vom Schüler besuchten Schule eingetragen. Sofern der Schüler einer Sonderschule angehörte, wurde dies durch den Zusatz „So" vermerkt. Den Münchner Stadtwerken – Verkehrsbetrieben habe ich meine datenschutzrechtlichen Bedenken gegen die Aufnahme dieses Zusatzes auf den Schülerfahrausweisen vorgetragen. Insbesondere habe ich darauf hingewiesen, daß schutzwürdige Belange der Betroffenen beispielsweise dadurch beeinträchtigt werden können, daß ein Kontrolleur unnötigerweise die Zugehörigkeit eines Schülers zu einer Sonderschule erfährt.

Auf meine Vorstellungen hin wird der Zusatz „So" auf den Schülerfahrausweisen künftig nicht mehr vermerkt.

3.9.6 Befreiung von der Rundfunkgebührenpflicht

Bei Datenschutzkontrollen habe ich festgestellt, daß Gemeinden eine sogenannte Rundfunkgebührenbefreiungskartei führen. Neben dieser Speicherung von Daten bei der Gemeinde ist datenschutzrechtlich noch von Bedeutung, daß die Gemeinden jeweils einen Abdruck des Bescheides über die Gebührenbefreiung an die Gebühreneinzugszentrale der Rundfunkanstalten (GEZ) übersenden.

Zur Rechtslage ist folgendes zu bemerken:

Nach § 5 Abs. 2 Satz 2 der Verordnung über die Befreiung von der Rundfunkgebührenpflicht vom 24. März 1981 (GVBl. S. 74) entscheidet über den Antrag auf Befreiung von der Rundfunkgebührenpflicht die Rundfunkanstalt auf Vorschlag der Gemeinde, bei der

der Antrag schriftlich einzureichen ist. Darüber hinaus kann die Rundfunkanstalt die Gemeinden zur Aushändigung des Befreiungsbescheides ermächtigen (§ 5 Abs. 2 Satz 3 der VO; vgl. auch Bekanntmachung des Bayer. Rundfunks vom 28. Juli 1978 StAnz. Nr. 31 Seite 2; Bekanntmachung des Bayer. Staatsministeriums für Arbeit und Sozialordnung vom 1. April 1981 – MABl. Seite 161). In der Praxis entscheiden jedoch die Gemeinden über die Anträge auf Befreiung von der Rundfunkgebührenpflicht selbst. Diese Praxis widerspricht zwar dem eindeutigen Wortlaut des § 5 Abs. 2 der Verordnung, ist aber wohl sinnvoll. Im Hinblick auf diese Rechtslage erscheint es auch zweifelhaft, ob die Gemeinden zulässigerweise die Rundfunkgebührenpflichtbefreiungskartei im derzeitigen Umfang führen.

Sofern die derzeitige Praxis als wirtschaftlich und bürgernah angesehen wird, rege ich an, die Verordnung über die Befreiung von der Rundfunkgebührenpflicht der Praxis anzupassen. Da mir von Vertretern der zuständigen Stellen zugesagt worden ist, daß eine entsprechende Novellierung erwogen wird, sehe ich zunächst davon ab, die bisherige Speicherung zu beanstanden. Vom Inhalt der geänderten Verordnung wird es abhängen, inwieweit die Speicherung der entsprechenden Daten bei der Gemeinde bzw. die Übermittlung der Daten an den Bayer. Rundfunk zulässig ist.

Besondere Bedenken ergeben sich zwangsläufig daraus, daß die Gemeinde einen Abdruck des Bescheides über die Rundfunkgebührenpflichtbefreiung an die GEZ übersendet, denn der Bescheid enthält auch die Gründe für die erfolgte Befreiung von der Gebührenpflicht. Zwar sind diese Gründe für die Entscheidung im Einzelfall von Bedeutung, für die Aufgabe der GEZ, die Rundfunkgebühren einzuziehen, sind sie jedoch meines Erachtens nicht erforderlich. Für sie müßte der Hinweis genügen, daß tatsächlich die Voraussetzungen für eine Befreiung erfüllt sind. Da es zu den Aufgaben des Datenschutzes gehört, umfassende Datenbanken über Minderheiten (Minderbemittelte, Schwerbehinderte) möglichst gering zu halten, ist die Speicherung der Befreiungsgründe bei der GEZ besonders bedenklich.

Ich gehe daher davon aus, daß im Zusammenhang mit der vorgenannten Novellierung der Verordnung über die Befreiung von der Rundfunkgebührenpflicht auch das gesamte Verfahren der Rundfunkgebührenpflichtbefreiung und der damit zusammenhängenden Datenspeicherungen sowie -übermittlungen überprüft wird.

### 3.9.7 Dienstanweisung für technische und organisatorische Maßnahmen des Datenschutzes

Bei Prüfungen im kommunalen Bereich hatte ich in den vergangenen Jahren angeregt, eine spezielle Dienstanweisung über die nach dem BayDSG erforderlichen technischen und organisatorischen Maßnahmen zum Datenschutz zu erlassen. In einer solchen Dienstanweisung sollten das Anlegen und Bearbeiten von Dateien, das Weitergeben von Daten, die Einsichtnahme in Dateien, der Transport von Datenträgern, das Aufbewahren von Dateien und das Vernichten von Datenträgern geregelt werden. Durch gelegentliche Kontrollen sollte sich der für den Datenschutz Zuständige auch von der Einhaltung der verfügten Maßnahmen überzeugen.

Die Erfahrung hat gezeigt, daß eine auf die Belange aller speichernden Stellen zugeschnittene Musterdienstanweisung unhandlich würde, da Gegebenheiten und Erfordernisse von Gemeinde zu Gemeinde recht verschieden sein könnten. Wichtiger als der Erlaß von Dienstanweisungen erscheint mir daher die Schulung der Mitarbeiter auf dem Gebiet des Datenschutzes. Nur so kann sich bei den zuständigen Mitarbeitern ein Blick für die jeweiligen Erfordernisse des Datenschutzes entwickeln. In einer solchen Schulung ist vor allem auf die Gefahren einzugehen, die bei Verstößen gegen das Datenschutzgesetz entstehen können.

Für den Fall, daß die Abfassung einer Dienstanweisung vorgesehen wäre, halte ich folgende Punkte für wichtig:

- Eine Dienstanweisung sollte sich stets an einen engbegrenzten Personenkreis richten;
- die Maßnahmen sollten sich an den Phasen der Datenverarbeitung orientieren und folgende Arbeitsschritte regeln:

  Anlegen und Bearbeiten von Dateien,
  Weitergabe von Daten,
  Aufbewahrung von Dateien und
  Vernichten von Daten;

- die angestrebten Maßnahmen sollen angemessen sein.

### 3.10 Datenschutz-Fortbildungsveranstaltungen

In Zusammenarbeit mit der Bayerischen Verwaltungsschule wurde 1981 begonnen, Fortbildungsveranstaltungen über Datenschutz in allen Regierungsbezirken Bayerns abzuhalten. Die Veranstaltungen sind für Mitarbeiter, die für den Vollzug des Datenschutzgesetzes zuständig sind, insbesondere Datenschutzsachbearbeiter, Datenschutzreferenten und Datenschutzbeauftragte, konzipiert. Um eine möglichst hohe Beteiligung sicherzustellen, werden sie eintägig abgehalten. Dabei wird in Kauf genommen, daß von den Besuchern teilweise eine länger als eintägige Unterrichtung für zweckmäßig gehalten wird, denn die Behörden können in der Regel Mitarbeiter nur für einen Tag problemlos abstellen. Auch der Aufwand an Reisekosten wird dadurch gering gehalten.

Die Fortbildungsveranstaltungen bieten:

- Schwerpunktmäßige Übersicht über rechtliche Datenschutzfragen nach dem BayDSG: Datenerhebung, -speicherung, -übermittlung, -sperrung und -löschung; Verantwortung; Kontrolle intern und extern; Rechte des Betroffenen.
- Schwerpunktmäßige Übersicht über Datensicherungsfragen aus der Praxis des Landesbeauftragten für den Datenschutz, Dateibegriff, Datenschutzregister, sensible Daten, Sicherungsmaß-

nahmen nach Art. 15 BayDSG, technische Einzelprobleme; gegebenenfalls mit Diskussion und Fragen der Teilnehmer.

- Behandlung von einzelnen Fällen aus der rechtlichen Datenschutzprüfung des Landesbeauftragten für den Datenschutz mit Diskussion (Melderecht, Standesämter, § 203 StGB u.ä.). Behandlung von einzelnen Datenschutzfragen aus dem Teilnehmerkreis. Gegebenenfalls, soweit Interesse, Erörterung von Problemfällen aus dem Bereich des SGB X (§§ 67 ff., Schutz von Sozialdaten).

Die bisherigen Veranstaltungen hatten einen erfreulichen Widerhall gefunden. Sie tragen zur intensiven Verbreitung der bei der Datenschutzprüfung durch den Landesbeauftragten gemachten Erfahrungen bei. In einigen Fällen wirkte dankenswerterweise auch der im Bayerischen Staatsministerium des Innern für Datenschutzrecht federführende Sachgebietsleiter am Unterricht mit.

