**Bayerischer Landtag**
10. Wahlperiode

Drucksache **10/4383**
02.08.84

# Sechster Tätigkeitsbericht des Landesbeauftragten für den Datenschutz

Berichtszeitraum 01. Januar 1983 bis 31. Dezember 1983

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

München, den 2. August 1984

An den
Herrn Präsidenten
des Bayerischen Landtags
München

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

Sehr geehrter Herr Landtagspräsident!

In der Anlage übersende ich gemäß Art. 28 Abs. 4 des Bayerischen Gesetzes zum Schutz vor Mißbrauch personenbezogener Daten bei der Datenverarbeitung vom 28. April 1978 den sechsten Tätigkeitsbericht für den Zeitraum vom 1. Januar 1983 bis 31. Dezember 1983.

Der Beirat hat den Entwurf in seiner Sitzung am 17. Juli 1984 vorberaten.

Mit vorzüglicher Hochachtung

**Dr. Konrad Stollreither**

Inhaltsübersicht

**Anlage:**
Muster des Datenschutz-Informations-Faltblattes des Bayer. Landesbeauftragen für den Datenschutz (liegt nur einem Teil der Auflage bei)

## 1. Vorbemerkung

Der meinem Tätigkeitsbericht für das Jahr 1982 vorangestellte Überblick stand unter der Überschrift „Fünf Jahre Datenschutz in Bayern". Er stellte das Ende der Aufbauphase und bemerkenswerte Veränderungen auf dem Arbeitsfeld nicht nur des bayerischen Datenschutzes fest:

- die technische Entwicklung zu immer mehr mittleren und kleineren Rechnern neben den Großrechenanlagen
- die Testphase und Einführung neuer Medien.

Das Ende der Aufbauphase in vorangegangenen Jahren mußte für 1983 den Blick auf Richtpunkte für die Zukunft wenden. Die angesprochenen technischen Entwicklungen mußten in diese Überlegungen mit einbezogen werden.

Dies führte zu folgenden Gedanken:

1. Es ist Aufgabe des Datenschutzes, die nach Art. 2 Abs. 1 in Verbindung mit Art. 1 Abs. 1 GG gewährleistete Privatsphäre zu schützen. Dies ist durch die Entscheidung des Bundesverfassungsgerichts vom 15. Dezember 1983 zum Volkszählungsgesetz 1983 bestätigt worden, das aus diesen Verfassungsbestimmungen das Grundrecht auf informationelle Selbstbestimmung abgeleitet hat. Dieses Grundrecht erfaßt aber den Schutz der Persönlichkeit schlechthin. Die durch öffentliche Stellen von Bürgern erhobenen Daten bedürfen daher des Schutzes ohne Rücksicht darauf, ob diese Daten automatisiert gespeichert, auf Karteikarten vermerkt oder in Akten festgehalten sind. Aus diesem Grunde erscheint es überprüfungsbedürftig, wenn in den Datenschutzgesetzen nur auf die in Dateien – automatisierten wie herkömmlichen – enthaltenen Daten abgestellt wird. Da grundsätzlich kein datenschutzfreier Raum besteht, muß deshalb auch für die in Akten festgehaltenen Daten auf die tragenden Bestimmungen der Verfassung zum Schutz der Persönlichkeit zurückgegriffen werden.
   Dies entspricht der von mir schon bisher vertretenen Auffassung.

   Auch der Begriff „Datenschutz", von dem auch die Gesetze „zum Schutz vor Mißbrauch personenbezogener Daten bei der Datenverarbeitung" ausgehen, erweist sich nicht selten als wenig hilfreich. Er führt immer wieder zu der unzutreffenden Meinung, Sinn und Grenze meiner Aufgabe bestehe darin, bloße Daten zu schützen. Nicht deutlich genug bringt der Begriff „Datenschutz" zum Ausdruck, daß sein Sinn allein darin bestehen kann, das vom Bundesverfassungsgericht aus dem Grundgesetz abgeleitete informationelle Selbstbestimmungsrecht des Bürgers zu schützen. Die Berücksichtigung des ganzen Informationszusammenhangs, in dem ein Datum erscheint, habe ich bei der Prüfung datenschutzrechtlicher Fragen stets als meine Aufgabe verstanden.

2. Die Verfassungsbeschwerden gegen das Volkszählungsgesetz, das Verfahren und die anschließenden Verhandlungen vor dem Bundesverfassungsgericht und schließlich die beiden Entscheidungen vom 13. April und 15. Dezember 1983 bedürfen, wie ich glaube, der besonderen Beachtung auch unter den folgenden Gesichtspunkten:

   a) Das Bundesverfassungsgesetz hat im vierten Leitsatz seines Urteils vom 15. Dezember 1983 festgestellt:
   „Das Erhebungsprogramm des Volkszählungsgesetzes 1983 führt nicht zu einer mit der Würde des Menschen unvereinbaren Registrierung und Katalogisierung der Persönlichkeit; es entspricht auch den Geboten der Normenklarheit und der Verhältnismäßigkeit. Indessen bedarf es zur Sicherung des Rechts auf informationelle Selbstbestimmung ergänzender verfahrensrechtlicher Vorkehrungen für Durchführung und Organisation der Datenerhebung."

   Das Gericht hat demnach die im Volkszählungsgesetz vorgesehene Datenerhebung für statistische Zwecke – im Gegensatz zur Weitergabe der erhobenen Einzeldaten, die sich auf bestimmte Personen beziehen – für verfassungskonform erachtet, wenn das Erhebungsverfahren entsprechend den Anforderungen des Urteils verbessert würde.

   Für meine Arbeit ziehe ich daraus den Schluß, nicht nur auf die Probleme und Gefährdungen durch automatisierte Datenverarbeitung hinweisen, sondern auch übertriebenen Ängsten und Befürchtungen steuern zu müssen – bei gleichzeitiger Gewähr für gesetzesgetreue Datenverarbeitung und -verwaltung.

   b) Für die Verwaltung ergibt sich aus den Ausführungen des Bundesverfassungsgerichts die Verpflichtung, ihr Handeln für den Bürger transparenter zu machen und ihn stärker als bisher über Erforderlichkeit und Verfahrensweise der Erfassung und Verarbeitung der von ihm zu fordernden Angaben hinzuweisen. Dies wird in manchen Fällen mehr als bisher der Unterstützung durch die Presse bedürfen, der auch im Sinne positiver Bürgeraufklärung im demokratischen Staat eine besondere Aufgabe zukommt.

   c) Das Verfahren vor dem Bundesverfassungsgericht ergab aber auch für Regierungen und Parteien beachtenswerte Aspekte. Sicherlich ist Datenschutz wegen seiner schwierigen Aufgabe, zwischen widerstreitenden Interessen einen verfassungskonformen Ausgleich zu bewirken, praktisch oft nur schwer „in Griff zu bekommen". Aber nicht nur meine persönlichen Erfahrungen, sondern der Eindruck der Verhandlungen vor dem Bundesverfassungsgericht lassen erkennen, daß im politischen Bereich in seiner Breite ganz allgemein – ohne Bezug auf einzelne Parteien – nicht immer genügend differenzierte Einblicke in die Probleme der Bewältigung des Schutzes der Persönlichkeit des Bürgers bestehen.

   Zusammenfassend kann ich feststellen, daß die Ereignisse im Berichtsjahr 1983, die weithin durch das bundesverfassungsgerichtliche Beschwerdeverfahren bestimmt waren, wesentliche Perspektiven für die künftige Arbeit des Bayerischen Landesbeauftragten für den Datenschutz ergeben haben.

Zu den Tätigkeitsberichten

Die Herausgabe des jährlichen Tätigkeitsberichts ist jedesmal für meine Mitarbeiter und für mich ein schweres Stück Arbeit – nach Umfang wie Inhalt; die Arbeit nimmt mehrere Wochen in Anspruch, nicht zuletzt dabei die Wochenenden. Da das Gesetz nur die Notwendigkeit seiner Erstattung, sonst aber nichts über Form und Darstellung des Tätigkeitsberichts festlegt, machen wir uns über sie verständlicherweise Jahr für Jahr Gedanken. So ist zu sagen:

Die tägliche Arbeit aller Bereiche der Bayer. Verwaltung wirft unzählige Fragen auf, von denen zwar eine recht statt-

liche Anzahl in den Gerichten verhandelt wird, aber nur die bedeutendsten Ergebnisse in den Entscheidungssammlungen der Gerichte oder in Fachzeitschriften veröffentlicht und damit einer daran interessierten Öffentlichkeit zugänglich gemacht werden. Dies genügt auch, da sie die in jahrzehntelanger Verwaltungsarbeit gewonnenen Erfahrungen nur zu ergänzen brauchen.

Für den Datenschutz fehlen entsprechend langjährige Erfahrungen. Auch Vollzugsbekanntmachungen und Erläuterungswerke können nur selten auf Detailfragen eingehen. Dies mag auch ein Grund dafür sein, daß der Gesetzgeber des Datenschutzgesetzes mit der „Verordnung" von Tätigkeitsberichten eine Publizität des Datenschutzes im Bereich der öffentlichen Verwaltung und darüber hinaus gewollt hat. Sie bewirkt möglicherweise, daß die korrekte Einhaltung von Datenschutzregeln und die rechtzeitige Klärung von offenen Datenschutzfragen von der Verwaltung mit mehr Aufmerksamkeit betrieben werden. Außerdem hat der Bericht die Aufgabe, in der Öffentlichkeit die Präsenz der unabhängigen Datenschutzkontrolle bewußt zu machen. Dies hat freilich auch zur Folge, daß aus dem Bereich des Datenschutzes bei öffentlichen Verwaltungsbehörden mehr Probleme bekannt werden, als aus vielen anderen Verwaltungssachgebieten.

Ich bitte, dies bei Durchsicht des Berichts zu bedenken und nicht den meist unzutreffenden Schluß zu ziehen, im Bereich des Vollzuges von Datenschutzvorschriften würden nur der Zahl nach um ein vielfaches mehr Fragen und Probleme entstehen, als in allen anderen Bereichen der Verwaltung, z. B. bei Umweltschutz, Bauen im Außenbereich oder der Planung von Straßentrassen.

Sinn und Notwendigkeit der Herausgabe ausführlicher Tätigkeitsberichte des Datenschutzes sehe ich auch darin, daß die Informationsverarbeitung allgemein in stürmischem Fortschritt begriffen ist und deshalb ihre Wirkungen, soweit sie Einschränkungen oder Beschränkungen des allgemeinen Persönlichkeitsrechts verursachen können, besonders beobachtet werden müssen. Ein Abstellen nur auf die möglicherweise problematischen Wirkungen automatisierter Informationsverarbeitung würde die Tätigkeitsberichte zwar von einer Vielzahl einzelner Datenschutzfälle und -fragen entlasten, aber letztlich als „Mängel-Liste", die sich überwiegend an den Normgeber, also Parlamente und Staatsregierung (als Verordnungsgeber), wendet, dem unmittelbaren Verwaltungsvollzug wenig Nutzen stiften.

So interessant eine solche Beschränkung aus der Sicht der Technologie-Folgen-Bewältigung sein könnte, so wenig wäre dies mit dem Auftrag an den Datenschutzbeauftragten, „über seine Tätigkeit" zu berichten, vereinbar (Art. 28 Abs. 4 Satz 1 BayDSG). Denn die Tätigkeit des Datenschutzbeauftragten und seiner Mitarbeiter ist im rechtlichen Bereich zu einem erheblichen Teil durch Bürgereingaben und Behördenanfragen bestimmt, die sich auf die Anwendung des schon bisher geltenden Rechts auf konkrete Datenschutz-Einzelfragen beziehen. Daß Bürgeranfragen unmittelbar beantwortet werden müssen, bedarf keiner Begründung. Dies gilt aber im Regelfall auch für die Anfragen von Behörden. Wenn diese sich vor einer eventuellen Beanstandung durch den Datenschutzbeauftragten nach dessen Beurteilung eines konkreten Falles erkundigen – z.B. wegen einer von Dritten erbetenen Datenübermittlung – muß meine Dienststelle Anfragen selbst beantworten und kann sie nicht der jeweiligen Aufsichtbehörde zur ausschließlichen Beantwortung abgeben. Zum Schutz des informationellen Selbstbestimmungsrechts der betroffenen Bürger muß nach meiner Überzeugung der Datenschutzbeauftragte mögliche Verletzungen bereits im Vorfeld vermeiden helfen. Die hierbei gesammelten Erfahrungen suche ich – soweit geeignet – durch die Mitteilung in den Tätigkeitsberichten auch anderen Verwaltungsstellen zugänglich zu machen. Im übrigen erzeugt die Zahl der Behördenanfragen beim Landesbeauftragten für den Datenschutz zwar für die sehr kleine Geschäftsstelle sehr viel Arbeit, sie ist aber objektiv gesehen gering, im Verhältnis zur Zahl der über 2000 bayerischen Gemeinden und der übrigen staatlichen und nichtstaatlichen bayerischen Behörden und damit im Verhältnis zur Gesamtheit der auftretenden Datenschutz-Fragen. Im Ergebnis kann davon ausgegangen werden, daß die Fälle, die mir von Behörden vorgetragen werden, meist Sonderfälle sind, die zur vorsorglichen Abwendung einer sonst möglichen Beanstandung im Sinne eines „vorgezogenen" Rechtsschutzes durch „rechtzeitige" Vorkehrungen geklärt werden sollten. Diesen hält das Bundesverfassungsgericht in seinem Volkszählungsurteil als effektiven Schutz des Rechts auf informationelle Selbstbestimmung (II 2 a, a.E.) für geboten. Da diese Praxis auch im vorliegenden Tätigkeitsbericht ihren Niederschlag findet, war m.E. an dieser Stelle hierüber zu berichten.

Für Gesetzentwürfe rege ich darüber hinaus erneut an, im „Vorblatt" des Gesetzentwurfs nicht nur die Frage nach Kosten und Alternativen der vorgesehenen Regelungen anzusprechen, sondern auch kurz auf die Auswirkungen des Gesetzvorhabens auf Erhebung und Nutzung personenbezogener Daten einzugehen (siehe 5. Tätigkeitsbericht Ziff. 1.3 Seite 6, a.E.).

### 1.1. **Der Beirat**

Einrichtung und Aufgaben des gem. Art. 29 BayDSG beim Landesbeauftragten für den Datenschutz gebildeten Beirats habe ich in den früheren Tätigkeitsberichten eingehend dargestellt.

Die dem Landtag angehörenden Mitglieder des Beirats werden jeweils für die Wahldauer des Landtags bestellt, die übrigen Mitglieder jeweils für 4 Jahre. Nach der Landtagswahl im Herbst 1982 sind die Mitglieder des Beirats neu bestellt worden. Mitglieder des Beirats und ihre Stellvertreter sind danach gegenwärtig:

Die Landtagsabgeordneten:

| | |
|---|---|
| Hermann Regensburger | Dr. Paul Wilhelm |
| Franz Josef | Brosch Manfred Humbs |
| Wolfgang Dandorfer | Johann Böhm |
| Franz Gruber | Konrad Kobler |
| Klaus Warnecke | Rolf Langenberger |
| Alfred Münch | Heinz Mehrlich |

Die Senatoren:

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

Für die Staatsregierung:

| | |
|---|---|
| Dr. Friedrich Giehl<br>Ministerialdirigent im<br>Bayer. Staatsministerium | Dr. Werner Böhme<br>Ministerialrat im<br>Bayer. Staatsministerium<br>des Innern der Finanzen |

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>der Anstalt für Kommunale<br>Datenverarbeitung<br>in Bayern |

Für die Sozialversicherungsträger:

| | |
|---|---|
| Franz-Martin Fehn<br>Erster Direktor<br>der Landesversicherungs-<br>anstalt Oberfranken und<br>Mittelfranken | Herbert Schmaus<br>Verwaltungsdirektor beim<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. |

Im Berichtsjahr tagte der Beirat viermal, nämlich am 25. Januar, 26. April, 12. Juli und 25. Oktober 1983. Er befaßte sich in seinen Sitzungen mit folgenden Punkten:

- Datenschutzrechtliche Beanstandungen bei Bayer. Behörden,
- Bericht über den Entwurf zum Staatsvertrag „Bildschirmtext",
- Bericht über die Novellierung des Bundesdatenschutzgesetzes,
- Bericht zum Stand und über das Ergebnis des Gesetzgebungsverfahrens zum Landesmeldegesetz,
- Unterrichtung über die datenschutzrechtlichen Probleme der Durchführung des Volkszählungsgesetzes,
- Bericht über datenschutzrechtliche Kontrollen im Polizeibereich,
- Bericht über datenschutzrechtliche Kontrollen im technischorganisatorischen Bereich,
- Vorberatung des Tätigkeitsberichts 1982 des Landesbeauftragten für den Datenschutz gem. Art. 28 Abs. 6 BayDSG,
- Bericht über die mündliche Verhandlung im Verfahren über die Verfassungsbeschwerden gegen das Volkszählungsgesetz,
- Unterrichtung über den Sachstand im Bereich „Neuer Medien",
- Bericht über das bisherige Verfahren der Auswertung der für die Wanderungsstatistik an das Bayer. Landesamt für Statistik und Datenverarbeitung übermittelten Meldedaten,
- Unterrichtung über den Beschluß der DSB-Konferenz und die DSBPressemitteilung zum Personalausweisgesetz,
- Bericht über den Stand der Überlegungen zu einem Bayer. Archivgesetz,
- Bericht über einen Modellversuch zur computergesteuerten Wirtschaftslichkeitsprüfung bei gesetzlichen Krankenkassen.

Zur Tätigkeit des Beirats siehe im übrigen in den Tätigkeitsberichten I unter 1.4, II unter 1.3, III unter 1.2.1, IV unter 1.5 und V unter 2.1.

## 1.2. Behandlung des 5. Tätigkeitsberichts im Parlament

Der Tätigkeitsbericht für das Jahr 1982 wurde am 26. Oktober 1983 im Ausschuß für Verfassungs-, Recht- und Kommunalfragen des Bayerischen Landtags und am 30. November 1983 im Rechts- und Verfassungsausschuß des Bayerischen Senats beraten.

1. Im Bayerischen Landtag erklärte der Berichterstatter, Abgeordneter Hermann Regensburger, nach der Vorstellung wesentlicher Punkte des Tätigkeitsberichts durch den Landesbeauftragten, daß in Bayern Datenschutz mit Augenmaß betrieben werde; d. h. daß Datenschutzbelange dort durchgesetzt würden, wo dies notwendig sei. Bestandteil des erfolgreichen Bayerischen Konzepts sei die rechtzeitige Einschaltung des Datenschutzbeauftragten bereits im Vorfeld des Erlasses von Gesetzen oder sonstigen Vorschriften. Er wies auf die Bedeutung der damit möglichen frühzeitigen Berücksichtigung von Datenschutzbelangen hin. Das Bundesverfassungsgericht bestätigte im übrigen in seinem Volkszählungsurteil vom Dezember 1983 die Notwendigkeit vorbeugenden Rechtsschutzes durch rechtzeitige Einschaltung der Datenschutzbeauftragten.

   Als besondere Aufgabe des Beirats sah der Berichterstatter die Erörterung von Problemen an, in denen Datenschutzbelange wegen unterschiedlicher Interessenlagen nicht sofort im erforderlichen Umfange berücksichtigt würden. Gerade die Beratungen zum Meldegesetz hätten gezeigt, wie sinnvoll die Vorberatung des Regierungsentwurfs im Beirat gewesen sei. Zur Volkszählung teilte der Berichterstatter die Sorge des Landesbeauftragten für den Datenschutz, ein Ersatz der Volkszählung könne in der Zusammenführung und Nutzung vorhandener Daten aus verschiedensten Verwaltungsbereichen gesucht werden. Eine solche Konzentration von personenbezogen Daten sei problematisch. Es sei gerade das Anliegen des Datenschutzes die Entstehung von Persönlichkeitsprofilen zu vermeiden. Mit einem Bayerischen Ausführungsgesetz zum Personalausweisgesetz werde sich der Beirat befassen, sobald es vorliege.

   MdL Regensburger verwies besonders auf die Datenschutzprobleme, die im Bereich der Neuen Medien zu lösen sind und hob die Bemühungen Bayerns um die Erarbeitung der nötigen bereichsspezifischen Datenvorschriften hervor. Der Berichterstatter ging dann auf die Arbeiten an einem Archivgesetz sowie auf Fragen eines Krebsregistergesetzes ein. Er kritisierte die Erschwerung der Datenschutzkontrolle ausgerechnet aufgrund der Vorschriften über das Steuergeheimnis in der Abgabenordnung und hielt eine gesetzliche Regelung für wünschenswert. Aus dem Arbeitsbereich des Landtags berichtete MdL Regensburger über die Neuregelung des Petitionsrechts, bei der auch beträchtliche Fortschritte für den Datenschutz erzielt worden seien. Die Geschäftsordnung des Bayerischen Landtags sei, auch auf Grund der Beratung durch den Datenschutzbeauftragten, so geändert worden, daß einerseits der Persönlichkeitsschutz und die Intimssphäre des Petenten bei der Behandlung seiner Eingaben gewährleistet sei, andererseits der Grundsatz der Öffentlichkeit der Ausschußsitzungen nicht unverhältnismäßig beeinträchtigt werde.

Der Berichterstatter stellte schließlich fest, daß der Tätigkeitsbericht keine Hinweise auf schwerwiegende Verstöße gegen Datenschutzbestimmungen oder Datenschutzskandale enthalte und kleinere Verstöße nicht auf Vorsatz beruhten. In einigen Bereichen seien die Bediensteten auch noch nicht genügend sensibilisiert. Zur Schärfung des Datenschutzbewußtseins der Bevölkerung und Verwaltung trage nicht zuletzt auch die Debatte im Landtagsausschuß bei.

Mitberichterstatter MdL Klaus Warnecke bestätigte, daß in Bayern keine größeren Datenschutzskandale stattgefunden hätten. Bayern befinde sich jedoch keineswegs in einer datenschützerischen Idylle, wie die schwierigen Erörterungen zum Meldegesetz mit der Einführung des Ordnungsmerkmals und der Speicherung der Seriennummer des Personalausweises ausweisen würden. Der Rückblick auf die vergangenen fünf Jahre Datenschutz in Bayern gestatte die Feststellung, daß ohne Datenschutzbeauftragten sicherlich einige handfeste und spektakuläre Auseinandersetzungen um Einzelfälle oder Datenschutzstrukturen stattgefunden hätten. Er hob die Stellung des Datenschutzes im Zielkonflikt zwischen Verwaltungszielen und Freiheitsbewußtsein der Bürger hervor und betonte die Notwendigkeit Datenschutz konkret auf den technologischen Wandel zu beziehen. Dieser erzeuge immer wieder neue Datenschutzprobleme. Dabei habe sich gezeigt, daß es schwierig sein könne, Datenschutzbelange rechtzeitig in gesetzliche Normierungen von Verwaltungsabläufen einzubringen.

MdL Warnecke betonte die Notwendigkeit, aus der Sicht des Datenschutzes den Neuen Medien – insbesondere dem Medium „Kabel" – große Aufmerksamkeit zu widmen, da im Zusammenhang mit der Abrechnung Daten zu speichern seien.

Der Mitberichterstatter vertrat die Ansicht, die Datenschutzberichte sollten der Verwaltung als eine Art Lexikon dienen. Manche Kapitel seien deshalb ganz bewußt im Stil praxisbezogener Anleitungen gehalten. In diesem Zusammenhang hob er auch die Notwendigkeit der Datenschutzkontrolle im technischen und organisatorischen Bereich hervor. Die Bürger hätten Anspruch darauf, daß die Verwaltung ihre Daten gegen unerlaubte Einsicht und Zugriffe sichere.

Der Ausschuß erörterte anschließend nochmals die Seriennummer des Personalausweises und deren evtl. Verwendung in anderen Verwaltungsbereichen, sowie Datenschutzfragen, die sich aus einer Vermehrung von polizeilichen Kontrollen mit Hilfe eines maschinenlesbaren Personalausweises ergeben könnten.

2. Im Bayerischen Senat wurde nach der Vorstellung des Tätigkeitsberichts durch den Landesbeauftragten für den Datenschutz im Rechts- und Verfassungsausschuß die Frage der Löschung von Eintragungen über Jugendstrafen in Datenbanken und im Zusammenhang damit die Anordnung über „Mitteilungen in Strafsachen" angesprochen. Eine ausführlichere Diskussion entspann sich um das Thema „Computerkriminalität" und die Frage, wie wahrscheinlich die Ausbreitung dieses Phänomens im Bereich der öffentlichen Verwaltung generell sei. Außerdem wurden die Datenweitergabe an kirchliche Einrichtungen zum Zwecke der Berechnung der Kirchensteuer, die Aufbewahrung von Karteikästen in Gemeinden, in Räumen die dem Publikumsverkehr zugänglich sind, sowie der Zugang der Polizei zu Kraftfahrzeug- oder Melderegistern außerhalb der Dienstzeit der Behörden, mit Hilfe eines eigenen Schlüssels, angesprochen.

### 1.3. **Arbeitsbedingungen der Geschäftsstelle**

Unter dieser Überschrift habe ich im 5. Tätigkeitsbericht darüber berichtet, daß der angestrebte Personalstand der Geschäftsstelle fast erreicht sei und eine weitere Stellenvermehrung nicht angestrebt werde, da bei normalem Arbeitsablauf die Arbeit mit den vorhandenen bzw. damals noch zu erwartenden Mitarbeitern bewältigt werden könne. Ich habe allerdings angemerkt, daß Sonderaktionen wie die jährliche Abfassung des Tätigkeitsberichts oder Stellungnahmen für das Bundesverfassungsgericht zum Volkszählungsgesetz oft einen Arbeitseinsatz von den Mitarbeitern erforderten, der weit auch über die bei obersten Dienstbehörden üblichen Dienststunden hinausgeht. Ich habe mit Hinblick auf die generell angespannte Haushaltslage geglaubt, dies in Kauf nehmen zu sollen (s.a. in den Tätigkeitsberichten IV Nr. 1.4, III Nr. 1.2.2 und II Nr. 1.4).

Seit der im Jahr 1983 begonnenen Diskussion zum Volkszählungsgesetz und, in geringerem Umfang, auch zum Gesetz über einen neuen Bundespersonalausweis, und seit Erlaß des Urteils des Bundesverfassungsgerichts zum Volkszählungsgesetz hat sich die Situation nun drastisch verschlechtert:
Meine Geschäftsstelle hatte bisher mit der Personal-Grundausstattung gearbeitet, die mir aufgrund meines 1979/80 gestellten Antrags im Haushalt 1981/82 zugestanden worden war. Daß ich im Personalbereich immer sehr zurückhaltend war und von Stellen-Ausschöpfungsmöglichkeiten stets nur mit äußerster Sparsamkeit Gebrauch machte, kann ich jederzeit belegen und ergibt sich auch aus meinen Tätigkeitsberichten.

Seit der Zeit, in der die Grundausstattung damals festgelegt wurde, hat sich der Arbeitsanfall jedoch vervielfacht. Erhebliche Überstunden sind die tägliche Regel, in bestimmten Arbeitsbereichen ist auch an Wochenenden Mehrarbeit zu leisten. Trotzdem ist die Flut der Eingaben von Bürgern und der Bitten um Stellungnahmen zu behördlichen Problemen mit den wenigen Mitarbeitern nicht mehr ausreichend zu bearbeiten. Kontrollen des Datenschutzes, die vom Landesbeauftragten selbst eingeleitet werden, also ohne eine Eingabe oder Anfrage Dritter, sind im rechtlichen Bereich fast nicht möglich, obwohl auch dies eine gesetzliche Aufgabe ist (Art. 28 Abs. 1 BayDSG). Es entsteht immer häufiger die Situation, daß zwar bei Behörden die technisch-organisatorische Seite des Datenschutzes, also die notwendigen Datensicherungsmaßnahmen, überprüft werden, daß aber die rechtliche Vorfrage, ob alle so gesicherten Daten überhaupt gespeichert oder in einem Online-Verfahren zur Verfügung gestellt werden dürften, mangels Personalkapazität nicht geprüft werden kann.

In letzter Zeit ist ein weiteres Anschwellen der Arbeitsmenge zu beobachten: Sie ist in erster Linie auf die Entscheidung des Bundesverfassungsgerichtes zum Volkszählungsgesetz zurückzuführen. Sie führt zu einer anhaltenden erhöhten Belastung, denn zahlreiche ADV-Verfahren und die ihnen zugrundeliegenden Rechtsnormen müssen nun überprüft und teilweise auch geändert werden. Auch die Basis des Datenschutzes und die Tätigkeit des Beauftragten, nämlich die Datenschutzgesetze selbst, bedürfen einer

Überarbeitung. Sich mit diesen Aufgaben intensiv zu befassen, ist vorrangige Aufgabe. Da die Entscheidung des Bundesverfassungsgerichts auch für den Vollzug zahlreicher Gesetze Probleme aufwirft und sich das Datenschutzbewußtsein verstärkt hat, sind zunehmend auch Fragen zur Anwendung des Datenschutzrechts in Behördenbereich zu klären. In gleichem Maße ist die Anzahl der Bürgeranfragen gestiegen, seit Oktober 1983 hat sich der durchschnittliche monatliche Eingang von neu zu bearbeitenden Fällen – unabhängig vom Einlauf zu schon in Arbeit befindlichen Fällen – etwa verdoppelt. Mit dem aufgrund der vorhandenen Stellen verfügbaren Personal ist diese Arbeit nicht mehr zu leisten.

Die öffentliche Diskussion zu den „Neuen Medien" gebietet eine wirksame Datenschutzkontrolle in diesem Bereich – nicht zuletzt im Interesse des Vertrauens der Bevölkerung. Dem trägt die Zuweisung dieser Aufgabe an den Datenschutzbeauftragten in Art. 1 Abs. 2, Art. 2 des Ausführungsgesetzes zum Bildschirmtext-Staatsvertrag Rechnung. Gleiches gilt für die weitere umfangreiche Aufgabenzuweisung (Kontrollkompetenz auch für den nichtöffentlichen Bereich) durch Art. 19 Abs. 2, 31 Abs. 4, 32 Abs. 2 und 33 Abs. 4 des Entwurfes des Medienerprobungs- und -entwicklungsgesetzes. Im Interesse einer sachgerechten Kontrolle der neuen Medien bin ich der Ansicht, daß diese Übertragung der gesamten Kontrolle auf den unabhängigen Datenschutzbeauftragten sehr sinnvoll ist. Dies setzt voraus, daß im Bereich der neuen Medien ein Datenschutzkontroll-System erstmals aufgebaut wird. Diese zusätzliche Arbeitsfülle läßt sich allerdings mit dem vorhandenen Personal nicht bewältigen. Ich habe daher eine, angesichts der anstehenden Aufgaben sehr bescheidene, Erweiterung um drei Personalstellen sowie die Schaffung einer weiteren Prüfbereichsleiterstelle zum Haushalt 1985/86 beantragt.

Ich erhoffe die Unterstützung von Landtag und Staatsregierung hierzu. Ohne Personalmehrung werde ich der erheblichen Bedeutung, die das Bundesverfassungsgericht einem „vorgezogenen Rechtsschutz" durch „die Beteiligung unabhängiger Datenschutzbeauftragter" für einen effektiven Schutz des Rechts auf informationelle Selbstbestimmung zugemessen hat, nicht hinreichend gerecht werden können (Ziff. II 2 a, a.E., des Urteils).

### 1.4. Konferenz der Datenschutzbeauftragten

Die Datenschutzbeauftragten der Länder und des Bundes und die Datenschutzkommission Rheinland-Pfalz haben im Berichtsjahr in vier Tagungen gemeinsam interessierende Fragen erörtert. Beispielhaft seien genannt die Erarbeitung einer gemeinsamen Entschließung zur Volkszählung 1983 (abgedruckt im Anhang zum 5. Tätigkeitsbericht), die Frage von Datenschutzkontrolle und Geheimhaltungsvorschriften, der Umfang der Prüfungskompetenz beim Verfassungsschutz, Sozialberichte bei Abhängigkeitskranken, Stand der Gesetzgebung zum Personalausweisgesetz, datenschutzrechtliche Anforderungen an den fälschungssicheren und maschinenlesbaren Personalausweis bzw. Paß, Ausführungsgesetze der Länder zum Bildschirmtext-Staatsvertrag, Datenschutzregelungen im Bereich von Sicherheitsbehörden, Datenerhebung im Zusammenhang mit Anträgen auf Kindergeld, Meldewesen, wissenschaftliche Untersuchungen im Bereich des psychiatrischen Maßregelvollzugs, klinische Krebsregister in Tumorzentren (abgedruckt als Anhang Nr. 7 zu diesem Bericht), Gesetzentwurf über die Sicherung und Nutzung von Archivgut, Beschluß einer gemeinsamen Stellungnahme zum Referentenentwurf für eine Novelle zum Bundesdatenschutzgesetz (die Erklärung ist in Anhang Nr. 4 zu diesem Bericht abgedruckt).

### 1.5. Berücksichtigung des Datenschutzrechts im Vorbereitungsdienst der Rechtsreferendare

Nachdem im Rahmen der Ausbildung der Beamten des gehobenen Dienstes eine eingehende Unterrichtung über Datenschutzrecht durchgeführt wird und neuerdings darüber hinaus auch Fortbildungsseminare über Datenschutz angeboten werden, hatte ich dem Bayerischen Staatsministerium des Innern vorgeschlagen, auch Rechtsreferendare im Rahmen ihres Vorbereitungsdienstes über Datenschutzrecht zu informieren. Das Ministerium hat die Regierungen, die hierfür zuständig sind, auf mein Angebot aufmerksam gemacht. Zusätzlich habe ich den Regierungen meine Mitarbeit bei dieser Unterrichtung angeboten. Inzwischen wurden Informationsveranstaltungen über Datenschutz durch eine juristische Mitarbeiterin meiner Geschäftsstelle bei den Regierungen von Schwaben und der Oberpfalz durchgeführt. Mit den Regierungen von Unterfranken und Oberfranken wurden Termine für eine Informationsveranstaltung festgelegt. Als Folge des Erlasses des Volkszählungsurteils durch das Bundesverfassungsgerichts ergibt sich meines Erachtens verstärkt die Notwendigkeit, auch in der Juristenausbildung Datenschutzrecht zu berücksichtigen.

## 2. Zur Auswirkung des Urteils des Bundesverfassungsgerichts zum Volkszählungsgesetz 1983 auf den Datenschutz

Die Auswirkungen des Volkszählungsurteils sind zur Zeit Gegenstand vieler Überlegungen (Leitsätze des Urteils s. Anlage Nr. 1). Die Datenschutzbeauftragten der Länder und des Bundes und die Datenschutzkommission Rheinland-Pfalz haben zu den Auswirkungen eine Entschließung gefaßt, die als Anhang Nr. 3 diesem Bericht beigefügt ist. Der nachfolgende Beitrag erhebt keinen Anspruch auf vollständige Durchleuchtung dieser komplizierten Materie. Ich hoffe jedoch, daß er einige Punkte klarer herauszuarbeiten hilft.

### 2.1. Wesentliche Aussagen des Urteils zum Datenschutz

Das Bundesverfassungsgericht hat festgestellt, daß im Rahmen des allgemeinen Persönlichkeitsrechts des Art. 2 Abs. 1 in Verbindung mit Art. 1 Abs. 1 GG das Recht auf „informationelle Selbstbestimmung" als Grundrecht zu beachten ist. Es umfaßt unter den Bedingungen der modernen Datenverarbeitung den Schutz des Einzelnen gegen „unbegrenzte" Erhebung, Speicherung, Verwendung und Weitergabe seiner persönlichen Daten und gewährleistet insoweit die Befugnis des Einzelnen, grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen (Leitsatz 1).

Einschränkungen dieses Rechts sind nur im überwiegenden Allgemeininteresse zulässig. Sie bedürfen einer verfassungsgemäßen gesetzlichen Grundlage, die dem rechtsstaatlichen Gebot der Normenklarheit entsprechen muß. Bei seinen Regelungen hat der Gesetzgeber ferner den Grundsatz der Verhältnismäßigkeit zu beachten. Auch hat er organisatorische und verfahrensrechtliche Vorkehrungen zu treffen, welche der Gefahr einer Verletzung des Persönlichkeitsrechts entgegenwirken (Leitsatz 2 des Urteils). In den Leitsätzen 3-5 ist die Anwendung der vorgenannten Grundsätze auf die Erhebung und Verarbeitung personenbezogener Daten für statistische Zwecke zusammengefaßt.

Dem Urteil ist also zu entnehmen, daß zumindest im Bereich automatisierter Verarbeitung zwangsweise erhobener

Daten vom Gesetzgeber Grenzen festgelegt werden müssen:

- für Datenerhebung – das Gericht spricht u.a. von der Beschränkung auf das für die Erreichung des Zieles erforderliche Minimum,
- für Datenspeicherung – das Gericht spricht in den Gründen von der Unzulässigkeit der Vorrats-Datensammlung,
- für die Verwendung – hier ist eine Begrenzung auf den gesetzlich bestimmten Zweck erforderlich – und
- für die Weitergabe von personenbezogenen Daten – hierzu fordert das Gericht Schutz vor Zweckentfremdung durch Weitergabe- und Verwertungsverbote.

Die Pflicht zur Begrenzung der Datenverarbeitung muß aber wohl auch für Fälle freiwilliger Angabe von Daten hinsichtlich der angegebenen Verwendungszwecke gelten, sowie in Fällen, in denen wichtige Leistungen für Betroffene von der Angabe von Daten abhängen und bei geheimer Beobachtung von Personen.

Die Begrenzung der Datenverarbeitung muß so weit erstreckt werden, weil für die verschiedensten Verwaltungsbereiche mittlerweile so viele verschiedene Daten über den Bürger erhoben werden, daß ihre unbegrenzte Nutzung bzw. ihr unbegrenzter Austausch tendenziell zu den vom Gericht für unzulässig erklärten Abbildern der Person führen könnte.

Das Recht auf informationelle Selbstbestimmung wirkt als Freiheitsrecht direkt gegenüber staatlicher Datenverarbeitungs-Tätigkeit. Es hat insofern eine Abwehrfunktion zum Schutze des jeweiligen Betroffenen. Seine Umsetzung durch Gesetzgeber und Verwaltung bewirkt aber auch eine Verteilung oder Zuteilung von Informationen, die einer freien Entscheidung von Behörden über die Verwendung personenbezogener Daten (z.B. im Rahmen von Datenübermittlungen), oder einer Zusammenfassung verschiedener Informationen über eine Person entgegensteht. Diese Wirkung könnte auch als Gewaltenteilungsfunktion des „Rechts auf informationelle Selbstbestimmung" bezeichnet werden, die der Vorstellung vom Staat als informationeller Einheit Grenzen setzt. Das Gericht erwähnt den Begriff der „informationellen Gewaltenteilung" selbst und zwar im Zusammenhang mit der erforderlichen Trennung der Kommunalstatistik von anderen Aufgaben der Gemeinden (IV 4b). Durch die Forderung nach grundrechtssichernden Abschottungsmaßnahmen verdeutlicht das Gericht die aus dem Grundrecht abgeleitete Notwendigkeit einer Strukturierung der dem Staat bzw. den Behörden über die Bürger zur Verfügung stehenden Informationsmenge. Demgegenüber wurde bisher, soweit keine Verschwiegenheitspflichten oder besondere Regelungen über die Informationsverteilung bestanden, tendenziell eher ein organisatorischer Freiraum der Behörden angenommen.