3.11 Prüfung der technischen und organisatorischen Datenschutzmaßnahmen

Im Berichtszeitraum wurden bei ca. 30 öffentlichen Stellen die technischen und organisatorischen Maßnahmen zur Datensicherung überprüft. Daneben fanden auch Kontrollen der Einhaltung des Datenschutzrechts statt (s.o. 3.1.9). Der Schwerpunkt lag wiederum im kommunalen Bereich und bei Landratsämtern, wobei in erster Linie kreisfreie Städte, Große Kreisstädte und größere kreisangehörige Gemeinden besucht wurden. Die übrigen Behörden sind dem Bereich der Sozialleistungsträger, dem Finanzbereich und dem medizinischen Bereich zuzuordnen. Etwa ein Drittel der besuchten Behörden bedient sich bei der automatisierten Datenverarbeitung eigener Anlagen.

Die festgestellten Mängel waren insgesamt gesehen weniger gravierend als bei früheren Besuchen. Das mag einerseits daran liegen, daß Erkenntnisse aus Kontrollen vergangener Jahre dazu beigetragen haben, zunehmend die Erfordernisse des Datenschutzes zu berücksichtigen. Andererseits scheint die Schulungstätigkeit auf dem Gebiet des Datenschutzes Früchte zu tragen, so daß elementare Verstöße, die durch organisatorische Maßnahmen leicht zu beheben sind, kaum noch auftraten. Dort wo man sich mit dem Datenschutz eingehender beschäftigt hatte, fand ich eine Reihe von wirksamen Datensicherungsmaßnahmen vor, so daß häufig nur noch Verbesserungsvorschläge zu machen waren.

Die Erfahrung zeigt, daß es in der Praxis viele Wege und Möglichkeiten gibt, Datenschutz und Datensicherung zu verwirklichen, und daß wegen der Unterschiedlichkeit der Gegebenheiten Problemlösungen der einen Behörde nicht ohne weiteres auf eine andere Behörde zu übertragen sind. Schließlich sei darauf hingewiesen, daß die technischen und organisatorischen Maßnahmen zur Datensicherung bei einer Großstadt anders aussehen als bei einer kleineren kreisangehörigen Gemeinde, was aber wiederum nicht zu dem Schluß führen darf, daß dort weniger Datenschutz erforderlich wäre. Nur läßt sich dort, wie die Erfahrung zeigte, häufig mit weniger Aufwand die gleiche Außenwirkung erzielen.

Bevor ich auf Mängel näher eingehen möchte, sei eine Bemerkung zur Durchführung der von mir geforderten Datensicherungsmaßnahmen gemacht. Soweit die Realisierung von Datensicherungsmaßnahmen hohe finanzielle Mittel erforderte, konnte naturgemäß nicht auf eine unmittelbare Erledigung gedrungen werden. In solchen Fällen sind organisatorische Zwischenlösungen geboten. Allgemein läßt sich aber sagen, daß die gestellten Forderungen im großen und ganzen erfüllt wurden. Darüber hinaus fiel auf, daß in Behörden, in denen die Datenschutzangelegenheiten im Wege der Geschäftsverteilung personell zugeordnet waren, in der Regel weniger Probleme auftraten, weil bereits eine Reihe von Vorarbeiten geleistet war.

3.11.1 Prüfungen bei kommunalen Rechenzentren

Beispielhaft seien an dieser Stelle eine Reihe von Forderungen aufgeführt, die ich an den Rechenzentrumsbetrieb einer kreisfreien Stadt stellte. Die Rechenanlage läuft im bedienerlosen Betrieb auch nachts, weshalb erhöhte Sicherungsmaßnahmen geboten sind.

- Der Maschinenraum ist außerhalb der Dienstzeit so abzusichern, daß eine unbefugte Nutzung der Anlage im bedienerlosen Betrieb bemerkt wird.
- Sofern die Sicherung der Datenbestände auf Magnetbändern oder Disketten erfolgt, ist für die im Rechenzentrum aufbewahrten maschinell lesbaren Datenträger eine wirksame Abgangskontrolle einzuführen.
- Die Reinigung des Rechenzentrums hat grundsätzlich im Beisein von Rechenzentrumspersonal zu erfolgen.
- Beim Einsatz von Direktabfrageprogrammen ist darauf zu achten, daß die Fachabteilungen lediglich die Daten erhalten, die sie für die Abwicklung ihrer Aufgaben benötigen.
- Wegen der Betriebsbereitschaft der Anlage auch während der Nachtzeit ist dafür zu sorgen, daß grundsätzlich nur solche Datensichtstationen an die Anlage angeschlossen werden, die Betriebsschlösser besitzen.
- Die Verwendung von Dienstprogrammen, insbesondere des Programms zur Dateiduplizierung auf Magnetband, ist grundsätzlich zu protokollieren. Die aufgezeichneten „Log-Informationen" sind durch geeignete Verfahren stichprobenweise auszuwerten.
- Sofern die Programme eigenentwickelt werden, ist zur Erfüllung der Organisationskontrolle die Einführung von Dokumentationsrichtlinien und eines förmlichen Freigabeverfahrens geboten.
- Die Produktionsergebnisse für die Fachabteilungen, die mit besonders sensiblen Daten arbeiten, sind bis zur Abholung verschlossen aufzubewahren.

Die meisten dieser Anforderungen sind organisatorisch ohne besonderen finanziellen Aufwand zu erfüllen. Einige Maßnahmen sind für einen ordnungsgemäßen Betriebsablauf ohnehin selbstverständlich.

Eine Raumsicherung über Alarmanlagen dient neben der Daten- auch der Objektsicherung. Wird Software durch den Anwender selbst erstellt, sind bei rechtzeitiger Einplanung Datensicherungs- und Protokollfunktionen mit geringem Mehraufwand zu realisieren. Schließlich ist darauf zu achten, daß im Bereich des Rechenzentrums, zu dem bei diesen kleineren Einheiten auch die Datenerfassung zu zählen ist, nur solche Personen ihren Arbeitsplatz besitzen, die in der automatisierten Datenverarbeitung tätig sind. Dieser Bereich ist demnach vom täglichen Publikumsverkehr der Fachabteilungen abzuschotten, was jedoch nicht eine Dislozierung des Rechenzentrums in ein anderes Gebäude bedeuten muß.

3.11.2 Prüfungen bei Kommunalbehörden

Nachfolgend sind beispielhaft Sicherungs-Anforderungen aufgeführt, die an den Betrieb der manuellen Datenverarbeitung (also Karteien) bei größeren Kommunalbehörden zu stellen sind:

- Im Sozialbereich (Jugendamt, Sozialamt, Wohngeldstelle usw.), in dem sensible personenbezogene Daten gespeichert werden, sind Karteien und Unterlagen mit personenbezogenen Daten grundsätzlich in verschließbaren Behältnissen aufzubewahren. Nach Dienstschluß sind diese Behältnisse abzuschließen und die Schlüssel sicher zu verwahren. Die Bediensteten sind auf diese Sicherungsmaßnahmen hinzuweisen und über den Sinn dieser Maßnahmen zu belehren. Dasselbe gilt insbesondere für sensible personenbezogene Daten in der Führerscheinstelle sowie im Standesamt für die Mitteilungen über Adoptionen.
- Im Bereich des Steueramts ist es erforderlich, personenbezogene Steuerunterlagen so aufzubewahren, daß unbefugte Dritte, wozu auch das Reinigungspersonal zählt, keine Kenntnis nehmen können.
- Es ist darauf zu achten, daß auch innerhalb der Kommunalbehörde Unterlagen mit sensiblen personenbezogenen Daten verschlossen transportiert werden.
- Nicht benötigte listenmäßige Auswertungen mit personenbezogenen Daten sollten möglichst nach Anfall unmittelbar durch den Sachbearbeiter selbst vernichtet werden.

3.11.3 Prüfungen bei Landratsämtern

Bei automatisierter Datenverarbeitung waren die Stellen über Datenstationen an zentrale Rechner der AKDB angeschlossen. Sie betreiben also keine Systeme, auf denen dezentral Daten gespeichert werden. Die Datenverarbeitung besteht im wesentlichen nur aus der Datenerfassung und der Übertragung der erfaßten Daten an den zentralen Rechner; Auskunftssysteme waren nicht im Einsatz. Die Ergebnisse der automatisierten Datenverarbeitung werden in Listen- oder Mikrofiche-Form durch Kurier oder per Post an die speichernde Stelle übermittelt.

Im Berichtszeitraum wurde die Kontrolle der technischen und organisatorischen Maßnahmen bei Landratsämtern auch auf die Verarbeitung manuell geführter Karteien ausgedehnt.

Die festgestellten Mängel der Datensicherung bezogen sich auf

- den Ablauf der automatisierten Datenverarbeitung,
- den Zugang zu den Diensträumen,
- die Aufbewahrung von manuell geführten Karteien,
- die Postverteilung.