Zu klären ist nun, wie weit die Pflichten von Gesetzgeber und Verwaltung gehen, Datenerhebung, Informationsmengen, Nutzung und Datenflüsse durch allgemeine Regelungen, bzw. durch Rücksichtnahmen im Einzelfall des Verwaltungsvollzugs, dem Anspruch des Art. 2 Abs. 1, 1 Abs. 1 GG anzupassen. Dies wird auf Jahre hinaus eine Aufgabe für Wissenschaft und Verwaltung, für Parlamente und Gerichte und nicht zuletzt auch für die Datenschutzbeauftragten sein. Gegenwärtig ist noch keine endgültige Klarheit – insbesondere keine einheitliche Meinung – in dieser Frage zu erkennen.

2.2. **Folgerungen für den Gesetzgeber**

2.2.1. Was darf oder muß der Gesetzgeber regeln?

Aus dem Urteil und seiner Begründung sind meines Erachtens drei voneinander unterscheidbare Bereiche zu erkennen, zu denen sich aus dem Recht auf informationelle Selbstbestimmung Forderungen ableiten lassen:

2.2.1.1 Der Bereich der Unzulässigkeit gesetzlicher Datenverarbeitungsregelungen wegen Verstoßes gegen das Persönlichkeitsrecht.

2.2.1.2 Der Bereich, in dem verfassungsgemäße gesetzliche Einschränkungen des Rechts auf informationelle Selbstbestimmung grundsätzlich möglich sind.

2.2.1.3 Der Bereich, in dem keine Einschränkungen des Rechts auf informationelle Selbstbestimmung feststellbar wären.

Zu 2.2.1.1:

Bereich der Unzulässigkeit gesetzlicher Datenverarbeitungsregelungen wegen Verstoßes gegen das Persönlichkeitsrecht:

a) Gesetze dürfen keine unzulässigen Verwendungszwekke zulassen:

Dem Urteil kann entnommen werden, daß eine Beschränkung der Datennutzung auf bestimmte Verwendungszwecke geboten sein kann. Die Verwendung bestimmter Daten für andere als diese Zwecke wäre dann gesetzlich auszuschließen. Dem Gesetzgeber wird damit auch eine allzu weite Festlegung der Verwendungszwekke von Verfassungs wegen versagt sein.

Deutlich zeigt sich dies an dem vom Gericht entschiedenen Fall der gesetzlich vorgesehenen Nutzung von Einzeldaten der Volkszählung für solche Zwecke der Verwaltung, die nicht strikt gesetzlich auf Statistik oder abstrakte Planung beschränkt waren. Soweit hätte der Gesetzgeber die Nutzbarkeit der Statistik-Daten nicht ausdehnen dürfen.

Aus dem entschiedenen Fall ist zu schließen, daß entsprechendes für andere Statistiken gilt. Der Gesetzgeber ist gehalten, in anderen Statistikgesetzen, soweit sie sich im grundgesetzlich unzulässigen Bereich bewegen, die Datennutzung zu begrenzen. Bereiche unzulässiger, auch durch Gesetz nicht in verfassungsmäßiger Weise regelbarer Datenverarbeitung sind aber auch außerhalb des Statistikbereichs zu erkennen:

Als Kriterium für die Zulässigkeit gesetzlicher Verwendungsregelungen wird vom Bundesverfassungsgericht immer wieder der Grundsatz der Verhältnismäßigkeit als Ausdruck des allgemeinen Freiheitsanspruches der Bürger gegenüber dem Staat genannt (z.B. II 16 a E). Einschränkungen des Grundrechts sind nur möglich, soweit sie zum Schutze öffentlicher Interessen unerläßlich sind. Diese Interessenabwägung führt nach dem Urteil zu dem Schluß, daß jegliche Datenverarbeitung auf die Verwendungszwecke bestimmter Verwaltungsbereiche begrenzt bleiben müsse.

Als Ergebnis sei – mit aller Vorsicht – der Schluß gezogen, daß der Gesetzgeber keine Verwendungszwecke von Daten zulassen darf, die tendenziell zu einer Vermischung von Daten aus Bereichen führen könnten, die ihrer Art nach abgeschottet sind (z.B. Sozialdaten, medizinische Daten, Steuerdaten). Dabei spielt für das Gericht

eine wichtige Rolle auch die Frage der Transparenz der Datenverarbeitung für die Bürger bzw. der „Undurchsichtigkeit der Speicherung und Verwendung von Daten unter den Bedingungen der ADV". Eine Datenweitergabe alleine unter dem Gesichtspunkt der Erforderlichkeit zur Aufgabenerfüllung des Datenempfängers kann in diesen Fällen nicht alleiniges Zulässigkeitskriterium sein.

b) Gesetze dürfen keine unbeschränkte Datenerhebung vorsehen:

Das Bundesverfassungsgericht verweist darauf, daß schon bislang anerkannt sei, daß die zwangsweise Erhebung personenbezogener Daten nicht unbeschränkt statthaft sei, „namentlich dann, wenn solche Daten für den Verwaltungsvollzug (etwa bei der Besteuerung oder der Gewährung von Sozialleistungen) verwendet werden sollen." (II 2 a).

c) Gesetze dürfen keine umfassende Registrierung bewirken:

Der Gesetzgeber darf keine umfassende Registrierung und Katalogisierung der Persönlichkeit durch Zusammenführung einzelner Lebens- und Personaldaten zur Erstellung von Persönlichkeitsprofilen der Bürger zulassen. Interessanterweise erstreckt das Gericht diese Aussage auf „Teilabbilder", die mit der Würde des Menschen nicht vereinbar sind (III, 1 a). Dies festzuhalten erscheint wichtig, weil die Wahrscheinlichkeit der Entstehung von Totalabbildern geringer ist. Teilabbilder jedoch, die unter Umständen auch besonders sensitive Informationen in Teilprofilen der Persönlichkeit zusammenführen oder entstehen lassen, sind eher denkbar. Ohne eine endgültige Aussage treffen zu wollen, denke ich hier z.B. an die Zusammenführung der Kenntnisse der verschiedenen Sparten einer Großstadtverwaltung über einen Bürger in einem einzigen Informationszusammenhang. Hier schließt sich die interessante Frage an, ob eine derart zusammengeführte Datenbasis allein durch die Verteilung von Zugriffsberechtigungen verschiedener Dienststellen auf verschiedenen Untermengen der Gesamtinformation wieder unbedenklich würde.

d) Gesetze dürfen keine Datenerhebungen vorsehen, die zu Verzicht auf Grundrechtsausübung führen:

Das Gericht führt (unter II 1 a) aus: „Wer damit rechnet, daß etwa die Teilnahme an einer Versammlung oder einer Bürgerinitiative behördlich registriert wird und daß ihm dadurch Risiken entstehen können, wird möglicherweise auf eine Ausübung seiner entsprechenden Grundrechte (Art.8, 9 GG) verzichten. Dies würde nicht nur die individuellen Entfaltungschancen des Einzelnen beeinträchtigen, sondern auch das Gemeinwohl, weil Selbstbestimmung eine elementare Funktionsbedingung eines auf Handlungs- und Mitwirkungsfähigkeit seiner Bürger gegründeten freiheitlichen demokratischen Gemeinwesens ist."

Dieser Aussage geht die Feststellung des Gerichtes voraus:

„Mit dem Recht auf informationelle Selbstbestimmung wäre eine Gesellschaftsordnung und eine diese ermöglichende Rechtsordnung nicht vereinbar, in der Bürger nicht mehr wissen können, wer was wann und bei welcher Gelegenheit über sie weiß. Wer unsicher ist, ob abweichende Verhaltensweisen jederzeit notiert und als Information dauerhaft gespeichert, verwendet oder weitergegeben werden, wird versuchen, nicht durch solche Verhaltensweisen aufzufallen."

Dem Gesetzgeber ist demnach mit Rücksicht auf das Recht auf informationelle Selbstbestimmung verwehrt, Datenerhebungen und Nutzungen anzuordnen, die möglicherweise zum Verzicht auf Grundrechtsausübungen führen. Ich halte diesen Hinweis des Gerichts besonders im Hinblick auf umfangreichere Datensammlungen für bedeutsam, von denen über den „psychischen Druck öffentlicher Anteilnahme" (Mikrozensusurteil) indirekt Auswirkungen in Richtung auf Normierung des Verhaltens oder der registrierbaren Lebensäußerungen ausgehen können. So könnten etwa größere Krankheitsregister Bedenken in dieser Richtung auslösen, da sie Bürger möglicherweise veranlassen würden, sich so zu verhalten, daß über sie nichts vermeintlich Negatives gespeichert würde.

e) Gesetze dürfen keine unzumutbaren Angaben fordern:

Unzumutbare intime Angaben und Selbstbezichtigungen können nach den Ausführungen des Gerichts nicht Gegenstand gesetzlicher Regelungen von Datenerhebung, -verarbeitung und -nutzung sein (II 2 a).

Zu 2.2.1.2:

Bereich, in dem verfassungsmäßige gesetzliche Einschränkungen des Rechts auf informationelle Selbstbestimmung grundsätzlich möglich sind:

a) allgemeine Anforderungen an gesetzliche Regelungen:

„Einschränkungen" oder „Beschränkungen" des Rechts auf informationelle Selbstbestimmung (so die Terminologie des Gerichts) sind zulässig aufgrund einer verfassungsmäßigen gesetzlichen Grundlage. Die Frage der Verfassungsmäßigkeit ist nach dem Urteil besonders an den Grundsätzen der Normenklarheit und der Verhältnismäßigkeit zu prüfen. Angesichts der vom Gericht festgestellten möglichen Gefährdungen durch Nutzung der ADV hat der Gesetzgeber dabei mehr als früher auch organisatorische und verfahrensrechtliche Vorkehrungen zu treffen, die der Gefahr einer Verletzung des Persönlichkeitsrechts entgegenwirken.

b) Statistikgesetze:

Als Beispiel für eine zulässige Einschränkung oder Beschränkung wäre nach dem Urteil eine Volkszählung der im VZG 1983 vorgesehenen Art zu nennen, allerdings ohne die Datenübermittlungen nach § 9 Abs. 1 – 3 VZG 83 und verbessert durch organisatorische und verfahrensrechtliche Maßnahmen, die im Urteil im einzelnen angesprochen sind. Diese wirken grundsätzlich in Richtung Aufrechterhaltung der ausschließlich statistischen Nutzung der erhobenen Daten durch Abschottung gegen das Risiko anderweitiger Nutzung.

Dementsprechend wären auch andere Statistiken bei entsprechenden flankierenden grundrechtssichernden Maßnahmen gesetzlich regelbar. Voraussetzung wäre, daß bei ihnen keine Gefahr unzulässiger Vermischung von Statistik und Verwaltungsvollzug, keine Gefahr des Verzichts auf Grundrechtsausübung, sowie keine Gefahr der Entstehung von Teilabbildern der Person gegeben ist und unzumutbare Angaben nicht gefordert werden. Eine Schwierigkeit liegt aber zweifellos darin, die erforderliche Genauigkeit zu bestimmen, mit der die Daten, das Verfahren und die Verwendungszwecke im Gesetz anzugeben sind (II 2 und IV 3 am Ende). Dabei sind

nach dem Urteil die Anforderungen an die Festlegung der statistischen Verwendungszwecke im Gesetz verhältnismäßig gering.

c) Überlegungen des Gerichts zu Art und Notwendigkeit gesetzlicher Regelungen:

Weitere Schlüsse hinsichtlich der Art der gebotenen gesetzlichen Regelungen läßt der Hinweis des Gerichts zu, daß beispielsweise die Regelungen in den Datenschutzgesetzen des Bundes und der Länder, die §§ 30, 31 der Abgabenordnung und § 35 i.V.m. §§ 67 – 86 SGB X, was die erforderlichen „Maßnahmen zum Schutze der Betroffenen" betrifft „in die verfassungsrechtlich gebotene Richtung weisen" (II 2. a).

Die Regelungen im Steuer- wie auch Sozialbereich haben im wesentlichen gemein, daß personenbezogene Daten aus diesem Bereich nach außen nur in eng begrenztem Maße, aufgrund relativ detaillierter Vorschriften übermittelt bzw. offenbart werden dürfen. Man kann die Entstehung dieser Bereiche als Umsetzung des Gedankens der informationellen Gewaltenteilung betrachten.

In den Regelungen der Datenschutzgesetze des Bundes und der Länder finden sich Ansätze in dieser Richtung in Vorschriften über die Erstreckung von besonderen Schweigepflichten auf Datenempfänger. Die Regelungen über Rechte des Betroffenen dienen dem Recht auf informationelle Selbstbestimmung unmittelbar. Unsicher erscheint dagegen, ob die allgemeinen Zulässigkeitsregeln der Datenschutzgesetze für den öffentlichen Bereich hier vom Bundesverfassungsgericht gemeint waren, da Änderungen des Verwendungszwecks der Daten, jedenfalls dem Wortlaut nach, nicht die Zulässigkeit beeinflussen.

Besonders interessant ist, in wieweit das Gericht überhaupt die Notwendigkeit zu gesetzlichen Regelungen sieht. Unmittelbar im Anschluß an das vorgenannte Zitat des Gerichts von AO, SGB X und Datenschutzgesetzen steht in den Urteilsgründen die Aussage:

„Wie weit das Recht auf informationelle Selbststimmung und im Zusammenhang damit der Grundsatz der Verhältnismäßigkeit sowie die Pflicht zu verfahrensrechtlichen Vorkehrungen den Gesetzgeber zu diesen Regelungen von Verfassungs wegen zwingen hängt von Art, Umfang und denkbaren Verwendungen der erhobenen Daten sowie der Gefahr des Mißbrauchs ab."

Aus diesem Satz kann entweder geschlossen werden, daß nur die Tiefe einer im übrigen stets erforderlichen Regelung von Art, Umfang und denkbarer Verwendung der erhoben Daten etc. abhängig sei. Die Frage „ob" von Verfassungs wegen eine gesetzliche Regelung überhaupt erforderlich sei, stelle sich dagegen nicht. Es kann aus dem zitierten Satz aber wohl auch abgeleitet werden, daß nach Art, Umfang und denkbaren Verwendungen der erhobenen Daten etc. auch Bereiche erkennbar sein könnten, in denen der Gesetzgeber von Verfassungs wegen zu Regelungen nicht gezwungen wäre. Zwei im Anschluß an den zitierten Satz vom Bundesverfassungsgericht selbst zitierte frühere Entscheidungen des Gerichts können hierzu einen Hinweis geben.

BVerfGE 49, 89 (142)

„ ... dies wird am deutlichsten in Art. 1 Abs. 1 Satz 2 GG ausgesprochen, wonach es Verpflichtung aller staatlichen Gewalten ist, die Würde des Menschen zu achten und zu schützen. Daraus können sich verfassungsrechtliche Schutzpflichten ergeben, die es gebieten, rechtliche Regelungen so auszugestalten, daß auch die Gefahr von Grundrechtsverletzungen eingedämmt bleibt. Ob, wann und mit welchem Inhalt sich eine solche Ausgestaltung von Verfassungs wegen gebietet, hängt von der Art, der Nähe und dem Ausmaß möglicher Gefahren, der Art und dem Rang des verfassungsrechtlich geschützen Rechtsguts sowie von den schon vorhandenen Regelungen ab."

BVerfGE 53, 30 (61):

„...3. Der Streitfall nötigt nicht zu der Prüfung, ob und inwieweit die verfassungsrechtliche Schutzpflicht und Mitverantwortung des Staates zum Erlaß von Regelungen der geschilderten Art zwingen ..."

Da in beiden Fällen auch das „ob" einer gesetzlichen Regelung angesprochen ist, gehe ich jedenfalls zunächst davon aus, daß das obige Zitat aus der Begründung des Volkszählungsurteils so zu lesen ist, daß von Art, Umfang und denkbaren Verwendungen der erhobenen Daten, sowie der Gefahr ihres Mißbrauchs auch abhängt, „ob" überhaupt eine gesetzliche Regelung erforderlich ist – umgekehrt gesagt, daß gesetzliche Regelungen nicht in allen Fällen erforderlich sein dürften.

Zu 2.2.1.3:

Der Bereich in dem keine Einschränkungen oder Beschränkungen des Rechts auf informationelle Selbstbestimmung feststellbar wären, in dem also ohnehin der verfassungsrechtliche Gesetzesvorbehalt entfiele:

Da eine klare Definition von Fällen, in denen Einschränkungen oder Beschränkungen des Rechts nicht vorliegen, sehr schwierig ist, wird teilweise dahin argumentiert, daß grundsätzlich jeder Umgang mit personenbezogenen Daten, wegen einer damit verbundenen, wenn auch noch so schwachen Einschränkung des Rechts, gesetzlich zu regeln sei. Bei besonders schwachen Einschränkungen müsse eben die gesetzliche Rechtsfolge entsprechend zurückhaltend ausfallen.

Ich halte für möglich, daß eine endgültige Klärung der Frage, in welchen Fällen eine gesetzliche Regelung nicht erforderlich ist, nicht notwendig wird, wenn nämlich in einem allgemeinen Datenschutzgesetz eine entsprechend weitgefaßte Erlaubnis zur Datenverarbeitung enthalten wäre. Damit ist aber auch die Frage nach der rechtlichen Bedeutung einer die gesamte Datenverarbeitung umfassenden Regelung im Datenschutzgesetz gestellt.

2.2.2. Bereichsspezifische oder allgemeine Datenschutzregelungen?

Die Anwendung des Volkszählungsurteils ist mit Sicherheit schwierig in dem vorgenannten zweiten Bereich, in dem nach Ansicht des Bundesverfassungsgerichts nunmehr ausreichende gesetzliche verfassungskonforme Regelungen vorhanden sein müssen, damit Datenerhebung, -verarbeitung und -nutzung und die Änderung von Nutzungen der Daten mit dem Recht auf informationelle Selbstbestimmung in Einklang stehen. Dieser zweite Bereich kann m.E. wiederum unterteilt werden in einen Teil, in dem die Notwendigkeit einer besonderen gesetzlichen Regelung wegen schwerwiegender Wirkungen gegenüber dem Betroffenen klarer

erscheint und einen zweiten Teil, in dem diese Klarheit nicht besteht, sei es wegen tatsächlicher Unklarheiten oder wegen Meinungsverschiedenheiten über Nutzungszwecke von Daten, oder über deren Auswirkungen auf den Betroffenen oder über etwaige Gefahren des Mißbrauchs. Im ersteren Teil hielte ich bereichsspezifische Datenschutzregelungen für angemessen, im zweiten Teil scheint sich mir aus mehreren Gründen eine pragmatische Verfahrensweise anzubieten:

a) zu Teil 1, Bereich schwerwiegender Wirkungen für Betroffene:

Beispiel für schwerwiegende Wirkungen von Datenverarbeitung im Bereich der öffentlichen Verwaltung sind wesentliche Teile der Datenerhebung, -verwendung und -weitergabe durch Sicherheitsbehörden, weil die betroffenen Personen mit rechtswidrigem Verhalten in Zusammenhang gebracht werden. Dies kann sich grundsätzlich auf alle Arten von Entfaltungschancen des Betroffenen negativ auswirken, und zwar unabhängig davon, ob er diese Wirkung selbst verursacht hat, oder ob der Informationszusammenhang u.U. ohne eigene Unkorrektheit zustande kam, was bei beobachtender Fahndung, oder auch bei Beobachtung durch Nachrichtendienste grundsätzlich möglich ist.

Ähnlich schwerwiegende Wirkungen könnten grundsätzlich von der Verarbeitung von Personaldaten durch den Arbeitgeber ausgehen, da sie sich unmittelbar auf die Lebensgrundlage, nämlich das Arbeitsverhältnis auswirken können.

Ein weiteres Beispiel wäre die Erhebung und Verarbeitung medizinischer Daten außerhalb des durch die ärztliche Schweigepflicht beim behandelnden Arzt geschützten Bereiches.

Wegen der weitreichenden Wirkungen völlig neuer Art hebt sich außerdem der Bereich der Neuen Medien aus der Verarbeitung personenbezogener Daten heraus.

Die genannten vier Bereiche sind nicht als abschließende Aufzählung gedacht.

In diesen Fällen erscheint mir die Notwendigkeit einer bereichsspezifischen gesetzlichen Regelung der Datenverarbeitung gegeben. Auch die Intensität einer gesetzlichen Regelung wird, wegen der gravierenden Auswirkungen die diese Datenverarbeitung haben kann, relativ groß sein müssen.

b) Zu Teil 2, Bereich einer pragmatischen Vorgehensweise:

Neben den vorgenannten Datenverarbeitungsbereichen mit gravierenderen Auswirkungen dürfte es eine kaum abschließend aufzählbare Zahl von Verwaltungsbereichen geben, deren Datenverarbeitung an Stelle von bereichspezifischen Regelungen auch durch allgemeinere Vorschriften in einem Bundes- bzw. Landesdatenschutzgesetz im Verhältnis zum Recht auf informationelle Selbstbestimmung ausreichend gesetzlich abgesichert werden könnte. Über den Umfang dieses Bereichs und die Möglichkeit, ihn durch allgemeines Datenschutzrecht abzudecken, bestehen derzeit wohl Meinungsverschiedenheiten. Unabhängig davon halte ich es jedoch für effektiver – von der Vorgehensweise her gedacht – zunächst zu prüfen, ob hier allgemeine Datenschutzregelungen ausreichen könnten, denn für die große Zahl von Verwaltungsbereichen, in denen personenbezogene Daten erhoben und verwendet werden, würde allein die Schaffung der bereichsspezifischen Regelungen sehr lange dauern. Bis dahin müßte aber bereits ein dem Urteil entsprechender Zustand hergestellt werden. Die Bereitschaft der Parlamente, eine Vielzahl von bereichsspezifischen Datenschutzregelungen zu erlassen, darf außerdem nicht überschätzt werden.

Als Vorgehensweise bietet sich meines Erachtens also an, zunächst gleichzeitig

- in den Verwaltungsbereichen, in denen besonders gravierend in das Recht auf informationelle Selbstbestimmung eingegriffen werden muß, durch bereichsspezifische Regelungen und
- durch Novellierung des Bundes- und der Landesdatenschutzgesetze zu versuchen, die Anforderungen des Volkszählungsurteils umzusetzen. Im Zuge der Erarbeitung der notwendigen Änderungen der Bundes- und der Landesdatenschutzgesetze wird sich ergeben, welche weiteren speziellen Bereiche – trotz aller Bemühungen – nicht in einer dem Volkszählungsurteil angemessenen Weise im allgemeinen Datenschutzrecht geregelt werden können. Auf diese Weise ließe sich bald eine Übersicht über die verbleibenden noch bereichsspezifisch gesetzlich zu regelnden Datenverarbeitungsbereiche entwikkeln.

### 2.3. **Folgerungen für den Verwaltungsvollzug**

Für die Vollzugsbehörden ist durch das Volkszählungsurteil eine schwierige Situation entstanden. Zwar hat die Verwaltung nicht das Verwerfungsrecht. Sie kann also nicht bestehende Gesetze wegen angenommener Verfassungswidrigkeit außer acht lassen. Gleichwohl besteht m.E. im Rahmen der bestehenden Gesetze die Notwendigkeit, Grundsätze des Bundesverfassungsgerichtsurteils zum Volkszählungsgesetz durch verfassungskonforme Auslegung bereits jetzt im Verwaltungsvollzug zur Geltung zu bringen – noch bevor die einschlägigen Gesetze daraufhin überprüft worden sind, ob sie angepaßt werden müssen. Aus dem Urteil ergeben sich für eine solche verfassungskonforme Auslegung auch Anhaltspunkte. Ohne Anspruch auf Vollständigkeit möchte ich dazu folgende Vorschläge unterbreiten:

#### 2.3.1. Verfassungskonforme Auslegung im Vollzug

Zunächst sind die oben dargestellten Forderungen an den Gesetzgeber daraufhin zu überprüfen, ob sie schon vor etwaigen Gesetzesänderungen im Verwaltungsvollzug berücksichtigt werden müßten:

- Die Übermittlung von Einzeldaten aus statistischen Erhebungen wäre wohl einzuschränken, soweit eine nur statistische bzw. abstrakt planerische Nutzung beim Datenempfänger nicht sichergestellt erscheint, vielmehr eine Vermischung mit Vollzugszwecken anzunehmen ist. Ggf. wäre an eine Vorlage zur gerichtlichen Klärung der Verfassungsmäßigkeit zu denken.
- Eine Beschränkung der Datennutzung auf den Erhebungszweck verursacht dagegen in vielen anderen Fällen – außerhalb des Statistikbereichs – mehr Schwierigkeiten.

  Einmal ist der Erhebungszweck in manchen Fällen gesetzlich nicht so deutlich festgelegt, daß eine Datennutzung daran zuverlässig gemessen werden könnte. Andererseits war nicht nur die Pflicht zur Verwendungsbegrenzung – soweit keine besonderen Verschwiegenheits- oder Geheimhaltungspflichten bestanden – bisher nicht bewußt, sondern Vorschriften wie Art. 17 Abs. 1

BayDSG legten eine entgegengesetzte Verfahrensweise nahe. Hierauf gehe ich im folgenden noch näher ein (s.a. 3.2)

- Umfassende Registrierungen personenbezogener Daten, wie etwa in einem „Mitgliederverzeichnis" nach § 319a RVO, sollten keinesfalls ohne genaue Prüfung, ggf. erst nach Konkretisierung der Rechtsgrundlage durch den Gesetzgeber, in Angriff genommen werden.
- Jede Datenerhebung ist im Rahmen der Erforderlichkeitsprüfung darauf zu untersuchen, ob sie möglicherweise den Verzicht von Bürgern auf Grundrechtsausübungen bewirken kann. Gegebenenfalls muß diese Wirkung am Verhältnismäßigkeitsgrundsatz gemessen werden. Dies kann im Einzelfall auch das Unterlassen einer Datenerhebung notwendig machen – zumindest dann, wenn das Gesetz diese nicht ausdrücklich vorsieht.
- Bei Datenerhebung ist auch zu prüfen, ob unzumutbare intime Angaben, oder Selbstbezichtigungen gefordert werden. Ggf. ist die Erhebung zu modifizieren.

2.3.2. Transparenz und Rechtmäßigkeit von Datenübermittlungen

Ein wichtiges Anliegen des Urteils ist es, durch die Rechtsordnung möglichst weitgehend sicherzustellen, daß die Bürger wissen, „wer was wann und bei welcher Gelegenheit über sie weiß" (II 1 a). Hieraus könnte für den Vollzug die Folgerung gezogen werden, die gegenwärtig bereits nach Art. 16 Abs. 2 BayDSG gebotene Information über den Verwendungszweck der erhobenen Daten möglichst deutlich zu gestalten. Im Rahmen dieser Information sollte auch auf vorgesehene Datenübermittlungen hingewiesen werden, insbesondere wenn sie Änderungen des Nutzungszwecks der Daten bewirken. Das Gericht hat dies, so meine ich, im Zusammenhang mit den Erörterungen über die Weitergabe der für die Volkszählung zu erhebenden Daten angedeutet (IV 1 am Ende):

> „Anders als bei Datenerhebungen zu ausschließlich statistischen Zwecken ist hier eine enge und konkrete Zweckbindung der weitergeleiteten Daten unerläßlich... zudem ist das Gebot der Normenklarheit von besonderer Bedeutung. Der Bürger muß aus der gesetzlichen Regelung klar erkennen können, daß seine Daten nicht allein zu statistischen Zwecken verwendet werden, für welche konkreten Zwecke des Verwaltungsvollzugs seine personenbezogenen Daten bestimmt und erforderlich sind und daß ihre Verwertung unter Schutz gegen Selbstbezichtigungen auf diesen Zweck begrenzt bleibt."

Wenn diese Aussage auch auf die Klarheit einer gesetzlichen Regelung abzielt, so wäre der Verwaltung doch im Rahmen des Art. 16 Abs. 2 BayDSG in vielen Fällen möglich, einstweilen im Verwaltungsvollzug durch Aufklärung beim Betroffenen Klarheit zu schaffen.

Mit der Bekanntgabe der Empfänger von Datenübermittlungen und der Verwendungszwecke auch der übermittelten Daten würde die Behörde allerdings sich und die empfangende Behörde an die Einhaltung der genannten Zwecke weitgehend binden. Es ist aber die Frage – je nach Art der Daten – ob eine solche Bindung an einen für den Betroffenen erkennbaren Zweck nach Erlaß des Urteils nicht ohnehin in vielen Fällen angenommen werden muß. Es dürfte geboten sein, eine Zweckänderung, die mit einer Datenübermittlung verbunden wäre, unter dem Gesichtspunkt der Verhältnismäßigkeit ihrer Auswirkungen auf den Betroffenen zu überprüfen. Die Pflicht zur Prüfung nach diesem Grundsatz könnte schon jetzt beispielsweise bei Übermittlungen nach Art. 17 Abs. 1 BayDSG im Rahmen der Prüfung, ob die Daten zur „rechtmäßigen" Erfüllung „erforderlich" sind, im Wege der Auslegung angenommen werden.

Zu prüfen wäre, ob eine Benachrichtigung des Betroffenen erfolgen sollte, wenn mit einer Übermittlung eine Änderung des Nutzungszwecks der Daten verbunden ist, die, gemessen am Verhältnismäßigkeitsgrundsatz, problematisch sein könnte. Dies würde zwar der Forderung des Gerichts, daß die Bürger wissen müßten, wer was über sie weiß, entgegenkommen. Wegen des großen Verwaltungsaufwands muß aber wohl eher überlegt werden, ob eine unter dem Gesichtspunkt des Verhältnismäßigkeitsgrundsatzes problematische Datenübermittlung nicht zu unterlassen wäre (es sei denn sie wäre zwingend vorgeschrieben) und die datenanfordernde Behörde die Daten bei Betroffenen selbst zu erheben hätte. Eine solche Verfahrensweise ist z.B. vom Grundsatz her in § 93 (1)3 AO vorgesehen.

2.3.3. Abschottung von Datenverarbeitungsbereichen

Zur Abschottung von Datenverarbeitungsbereichen voneinander durch organisatorische und verfahrensrechtliche Vorkehrungen:

a) Zur Notwendigkeit der Abschottung:

Die Verwaltung muß z. B. den Hinweis auf die Notwendigkeit der Abschottung der Kommunalstatistik-Daten von Daten für andere Verwaltungsaufgaben der Kommune beachten (IV 4 b).

Ähnliche Unvereinbarkeiten wie zwischen Statistik und allgemeinen Verwaltungsdaten bestehen möglicherweise auch zwischen anderen Datenbereichen der Verwaltung. So wäre die Notwendigkeit der Abschottung zwischen Patienten-Daten und sonstigen Kommunalverwaltungsdaten, Sozialdaten und anderen Verwaltungsdaten und Daten der Sicherheitsbehörden gegenüber Daten anderer Behörden naheliegend: Teilweise besteht eine solche Abschottung ja bereits.

Ein weiterer Maßstab für konkrete Maßnahmen der informationellen Gewaltenteilung könnte sein, daß innerhalb von Bereichen, die nach außen hin abgeschottet sind, nicht so viele Informationen über einen Betroffenen vorhanden sein dürften, daß die Datenmenge den problematischen „Teilabbildern", also Persönlichkeitsprofilen, nahe käme. Als weiterer Schritt wäre zu überlegen, inwieweit innerhalb solcher Bereiche Verknüpfungen von Daten verschiedener Verwaltungsbereiche oder gemeinsame Datennutzungen in ihren Wirkungen unverhältnismäßig sein könnten und daher unterbleiben müßten und welche die angemessenen Mittel wären, sie zu verhindern.

b) Zur Art der Abschottung:

Für die Beantwortung der Frage, ob gemeinsam im automatisierten Verfahren gespeicherte Datenbestände verschiedener Behörden unter dem Gesichtspunkt der Verhinderung unzulässiger Nutzungsänderungen als voneinander hinreichend abgeschottet angesehen werden können, ist von Bedeutung, für wie zuverlässig einmal eingerichtete Zugriffsberechtigungen oder -sperren zu halten sind. Hierbei spielt auch der Aufwand eine Rol-

le, der erforderlich ist, um eingerichtete Zugriffsberechtigungen oder -sperren abzuändern oder aufzuheben.

Bei der rechtlichen Einordnung dieses Sachverhalts stellt sich die Frage, ob die datenschutzrechtliche Forderung der Herstellung und besonders der Erhaltung der korrekten Zugriffsberechtigungen lediglich auf der Forderung des Art. 15 BayDSG (entsprechend § 6 BDSG mit Anlage) beruht, die erforderlichen technischen und organisatorischen Maßnahmen der Datensicherung durchzuführen, oder ob hier auch Vorgaben auf Grund des Rechts auf informationelle Selbstbestimmung anzunehmen wären. Von Bedeutung ist dabei, daß die Verpflichtung zur Datensicherung aus Art. 15 BayDSG unter dem generellen Vorbehalt des Art. 15 Abs. 1 Satz 2 steht („erforderlich sind Maßnahmen nur, wenn ihr Aufwand in einem angemessenen Verhältnis zu dem angestrebten Schutzzweck steht"). Schutzzweck könnte nach der neuesten Rechtsprechung des Bundesverfassungsgerichts auch der Schutz vor einer Änderung des Nutzungszwecks der Daten als Folge ihrer Inanspruchnahme durch eine andere Dienststelle sein. Aus Art. 15 Abs. 1 S. 2 BayDSG ergibt sich aber, daß Maßnahmen, die beispielsweise finanziell nicht in einem angemessenen Verhältnis zu dem angestrebten Schutzzweck stehen würden, nicht erforderlich wären.

Nach dem Volkszählungsurteil ist davon auszugehen, daß Nutzungsänderungen, z.B. im Zuge des Zugriffs Dritter auf Daten, Einschränkungen des Persönlichkeitsrechts darstellen können. In diesem Falle müssen sie, soweit sie nicht bereits verfassungs- rechtlich bedenklich sind, durch Gesetz erlaubt sein und dürfen nur im Rahmen der gesetzlichen Zulassung vollzogen werden. Dem muß auch die Organisation der Datenverarbeitung Rechnung tragen. Das Bundesverfassungsgericht selbst hat organisatorische und verfahrensrechtliche Vorkehrungen gefordert, die der Gefahr einer Verletzung des Persönlichkeitsrechts entgegenwirken (Leitsatz 2).

Die Verarbeitung besonders schutzwürdiger Daten zusammen mit Daten aus dem Vollzug anderer Verwaltungsaufgaben (für andere Dienststellen) auf ein und derselben ADV-Anlage kann rechtlich daher nur als zulässig angesehen werden, wenn der Einsatz der verfügbaren organisatorischen und verfahrensmäßigen Mittel die Gefahr einer Verletzung des Persönlichkeitsrechts durch anderweite Nutzung hinreichend sicher ausschließt. Auf die Verfahrensvorschrift des Art. 26 Abs. 3 BayDSG sei in diesem Zusammenhang hingewiesen. Danach bedarf die Verarbeitung von personenbezogenen Daten aus verschiedenen Verwaltungszweigen auf einer ADV-Anlage der Zustimmung der beteiligten obersten Dienstbehörden.

Schon bisher war davon auszugehen, daß eine gemeinsame Verarbeitung von Daten unterschiedlicher Verwaltungsbereiche auf einer ADV-Anlage ohne jeden Zugriffsschutz unzulässig ist. Zu einer Abwägung zwischen Aufwand von Schutzmaßnahmen (Zugriffsschutz) und angestrebtem Schutzzweck im Rahmen von Art. 15 Abs. 1 Satz 2 BayDSG war insoweit nach dem Stand der Technik bereits kein Raum mehr.

Darüber hinaus ist aber zu klären, ob z.B. die gemeinsame Verarbeitung von Patientendaten (die der ärztlichen Schweigepflicht unterliegen) und sonstigen Verwaltungsdaten einer anderen Behörde auf derselben ADV-Anlage, oder auf verbundenen Rechnern, unter Einsatz von – u.U. abgestuftem – Paßwortschutz als hinreichend voneinander abgeschottet anzusehen ist. Hierbei ist auch der jeweilige Aufwand für eine Änderung oder Aufhebung des Paßwortschutzes zu bedenken. Ist er gering, und wäre eine Änderung nachträglich nicht feststellbar, könnte eine ausreichend zuverlässige Abschottung durch ADV-technische Maßnahmen kaum angenommen werden. Die Abschottung entspräche eher der Wirkung einer innerdienstlichen Weisung an das Personal, bestimmte Datenarten nicht gemeinsam zu nutzen, die durch – ansich zu Gebote stehende – ADV-Maßnahmen kaum unterstützt wäre. Mehr Sicherheit könnte im Einzelfall dagegen wohl die Verarbeitung der zu trennenden Datenbereiche (also z.B. Patienten- und sonstige Verwaltungsdaten) auf völlig getrennten Rechnern bieten, die keine hardwaremäßige Verbindung aufweisen.

Ein anderes Beispiel für Datenbereiche, die nach dem Volkszählungsurteil besonders sorgfältig getrennt zu verarbeiten wären, sind, wie oben erwähnt, Datenmengen, die bei gemeinsamer Verarbeitung verfassungsrechtlich unzulässige Bilder bzw. Teilabbilder der Person darstellen würden.

Dieser Überlegung kann wohl nicht in jedem Falle das Argument des Art. 15 Abs. 1 Satz 2 BayDSG entgegengesetzt werden, daß nämlich die Aufteilung von Datenbeständen auf hardwaremäßig getrennte Rechner wegen des finanziellen und organisatorischen Aufwands nicht in einem angemessenen Verhältnis zu dem angestrebten Schutzzweck stehe. Möglicherweise kann im Einzelfall der verfassungsrechtlichen Forderung, unzulässige Teilabbilder nicht herzustellen bzw. besonders sensitive Datenbestände gegen unzulässige Änderungen des Nutzungszwecks sicher abzuschirmen, keine andere Maßnahme aus dem Katalog des Art. 15 Abs. 2 hinreichend genügen.

### 3. Fortentwicklung des allgemeinen Datenschutzrechts (BDSG und BayDSG)

Auf den Referentenentwurf eines Änderungsgesetzes zum Bundesdatenschutzgesetz einzugehen, der meine Geschäftsstelle im Berichtsjahr beschäftigt hat, halte ich in diesem Tätigkeitsbericht nicht mehr für erforderlich. Das im Dezember ergangene Urteil des Bundesverfassungsgerichts zum Volkszählungsgesetz 1983 führt gerade auch für die Novellierung des Bundesdatenschutzgesetzes zu neuen Überlegungen, die in einem neuen Gesetzentwurf ihren Niederschlag finden sollen. Die Datenschutzbeauftragten der Länder und des Bundes und die Datenschutzkommission Rheinland-Pfalz hatten zu dem Referentenentwurf eine Stellungnahme ausgearbeitet, deren wesentliche Punkte gleichwohl von allgemeinem Interesse sein dürften. Die Stellungnahme vom 4.11.1983 ist als Anhang Nr. 4 zu diesem Bericht abgedruckt.

Meine zu dem Referentenentwurf gegenüber dem Bayer. Staatsministerium des Innern abgegebene Stellungnahme beschränkte sich auf einen mir wichtig erscheinenden Punkt, der in der Novellierungsdiskussion bisher nur eine Nebenrolle gespielt hatte, nämlich die Anpassung der Konzeption des Bundesdatenschutzgesetzes an die bereits eingetretene und zu erwartende Entwicklung der ADV-Technik.

Das Datenschutzgesetz hat die Aufgabe, Probleme, die durch moderne Datenverarbeitungstechniken für den Schutz der Persönlichkeit entstehen können, praktikabel zu lösen; so sollen auch die neuesten Formen der Datenverarbeitung grundsätzlich zum allgemeinen Nutzen in Privatwirtschaft und öffentlicher Verwaltung eingesetzt werden können. Es kann nicht Aufgabe des Datenschutzrechts sein, Fortschritt auf diesem Gebiet zu unterbinden, andererseits muß der Datenschutz als Korrelat zur Datenverarbeitung erkannt werden.

Gemessen an den vielfältigen Verwendungsmöglichkeiten der automatisierten Datenverarbeitung erscheint das gegenwärtige Bundesdatenschutzgesetz – auch die im Berichtsjahr vorgelegte Novelle hätte daran im Prinzip nicht viel geändert – überholt. Das BDSG geht von der Vorstellung aus, daß mit rechtlichen Regelungen über die Zulässigkeit der Speicherung und Übermittlung bestimmter einzelner Daten einzelner betroffener Personen ein wirksamer und angemessener Schutz vor unerwünschten Folgen der Anwendung automatisierter Datenverarbeitung möglich sei. Dies traf Anfang der siebziger Jahre, als die Konzeption des BDSG entstand, wohl zu. Das Wesen automatisierter Datenverarbeitung ist seither aber deutlicher geworden. Es besteht gerade nicht nur im Ermöglichen der Speicherung und Übermittlung einzelner Daten einzelner Betroffener; diese Möglichkeit bestand schon vor der Automatisierung, in manuellen Verfahren. Charakteristisch für automatisierte Datenverarbeitung einschließlich neuer Kommunikationswege, die durch „Neue Medien" eröffnet werden, ist dagegen die Möglichkeit, sehr große Mengen von Daten

- zu speichern, nach bestimmten Merkmalen abzugleichen und zu sortieren,
- zu übermitteln, zu verknüpfen, zusammenzuführen, zentral verfügbar und selektiert abrufbar zu halten.

Die Massendatenverarbeitung, die Bewältigung riesiger Informationsmengen ist das typische Merkmal der ADV. Hieran knüpft das Datenschutzgesetz jedoch Rechtsfolgen in nicht genügendem Maße. Dies gilt vor allem für die Zulässigkeitsbestimmungen. Die Vorschriften über die erforderlichen technischen und organisatorischen Maßnahmen setzen jeweils die rechtliche Befugnis, zum Beispiel zur Benützung von DV-Systemen, zum Zugriff auf Daten oder zu ihrer Kenntnisnahme, Veränderung oder Löschung voraus. Sie setzen sich jedoch nicht damit auseinander, daß die automatisierte Datenverarbeitung

- die Nutzbarkeit personenbezogener Daten für andere Verwendungszwecke als den ursprünglichen Zweck durch die verfügbaren Abgleichs-, Sortier-, Verknüpfungs- und Übermittlungstechniken und die Abrufbarkeit im Direktzugriff stark erhöht wird, daß dadurch ausgelöst,
- der „psychische Druck öffentlicher Anteilnahme", der die freie Entfaltung der Persönlichkeit zu hemmen vermag, weil Betroffene sich zunehmend so verhalten werden, daß große Datensammlungen nur (vermeintlich) Positives über sie enthalten, verstärkt wird und daß
- die Möglichkeiten, viele Informationen zu nutzen, immer ungleichmäßiger verteilt werden, weil relativ wenige, die den Zugang zu großen EDV-Systemen besitzen, immer mehr über erhebliche Teile der Bevölkerung wissen und nutzen können.

In den nächsten Jahren werden außerdem Entwicklungen eintreten, auf die das Bundesdatenschutzgesetz aus der Sicht des Persönlichkeitsschutzes, aber auch der Praktikabilität seiner Regelungen, angemessen reagieren müßte:

- Beim Medium „Bildschirmtext" hat sich bereits gezeigt, daß das Datenschutzgesetz keine zutreffenden Anknüpfungspunkte und Rechtsfolgen enthielt, so daß im Staatsvertrag und den Ausführungsgesetzen Spezialregelungen erforderlich waren. Weitere Kommunikationsformen, deren Entwicklung zum Teil bereits weit gediehen ist, werden zusätzliche Reaktionen des Gesetzgebers erfordern. Auch hier sollte meines Erachtens der Versuch unternommen werden, im allgemeinen Datenschutzrecht grundsätzliche rechtliche Positionen als notwendige Korrektive festzuschreiben.
- Die Ausbreitung der „personal computer" oder „home computer" wird so stark zunehmen, daß die Regelungen des BDSG, die nach dem Wortlaut des Gesetzes auch für diese Geräte gelten, beispielsweise über die Benachrichtigung der Personen, über die Daten gespeichert sind, nicht mehr vollziehbar sein werden. Auch könnte die Datenschutzkontrolle über diese im privaten und gewerblichen Bereich verwendeten kleinen ADV-Anlagen kaum noch effektiv sein.
- Die Weiterentwicklung der Groß-EDV wird zu nahezu unbegrenzten Speicherkapazitäten und zu stark vereinfachtem Umgang mit den Computern führen. Über die sog. Mustererkennung werden Möglichkeiten entstehen, Bilder maschinell auszuwerten. Es können bei vertretbarem finanziellem Aufwand immer noch größere personenbezogene Datensammlungen entstehen. Dabei kann die Quantität der Daten unter Berücksichtigung der besseren Auswertungsmöglichkeiten zu einer so starken Verbesserung des Informationsinhaltes führen, daß die Quantität in eine neue Qualität umschlägt.

Gerade durch die Weiterentwicklung der Datenbank-Software wird ein bisher schon zu beobachtendes Phänomen verstärkt: Personenbezogene Daten werden immer leichter technisch und organisatorisch beliebig verbindbar gespeichert, so daß bestehende rechtliche Zuständigkeitsgrenzen nicht mehr identische und ausschließliche Kenntnisnahme- und Nutzungsmöglichkeiten über die erforderlichen Informationen entsprächen, wie zu der Zeit, als die jeweiligen Gesetze über die Zuständigkeiten erlassen wurden. Eine Organisation der Daten und ihrer Zuordnung zu Dienststellen, die der rechtlich vorgegebenen Zuständigkeit völlig widerspräche, würde nicht mehr Aufwand erfordern, als die Organisation der rechtmäßigen Nutzung. Die gesamte Menge der für die verschiedenen, mit einer ADV-Anlage unterstützten Behörden zu speichernden Daten könnte u.U. zu jedem Betroffenen gemeinsam gespeichert werden. Sie würde dann nur noch durch die Generierung der entsprechenden Zugriffsberechtigungen und -beschränkungen strukturiert. Die „informationelle Gewaltenteilung" auch zwischen Behördenbereichen, die durch feste Zuteilung von Zuständigkeiten und auch von Informationen an die verschiedenen Behörden gesichert war, könnte dadurch an Wirkung erheblich verlieren. Die Struktur der Behörden selbst könnte sich außerdem von der Informationsbasis her stark verändern, ohne daß dies notwendig dem Nichtfachmann oder gar dem Bürger frühzeitig erkennbar würde. Angesichts der für ADV-Anlagen, Software und Personal aufgewandten Mittel ist nicht sicher, daß die erforderliche Anpassung zwischen rechtlichen Vorgaben und tatsächlicher Organisation zu Änderungen im ADV-Bereich führen würde. Der Gesetzgeber sähe sich wohl in der Rolle des Notars bereits „programmierter" Strukturen.

All dies würde die „Undurchsichtigkeit der Speicherung und Verwendung von Daten unter den Bedingungen der automatisierten Datenverarbeitung" (BVerfG) bei der Mehrheit der Bevölkerung erhöhen. Ich halte es daher für eine Aufgabe des Bundesdatenschutzgesetzes, jedenfalls der jetzt schon erkennbaren Entwicklung der automatisierten Datenverarbeitung soweit Rechnung zu tragen, daß sich die Diskussion um automatisierte Verwaltungsverfahren wieder der Einhaltung der Datenschutzgesetze zuwendet und die Frage nach der Verfassungsmäßigkeit von DV-Verfahren und damit der Verfassungsmäßigkeit des Handelns von Behörden in diesem Bereich nicht mehr gestellt zu werden braucht.

In meiner Stellungnahme habe ich zu bedenken gegeben, daß auch die Einführung von Prüfverfahren für größere ADV-Verfahren im Bundesdatenschutzgesetz zu einer rechtzeitigen Klärung möglicher Folgen des Verfahrens führen und Emotionen abbauen könnte. Eine gründliche, systematische Erörterung der Risiken größerer ADV-Systeme wird gegenwärtig vor deren Einführung meines Wissens nicht durchgeführt. Ein bemerkenswerter Ansatz in dieser Richtung ist allerdings in Art. 26 Abs. 2 und 4 des Bayer. Datenschutzgesetzes enthalten. Dort ist eine besondere datenschutzrechtliche Freigabe und deren Mitteilung an den Landesbeauftragten für den Datenschutz vorgesehen. Allerdings ist auch dieses Verfahren, nicht zuletzt angesichts der beschränkten Personalkapazität des Landesbeauftragten für den Datenschutz, kein hinreichender Ersatz für eine gründliche Abklärung der Folgen größerer neuer ADV-Verfahren im Sinne einer Diskussion von Technologie-Folgen.

Ich habe in meiner Stellungnahme vorgeschlagen, umgehend eine umfassende Bestandsaufnahme der zum BDSG zu lösenden spezifischen, durch die technische Entwicklung bedingten ADV-Probleme zu erstellen, die notwendigen Gutachten in Auftrag zu geben und Anhörungen möglichst bald zu beginnen. Ich habe auch die Sorge geäußert, daß ein kurzfristig vorgelegter Novellierungsvorschlag bewirken könnte, daß in absehbarer Zeit nicht mehr damit zu rechnen sei, daß die Vorarbeiten für die notwendige Anpassung des BDSG an die fortgeschrittene Technik in einem weiteren Gesetzentwurf in Angriff genommen würde.

Hierzu hat sich allerdings durch das Urteil des Bundesverfassungsgerichts zum Volkszählungsgesetz teilweise eine neue Situation ergeben. Es muß jetzt möglichst bald geprüft werden, inwieweit insbesondere die bisherigen Zulässigkeitsvorschriften des Bundesdatenschutzgesetzes den Anforderungen des Urteils noch entsprechen.

## 4. Bericht zur Datenschutzkontrolle im rechtlichen Bereich

### 4.1. Neue Medien

Unter dem Stichwort „Neue Medien" verbirgt sich ein ständig wachsendes Bündel neuer Kommunikationstechniken. Neben Bildschirmtext und Kabelrundfunk sind inzwischen auch die Fernwirkdienste von der Diskussion in einer breiteren Öffentlichkeit erfaßt. Daneben sind noch Satelliten-Fernsehen, Videotext und weitere von der Dt. Bundespost in der Entwicklung befindliche Nutzungsformen, insbesondere der Aufbau eines digitalisierten Fernmeldenetzes, von Bedeutung. Aus datenschutzrechtlicher Sicht habe ich mich vorrangig mit Bildschirmtext, dem Kabelpilotprojekt München und den Fernwirkdiensten auseinandergesetzt, weil hier teilweise sensible personenbezogene Daten anfallen und die Einführung bzw. Erprobung dieser Medien unmittelbar bevorsteht.

Auf meine Ausführungen im 4. und 5. Tätigkeitsbericht nehme ich Bezug.

#### 4.1.1. Bildschirmtext

##### 4.1.1.1. Gesetzliche Regelungen

Bildschirmtext gestattet umfangreiche Nutzungsmöglichkeiten durch Abruf von Informationsangeboten aus den Bildschirmtextzentralen und durch die Kommunikation mit externen Rechnern sowie mit der Möglichkeit, Mitteilungen an andere zu übersenden. Weil alle bei dieser Kommunikation anfallenden personenbezogenen Informationen über die technischen Einrichtungen fließen, die zur Nutzung von Bildschirmtext bereitgestellt werden, mit diesen dort angefallenen Daten die Gebühren abgerechnet werden und somit bei diesen Einrichtungen ein umfangreiches personenbezogenes Datenpotential entstehen kann, ist dem Schutz dieser Daten besonderes Augenmerk zu schenken. Die Ministerpräsidenten der Länder haben dieses Problem erkannt und im Bildschirmtext-Staatsvertrag, den sie am 18. März 1983 unterzeichnet haben, eine bereichsspezifische Datenschutzregelung aufgenommen. Diese Bestimmung setzt der Verarbeitung personenbezogener Daten durch den Betreiber der Bildschirmtextzentrale sowie durch die Anbieter enge Grenzen. Zu Einzelheiten verweise ich insbesondere auf Art. 9 Bildschirmtext-Staatsvertrag sowie meine Ausführungen im 5. Tätigkeitsbericht (S. 10 ff.).

Der Landtag des Freistaates Bayern hat bei Stimmenthaltung der SPD-Fraktion mit Beschluß vom 19. Juli 1983 dem Staatsvertrag über Bildschirmtext zugestimmt. In Kraft getreten ist der Staatsvertrag nach seinem Art. 16 Abs. 2 am 1. September 1983 in den Ländern Bayern, Berlin, Hessen, Nordrhein-Westfalen und Schleswig-Holstein. Zwischenzeitlich haben alle Länder dem Staatsvertrag zugestimmt. Ebenfalls am 1. September 1983 ist das Gesetz zur Ausführung des Staatsvertrages über Bildschirmtext in Kraft getreten. Dieses Gesetz regelt die Zuständigkeiten zur Überwachung der wesentlichen Bestimmungen des Bildschirmtext-Staatsvertrages und legt die Pflichten der Anbieter und Betreiber gegenüber den Kontrollinstanzen fest. Während zur zuständigen Verwaltungsbehörde im Sinne von Art. 13 des Bildschirmtext-Staatsvertrages die Regierungen bestimmt worden sind – dies entspricht der Regelung hinsichtlich der Datenschutzkontrollen über nichtöffentliche Stellen nach dem Bundesdatenschutzgesetz - überwacht bei den bayerischen öffentlichen Stellen die Einhaltung der Datenschutzvorschriften des Bildschirmtext-Staatsvertrages der Bayer. Landesbeauftragte für den Datenschutz. Weil beim Einsatz des Mediums „Bildschirmtext" im öffentlichen wie im nichtöffentlichen Bereich im wesentlichen die gleichen Probleme auftreten, verlangt das Ausführungsgesetz eine enge Zusammenarbeit zwischen den Regierungen und dem Landesbeauftragten für den Datenschutz, die über die vergleichbare Regelung im Bayer. Datenschutzgesetz (Art. 31 Abs. 3) hinausgeht.

##### 4.1.1.2. Betriebsaufnahme von Bildschirmtext

Die bundesweite Einführung von Bildschirmtext nach dem neuen CEPT-Standard, die ursprünglich für September 1983 geplant war, ist auf Juli 1984 verschoben worden.

Stattdessen hat die Bundespost eine Übergangstechnik auf der Basis der Versuchstechnik zur Verfügung gestellt, die aber zumindest schon teilweise den Leistungsumfang der neuen Technik aufweist. Seit September 1983 können etwa 5.000 neue Teilnehmer den Anschluß an die Datenbank der Berliner Bildschirmtextzentrale erhalten. Großsammelanschlüsse, die den Zugang nach Berlin eröffnen, sind in einer Reihe deutscher Städte eingerichtet worden. Damit kann von diesen Städten aus mit dem Bildschirmtext-Rechner in Berlin zur Ortsgebühr verkehrt werden. Im größeren Umfang können neue Anbieter und neue Teilnehmer erst nach der endgültigen Inbetriebnahme ab Juli 1984 angeschlossen werden. Bis dahin bleiben auch die für die Pilotprojekte in Berlin und Düsseldorf eingesetzten Bildschirmtextzentralen in Betrieb, die noch mit der alten Technik nach dem sog. PRESTEL-Standard arbeiten.

Neben diesen technischen Schwierigkeiten der Einführung des bundesweiten Bildschirmtext-Betriebes waren auch rechtliche Probleme in der Übergangsphase vom Versuch- zum Echtbetrieb zu beachten. Mit dem Inkrafttreten des Bildschirmtext-Staatsvertrages in den Ländern Berlin und Nordrhein-Westfalen sind die dortigen Versuchsgesetze außer Kraft getreten. Damit änderte sich auch die zuständige Verwaltungsbehörde, die für die Überwachung der Einhaltung der Rechtsvorschriften bei Bildschirmtext zuständig ist. Für die in Berlin und Düsseldorf angeschlossenen Anbieter war nach dem 1.9.1983 nicht mehr die nach den dortigen Versuchsgesetzen zuständige Behörde für jeweils alle dort angeschlossenen Anbieter zuständig, sondern entsprechend der Regelung des Staatsvertrages die jeweilige Sitzbehörde des Anbieters. Das bedeutet, daß nach diesem Stichtag ein Teil der Anbieter, die ihren Sitz in Ländern haben, in denen der Staatsvertrag noch nicht verabschiedet und ein Bildschirmtext-Ausführungsgesetz noch nicht erlassen war, von keiner bereichsspezifischen Bildschirmtext-Regelung erfaßt gewesen ist. Für Bayern hat es eine solche Rechtslücke allerdings nicht gegeben, weil, wie erwähnt, auch in Bayern der Bildschirmtext-Staatsvertrag bereits zum 1.9.1983 in Kraft getreten ist.

4.1.1.3. Probleme der Umsetzung der Datenschutzregelung im Staatsvertrag durch die Dt. Bundespost

Hinsichtlich der Frage, ob die Datenschutzbestimmung des Bildschirmtext-Staatsvertrages auch für die Dt. Bundespost in ihrer Funktion als Betreiber gilt, bestanden zwischen den Ministerpräsidenten und der Dt. Bundespost von Anfang an Meinungsverschiedenheiten. Die Dt. Bundespost ist der Auffassung, daß sie durch den Staatsvertrag aus kompetenz-rechtlichen Gründen nicht verpflichtet werden kann. Demgegenüber halten die Länder die Post in ihrer Funktion als Betreiber durch Art. 9 Bildschirmtext-Staatsvertrag (Btx-StV) für gebunden. Bei der Formulierung der Datenschutzbestimmung im Staatsvertrag waren sie davon ausgegangen, daß die Dt. Bundespost jedenfalls nach den in Art. 9 enthaltenen Grundsätzen verfahren und für ihren Bereich entsprechende Vorschriften erlassen werde. Die Dt. Bundespost hat hierzu den Ländern schriftlich mitgeteilt, daß sie „nach den in Art. 9 enthaltenen Grundsätzen verfahren und für ihren Bereich entsprechende Vorschriften" vorsehen werde.

Regelungsdefizit

Zwar hat die Dt. Bundespost zwischenzeitlich in die Fernmeldeordnung in der Fassung der 22. Änderungsverordnung einige Regelungen zu Bildschirmtext aufgenommen. Ein Vergleich dieser Regelungen mit der Datenschutzvorschrift des Bildschirmtext-Staatsvertrages macht jedoch Defizite der Postregelung deutlich:

Während beispielsweise nach Art. 9 Abs. 3 Satz 1 Btx-StV die Speicherung der Abrechungsdaten darauf angelegt sein muß, daß „Zeitpunkt, Dauer, Art, Inhalt und Häufigkeit bestimmter, von den einzelnen Teilnehmern in Anspruch genommener Angebote nicht erkennbar sind", bestimmt § 13 Abs. 12 Satz 4 Fernmeldeordnung, daß zu den Abrechnungsdaten (Vergütungsdaten) „weder die Nummer noch der Inhalt einer abgerufenen Bildschirmtextseite gehören". Damit wird zumindest durch die Fernmeldeordung nicht ausgeschlossen, daß Zeitpunkt, Dauer und Häufigkeit bestimmter, entgeltpflichtiger in Anspruch genommener Angebote von der Dt. Bundespost als Betreiber gespeichert werden dürfen. Art und Umfang der Speicherung der Abrechnungsdaten sind aus datenschutzrechtlicher Sicht deshalb von besonderer Bedeutung, weil aus ihnen möglicherweise Rückschlüsse auf das Benutzerverhalten des einzelnen Teilnehmers gezogen werden können.

Weiterhin fehlt eine eindeutige Bestimmung in der Fernmeldeordnung, welche Abrechnungsdaten im Streitfalle dem Anbieter übermittelt werden. Die jetzige Formulierung, wonach „die rückständigen Vergütungen sowie die für die Durchsetzung des Anspruchs erforderlichen Vergütungsdaten .... im Rahmen der technischen und betrieblichen Möglichkeiten der Dt. Bundespost den jeweiligen Anbietern oder deren Empfangsbevollmächtigten (§ 10 Abs. 8) mitgeteilt" werden, ist viel zu allgemein, um die Datenschutzbelange der betroffenen Teilnehmer ausreichend zu gewährleisten.

Die Dt. Bundespost hat auf die Forderung der Datenschutzbeauftragten, ausreichende Rechtsvorschriften zu erlassen, erklärt, daß es offengeblieben sei, ob sie die materiellen Anforderungen des Art. 9 Btx-StV durch verordnungsmäßige Regelung, Verwaltungsanweisungen oder durch bloße Vorkehrungen im technisch-betrieblichen System zu gewährleisten habe. Hierzu ist jedoch folgendes festzuhalten:

Notwendigkeit einer gesetzlichen Regelung

Angesichts der durch den Betrieb des Bildschirmtextsystems möglichen Gefährdungen für die Privatsphäre der Bürger sind nach der Rechtsprechung des Bundesverfassungerichts durch Gesetz diejenigen organisatorischen und verfahrensrechtlichen Vorkehrungen zu treffen, welche diesen Gefahren einer Verletzung des Persönlichkeitsrechts entgegenwirken. Daher ist es auch den übrigen Landesbeauftragten für den Datenschutz schwer verständlich, daß die Dt. Bundespost derzeit offenbar nicht bereit ist, entweder den Staatsvertrag für sich gelten zu lassen oder entsprechende gesetzliche Regelungen zu schaffen. Spätestens seit dem Urteil des Bundesverfassungsgerichts zur Volkszählung ist die vorgenannte schriftliche Erklärung der Dt. Bundespost, daß sie neben Verwaltungsanweisungen auch Vorschriften erlassen werde, in verfassungskonformer Weise nur als Verpflichtung zu verstehen, Rechtsnormen zu schaffen. Weil die Dt. Bundespost den Staatsvertrag aber nicht unmittelbar für sich gelten läßt, bestehen nun Regelungslücken im Bundesrecht. Offensichtlich würdigt die Dt. Bundespost nicht im ausreichenden Maße, daß die Ministerpräsidenten mit der verschärften Datenschutzregelung im Staatsvertrag den erhöhten Gefahren begegnen und den

eventuell vorhandenen Ängsten der Bevölkerung Rechung tragen wollten.

Ich betone deshalb ausdrücklich, daß eine Regelung des Datenschutzes bei Bildschirmtext sich nicht in einer einseitigen Verpflichtungserklärung der Dt. Bundespost gegenüber den Ländern, in Verwaltungsanweisungen oder in Vorkehrungen im technisch-betrieblichen System erschöpfen kann. Selbst das Fernmeldegeheimnis, dessen Reichweite auf Bildschirmtext ohnehin nicht unbestritten ist, befreit nicht von der Notwendigkeit, zusätzliche grundrechtssichernde gesetzliche Regelungen zu schaffen, die den besonderen Gefahren von Bildschirmtext begegnen.

Bei der Diskussion des Bildschirmtext-Staatsvertrages und des Ausführungsgesetzes in den Ausschüssen des Bayer. Landtages sowie des Bayer. Senates habe ich auf entsprechende Fragen die Datenschutzregelung im Bildschirmtext-Staatsvertrag als grundsätzlich ausreichend bezeichnet. Bei diesen Erklärungen hatte ich darauf vertraut, daß die Dt. Bundespost die den Ministerpräsidenten gegenüber abgegebene Verpflichtung einhält und ungeachtet kompetenzrechtlicher Meinungsverschiedenheiten alles tut, was für eine effektive Umsetzung der Bestimmungen des Staatsvertrages notwendig ist. Durch diese Erklärungen und meine Mitwirkung bei der Schaffung der Datenschutzvorschrift im Staatsvertrag habe ich gegenüber Regierung, Landtag und Senat eine Verantwortung für eine ausreichende Berücksichtigung des Persönlichkeitsschutzes bei Einführung von Bildschirmtext übernommen. Angesichts dieser Verantwortung habe ich auch den Bayer. Ministerpräsidenten erst kürzlich schriftlich gebeten, mich insbesondere in der Forderung nach ausreichenden rechtlichen Regelungen für den Betrieb von Bildschirmtext durch die Dt. Bundespost zu unterstützen.

#### 4.1.1.4. Datenschutzfragen beim technischen System-Konzept der Dt. Bundespost

Aus der eben genannten Verantwortung und der Zuständigkeit für die Überwachung der Einhaltung der Datenschutzbestimmungen bei Anwendung des Bildschirmtextes in Bayern, habe ich mich auch um Informationen über das technische System-Konzept von Bildschirmtext bemüht. Nachdem die Dt. Bundespost mit Informationen gegenüber den Landesbeauftragten für den Datenschutz zunächst sehr zurückhaltend gewesen war, hat sie zwischenzeitlich auf einer besonderen Informationsveranstaltung das System-Konzept mündlich erörtert und einige Unterlagen ausgehändigt. Allerdings stehen noch einige Materialien aus, die erst eine abschließende datenschutzrechtliche Bewertung des System-Konzepts der Dt. Bundespost gestatten würden.

Ganz ohne Zweifel ist anzuerkennen, daß sich aus dem bisher bekanntgewordenen System-Konzept der Dt. Bundespost ergibt, daß die Post gewillt ist, die Datenschutzbelange der Teilnehmer und Anbieter zu berücksichtigen. So hat die Bundespost beispielsweise Maßnahmen ergriffen, die verhindern sollen, daß der Teilnehmer seine Identität unbeabsichtigt an den Anbieter preisgibt. Der Anbieter könnte nämlich die von der Dt. Bundespost eingeblendeten personenbezogenen Daten des Teilnehmers auf dessen Bildschirm für den Teilnehmer unlesbar machen, indem er den Hintergrund des Bildschirms in gleicher Farbe wie die eingeblendeten Teilnehmerdaten gestaltet. Um ein solches Vorgehen des Anbieters nach Möglichkeit auszuschließen, hat die Bundespost vorgesehen, daß Seiten, die personenbezogene Daten enthalten, grundsätzlich nur mit „19" abgesandt werden können. Für den Teilnehmer ist es in diesem Zusammenhang also wichtig zu wissen, daß bei einem Absenden mit „19" personenbezogene Daten übermittelt werden können. Weiter blendet die Bundespost den Buchstaben „P" auf den Bildschirm ein, wenn die Dt. Bundespost personenbezogene Daten auf dem Bildschirm einstellt. Dieses Zeichen „P" ist durch den Anbieter nicht verdeckbar. Außerdem hat die Dt. Bundespost vorgeschrieben, daß sämtliche Endgeräte eine sogenannte „weiße Taste" besitzen müssen, deren Betätigung dazu führt, daß der Bildschirm in Schwarz-WeißDarstellung erscheint. In dieser Darstellung ist es aber dem Anbieter nicht möglich, eingeblendete personenbezogene Daten unlesbar zu machen.

Allerdings hat die bisherige Systemgestaltung ein nicht unerhebliches Datenschutzproblem aufgeworfen: Wie oben bemerkt, muß nach Art. 9 Abs. 3 die Speicherung der Abrechnungsdaten so angelegt sein, daß Zeitpunkt, Dauer, Art, Inhalt und Häufigkeit bestimmter von den einzelnen Teilnehmern in Anspruch genommenen Angebote nicht erkennbar sind. Tatsächlich speichert die Dt. Bundespost bei entgeltpflichtigem Seitenabruf auch nicht die Tatsache, daß eine bestimmte entgeltpflichtige Seite abgerufen worden ist. Aber die Dt. Bundespost speichert in ihrem „Entgeltsatz" neben dem Zeitpunkt der „Sitzung" (Verbindung mit der Bildschirmtextzentrale oder Bildschirmtextvermittlungsstelle) auch die Leitseite, unter der eine entgeltpflichtige Seite abgerufen worden ist. Dies mag zunächst datenschutzrechtlich nicht von Belang sein, da eine Leitseite keinen unmittelbaren Rückschluß auf die tatsächlich abgerufene Einzelseite zulassen muß. Dabei muß man jedoch wissen, daß der einzelne Anbieter sein Angebot schon heute unter 30 Leitseiten aufteilen kann. Nach einer weiteren Ausbaustufe soll nach Angaben der Dt. Bundespost die Anzahl der möglichen Leitseiten pro Anbieter auf über 60 erhöht werden. Damit besteht aber die Möglichkeit, daß der einzelne Anbieter bestimmte Angebotsgruppen jeweils unter einer Leitseite zusammenfaßt. Geschieht dies, kann sich bereits aus der Speicherung der Leitseite ein Rückschluß auf „Art" oder „Inhalt" bestimmter von den Teilnehmern in Anspruch genommenen Angebote ergeben. Zwar übermittelt die Dt. Bundespost selbst bei Nichtzahlung der Entgelte durch den Teilnehmer dem Anbieter nur Namen, Anschrift des Teilnehmers und den ausstehenden Geldbetrag, nicht aber die Leitseite, doch ist dies zum einen, wie oben bemerkt, durch die derzeitige Fassung der Fernmeldeordnung nicht festgeschrieben. Außerdem wären zumindest durch Auswertung der Daten bei der Bundespost entsprechende Rückschlüsse auf das Teilnehmerverhalten möglich. Wenn ich auch der Dt. Bundespost nicht unterstelle, daß sie ihrerseits die entsprechenden Daten auswertet, so ist doch weiter zu bedenken, daß ein privater Betreiber – solche sind nach dem Bildschirmtext-Staatsvertrag grundsätzlich denkbar – nach dem gleichen System-Konzept der Dt. Bundespost verfahren und seinerseits entsprechende Auswertungen vornehmen könnte. Würde im Hinblick auf Art. 9 Abs. 3 Btx-StV die Dt. Bundespost insoweit nicht beanstandet, könnte wohl auch einem privaten Betreiber, der das gleiche System-Konzept verwendet, diese Bestimmung nicht entgegengehalten werden.

Neben dieser Datenschutzproblematik sind noch weitere Punkte des System-Konzepts aus der Sicht des Daten-

schutzes zumindest diskus- sionsbedürftig. Ich hoffe, daß die Dt. Bundespost mich über die technischen Komponenten des Bildschirmtextsystems fortlaufend und umfassend informiert. Dies verlangt schon die enge Verflechtung von Netz- und Nutzungsbereich. Auch in diesem Zusammenhang ist zu berücksichtigen, daß nach Ansicht des Bundesverfassungsgerichts die Kontrolle der Datenverarbeitung durch unabhängige Datenschutzinstanzen wesentliche Voraussetzung eines wirksamen Grundrechtsschutzes ist.

Als Resümee der derzeitigen Umsetzung der Datenschutzvorschriften des Bildschirmtext-Staatsvertrages durch die Dt. Bundespost läßt sich also zweierlei festhalten: Auch im Bundesbereich sind ausreichende Rechtsvorschriften zu schaffen, die den materiellen Anforderungen des Art. 9 Btx-StV zumindest entsprechen. Weiterhin ist auch das System-Konzept der Dt. Bundespost so zu gestalten, daß die Datenschutzanforderungen verwirklicht werden.

4.1.1.5. Erste Prüferfahrungen bei Bildschirmtext

- Ein Versandhaus hatte vom Teilnehmer verlangt, seine Personalien bereits abzusenden, bevor er in den eigentlichen Bestelldienst eingetreten war. Das Versandhaus hatte hier die Ansicht vertreten, daß es selbst über die Dialog-Struktur bei Bestelldiensten bestimmen können müsse. Mit dem Versandhaus wurde vereinbart, daß der Teilnehmer erst bei Beginn des Bestelldienstes zur Übersendung seiner Personalien aufgefordert werden dürfe und daß die Personalien des Teilnehmers unmittelbar gelöscht werden, wenn der Dialog zwischen Teilnehmer und Versandhaus ohne Bestellung abgeschlossen wird.
- Eine bayerische Fremdenverkehrsgemeinde, die ein Gewinnspiel über Bildschirmtext veranstaltet hatte, hatte die Gewinner dieses Gewinnspiels, ohne diese um ihre Einwilligung zu befragen, in ihr Bildschirmtextangebot aufgenommen. Die Fremdenverkehrsgemeinde hat zwischenzeitlich meinen Bedenken Rechnung getragen.
- Im Bildschirmtextangebot eines Universitäts-Instituts waren nicht nur dessen Leiter, sondern auch die Sekretärinnen und wissenschaftliche Mitarbeiter namentlich aufgenommen, wobei bei letzteren noch deren Arbeitsschwerpunkt genannt war. Ich habe deutlich gemacht, daß derartige Angaben über Mitarbeiter nur mit deren ausdrücklicher Einwilligung in Bildschirmtext eingestellt werden dürfen.
- Noch ungeklärte Datenschutzfragen treten auf, wenn Sparkassen ihre Dienste über Bildschirmtext anbieten. Diskussionsbedürftige Fragen sind hier der Umfang der Datenerhebung, die Angabe des Überweisungszweckes auf dem Bildschirmtextformular, die Erhebung der System-Nummer auf der Antwortseite der Sparkasse und die Tatsache, daß über ein zentrales Rechenzentrum der Sparkassen in Duisburg – also bei einem weiteren Rechenzentrum – ein paralleler Datensatz über den Teilnehmer geführt wird. Dabei ist zu bemerken, daß dieser Bildschirmtextbetrieb der Sparkasse noch weitgehend Versuchscharakter hat.
- Im übrigen ist mir bekanntgeworden, daß Probleme hauptsächlich bei sog. „Kleinanbietern" auftreten. Teilweise beschimpfen sich Anbieter gegenseitig über Bildschirmtext und stellen beleidigende Briefe in ihr Angebot ein, so daß sie jedem Teilnehmer zugänglich sind. Manche Anbieter wollen sich der Verantwortung möglicherweise dadurch entziehen, daß sie sich als „Unteranbieter" bezeichnen und hinsichtlich rechtlicher Konsequenzen auf „einen Oberanbieter" verweisen.
- Bisher nicht aus Bayern, jedoch aus einem anderen Bundesland sind mir Probleme bekanntgeworden, die durch die Verwendung von Kleinrechnern als Bildschirmtext-Endgeräte auftreten können. Hier gibt es offensichtlich Möglichkeiten, gegen den Willen eines Teilnehmers Daten abzurufen oder diesen unbewußt zum Abruf entgeltpflichtiger Seiten zu veranlassen.

Im Zusammenhang mit der Kontrolltätigkeit möchte ich noch auf ein weiteres Problem aufmerksam machen. Die Kontrolltätigkeit durch den Bayer. Datenschutzbeauftragten – gleiches gilt für alle anderen Überwachungsinstanzen – kann zu nicht unerheblichen Kosten allein dadurch führen, daß neben den zu bezahlenden Fernmeldegebühren auch das Entgelt für die zu Prüfungszwecken abgerufenen entgeltpflichtigen Seiten gezahlt werden muß. Dies unterscheidet sich von der sonstigen Überwachungstätigkeit der Behörden. Weil es jedem Anbieter möglich ist, pro Seite ein Entgelt von 9,99 DM zu verlangen, könnte eine effektive Überwachung schnell an Kostenproblemen scheitern.

4.1.2. Kabelkommunikation

4.1.2.1. Kabelpilotprojekt

Zum 1. April 1984 hat die Münchner Pilot-Gesellschaft für Kabel-Kommunikation mbH (MPK) den Sendebetrieb aufgenommen. Über Breitbandkabel bietet die MPK derzeit neben den ortsüblichen Programmen (ARD, ZDF, BR III, ORF I, ORF II) die herangeführten Programme des Dritten Programms der Sendekette Südwest-Funk, Süddeutscher Rundfunk, Saarländischer Rundfunk sowie der Schweizer Rundfunkgesellschaft (1. Programm) und 4 Satellitenprogramme an. Außerdem werden 6 neue Programme, darunter Kabeltext/Telezeitung als neue Programme angeboten. Im Hörfunkbereich sind 21 Programme zu empfangen. Weitere Programme sind in Kürze zu erwarten, so auch ein sog. „Spielfilmkanal". Außerdem werden gegen zusätzliches Entgelt Telespiele, Videospiele und ein sog. „Tele-Club" angeboten. Auch die Zahl der Textangebote wird steigen.

Zum Kabelpilotprojekt und den datenschutzrechtlichen Fragen verweise ich auf meinen 4. und 5. Tätigkeitsbericht.

4.1.2.2. Neue Risiken

Zum Teil wiederholend und zum Teil ergänzend zu meinen Ausführungen im 4. und 5. Tätigkeitsbericht darf ich zu den Datenschutzaspekten der Kabelkommunikation noch folgendes vortragen:

Die Benutzung der Kabelmedien durch den Bürger weist im Vergleich zur Kommunikation über die herkömmlichen Medien die (schon bei Bildschirmtext festgestellte) Besonderheit auf, daß die Tatsache des Kommunikationsvorganges und teilweise auch der Inhalt der Kommunikation jedenfalls während der Dauer des Kommunikationsvorganges auf technischen Einrichtungen festgehalten sind. Die neuen Gefahren für die Privatsphäre, denen der Datenschutz sein Augenmerk zuwenden muß, liegen demnach in erster Linie in der technisch grundsätzlich möglichen umfassenden Sammlung personenbezogener Daten in den technischen Einrichtungen, welche zur Vermittlung von Rundfunksendungen und zur Nutzung von anderen Kabeldiensten, wie etwa von Textdiensten, bereit gestellt werden. Über diese technischen Einrichtungen werden die Rundfunksendun-

gen vermittelt und wird die vollständige Kommunikation zwischen den Anbietern von Diensten und den diese nutzenden Teilnehmern abgewickelt. Des weiteren gehen über technische Einrichtungen alle über die anderen Kabeldienste abzuwickelnde Angebotsforderungen und fließen nach Verwirklichung des Rückkanals alle zwischen Teilnehmer und Anbieter ausgetauschten Daten. Zumindest teilweise fallen über diese Einrichtungen auch die für die Gebührenabrechnung notwendigen Informationen an. Technisch wäre es zumindest möglich, aus diesen dabei angefallenen Daten Rückschlüsse auf die Interessengebiete des einzelnen Teilnehmers zu ziehen. Dies könnte zu einer verfassungsrechtlich bedenklichen Profilbildung führen. Schließlich könnte z.B. festgestellt werden, zu welchen Zeiten der einzelne Teilnehmer Dienste genutzt hat, also wann er bestimmte Interessen nach Rundfunksendungen oder anderen Diensten geäußert hat und demnach auch in seiner Wohnung gewesen ist. Insbesondere über das Angebot von Telespielen könnte selbst die Geschicklichkeit des einzelnen Teilnehmers registriert und entsprechend ausgewertet werden, mit der er den Anforderungen des Spiels entsprochen hat.