Bezüglich der Organisation der Datenverarbeitung habe ich gefordert:

- Werden als Datenträger für die Datenerfassung Disketten oder Magnetkassetten benützt, ist darauf zu achten, daß bespielte Datenträger grundsätzlich unter Verschluß gehalten werden, sofern sie nicht gerade für die Erfassung und Übertragung an die AKDB benützt werden. Das Bedienerhandbuch ist nach Dienstschluß ebenfalls verschlossen aufzubewahren. Nach der Datenerfassung sind Belege mit sensiblen Daten in verschlossenen Mappen durch die Datenerfassungskräfte in die Postverteilerstelle zu bringen oder direkt bei der Fachabteilung abzugeben.

  Dieses Verfahren empfiehlt sich auch bei Erfassungsarbeiten, die im Auftrag für kreisangehörige Gemeinden und andere öffentliche Stellen durchgeführt werden.

Häufig treten auch Probleme bei der Postverteilung auf. Wird die eingehende Post durch das Personal der Postverteilerstelle geöffnet und in die Fächer der einzelnen Sachgebiete gelegt, so ist durch geeignete Maßnahmen sicherzustellen, daß von Unterlagen mit sensiblen personenbezogenen Daten ausschließlich Befugte Kenntnis nehmen können. Bei der auslaufenden Post empfehle ich, grundsätzlich Dokumente mit sensiblen personenbezogenen Daten bereits durch die Fachreferate verschlossen an die Postverteilerstelle geben zu lassen.

3.11.4 Prüfungen im medizinischen Bereich

Im medizinischen Bereich wurden neben einem Großrechenzentrum und der Patientenverwaltung eines großen Krankenhauses, die automatisierte Verfahren anwendet, auch eine Anzahl von Kliniken überprüft, die Patientendaten lediglich manuell bearbeiten.

Die Prüfungen zeigten, daß bei den automatisierten Verfahren die im Rechenzentrum gespeicherten Patientendaten gegen den Zugriff Unbefugter am sichersten sind. Ich habe dort noch die Installation einer automatischen Zugangssicherung und die Einführung einer maschinell geführten Datenträgerverwaltung angeregt. Darüber hinaus habe ich eine physische Zuordnung bestimmter Datensichtstationen zu bestimmten Aufgabenbereichen (siehe Textziffer 3.12.2) gefordert.

Bei der Kontrolle einer Klinik in Nordbayern wurde festgestellt, daß aus Sparsamkeit die Rückseite von nicht benötigten Karteikarten-Duplikaten als Notizpapier verwendet wurde, obwohl die Vorderseite aktuelle Patientendaten enthielt. Ich habe diese Praxis, die sich offenbar nur aus Gedankenlosigkeit entwikkelt hatte, beanstandet. Die Notizblöcke wurden eingezogen und vernichtet. Weitere Mängel fand ich bei der Zugangssicherung und bei der Aufbewahrung von Patientendaten. Schließlich habe ich Anregungen für eine datenschutzgerechte „Abgangskontrolle" manuell geführter Krankengeschichten gegeben.

Ein bedeutendes medizinisches Projekt, in dem eine Vielzahl von sensiblen Patientendaten gespeichert und verarbeitet werden, wurde außer Haus bei einer anderen Stelle im Auftrag abgewickelt. Um die Datensicherungsmaßnahmen besser beurteilen zu können, forderte ich vom Auftraggeber die Dokumentation des Verfahrens an. Zu meinem Erstaunen bestand diese lediglich aus stichpunktartigen Angaben zum technischen und organisatorischen Konzept des Verfahrens, die für ein Gutachten über die Wirksamkeit der technischen und organisatorischen Datensicherungsmaßnahmen nicht ausreichend waren. Ich habe schließlich gefordert, dieses Verfahren möglichst bald auf einen klinikeigenen Rechner zu übernehmen.

### 3.11.5 Sonstige Prüfungen

Die Prüfungen bei einer Landesversicherungsanstalt (LVA) und bei gesetzlichen Krankenkassen zeigten erfreulicherweise, daß dort bereits eine Reihe von wirksamen Datensicherungsmaßnahmen realisiert waren. Der Gesamteindruck der bei der LVA durchgeführten technischen und organisatorischen Maßnahmen des Datenschutzes war positiv, im unmittelbaren Bereich des Rechenzentrums sogar mustergültig. Ein äußerst positives Bild ergab die Prüfung bei der Allgemeinen Ortskrankenkasse Lindau. Dort hatte u.a. die Innenrevision selbständig eine Schwachstellenanalyse der Datensicherungsmaßnahmen erstellt, deren Ergebnisse dann ins Konzept der technischen und organisatorischen Maßnahmen des Datenschutzes einflossen. Auch die Kontrolle bei einer staatlichen Kurverwaltung gab lediglich Anlaß zu Verbesserungsvorschlägen für Datensicherungsmaßnahmen, nicht aber zu Beanstandungen.

## 3.12 Technische Einzelprobleme

### 3.12.1 Datenschutzgerechte Vernichtung von ausgesonderten Unterlagen mit personenbezogenen Daten

Eine Panne, die bei der Vernichtung von Krebsvorsorgebefunden aufgetreten war, gibt Anlaß, an grundsätzliche Forderungen zu Datensicherungsmaßnahmen bei der Verarbeitung und Speicherung von personenbezogenen Daten in manuell geführten Dateien zu erinnern. Personenbezogene Daten dieser Sensibilität sind grundsätzlich so zu sichern, daß sie von Unbefugten weder zur Kenntnis genommen, noch verändert oder gelöscht werden können. Als technische Sicherungsmaßnahme bei der Aufbewahrung empfiehlt sich die Lagerung in einem Stahlschrank mit Sicherheitsschloß. Bei der Vernichtung solcher Unterlagen ist darauf zu achten, daß sie schnell und zuverlässig vernichtet werden und nicht in die Hände Unbefugter fallen können.

Problematisch erscheint es, Unterlagen dieser Sensibilität durch einen Dritten vernichten zu lassen. Wenigstens ist für solche Fälle mit dem Auftragnehmer bei Zuwiderhandlung eine Vertragsstrafe (vergl. Nr. 3.6 der Vollzugsbekanntmachungen zum Bayer. Datenschutzgesetz) zu vereinbaren. Nach Möglichkeit sollte aber ein Mitarbeiter der auftraggebenden Behörde bei der Vernichtung der Unterlagen anwesend sein. Der Auftragnehmer hat im übrigen die Möglichkeit, sich für den Schadensfall bei darauf spezialisierten Unternehmen zu versichern.

Die Vernichtung solcher Unterlagen unmittelbar durch den Sachbearbeiter selbst wird dem Datenschutz am besten gerecht. Für solche Fälle ist die Anschaffung eines Papierzerkleinerungsapparats zu empfehlen.

### 3.12.2 Auskunftssystem Kommunales Finanzwesen der AKDB

Die Anstalt für Kommunale Datenverarbeitung in Bayern legte mir im Berichtszeitraum das Konzept für den Datenschutz im „Auskunftssystem Kommunales Finanzwesen" zur Stellungnahme vor.

Das Auskunftssystem im Finanzwesen soll den Stellen, die über Wähl- bzw. Standleitungen an einen Großrechner der AKDB angeschlossen sind, die direkte Abfrage über Datensichtstation auf ihren zentral gespeicherten Datenbestand ermöglichen. Pro Abgaben- bzw. Steuerart ist im zentralen Rechner ein gemeinsamer Datenbestand für alle Benutzer angelegt. Damit jeweils nur die berechtigten Stellen auf die Datensätze zugreifen können, die sie für ihre Aufgabenerledigung benötigen, ist eine differenzierte Zugriffsschutzautomatik erforderlich, die die logischen Datenbestände innerhalb einer physischen Datei voneinander abschottet.

Durch eine feste Zuordnung der angeschlossenen Datenstationen vom zentralen Rechner aus wird erreicht, daß nur derjenige Dateiausschnitt zur Verfügung gestellt wird, der in den Zuständigkeitsbereich der jeweiligen Stelle fällt. Darüber hinaus existieren Benutzerkennungen, über die eine zusätzliche Zugriffskontrolle innerhalb der speichernden Stelle erreicht werden kann.

Dieses Konzept erfüllt hinsichtlich der Zugriffssicherung die Erfordernisse des Datenschutzes. Eine Abfrage von einer behördenfremden Datenstation aus ist nicht möglich. Bei Betrieb von Direktauskunftverfahren halte ich diese Methode der Zugriffssicherung für unbedingt erforderlich. Schließlich sollte die Tastatur der eingesetzten Datensichtstationen abschließbar sein.

Die Anstalt für Kommunale Datenverarbeitung in Bayern sagte mir die Prüfung folgender Anregungen zu:

- Dezentrale Protokollierung unberechtigter Zugriffsversuche bei Einsatz von Mehrplatzsystemen,

- bei Anschluß über Standleitungen selbständiges Inaktivieren des Bildschirmprogrammes bei längeren Pausen.