Blieben diese technischen Möglichkeiten rechtlich ungezügelt, wären mit ihnen nicht unerhebliche Risiken für die durch Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 Grundgesetz geschützte Privatsphäre und das daraus abgeleitete Grundrecht auf informationelle Selbstbestimmung verbunden. Denn die Auswirkungen neuer Kabelmedien lassen sich wie folgt zusammenfassen:

- Die Nutzung der Kabelmedien kann, wie dies bereits bei Bildschirmtext der Fall ist, zu einer stärkeren Individualisierung bisher anonym gebliebener Lebenssachverhalte und zu einer zumindest kurzfristigen Speicherung derartiger Lebensäußerungen auf einem elektronischen Medium führen.
- Werden die während der Nutzung der Kabelmedien in den technischen Einrichtungen angefallenen personenbezogenen Daten nicht sofort nach Ende der jeweiligen Sendung oder des Abrufs des einzelnen Dienstes gelöscht, sondern über einen längeren Zeitraum gespeichert und vielleicht noch mit anderen Daten über einen Betroffenen zusammengeführt, ließen sich daraus Persönlichkeitsprofile über die einzelnen Bürger bilden.
- Bisherige Erfahrungen zeigen, daß personenbezogene Daten, die von ihrem Inhalt her interessante Rückschlüsse auf die Lebensweise der einzelnen Bürger erlauben, dem besonderen Risiko einer Zweckänderung unterliegen, weil sie für Wirtschaft und öffentliche Verwaltung von Interesse sein könnten.
- Aus der Auswertung der bei den verschiedenen Kommunikationsvorgängen bei den neuen Medien angefallenen Daten könnte zumindest rein theoretisch in Verbindung mit den im Wege der Fernwirkdienste erlangten Informationen eine weitgehende Verhaltenskontrolle der Bürger aufgebaut werden. Gerade weil eine solche Verhaltenskontrolle heute niemand wünscht, sind die rechtlichen und die technischen Vorkehrungen zu schaffen, die einen entsprechenden Mißbrauch der Daten verhindern.

4.1.2.3. Notwendigkeit einer gesetzlichen Regelung zum Datenschutz

Wegen des mit der Einführung der Kabelmedien verbundenen Risikos für die verfassungsrechtlich geschützte Privatsphäre der Bürger bedarf die Einführung solcher Kabelmedien nicht allein zur Sicherstellung der Ausgewogenheit der Programme, sondern auch aus dem Gesichtspunkt des Datenschutzes eines Gesetzes. Diese von mir schon früher vertretene Ansicht ist zuletzt, wenn auch nur mittelbar, durch das Urteil des Bundesverfassungsgerichts zum Volkszählungsgesetz 1983 bestätigt worden.

In diesem Zusammenhang scheinen mir folgende Sätze aus der Entscheidungsbegründung wesentlich: „Individuelle Selbstbestimmung setzt aber – auch unter den Bedingungen moderner Informationstechnologien – voraus, daß dem Einzelnen Entscheidungsfreiheit über vorzunehmende oder zu unterlassende Handlungen einschließlich der Möglichkeit gegeben ist, sich auch entsprechend dieser Entscheidung tatsächlich zu verhalten. Wer nicht mit hinreichender Sicherheit überschauen kann, welche ihn betreffende Informationen in bestimmten Bereichen seiner sozialen Umwelt bekannt sind und wer das Wissen möglicher Kommunikationspartner nicht einigermaßen abzuschätzen vermag, kann in seiner Freiheit wesentlich gehemmt werden, aus eigener Selbstbestimmung zu planen oder zu entscheiden". Das Bundesverfassungsgericht führt weiter aus, daß die freie Entfaltung der Persönlichkeit unter den modernen Bedingungen der Datenverarbeitung den Schutz des Einzelnen gegen „unbegrenzte Erhebung, Speicherung, Verwendung und Weitergabe seiner persönlichen Daten" voraussetzt. Wenngleich das vom Bundesverfassungsgericht aus Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG abgeleitete Grundrecht auf informationelle Selbstbestimmung nicht schrankenlos gewährleistet ist, bedürfen Beschränkungen dieses Rechts doch einer verfassungsmäßigen gesetzlichen Grundlage. Dabei hängt die Frage, wie weit das Recht auf informationelle Selbstbestimmung den Gesetzgeber bereits von Verfassung wegen zu Regelungen zwingt, von Art, Umfang und denkbaren Verwendungen der Daten sowie der Gefahr ihres Mißbrauchs ab. Das Bundesverfassungsgericht hat in diesem Zusammenhang weiter deutlich gemacht, daß die Sammlung von Daten auf das erforderliche Minimum zu beschränken ist, das zum Erreichen des mit ihnen verfolgten Zweckes notwendig ist. Die Verwendung der Daten ist auf den gesetzlich bestimmten Zweck begrenzt. Gegen Zweckentfremdung ist ein amtshilfefester Schutz durch Weitergabe- und Verwertungsverbote erforderlich. Schließlich ist nach Ansicht des Bundesverfassungsgerichts auch im Interesse eines vorgezogenen Rechtsschutzes „die Beteiligung unabhängiger Datenschutzbeauftragter von erheblicher Bedeutung für einen effektiven Schutz des Rechts auf informationelle Selbstbestimmung".

Gerade wegen der möglichen Verunsicherung der Bevölkerung kommt dem Datenschutz bei den neuen Medien eine weitere wichtige Funktion zu. Meines Erachtens kann das Vorhandensein eines wirkungsvollen Datenschutzes verhindern, daß die bestehenden Risiken zu einer Beunruhigung weiterer Bevölkerungskreise führen. Dazu muß der Datenschutz aber zweierlei gewährleisten:

- Eine eindeutige materielle Regelung muß den bei Nutzung der neuen Medien möglichen Gefahren wirkungsvoll begegnen.
- Zur Gewährleistung einer effektiven Umsetzung dieser materiellen Regelung bedarf es einer wirkungsvollen, auch in der Bevölkerung anerkannten unabhängigen Datenschutzkontrolle.

Die Datenschutzbeauftragten haben entsprechend ihrer Forderung, daß zur Sicherung des Datenschutzes bei den neuen Medien eine gesetzliche Regelung erforderlich ist, vorbehaltlich der bei den einzelnen Projekten in den Ländern entstehenden Gestaltungsunterschiede nach dem gegenwärtigen Erkenntnisstand eine Musterregelung vorgeschlagen. Diese ist im Anhang (Nr. 5) wiedergegeben.

4.1.2.4. Entwurf eines Medienentwicklungs- und -erprobungsgesetzes

Der von der Staatsregierung vorgelegte Entwurf eines Gesetzes über die Erprobung und Entwicklung neuer Rundfunkangebote und anderer Mediendienste in Bayern (Medienerprobungs- und -entwicklungsgesetz – MEG) enthält neben einer sehr ausführlichen Datenschutzbestimmung in seinem Art. 19 noch bei den sog. „anderen Diensten" Datenschutzregelungen. Ich begrüße es, daß die Bayer. Staatsregierung den Datenschutz bei den neuen Medien berücksichtigt hat. Ohne auf Einzelheiten dieser Bestimmungen einzugehen – über Einzelheiten des materiellen Inhalts der Vorschriften wird in den entsprechenden Gremien zu sprechen sein – möchte ich auf einen Punkt besonders hinweisen.

Die Überwachung des Datenschutzes ist gem. Art. 19 Abs. 2 und 3 Entwurf des MEG dem Landesbeauftragten für den Datenschutz übertragen worden. Damit soll der Landesbeauftragte für den Datenschutz nicht nur die Landeszentrale, sondern auch die Kabelgesellschaft und die Betreiber von Kabelanlagen überwachen. Durch die Erweiterung der Überwachungstätigkeit des Datenschutzbeauftragten von öffentlichen auch auf die privaten Stellen wird dem verfassungsrechtlichen Erfordernis einer ausreichenden Datenschutzkontrolle in erfreulicher Weise Rechnung getragen. Eine Zersplitterung der Datenschutzkontrolle, wie sie im sonstigen Datenschutzrecht üblich ist, hätte befürchten lassen, daß in diesem eng zusammengehörigen Aufgabenbereich der Medienerprobung und -entwicklung eine wirklich effektive Datenschutzkontrolle nicht möglich gewesen wäre. Mit diesem Schritt zur „Datenschutzkontrolle in einer Hand" ist die Bayer. Staatsregierung richtungsweisend in der deutschen Mediengesetzgebung. Ich halte diese Entscheidung im Entwurf auch aus einem anderen Grund für wichtig. Eine wirksame Datenschutzkontrolle kann das Vertrauen in den sachgerechten Umgang der bei Einführung von neuen Medien anfallenden personenbezogenen Daten stärken und damit die Akzeptanz der neuen Medien bei den Bürgern erhöhen. Die Übertragung der externen Kontrolle auf den unabhängigen Datenschutzbeauftragten ist hierbei ein wichtiger Beitrag.

4.1.3. Fernwirkdienste

4.1.3.1. Übersicht

Als ich in meinem letzten Tätigkeitsbericht zu den datenschutzrechtlichen Fragen der Fernwirk- und Fernmeldedienste Stellung bezogen hatte, war ich noch davon ausgegangen, daß diese Dienste erst im Endzustand der Erprobung breitbandiger Dienste beim Kabelpilotprojekt in München zur Verfügung stehen könnten. Zwischenzeitlich ist jedoch bekanntgeworden, daß die Deutsche Bundespost zur Zeit auf dem schmalbandigen Telefonnetz ein Fernwirksystem erprobt. Nach den mir vorliegenden Informationen beabsichtigt die Deutsche Bundespost im Bereich der digitalen Dienste die Einführung einiger neuer Dienstleistungsangebote. Neben der Dienstleistung „Telebox" ist auch der Dienst „Temex" geplant. Unter „Temex" versteht die Post das Dienstleistungsangebot, Fernwirksignale unter Mitbenutzung der Fernsprech-Anschlußleitung zu übertragen. Dabei werden Fernwirksignale zwischen privaten Endstellen und privaten Leitstellen über ein spezielles postalisches Fernwirkübermittlungssystem gesendet. Temex benutzt hierbei das Fernsprechnetz und die bestehenden Datennetze.

Folgende Anwendungsgebiete des Dienstes „Fernwirken" sind vorgesehen:

- „Fernmessen", als das Ablesen von Geräten und Zahlen, beispielsweise bei Wasser, Gas, Strom und Öl;
- „Fernanzeigen", hiermit kann eine Außenstelle über Notsituationen unterrichtet weden, etwa bei der Altenhilfe, Patientenversorgung, beim Ausfallen von Haushaltseinrichtungen und bei Feuer;
- „Fernschalten", von außerhalb der Wohnung kann die Heizung oder die Beleuchtung eingeschaltet werden, bei Alarmsituationen werden Sirenen betätigt und das Personal alarmiert sowie
- „Ferneinstellen", hierunter ist das Lenken von Versorgungsgütern, wie Gas, Wärme, Strom zu verstehen oder die Information von Verkehrsteilnehmern an Autostraßen oder Haltestellen.

Nach Ansicht der Bundespost bietet sich hier insbesondere für Kommunen eine Dienstleistung, die für die Stadtwerke, für Umweltschutzämter, für das Gesundheitswesen, die Sozialhilfe und die Feuerwehr interessant sei. Auch Polizei, Sicherheitsdienste, Wohngesellschaften und Krankendienste sind potentielle Anwender. Die Zahl der Haushalte, die nach Ansicht der Deutschen Bundespost an Temex mit der Möglichkeit des Anzeigens von Notsituationen interessiert seien, wird auf etwa 2,5 Millionen Wohneinheiten geschätzt.

Bei der Einführung dieses Dienstes will die Deutsche Bundespost schrittweise vorgehen, so soll noch im 2. Halbjahr 1984 in München und in Darmstadt mit dem Systemversuch begonnen werden.

4.1.3.2. Regelungsbedarf

Weil Fernwirksysteme erlauben, von außen in einer Wohnung Wirkungen auszulösen, Messungen vorzunehmen und Beobachtungen anzustellen, berühren sie maßgeblich die durch Art. 2 Abs. 1 in Verbindung mit Art. 1 Abs. 2 Grundgesetz geschützte Privatsphäre und das Grundrecht der Unverletzlichkeit der Wohnung (Art. 13 Grundgesetz). Deshalb hatte ich bereits im letzten Tätigkeitsbericht eine Reihe von Bedingungen genannt, die meines Erachtens erfüllt sein müssen, um nachteilige Folgen derartiger Dienste für den Bürger zu vermeiden. Dabei hatte ich insbesondere deutlich gemacht, daß Fernwirkdienste nicht zur Kontrolle der Betroffenen führen dürfen. Außerdem muß meines Erachtens der Betroffene über Art, Umfang und Häufigkeit der jeweiligen Fernwirkung unterrichtet sein. Gegen den Willen des Bürgers darf er Fernmessungen und Fernwirkungen überhaupt nicht ausgesetzt werden. Ich hatte daher bereits im letzten Jahr wegen der möglichen Auswirkungen derartiger „Fernwirkdienste" auf die Grundrechtspositionen der Bürger gefordert, rechtzeitig vor Einführung dieser Dienste eine gesetzliche Regelung zu schaffen, die die vorgenannten Forderungen berücksichtigt. In diesem Anliegen bin ich zwischenzeitlich von der Konferenz der Daten-

schutzbeauftragten des Bundes und der Länder unterstützt worden, die anläßlich ihrer Sitzung am 6./7. Juni 1984 folgendes gefordert hat:

„Um eine Verletzung dieser Grundrechte auszuschließen und ausreichenden Datenschutz zu gewährleisten, müssen vor Einführung von Fernwirkdiensten daher eindeutige gesetzliche Regelungen geschaffen werden, die auch die von der Verfassung vorgesehene Kompetenzverteilung zwischen Ländern und Bund berücksichtigt. Solange derartige bereichsspezifische Regelungen fehlen, darf die Deutsche Bundespost Telefon-Fernwirkdienste nicht einführen." Der vollständige Beschluß ist im Anhang (Nr. 5a) wiedergegeben.

Eine Arbeitsgruppe der Datenschutzbeauftragten hatte daher auch den Vorschlag für eine gesetzliche Regelung erarbeitet, der im Anhang 8 Nr. 5) wiedergegeben ist.

Die Bayerische Staatsregierung hat mein Anliegen ebenfalls aufgegriffen und in dem Gesetzentwurf zum Medienentwicklungs- und -erprobungsgesetz eine Regelung über Fernwirkdienste aufgenommen. Ich begrüße es außerordentlich, daß die Bayer. Staatsregierung meine Anregungen, für Fernwirkdienste rechtzeitig eine gesetzliche Regelung zu schaffen, aufgegriffen hat und die Geltung dieser Regelungen auch auf schmalbandige Netze erstreckt hat. Weil die Kompetenzfrage hinsichtlich der Nutzung solcher neuen Dienste nicht gänzlich unbestritten ist, hat die Bayer. Staatsregierung damit rechtzeitig Position bezogen. Diese Bestimmung reicht in ihrem Regelungsgehalt allerdings nicht so weit, wie die vorgenannte von den Datenschutzbeauftragten erarbeitete Musterregelung. Die im Entwurf vorgesehene Bestimmung verlangt jedoch, daß der Teilnehmer vor Einsatz von Fernwirkdiensten über deren Verwendungszweck und Wirkungsweise unterrichtet wird, und setzt die Einwilligung des Teilnehmers voraus. Außerdem werden von der Vorschrift gerade die Fernwirkdienste erfaßt, bei denen eine besondere Gefährdung für das Persönlichkeitsrecht des Teilnehmers besteht. Angesichts der Tatsache, daß das Medienentwicklungs- und -erprobungsgesetz gerade der Erprobung neuer Dienste dienen soll und spätestens 1992 außer Kraft treten soll, habe ich gegen diese Regelung letztlich keine durchgreifenden datenschutzrechtlichen Bedenken geltend gemacht.

#### 4.1.4. Grenzüberschreitender Datenverkehr bei den „Neuen Medien"

Die Einführung neuer Medien wird aller Voraussicht nach den zwischenstaatlichen Datenverkehr erweitern. Die technischen Möglichkeiten von Bildschirmtext, über Telefonleitungen Verbindungen herzustellen, gestattet es einerseits von Deutschland aus beispielsweise in das britische Prestel-System zu gelangen und erlaubt andererseits Ausländern, das deutsche Bildschirmtextsystem zu benutzen. Außerdem sind im deutschen Bildschirmtextsystem auch ausländische Anbieter zugelassen. Es ist davon auszugehen, daß die von diesen Anbietern erhobenen Daten zumindest zu einem Teil in das Ausland übermittelt werden.

Dem Bürger, dessen personenbezogene Daten über Grenzen hinweg übermittelt werden, muß deutlich gemacht werden, wie weit deutsches Datenschutzrecht reicht und inwieweit seine Daten im Ausland benützt werden können. Darüber hinaus muß sichergestellt werden, daß grenzüberschreitender Datenverkehr mit personenbezogenen Daten nicht dazu mißbraucht wird, die jeweiligen nationalen Datenschutzbestimmungen zu umgehen. Deshalb sind zum einen die Gesetzgeber aufgefordert, Regelungen für den grenzüberschreitenden Datenverkehr bei neuen Medien zu schaffen. Außerdem ist eine internationale Zusammenarbeit der jeweiligen nationalen Kontrollinstitutionen für den Datenschutz bei der Überwachung neuer Medien geboten.

Mit diesen Problemen der neuen Medien hat sich die „Arbeitsgruppe Massenmedien der internationalen Konferenz der Datenschutzbeauftragten" in ihrer Sitzung in Berlin am 5./6. September 1983 befaßt. Die Arbeitsgruppe, an der auch ich teilgenommen habe, hat für die 5. Sitzung der Internationalen Konferenz der Datenschutzbeauftragten zur Gewährleistung des Datenschutzes bei neuen Medien einen Beschlußvorschlag erarbeitet. Die internationale Konferenz hat einen entsprechenden Beschluß am 18. Oktober 1983 gefaßt. Er ist im Anhang (Nr. 6) abgedruckt. Die internationale Konferenz fordert darin angesichts der mit Einführung neuer Medien verbundenen Risiken rechtliche sowie technisch-organisatorische Maßnahmen, die den Persönlichkeitsschutz der Bürger sichern. Die Datenschutzbeauftragten erwarten, daß der Mindeststandard der Richtlinien über den Datenschutz und den grenzüberschreitenden Verkehr mit personenbezogenen Daten der OECD vom 23. September 1980 sowie der Datenschutzkonvention des Europarates vom 28. Januar 1981 auch bei der Nutzung neuer Medien gewährleistet sein sollte. Außerdem hält die Konferenz eine internationale Zusammenarbeit der Kontrollinstitutionen für den Datenschutz bei der Überwachung neuer Medien für geboten.

### 4.2. **Rechtspflege**

Schwerpunkte meiner Tätigkeit im Bereich der Rechtspflege waren die Anordnung über Mitteilungen in Zivilsachen (MiZi) und die Anordnung über Mitteilungen in Strafsachen (MiStra). Aufgrund dieser Anordnungen haben Gerichte und Staatsanwaltschaften in einer Vielzahl von Fällen an andere Behörden und Institutionen Mitteilungen über Straf- und Zivilverfahren sowie über Erkenntnisse zu machen, die im Laufe von Verfahren gewonnen worden sind. Viele dieser Mitteilungen enthalten für den davon Betroffenen sehr sensible Daten, weshalb dem Persönlichkeitsschutz bei diesen Anordnungen besonderes Augenmerk zu widmen ist. Bezüglich der Einzelheiten verweise ich auf die nachstehenden Ausführungen.

Nicht nur bei diesen Anordnungen, sondern auch bei dem sonstigen sehr umfangreichen Umgang der Justiz mit personenbezogenen Daten sind die vom Bundesverfassungsgericht in seiner Entscheidung zum Volkszählungsgesetz 1983 entwickelten Grundsätze von maßgeblicher Bedeutung. Es wird zu prüfen sein, inwieweit bestehende Vorschriften überarbeitet und insbesondere konkretisiert (z.B. § 163 Strafprozeßordnung) und inwieweit überhaupt neue Rechtsvorschriften für den Umgang der Justiz mit personenbezogenen Daten (z.B. MiStra, MiZi) geschaffen werden müssen. Daneben werden die tragenden Grundsätze dieses Urteils gerade auch bei den ausschließlich in Akten verarbeiteten Daten zu beachten sein. Es dürfte nunmehr endgültig keine Zweifel geben, daß dem Persönlichkeitsschutz auch im gerichtlichen und staatsanwaltschaftlichen Verfahren hohes Augenmerk gewidmet werden muß.

Neben den mehr grundlegenden Ausführungen zu MiStra und MiZi schildere ich nachfolgend noch eine Reihe von

Einzelfällen aus dem Justizbereich. Im Berichtszeitraum habe ich grundsätzlich keine gravierenden Verstöße gegen das Datenschutzrecht festgestellt. Mit der Schilderung dieser Einzelfälle will ich erreichen, das Bewußtsein der Justizbediensteten für den Persönlichkeitsschutz im alltäglichen Umgang mit personenbezogenen Daten zu schärfen.

An dieser Stelle will ich auch vermerken, daß ich die Bereitschaft im Staatsministerium der Justiz, Datenschutzbelange zu berücksichtigen, außerordentlich begrüße.

4.2.1. Anordnung über Mitteilungen in Zivilsachen (MiZi)

Die Anordnung über Mitteilungen in Zivilsachen wurde in bundeseinheitlicher Fassung zwischen den Landesjustizverwaltungen und dem Bundesminister der Justiz vereinbart. Aufgrund dieser Anordnung, die teilweise nur gesetzliche Mitteilungspflichten wiedergibt, haben im Verfahren der streitigen Zivilgerichtsbarkeit und der freiwilligen Gerichtsbarkeit die Gerichte von Amts wegen Mitteilungen nach dieser Anordnung zu machen. Hierbei sind vor allem mitzuteilen gerichtliche Entscheidungen, gerichtliche Urkunden und Eintragungen in das Grundbuch oder in ein Register. Die Bandbreite der in der Anordnung über Mitteilungen in Zivilsachen enthaltenen Mitteilungspflichten ist groß. Sie reicht z.B. von Mitteilungen zur Herbeiführung einer Tätigkeit des Vormundschaftsgerichts über Mitteilungen zur Veranlassung von Entmündigungsverfahren, Mitteilungen über Grenzstreitigkeiten, Mitteilungen über die Anordnung oder Fortdauer einer Freiheitsentziehung, Mitteilungen über die Unterbringung in einer Heil- oder Pflegeanstalt und über die Beurlaubung eines Untergebrachten, Mitteilungen über die Beurkundung von Schenkungen, Mitteilungen über Klagen auf Räumung von Wohnraum bei Zahlungsverzugs des Mieters, Mitteilungen über Klagen und über Anträge auf Bewilligung der Prozeßkostenhilfe bei Vorhandensein von Kindern bis zu Mitteilungen über Todeserklärungen und Feststellungen der Todeszeit. Sie betreffen also insbesondere Mitteilungen in Mietsachen, in Unterhaltssachen, in Entmündungssachen, in Ehesachen, in Kindschaftssachen sowie in einer Reihe von Vollstreckungsverfahren. Ob die Anordnung über Mitteilungen in Zivilsachen vom 1. Oktober 1967 mit ihren späteren Änderungen und Ergänzungen Belange des verfassungsrechtlich garantierten Persönlichkeitsschutzes in ausreichendem Maße berücksichtigt, muß geprüft werden. Für eine Reihe von Mitteilungen dürfte jedenfalls eine ausreichende gesetzliche Grundlage fehlen.

Die Datenschutzbeauftragten des Bundes und der Länder haben die Notwendigkeit einer Überprüfung der MiZi unter dem Gesichtspunkt des Datenschutzes erörtert und sich auf ihrer Konferenz am 6./7. Juni 1984 auf folgende gemeinsame Stellungnahme geeinigt:

Die Datenschutzbeauftragten des Bundes und der Länder halten eine alsbaldige grundlegende Überprüfung der bundeseinheitlichen Anordnung über Mitteilungen in Zivilsachen (MiZi) durch die Justizverwaltung in Bund und Ländern für erforderlich:

1. Die MiZi sieht in einer Vielzahl von Verfahren die Übermittlung personenbezogener Daten von den Gerichten der streitigen Zivilgerichtsbarkeit und der freiwilligen Gerichtsbarkeit an Finanzbehörden, Sozialbehörden, Staatsanwaltschaften, Standesämter und andere öffentliche Stellen vor. Mitteilungen dieser Art stellen in aller Regel einen Eingriff in das nach Artikel 2 Abs. 1 i.V. mit Artikel 1 Abs. 1 GG geschützte Recht auf informationelle Selbstbestimmung dar und bedürfen deshalb einer verfassungsgemäßen gesetzlichen Grundlage, die den rechtsstaatlichen Geboten der Normenklarheit und Verhältnismäßigkeit entsprechen muß. Ein Teil der Mitteilungspflichten läßt sich auf Rechtsvorschriften zurückführen. Für andere Mitteilungspflichten ist eine Rechtsgrundlage nicht ersichtlich.

   Eine Überprüfung der Rechtsgrundlagen der Mitteilungspflichten muß mit einer Überprüfung der Erforderlichkeit der Mitteilungen Hand in Hand gehen. Es wird zu prüfen sein, ob nicht manche Mitteilungen angesichts eines veränderten gesellschaftlichen Umfeldes und eines Wandels der Verwaltungsaufgaben ihren Sinn verloren haben. Soweit Mitteilungen für erforderlich gehalten werden, müssen ihre Voraussetzungen und ihr Umfang durch Rechtsvorschrift festgelegt werden.

2. Die bestehende Generalklausel, daß Mitteilungen im Einzelfall auch dann zu machen sind, wenn sie zwar nicht ausdrücklich vorgeschrieben, aber durch ein besonderes öffentliches Interesse geboten sind, bedarf der Überprüfung. Eine solche Klausel darf nicht dazu führen, daß die auf den Einzelfall bezogenen Regelungen und die dort vorgesehenen Beschränkungen umgangen werden. Soweit auf eine Generalklausel nicht verzichtet werden kann, muß auch sie den oben genannten verfassungsrechtlichen Anforderungen Rechnung tragen.

3. Grundsätzlich sollte sich die Übermittlung auf den Tenor der Entscheidung beschränken. Die Übermittlung von Entscheidungsgründen ist nur zuzulassen, wenn deren Kenntnis für die Aufgabenerfüllung der zu benachrichtigenden Behörde erforderlich ist. Insoweit ist zu prüfen, ob nicht die Übermittlung von Entscheidungsgründen – in Umkehrung des bisher praktizierten Regel-Ausnahme-Verhältnisses – auf ausdrücklich geregelte Ausnahmefälle begrenzt werden kann. Wo eine Abwägung im Einzelfall vorgesehen werden muß, sollte sie durch den Richter oder im Rahmen der ihm nach dem Rechtspflegergesetz übertragenen Aufgaben durch den Rechtspfleger erfolgen.

4. Außerdem sollte besonders darauf geachtet werden, daß
   - Datenübermittlungen den betroffenen Bürgern im Hinblick auf Inhalt, Adressat und zugrundeliegende Rechtsgrundlage transparent zu machen sind,

     übermittelte Daten nur im Rahmen des Zwecks, zu dem sie über-mittelt wurden, genutzt werden dürfen (Zweckbindung),
   - die notwendigen technisch-organisatorischen Maßnahmen der Da- tensicherung vorzusehen sind und
   - die Aufbewahrungsdauer, unter Berücksichtigung auch der Belange der Betroffenen, auf das erforderliche Maß zu beschränken ist.

Die Datenschutzbeauftragten des Bundes und der Länder gehen davon aus, daß sie an den weiteren Überlegungen der Justizverwaltungen rechtzeitig beteiligt werden.

4.2.2. Schuldnerverzeichnis

Nach § 915 Zivilprozeßordnung (ZPO) hat das Amtsgericht – Vollstreckungsgericht das Schuldnerverzeichnis zu führen. In das Schuldnerverzeichnis werden die Personen eingetragen, die die eidesstattliche Versicherung über ihr Ver-

mögen abgegeben haben oder gegen die wegen Nichtabgabe der eidesstattlichen Versicherung Haft angeordnet worden ist, sowie unter bestimmten Voraussetzungen die Haftvollstreckung.

4.2.2.1. Abschriften aus dem Schuldnerverzeichnis

Bereits in meinem 3. Tätigkeitsbericht hatte ich darauf hingewiesen, daß eine nicht unerhebliche Zahl von Institutionen und Personen Abschriften aus dem Schuldnerverzeichnis erhält. Weil die Beachtung der Löschungsfrist nach § 915 Abs. 2 ZPO bei den Empfängern der Abschriften in der Praxis vielfach nicht gewährleistet ist, hatte ich die bisherige Handhabung der Verteilung von Abschriften aus dem Schuldnerverzeichnis als dringend änderungsbedürftig bezeichnet. Zwar hatte auf ensprechende Anregungen der Datenschutzbeauftragten des Bundes und der Länder der Bundesminister der Justiz im Dezember 1980 einen Entwurf einer „Verordnung über Abschriften aus den Schuldnerverzeichnissen" erarbeitet, doch ist zu meinem Bedauern bis heute eine entsprechende Verordnung noch nicht erlassen worden. Ich habe das Bayerische Staatsministerium der Justiz gebeten, sich beim Bundesminister der Justiz mit Nachdruck für eine Beschleunigung der Vorarbeiten an einer Neugestaltung einer entsprechenden Regelung einzusetzen.

4.2.2.2. Löschung der Eintragungen

Mit den praktischen Erfahrungen der in § 915 Abs. 2 ZPO geregelten Löschungspflicht für das Schuldnerverzeichnis hatte ich mich im 5. Tätigkeitsbericht auseinandergesetzt. In diesem Zusammenhang hatte ich berichtet, daß ich bei einer Prüfung in einem großen bayerischen Amtsgericht festgestellt hatte, daß die Löschung der Eintragungen nicht sachgerecht vorgenommen worden war. Bereits im damaligen Berichtszeitraum hatte das betroffene Amtsgericht auf meine Vorstellungen hin angeordnet, daß die Löschung im Schuldnerverzeichnis auf den Karteikarten deutlich und vollständig vollzogen wird. Ich habe mich bei einer Nachprüfung davon überzeugt, daß nun entsprechend den Vorschriften verfahren wird. In diesem Zusammenhang hatte ich auch das Bayer. Staatsministerium der Justiz eingeschaltet. Dieses hatte mir mitgeteilt, es beabsichtige, für das Schuldnerverzeichnis einen einheitlichen Kartenvordruck einzuführen. An der Neugestaltung der Karteikarte bin ich nicht beteiligt worden.

4.2.2.3. Personenverwechslung

Mit der Praxis des Schuldnerverzeichnisses hatte ich mich auch aufgrund einer Bürgereingabe erneut zu befassen:

Ein Petent hatte bei dem zuständigen Gewerbeamt die Erlaubnis für die Tätigkeit als Immobilienmakler beantragt. Ihm wurde jedoch bedeutet, daß eine Gewerbeerlaubnis nicht erteilt werden könne, weil über ihn ein Eintrag im Schuldnerverzeichnis beim Amtsgericht vorliege. Die Einsichtnahme in das Schuldnerverzeichnis zeigte ihm, daß tatsächlich ein Eintrag über eine namensgleiche Person vorhanden war. Weitere eindeutige identifizierende Angaben wie Geburtsdatum oder Geburtsort waren nicht eingetragen.

Wie oben bereits angesprochen, erhalten eine nicht unerhebliche Zahl von Institutionen und Personen Abschriften aus den Schuldnerverzeichnissen. Sind nun die Eintragungen im Schuldnerverzeichnis mangels hinreichender Identifizierung des einzelnen Schuldners nicht eindeutig, besteht die Gefahr, daß unbeteiligte Dritte mit dem Schuldner verwechselt werden und entsprechende Nachteile erleiden. Ich habe mich deshalb über den konkreten Fall hinaus mit der Angelegenheit befaßt und untersucht, wie das betroffene Amtsgericht Eintragungen im Schuldnerverzeichnis im allgemeinen handhabt. Meine Ermittlungen hatten folgendes ergeben:

Eintragungen im Schuldnerverzeichnis umfassen neben Name, Vorname und Anschrift des Schuldners in einer Vielzahl von Fällen auch den Beruf und das Geburtsdatum. Letzteres ist z.B. dann der Fall, wenn die Eintragung auf der Abgabe der eidesstattlichen Versicherung beruht, aus der das Geburtsdatum des Schuldners ersichtlich ist. Wie mir die mit der Eintragung befaßten Justizbediensteten sowie der für die Aufsicht über das Vollstreckungsgericht zuständige Richter versichert haben, wird das Geburtsdatum, soweit es bekannt ist, auch immer eingetragen. Tatsächlich wurde bei der an Ort und Stelle durchgeführten Überprüfung keine Eintragung gefunden, bei der etwa anders verfahren worden wäre. Allerdings gibt es daneben Fälle, in denen das Vollstreckungsgericht das Geburtsdatum des Schuldners nicht kennt und dieses deshalb auch nicht eintragen kann. Auch in solchen Fällen – es handelt sich hierbei regelmäßig um Haftanordnungen auf Antrag des Gläubigers – ist das Amtsgericht-Vollstreckungsgericht nach § 915 ZPO zur Eintragung des Schuldners verpflichtet; das Vollstreckungsgericht darf die Eintragung nicht etwa deshalb ablehnen, weil sich aus den zur Verfügung stehenden Unterlagen kein Geburtsdatum oder ein anderes zusätzliches Identifikationsmerkmal ergibt. Es hat auch keine rechtliche Möglichkeit, etwa vom Gläubiger, der die Haftanordnung beantragt, die Angabe des Geburtsdatums des Schuldners zu verlangen.

Es liegt auf der Hand, daß bei identischem Namen die Anschrift, die sich jederzeit ändern kann, allein kein sicheres Identifikations- bzw. Unterscheidungsmerkmal ist. Um die sich hieraus ergebenden Verwechslungsgefahren möglichst auszuschalten, sollte das Amtsgericht-Vollstrekkungsgericht jedoch bei Auskünften zumindest auf etwa abweichende Anschriften oder fehlende Identifikationsmerkmale hinweisen. Erhält die anfragende Stelle entsprechende Hinweise, so ist sie gehalten, sich besonders sorgfältig über die Identität der Person, über die angefragt wird, mit der namensgleichen aber unter anderer Anschrift eingetragenen Person zu vergewissern.

In dem konkreten Fall hätte es bei gewissenhafter Beachtung dieses Verfahrens nicht zu der bedauerlichen Verwechslung kommen dürfen. Warum sie gleichwohl geschehen ist, konnte sich leider nicht mehr aufklären lassen. Ich hatte mich jedoch davon überzeugt, daß der Fehler jedenfalls nicht auf einer fehlerhaften oder gar nachlässigen Eintragungspraxis des Amtsgerichts beruhte.

Auch dieser Vorgang zeigt, daß es dringend erforderlich ist, eine Regelung zu schaffen, die die Erteilung von Abschriften und Auskünften aus dem Schuldnerverzeichnis und deren Behandlung bei den Empfängern eindeutig regelt.

4.2.3. Prozeßkostenhilfe

Fragen der Prozeßkostenhilfe hatte ich in meinem 3. Tätigkeitsbericht angesprochen. Dabei hatte ich darauf hingewiesen, daß derjenige, der Prozeßkostenhilfe beantragt, eine Erklärung abgeben muß über seine persönlichen und wirtschaftlichen Verhältnisse, insbesondere Familienverhält-

nisse, Beruf, Vermögen, Einkommen und Lasten, sowie dem Antrag entsprechende Belege beizufügen hat. Wegen der möglichen Sensibilität dieser Angaben kann der Antragsteller ein erhebliches Interesse daran haben, daß seine Angaben anderen Personen möglichst nicht bekannt werden. Diesem, auch von den Datenschutzbeauftragten unterstützten Anliegen haben die Landesjustizverwaltungen zumindest insoweit Rechnung getragen, als sie in den entsprechenden Durchführungsbestimmungen festgelegt haben, daß die bei Durchführung der Prozeßkostenhilfe angefallenen Unterlagen getrennt vom Hauptakt in einem Beiheft aufzubewahren sind.

Offengeblieben und bislang in der Rechtsprechung auch nicht abschießend entschieden war die Frage, inwieweit im Prozeßkostenhilfeverfahren der Gegner des Antragsstellers Einsicht in diese Unterlagen nehmen kann. In erfreulicher Weise hat nun der Bundesgerichtshof in seinem Beschluß vom 15.11.1983 (Az.: VI ZR 100/83, NJW 1984, S. 740) festgestellt, daß in Prozeßkostenhilfeverfahren der Gegner des Antragstellers kein Anhörungsrecht zu den Angaben über die persönlichen und wirtschaftlichen Verhältnisse und insoweit auch kein Recht auf Einsicht in die diese Angaben enthaltenen Aktenteile hat. Der Bundesgerichtshof hat hierzu ausgeführt, daß gesetzlich ein solches Anhörungs- und damit ein Einsichtsrecht (§ 299 ZPO) nicht vorgeschrieben sei. Soweit nämlich über die persönlichen und wirtschaftlichen Voraussetzungen der Gewährung von Prozeßkostenhilfe zu entscheiden sei, sei der Gegner nicht Verfahrensbeteiligter. Das Gesetz sehe eine Mitwirkung des Prozeßgegners bei der Ermittlung der persönlichen und wirtschaftlichen Voraussetzungen für die Gewährung der Prozeßkostenhilfe gerade nicht vor. Die Prüfung dieser Voraussetzungen beim Antragsteller sei allein Sache des Gerichts. Da also mithin kein Anhörungsrecht des Gegners zu den vom Antragsteller gemachten Angaben zu seinen persönlichen und wirtschaftlichen Verhältnissen bestünde und der Gegner insoweit auch nicht Verfahrensbeteiligter sei, habe er auch nicht nach § 299 Abs. 1 ZPO ein Recht auf Einsichtnahme in den diese Angaben enthaltenden, im übrigen gesondert geführten Teil der Prozeßakten.

4.2.4. Testamentseröffnung

Der nachfolgende Vorgang zeigt meines Erachtens, daß Bestimmungen zum Schutz der persönlichen Sphäre – hierzu gehören auch grundsätzlich die Vermögensverhältnisse, wie sie oftmals aus einem Testament ersichtlich sind – schon lange vor jeder Datenschutzdiskussion gesetzlich verankert gewesen sind. Er zeigt aber außerdem, daß in der alltäglichen Praxis die schützenswerte Privatsphäre der Bürger nicht immer ausreichend beachtet wird.

Nach § 2262 BGB hat das Nachlaßgericht die Beteiligten, also z.B. Erben und Vermächtnisnehmer, welche bei der Eröffnung des Testaments nicht zugegen gewesen sind, von dem sie betreffenden Inhalt des Testaments in Kenntnis zu setzen.

Ein Bürger hat mir nun vorgetragen, daß ein Nachlaßgericht die Vermächtnisnehmer nicht nur von der sie betreffenden Bestimmung des Testaments unterrichte, sondern sie vom Inhalt des gesamten Testaments in Kenntnis setze. Auf meinen Vorhalt, daß diese Praxis nicht der in § 2262 BGB enthaltenen ausdrücklichen Regelung entspreche, hat das betroffene Nachlaßgericht erklärt, daß diese Verfahrensweise seit geraumer Zeit praktiziert werde und daß an dieser Berechtigung keinerlei Zweifel bestünden. Vielmehr ziele diese Verfahrensweise auf die Gleichbehandlung aller Verfahrensbeteiligten ab, unabhängig davon, ob sie bei dem Termin zur Eröffnung des Testaments anwesend seien oder nicht.

Diese Argumente, die ein Festhalten an der bisherigen Praxis rechtfertigen sollten, konnten mich nicht überzeugen. Insbesondere konnte ich keine unzulässige Ungleichbehandlung erkennen, wenn der Vermächtnisnehmer im Eröffnungstermin nicht anwesend ist und im nachhinein nur den ihn betreffenden Inhalt des Testaments erfährt. Die Bestimmung des § 2262 BGB entspricht nämlich dem Datenschutzgrundsatz, daß nur die Daten übermittelt werden sollen, die im jeweiligen Falle erforderlich sind.

Das Bayerische Staatsministerium der Justiz hatte mir mitgeteilt, daß es sich im vorliegenden Falle ersichtlich um eine auf den Bezirk eines Amtsgerichts beschränkte Praxis des dortigen Nachlaßgerichts handle. Die Nachlaßrechtspfleger des Amtsgerichts würden im Wege der Dienstaufsicht zur künftigen Beachtung des § 2262 BGB angehalten, die Einhaltung der Anordnung werde überprüft.

4.2.5. Mitteilungen in Strafsachen (MiStra)

4.2.5.1. Neufassung der Anordnung

Gerichte und Staatsanwaltschaften unterrichten nach der Anordnung über Mitteilungen in Strafsachen (MiStra) bestimmte andere öffentliche Stellen über die Einleitung eines Ermittlungsverfahrens bzw. die Erhebung der öffentlichen Klage und den jeweiligen Ausgang des Verfahrens. Hierzu hatte ich bereits in den letzten Tätigkeitsberichten Stellung genommen. Bereits 1980 hatten die Landesbeauftragten und der Bundesbeauftragte für den Datenschutz sowie die Datenschutzkommission Rheinland-Pfalz in einem Beschluß gefordert, die MiStra so zu überarbeiten, daß nur noch die Vorschriften bestehen bleiben, für die eine gesetzliche Rechtsgrundlage besteht, oder andernfalls eine eindeutige gesetzliche Grundlage zu schaffen. Dabei sollte auch der Umfang der bisherigen Mitteilungspflichten entsprechend dem zwischenzeitlich eingetretenen Verständnis des Persönlichkeitsschutzes verringert werden.

Der von der Justizministerkonferenz in dieser Angelegenheit eingesetzte Unterausschuß hatte die Anordnung über Mitteilungen in Strafsachen einer Überprüfung unterzogen und einen Entwurf für die Überarbeitung der MiStra vorgelegt.

So sehr ich einerseits begrüße, daß dieser Entwurf wenigstens den Wegfall einiger Mitteilungspflichten und eine Überarbeitung einzelner Bestimmungen unter Datenschutzgesichtspunkten vorsieht, so habe ich doch mit Bedauern festgestellt, daß die im Beschluß der Datenschutzbeauftragten genannten Forderungen und Anregungen nur zu einem geringen Teil aufgegriffen worden sind. Überrascht hat mich hierbei inbesondere, daß der Entwurf offensichtlich an der bisherigen Rechtsqualität der MiStra als Verwaltungsvorschrift festhält, obwohl der Unterausschuß der Justizministerkonferenz selbst sich für die Schaffung einer Rechtsnorm ausgesprochen hatte. Mit allen Landesbeauftragten für den Datenschutz (vgl. Anhang Nr. 11) bin ich mir einig, daß die MiStra einer eindeutigen Rechtsgrundlage bedarf, weil derartige Mitteilungen für die Betroffenen einen Eingriff darstellen. Bei einer meines Erachtens dringend erforderlichen erneuten Überarbeitung der MiStra sollten folgende Gesichtspunkte besonders beachtet werden:

4.2.5.2. Grundsätze für die MiStra

- Die Zahl der Mitteilungsfälle muß weiter eingeschränkt werden. Auch ist der bekannte Datenschutzgrundsatz zu berücksichtigen, daß nur die Daten übermittelt werden dürfen, die andere Stellen zu ihrer gesetzlich zugewiesenen Aufgabenerfüllung unbedingt benötigen. Hierbei ist ein strenger Maßstab anzuwenden. Mit diesem Grundsatz ist es nicht zu vereinbaren, daß der vorliegende Entwurf neben einer Vielzahl von einzelnen Mitteilungsvorgängen noch zusätzlich weitere generalklauselartig formulierte Bestimmungen enthält, die weitere Mitteilungen ermöglichen. Wenn Mitteilungen etwa auch dann vorgenommen werden dürfen, wenn sie zwar nicht ausdrücklich vorgeschrieben, aber „durch ein besonderes öffentliches Interesse geboten" sind oder sie auf jedes Ersuchen einer Behörde erfolgen, soweit nicht „erhebliche Bedenken entgegenstehen", so liegt darin die Gefahr, daß die im übrigen auf den Einzelfall bezogenen Regelungen und deren bewußte Beschränkungen umgangen werden. Damit wäre aber der Sinn der Einzelregelungen der MiStra gefährdet, nämlich die mögliche Beeinträchtigung der durch Art. 1 Abs. 1 und Art. 2 Abs. 1 GG geschützte Persönlichkeitsphäre des Betroffenen zu begrenzen.

- Eine Einschränkung der Mitteilungen ist darüber hinaus beispielsweise auch bei fahrlässig begangenen Straftaten notwendig. Die fahrlässige Begehung weist grundsätzlich auf ein geringeres Maß an strafrechtlicher Vorwerfbarkeit hin. Verfahren, die Fahrlässigkeitstaten betreffen, sollten daher grundsätzlich nicht mitgeteilt werden. Dies gilt im besonderen Maße bei fahrlässig begangenen Verkehrsstraftaten. Nur bei engem Bezug zur beruflichen Tätigkeit des von der Mitteilung Betroffenen und bei besonderem Gewicht des verletzten Rechtsguts könnten Ausnahmen zugelassen werden.

- Wegen der Auswirkungen, die die Mitteilungen für den Betroffenen haben können, sollten diese im Regelfall vom Richter oder Staatsanwalt veranlaßt werden. Nur in den Fällen, in denen nach den Einzelregelungen der MiStra keinerlei Entscheidungsspielraum besteht, sollte die Geschäftsstelle zur Anordnung der Mitteilung befugt sein. Diese Umkehrung des im Entwurf von der geltenden Fassung der MiStra enthaltenen Regel- und Ausnahmeverhältnisses erscheint dringend erforderlich.

- Entgegen der bisherigen Regelung und Praxis sollten die Mitteilungen in Strafsachen möglichst erst nach rechtskräftigem Abschluß der Strafverfahren vorgenommen werden. Die Mitteilung in Strafsachen sollen die zu benachrichtigenden Behörden in Kenntnis von den Vorgängen setzen, auf die sie im Rahmen des ihnen zugewiesenen gesetzlichen Aufgabenbereichs zu reagieren haben. Ein strafrechtlich relevanter Sachverhalt läßt sich jedoch abschließend erst nach Abschluß des Strafverfahrens beurteilen. Ausnahmen hinsichtlich einer vorzeitigen Mitteilung müssen auf die Fälle beschränkt werden, in denen wegen der Bedeutung des möglichlicherweise verletzten Rechtsgutes die begründete Annahme besteht, daß vorzeitige Maßnahmen veranlaßt sind. Auch soweit derartige Ausnahmen berechtigt sind, dürfen Mitteilungen grundsätzlich erst zum Zeitpunkt der Erhebung der öffentlichen Klage gemacht werden. Denn erst zu diesem Zeitpunkt ist bereits eine gewisse Erfolgsaussicht der Klage nach der Beurteilung des Staatsanwalts anzunehmen. Mitteilungen bereits bei der Einleitung des Ermittlungsverfahrens könnten allenfalls auf die wenigen Ausnahmefälle beschränkt sein, in denen begründete Anhaltspunkte vorliegen, daß die zu benachrichtigende Behörde sofortige Maßnahmen einleiten muß.

- Des weiteren ist auch der Inhalt der Mitteilungen auf das im Einzelfall wirklich notwendige Mindestmaß zu beschränken. Das bedeutet, daß im Regelfall die Mitteilung der Tatsache einer Verurteilung unter Angabe der Straftat genügen wird. Dabei ist zu berücksichtigen, daß die Urteilsgründe vielfach Angaben zu weiteren Personen wie etwa Zeugen, Hinweisgebern oder Mittätern enthalten, deren Persönlichkeitsrechte durch eine Mitteilung an andere öffentliche Stellen beeinträchtigt werden könnten. Eine Mitteilung des vollständigen Urteils muß meines Erachtens auf die Fälle beschränkt sein, in denen die zu benachrichtigende Behörde nur aufgrund umfassenderer Kenntnis des dem Strafverfahren zugrundeliegenden Sachverhalts geeignete Maßnahmen treffen kann.

- Ein weiterer Gesichtspunkt, der bei der Diskussion um die Mitteilungen in Strafsachen teilweise übersehen wird, ist die Verwendung und weitere Aufbewahrung dieser Mitteilungen bei den empfangenden Behörden. Wegen der Sensibilität der aufgrund der MiStra mitgeteilten Daten haben die empfangenden Behörden den Grundsatz der Zweckbindung besonders zu beachten. Die strenge Zweckbindung soll dabei verhindern, daß Daten für andere als die ursprünglich vorgesehenen Zwecke Verwendung finden oder gar an andere Stellen gelangen. Durch eine Beschränkung der Aufbewahrungsdauer muß überdies sichergestellt werden, daß die Bürger nicht über das Institut der Mitteilungen in Strafsachen mit einer strafrechtlichen Verurteilung länger konfrontiert werden dürfen, als dies nach dem Bundeszentralregistergesetz statthaft wäre.

- Das informationelle Selbstbestimmungsrecht, das selbstverständlich auch dem Straftäter zusteht, setzt grundsätzlich voraus, daß der Betroffene über die zu seiner Person vorliegenden Daten und – das ist hier das wesentlichste – auch darüber unterrichtet wird, an welche Stellen seine Daten weitergeleitet worden sind. Daher ist der Betroffene grundsätzlich davon zu benachrichtigen, welche Stellen Mitteilungen nach der MiStra erhalten haben. Dem Betroffenen ist es dann möglich zu entscheiden, ob er ggf. selbst die aufgrund der MiStra unterrichteten Stellen über den dem Strafverfahren zugrundeliegenden Sachverhalt aus seiner Sicht informiert und so der empfangenden Behörde eine umfassendere Beurteilung der Straftat ermöglicht. Die im Entwurf vorgesehene Unterrichtung des Betroffenen sollte daher so erweitert werden, daß der Betroffene generell von Mitteilungen Kenntnis erlangt. Von der Benachrichtigung darf meines Erachtens nur dann abgesehen werden, wenn schwerwiegende Bedenken in der Person des Betroffenen entgegenstehen.

- Schließlich ein auf den ersten Blick nur marginaler Gesichtspunkt, dem in der Praxis jedoch größere Bedeutung zukommt: Die Mitteilungen müssen so eindeutig adressiert sein, daß sichergestellt ist, daß von diesen Mitteilungen nur die Personen in den zu benachrichtigenden Behörden Kenntnis erlangen, welche diese Kenntnis zu ihrer Aufgabenerfüllung benötigen. Dies

werden im Regelfall nur die Personalsachbearbeiter sein. Außerdem sind derartige Mitteilungen in jedem Fall verschlossen zu versenden. Ein mir bekanntgewordener Fall beweist, daß dies derzeit nicht in allen Fällen gewährleistet ist.

4.2.5.3. Verstoß gegen Nr. 15 MiStra

So hatte eine Staatsanwaltschaft entsprechend der Mitteilungspflicht nach Nr. 15 MiStra eine Behörde von einem gegen einen Angehörigen dieses Amtes gerichteten Strafbefehl unterrichtet. Die Mitteilung war weder an den Leiter der Behörde oder an seinen Vertreter adressiert, noch war sie als „vertrauliche Personalsache" gekennzeichnet. Dies hatte zur Folge, daß diese Mitteilung im normalen Posteinlauf geöffnet und bearbeitet worden war. Diese Sachbehandlung stand im Widerspruch zur geltenden Regelung in Nr. 15 Abs. 3 Satz 2 MiStra. Sie war geeignet, den Betroffenen in seinen schutzwürdigen Belangen zu beeinträchtigen. Der Leiter der Staatsanwaltschaft hat mir mitgeteilt, daß es sich im vorliegenden Fall um eine einmalige Fehlleistung eines erfahrenen und zuverlässigen Beamten gehandelt haben dürfte. Er werde aber dieses Vorkommnis zum Anlaß nehmen, seine Mitarbeiter wiederholt und nachdrücklich auf die Einhaltung der entsprechenden Bestimmung der MiStra hinzuweisen.

4.2.5.4. Verwirklichung des Datenschutzes

Die Aussichten, daß die Datenschutzbelange bei einer Überarbeitung der Mitteilungen in Strafsachen in Bayern nachhaltig berücksichtigt werden, sind meines Erachtens sehr günstig. So hat der beim Landesbeauftragten für den Datenschutz gebildete Beirat auf seiner Sitzung am 21.2.1984 nach einer ausführlichen Erörterung der Datenschutzprobleme der MiStra folgenden Beschluß gefaßt:

1. Der Beirat unterstützt im Grundsatz die Stellungnahme der Datenschutzbeauftragten des Bundes und der Länder zum Entwurf der MiStra.
2. Der Beirat hält eine Überprüfung der MiStra und des Entwurfs der Justizverwaltungen anhand der Grundsätze des Urteils des Bundesverfassungsgerichts zum Volkszählungsgesetz 1983 für notwendig.
3. Der Beirat bittet die Staatsregierung darauf hinzuwirken, daß
   a) eine Rechtsgrundlage für die MiStra geschaffen wird, soweit eine solche nicht schon besteht;
   b) die Beachtung der Zweckbindung in allen Mitteilungsfällen sichergestellt wird;
   c) in den Fällen, in denen ein Entscheidungsspielraum besteht, die Entscheidung durch einen Richter oder Staatsanwalt erfolgt;
   d) Mitteilungen grundsätzlich erst nach rechtskräftigem Abschluß des Strafverfahrens erfolgen und
   e) der Betroffene grundsätzlich von Mitteilungen benachrichtigt wird.

Besonders erfreulich waren die Ausführungen des Bayer. Staatsministers der Justiz im Ausschuß für Verfassungs-, Rechts- und Kommunalfragen des Bayer. Landtags am 28.3.1984. Er hatte hierbei ausdrücklich erklärt, daß das Staatsministerium der Justiz bei den weiteren Überlegungen von folgenden Grundsätzen ausgehen wird:

1. Die Mitteilungen in Strafsachen müssen so geregelt werden, daß den Anforderungen, die das Bundesverfassungsgericht im Urteil zum Volkszählungsgesetz entwikkelt hat, voll entsprochen wird. Wir wollen nicht, daß die Tätigkeit der Justiz in diesem Bereich verfassungsrechtlichen Zweifeln unterliegt.
2. Den berechtigten Mitteilungsbedürfnissen der anderen Verwaltungen muß Rechnung getragen werden.
3. Im Interesse der Betroffenen und im Interesse der überlasteten Strafrechtspflege muß bei der Notwendigkeit von Mitteilungen jedoch ein strenger Maßstab angelegt werden. Es ist notwendig, die Justiz auch in diesem Bereich zu entlasten. Die Mitteilungspflichten müssen gegenüber dem gegenwärtigen Stand eingeschränkt werden.
4. Die Regelung über die Mitteilungspflicht muß für die Justizbehörden einfach anzuwenden sein. Eine Entscheidung durch den Richter oder Staatsanwalt darf nur in Ausnahmefällen notwendig sein. Der Betroffene muß bereits aus der abstrakten Regelung entnehmen können, in welchen Fällen und an welche Stelle eine Mitteilung gemacht wird.
5. Im Bereich der Empfänger-Behörden muß bestimmt werden, daß die Mitteilungen nur zweckgebunden verwertet werden dürfen und wie lange eine Verwertung möglich ist.

Ich begrüße diese klare Stellungnahme, die die wesentlichen Anforderungen des Datenschutzes berücksichtigt.

Hinsichtlich des weiteren Fortgangs bei der Überarbeitung der MiStra hat mir das Bayer. Staatsministerium der Justiz mitgeteilt, daß noch vor der parlamentarischen Sommerpause eine Äußerung des Bundesjustizministeriums – insbesondere auch zum weiteren zeitlichen Vorgehen – zu erwarten sei. Unabhängig von der Überarbeitung oder Neufassung der MiStra wird zu prüfen sein, in welchem Umfang in der Übergangszeit bis zur Schaffung einer Rechtsgrundlage Mitteilungen gemacht werden.

4.2.5.5. Mitteilungen an die Polizei (Nr. 11 MiStra)

Nach Nr. 11 MiStra hat die Staatsanwaltschaft die Polizei über den Ausgang eines Strafverfahrens zu unterrichten, wenn die Polizei durch Übersendung eines entsprechenden Vordrucks darum gebeten hat. Anläßlich datenschutzrechtlicher Überprüfungen bei Polizeibehörden ist mir bekannt geworden, daß dieser nach Nr. 11 vorgesehene Informationsrückfluß aus dem Justizbereich zur Polizei in vielen Fällen nicht stattfindet. Die Kenntnis vom Ausgang eines Verfahrens ist jedoch für die polizeiliche Arbeit insbesondere im Hinblick auf die Führung und Bewertung der kriminalpolizeilichen personenbezogenen Sammlungen (KpS) von maßgeblicher Bedeutung.

So können die Polizeibehörden den Regelungen zur Aufbewahrungsdauer in den KpS-Richtlinien vielfach nur dann pflichtgemäß nachkommen, wenn sie die Mitteilung über den Ausgang eines Verfahrens erhalten haben. Die Aufbewahrung polizeilicher Unterlagen ist nach Nr. 6 der KpS-Richtlinien nur solange zulässig, wie es zur rechtmäßigen Erfüllung der in der Zuständigkeit der aufbewahrenden Stelle liegenden Aufgaben erforderlich ist. Die in Nr. 6.1 der KpS-Richtlinien enthaltende Abwägungspflicht zwischen dem öffentlichen Interesse, auf polizeiliche Kenntnisse zu-

rückgreifen zu können, und dem Grundrecht auf freie Entfaltung der Persönlichkeit kann sachgerecht nur vollzogen werden, wenn die abschließende Wertung der dem Beschuldigten zur Last gelegten Handlung bekannt ist. Nr. 6.4.3 der KpS-Richtlinien enthält eine Aussonderungspflicht, wenn die Ermittlungen oder eine der Polizei bekannte Entscheidung der Staatsanwaltschaft oder eines Gerichtes ergeben, daß die Gründe, die zur Aufnahme in die KpS geführt haben, nicht zutreffen. Nach Nr. 6.2.2 der KpS-Richtlinien ist in den Fällen von geringerer Bedeutung nach kürzerer Frist als in den nach Nr. 6.2.1 genannten Regelfristen auszusondern. Diese Richtlinien können nicht vollzogen werden, wenn eine Mitteilung über den Ausgang des Verfahrens unterbleibt, die möglicherweise auch eine Aussage zur „geringen Bedeutung" enthält oder ausweist, daß den Betroffenen kein Tatvorwurf trifft.

Daher habe ich beim Bayer. Staatsministerium der Justiz angeregt, die meldepflichtigen Stellen seines Geschäftsbereichs an die Beachtung von Nr. 11 MiStra zu erinnern. Zu meiner Überraschung hat mir das Bayer. Staatsministerium der Justiz nun mitgeteilt, daß das Staatsministerium des Innern ihm berichtet habe, daß lediglich in wenigen Einzelfällen entgegen Nr. 11 Abs. 1 MiStra die übermittelten Vordrucke seitens der Justizbehörden nicht ausgefüllt zurückgesandt worden seien und im allgemeinen von einem korrekt funktionierenden Informationsfluß ausgegangen werden könne. Das Staatsministerium der Justiz hat es im Hinblick auf diese Feststellungen nicht für erforderlich gehalten, meiner Anregung zu folgen, die Praxis seines Geschäftsbereichs an die Beachtung der Nr. 11 MiStra zu erinnern. Allerdings steht dieser Bericht des Staatsministeriums des Innern im Widerspruch zu meinen oben angemerkten Erfahrungen bei der Polizei.

Das Bayer. Staatsministerium des Innern hat mich allerdings zwischenzeitlich davon unterrichtet, daß der Arbeitskreis II „Öffentliche Sicherheit und Ordnung" der Arbeitsgemeinschaft der Innenministerien der Länder in seiner Sitzung am 26./27. Semptember 1983 beschlossen habe, einen Auschuß mit der Erarbeitung eines einheitlichen Formblattes für die Unterrichtung der Polizei durch die Justizstellen über den Ausgang des Strafverfahrens zu beauftragen. Dies begrüße ich.

Ich würde es ferner begrüßen, wenn das von diesem Arbeitskreis erarbeitete Formblatt im wesentlichen dem in Baden-Württemberg kürzlich eingeführten Mitteilungsvordruck entsprechen würde. Auf diesem kann die Justiz der Polizei detailliert mitteilen, weshalb ein Angeklagter verurteilt, weshalb ein Verfahren eingestellt oder ob der Angeklagte freigesprochen und dabei ggf. der Grundsatz „in dubio pro reo" angewandt worden ist. Hierzu hatte das Justizministerium des Landes Baden-Württemberg mit Allgemeinverfügung eine erfreulich klare Anordnung getroffen, aus der sich der Umfang der Mitteilungen nach Nr. 11 bei Einstellungen und bei freisprechenden Urteilen sowie Verurteilungen deutlich ergibt.

4.2.6. Richtlinien für das Strafverfahren

Die Richtlinien für das Straf- und Bußgeldverfahren (RiStBV) geben dem Staatsanwalt Anleitungen für die Abwicklung von Strafverfahren. Einige Hinweise dieser Richtlinien wenden sich auch an den Richter. In Nr. 185 und 185 a wird die Gewährung der Akteneinsicht geregelt.

Im 5. Tätigkeitsbericht hatte ich berichtet, daß diese Richtlinien geringfügig novelliert worden waren, hierbei eine Änderung der Richtlinien in dem von mir vorgeschlagenen Sinne jedoch nicht vorgenommen worden war. Ich hatte daher die Erwartung ausgesprochen, daß bei Anwendung der Vorschriften in Nr. 185 und 185 a RiStBV bei der Gewährung des Akteneinsichtsrechts gleichwohl die von mir als notwendig erachtete Güterabwägung vorgenommen wird und daß die Einsichtnehmenden auf die Zweckbindung der Daten hingewiesen und ihnen ggf. Auflagen gemacht werden. Zwischenzeitlich hat das Bayer. Staatsministerium der Justiz die staatsanwaltschaftliche und gerichtliche Praxis in Bayern auf meine Anregungen hingewiesen und zum Ausdruck gebracht, daß meinem Anliegen bereits jetzt bei der Anwendung der geltenden Regelungen der RiStBV angemessen Rechnung getragen werden soll. Dies begrüße ich. Es wird nun darauf ankommen, ob meine Vorstellungen in der praktischen Handhabung der Regelungen tatsächlich hinreichend berücksichtigt werden. Die diesbezügliche Praxis werde ich aufmerksam beobachten.

4.2.7. Beschlagnahme von Akten

Als die Leiche eines neugeborenen Säuglings gefunden worden war, bat die zuständige Kriminalpolizeiinspektion die Allgemeine Ortskrankenkasse um Amtshilfe zur Aufklärung der Tat. Die Polizei begründete ihr Ersuchen damit, daß es zur Identifizierung des unbekannten Säuglings geboten sei, bei den Sozialversicherungsträgern festzustellen, welche Frauen in einem bestimmten Zeitraum Mutterschaftshilfe oder ähnliche Leistungen in Anspruch genommen hätten. Die Allgemeine Ortskrankenkasse wies die Polizei darauf hin, daß eine Offenbarung der gewünschten Daten nach § 73 Nr. 1 Sozialgesetzbuch 10. Teil nur zulässig sei, soweit sie aufgrund richterlicher Anordnung erforderlich sei. Daraufhin wurde durch Beschluß des zuständigen Amtsgerichts die Durchsuchung der Geschäftsräume der Allgemeinen Ortskrankenkasse „nach kassenärztlichen Behandlungsscheinen der im jeweiligen Bezirk ansässigen Frauenärzte" für einen bestimmten Zeitraum angeordnet.

Datenschutzrechtlich von Bedeutung ist nun, daß nachfolgend die zuständige Polizeidienststelle mit der betroffenen AOK vereinbarte, daß für die polizeilichen Ermittlungen nur bestimmte nun näher bezeichnete Offenbarungen erforderlich seien. Damit blieb diese Vereinbarung zwischen Polizei und AOK bezüglich des Umfangs der erforderlichen Daten sowohl hinter dem ursprünglichen Offenbarungsersuchen der Kriminalpolizeiinspektion als auch hinter dem richterlichen Beschluß zurück.

In Anbetracht der durch Art. 97 Abs. 1 Grundgesetz und Art. 85 Bayer. Verfassung garantierten richterlichen Unabhängigkeit kann ich den vorstehenden richterlichen Beschluß nicht bewerten. Ich habe allerdings dem Bayer. Staatsministerium der Justiz mitgeteilt, daß die Staatsanwaltschaft bei ihrer auf einen richterlichen Beschluß hinzielenden Antragsstellung dem Verfassungsgrundsatz der Verhältnismäßigkeit in ausreichendem Maße Rechnung tragen muß. Dies bedeutet z.B., daß ein Antrag der Staatsanwaltschaft, der auf Beschlagnahme sensibler Daten abzielt, möglichst eng gefaßt und auf das erforderliche Minimum beschränkt sein muß. Im übrigen ist die Offenbarung personenbezogener Daten, wie oben bemerkt, nach § 73 SGB X nur zulässig, soweit sie auf richterliche Anordnung hin „erforderlich" ist. Das Gebot zur Beachtung des Grundsatzes

der Verhältnismäßigkeit gilt aber nicht nur für die richterliche Anordnung im Sinne des § 73 SGB X, sondern bereits für den Antrag der Staatsanwaltschaft. § 162 Abs. 1 StPO setzt voraus, daß die Staatsanwaltschaft die Vornahme einer bestimmten richterlichen Untersuchungshandlung für erforderlich hält. Darüber hinaus ist die Staatsanwaltschaft nach Nr. 4 der Richtlinien für das Straf- und Bußgeldverfahren zur besonderen Berücksichtigung des Verhältnismäßigkeitsgrundsatzes verpflichtet.

Das Bayer. Staatsministerium der Justiz hat mir mitgeteilt, daß die Frage der Antragsstellung der Staatsanwaltschaft im Vollzug des § 73 SGB X anläßlich einer Dienstbesprechung mit den Leitern der Staatsanwaltschaften erörtert wird.

4.2.8. Persönlichkeitsschutz der Zeugen im Strafprozeß

Mit dem Schutz der Zeugen im Strafprozeß hatte ich mich bereits kurz in meinem 4. und 5. Tätigkeitsbericht befaßt. Dabei hatte ich darauf hingewiesen, daß im Hinblick auf den Bedeutungswandel des Öffentlichkeitsgrundsatzes der Hauptverhandlung, nämlich von der öffentlichen Kontrolle zum Schutz gegen Willkür zur Stillung des Informationsinteresses der Allgemeinheit, nun der verfassungsrechtlich garantierte Schutz der Persönlichkeit des Angeklagten und der anderen Verfahrensbeteiligten verstärkt berücksichtigt werden müßte.

Das Bayerische Staatsministerium der Justiz hat nun am 8. Juni 1983 eine Verwaltungsvorschrift erlassen, die dem Persönlichkeitsschutz der Zeugen im Strafprozeß stärker zur Geltung verhelfen soll. Darüber hinaus werden auf Vorschlag Bayerns die Regelungen dieser Verwaltungsvorschrift und einer weiteren gemeinsamen Bekanntmachung betreffend den Opferschutz im Strafverfahren im wesentlichen in die bundeseinheitlichen Richtlinien für das Strafverfahren und das Bußgeldverfahren übernommen. Dagegen fand ein Antrag der Bayerischen Staatsregierung im Bundesrat keine Mehrheit, in § 172 GVG für die Opfer von Straftaten gegen die sexuelle Selbstbestimmung ein Antragsrecht vorzusehen. Jedoch hat der Bundesrat die Bundesregierung aufgefordert zu prüfen, wie die Privatsphäre der von einem Strafverfahren Betroffenen besser als bisher geschützt werden kann.

Obzwar diese Fragen nicht zum Datenschutzbereich im engeren Sinne gehören und ich insoweit von meinem mir durch Artikel 28 Abs. 4 Satz 2 BayDSG eingeräumten Recht Gebrauch mache, Verbesserungen des Datenschutzes anzuregen, messe ich dem Schutz der Zeugen im Strafprozeß besondere Bedeutung bei und werde die Angelegenheit weiter aufmerksam verfolgen und gegebenenfalls eigene Vorschläge entwickeln.

4.2.9. Zustellungen

Ein Bürger, der Adressat einer von einem Amtsgericht veranlaßten Zustellung war, hat sich bei mir darüber beschwert, daß im Anschriftenfeld sein Geburtsdatum offen angegeben war. Wie der Petent weiter ausführte, würde laut einer ihm fernmündlich gegebenen Auskunft bei diesem Amtsgericht regelmäßig so verfahren. Wenn es sich auch aus meiner Sicht bei dieser Frage um kein Datenschutzproblem von grundlegender Bedeutung handelt, so bestehen gegen eine solche generelle Handhabung datenschutzrechtliche Bedenken. Angaben, die für die Zustellung nicht unbedingt erforderlich sind, sollten im Anschriftenfeld behördlicher Schreiben nicht erscheinen. Diese Auffassung hatte ich auch schon anderen Behörden vorgetragen mit dem Erfolg, daß die behördliche Praxis daraufhin meiner Auffassung jeweils Rechnung getragen hat.

Dabei verkenne ich nicht, daß es im Einzelfall, insbesondere in ländlichen Gebieten, vorkommen kann, daß verschiedene Personen gleichen Vor- und Nachnamens im selben Anwesen wohnen. Die Notwendigkeit der Angabe des Geburtsdatums ist auch damit begründet worden, daß es in der Vergangenheit diesbezüglich zu Falschzustellungen gekommen sei. Zur Vermeidung solcher für die Betroffenen im Einzelfall peinlichen Falschzustellungen habe man auf die Angabe des Geburtsdatums als zusätzliches Unterscheidungsmerkmal zurückgegriffen. Es ist sicherlich einzuräumen, daß eine Falschzustellung die Betroffenen in weit schwerwiegenderem Maße belasten kann als die Angabe des Geburtsdatums. Gleichwohl können die wenigen Fälle der Falschzustellungen meines Erachtens die generelle Angabe des Geburtsdatums nicht rechtfertigen.

Das Bayer. Staatsministerium der Justiz, dem ich von dem Vorgang Kenntnis gegeben hatte, hat darauf hin die Gerichte und Staatsanwaltschaften seines Zuständigkeitsbereichs gebeten, „das Geburtsdatum des Adressaten künftig nur in den Fällen in die Postanschrift aufzunehmen, in denen Anhaltspunkte dafür bestehen, daß dies zur Vermeidung von Fehlzustellungen geboten ist". Diese klare und datenschutzfreundliche Weisung begrüße ich; sie ist eine sachgerechte und ausgewogene Lösung.

4.2.10. Strafvollzug

Aus den unterschiedlichen Eingaben von Strafgefangenen wird das Anliegen deutlich, daß Außenstehende möglichst nicht Kenntnis von der Inhaftierung erhalten. Für dieses Anliegen habe ich grundsätzlich Verständnis, denn eine Kenntnisnahme Dritter kann im Einzelfall die Wiedereingliederung des Straftäters in die Gesellschaft gefährden. Dabei ist zu berücksichtigen, daß die Erkenntnis von der Bedeutung der Resozialisierung sich in den letzten Jahrzehnten im Strafrecht zunehmend durchgesetzt hat und nach allgemeiner Auffassung die Resozialisierung neben dem Schutz der Allgemeinheit vor weiteren Straftaten als eines der herausragenden Ziele, namentlich des Vollzugs von Freiheitsstrafen angesehen wird (BVerfGE 35, 202/235). Dabei ist auch zu bedenken, daß nicht nur der Straffällige auf die Rückkehr in die freie menschliche Gesellschaft vorbereitet werden muß, diese muß ihrerseits bereit sein, ihn wieder aufzunehmen. Nach den Erfahrungen der Praxis scheitert die Resozialisierung aber in vielen Fällen an der Ablehnung, mit der die Umwelt dem Entlassenen begegnet. Daher muß es im Interesse eines auf Resozialisierung ausgerichteten Strafvollzuges liegen, die Kenntnis von der Inhaftierung des Strafgefangenen auf einen möglichst kleinen Kreis zu beschränken (zum besonderen Problem bei Untersuchungsgefangenen vgl. BVerG E 34, 369/382).

4.2.10.1. Haftraumbeschilderung

Ein Strafgefangener hat sich darüber beklagt, daß Besucher der Justizvollzugsanstalt, die teilweise in größeren Gruppen zur Besichtigung durch die Zellentrakte geführt werden, von den an den Hafträumen der Strafgefangenen vermerkten Daten Kenntnis nehmen. Die sog. „Haftraumschilder" enthalten den Namen des Gefangenen, dessen Gefangenen-Buchnummer, die Zugehörigkeit zu einem bestimmten

Betriebsteil der Justizvollzugsanstalt, die besondere Kostform, die Konfession, Teilnahme an bestimmten Kursen, sowie Art der Arbeit oder etwaige Arbeitslosigkeit.

Hinsichtlich der auf den Haftraumschildern enthaltenen Informationen ist grundsätzlich ein schutzwürdiges Interesse der Strafgefangenen anzuerkennen, daß Besucher nicht von ihren persönlichen Verhältnissen Kenntnis nehmen können. Auch insoweit hat eine Abwägung zu erfolgen, die einerseits die Belange des Betroffenen berücksichtigt und auf der anderen Seite auch die Interessen der Allgemeinheit sowie Belange des geordneten Strafvollzugs in Betracht zu ziehen hat. Wie mir die Justizverwaltung mitgeteilt hat, werden zu Besichtigungen der betroffenen Justizvollzugsanstalt nur solche Personenkreise zugelassen, bei denen ein beruflicher Bezug oder ein berücksichtigungswürdiges staatsbürgerliches Interesse besteht. Hierbei werde auch das Ziel verfolgt, bei diesen Gruppen Verständnis für den Strafvollzug und die Gefangenenarbeit zu wecken und auf diese Weise die Resozialisierung der Gefangenen zu fördern. Eine Vielzahl von Arbeitsvermittlungen nach der Entlassung habe ihren Ursprung in derartigen Besichtigungen. Ich bin daher der Auffassung, daß zur Wahrung der schutzwürdigen Belange der Strafgefangenen die Einstellung jeglicher Führungen aus den genannten Gründen auch unter Berücksichtigung der berechtigten Interessen der Gefangenen in der Tat nicht gefordert werden kann. Auch ein völliger Verzicht auf die Haftraumbeschilderung in der Justizvollzugsanstalt dürfte kaum in Betracht kommen. Die Haftraumbeschilderung ist eine wohl sinnvolle und auch erforderliche Maßnahme der Vollzugsorganisation. Zum Informationsinhalt der Haftraumschilder haben meine Erkundigungen im übrigen ergeben, daß Besucher zumindest die Religionszugehörigkeit der Gefangenen aus den Angaben aus den Haftraumschildern wohl nur in den seltensten Fällen entnehmen können, weil die Schilder insoweit nur farbige Streifen enthalten, deren Bedeutung den Besuchern nicht bekannt sein dürfte. Ferner wird auch die Arbeitslosigkeit nur durch eine Abkürzung wiedergegeben.

Die Berücksichtigung der schutzwürdigen Belange muß deshalb von den Justizvollzugsanstalten auf andere Weise sichergestellt werden. Wie dem Tätigkeitsbericht des Hamburgischen Datenschutzbeauftragten für 1983 zu entnehmen ist, wurde das Problem in der dortigen Justizvollzugsanstalt Vierlande dadurch gelöst, daß die Namensschilder für die Dauer der Besichtigung entfernt werden. Ich verkenne nicht, daß diese Lösung zumindest bei größeren Anstalten einen Verwaltungsaufwand erfordern würde, der die Grenze des Vertretbaren zu überschreiten droht. Grundsätzlich sollte diese Lösungsmöglichkeit jedoch im Auge behalten werden. Meines Erachtens müssen auch in bayerischen Justizvollzugsanstalten Lösungen denkbar sein, in denen durch einfache, nur geringen Aufwand erfordernde organisatorische Maßnahmen einer möglichen Beeinträchtigung der Persönlichkeitsrechte von Gefangenen vorgebeugt werden kann. Solche sich bietende Möglichkeiten müssen von den Justizvollzugsanstalten genützt werden. Das Argument, das der Vorstand der betroffenen Justizvollzugsanstalt vertreten hat, die Offenbarung des Namens eines Gefangenen könne diesen schon deshalb nicht in seinen Rechten verletzen, weil gegen ihn öffentlich verhandelt und hierüber in der Presse berichtet worden sei, kann ich jedenfalls nicht gelten lassen.