3.12.3 Datensicherung bei Umbauarbeiten

Umbauarbeiten in Rechenzentren dürfen nicht dazu führen, daß Datensicherungsmaßnahmen ausgeschaltet werden. In einem Fall wurde bekannt, daß während der Umbauarbeiten Gegenstände aus dem Rechenzentrum entwendet worden waren, die zwar nicht unter das Datenschutzgesetz fielen, daß es aber ohne größere Schwierigkeiten auch möglich gewesen wäre, an Unterlagen mit personenbezogenen Daten heranzukommen.

3.12.4 Transport von maschinell lesbaren Datenträgern

Bei den Kontrollen der technischen und organisatorischen Maßnahmen zur Datensicherung hat sich gezeigt, daß die meisten Stellen, die maschinell lesbare Datenträger an andere Stellen versenden, für die ordnungsgemäße Abwicklung des Versands bestimmte Regelungen getroffen haben. Da auf maschinell lesbaren Datenträgern, wie Magnetband, Kassette oder Diskette, beträchtliche Informationsmengen gespeichert werden können, erscheint dieses Problem wichtig genug, um an dieser Stelle an Hand praktischer Fälle behandelt zu werden.

Ein maschinell lesbarer Datenträger kann eine komplette Datei beinhalten. Es ist denkbar, daß im Zuge der Erstellung einer Stammdatei Erstdatenbestände auf Kassette oder Diskette im Zuge der Auftragsdatenverarbeitung auf dem Postwege versandt werden. Ähnlich verhält es sich bei Druckdatenbeständen, die zur Mikroverfilmung gehen. Hier ist besondere Vorsicht geboten, da es sich um Dateien handelt, die in der Regel so aufgezeichnet sind, daß auch Außenstehende ohne Kenntnis des Satzaufbaues die gespeicherten Daten einer bestimmbaren Person zuordnen können, meist sind die Feldinhalte noch mit erläuterndem Text versehen.

Anders zu beurteilen sind Fälle, in denen Bewegungsdaten auf maschinell lesbaren Datenträgern versandt werden. Die Veränderungen werden meist mit einem Zuordnungsmerkmal, das nur der speichernden und verarbeitenden Stelle bekannt ist und in der Regel in verschlüsselter Form auf dem maschinell lesbaren Datenträger aufgezeichnet. Wenn keine Neuzugänge für die Stammdatei enthalten sind, ist der Versand einer solchen Datei aus der Sicht des Datenschutzes unproblematisch, da Außenstehende diese Fragmente in aller Regel nicht entschlüsseln, zumindest jedoch nicht ohne weiteres bestimmten Personen zuordnen können.

Beim Transport von Datenträgern mit personenbezogenen Daten ist folglich stets zu prüfen, inwieweit Außenstehende aufgezeichnete Daten nutzen oder mißbrauchen könnten. Die vom staatlichen Koordinierungsausschuß Datenverarbeitung herausgegebenen Orientierungshilfen für Datensicherungsmaßnahmen in Großrechenzentren (Datensicherungskatalog) enthalten für die Transportkontrolle je nach Sensibilität der Daten abgestufte Sicherungsmaßnahmen.

Ein weiteres Problem ist die Übermittlung von Restdaten auf maschinell lesbaren Datenträgern. Werden Magnetbänder, Disketten oder Kassetten für den Datenaustausch verwendet, ist nicht auszuschließen, daß im Anschluß an das Dateiende der zur Übermittlung bestimmten Daten noch Altdaten einer früheren Datei gespeichert sind. Um sicherzugehen, daß keine personenbezogenen Daten unbefugt offenbart werden, sollte deshalb grundsätzlich der Speicherbereich hinter der Dateiendemarke bis zum Bandende gelöscht werden.

3.12.5 Datensicherung und Fernwartung von Datenverarbeitungssystemen

Datenfernverarbeitung und Online-Verfahren werden häufig mit Skepsis betrachtet, da befürchtet wird, über technische Einrichtungen sei leichter an Daten heranzukommen als über herkömmliche, überschaubare, manuell unterstützte Verfahren. Bei genauerer Betrachtung zeigt sich jedoch, daß maschinelle Sicherungen im allgemeinen zuverlässiger und vor allem unbestechlicher arbeiten. Die unbefugte Manipulierung der technischen Systeme erscheint allerdings wegen der Kompliziertheit der Verfahren weniger kontrollierbar.

Die Hersteller von DV-Anlagen gehen immer häufiger dazu über, Kundensysteme über Datenfernverarbeitung von der Wartungsdienstzentrale aus zu betreuen. Diese Methode heißt Fernwartung.

Der Fernwartung liegt die Idee zugrunde, dezentral gesammelte Erfahrungen zentral zu sammeln und allgemein verfügbar zu machen. Die Vorteile der Fernwartung liegen hauptsächlich in der Leistungssteigerung durch schnelleres Reagieren auf Fehlerzustände, in der vorbeugenden Systemüberwachung und in der Senkung der Wartungskosten.

Fernwartung kann sich sowohl auf die Hardware als auch auf die Software beziehen. Bei Fernwartung der Hardware werden sogenannte Systemstatusinformationen, die vom System in eigenen Dateien abgespeichert werden, regelmäßig abgefragt. Diese Informationen bestehen in erster Linie aus Gerätedaten, also nicht personenbezogenen Daten. Enthalten diese Informationen Anwenderdaten, so sind diese so fragmentarisch, daß ein konkreter Personenbezug nahezu ausgeschlossen ist. Bei der Wartung peripherer Geräte ist ein Montieren eines Kundendatenträgers für die Fehlersuche in der Regel nicht notwendig. Viele Geräte besitzen bereits eigene Speichermedien, z. B. Disketten, für die Aufnahme dieser Informationen.

Die Häufigkeit der Fernwartung gegenüber herkömmlicher Wartung vor Ort verdeutlichen Vergleichszahlen (IBM):

| | |
|---|---|
| Fehleranalyse vor Ort | 96% |
| Fehleranalyse durch Fernwartung | 4% |

Besondere Aufmerksamkeit aus der Sicht des Datenschutzes ist der Fernwartung der Software zu widmen. Obwohl auch hier keine Kundenprogramme ge-

wartet werden, können Anwenderdaten in Form von Dateiausschnitten (Puffer) und Paßworttabellen in ferngewarteten Basissoftware-Systemen enthalten sein. Hier muß vom Anwender dafür Vorsorge getroffen werden, daß lediglich solche Daten der Wartung zur Verfügung stehen, deren Weitergabe datenschutzrechtlich unbedenklich ist. Die Hersteller haben eine Reihe von Hilfen zur Verfügung gestellt, die den Anforderungen des Datenschutzes standhalten können.

Von der Fernwartung der Software wird in der Praxis noch weniger Gebrauch gemacht. Die Vergleichszahlen der IBM lauten:

| | |
|---|---|
| Fehleranalyse vor Ort | 99,9% |
| Fehleranalyse durch Fernwartung | 0,1% |

Bei Einsatz der Fernwartung ist auf die Einhaltung folgender Regeln zu achten:

1. Das Betriebssystem muß einen Paßwortschutz bieten.
2. Der Anwender definiert Art und Umfang der Fernwartung, sowohl auf Hard- als auch auf Software bezogen.
3. Der Service-Zentrale ist nur Zugriff auf solche Dateien zu gestatten, die vom Rechenzentrum bzw. Anwender unter dem Paßwort der Wartung eingerichtet wurden.
4. Die Verbindung zur Service-Zentrale kann einzig und allein vom Rechenzentrum aufgebaut werden.
5. Das Rechenzentrum muß alle Datenübertragungen an die Service-Zentrale mitverfolgen. Außerdem werden alle Dienste und Datenübertragungen auf maschinell auswertbaren Datenträgern protokolliert. Auswerteprogramme für die Protokolldateien sind vom Hersteller zur Verfügung zu stellen.
6. Das Rechenzentrum muß die Möglichkeit besitzen, den Dialog von Service-Zentrale und Rechner jederzeit zu unterbrechen.

Zusammengefaßt läßt sich daher sagen:

Bei Fernwartung wird durch die vorbeugende Wartung die technische Sicherheit nicht vermindert, sondern erhöht. Bei Fernwartung der Hardware bleiben die Programmbibliotheken und Daten der Anwender unberührt. Bei Fernwartung der Software ist darauf zu achten, daß auf solche Dateien und Programmbibliotheken des Anwenders, die er nicht zur Verfügung stellen will, nicht zugegriffen werden kann.

3.12.6 Leitsätze für Datensicherungsmaßnahmen

Der Hessische Landesautomationsausschuß und der Kommunale Automationsausschuß in Hessen haben für die automatisierte Datenverarbeitung im öffentlichen Bereich sogenannte Datenverarbeitungsleitsätze (DVL) erlassen. Diese Datenverarbeitungsleitsätze enthalten in der „Checkliste zur Konkretisierung der Datenschutzanforderungen" auch Datenschutzmaßnahmen.

Aus dem bayerischen kommunalen Bereich bin ich um Stellungnahme gebeten worden, ob eine derartige Vorgehensweise nicht auch für Bayern den Vorteil brächte, gewisse Standards für technische Maßnahmen zur Sicherstellung des Datenschutzes zu definieren. Ich bin jedoch der Ansicht, daß die Voraussetzungen in Bayern grundsätzlich anders liegen als in Hessen und daher auch anders zu beurteilen sind. Im öffentlichen Bereich ist in Hessen die Abwicklung automatisierter Verfahren auf die Rechenzentren des Hessischen DV-Verbundes (HZD und 5 KGRZ) konzentriert.

Im staatlichen Bereich des Freistaates Bayern wurden vom Koordinierungsausschuß Datenverarbeitung Orientierungshilfen für Datensicherungsmaßnahmen in Großrechenzentren herausgegeben (Datensicherungskatalog). Außerdem wurden im staatlichen Bereich die Richtlinien für die Durchführung von Projekten der automatischen Datenverarbeitung (ADV-Projektrichtlinien) eingeführt. Wegen der unterschiedlichen Organisation und Struktur der datenverarbeitenden Stellen und Rechenzentren scheint mir der Versuch wenig sinnvoll, allgemein verwendbare Datensicherungsstandards zu definieren. Diese Problematik kompliziert sich noch zunehmend durch die Weiterentwicklung der Technik. Schließlich würde die Definition von technischen Standards wohl ein zu starres Instrumentarium schaffen, das den datenverarbeitenden Stellen bei der Auswahl der Datensicherungsmaßnahmen keinen Spielraum mehr ließe. Häufig wäre auch schwierig zu beurteilen, ob dem Grundsatz der Angemessenheit von Maßnahmen Rechnung getragen ist.

Die Erfahrung zeigte, daß das Bayer. Landesamt für Datenverarbeitung und die Anstalt für Kommunale Datenverarbeitung in Bayern, die für öffentliche Stellen bei der maschinellen Abwicklung von Verwaltungsaufgaben im Auftrag tätig werden, in ihren internen Organisationsrichtlinien wirksame und ausreichende Datensicherungsmaßnahmen vorgeschrieben haben.

3.12.7 Speicherung auf Mikrofiche

In den bayerischen Vollzugsbekanntmachungen zum Bundesdatenschutzgesetz vom 30. Januar 1979 ist unter Nr. III Nr. 2.2 festgestellt, daß sich eine Datei auch aus Mikrofiches zusammensetzen kann. Die Kontrolltätigkeit zeigte, daß Mikrofiche-Sammlungen häufig anstelle von Karteikartensammlungen oder Listen geführt werden. Die Mikrofiche-Sammlungen besitzen im allgemeinen einen sog. Index-Fiche, der Hinweise für das Auffinden bestimmter Fälle enthält. Auf Mikrofiche-Sammlungen ist daher grundsätzlich das BayDSG anwendbar.

## 4. Datenschutz beim Bayerischen Rundfunk

Wie bereits in früheren Tätigkeitsberichten dargelegt, ist in Art. 21 des Bayerischen Datenschutzgesetzes das Datenschutzrecht für den Bayerischen Rundfunk gesondert geregelt. Danach ist für die Kontrolle der Einhaltung des Bayerischen Datenschutzgesetzes und anderer Vorschriften über den Datenschutz bei der gesamten Tätigkeit des Bayerischen Rundfunks ausschließlich der Datenschutzbeauftragte des Bayerischen Rundfunks zuständig. Nach Art. 21 Abs. 3

Satz 5 BayDSG hat dieser den Organen des Bayerischen Rundfunks jährlich einen Bericht über seine Tätigkeit zu erstatten und diesen dem Landesbeauftragten für den Datenschutz zu übermitteln. Dieser Verpflichtung ist er mit der Vorlage seines dritten Tätigkeitberichts für den Zeitraum vom 1. Januar bis 31. Dezember 1981 nachgekommen.

Folgende Schwerpunkte lassen sich diesem dritten Tätigkeitsbericht entnehmen:

Der Datenschutzbeauftragte berichtet, daß beim Bayerischen Rundfunk 18 automatisierte Dateien und 46 manuelle Dateien bzw. Karteien mit personenbezogenen Daten geführt werden. In diesen Dateien sind 180 verschiedene Personaldatenelemente gespeichert, wobei sehr häufig die gleichen Daten in den verschiedenen Dateien auftauchen. Der Datenschutzbeauftragte ist der Ansicht, daß seines Erachtens sowohl aus betriebswirtschaftlichen als auch aus datenschutzrechtlichen Gründen die Auswertung des Datenschutzregisters zu dem Ergebnis führe, daß die Einführung eines Personaldatensystems beim Bayerischen Rundfunk als erforderlich erscheine. Gerade aus datenschutzrechtlichen Gründen sei es für den einzelnen Mitarbeiter auf Dauer problematisch, wenn eine solche Vielzahl unterschiedlicher Daten in so zahlreichen Dateien geführt werde. Es sei offensichtlich, daß insoweit eine Kontrolle der verschiedenen Dateien hinsichtlich Datenschutz und Datensicherung schon aus Gründen der großen Zahl Probleme mit sich bringe. Insbesondere werde deutlich, daß die Veränderung einzelner Daten, z.B. der Anschrift, zu einem umfangreichen Änderungsdienst zwinge, der gleichzeitig 15 bis 20 Dateien betreffe. Hierzu sei eine Vielzahl von Personal und ein großer Kontrollaufwand notwendig. Ein Personaldatensystem böte demgegenüber den Vorteil, daß alle zum einzelnen Mitarbeiter gespeicherten Daten an einer Stelle zusammengeführt würden und Änderungen nur einmal von einer Person für alle durchgeführt werden könnten.

Der Datenschutzbeauftragte des Bayerischen Rundfunks hat die Hintergründe der Presseveröffentlichung von Auszügen aus dem Prüfungsbericht des Bayerischen Rechnungshofs, die Frage der Telefondatenerfassung bei Mitarbeitern, das bei der Befreiung von der Rundfunkgebührenpflicht geübte Verfahren sowie die Vorgehensweise bei der Ermittlung noch nicht gemeldeter Rundfunkteilnehmer einer ausführlichen datenschutzrechtlichen Bewertung unterzogen. Hinsichtlich einer von ihm für erforderlich gehaltenen Überprüfung der Datensicherheit im Rechenzentrum des Bayerischen Rundfunks regt er die Beiziehung eines unabhängigen Gutachters an. Diese Art der Überprüfung sei auch bei anderen Rundfunkanstalten bereits mit Erfolg praktiziert worden.

Der Datenschutzbeauftragte des Bayerischen Rundfunks stellt fest, daß er wiederum in einer Reihe von Einzelfällen entweder auf Anregung einzelner Mitarbeiter, einzelner Abteilungen des Bayerischen Rundfunks oder von Amts wegen tätig geworden sei und hierbei ein Grund zur formellen Beanstandung nicht habe festgestellt werden können. Seine entsprechenden Hinweise hätten bei den zuständigen Stellen Beachtung gefunden. Im übrigen habe es sich auch im Berichtszeitraum als ausreichend erwiesen, für die Zukunft Maßnahmen zur Verbesserung des Datenschutzes zu empfehlen. Themen dieser Tätigkeit seien insbesondere gewesen:

- die Vernichtung von Altpapier und Akten beim Bayerischen Rundfunk,
- die Übermittlung von Gehaltsdaten leitender Mitarbeiter an die Kommission zur Ermittlung des Finanzbedarfs der Rundfunkanstalten (KEF),
- die Einhaltung des Datenschutzes bei der Abgabe von Drittschuldnererklärung durch den Bayerischen Rundfunk,
- Fragebogenaktionen durch verschiedene Institutionen bei den Mitarbeitern des Bayerischen Rundfunks,
- die Verpflichtung auf das Datengeheimnis bei den Beauftragten des Bayerischen Rundfunks,
- die Entfernung ärztlicher Gutachten aus den Personalakten und ihre Ablage in den Patientenakten des Betriebsarztes.