4.2.10.2. Nachsendeanschrift

Ein Strafgefangener hat gerügt, daß die ihm nach seiner Verlegung von einer in eine andere bayerische Justizvollzugsanstalt nachgesandte Post als Nachsendeanschrift den Vermerk „JVA" trage. Dadurch könnten Dritte von der Tatsache seines Aufenthalts in einer Justizvollzugsanstalt Kenntnis erlangen, wodurch er in seinen schutzwürdigen Belangen beeinträchtigt werde.

Dem Interesse des Strafgefangenen, daß beim Nachsenden oder Rücksenden von Post seine Gefangenschaft nicht erkennbar wird, trägt Nr. 40 Abs. 2 Vollzugsgeschäftsordnung (VGO) Rechnung. Dieser lautet wie folgt:

„Beim Nachsenden und Rücksenden von Post ist durch geeignete Maßnahmen dafür Sorge zu tragen, daß die Gefangenschaft des Adressaten nicht erkennbar ist. Bei Bedarf ist ein Deckumschlag zu verwenden."

Die Vollzugsbehörde ist grundsätzlich gehalten, sich nach dieser Vorschrift zu richten.

Nach meinen Ermittlungen ist von einer Justizvollzugsanstalt Nr. 40 Abs. 2 VGO nicht immer beachtet worden. Der Vorstand dieser JVA hat allerdings versichert, daß er die Bediensteten zwischenzeitlich erneut und eindringlich belehrt und auf die Einhaltung dieser Vorschrift hingewiesen habe. Meine Ermittlungen haben aber auch ergeben, daß wohl nicht ganz ausgeschlossen werden kann, daß manchen Verlagen, Warenhäusern und ähnlichen Einrichtungen die Anschriften der Justizvollzugsanstalten ohnehin nicht ganz unbekannt sind. Weil umadressierte Briefe teilweise durch die Post an den Absender zurückgeleitet werden, können jene von der geänderten Anschrift Kenntnis nehmen. In diesen Fällen wird ggf. von den Justizvollzugsanstalten zu prüfen sein, entsprechend der Regelung in Nr. 40 Abs. 2 Satz 2 VGO Deckumschläge zu verwenden.

4.2.10.3. Briefüberwachung

Die in meinem 5. Tätigkeitsbericht angesprochene Frage der Briefüberwachung und die im Rahmen der Briefüberwachung auf der ausgehenden Post angebrachten Sichtvermerke haben mich erneut beschäftigt. Nach wie vor halte ich die Anbringung eines Sichtvermerks nicht für schlechthin unzulässig. Denn nach § 29 Abs. 3 Strafvollzugsgesetz darf der Schriftwechsel der Strafgefangenen aus Gründen der Behandlung oder Sicherheit oder Ordnung der Anstalt überwacht werden. Die einschlägige Verwaltungsvorschrift sieht insoweit ausdrücklich vor, daß ein Sichtvermerk angebracht werden kann. Allerdings ist nach meiner Auffassung das hinter der Kontrolle stehende Interesse der Justizvollzugsanstalt an der Aufrechterhaltung der Sicherheit und Ordnung der Anstalt abzuwägen mit den schutzwürdigen Interessen des Strafgefangenen an der Geheimhaltung seines derzeitigen Aufenthalts. In dem Fall, mit dem ich mich auseinanderzusetzen hatte, hatte ich zu berücksichtigen, daß es sich um eine Justizvollzugsanstalt mit dem höchsten Sicherheitsgrad handelt. Der bei der Abwägung anzulegende Maßstab hat dem besonderen Sicherheitsbedürfnis einer solchen Anstalt Rechnung zu tragen und läßt daher die Anbringung von Sichtvermerken von vorneherein eher gerechtfertigt erscheinen als etwa in Anstalten mit geringerem Sicherheitsgrad.

Allerdings gelten diese Überlegungen jedoch nicht für Schul- und Prüfungsbescheinigungen und ähnliche Urkunden. Mit der betroffenen Justizvollzugsanstalt bin ich mir einig, daß auf diese Bescheinigungen grundsätzlich kein

Sichtvermerk angebracht werden darf. Die Ermittlungen hatten ergeben, daß lediglich in einem einzigen Fall in der jüngeren Vergangenheit auf einer derartigen Urkunde versehentlich ein Sichtvermerk angebracht worden ist. Dieser Vorgang ist nach Auskunft der JVA dienstaufsichtlich gerügt und zum Anlaß für eine nochmalige diesbezügliche Belehrung der Bediensteten genommen worden.

4.2.10.4. Paketmarken

Die Verwendung von Paketmarken in Justizvollzugsanstalten ist ein weiteres Problem, das an mich herangetragen worden ist. Zum Verständnis ist hierzu zunächst folgendes zu sagen:

Nach § 33 Abs. 1 Strafvollzugsgesetz darf der Gefangene dreimal jährlich Pakete mit Nahrungs- und Genußmitteln empfangen. Der Empfang weiterer Pakete oder solcher mit anderem Inhalt bedarf der Erlaubnis der Vollzugsbehörde. Damit besteht für die Vollzugsbehörde das Recht und die Pflicht, den Empfang von Paketen zu überwachen und nicht genehmigte Pakete an den Absender zurückzusenden. Zu diesem Zweck bestimmt Nr. 4 Satz 2 der Verwaltungsvorschriften zu § 33 Strafvollzugsgesetz, daß die Verwendung einer von der Anstalt ausgegebenen Paketmarke vorgeschrieben werden kann. Diese Paketmarke hat der Strafgefangene zunächst dem Absender eines Paketes zuzuleiten, damit dieser sie auf dem an den Gefangenen gerichteten Paket anbringt. Diese Regelung hält die Rechtsprechung zur Verringerung des Verwaltungsaufwandes und zur Erleichterung der Kontrolle für zulässig. Auch das Bundesverfassungsgericht hat keine verfassungsrechtlichen Bedenken gegen die Verwendung einer neutral gehaltenen Paketmarke (BVerfG E 34, S. 369/382). Allerdings ist zu berücksichtigen, daß durch Verwendung von Paketmarken Dritte Kenntnis vom Aufenthaltsort des Gefangenen erhalten können. In Anbetracht der oben geschilderten Bedeutung der Wiedereingliederung der Strafgefangenen in die Gesellschaft, die durch die Kenntnis der Tatsache der Inhaftierung im Einzelfall erschwert werden kann, sollte von Paketmarken in möglichst schonender Weise und nur im erforderlichen Umfang Gebrauch gemacht werden. Keinesfalls darf für alle möglichen Sendungen die Verwendung von Paketmarken verlangt werden.

4.2.10.5. Aufbewahrung der Gefangenenpersonalakten

Durch Berichte in den Medien wurde ich darauf aufmerksam, daß ein entlassener Strafgefangener in seinem Privatkeller Unterlagen des Sozialdienstes einer Justizvollzugsanstalt gefunden hat. Dabei hat es sich um Schriftstücke aus abgeschlossenen Vorgängen aus den Jahren 1970/71 – 1980 gehandelt. Diese Unterlagen waren versehentlich der sichergestellten Habe eines Gefangenen zugerechnet worden. Meine Ermittlungen haben ergeben, daß es sich hier um einen wohl einmaligen bedauerlichen Vorfall gehandelt hatte. Der Leiter der betroffenen Justizvollzugsanstalt hat in einer erfreulich deutlichen Dienstanweisung die einschlägigen Bestimmungen allen Bediensteten nochmals in Erinnerung gebracht. Das Bayer. Staatsministerium der Justiz hat zugesichert, den Themenkreis verstärkt in die Fortbildung der Justizvollzugsbediensteten einzubeziehen.

4.2.11. Handbuch der Justiz

Der Deutsche Richterbund gibt periodisch das „Handbuch der Justiz" heraus, in dem Name, Dienststellung, Beförderungsdatum und Geburtsdatum der in der Bundesrepublik Deutschland tätigen Richter, Staatsanwälte und Justizministerialbeamten (höherer Dienst) wiedergegeben sind. Die Herausgeber dieses Handbuchs erhalten die notwendigen Daten von den jeweiligen Landesjustizverwaltungen und dem Bundesminister der Justiz. Seit Jahren wird die Frage erörtert, inwieweit für diese Datenübermittlung an den Herausgeber des Handbuches die Einwilligung der Betroffenen erforderlich ist. Für die Beurteilung dieser Frage lassen sich der Entscheidung des Bundesverfassungsgerichtes zum Volkszählungsgesetz 1983 neue Gesichtspunkte entnehmen.

Das Handbuch der Justiz hat eine lange Tradition. Es erlaubt dem einzelnen Justizangehörigen sich über die Beförderungspraxis der personalverwaltenden Stellen zu informieren und die eigene berufliche Situation innerhalb der Justiz zu bewerten. Diese Offenlegung kann allerdings auch zur Folge haben, daß sich ältere, nicht beförderte Justizangehörige durch diese Offenlegung im Handbuch der Justiz bloßgestellt fühlen. Neben dieser „inneren Transparenz" vermittelt das Handbuch auch Außenstehenden einen Überblick über Justizangehörige. Hieran kann im Einzelfall insbesondere für Rechtsanwälte ein Interesse bestehen. Andererseits ermöglicht die Veröffentlichung dieser Daten Dritten, diese Daten für andere Zwecke zu verwerten, beispielsweise für Werbemaßnahmen oder den Adreßhandel.

Zur rechtlichen Bewertung der Datenübermittlung von den Justizverwaltungen an die Herausgeber des Handbuchs der Justiz ist folgendes festzustellen:

Soweit Daten aus Personalakten entnommen werden, bemißt sich die Zulässigkeit einer Datenübermittlung zunächst nach dem Personalaktenrecht. Das Bundesverwaltungsgericht hat in ständiger Rechtsprechung Grundsätze für den besonderen Schutz der Personalakten entwickelt. Danach dürfen Personalakten ohne Einwilligung des Beamten grundsätzlich nur von einem eng begrenzten Personenkreis mit besonderer dienstlicher Verantwortung eingesehen werden. Sie genießen sowohl im dienstlichen Interesse als auch im schutzwürdigen persönlich-privaten Interesse des Beamten einen besonderen Vertrauensschutz. Sie gehören zu den Vorgängen, die ihrem Wesen nach geheimgehalten werden müssen. Auskünfte aus den Personalakten sind nach der Rechtsprechung des Bundesverwaltungsgerichts nur zulässig, wenn nach den Umständen des Einzelfalles dem schutzwürdigen Interesse der Beamten an der Geheimhaltung ein überwiegendes schutzwürdiges Interesse der Allgemeinheit oder eines Dritten an der Auskunftserteilung gegenübersteht.

Soweit Personaldaten der Justizangehörigen in Dateien geführt werden, sind grundsätzlich die jeweils einschlägigen Landesdatenschutzgesetze oder das Bundesdatenschutzgesetz für die Justizangehörigen des Bundes anwendbar. Diese Regelungen in den Datenschutzgesetzen werden durch das sog. „Personalaktengeheimnis", das von der Rechtsprechung, wie bemerkt, entwickelt worden ist, nicht verdrängt. Den Datenschutzgesetzen gehen grundsätzlich nur „besondere Rechtsvorschriften" vor. Eine solche Rechtsvorschrift oder Vorschrift über den Datenschutz fehlt hinsichtlich des Personalaktengeheimnisses. Während für die Übermittlung von Daten der Justizangehörigen des Bundes die Datenübermittlung nach § 7 Abs. 3 i.V.m. § 24 BDSG zu beurteilen wäre, gelten für die Justizangehörigen der Länder i.d.R. die jeweiligen Vorschriften der Landesda-

tenschutzgesetze bezüglich der Datenübermittlung von Stellen des öffentlichen Bereichs an Stellen außerhalb dieses Bereichs. Nach Art. 18 Abs. 1 BayDSG wäre zu prüfen, inwieweit die Herausgeber des Handbuchs der Justiz ein berechtigtes Interesse an der Kenntnis der zu übermittelnden Daten glaubhaft machen und ob durch eine derartige Datenübermittlung schutzwürdige Belange der Justizangehörigen beeinträchtigt würden. Diese Abwägung entspricht weitgehend derjenigen, die das Bundesverwaltungsgericht im Rahmen der Grundsätze zum Personalaktengeheimnis entwickelt hat. Bei beiden Abwägungen, also Datenübermittlungen aus Akten oder aus Dateien, sind nun die vom Bundesverfassungsgericht entwickelten Grundsätze zum Recht auf informationelle Selbstbestimmung heranzuziehen. Dieses Grundrecht gewährleistet „die Befugnis des Einzelnen, grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen". „Die Verwendung der (von öffentlichen Stellen erhobenen) Daten ist auf den gesetzlich bestimmten Zweck begrenzt". Die Zweckbindung ist damit eine wesentliche Voraussetzung für den zulässigen Umgang mit personenbezogenen Daten. Eine Weitergabe personenbezogener für Zwecke der Personalverwaltung erhobener Daten an nichtöffentliche Stellen ist damit eine Zweckänderung und greift in das Recht auf informationelle Selbstbestimmung ein. Bei dieser Beurteilung kann grundsätzlich nicht zwischen den einzelnen von den personalverwaltenden Stellen an die Herausgeber des Handbuchs der Justiz übermittelten Daten unterschieden werden. Denn unter den Bedingungen der automatischen Datenverarbeitung, von denen auch dann auszugehen ist, wenn in einem Einzelfall die übermittelten Daten zunächst manuell weiterverarbeitet werden, gibt es nach Ansicht des Bundesverfassungsgerichts „kein belangloses Datum" mehr. Dies ist bei der Beurteilung einer Datenübermittlung nach dem Personalaktengeheimnis wie nach den jeweiligen Datenschutzgesetzen entsprechend zu berücksichtigen. Das hat zur Folge, daß eine Übermittlung der Daten über Justizangehörige von den personalverwaltenden Stellen an die Herausgeber des Handbuchs der Justiz wegen der damit gegebenen Zweckänderung der Daten einen Eingriff in das Recht auf informationelle Selbstbestimmung darstellt und somit mangels einer gesetzlichen Regelung der Einwilligung der Betroffenen bedarf.

Bei der Frage, in welcher Form eine Einwilligung im Einzelfall zu erteilen und wie weitgehend im Einzelfall die Aufklärung über Zweck, Reichweite und Auswirkungen der Einwilligung zu erfolgen hat, ist auf den jeweils betroffenen Personenkreis abzustellen. Während im Regelfall an die Aufklärung über die Bedeutung der Einwilligung hohe Anforderungen zu stellen sind und zu verlangen ist, daß der Betroffene die Einwilligung ausdrücklich erklärt, kann von dem durch die Datenübermittlung an das Handbuch der Justiz betroffenen Personenkreis – dies sind grundsätzlich nur Volljuristen – angenommen werden, daß er ohne nähere Aufklärung die Wirkung einer Einwilligung erkennt und diese beispielsweise auch durch „Schweigen" erklären kann. Ich bin daher der Ansicht, daß die betroffenen Justizangehörigen vor jeder Datenübermittlung von den personalverwaltenden Stellen an die Herausgeber des Handbuchs der Justiz unter Angabe über den jeweiligen Datenumfang zu unterrichten sind, daß aber die Einwilligung von Angehörigen dieses Personenkreises auch durch Schweigen, also konkludent, erteilt werden kann. Eine wirksame konkludente Einwilligung setzt allerdings voraus, daß die Betroffenen durch geeignete Maßnahmen der Justizverwaltung tatsächlich von der beabsichtigten Datenübermittlung Kenntnis erlangen und außerdem wissen, daß ihr Schweigen als Zustimmung gewertet wird.

### 4.3. **Sicherheitsbereich**

#### 4.3.1. Neue Qualität der Datenverarbeitung

Wie in nahezu allen Lebensbereichen wächst auch im Bereich der Sicherheitsbehörden die Automatisierung. Die Anwendung von Spurendokumentationssystemen und die Einführung der Datei „Kriminalaktennachweis" mögen Belege aus jüngster Zeit sein. Daneben nehmen auch die Möglichkeiten zu, über bei den Polizeibehörden installierte Datensichtgeräte Daten aus Datenbanken abzurufen, die bei anderen Behörden eingerichet sind. Statt einer Auskunftserteilung auf begründetes Auskunftsersuchen durch die datenführende Stelle können nun Polizeibeamte im Rahmen des eröffneten Datenzugangs selbst Daten abrufen. Zugang zu den Melderegistern, zu den Daten der Kfz-Zulassungsstellen und der Anschluß an das Zentrale Verkehrsinformationssystem sind Beispiele hierfür.

Aus dem Gesichtspunkt eines Persönlichkeitsschutzes, der bei aller Anerkennung der Notwendigkeit eines ausreichenden Datenzugangs durch die Polizei gewährleistet sein muß, sind die Erforderlichkeit jeder neuen Automation und der Zugang zu Datenbanken anderer Stellen bezüglich jedes einzelnen Datums auf ihre strikte Erforderlichkeit zur gesetzlichen Aufgabenerfüllung zu prüfen. Dabei ist auch der Grundsatz der Verhältnismäßigkeit zu beachten. So kann ein Online-Anschluß an eine Datenbank einer anderen Behörde dann nicht gerechtfertigt sein, wenn in vergleichsweise wenigen Fällen bestimmte personenbezogene Daten von der Polizei benötigt werden. Statt eines Online-Anschlusses sind hier gegebenenfalls andere organisatorische Maßnahmen zu wählen, die den Bedürfnissen der Polizei nach Datenübermittlung im Einzelfall gerecht werden.

Bei jedem neuen Automationsvorhaben und bei jedem Anschluß an Datenbanken anderer Behörden wird die Polizei auch zu bedenken haben, wie diese zunehmende Automatisierung von den Bürgern aufgenommen und bewertet wird. Bei dem beachtenswerten Bestreben der Polizei, die Erfüllung der ihr gesetzlich zugewiesenen Aufgaben der Gefahrenabwehr und der Aufklärung von Straftaten zur Sicherheit der Bürger zu verbessern, wird die Polizei alles vermeiden müssen, was auch in solchen Teilen der Bevölkerung, die als loyale Staatsbürger die Rechte und Pflichten der Sicherheitsbehörden respektieren, die Befürchtung auslösen kann, die Gefährdungen durch die Automation könnten den persönlichen Sicherheitsgewinn übersteigen.

Daneben muß es aber auch gelingen, das Bewußtsein bei den einzelnen Polizeibeamten zu schärfen, daß Speicherung, Übermittlung und sonstige Verwendung personenbezogener Daten auf ein Minimum beschränkt sein müssen. Gerade im Hinblick auf eine zunehmende Automatisierung ist dieser Grundsatz der „Beschränkung auf das Minimum" auch bei der Aufnahme von Daten in Akten zu berücksichtigen. In den Akten sind vielfach die Grundlagen, aus denen Daten in automatisierte Dateien oder Datenbanken übernommen werden. Der einzelne Beamte muß erkennen, daß die Automatisierung bisher verstreuter und zum Teil schwer zugänglicher Daten eine neue Qualität der Datenverarbeitung bedeutet und damit neue Auswirkungen für den Per-

sönlichkeitsschutz der Bürger mit sich bringt. So konnte etwa ein Bürger die lange Aufbewahrung der polizeilichen Ermittlungsakten wegen einer „Jugendsünde" relativ gelassen hinnehmen, solange er sicher sein konnte, daß diese Daten lediglich im Aktenraum einer Polizeidienststelle nur den dort tätigen Polizeibeamten zugänglich waren. Wären diese Daten oder ein Hinweis darauf jedoch landesweit zugänglich, kann eine lange Aufbewahrung dieser Daten den Bürger über Gebühr belasten.

Gerade auch im Hinblick auf diese verschärften Auswirkungen der polizeilichen Datenverarbeitung für die Persönlichkeitssphäre des Bürgers ist es nun dringend erforderlich, daß für die polizeiliche Datenverarbeitung eindeutige gesetzliche Grundlagen geschaffen werden.

4.3.2. Notwendigkeit einer gesetzlichen Regelung

Über die allgemeinen Ausführungen zum Urteil des Bundesverfassungsgerichts zum Volkszählungsgesetz hinaus nehme ich im folgenden unter Berücksichtigung dieses Urteils zur Frage der Erforderlichkeit einer bereichsspezifischen polizeilichen Datenschutzregelung kurz Stellung.

Die Frage wurde bislang kontrovers diskutiert, inwieweit über die derzeit bestehenden Regelungen in den, die Polizei oder den Verfassungsschutz berührenden, Gesetzen hinaus für die Datenverarbeitung durch Sicherheitsbehörden eine besondere Regelung erforderlich ist. Hierzu hat das Bundesverfassungsgericht durch die Definition des aus Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 Grundgesetz abgeleiteten Grundrechts auf informationelle Selbstbestimmung in einigen wichtigen Punkten eine Klärung gebracht. Polizeiliche Datenverarbeitung bedarf nunmehr grundsätzlich einer ausdrücklichen Rechtsgrundlage, weil sie in der Regel das Recht auf informationelle Selbstbestimmung berührt.

Dieses Recht auf informationelle Selbstbestimmung enthält die „Befugnis des Einzelnen, grundsätzlich selbst zu entscheiden, wann und innerhalb welcher Grenzen persönliche Lebenssachverhalte offenbart werden." Darin eingeschlossen ist „die Befugnis des Einzelnen, grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen". Diese Befugnis sieht das Bundesverfassungsgericht „vor allem deshalb gefährdet, weil bei Entscheidungsprozessen nicht mehr wie früher auf manuell zusammengetragene Karteien und Akten zurückgegriffen werden muß, vielmehr heute mit Hilfe der automatisierten Datenverarbeitung Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren Person technisch gesehen unbegrenzt speicherbar und jederzeit ohne Rücksicht auf Entfernungen in Sekundenschnelle abrufbar sind." Andererseits wäre mit dem Recht auf informationelle Selbstbestimmung eine Rechtsordnung nicht vereinbar „in der Bürger nicht mehr wissen können, wer was wann und bei welcher Gelegenheit über sie weiß. Wer unsicher ist, ob abweichende Verhaltensweisen jederzeit notiert und als Information dauerhaft gespeichert, verwendet oder weitergegeben werden", wird „möglicherweise auf eine Ausübung seiner entsprechenden Grundrechte verzichten". Dies würde jedoch die individuellen Entfaltungschancen des Einzelnen beeinträchtigen. Selbstverständlich ist dieses Grundrecht nicht schrankenlos gewährleistet. Eingriffe bedürfen allerdings eines Gesetzes.

Bezüglich der Datenerhebung stellt das Bundesverfassungsgericht fest, daß bei der Bewertung der Tragweite eines Eingriffs „nicht allein auf die Art der Angaben abgestellt werden" kann, sondern daß entscheidend „ihre Nutzbarkeit und Verwendungsmöglichkeit" seien. Dies wiederum hänge von dem Zweck, dem die Erhebung dient, und von den technischen Möglichkeiten der Datenverarbeitung ab. Daraus ist jedenfalls der Schluß zu ziehen, daß „zwangsweise" Datenerhebungen durch die Polizei eines Gesetzes bedürfen. Solche Datenerhebungen liegen immer dann vor, wenn der Bürger auf Grund eines Gesetzes zu Angaben verpflichtet ist. Auf eine besondere gesetzliche Regelung der Datenerhebung kann nur dann verzichtet werden, wenn diese wirklich freiwillig erfolgt, also mit entsprechender Aufklärung der Betroffenen. Kann die Polizei den Betroffenen über Grund und Zweck der Befragung aus polizeitaktischen oder sonstigen Gründen nicht aufklären, stehen derartige Datenerhebungen ebenfalls unter einem Gesetzesvorbehalt. Denn solche Datenerhebungen können sehr wohl zur Folge haben, daß der Betroffene sich in seiner Handlungsfreiheit beeinträchtigt sieht. Soweit die Polizei Daten über einen Betroffenen dadurch erlangt, daß sie Dritte befragt, bedarf sie hierfür ebenfalls eines Gesetzes. Denn auch diese Form der Informationserhebung kann die Entscheidungsfreiheit des Betroffenen beeinträchtigen. Gleiches dürfte auch für die Fälle gelten, in denen die Polizei den Bürger in der Öffentlichkeit mit der Absicht beobachtet, hieraus Daten zu gewinnen oder auf dieser Grundlage polizeiliche Maßnahmen zu ergreifen. Dies kann eine entsprechende Beobachtung der Verhaltensweisen im Straßenverkehr oder das Fotografieren von Bürgern sein.

Wegen der Auswirkungen auf das Grundrecht auf informationelle Selbstbestimmung, also „die Befugnis des Einzelnen, grundsätzlich selbst über die Preisgabe und die Verwendung seiner persönlichen Daten zu bestimmen", ist aus den gleichen Gründen auch für die übrige polizeiliche Datenverarbeitung, also insbesondere das Speichern und Übermitteln personenbezogener Daten durch die Polizei, ein Gesetz erforderlich.

Die bisherigen Regelungen in den Polizeigesetzen – dies gilt erst recht für die entsprechenden Rechtsgrundlagen für die Tätigkeit des Bayer. Landesamtes für Verfassungsschutz -, welche Befugnisse für bestimmte polizeiliche Eingriffe enthalten, genügen für Eingriffe durch polizeiliche Datenverarbeitung grundsätzlich nicht. Im Hinblick auf die vom Bundesverfassungsgericht entwickelten Grundsätze der Normenklarheit ist eine spezielle bereichsspezifische gesetzliche Regelung für die Erhebung und Verarbeitung von personenbezogenen Daten durch die Polizei und die Verfassungsschutzbehörden erforderlich. Weil eine pauschale Generalermächtigung hierfür nicht genügt, werden Datenerhebung, Datenverarbeitung und die in diesem Zusammenhang durch das Bundesverfassungsgericht dem Bürger zustehenden Aufklärungs- und Auskunftsrechte im einzelnen geregelt werden müssen.

4.3.3. Prüfungen bei Polizeibehörden

Im Berichtszeitraum habe ich datenschutzrechtliche Prüfungen beim Präsidium der Bayer. Grenzpolizei, dem Polizeipräsidium Unterfranken, 5 Polizeidirektionen, 11 Polizei- bzw. Kriminalpolizeiinspektionen und einer Wasserschutzpolizeistation durchgeführt. Diese im Regelfall nur kurzen Besuche bei den einzelnen Polizeibehörden dienten neben der Feststellung, ob die Datenschutzvorschriften beachtet werden, auch der persönlichen Kontaktaufnahme. Ich habe

die Erfahrung gemacht, daß das zwischen Datenschutz und Polizei manchmal bestehende Spannungsverhältnis durch persönliches Kennenlernen und Gespräche am besten abgebaut werden kann. Schwerpunkte der Kontrollen und der dabei geführten Gespräche waren

- der Datenverkehr zwischen der Polizei und anderen Behörden,
- die Führung der kriminalpolizeilichen Sammlungen, hierbei insbesondere die Einhaltung der Aussonderungsfristen,
- die Regelungen über den Zugriff auf Karteien/Dateien außerhalb der normalen Dienstzeit und
- der polizeiliche Fahndungsabgleich.

In nahezu allen Fällen verliefen die Gespräche und die Prüfungen in einer sehr erfreulichen Atmosphäre. In keinem Fall wurde meinen Mitarbeitern der Zutritt zu Räumen verweigert oder die Einsichtnahme in Akten oder Karteien untersagt. Dies begrüße ich. Schwerwiegende Verstöße gegen Datenschutzvorschriften habe ich in keinem Falle festgestellt. Verschiedentlich habe ich kritisiert, daß die Führung der kriminalpolizeilichen Sammlung und der entsprechenden Suchkarten nicht in allen Punkten den KpS-Richtlinien entspricht. Insbesondere mangelte es an der richtigen Eintragung der Aussonderungsfristen und in einigen Fällen auch an deren Beachtung. In diesem Zusammenhang habe ich auch immer wieder festgestellt, daß als Aussonderungsfristen schematisch die Regelfristen nach den KpS-Richtlinien eingetragen worden sind, obwohl in einer Reihe von Fällen das Setzen von kürzeren Fristen veranlaßt gewesen wäre. Dieses Verhalten war teilweise darauf zurückzuführen, daß mit dieser Aufgabe Hilfskräfte betraut waren. Im übrigen konnte in einer Reihe von Fällen eine sachgerechte Führung der Kriminalakten schon deswegen nicht garantiert werden, weil den Polizeibehörden der Ausgang des Verfahrens nicht bekannt war. Allerdings habe ich auch festgestellt, daß selbst dann, wenn die Staatsanwaltschaft beispielsweise Verfahrenseinstellungen nach § 170 Abs. 2 StPO oder Freisprüche mitgeteilt hatte, die Regelfristen unverändert geblieben und die Akten nicht ausgesondert worden waren. Doch waren dies letztlich einzelne Fälle.

Ich habe allerdings den Eindruck gewonnen, daß über den genauen Umfang der in Akten oder Karteien aufzunehmenden Daten Unsicherheit herrscht. Das Beispiel einer Staatsschutzkartei, die bei einer Kriminalpolizeiinspektion geführt wird und in der Daten enthalten waren, die jedenfalls zur polizeilichen Aufgabenerfüllung nicht erforderlich waren, zeigt, daß immer wieder nach dem Grundsatz verfahren wird, im Zweifel für die Aufnahme. Auffällig ist auch, daß die Aufbewahrungsdauer sonstiger polizeilicher Unterlagen von Dienststelle zu Dienststelle schwankt. So werden beispielsweise Unterlagen über durchgeführte Blutentnahmen teilweise nach Erledigung des Vorgangs, in manchen Fällen nach 5 Jahren und an anderer Stelle erst nach 10 Jahren vernichtet. Es kann auch keinen Zweifel geben, daß die Aufbewahrung von Verwarnungsbelegen und Ordnungswidrigkeitenanzeigen über einen Zeitraum von 20 Jahren unzulässig ist. Auch die Aufbewahrung von Fallakten über Todesfälle, die keinen Verdacht auf Straftaten begründen, über einen Zeitraum von 10 Jahren ist nicht erforderlich.

Auch die Datensicherung sollte bei einigen Dienststellen verbessert werden. So wurden z.B. bei einer Kriminalpolizeiinspektion die Kartei der Rauschgifttäter sowie die Fahndungs-Lichtbild-Kartei in offenen Holzkästen untergebracht, die unverschlossen auf einem Schrank im Erdgeschoß aufbewahrt waren. Ein Zugriff Unbefugter auf diese besonders sensiblen Daten war damit nicht im erforderlichen Maße ausgeschlossen.

### 4.3.4. Kriminalpolizeiliche Sammlungen (KpS)

#### 4.3.4.1. Umsetzung der Richtlinien

Die Richtlinien für die Führung kriminalpolizeilicher personenbezogener Sammlungen (KpS-Ri) sind in Bayern nun seit gut zwei Jahren in Kraft. Sie haben sich aus der Sicht des Datenschutzes unbeschadet der Notwendigkeit einer gesetzlichen Regelung grundsätzlich bewährt.

Im Zusammenhang mit der in Nr. 6 der KpS-Ri geregelten Aufbewahrungsdauer haben sich im Vollzug einige Unsicherheiten gezeigt. So bestimmt 6.1 KpS-Ri, daß die Aufbewahrung von Kriminalakten solange zulässig ist, wie dies zur rechtmäßigen Erfüllung der in der Zuständigkeit der Aufbewahrungsstelle liegenden Aufgaben erforderlich ist. Sobald die Aufbewahrung nicht mehr zulässig ist, sind die Unterlagen auszusondern. Um den Vollzug dieser Aufbewahrungsbestimmung zu vereinheitlichen, enthalten die KpS im Sinne einer „verallgemeinernden Interessenabwägung" für die Aussonderung sog. „Regelfristen". Diese lauten für Erwachsene 10 Jahre, für Jugendliche 5 und für Kinder 2 Jahre. Daneben wird unter anderem bestimmt, daß in Fällen von geringerer Bedeutung die Aussonderung grundsätzlich nach kürzerer Frist zu erfolgen hat und daß diese bereits bei Einstellung der Unterlagen entsprechend zu vermerken ist.

Meine Erfahrungen haben nun gezeigt, daß in der überwiegenden Zahl der Fälle nahezu automatisch die Regelfristen für die Aussonderung verfügt werden. Weder die Bestimmung der Aussonderung nach kürzer Frist bei Geringfügigkeit noch der allgemeine Grundsatz, daß die Aufbewahrung nur solange zulässig ist, wie sie für die Aufgabenerfüllung erforderlich ist, führen zu einer mehr auf den Einzelfall abgestellten Vergabe der Aufbewahrungsfristen. Da die mit der Führung der Kriminalakten befaßten Bediensteten mangels näherer Kenntnis des Akteninhalts häufig zur Vergabe der Regelfristen neigen, sollte überlegt werden, ob die Vergabe der Fristen nicht vom jeweiligen Kriminalsachbearbeiter vorgenommen werden sollte. Wegen seiner Sachnähe könnte er wohl am besten entscheiden, wie lange die Unterlagen zur polizeilichen Aufgabenerfüllung erforderlich sind.

Im Zusammenhang mit der Aufbewahrung von Kriminalakten sind noch weitere Probleme deutlich geworden:

- Die KpS-Richtlinien bestimmen, daß abweichend von den vorgenannten Regelungen zur Aufbewahrungsdauer die polizeilichen Unterlagen auszusondern sind, wenn die polizeilichen Ermittlungen oder eine der Polizei bekanntgewordene Entscheidung der Staatsanwaltschaft oder eines Gerichtes ergeben, daß die Gründe, die zur Aufnahme in die Kriminalaktensammlung geführt haben, nicht zutreffen. Diese Voraussetzungen liegen immer dann vor, wenn der Betroffene infolge erwiesener Unschuld freigesprochen worden ist oder die Staatsanwaltschaft das Verfahren nach § 170 Abs. 2 Strafprozeßordnung eingestellt hat, weil der Betroffene die ihm zur Last gelegte Straftat nicht begangen hat. Unabhängig von dem Problem, daß die Polizei nicht in allen Fällen

über den Verfahrensausgang bei Gericht oder der Staatsanwaltschaft unterrichtet wird – hierauf wird an anderer Stelle eingegangen – hat die Polizei in den vorgenannten Fällen die entsprechenden Unterlagen aus ihren Kriminalakten zu entfernen.

- Aussonderung bedeutet nach dem insoweit eindeutigen Wortlaut der KpS-Richtlinien, daß diese Unterlagen zu vernichten sind. Diese Bestimmung darf nicht dadurch umgangen werden, daß die Unterlagen zwar aus der Kriminalaktensammlung entfernt, aber statt sie der Vernichtung zuzuführen, sie in die Fallakten eingeordnet werden. Sollte die sog. „Vorgangsverwaltung" auch noch automatisiert werden, wäre es denkbar, daß diese Unterlagen ohne größeren Aufwand über die Fallakten personenbezogen auffindbar wären.

  In diesem Zusammenhang ist noch auf eine interessante Entscheidung des Bayer. Verwaltungsgerichtshofs vom 27.9.1983 Nr. 21 B 82 A 2261 hinzuweisen. Der Bayer. Verwaltungsgerichtshof hatte sich in dieser Entscheidung mit einem Anspruch auf Vernichtung von Kriminalakten auseinanderzusetzen. Hierbei hat das Gericht festgestellt, „daß die Führung und weitere Aufbewahrung einer Kriminalakte einen über den polizeiinternen Bereich hinausgehender Eingriff in die Rechte des Klägers aus Art. 2 Abs. 1 GG (Grundgesetz) darstellt und nur auf Grund einer entsprechenden Befugnisnorm rechtmäßig ist, daß aber die allgemeine Aufgabenzuweisung der Gefahrenabwehr in Art. 2 Abs. 1 PAG (Polizeiaufgabengesetz) hierzu nicht ausreicht". Im konkreten Fall hatte das Gericht die Klage auf Vernichtung der Akten abgewiesen.

4.3.4.2. Aktenaussonderung beim Bayer. Landeskriminalamt

Die beim Bayer. Landeskriminalamt am 1.11.1979 begonnene Sonderaktion zur Bereinigung der kriminalpolizeilichen Aktensammlung hatte ich bereits in meinem letzten Tätigkeitsberichten angesprochen. Nach Mitteilung des Bayer. Landeskriminalamtes, das für diese Sonderaktion ständig eine Gruppe von Kriminalpolizeibeamten abgestellt hatte, ist die Aktenbereinigung am 30.11.1983 abgeschlossen worden. Bei Beginn dieser Maßnahme am 1.11.1979 hatte das Bayer. Landeskriminalamt einen Bestand von 718.375 Kriminalakten. Am 30.11.1983 enthielt die Aktensammlung noch 373.131 Kriminalakten. Da in der Zwischenzeit 164.568 Kriminalakten neu angelegt worden sind, sind in den 49 Monaten der Bereinigungsaktion insgesamt 509.812 Kriminalakten ausgesondert und vernichtet worden. Der Aktenbestand des Bayer. Landeskriminalamtes hat sich somit um ca. 50% verringert.

Ich begrüße es außerordentlich, daß das Bayer. Landeskriminalamt als die zentrale bayerische Dienststelle für kriminalpolizeiliche Aufgaben die Aktenbereinigung mit besonderem Engagement vorbildlich durchgeführt hat. In diesem Zusammenhang möchte ich noch einmal deutlich machen, daß nicht die Vernichtung von Daten an sich das alleinige Erfolgskriterium eines Datenschutzbeauftragten sein kann. Werden hingegen die Akten und die sonstigen Datensammlungen so bereinigt, daß sie nur noch das für die gesetzliche Aufgabenerfüllung erforderliche Maß an Daten enthalten, ist ein solches Ergebnis nicht allein aus Datenschutzgründen erfreulich. Gleichzeitig erlauben solcher Art bereinigte Akten auch eine effektivere Aufgabenerfüllung der Behörde. Nicht die absolute Zahl von Informationen ist wichtig, sondern entscheidend ist deren Relevanz. Insoweit können die Belange des Datenschutzes mit den Behördeninteressen weitgehend deckungsgleich sein.

4.3.4.3. Kriminalaktensammlung beim Polizeipräsidium München

Die Kriminalaktensammlung des Polizeipräsidiums München umfaßt derzeit einen Bestand von 1 Million personenbezogener Akten. Diese Zahl ist bemerkenswert hoch in Anbetracht der Tatsache, daß im Zuständigkeitsbereich des Polizeipräsidiums München gut 1 1/2 Millionen Einwohner leben, Säuglinge und Greise eingeschlossen. Zwar hat auch das Polizeipräsidium München für die Aussonderung nicht mehr aktueller Akten eine ständige Gruppe von Dienstkräften eingesetzt, doch ist diese offensichtlich auch nicht annähernd in der Lage den Aktenbestand entsprechend den KpS-Richtlinien zu bereinigen. Im übrigen erscheint auch das Verhältnis der Zahlen der überprüften mit der Menge der anschließend vernichteten Akten bedenklich. Stichproben deuten daraufhin, daß beim Polizeipräsidium München wohl zu wenige Akten der Aussonderung zugeführt werden. So sind in den Jahren 1979 – 1983 zwar 547 955 Akten überprüft, aber nur 98 827 Akten vernichtet worden. Allerdings hat die Aussonderung in den letzten beiden Jahren zugenommen.