Unter der Überschrift „Datenschutz bei der GEZ" weist der Datenschutzbeauftragte des Bayerischen Rundfunks darauf hin, daß der Datenschutz bei der GEZ nach wie vor ein Schwerpunkt der Tätigkeit der Rundfunk-Datenschutzbeauftragten sei. Der Arbeitskreis Datenschutzbeauftragte habe deshalb auch im Berichtszeitraum dafür gesorgt, daß die GEZ weiterhin an der Vervollkommnung ihrer technischen und organisatorischen Vorkehrungen arbeite, um so den Datenschutz ständig zu verbessern. Die von den Landesrundfunkanstalten und dem ZDF getragene GEZ hatte zum 31. Dezember 1981 einen Bestand von 23748247 Hörfunkteilnehmern und 21490547 Fernsehteilnehmern zu verwalten. Dabei führe die GEZ 4001281 gebührenpflichtige und 261909 gebührenbefreite Hörfunkteilnehmer des Bayerischen Rundfunks. Bei den Fernsehteilnehmern des Bayerischen Rundfunks waren 3620451 Teilnehmer gebührenpflichtig und 199912 gebührenbefreit. Im Bereich des Bayerischen Rundfunks ergingen 138868 Gebührenbescheide. Gegen säumige Rundfunkgebührenzahler wurden 9895 Vollstreckungen eingeleitet und gegen Schwarzseher und -hörer wurden 1803 Anträge auf Verfolgung als Ordnungswidrigkeit gestellt. Die GEZ bearbeitet und beantwortet einfache Anfragen und sonstige Routineschriftwechsel in Datenschutzangelegenheiten selbständig. Geschäftsvorfälle mit grundsätzlichem Charakter und Anfragen schwierigerer Art gibt sie jedoch an den Datenschutzbeauftragten der jeweils zuständigen Landesrundfunkanstalt weiter.

In seiner Zusammenfassung weist der Rundfunkbeauftragte des Bayerischen Rundfunks darauf hin, daß sich die Anzahl der Auskunftsersuchen und der sonstigen Reaktionen von Rundfunkteilnehmern und Dritten zu Fragen des Datenschutzes im Jahre 1981

im Vergleich zum Vorjahr bei der GEZ etwas erhöht habe. Die Gründe für diesen Anstieg sieht er in dem zunehmenden Datenschutzbewußtsein der Bevölkerung.

Eine Lücke im Datenschutz sieht der Datenschutzbeauftragte des Bayerischen Rundfunks in der auf Dateien begrenzten Geltung der Datenschutzgesetze. Diese Beschränkung auf Dateien sei bei den Betroffenen weithin auf Unverständnis gestoßen. Insbesondere werde seines Erachtens nicht verstanden, warum die Übermittlung aus Akten und anderen Aufzeichnungen an Dritte nicht von den Datenschutzgesetzen geregelt werde und der Betroffene insoweit keinen Auskunftsanspruch habe. Der Flucht in die Akte seien damit Tür und Tor geöffnet.

**Anhang 1**

## Vorschlag zur Neufassung von Vorschriften der Datenschutzgesetze über On-line-Anschlüsse

A. Die Datenschutzbeauftragten des Bundes und der Länder schlagen vor, zur Regelung der Zulässigkeit von automatisierten Abrufverfahren (On-line-Verfahren) im öffentlichen Bereich das Bundesdatenschutzgesetz wie folgt zu ändern:

1. § 2 Abs. 2 Nr. 2 wird wie folgt neu gefaßt:

   2. Übermitteln (Übermittlung) das Bekanntgeben gespeicherter oder durch Datenverarbeitung unmittelbar gewonnener Daten an einen Dritten in der Weise, daß die Daten durch die speichernde Stelle an den Dritten weitergegeben werden oder daß der Dritte zum Abruf oder zur Einsicht bereitgehaltene Daten abruft oder einsieht,

2. Nach § 11 ist folgender § 11 a einzufügen:

   § 11 a Automatisiertes Abrufverfahren

   (1) Die Einrichtung eines automatisierten Verfahrens, das den Abruf personenbezogener Daten durch Dritte ermöglicht, ist nur zulässig, soweit

   1. die zum Abruf bereitgehaltenen Daten ihrer Art nach für den Empfänger erforderlich sind,
   2. das Bereithalten der Daten zum sofortigen Abruf durch den Empfänger unter Berücksichtigung der schutzwürdigen Belange der Betroffenen und der Aufgaben der beteiligten Stellen angemessen ist und
   3. die Voraussetzungen des Abs. 2 erfüllt sind.

   Personenbezogene Daten, die einem Berufs- oder besonderen Amtsgeheimnis (§ 45, S. 2 Nr. 1, S. 3) unterliegen, dürfen nicht in ein automatisiertes Abrufverfahren aufgenommen werden.

   (2) Die zuständigen obersten Bundesbehörden legen den Anlaß und den Zweck der Übermittlung, die Datenempfänger, die zu übermittelnden Daten und die nach § 6 des Gesetzes erforderlichen technischen und organisatorischen Maßnahmen fest. Insbesondere muß gewährleistet sein, daß die Zulässigkeit des Abrufs im Einzelfall kontrolliert werden kann. Für automatisierte Abrufverfahren unter Beteiligung von Sicherheitsbehörden bedarf es darüber hinaus einer ausdrücklichen gesetzlichen Zulassung. Dies gilt nicht für den Anschluß von Sicherheitsbehörden an Datenbestände, die jedermann zur Benutzung offenstehen. Die Rechtsvorschriften über den Datenaustausch zwischen Verfassungsschutzbehörden nach dem BVerfG und zwischen Polizeibehörden nach dem BKAG bleiben unberührt.

   (3) Der Bundesbeauftragte für den Datenschutz ist über die geplante Einrichtung oder Änderung eines automatisierten Abrufverfahrens zur Übermittlung rechtzeitig zu unterrichten.

3. Nach § 11 a ist folgender § 11 b einzufügen:

   § 11 b Rechtsverordnung zum Datenschutz

   Die Bundesregierung kann durch Rechtsverordnung für bestimmte Sachgebiete im Rahmen einer an sich zulässigen Datenverarbeitung die Voraussetzungen näher regeln, unter denen personenbezogene Daten erhoben, verarbeitet oder sonst genutzt werden dürfen. Sie muß insbesondere die schutzwürdigen Belange der Betroffenen, berechtigte Interessen Dritter und Aufgaben der öffentlichen Verwaltung gegeneinander abwägen. In der Rechtsverordnung sind die für die Übermittlung zugelassenen Daten, ihre Empfänger, der Zweck sowie das Verfahren der Übermittlung festzulegen.

B. 1. Soweit durch die vorgeschlagene Fassung von § 2 Abs. 2 Nr. 2 BDSG der Übermittlungsbegriff auch für den nicht-öffentlichen Bereich geändert wird, halten die Datenschutzbeauftragten es für erforderlich, daß auch in dem Dritten und Vierten Abschnitt des Bundesdatenschutzgesetzes eine Regelung aufgenommen wird, die den sachlichen Anforderungen des vorgeschlagenen § 11 a Rechnung trägt.

2. Im Hinblick auf den vorgeschlagenen § 11 a Abs. 2 gehen die Datenschutzbeauftragten davon aus, daß in Anlehnung an die Regelung in sieben Bundesländern in das Bundesdatenschutzgesetz für Übermittlungen in den nicht-öffentlichen Bereich eine Vorschrift aufgenommen wird, nach der der Empfänger die übermittelten Daten nur für den Zweck verwenden darf, zu dessen Erfüllung sie ihm übermittelt wurden.

**Anhang 2**

Stand: 2. Oktober 1981

## Mindestanforderungen für den Datenschutz bei den Zentralen Namenskarteien der Staatsanwaltschaften

### Bestandsaufnahme

Die Staatsanwaltschaften führen zentrale Namenskarteien. Diese sind Hilfsmittel der Aktenführung für die bei den Staatsanwaltschaften aufbewahrten Akten. Der Umfang der in den zentralen Namenskarteien niedergelegten Daten, der Zeitraum ihrer Aufbewahrung und der Zugriff auf sie ist in den einzelnen Ländern und teilweise sogar innerhalb der Länder unterschiedlich geregelt. Bei einzelnen Staatsanwaltschaften sind die zentralen Namenskarteien automatisiert. Bei aller Unterschiedlichkeit ist den zentralen Namenskarteien gemeinsam, daß sie die Voraussetzung des Dateibegriffs im Sinne der Datenschutzgesetze erfüllen.

Wegen des in der Natur der Sache liegenden Bezugs zu Strafsachen zählen die in den zentralen Namenskarteien geführten Angaben zu den besonders sensiblen Daten, die die schutzwürdigen Belange der Betroffenen besonders nachhaltig berühren können. Dies gilt vor allem, wenn die Daten von Unschuldigen gespeichert sind, weil bereits der Ort der Speicherung einen belastenden Kontext vermittelt.

Die Datenschutzbeauftragten begrüßen ausdrücklich die zwischenzeitlich in einigen Ländern feststellbaren Bemühungen, diesen Gefährdungen zu begegnen und dem Datenschutz zur Geltung zu verhelfen. Erwähnenswert sind die Rundverfügung des Justizministers des Landes Nordrhein-Westfalen vom 8. Dezember 1980, wonach die Zentralnamenkartei ausschließlich der staatsanwaltschaftlichen Tätigkeit dient, und die technischen und organisatorischen Maßnahmen bei der Staatsanwaltschaft Nürnberg, die durch abgestufte Aussonderungsfristen die Berücksichtigung der individuellen Besonderheiten der einzelnen Betroffenen erlauben.