Auch die Verantwortlichen des Polizeipräsidiums München sind sich der Tatsache bewußt, daß ein nicht unerheblicher Teil der Kriminalakten nach den geltenden Bestimmungen in der vorliegenden Form nicht mehr geführt werden dürfte. Deshalb ist zumindestens Sorge dafür getragen, daß auf Anfragen anderer Behörden Auskünfte aus den Polizeiakten nur in dem Umfang gegeben werden, als diese noch zulässigerweise geführt werden dürften. Allerdings ist selbst bei dieser Verfahrensweise nicht zu verhindern, daß sich die Kriminalpolizeibeamten in einer Vielzahl von Fällen mit überholten Aktenbeständen befassen müssen und von Vorgängen Kenntnis nehmen, die eigentlich hätten vernichtet sein sollen.

Ich bin der Auffassung, daß das Polizeipräsidium München die Aktenbereinigung stark beschleunigen muß und hier gegebenenfalls andere organisatorische Maßnahmen zur Erreichung dieses Ziels getroffen werden müssen.

4.3.5. Kriminalaktennachweis (KAN)

Der Kriminalaktennachweis (KAN) dient dem Nachweis von Kriminalakten, die beim Bund und bei den Ländern geführt werden. Der Kriminalaktennachweis wird als Datei auf verschiedenen Ebenen geführt. Als sog. „Bundesgionaler KAN" bei den Polizeidirektionen und dem Polizeipräsidium München.

Der Bundes-KAN wird vom Bundeskriminalamt im System INPOL-Bund neben der Personenfahndung, der Haftdatei, der Sachfahndung und den erkennungsdienstlichen Daten geführt. Entgegen ursprünglichen Plänen sind im Bundes-KAN nicht mehr alle kriminalpolizeilich relevanten Unterlagen erfaßt. Vielmehr soll sich der Bundes-KAN darauf beschränken, Hinweise auf besonders schwere Straftaten oder Straftaten mit überregionaler Bedeutung zu geben. Aus der Sicht des Datenschutzes ist diese Beschränkung des Bundes-KAN zu begrüßen. Die Praxis muß allerdings zeigen, inwieweit diese Abschichtung nach wirklich bundesweit relevanten Straftaten vollzogen wird. Ein weiteres

Problem zeigt sich in diesem Zusammenhang in der zentralen Registrierung erkennungsdienstlicher Unterlagen beim Bundeskriminalamt (insofern verweise ich auf den 5. Tätigkeitsbericht des Bundesbeauftragten für den Datenschutz S. 88).

Im „Landes-KAN" und im „regionalen KAN" werden die Kriminalakten bayerischer Polizeivollzugsdienststellen nachgewiesen. Sie geben Auskunft, ob über eine bekannte Person bei Dienststellen der bayerischen Polizei Akten geführt werden. Eine bayerische Besonderheit ist die Aufteilung des für bayerische Kriminalakten geführten Kriminalaktennachweises in einen „Landes-KAN" und in einen „regionalen KAN". In dem bei den einzelnen Polizeidirektionen geführten regionalen KAN werden weitgehend dezentralisiert die Nachweise über Akten der Personen geführt, die lediglich auf örtlicher Polizeiebene von Bedeutung sind. Mit dieser weiteren Aufteilung des Kriminalaktennachweises wird dem Grundsatz des Datenschutzes Rechnung getragen, daß jede Behörde nur die Daten speichern und nur auf die Daten zugreifen darf, die sie zu ihrer gesetzlichen Aufgabenerfüllung braucht.

Zur Errichtung der Datei „Kriminalaktennachweis" hat das Bayer. Staatsministerium des Innern inzwischen eine Errichtungsanordnung erlassen. Diese Errichtungsanordnung trägt Datenschutzbelangen in einer Reihe von Bestimmungen Rechnung. Neben der begrüßenswerten Tatsache der Aufteilung „in Landes-KAN" und „regionalen KAN" ist ebenfalls erfreulich, daß unter bestimmten Voraussetzungen Informationen über Personen nicht aufgenommen werden, die lediglich als Ersttäter von Antrags- und Fahrlässigkeitsdelikten aufgetreten sind.

Das Bayer. Staatsministerium des Innern hatte mir zu der Errichtungsanordnung Gelegenheit zur Stellungnahme gegeben. Obwohl manchen meiner Anregungen Rechnung getragen worden ist, sind doch einige Bedenken unberücksichtigt geblieben. So hatte ich beispielsweise darauf hingewiesen, daß der Katalog der neben den rechtmäßigen Personalien aufzunehmenden personengebundenen Hinweise äußerst umfangreich ist. Zwar wurden die ursprünglich vorgesehenen Hinweise „Sexuell abartig" und „Homosexuell" gestrichen, doch habe ich auch bei der großen Zahl der nach wie vor bestehenden Hinweise erhebliche Zweifel, ob alle diese Daten in einem Kriminalaktennachweis, der eine Schnellorientierung über die einzelnen Personen ermöglichen soll, wirklich erforderlich sind. Meines Erachtens würde es hier genügen, wenn der Sachbearbeiter die entsprechenden personengebundenen Hinweise bei einer Durchsicht im Kriminalakt des Betroffenen vorfindet und auf diese Weise die notwendigen Informationen erhält. Im KAN selbst sollten nur die personengebundenen Hinweise aufgenommen werden, die der einzelne Polizeibeamte sofort bei Erfüllung seiner Aufgaben benötigt. Hierzu können die Hinweise „Bewaffnet", „Gewalttätig" und „Ausbrecher" gehören, um einige aufzuzählen, die für die Sicherheit des Polizeibeamten wie auch des Betroffenen notwendig sind.

Den Aufbau der Datei „Kriminalaktennachweis" auf Landes- und regionaler Ebene werde ich beobachten. Dabei beabsichtige ich mein Augenmerk insbesondere darauf zu richten, ob die Abschichtung zwischen Bundes-, Landes- und regionalem KAN beachtet wird und nur solche Kriminalakten registriert werden, die nach den Richtlinien über kriminalpolizeiliche Sammlungen auch tatsächlich geführt werden dürften.

4.3.6. Spurendokumentationssysteme

Spurendokumentationssysteme (SPUDOK) sollen die Ermittlungsbehörden bei der Bearbeitung umfangreicher Ermittlungsverfahren unterstützen. Das Bayerische Staatsministerium des Innern hat den Einsatz von Spurendokumentationssystemen freigegeben, soweit sie in Ermittlungsverfahren zur Aufklärung von Straftaten oder zur Unterstützung von Sonderkommissionen bei der Ermittlungstätigkeit erforderlich sind. Wie bereits im letzten Tätigkeitsbericht dargestellt, soll der Einsatz von Spurendokumentationssystemen der Polizei erlauben, einen Überblick über eine Vielzahl von Hinweisen und Spuren jeder Art zu erhalten, die im Rahmen der polizeilichen Ermittlungstätigkeit angefallen sind. Gegenüber anderen polizeilichen Datenverarbeitungssystemen zeichnen sich Spurendokumentationssysteme dadurch aus, daß in jeder Datengruppe recherchierbare personenbezogene Daten enthalten sein können und außerdem Verknüpfungen zu anderen Daten durch entsprechende Hinweise möglich sind. Außerdem können die Daten nicht nur formatiert, sondern auch im Freitext gespeichert werden. Wegen dieser umfangreichen Speicher- und Verknüpfungsmöglichkeiten sind Spurendokumentationssysteme sehr flexibel. Der verstärkte Einsatz dieser Systeme und neuere Überlegungen in Bund und Ländern, ihre Spurendokumentationssysteme gegenseitig abzugleichen, machen es dringend erforderlich, die datenschutzrechtlichen Probleme bei Anwendung dieser Systeme zu klären.

Aus datenschutzrechtlicher Sicht ist neben den bereits in meinem 5. Tätigkeitsbericht aufgezeigten Problemen der Speicherung vieler Nichttatverdächtiger in den Spurendokumentationssystemen und der Speicherung grundsätzlich aller Daten bis zum endgültigen Abschluß des Ermittlungsverfahrens auch bedeutsam, daß die umfangreichen Speicher- und Verknüpfungsmöglichkeiten der großen Freitextdatenbestände das verstärkte Risiko in sich bergen, daß Unschuldige durch eine „Verdachtsverdichtung" zu Verdächtigen werden. Dies jedenfalls ist für jeden Unschuldigen ein schwerer Eingriff. Nicht zuletzt aus diesem Grunde wird zu überlegen sein, inwieweit Umfang und Grenzen des Einsatzes polizeilicher Spurendokumentationssysteme sowie deren eventuelle Verbindung mit anderen Datensammlungen einer gesetzlichen Grundlage bedürfen. Keinesfalls darf der im Einzelfall möglicherweise berechtigte Wunsch von Verteidigern, Spurenakten einzusehen, als Alibi für die Polizeibehörden dienen, die im Rahmen von Spurendokumentationssystemen angesammelten großen Datenmengen über einen langen Zeitraum aufzubewahren, ohne zwischenzeitlich die Daten zu bereinigen und die Daten von Unschuldigen und erkennbar Nichtbeteiligten zu löschen. Die Auffassung des Bundesverfassungsgerichts, daß „Persönlichkeitsrechte Dritter gegenüber der gebotenen Wahrheitsermittlung im Strafverfahren regelmäßig nachrangig" seien (BVerfGE 63, S. 45/72), darf nicht dazu führen, die Persönlichkeitsrechte der Betroffenen völlig zurückzustellen.

Solange entsprechende ausdrückliche Regelungen für Spurendokumentationssysteme fehlen, sind in diesen Systemen aufgenommene Daten, wie dies bereits die KpS-Richtlinien bestimmen, nach kürzeren als den in diesen Richtlinien genannten Regelfristen bzw. bereits im Rahmen der laufenden Sachbearbeitung auszusondern, wenn

- sie Anzeigenerstatter, Hinweisgeber, Zeugen oder Geschädigte betreffen,

- die Ermittlungen ergeben, daß die Gründe, die zur Aufnahme geführt haben, nicht zutreffen oder
- ihre Kenntnis zur rechtmäßigen Aufgabenerfüllung nicht mehr erforderlich ist.

Keinesfalls darf jedoch der Grundsatz bestehen, daß jedes in einem Spurendokumentationssystem aufgenommene Datum bis zum Zeitpunkt des rechtskräftigen Urteils gespeichert bleiben darf. Schließlich ist gerade wegen der breiten Materialfülle sicherzustellen, daß der Grundsatz der Zweckbindung streng beachtet wird. Die Informationen dürfen also nur für das Verfahren verwendet werden, für das sie eingestellt worden sind, und nur den Beamten zugänglich sein, die mit der Bearbeitung des entsprechendenen Verfahrens betraut sind. Schließlich sollte, um die Gefahr von Fehlbeurteilungen möglichst gering zu halten, bei der Speicherung bereits deutlich gemacht werden, ob die gespeicherten Personen Verdächtige, Zeugen, Hinweisgeber oder „andere Personen" sind.

4.3.7. Personengebundene Hinweise und Verwendung des Begriffs „Zigeunername"

Aufgabe des Datenschutzes ist es auch, jeder Form von personenbezogener Datenverarbeitung entgegenzuwirken, die geeignet ist, einer Diskriminierung ethnischer Gruppen Vorschub zu leisten.

So hatte ich mich auch mit der Frage einer möglichen Sondererfassung von Landfahrern oder von Angehörigen der Volksgruppen der Sinti und Roma schon seit langem befaßt. Meine diesbezüglichen Feststellungen sowie die mehrfach eindeutigen Aussagen des Bayer. Staatministeriums des Innern hatten ergeben, daß eine derartige Sondererfassung dieser Bevölkerungsgruppen weder im Bayer. Landeskriminalamt noch bei bayerischen Polizeibehörden erfolgt. Allerdings bestand jedoch ein diese Volksgruppen berührendes Problem:

In dem weitgehend bundeseinheitlichen polizeilichen Informationssystem „INPOL" wird neben anderen Namenskürzeln auch das Kürzel „ZN", das Zigeunername bedeutet, verwendet. Speziell in dieser Angelegenheit hatte ich mich schriftlich an das Bayer. Staatsministerium des Innern gewandt und um Mitteilung gebeten, ob auf die Verwendung dieses Kürzels wegen dessen diskriminierender Wirkung verzichtet werden könne. Die Verwendung des Kürzels „ZN" wurde damit begründet, daß der „Zigeunername" nicht mit dem Namen im Geburtsregister identisch sei, wie dies vergleichbar auch bei Künstlernamen oder Ordensnamen der Fall sei. Die Aufnahme des „Zigeunernamens" sei deshalb ein notwendiges Hilfsmittel zur eindeutigen Identifizierung. Im übrigen erfolge die Erfassung dieser Namen nur, wenn die Personen einer Straftat verdächtig seien oder wegen Verdachts einer Straftat gesucht würden.

Meine eigenen Ermittlungen hatten im übrigen ergeben, daß das Kürzel „ZN" zumindest kein Suchbegriff im Informationssystem „INPOL" ist. Über die den Polizeibeamten zugängigen Datensichtgeräte war es demnach nicht möglich, beispielsweise alle gespeicherten Personen dieser ethnischen Gruppe auf einmal zu erhalten oder überhaupt mit der Verwendung allein dieses Kürzels auf einen bestimmten Angehörigen dieser Personengruppe zu stoßen.

Um möglichst jede, diese Personengruppe diskriminierende Verwendung der mit „ZN" oder „Landfahrer" gekennzeichneten Daten auszuschließen, hatte ich mich gleichwohl für deren Streichung ausgesprochen. So begrüße ich es, daß in den polizeilichen Informationssystemen nunmehr der personengebundene Hinweis „Landfahrer" gestrichen wird. Weiterhin war es konsequent, im INPOL-System der Polizei die Kennung „ZN", welche die Abkürzung für „Zigeunername" war, entfallen zu lassen. Dabei kann hingenommen werden, daß künftig im Datenfeld „SN" („Sonstiger Name") zusammen mit anderen sonstigen Namen auch diejenigen Namen gespeichert werden, mit denen Zigeuner von ihren Familienangehörigen und Freunden gerufen werden. Allerdings wird durch die daneben beschlossene Einführung eines neuen personengebundenen Hinweises „HWAO" (Häufig wechselnder Aufenthaltsort), der bei solchen Personen vermerkt wird, die ihren Aufenthaltsort häufig wechseln, und die Beibehaltung des Merkmals „LAST" für Stadt- und Landstreicher das beabsichtigte Ziel, einer möglichen Diskriminierung der „Zigeuner" entgegenzuwirken, zumindest teilweise wieder zunichte. Das Merkmal „HWAO" findet grundsätzlich für Betroffene ohne festen Wohnsitz oder mit häufig wechselndem Aufenthaltsort Anwendung. Dieser Hinweis ist also nicht auf „Zigeuner" beschränkt. Wenn jedoch neben dem neuen personengebundenen Hinweis „HWAO" auch der Hinweis „LAST" für Stadt- und Landstreicher beibehalten bleibt, ist dies aus datenschutzrechtlicher Sicht problematisch. Findet sich nämlich bei einem Betroffenen der Hinweis „HWAO", jedoch nicht der Hinweis „LAST", so liegt die Vermutung nahe, daß es sich bei der betroffenen Person um einen „Zigeuner" handelt. Meines Erachtens könnte diesem Risiko dadurch begegnet werden, daß der Hinweis „LAST" entfällt und nur der Hinweis „HWAO" beibehalten wird. Dieser Hinweis könnte sodann bei allen Personen, die häufig ihren Aufenthaltsort wechseln oder aus welchen Gründen auch immer keinen festen Wohnsitz haben, Anwendung finden. Ein ethnischer Bezug wäre nicht mehr zu erkennen.

4.3.8. Verkehrsordnungswidrigkeiten

Mit dem Verfahren zu Verkehrsordnungswidrigkeiten hatte ich mich unter verschiedenen Gesichtspunkten zu befassen.

4.3.8.1. Umfang der Datenerhebung

Der Umfang der Datenerhebung im Anhörungsverfahren wegen Verkehrsordnungswidrigkeiten war bislang nicht auf das erforderliche Maß beschränkt. Ebenfalls fehlte auf den Formblättern der nach Art. 16 Abs. 2 BayDSG erforderliche Hinweis, welche Angaben freiwillig sind. Das Bayer. Staatsministerium des Innern hat mir nun schriftlich mitgeteilt, daß der Umfang der Datenerhebung im Bußgeldverfahren wegen Verkehrsordnungswidrigkeiten künftig eingeschränkt wird. So wird auf die Merkmale „Familienstand, Beruf und Staatsangehörigkeit" verzichtet. Freiwillige Angaben des Betroffenen werden als solche in den Formularen eindeutig erkennbar sein.

4.3.8.2. Dauer der Speicherung

Zur Dauer der bei Ahndung bußgeldbewehrter Straßenverkehrsverstöße gespeicherten Daten durch das Polizeipräsidium München habe ich folgendes festgestellt:

Grundsätzlich speichert das Polizeipräsidium München die Daten von Verkehrsverstößen über einen Zeitraum von 4 Monaten. Diese Verfahrensweise stützt die Polizei zum

einen darauf, daß nicht vorhergesehen werden kann, in welchen Verfahren nachträglichen Einwendungen zu begegnen ist, und zum anderen auf zwingende organisatorische, kassentechnische und statistische Gründe. Nach Ablauf dieser Frist werden die Daten gelöscht. Aus Datenschutzgründen habe ich gegen diese Verfahrensweise keine Bedenken erhoben.

4.3.8.3. Angabe der Namen auf Überweisungsträgern

So hatte ein Bürger gerügt, daß die Zentrale Bußgeldstelle auf den Überweisungsträgern den Namen des Betroffenen eintrage, wodurch dem angewiesenen Geldinstitut die Tatsache eines Bußgeldverfahrens bekannt würde. Auf meine entsprechende Anfrage hin hat die Zentrale Bußgeldstelle mitgeteilt, daß sie keine Möglichkeit sehe, das betreffende Bußgeldverfahren auf den Überweisungsträgern durch nicht personenbezogene Daten zu kennzeichnen, wie ich dies zunächst angeregt hatte. Der Name des Betroffenen auf dem Überweisungsträger sei unverzichtbar. Etwa 50% der Bußgeldbescheide würden nicht maschinell erstellt. In all diesen Fällen müßte der Zahlschein von Hand dem jeweiligen Vorgang zugeordnet werden. Fehler bei der Zuordnung seien bisher selten, da die Sortierkräfte sich nach dem Namen orientieren könnten. Außerdem sei die Angabe des Namens auf dem Überweisungsträger für die Vornahme von Umbuchungen wegen Überzahlungen oder Doppelzahlungen sowie für Rückzahlungen notwendig. Auch bei Stornierungen der Geldinstitute sei ohne Angabe des Namens eine erneute Sollstellung des richtigen Betroffenen nicht möglich. Ebensowenig könne auf das Aktenzeichen bei den Überweisungsträgern verzichtet werden, da sonst einlaufende Zahlungen des Betroffenen nicht zugeordnet und verbucht werden könnten.

Bei meiner Überprüfung des Sachverhalts hatte ich im übrigen auch festgestellt, daß ein Verzicht auf die Angabe von Aktenzeichen und Namen des Betroffenen auf den Überweisungsträgern auch nicht zwangsläufig dazu führen würde, daß dem angewiesenen Geldinstitut die Tatsache eines Bußgeldverfahrens nicht mehr bekannt würde. Da die Überweisungen zwangsläufig immer an den Empfänger „Zentrale Bußgeldstelle" gehen und diese Stelle nur Zahlungen von Bußgeldern und Kosten des Bußgeldverfahrens entgegennimmt, ist ohnehin jedem Mitarbeiter eines Geldinstitutes allein durch die Angabe des Empfängers der Grund für die Überweisung offenkundig. Deshalb hatte ich auch meine zunächst geäußerten Bedenken gegen die Angabe von Aktenzeichen und Namen auf den vorgedruckten Überweisungsträgern zurückgestellt. Will ein Betroffener vermeiden, daß sein Bankinstitut von der Tatsache eines Bußgeldverfahrens Kenntnis erlangt, muß er entweder die Zahlungen bar bei der Zentralen Bußgeldstelle leisten oder sich einer Postüberweisung bedienen.

4.3.9. Datenmißbrauch durch Polizeibeamte

Nachweislich sind mir im Berichtszeitraum nur zwei Fälle bekannt geworden, in denen Polizeibeamte unter Ausnützung ihrer Dienststellung für private Zwecke Daten abgerufen und weitergegeben haben. Soweit Bürger nur ganz allgemein gehaltene Verdachtsmomente ohne wirklich konkrete Hinweise mitteilen oder anonym Polizeibeamte des Datenmißbrauchs beschuldigen, kann ich diesen Hinweisen in der Regel nicht nachgehen. Wenn auch die im folgenden dargelegten Fälle nicht zu verallgemeinern sind, belegen sie doch, daß es echte Mißbrauchsfälle im Polizeibereich gibt. Solche Fälle werden sich wohl auch nie ganz vermeiden lassen. Auch ist zu berücksichtigen, daß mit zunehmender Automatisierung der Polizeidaten und mit dem Anschluß der Polizei an Datenbestände anderer Behörden der dem einzelnen Polizeibeamten durch Direktabfragen zu Verfügung stehende Datenbestand erheblich gewachsen ist. Ob dies den Anreiz zu mißbräuchlichem Datenabruf fördert, kann ich nicht abschließend beurteilen, jedenfalls kann im Mißbrauchsfalle der Schaden für den betroffenen Bürger wesentlich größer werden. Die Dienststellen der Polizei werden sich daher zunehmend mit der Frage nach ausreichenden Datensicherungsmaßnahmen auseinandersetzen müssen. Dieses Problem kann aber auch nicht völlig außer acht bleiben bei den Entscheidungen, ob weitere Datenbestände der Polizei automatisiert oder der Polizei im Wege des Direktabrufs zugänglich gemacht werden sollen.

Nun zu den beiden Fällen:

Wohl um seine frühere Freundin zurückzugewinnen, teilte ihr ein Polizeibeamter nach Einsichtnahme in die entsprechenden kriminalpolizeilichen Unterlagen mit, daß gegen ihren derzeitigen Verlobten polizeiliche Erkenntnisse vorliegen.

Sowohl diese Einsichtnahme in die entsprechenden polizeilichen Unterlagen wie die nachfolgende Datenweitergabe waren unzulässig. Sie stellen auch einen groben Verstoß gegen die KpS-Richtlinien dar. Eine Weitergabe solcher Daten an Privatpersonen ist ausdrücklich nicht gestattet. Der Inhalt der kriminalpolizeilichen Sammlungen ist vertraulich und grundsätzlich nur für den Dienstgebrauch innerhalb der Polizei bestimmt.

Der zweite Fall ist zwar in den Medien bereits ausführlich wiedergegeben worden, gleichwohl möchte ich ihn wegen seiner exemplarischen Bedeutung kurz ansprechen.

Ein Polizeidirektor, Chef einer bayerischen Polizeidirektion, hatte in den letzten Dezembertagen 1983 privat in seiner Eigenschaft als Mitglied des Bezirksschiedsgerichts einer politischen Partei über ein Datensichtgerät der Polizeidirektion beim Einwohnermeldeamt die Ab- und Anmeldedaten eines Einwohners feststellen lassen und die hierdurch gewonnenen Erkenntnisse sowohl an den Vorsitzenden des Parteischiedsgerichts als auch an den Bezirksvorsitzenden der Partei weitergegeben. Das Besondere an diesem Fall lag darin, daß der Polizeidirektor den seinerzeitigen Presseverlautbarungen zufolge Pressevertretern gegenüber die genannten Tatsachen bestätigt und dies als rechtmäßigen Vorgang, der üblich sei, bezeichnet haben soll. Er wurde wörtlich wie folgt zitiert: „Ich habe kein Unrechtsbewußtsein, denn ich habe ja nichts anderes getan, als mein dienstliches Wissen für meine Tätigkeit als juristischer Beisitzer im (Partei)-Schiedsgericht zu nutzen."

Der durch diese öffentliche Einlassung entstandene Eindruck, die Polizei würde dienstliche Kenntnisse über Daten von Bürgern nicht ausschließlich für dienstliche Zwecke verwenden, hat mich veranlaßt, umgehend meinerseits öffentlich eine vorläufige Stellungnahme abzugeben. Dabei habe ich auch meine Besorgnis zum Ausdruck gebracht, daß der Vorfall bei der Bevölkerung Beunruhigung über den bekanntgewordenen Umgang mit Daten auslösen kann. Nachdem der Polizeidirektor auch in seiner dem Staatsministerium des Innern gegenüber abgegebenen Stellungnah-

me den bekanntgewordenen Sachverhalt bestätigt hatte, habe ich durch einen Vertreter meiner Dienststelle auch an Ort und Stelle Ermittlungen durchgeführt. Datenschutzrechtlich ist dieser Sachverhalt wie folgt zu bewerten:

Der Abruf von Daten aus dem Melderegister über ein Polizeiterminal ist rechtlich als Übermittlung dieser Daten von der Meldebehörde an die Polizei zu bewerten. Eine solche Übermittlung ist nach Art. 31 Abs. 1 Meldegesetz nur zulässig, wenn dies zur rechtmäßigen Erfüllung der in der Zuständigkeit der Meldebehörde oder in der Zuständigkeit der Polizeibehörde liegenden Aufgaben erforderlich ist. Beides war offensichtlich nicht der Fall. Der Abruf für nicht dienstliche, und damit private Zwecke, wie er hier vorlag, war unzulässig. Nach Art. 31 Abs. 6 MeldeG darf der Datenempfänger die ihm übermittelten (abgerufenen) Daten nur für den Zweck verwenden, zu dessen Erfüllung sie ihm übermittelt worden sind. Dabei kommen selbstverständlich nur solche Zwecke in Betracht, die im Rahmen der rechtmäßigen Aufgabenerfüllung der Polizei liegen. Eine Unterrichtung Dritter über Meldedaten aus nichtdienstlichen Gründen ist selbstverständlich kein Zweck im Sinne dieser Vorschrift. Erst recht schließt Art. 31 Abs. 6 Meldegesetz eine Weitergabe von Melderegisterdaten von vornherein aus, die die Polizei nicht zur rechtmäßigen Aufgabenerfüllung erlangt hat. Die Weitergabe der unzulässig abgerufenen Daten war daher ebenfalls unzulässig.

Den Datenabruf und die Datenweitergabe durch den Polizeidirektor habe ich gemäß Art. 30 Abs. 1 BayDSG beanstandet. Im übrigen habe ich die Angelegenheit zum Anlaß genommen, über den konkreten Vorfall hinaus den allgemeinen Umgang mit Meldedaten bei der betreffenden Polizeidirektion in meine Ermittlungen einzubeziehen. Die in der Folgezeit vorgenommenen Überprüfungen und die in Absprache mit dem zuständigen Präsidium getroffenen weiteren Kontrollmaßnahmen haben keinen Anlaß zu weiteren Beanstandungen gegeben. Schließlich habe ich auch noch beim betroffenen Einwohnermeldeamt die Bereitstellung von Daten aus dem Melderegister ganz generell geprüft. Auch insoweit hat sich kein Anlaß zu Beanstandungen ergeben.

### 4.3.10. Grenzkontrolle

Die im Rahmen der Grenzkontrolle durchgeführten Überprüfungen haben wiederum eine Reihe von Bürgern veranlaßt, sich wegen der befürchteten Speicherung ihrer Daten an mich zu wenden. In allen Fällen, denen ich nachgegangen war, haben sich die Befürchtungen der Bürger als unbegründet erwiesen. Weder werden im Rahmen der Grenzkontrolle die Personalpapiere abgelichtet – das von der Grenzpolizei verwendete Kontrollgerät wird manchmal mit Kopierautomaten verwechselt – noch werden die auf andere Weise notierten Daten über den Kontrollzweck hinaus gespeichert. So führen z.B. die Beamten der Bayer. Grenzpolizei die Kontrolle in Reisezügen des grenzüberschreitenden Verkehrs stichprobenweise in der Weise durch, daß die Personalien einer bestimmten Anzahl von Personen notiert und mit dem Fahndungsbuch verglichen werden. Bei negativem Vergleich werden die Notizen unverzüglich noch im Dienstraum der Grenzpolizei am jeweiligen Bahnhof ordnungsgemäß vernichtet. Diese Kontrolltätigkeit entspricht im übrigen der gesetzlichen Aufgabe der Grenzpolizei nach Art. 5 Abs. 1 Polizeiorganisationsgesetz.

### 4.3.11. Nachrichtendienste

Aus der Sicht des Bayerischen Landesbeauftragten für den Datenschutz sind unter dem Stichwort Nachrichtendienste zwei Bereiche zu berücksichtigen: Zum einen zählt hierzu die Datenverarbeitung des Bayerischen Landesamtes für Verfassungsschutz und zum anderen sind die Datenübermittlungen bayerischer Behörden an andere Verfassungsschutzbehörden, den Bundesnachrichtendienst und den MAD zu bewerten. Wie ich schon in früheren Tätigkeitsberichten deutlich gemacht habe, ist es mir aus der Natur der Sache heraus versagt, Einzelheiten aus meiner Tätigkeit im Verfassungsschutzbereich zu berichten. Ich werde mich daher auch diesmal darauf beschränken, einige grobe Linien zu zeichnen.

#### 4.3.11.1. Prüftätigkeit beim Bayerischen Landesamt für Verfassungsschutz

Neben einer Reihe von Prüfungen in Einzelfällen habe ich das Landesamt für Verfassungsschutz wiederum zu einer generellen Prüfung aufgesucht. Neben einer Querschnittsprüfung habe ich mich noch mit speziellen, im Berichtszeitraum angefallenen aktuellen Fragen befaßt.

Ein Grund zu einer Beanstandung hat sich aus dieser stichprobenartigen Überprüfung nicht ergeben. Im einzelnen wurde aber beispielsweise festgestellt, daß gerade die erstmaligen Eintragungen in Akten oder auf Karteikarten Tatsachen enthalten, aus denen sich ein Bezug zur gesetzlichen Tätigkeit des Landesamts für Verfassungschutz nicht eindeutig hat entnehmen lassen. Zwar konnte in allen diesen Fällen nach Rücksprache mit den jeweils zuständigen Sachbearbeitern festgestellt werden, daß im Zusammenhang mit den eingetragenen Tatsachen Erkenntnisse gewonnen worden waren, welche für die Tätigkeit des Landesamts für Verfassungsschutz relevant waren, doch ließen sich diese nur aus anderen Akten entnehmen. Um hier Fehlbeurteilungen zu vermeiden, habe ich angeregt, daß zumindest stichwortartig der Bezug zur erforderlichen gesetzlichen Aufgabenerfüllung des Landesamtes für Verfassungsschutz deutlich wird.

Zur Problematik des Datenverkehrs des Landesamtes für Verfassungsschutz mit der Polizei, die ich im letzten Tätigkeitsbericht bereits angesprochen habe, steht eine Lösung der aufgeworfenen Fragen noch aus. Die bereits vor einem Jahr geäußerten Bedenken bestehen nach wie vor. Ergänzend sei hierzu noch bemerkt, daß es bedenklich erscheint, wenn auf einem an die Polizei übersandten Fragebogen Hinweise angebracht werden, die eine Bewertung des Landesamtes für Verfassungsschutz enthalten, aber für die Polizei zu deren Aufgabenerfüllung nicht erforderlich sind. Zu Datenübermittlungen der Polizei an Verfassungsschutzbehörden siehe auch nachfolgend Nr. 4.3.11.2.

Wie ich bereits bei früheren Prüfungen festgestellt habe, wird bei Personen, zu denen beim Landesamt für Verfassungsschutz Akten geführt werden, teilweise auch die Tatsache der Teilnahme an Veranstaltungen vermerkt, die von staatstragenden Organisationen durchgeführt werden. Das Bundesverfassungsgericht (E 65, 1/43) stellt folgendes fest: „Wer damit rechnet, daß etwa die Teilnahme an einer Versammlung oder einer Bürgerinitiative behördlich registriert wird und daß ihm dadurch Risiken entstehen können, wird möglicherweise auf eine Ausübung seiner entsprechenden Grundrechte (Art. 8, 9 GG) verzichten. Dies würde nicht nur die individuellen Entfaltungschancen des Einzel-

nen beeinträchtigen, sondern auch das Gemeinwohl, weil Selbstbestimmung eine elementare Funktionsbedingung eines auf Handlungs- und Mitwirkungsfähigkeit seiner Bürger begründeten freiheitlichen demokratischen Gemeinwesens ist." Gegen ein Speichern der Tatsache einer solchen Veranstaltungsteilnahme bestehen nur dann keine nachhaltigen Bedenken, wenn die betroffene Person hierbei im konkreten Einzelfall in einer für die Tätigkeit des Landesamts für Verfassungsschutz relevanten Weise auftritt. Dies gilt auch bei solchen Personen, zu denen berechtigt aus anderen Gründen Akten geführt werden. Im übrigen wird in diesem Bereich dafür Sorge zu tragen sein, daß die Polizeibehörden künftig Meldungen unterlassen oder zumindest wesentlich einschränken, die nur die Ausübung staatsbürgerlicher Rechte betreffen und im Einzelfall keinen Bezug zum Aufgabenbereich des Landesamtes für Verfassungsschutz haben.

Soweit das Landesamt für Verfassungsschutz den Vorstellungen des Landesbeauftragten für den Datenschutz nicht gefolgt ist, ist allerdings auch zu berücksichtigen, daß zumindest in Grenzfällen bei der Bewertung der Erforderlichkeit einer bestimmten Datenverarbeitung der Auffassung der zuständigen Fachbehörde ein Vorrang einzuräumen ist.

### 4.3.11.2. Datenübermittlung der Polizei an Nachrichtendienste

Einzelne Datenübermittlungen von der Polizei an Nachrichtendienste, die mir bekannt geworden sind, geben Anlaß zu der Vermutung, daß Polizeibehörden auf entsprechende Anfragen der Verfassungsschutzbehörden teilweise unkritisch sämtliche ihnen bekannten Informationen weitergeben, obwohl teilweise eindeutig erkennbar ist, daß diese Informationen für die Tätigkeit der Nachrichtendienste ohne Belang sind. Zwei der Fälle gebe ich nachfolgend wieder:

- Eine bayerische Polizeibehörde gab dem BND die schriftliche Auskunft, daß der Betroffene nach den vorliegenden Unterlagen acht Jahre zuvor durch eine Landespolizeistation wegen Verdachts des Automatenaufbruchs erkennungsdienstlich behandelt worden war. Der Betroffene war zur Tatzeit Jugendlicher. Der Ausgang des Verfahrens, oder ob überhaupt ein Verfahren eingeleitet worden war, war der Polizeibehörde nicht bekannt und konnte deshalb auch nicht mitgeteilt werden. Bei der Polizeistation waren über den Betroffenen ebenfalls keine Unterlagen mehr vorhanden.
- Eine andere bayerische Polizeibehörde eröffnete dem BND die Tatsache, daß über einen Jugendlichen eine Aktenvormerkung wegen gemeinsam begangenen Fahrraddiebstahls bestehe. Hinweise auf den Ausgang des Verfahrens lagen ebenfalls nicht vor.

Ich habe in diesen Fällen dem Bayerischen Staatsministerium des Innern als der obersten Dienstbehörde mitgeteilt, daß gegen die Zulässigkeit und Erforderlichkeit der erteilten Auskünfte Bedenken bestehen. Diese Vorgänge geben nämlich über den konkreten Einzelfall hinaus Anlaß, die Art der Auskunftstätigkeit bayerischer Polizeibehörden gegenüber Bundesdiensten allgemein zu überdenken. Nicht jede den Polizeibehörden vorliegende Erkenntnis über eine bestimmte Person ist für diese Nachrichtendienste im Rahmen ihrer Aufgabenerfüllung erforderlich. Hingegen kann die Übermittlung solcher Daten an Nachrichtendienste sehr wohl geeignet sein, schutzwürdige Belange der Betroffenen zu beeinträchtigen. Aus datenschutzrechtlicher Sicht ist es daher bedenklich, wenn bayerische Polizeibehörden Nachrichtendienste des Bundes so geringfügige Erkenntnisse übermitteln, ohne daß irgendeine nachrichtendienstliche oder sonst im Rahmen der Aufgabenerfüllung dieser Behörden liegende Relevanz ersichtlich wäre. Dies gilt insbesondere für lang zurückliegende „Jugendverfehlungen", zumal, wenn deren strafrechtlicher Ausgang unbekannt ist, oder sie möglicherweise nicht einmal zu einem förmlichen Ermittlungsverfahren geführt haben.

Neben dieser mehr im Tatsächlichen liegenden Problematik befasse ich mich auch mit der Lösung der Rechtsfragen, die bei Datenübermittlungen an den Bundesnachrichtendienst und den MAD im Hinblick auf das in Art. 17 Abs. 1 BayDSG ausdrücklich genannte und seit Ablauf der Übergangsbestimmung des Art. 37 Abs. 3 BayDSG zwingend vorgeschriebene Erfordernis auftreten, daß die Aufgaben durch „Rechtsnorm" zugewiesen sein müssen. Wie der Öffentlichkeit bekannt ist, bestehen für die genannten Dienste keine abschließenden und umfassenden gesetzlichen Aufgabenzuweisungen. Dieses Problem stellt sich jedoch nicht nur aufgrund der besonderen Regelungen im Bayerischen Datenschutzgesetz. Spätestens durch die Entscheidung des Bundesverfassungsgerichts zum Volkszählungsgesetz 1983 ist deutlich geworden, daß die Datenübermittlung an Nachrichtendienste schlechthin wegen ihres Eingriffscharakters einer gesetzlichen Befugnis bedarf. Um die Nachrichtendienste nicht von den für sie dringend erforderlichen Informationsflüssen abzuschneiden, scheint mir eine Klärung dieser Fragen vordringlich. Ich werde mich für eine sachgerechte Lösung einsetzen, die auch die schutzwürdigen Belange der betroffenen Bürger ausreichend berücksichtigt.

### 4.3.11.3. Amtshilfe zwischen der Grenzpolizei und den Nachrichtendiensten

Zur Regelung der Amtshilfe des Bundesgrenzschutzes für die Verfassungsschutzbehörden und den Bundesnachrichtendienst ist der Entwurf einer neuen Dienstanweisung erarbeitet worden. Sie soll die bisherigen Weisungen des Bundesinnenministeriums ersetzen. Für die Zusammenarbeit der Bayerischen Grenzpolizei mit diesen Behörden ist die zuletzt für den Bundesgrenzschutz geltende Regelung nicht übernommen worden; hierüber hatte ich im 3. Tätigkeitsbericht auf Seite 24 berichtet. Wenngleich auch der nun vorliegende Entwurf der neuen Dienstanweisung für die Amtshilfe des Bundesgrenzschutzes selbst bei deren Inkrafttreten für die Bayerische Grenzpolizei nicht unmittelbar gelten würde, hätte ich auch gegen eine Übernahme dieser Regelung für die Bayerische Grenzpolizei grundlegende Bedenken. Wie ich dies schon an anderer Stelle ausgeführt habe, erscheint mir insbesondere im Hinblick auf die Entscheidung des Bundesverfassungsgerichts zum Volkszählungsgesetz 1983 die Schaffung einer eindeutigen gesetzlichen Regelung bzw. deren Verbesserung für die im Rahmen der Durchführung der Amtshilfeersuchen der Verfassungsschutzbehörden und des Bundesnachrichtendienstes notwendige Datenübermittlung geboten. Der Gesetzgeber ist gefordert, die derzeitige Unsicherheit über den zulässigen Umfang der im Rahmen der Amtshilfe zu übermittelnden Daten durch eindeutige Regelungen zu beseitigen. Es kann nicht dem einzelnen Grenzpolizeibeamten überlassen bleiben, in welchem Umfang er auf entsprechende Ersuchen personenbezogene Daten an Nachrichtendienste

übermittelt und wie er hierbei den Persönlichkeitschutz der Betroffenen berücksichtigt.