### Forderungen an datenschutzgerechte Führung der Namenskarteien

Wegen der bereits in der Speicherung in den zentralen Namenskarteien liegenden Gefährdung für die Betroffenen sind die Datenschutzbeauftragten der Ansicht, daß „die Einrichtung des Namensverzeichnisses noch stärker auf die Funktion des Hilfsmittels der Aktenführung ausgerichtet werden" sollte. Die Datenschutzbeauftragten begrüßen die insoweit gleichlautende Entschließung der ORGSTA in Bad Dürkheim anläßlich der Sitzung vom 15. bis 17. Oktober 1980. Auf dieser Grundlage geben die Datenschutzbeauftragten folgendes zu bedenken:

### Speicherung

Über die zur Identifizierung der im Namensverzeichnis geführten Person unbedingt erforderlichen Daten und das staatsanwaltschaftliche Aktenzeichen hinaus dürfen nur solche Daten gespeichert werden, die ebenfalls zur rechtmäßigen Aufgabenerfüllung erforderlich sind. Auch hierbei ist der Grundsatz der Verhältnismäßigkeit zu beachten. Die Speicherung des Namens des Anzeigenerstatters beispielsweise begegnet – von den UJs-Sachen abgesehen – erheblichen Bedenken. Wird der Tatvorwurf gespeichert, kann den schutzwürdigen Belangen des Betroffenen dadurch Rechnung getragen werden, daß die Auskunftserteilung aus der Kartei untersagt und die Kartei nicht als Entscheidungsgrundlage herangezogen wird. Andernfalls ist Sorge dafür zu tragen, daß die diesbezüglichen Eintragungen entsprechend einem geänderten Erkenntnisstand der Staatsanwaltschaft berichtigt werden. Wird ein Verfahren nach § 170 Abs. 2 StPO eingestellt oder erfolgt Freispruch, ist zu prüfen, inwieweit diese Tatsachen entweder ausdrücklich in den zentralen Namenskarteien vermerkt oder aber die entsprechenden Eintragungen gelöscht werden. Je belastender Eintragungen für den Betroffenen sind, desto mehr muß darauf geachtet werden, daß die Eintragungen richtig sind. Wird beispielsweise neben dem Tatvorwurf die Tatsache der Anklageerhebung niedergelegt, muß der Freispruch eingetragen werden. Dies gilt zumal dann, wenn die zentralen Namenskarteien nicht ausschließlich internen Zwecken der Staatsanwaltschaft dienen. Eine Speicherung von über den Akteninhalt hinausgehenden Daten dürfte, weil mit dem Zweck der zentralen Namenskartei nicht vereinbar, unzulässig sein. Damit verbietet sich auch die Verbindung automatisierter Namensdateien etwa mit polizeilichen Datenbanken zu einem gemeinsamen System.

### Übermittlung

Aus der Funktion der zentralen Namenskartei, als Hilfsmittel der Aktenführung zu dienen, ergibt sich bereits eine weitgehende Beschränkung der Übermittlung. Für die Beurteilung von Datenübermittlungen an Behörden gilt, daß den zentralen Namenskarteien nicht die Aufgabe eines Ersatzzentralregisters zukommen darf. Dies gilt auch für die Polizei, soweit sie nicht in einem konkreten Ermittlungsverfahren tätig ist. Soweit Behörden auf Grund der ihnen zugewiesenen Aufgaben einen Auskunftsanspruch gegenüber dem Bundeszentralregister haben, müssen sie diesen geltend machen. Einen Auskunftsanspruch aus der zentralen Namenskartei rechtfertigt jener nicht. Gleiches gilt, wenn Behörden ein Einsichtsrecht in bestimmte Strafakten haben. Eine unmittelbare Auskunft aus der zentralen Namenskartei ist – beschränkt auf das Aktenzeichen – nur den Behörden zu erteilen, die dieses Aktenzeichen benötigen, um zu einem anhängigen Strafverfahren weitere Unterlagen gezielt nachreichen zu können, oder dieses Aktenzeichen aus anderen Gründen zur rechtmäßigen Aufgabenerfüllung benötigen. Privaten Dritten ist ohne Einwilligung des Betroffenen keine Auskunft aus den zentralen Namenskarteien zu erteilen. Sie sind gegebenenfalls auf die Akteneinsicht zu verweisen.

Soweit Auszüge aus der zentralen Namenskartei zur Unterrichtung des sachbearbeitenden Staatsanwalts in die Strafakten eingelegt werden, sind diese Auszüge vor Weiterleitung an das Gericht oder an andere Behörden aus den Akten zu entfernen.

### Sperrung/Löschung

Die Frist, innerhalb der die zentralen Namenskarteien zur gewöhnlichen Sachbearbeitung zur Verfügung stehen, ist erheblich zu verkürzen. Begrüßenswerte Beispiele zeigen, daß eine Sperrung drei Jahre nach dem letzten Eintrag, spätestens nach sieben Jahren, einer ordnungsgemäßen Aufgabenerfüllung der Staatsanwaltschaft nicht generell entgegensteht. Eventuell sind für Sperrung und Löschung unter Berücksichtigung des Grundsatzes der Verhältnismäßigkeit zeitlich abgestufte Fristen entsprechend der Schwere der im Einzelfall zur Last gelegten Straftat und des weiteren strafrechtlich relevanten Verhaltens des einzelnen zu erwägen. Im übrigen kann die Tatsache einer Verfahrenseinstellung oder eines Freispruchs im Einzelfall die sofortige Löschung oder zumindest Sperrung der Daten des Betroffenen erforderlich machen, um beispielsweise schutzwürdige Belange Unschuldiger zu wahren.

**Entscheidungsgrundlage**

Die zentralen Namenskarteien können allenfalls ein mehr oder weniger unvollständiges Abbild der Strafakten sein. In dieser naturnotwendigen Verkürzung des Akteninhaltes liegt die Gefahr, daß aus den in der zentralen Namenskartei niedergelegten Daten falsche Schlüsse gezogen werden. Um derartige mögliche Belastungen für die Betroffenen zu vermeiden, dürfen die aus den zentralen Namenskarteien gewonnenen Informationen nicht Grundlage für Entscheidungen sein. Entscheidungen, jedenfalls solche zum Nachteil eines Betroffenen, sind auch künftig ausschließlich auf die Strafakten zu stützen, für deren Führung die zentralen Namenskarteien nur Hilfsmittel sein sollen.

**Technische und organisatorische Maßnahmen**

Die Ausgestaltung der zentralen Namenskarteien obliegt den Landesjustizverwaltungen. Es kann nicht Aufgabe der Datenschutzbeauftragten sein, nur eine einzige bestimmte Konzeption als mit dem Datenschutz vereinbar zu fordern. Ein umfangreicherer Datenbestand und eine wenn auch nur begrenzt zugelassene Übermittlung aus den Zentraldateien bedeuten höhere Gefährdungen für die schutzwürdigen Belange der Betroffenen. Ihnen muß durch entsprechend wirksamere technische und organisatorische Maßnahmen begegnet werden. Vorkehrungen gegen Auskünfte an Unbefugte, unbefugten Zugriff und unzulässige Datenermittlungen sind notwendig. Außerdem muß sichergestellt sein, daß Löschungen auf Karteikarten zur Unlesbarkeit der betroffenen Daten führen. Die Datenschutzbeauftragten begrüßen, daß auch in diesem Bereich in der staatsanwaltschaftlichen Praxis bereits ein Bemühen um den Datenschutz zu erkennen ist. Die erfreulichen Ansätze sind jedoch auf alle Staatsanwaltschaften auszudehnen.

Die Datenschutzbeauftragten fordern die Landesjustizverwaltungen daher auf, entsprechend der eingangs zitierten Entschließung der ORGSTA, die Einrichtung der zentralen Namensverzeichnisse noch stärker auf die Funktion des Hilfsmittels der Aktenführung auszurichten und auch bei deren Führung die Belange des Datenschutzes nachhaltig zu berücksichtigen. Sie bitten die Landesjustizverwaltungen um Unterrichtung über das auf diesem Gebiet bisher Veranlaßte sowie die vorgesehenen weiteren Maßnahmen.

Darüber hinaus müssen auch die in den Aufbewahrungsbestimmungen der Justizverwaltungen getroffenen Fristenregelungen für die Aufbewahrung von Strafakten deutlich verkürzt werden.

**Anhang 3**

## Rechtliche Grundlagen des Datenschutzes in Bayern

3.1 Vorschriften:

Für alle bayerischen Behörden gilt das Bayer. Datenschutzgesetz (BayDSG, BayGVBl 1978 S. 165), Ausnahme: Soweit sie am Wettbewerb teilnehmen (Art. 22 BayDSG) oder Sozialleistungsträger sind (§ 35 SGB I, § 79 SGB X).

Für Bundesbehörden gilt das Bundesdatenschutzgesetz, 2. Abschnitt (BDSG, Bundesgesetzblatt I S. 201).

Für die Privatwirtschaft gilt ebenfalls das Bundesdatenschutzgesetz, 3. bzw. 4. Abschnitt. Das BayDSG legt insoweit nur noch die zuständigen Aufsichtsbehörden fest.

Neben den Datenschutzgesetzen sind aber auch eine Vielzahl von Gesetzen zu beachten, die das Persönlichkeitsrecht bzw. einzelne Geheimnisse schützen. Als Beispiel seien § 35 des Sozialgesetzbuches I (Sozialgeheimnis), § 203 StGB (u.a. ärztliche Schweigepflicht), § 30 Abgabenordnung (Steuergeheimnis) und Art. 30 des Bayer. Verwaltungsverfahrensgesetzes (Amtsverschwiegenheit) genannt. Außerdem gibt es spezielle Datenschutzvorschriften, wie Art. 13 des Bayer. Krankenhausgesetzes vom 21. Juli 1974 über die Behandlung von Patientendaten (GVBl S. 256). 1980 sind als sog. bereichsspezifische Datenschutzbestimmungen das Gesetz zur Änderung des Gesetzes über Personalausweise vom 6. März 1980 (BGBl I S. 270), das Melderechtsrahmengesetz vom 16. August 1980 (BGBl I S. 1429) sowie das Zehnte Buch Sozialgesetzbuch – SGB X – vom 18. August 1980 (BGBl I S. 1469) erlassen worden. Voraussichtlich 1982 wird ein neues Landesmeldegesetz verabschiedet werden.

Spezielle Schutznormen gehen dem Bayerischen bzw. dem Bundesdatenschutzgesetz vor. BayDSG und BDSG sind Auffanggesetze, die einen Mindeststandard an Datenschutz gewährleisten.

Der Gesetzgeber ist davon ausgegangen, daß besonders empfindliche Bereiche durch spezielle Datenschutzregelungen angemessener geregelt werden können und müssen.

Für die Anwendung des BayDSG sind folgende Ausführungsbestimmungen erlassen worden:

- Die Bekanntmachung zum Vollzug des BayDSG vom 12. September 1978 (MABl S. 688 ff.); ergänzt durch Bekanntmachung vom 4. September 1979 (MABl S. 527 und KMBl I 1980 S. 39).
- Die Bekanntmachung zum Vollzug des BayDSG vom 4. September 1979 (MABl S. 527), durch die die Vollzugsbekanntmachung zum BDSG vom 30. Januar 1979 (MABl S. 22) über die Maßnahmen zur Datensicherung für entsprechend anwendbar erklärt wurde (siehe auch KMBl 1980 S. 39).
- Die Verordnung über das Datenschutzregister vom 23. November 1978 (Datenschutzregisterverordnung – DSRegV – GVBl S. 783). Sie legt den Inhalt des Datenschutzregisters fest, regelt die Einsicht in das Register, beschränkt die Meldepflicht der speichernden Stellen und bestimmt den Umfang der jährlichen Veröffentlichung aus dem Register.
- Die Kostenordnung für die Tätigkeit des Technischen Überwachungsvereins Bayern e.V. beim Vollzug der Datenschutzgesetze vom 16. August 1979 (Datenschutzkostenordnung – DSchKO –, GVBl S. 287). Nach Art. 32 BayDSG begutachtet der TÜV technische Fragen als Sachverständiger für die Aufsichtsbehörden über die Privatwirtschaft.
- Die Bekanntmachung des Bayer. Staatsministeriums des Innern vom 14. Juli 1978 zum Vollzug des Bayer. Melde-

gesetzes (MABl S. 553), geändert durch Bekanntmachung vom 11. September 1978 (MABl S. 650), über die Auswirkungen des Datenschutzrechts auf das Melderecht – insbesondere die Erteilung von Auskünften aus dem Melderegister (Änderung des Meldegesetzes und der Ausführungsvorschriften voraussichtlich im Laufe des Jahres 1982).

- Die Bekanntmachung des Bayer. Staatsministeriums für Unterricht und Kultus vom 23. November 1978 mit erläuternden Hinweisen zum Vollzug der Datenschutzregisterverordnung (KMBl I 21/78, S. 585).
- Die Bekanntmachung des Bayer. Staatsministeriums für Unterricht und Kultus vom 9. April 1979 mit erläuternden Hinweisen für die Schulen zum Vollzug des Bayerischen Datenschutzgesetzes (KMBl 9/79, S. 187).
- Die Allgemeine Verwaltungsvorschrift des Bayer. Staatsministeriums für Wirtschaft und Verkehr für die Behandlung von Anzeigen nach den §§ 14 und 55 c der Gewerbeordnung vom 2. Januar 1980 (WVMBl S. 1). Dort wird unter Nr. 6 die Anwendung des Datenschutzgesetzes auf die Sammlung der Gewerbeanzeigen – besonders die Erteilung von Auskünften über Gewerbetreibende – geregelt.
- Die Bekanntmachung des Bayer. Staatsministeriums für Arbeit und Sozialordnung zum Vollzug des § 139 b Abs. 1 Satz 3 der Gewerbeordnung (GewO) – Wahrung der Geheimhaltungspflicht bei Gewerbeaufsichtsämtern – vom 7. November 1980 (AMBl S. 262).
- Die Bekanntmachung vom 29. April 1980 zum Vollzug datenschutzrechtlicher Vorschriften im Geschäftsbereich des Bayer. Staatsministeriums für Ernährung, Landwirtschaft und Forsten (LMBl 7/80, S. 51).

Zum Vollzug des BDSG wird auf folgende Bestimmungen hingewiesen:

- Vollzugsbekanntmachung des Bayer. Staatsministeriums des Innern vom 12. Juli 1978 (MABl S. 451), geändert durch Bekanntmachung vom 27. März 1981 (MABl S. 150), zu wichtigen Anwendungsfragen.
- Vollzugsbekanntmachung des Bayer. Staatsministeriums des Innern vom 30. Januar 1979 MABl S. 22) über Maßnahmen zur Datensicherung.

3.2 Inhalt der Datenschutzgesetze:

Siehe hierzu Broschüre „Datenschutzrecht" mit dem Text des Bayer. und des Bundesdatenschutzgesetzes und der Datenschutzregisterverordnung. Im 1. und 2. Tätigkeitsbericht finden sich außerdem Ausführungen zum wesentlichen Inhalt der Datenschutzgesetze.

**Anhang 4**

## Anschriften der Datenschutz-Kontrolle

Die Einhaltung der Datenschutzvorschriften wird von folgenden Stellen kontrolliert, an die sich jedermann wenden kann.

**Öffentlicher Bereich (Behörden):**

1. Der Landesbeauftragte für den Datenschutz

   Dr. Konrad Stollreither
   Wagmüllerstr. 18/II, 8000 München 22,
   Tel. 089/2 37 03-341

   Kontrolle bei Bayer. Landesbehörden, wie z.B. Gemeinde oder Stadtverwaltung, Landratsamt, Finanzamt, Polizei, Allgemeine Ortskrankenkasse.

2. Der Bundesbeauftragte für den Datenschutz

   Prof. Dr. Hans-Peter Bull
   Stephan-Lochner-Str. 2, 5300 Bonn 2,
   Tel. 02 21/37 50 91–98

   Kontrolle des Datenschutzes bei Behörden des Bundes, wie z.B. Kreiswehrersatzamt, Arbeitsamt, Post.

**Nichtöffentlicher Bereich (Privatwirtschaft):**

Regional zuständige Aufsichtsbehörden:

Regierung von Oberbayern
Maximilianstr. 39
8000 München 22
(Tel. 089/2176-230 oder 388)

Regierung von Niederbayern
Regierungsplatz 50
8300 Landshut
(Tel. 0871/8221)

Regierung der Oberpfalz
Emmeransplatz 8/9
8400 Regensburg
(Tel. 0941/5641)

Regierung von Oberfranken
Ludwigstr. 20
8580 Bayreuth
(Tel. 0921/6041)

Regierung von Mittelfranken
Schloß
8800 Ansbach
(Tel. 0981/531)

Regierung von Unterfranken
Peterplatz 9
8700 Würzburg
(Tel. 0931/3801)

Regierung von Schwaben
Fronhof 10
8900 Augsburg
(Tel. 0821/31051)

Oberste Aufsichtsbehörde: Bayer. Staatsministerium des Innern
Odeonsplatz 3
8000 München 22
(Tel. 089/21921)

Kontrolle des Datenschutzes bei privaten Stellen in Bayern, wie z.B. Banken, Versicherungen, Firmen, Auskunfteien, Kreditschutzeinrichtungen

**Anhang 5**

## Stichwortverzeichnis

zum 4. Tätigkeitsbericht des
Bayerischen Landesbeauftragten für den Datenschutz

Hinweis: Ein Stichwortverzeichnis zu den ersten drei Tätigkeitsberichten findet sich im Anhang 6.

(römische Ziffer = Tätigkeitsbericht
arabische Ziffer = Seitennummer)

**Anhang 6**

## Stichwortverzeichnis

zum 1., 2. und 3. Tätigkeitsbericht des bayerischen Landesbeauftragten für den Datenschutz

(römische Ziffer = Tätigkeitsbericht
arabische Ziffer = Seitennummer)