### 4.4. Fälschungssicherer, maschinenlesbarer Personalausweis

Im Berichtsjahr hatten sich die Datenschutzbeauftragten der Länder und des Bundes und die Datenschutzkommission Rheinland-Pfalz mehrfach mit den Überlegungen zur Einführung des neuen Personalausweises auseinanderzusetzen. Unter anderem haben sie am 13.9.1983 über einen internen Musterentwurf eines Landesausführungsgesetzes zum Bundespersonalausweisgesetz beraten. Da dieses zunächst nicht weiterverfolgt wurde, vielmehr als Folge des Volkszählungsurteils mit einer Änderung des Bundespersonalausweisgesetzes zu rechnen ist, gehe ich auf Einzelheiten der Diskussion zu dem Vorentwurf für ein das Bundesgesetz ausführendes Landesgesetz nicht weiter ein. Der Bundesbeauftragte für den Datenschutz war vom Innenausschuß des Deutschen Bundestags Anfang 1984 um eine Stellungnahme zu den Auswirkungen des Volkszählungsurteils, u.a. auch hinsichtlich des Personalausweisgesetzes, gebeten worden. Er hat seine Stellungnahme im April 1984 vorgelegt. Die Reaktion des Bundesgesetzgebers bleibt nun abzuwarten.

Zur Einführung des maschinenlesbaren Personalausweises sei allgemein darauf hingewiesen, daß es nicht Aufgabe des Datenschutzbeauftragten ist, über die Erforderlichkeit eines maschinenlesbaren Personalausweises zu entscheiden, sondern vielmehr auf Gefahren hinzuweisen, die sich u.U. künftig als Folge seiner Einführung ergeben könnten. Die Einführung eines fälschungssicheren Personalausweises berührt dagegen – unabhängig von möglichen Folgen der maschinellen Nutzung des Ausweises – den Datenschutz nicht.

Überlegungen zu möglicherweise problematischen Folgen der Einführung und maschinellen Nutzung eines (maschinenlesbaren) Ausweises ergeben sich in folgenden Punkten:

a) Die bisherige manuelle Ausweiskontrolle erscheint für den Betroffenen überschaubarer. Solange der Ausweis nicht auf ein Sichtgerät gelegt oder in den Dienstraum der Polizei mitgenommen wird, findet kein unbemerkter Datenabgleich oder evtl. eine Datenspeicherung statt. Demgegenüber sind die Abgleichs- oder Speicherungsmaßnahmen, die sich an ein maschinelles Lesen des neuen Ausweises anknüpfen können, für den Kontrollierten nicht erkennbar. Damit Bürger und Polizei wissen, welche Maßnahmen zulässig sind, und um diesbezügliche Unklarheiten auszuräumen, bedarf es möglichst präziser Vorschriften über die Nutzung des Ausweises.

   Abfragen in polizeilichen Informationssystemen könnten bewirken, daß personenbezogene Daten, die bei der Anfrage verwendet werden, protokolliert würden.

   Die Datenschutzbeauftragten haben daher gefordert, daß Anfragen in Informationssystemen der Sicherheitsbehörden, die aus Anlaß von Personenkontrollen vorgenommen werden, grundsätzlich nicht personenbezogen protokolliert werden. Einem gesetzlich normierten Protokollierungsverbot käme deshalb im Sinne des verfassungsrechtlich gebotenen vorbeugenden Rechtsschutzes eine ganz erhebliche Bedeutung zu. Es erscheint mir auch in besonderem Maße geeignet, die Befürchtungen und Verunsicherungen weiter Teile der staatstreuen Bevölkerung zu zerstreuen. Polizeiliche Belange dürften einem solchen Verbot nicht entgegenstehen, da es ohnehin nur die bestehende und beabsichtigte Praxis festschreiben würde. Sollten gegen ein uneingeschränktes Protokollierungsverbot gleichwohl Bedenken bestehen, etwa weil aus polizeilicher Sicht die Möglichkeit zu personenbezogener Protokollierung für bestimmte Bereiche offengehalten werden müßte, könnte diesem Umstand durch eine eng umgrenzte Ausnahmeregelung zum Schutz hochwertiger Rechtsgüter Rechnung getragen werden. Der Datenschutzbeauftragte sollte dabei über Ausnahmen unterrichtet werden.

   Dateien, die Daten des Ausweises bzw. seiner für maschinelles Lesen vorgesehene Lesezeile enthalten, wären wesentlich eindeutiger miteinander verknüpfbar, als dies bisher ohne solche Identifikationsdaten möglich war. Die maschinell lesbare Lesezeile könnte daher die Nutzung des Ausweises als möglicherweise immer weitergehend nutzbares einheitliches Daten-Verknüpfungsinstrument fördern. Dem mit Verknüpfungen unter Umständen verbundenen Risiko von Einschränkungen des informationellen Selbstbestimmungsrechts sollten von vorneherein Regelungen im Personalausweisgesetz Rechnung tragen. Die ausführliche Diskussion der Risiken hat zu diesem Punkt aber die Notwendigkeit weiterer Verbesserungen erkennbar werden lassen. Diese betreffen vor allem eine noch genauere Festlegung der zulässigen Nutzung der Ausweisdaten, insbesondere auch der Seriennummer des Ausweises, im Personalausweisgesetz des Bundes.

   Eine etwaige Vervielfachung der Personenkontrollen nicht nur an der Grenze, die als Folge der Maschinenlesbarkeit des Ausweises denkbar wäre, müßte, falls sie vom Gesetzgeber gewollt ist, im Gesetz selbst unter Beachtung des Grundsatzes der Verhältnismäßigkeit angeordnet sein. Eine Vervielfachung der Kontrollen könnte in mehrerlei Hinsicht auf den Betroffenen wirken:

   - Sie würde objektiv bewirken, daß wesentlich mehr Personen kurzzeitig als Verdächtige gelten. Davon Betroffene empfinden dies nach meiner Erfahrung jedoch subjektiv unterschiedlich: Teils würde dies als eine hinnehmbare Maßnahme, allenfalls eine Belästigung empfunden, teils allerdings als eine belastende Verstärkung staatlicher Datenerhebung. Das Bundesverfassungsgericht hatte die hieraus entstehende Belastung als Eingriff gewertet, der der verfassungsmäßigen, insbesondere verhältnismäßigen gesetzlichen Grundlage bedarf (E 59/95/98).
   - Sie würde ebenso das Risiko erhöhen, infolge fehlerhafter Daten in den abgefragten Polizeidateien irrtümlich festgenommen zu werden (kürzlich ging beim Landesbeauftragten eine entsprechende Beschwerde eines zu Unrecht Festgenommenen ein).
   - Sie würde durch vervielfachte Kontrolle die in den letzten Jahrzehnten jedenfalls zwischen den westeuropäischen Ländern und der Bundesrepublik gewachsene, weitgehend unkontrollierte Freizügigkeit beeinträchtigen.

   Ich halte nicht für sicher, daß die den Sicherheitsbehörden derzeit eingeräumte Befugnis zur Grenzkontrolle von Ausweispapieren ganz allgemein eine wesentliche

Erhöhung der Kontrolldichte rechtfertigen würde, sofern nicht die Sicherheitslage aus besonderem Anlaß vorübergehend eine erhöhte Kontrolldichte geboten und erforderlich erscheinen läßt. Dies gilt jedenfalls, wenn und soweit diese Erhöhung nur durch die Maschinenlesbarkeit des Ausweises, also die technische Möglichkeit zur Beschleunigung der Ausweiskontrolle, ausgelöst würde. Eine Vervielfachung der Kontrollen müßte daher, soweit sie durch überwiegendes Interesse der Allgemeinheit zu rechtfertigen wäre, vom Gesetzgeber selbst vorgesehen werden, was im Personalausweisgesetz des Bundes bisher unterblieben ist. Erkennbar war in diesem Gesetz dagegen das Bestreben, den Personalausweis fälschungssicher zu gestalten.

b) Datenerhebung mit Hilfe des Personalausweises durch Behörden ist (im Sinne der Ausführungen des Bundesverfassungsgerichts in den Gründen des Volkszählungsurteils) eine zwangsweise Erhebung personenbezogener Daten. Sie setzt nach dem Urteil voraus,

> „daß der Gesetzgeber den Verwendungszweck bereichsspezifisch und präzise bestimmt und daß die Angaben für diesen Zweck geeignet und erforderlich sind. Damit wäre die Sammlung nichtanonymisierter Daten auf Vorrat zu unbestimmten oder noch nicht bestimmbaren Zwecken nicht zu vereinbaren. Auch werden sich alle Stellen, die zur Erfüllung ihrer Aufgaben personenbezogene Daten sammeln, auf das zum Erreichen des angegebenen Zieles erforderliche Minimum beschränken müssen. Die Verwendung der Daten ist auf den gesetzlich bestimmten Zweck begrenzt. Schon angesichts der Gefahren der automatischen Datenverarbeitung ist ein – amtshilfefester – Schutz gegen Zweckentfremdung durch Weitergabe- und Verwertungsverbote erforderlich. Als weitere verfahrensrechtliche Schutzvorkehrungen sind Aufklärungs-, Auskunfts- und Löschungspflichten wesentlich" (II 2a).

Es müssen aus dem Volkszählungsurteil des Bundesverfassungsgerichts deshalb noch Konsequenzen für eine Präzisierung des Bundespersonalausweisgesetzes gezogen werden.

c) Stellungnahme der Datenschutzbeauftragten und des Bayerischen Staatsministerium des Innern:

Im Berichtsjahr hatten die Landesbeauftragten für den Datenschutz, der Bundesbeauftragte für den Datenschutz und die Datenschutzkommission Rheinland-Pfalz in der eingangs erwähnten Beratung zum Personalausweisgesetz zur Erforderlichkeit bereichspezifischer Datenschutzregelungen u.a. festgestellt:

> „.... Durch die Maschinenlesbarkeit des Ausweises werden die nachfolgend aufgeführten datenschutzrechtlichen Probleme verschärft, deren Lösung die Datenschutzbeauftragten von Bund und Ländern bereits früher gefordert haben, die aber durch die bisher erlassenen polizeilichen Richtlinien (insbesondere KpS- und Dateienrichtlinien sowie die Regelung über die Amtshilfe zwischen Bundesgrenzschutz und Nachrichtendiensten) noch nicht erreicht ist:
>
> 2.1
> Im Polizeirecht des Bundes und der Länder und im Strafverfahrensrecht sind gesetzliche Grundlagen für die Informationsverarbeitung der Polizei, insbesondere für die polizeiliche Beobachtung und die Identitätsfeststellung zu schaffen. Ziel dieser Regelung muß es auch sein, den Umfang der Personenkontrollen im Hinblick auf die Nutzung des maschinenlesbaren Ausweises zu begrenzen.
>
> 2.2
> Zulässigkeit und Grenzen des Informationsaustausches zwischen Polizei und Nachrichtendiensten sind gesetzlich zu regeln.
>
> 2.3
> Der Beschluß der Innenministerkonferenz vom 2. September 1977, der vorsieht, daß alle Personen, die der Polizei bei der Erfüllung ihrer Aufgaben bekannt werden, durch Abfrage in der Personenfahndungsdatei überprüft werden, muß aufgehoben werden. Die vorhandenen Rechtsgrundlagen lassen eine derart umfassende Überprüfung nicht zu. Das gleiche gilt für einen routinemäßigen Abgleich mit den Fahndungsdateien im Rahmen von Verkehrskontrollen.
>
> 2.4
> Eine Rechtsgrundlage für den Anschluß der Länderpolizeien an die zollrechtliche Überwachung ist nicht ersichtlich. Dieser Anschluß ist zu lösen.
>
> 3. Für die Praxis der Polizeikontrollen, insbesondere unter Verwendung des maschinenlesbaren Personalausweises, sind Richtlinien zu erlassen, die den Grundsatz der Verhältnismäßigkeit konkretisieren."

Die Datenschutzbeauftragten wiesen auch darauf hin, daß sie bereits im November 1979 datenschutzrechtliche Anforderungen an die Einführung des fälschungssicheren maschinenlesbaren Personalausweises gestellt hatten. In das Bundespersonalausweisgesetz waren daraufhin entscheidende datenschutzrechtliche Regelungen aufgenommen worden. Die Datenschutzbeauftragten betonten jedoch seinerzeit, daß ein maschinenlesbarer Personalausweis nur in Verbindung mit einem datenschutzgerechten Melderecht und bereichsspezifischen Datenschutzregelungen für den Sicherheitsbereich hinnehmbar sei. Anknüpfend an diese Forderung nahm der Deutsche Bundestag bei der Verabschiedung des Personalausweisgesetzes am 17.1.1980 den nachstehenden Entschließungsantrag an (vergl. Bundestagsdrucksache 8/3498):

> „Der Deutsche Bundestag ist der Auffassung, daß angesichts der raschen Fortentwicklung der automatischen Datenverarbeitung und deren Einsatz in der öffentlichen Verwaltung über die Verabschiedung des Gesetzes zur Änderung des Gesetzes über Personalausweise hinaus weitere Maßnahmen erforderlich sind, um einen ausreichenden Schutz der Persönlichkeitsrechte der Bürger gegen mißbräuchliche Verwendung ihrer persönlichen Daten zu gewährleisten.
>
> Die Bundesregierung wird deshalb ersucht,
>
> 1. den Entwurf eines datenschutzgerechten Melderechtsrahmengesetzes einzubringen und

2. die Arbeiten zur Entwicklung bereichsspezifischer Datenschutzregelungen für die Sicherheitsbehörden nachdrücklich fortzusetzen."

Dem ist inzwischen im Bereich des Melderechts durch den Erlaß des Melderechtsrahmengesetzes und des Landesmeldegesetzes weitgehend Rechnung getragen worden. Hierauf hat auch das Bayer. Staatsministerium des Innern in seiner Stellungnahme zu den Äußerungen der Datenschutzbeauftragten hingewiesen und auf die weiteren bereichsspezifischen Regelungen im Sozialgesetzbuch und in den Richtlinien für die Führung kriminalpolizeilicher personenbezogener Sammlungen verwiesen. Damit seien in einem Zeitraum von knapp 3 Jahren durch gesetzgeberische Maßnahmen ganz entscheidende Fortschritte mit dem Ziel „mehr Datenschutz im Sicherheitsrecht" getan worden. Das Staatsministerium des Innern sei bemüht, diese neuen gesetzlichen Grundlagen nunmehr auch Schritt für Schritt in der praktischen Verwaltung umzusetzen. Das Ministerium hat besonders darauf aufmerksam gemacht, daß in Bayern eine automatische personenbezogene Protokollierung von INPOL-Abfragen aufgrund von Personenkontrollen der Personalausweise nicht vorgenommen werde. Die Sorge der Datenschutzbeauftragten, daß durch die Protokollierung von INPOL-Abfragen bei Ausweiskontrollen an den Grenzen und Flughäfen neue Dateien oder gar „Bewegungsbilder" entstehen könnten seien damit für Bayern gegenstandslos.

d) Die unterschiedliche Ausgestaltung von § 3 Abs. 5 Satz 1 PAuswG (Verwendungsverbot des Personalausweises zur automatischen Einrichtung und Erschließung von Dateien im öffentlichen Bereich) einerseits und § 4 Satz 2 PAuswG (Verwendungsverbot des Personalausweises zur automatischen Erschließung von Dateien im nichtöffentlichen Bereich) andererseits halte ich nach wie vor für nicht gerechtfertigt. Es spricht schon manches dafür, daß diese unterschiedliche Regelung auf ein reines Redaktionsversehen zurückzuführen ist. Die vom Innenausschuß des Deutschen Bundestages zunächst empfohlene Fassung der §§ 3 und 4 PAuswG (BT-Drs. 8/3498) enthielt einheitlich für den öffentlichen und für den nichtöffentlichen Bereich Verwendungsverbote zur Erschließung von Dateien. In der Beschlußempfehlung des Innenausschusses wird insoweit zur Begründung ausgeführt, daß die für den privatrechtlichen Bereich normierten Verbote mit den Beschränkungen korrespondierten, die der Gesetzgeber der öffentlichen Verwaltung auferlegt hat, und daß der Schutz der Privatsphäre des Bürgers sowohl im hoheitlichen wie im nichtöffentlichen Bereich gewährleistet sein muß. Ursprünglich war somit nach den Intentionen des Innenausschusses eindeutig hinsichtlich der Verwendungsverbote eine gleiche Regelung für den öffentlichen wie den nichtöffentlichen Bereich vorgesehen.

In einem späteren Stadium hat der Gesetzgeber bekanntlich die Anregung aufgegriffen, das Verwendungsverbot für die „Erschließung" auch auf die „Einrichtung" von Dateien zu erstrecken. Aus den mir vorliegenden Materialien zur Entstehungsgeschichte ist jedoch nicht ersichtlich, daß er dabei die Ausdehnung auf den öffentlichen Bereich (§ 3 Abs. 4 und 5 PAuswG) sowie einen Teil des nichtöffentlichen Bereichs (§ 4 Satz 2, 1. Alternative) beschränken, den anderen Teil des nichtöffentlichen Bereichs (§ 4 Satz 2, 2. Alternative) dagegen absichtlich ausnehmen und so eine bewußte Differenzierung herbeiführen wollte. Unabhängig von der Frage einer versehentlichen oder bewußten Differenzierung sehe ich für eine solche Differenzierung in keinem Fall einen rechtfertigenden Grund. Sinn und Zweck der einschlägigen Regelungen ist es, gesetzliche Vorkehrungen zu treffen gegen die mit einer automatischen Verwendung des Personalausweises verbundenen Risiken für die Persönlichkeitsrechte der Betroffenen. Mir ist aber bisher kein überzeugendes Argument bekanntgeworden, warum diese Risiken bei der automatischen Einrichtung im nichtöffentlichen Bereich geringer sein sollen als bei der automatischen Einrichtung im öffentlichen Bereich.

## 4.5. **Statistik**

### 4.5.1. Volkszählung 1983

Im Vorgriff auf den Tätigkeitsbericht für das Jahr 1983 habe ich bereits im 5. Tätigkeitsbericht über meine Stellungnahme zum Verfahren über den Erlaß einer Einstweiligen Anordnung gegen das Volkszählungsgesetz berichtet. Der 5. Tätigkeitsbericht enthält außerdem (als Anhang 1) den Beschluß der Datenschutzbeauftragten zur Volkszählung 1983 vom 22.3.1983 (Seite 64 und 65). Zum Volkszählungsurteil finden sich in diesem Tätigkeitsbericht Ausführungen an anderer Stelle (Nr. 2).

Unabhängig davon ist zu berichten, daß ich, wie auch die anderen Datenschutzbeauftragten der Länder und des Bundes, mit ungewöhnlich vielen Eingaben und Anfragen aus der Bevölkerung zur Volkszählung befaßt und dadurch mit einer zusätzlichen Arbeitsfülle belastet wurde, die zu einer teilweise erheblichen Verzögerung der Erledigung anderer Anfragen führen mußte. Auch an zahlreichen Diskussionsveranstaltungen über die Volkszählung nahmen Mitarbeiter meiner Geschäftsstelle teil. Eine ausführliche Schilderung der Tätigkeit des Landesbeauftragten für den Datenschutz bzw. seiner Mitarbeiter im Zusammenhang mit der Volkszählung und eine Darstellung der schriftlichen und mündlichen Äußerungen im verfassungsgerichtlichen Verfahren erübrigt sich in diesem Bericht, da die damaligen Überlegungen durch das inzwischen ergangene Urteil des Bundesverfassungsgerichts jedenfalls zum Teil überholt sind.

Im Zusammenhang mit dem Verfahren vor dem Bundesverfassungsgericht wurde gegen „den Datenschutz" wiederholt in der Öffentlichkeit der Vorwurf erhoben, er habe bezüglich des Volkszählungsgesetzes 1983 versagt und dessen datenschutzrechtliche Problematik verkannt.

Für Bayern darf ich dazu darauf hinweisen, daß bereits mein 1. Tätigkeitkeitsbericht unter Nr. 4.2 Bedenken zum Volkszählungsgesetz wiedergab, die sich im wesentlichen auf eine Regelung bezogen, die inzwischen das Bundesverfassungsgericht als verfassungswidrig festgestellt hat: Die Weitergabe personenbezogener Daten aus den Volkszählungsfragebögen an Gemeinden und andere öffentliche Stellen. Ein Schreiben, das ich 1979 an den Vorsitzenden den Innenausschusses des Deutschen Bundestages gerichtet hatte, wies auf die gleichen Bedenken hin. In ihm ist u.a. ausgeführt: „Die vom Volkszählungsgesetz vorgesehenen Möglichkeiten der Übermittlung von personenbezoge-

nen Einzelangaben gehen meines Erachtens über den Rahmen dessen, was die Allgemeinheit unter Statistik bisher verstanden hat, hinaus. Der befragte Bürger wird nicht damit rechnen, daß die für statistische Zwecke erhobenen Daten – wenn auch ohne Namen, also „schwach anonymisiert" – z. B. an Gemeinden oder sonstige Städte übermittelt werden. Nach meinen Erfahrungen mit der Erhebung zum Mikrozensus werden datenschutzbewußte Bürger hieran Anstoß nehmen. Eine Reaktion des Gesetzgebers hierauf war seinerzeit nicht erkennbar. Bei der Erstellung der Fragebogen für die Volkszählung war der Landesbeauftragte nicht eingeschaltet.

Die Fragen, die aus der Sicht des Datenschutzes für die Volkszählung Bedeutung haben konnten, wurden mit dem Bayerischen Statistischen Landesamt und dem Bayerischen Staatsministerium des Innern wiederholt besprochen. In vielen Einzelfragen wurde dabei weitgehend Übereinstimmung erzielt. Auch in anderen Bundesländern wurden derartige Gespräche geführt. In der Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 22.3.1983 wurden die erörterten Maßnahmen gemeinsam beraten und in einem Konferenzbeschluß in 15 Punkten festgehalten (siehe Anlage im 5. Tätigkeitsbericht). Diese 15 Punkte waren für Bayern bereits überwiegend mit dem Staatsministerium des Innern und dem Statistischen Landesamt in datenschutzgerechtem Sinne geklärt.

Das Bundesverfassungsgericht erließ am 13. April 1983 die Einstweilige Anordnung, in der der Vollzug des Volkszählungsgesetzes ausgesetzt wurde. Das Gericht ging dabei offenbar u.a. auch davon aus, daß die Erfüllung der von den Datenschutzbeauftragten gestellten 15 Forderungen für eine datenschutzgerechte Erhebung der Volkszählungsdaten im Vollzug nicht sichergestellt sei. Auf eine diesbezügliche Frage des Gerichts in der mündlichen Verhandlung, konnte der Vertreter des Bundes nicht für die Länder sprechen; die Länder waren, mit Ausnahme von Hamburg, das für die Aussetzung stimmte, bei diesem Verhandlungstermin in Karlsruhe nicht vertreten.

Für die Haltung von Datenschutzbeauftragten gegenüber dem Bundesverfassungsgericht war auch maßgebend, was der Bundesbeauftragte für den Datenschutz in einem „Nachwort zur Volkszählungsdiskussion" wie folgt formulierte: „Die Datenschutzbeauftragten hatten keine Befugnis, Gesetze vor dem Bundesverfassungsgericht anzufechten. Sie konnten deshalb vor der Entscheidung des Gerichts nur auf eine verfassungskonforme und datenschutzgerechte Durchführung des vom Bundestag beschlossenen Gesetzes hinwirken. Dies ist geschehen."

Zur Hauptverhandlung habe ich zu den vom Bundesverfassungsgericht an mich – wie auch an die übrigen am Verfahren Beteiligten - gestellten Fragen eine Stellungnahme abgeben. Die Fragen sind im Anhang zu diesem Tätigkeitsbericht wiedergegeben (Anhang Nr. 2).

In der Hauptverhandlung am 18./19. Oktober 1983 nahm ich zu drei Fragenkomplexen mündlich Stellung, um deren Behandlung das Bundesverfassungsgericht gebeten hatte:

1. Verfassungsrechtlicher Prüfungsmaßstab (Grundrechtsschutz bei Eingriffen und Gefährdung durch Datenerhebung und automatische Datenverarbeitung – Besonderheiten bei statistischen Erhebungen und Verarbeitungen),
2. Problematik der Übermittlungsregelungen des Volkszählungsgesetzes 1983 (§9 Abs. 1 – Abs. 4),
3. Zur Frage ob und welche Teile der Organisation und des Verfahrens einer Zählung (Befragung) durch das Gesetz selbst oder zumindestens durch Rechtsverordnung geregelt werden müssen.

Zur Frage 2, die nun nach der Entscheidung über die Verfassungswidrigkeit eines wesentlichen Teils der Datenübermittlungen des VZG, besonders bedeutsam ist, habe ich in der mündlichen Verhandlung ausgeführt:

1. Datenübermittlungen erhöhen generell die Wahrscheinlichkeit von Nutzungsänderungen. In den Abs. 2 – 4 des § 9 läßt das Volkszählungsgesetz jedoch eine vom Regelungstypus der Statistik abweichende Nutzung der Einzeldaten nicht zu. Zu prüfen ist, ob das Gesetz in Verbindung mit den Regelungen des Bundesstatistikgesetzes den Empfänger der Daten hinreichend an diesen Nutzungstypus bindet. Soweit im Einzelfall also die Übermittlung statistisch aggregierter Ergebnisse nicht genügt, müßte sichergestellt sein, daß beim Empfänger die Einzeldaten ebenfalls nur für statistische Zwecke verwertet werden.

   Es wäre daher auch zu fordern, daß Einzeldaten nur an eine solche Organisationseinheit der empfangenden Behörde gegeben werden, die ausschließlich mit statistischen Nutzungen, nicht aber mit Vollzugsaufgaben befaßt ist. Weiter ist zu fordern, daß diese statistische Organisationseinheit von anderen Teilen der Behörde ausreichend abgeschottet ist. Dies könnte z. B. im Bereich einer Stadt problematisch sein, wenn oder soweit dort die Notwendigkeit einer solchen funktionalen Trennung nicht anerkannt wird. Insoweit wäre eine Verdeutlichung im Statistikgesetz über die Regelung des § 9 Abs. 5 VZG hinaus dringend zu begrüßen.
2. Zum Melderegisterabgleich des § 9 Abs. 1 VZG ist festzustellen, daß er nachteilig empfundene Wirkungen auslösen kann. Wer bei diesem Abgleich zwischen direkten Folgen und indirekten Wirkungen der Berichtigung des Melderegisters unterscheidet, verkennt, daß die Zusicherung des § 9 Abs. Satz 2 VZG allgemein nicht so verstanden wird, daß sie sich ausschließlich nur auf unmittelbare Nachteile bezieht. Sie wird vielmehr als Schutz vor irgendwelchen Nachteilen aufgefaßt. Dies muß dem Betroffenen zugute gehalten werden. Er vermag die Einzelheiten des Verfahrens, die teils direkte, teils indirekte Wirkungen haben, nicht zu erkennen. Der Betroffene kann sich mithin aufgrund des Hinweises in § 9 Abs. 1 Satz 2 VZG nicht auf das einrichten, was durch die Berichtigung des Melderegisters ausgelöst werden kann. Hieraus ergibt sich m.E. eine mangelnde Bestimmtheit von § Abs. 1 VZG."

Die Leitsätze des Urteils des Bundesverfassungsgerichts zum Volkszählungsgesetz sind im Anhang zu diesem Tätigkeitsbericht unter Nr. 1 wiedergegeben.

Der Gesamtkomplex „Volkszählungsgesetz 1983" hat für Bürger, Regierung, Verwaltung wie für den Datenschutz recht wesentliche Erkenntnisse und Lehren gebracht, auf die ich zu Beginn dieses Tätigkeitsberichts eingehe.

### 4.5.2. Bodennutzungs- und Ernteerhebung

Im Zuge der Bundesstatistik nach dem Gesetz über die Bodennutzungs- und Ernteerhebung wurden bisher auch Na-

men und Anschriften von Pächtern und Verpächtern von Pachtflächen erhoben, obgleich § 4 Abs. 1 Nr. 1 des Gesetzes dies nicht vorsieht. Auf Nachfragen im Berichtsjahr wurde mir von den zuständigen Stellen mitgeteilt, daß im 2. Gesetz zur Änderung statistischer Rechtsvorschriften (2. Statistikbereinigungsgesetz) eine Ermächtigung zur Erhebung und Speicherung von Namen und Anschrift des Pächters und Verpächters geschaffen werden sollte. Dieses Gesetz ist jedoch nicht ergangen. Es kann wohl davon ausgegangen werden, daß auch das Gesetz über die Bodennutzungs- und Ernteerhebung im Zusammenhang mit der Änderung von Statistikgesetzen auf Grund des Volkszählungsurteils entsprechend überarbeitet wird.

4.5.3. Nutzung von Unterlagen aus der Bodennutzungserhebung

Wie schon im 4. Tätigkeitsbericht unter Nr. 3.1.9, S. 18, berichtet, habe ich bei einer Gemeinde festgestellt, daß Unterlagen aus der Bodennutzungserhebung (Fotokopien) entgegen § 11 des Bundesstatistikgesetzes i.V. mit dem Gesetz über die Bodennutzungs- und Ernteerhebung aufbewahrt und als Grundlage zur Erstellung von Bescheinigungen für verschiedene Stellen genutzt wurden. Ich habe die Gemeinde mehrmals auf die Unzulässigkeit des Verfahrens hingewiesen. Da nicht auszuschließen ist, daß der geschilderte Umgang mit Angaben aus der Bodennutzungserhebung auch noch in anderen Gemeinden praktiziert wird, sei darauf erneut aufmerksam gemacht.

4.5.4. Datenabgleich im Landesamt für Statistik und Datenverarbeitung

Wie ich erfuhr, wurden Meldedaten, die dem Bayerischen Landesamt für Statistik und Datenverarbeitung zum Vollzug des Gesetzes über die Statistik der Bevölkerungsbewegung und die Fortschreitung des Bevölkerungsstandes übermittelt wurden, dort seit Ende der 60-er Jahre auch mit personenbezogenen Fahndungsdaten abgeglichen, die dem Amt aus dem Bereich der Polizei übermittelt wurden. Im Trefferfalle wurden Daten der betroffenen Personen der Sicherheitsbehörde übermittelt.

Dieses Verfahren, das als Auftragsabwicklung für Polizeibehörden angesehen worden war, ist im Laufe des Berichtsjahres eingestellt worden. Das Bayerische Staatsministerium des Innern vertrat hierzu die Auffassung, daß das Verfahren auf der Grundlage des neuen Melderechts durch regelmäßige Datenübermittlungen der Meldebehörden an die Polizei ersetzt werden müsse (s.a. Anmerkung zur Datenübermittlungsverordnung zum MeldeG in diesem Bericht unter Nr.4.7.5).

4.5.5. Agrarberichterstattung

In einer Eingabe wurde die Notwendigkeit einzelner statistischer Fragen im Rahmen der Agrarberichterstattung bezweifelt. Da eine Stellungnahme der zuständigen Stellen vor der Entscheidung des Bundesverfassungsgerichts zum Volkszählungsgesetz nicht zu erwarten war, wurde die Prüfung der Fragen einstweilen zurückgestellt. Der Petent wurde entsprechend unterrichtet.

4.5.6. Erhebungsbogen für Prüfungskandidaten nach dem Hochschulstatistikgesetz

Aufgrund des Hochschulstatistikgesetzes werden mit einem Erhebungsbogen Daten über Prüfungskandidaten von Hochschulen für die amtliche Statistik erhoben. Als Eingriff in die Persönlichkeitssphäre des Prüfungskandidaten beruht diese Erhebung auf § 9 des Hochschulstatistikgesetzes. In dem Bogen werden u.a. Name, Geburtsort, Geburtsdatum, Geschlecht, Familienstand und Staatsangehörigkeit des Prüfungskandidaten erhoben. Auch wenn § 9 Abs. 1 HStatG die Erhebung von „Angaben zu Personen" vorsieht, so ist doch zweifelhaft, ob sämtliche vorgenannte Daten als „Angaben zu Personen" erforderlich sind. Dies gilt meines Erachtens insbesondere für die volle Nennung des Familien- und Vornamens. Meines Erachtens wäre bei der Prüfungskandidaten-Statistik eine Erhebung ohne Namen, also eine weitgehende Anonymisierung der Daten geboten.

Ich habe in meiner Äußerung gegenüber dem Bayer. Landesamt für Statistik und Datenverarbeitung dargelegt, daß die Nennung des Namens und eines sonstigen Identifikationsschlüssels m.E. doch nur dann erforderlich ist, wenn die Führung einer „Verlaufs"-Statistik geboten ist. Dabei wies ich darauf hin, daß das Hochschulstatistikgesetz bereits zwischen Bestandsstatistiken und Verlaufsstatistiken unterscheidet. Zum Beispiel ist in § 4 HStatG für Studenten auch eine Verlaufsstatistik vorgesehen. Dagegen enthält § 9 HStatG für die Prüfungskandidaten-Statistik keine solche ausdrückliche Anordnung einer Verlaufsstatistik. Da eine Verlaufsstatistik einen besonders starken Eingriff in die Persönlichkeitssphäre des Einzelnen darstellt, indem sie das Nachvollziehen der individuellen Persönlichkeitsentwicklung ermöglicht, bedarf sie meines Erachtens einer ausdrücklichen Rechtsgrundlage. Soweit die Rechtsgrundlage, wie im Fall des § 9 HStatG, die Verlaufsstatistik nicht nennt, würde ich daher davon ausgehen, daß der Gesetzgeber die Erhebung als Bestandsstatistik für ausreichend angesehen hatte. Für eine Bestandsstatistik erscheinen jedoch Angaben, die lediglich der Identifikation des Prüfungskandidaten dienen und die für sich gesehen keinen Aussagewert haben – jedenfalls Name und Geburtsort – nicht für erforderlich. Bedenken habe ich außerdem gegen die Erhebung der Matrikelnummer und die Erhebung von Daten über die Berechtigung zum Hochschulstudium geäußert, da sie in § 9 nicht als Erhebungstatbestände genannt sind. Dort ist lediglich der „Studienverlauf" zur Erhebung vorgesehen.

Das Bayer. Landesamt für Statistik und Datenverarbeitung hat demgegenüber die Ansicht vertreten, daß diese Datenerhebungen auf das Hochschulstatistikgesetz gestützt werden können. Auf Grund des Urteils des Bundesverfassungsgerichts zum Volkszählungsgesetz wird meines Wissens gegenwärtig erörtert, ob und inwieweit das Hochschulstatistikgesetz abzuändern sei. Im Rahmen dieser Überlegungen werde ich die vorstehende Problematik einbringen. Den Bundesbeauftragten für den Datenschutz, der in der Regel bei Entwürfen von Bundesgesetzen mit Auswirkungen auf den Datenschutz Gelegenheit zur Äußerung hat, habe ich über die geschilderten Bedenken unterrichtet.

In letzter Zeit erreichten mich zu dieser Problematik weitere Eingaben von Prüfungskandidaten. So wandte sich ein Petent mit der Schilderung des folgenden Sachverhalts an mich: Er war Studierender und Prüfungskandidat an einer bayerischen öffentlichen Hochschule. Anläßlich seiner Anmeldung zur Prüfung hatte er neben dem Anmeldebogen für die Prüfung den Erhebungsbogen für Prüfungskandidaten des Bayerischen Landesamt für Statistik und Datenver-

arbeitung auszufüllen und abzugeben. Da der Pentent inhaltliche Bedenken gegen einige Fragen des Erhebungsbogens für Prüfungskandidaten hatte, füllte er ihn nicht vollständig aus. Daraufhin wurde ihm zunächst von dem Beamten des Prüfungsamts der Hinweis gegeben, daß seine Anmeldung zur Prüfung ohne den vollständig ausgefüllten Erhebungsbogen nicht angenommen werden könne. Diese Haltung wurde in der Folge jedoch von Seiten der Hochschule nicht mehr aufrecht erhalten.

Ich bin der Auffassung, daß eine derartige Koppelung des Vollzugs von Prüfungsordnungen mit der Datenerhebung nach dem Hochschulstatistikgesetz unzulässig wäre. Ich halte es grundsätzlich für unverhältnismäßig, die Zulassung zu einer Prüfung von der (vollständigen) Ausfüllung eines rein statistischen Fragebogens abhängig zu machen. Soweit mir bekannt ist, sehen Prüfungsordnungen das Ausfüllen statistischer Fragebögen nicht als Zulassungsvoraussetzung vor. Ich habe mich mit dem Bayerischen Staatsministerium für Unterricht und Kultus in Verbindung gesetzt.

## 4.6. **Kommunalbereich**

### 4.6.1. Einheitliche Grundstücke- und Gebäudedatei mit Nebendateien als zentrales und umfassendes Informationssystem

Im Berichtsjahr beschäftigten mich Fragen des Datenschutzes, die sich bei der Einrichtung einer einheitlichen Grundstücks- und Gebäudedatei mit Nebendateien als zentrales und umfassendes Informationssystem einer kreisfreien Gemeinde ergeben können. Die Erörterung dieser Fragen ist noch nicht abgeschlossen, da auch die Konzeption der Datei einschließlich ihres Umfangs bei der Stadt noch nicht feststeht. Dies gilt auch für den Umfang der Personenbezogenheit der Angaben in einer solchen Datei, der für die datenschutzrechtliche Bewertung des Systems von entscheidender Bedeutung ist. Vorsorglich gab ich in diesem Zusammenhang folgendes zu bedenken:

Viele Daten der verschiedensten Verwaltungsbereiche der Stadt lassen sich auf Grundstücke beziehen oder stehen mit ihnen in Zusammenhang. Problematisch könnte bei einer Zusammenfassung solcher Daten nicht nur die Aufnahme sensibler Daten in die Datei, sondern auch die Tatsache sein, daß das Zusammenführen von Daten aus den unterschiedlichsten Behörden der Stadt eine recht weitgehende Registrierung und Katalogisierung einzelner Einwohner bewirken könnte. Soweit bisher erkennbar ist, werden die zusammengeführten Daten in ihrer Gesamtheit für keine Stelle der Stadt zur rechtmäßigen Erfüllung der durch Rechtsnorm zugewiesenen Aufgaben erforderlich sein. Die gesamte Information, oder auch beliebige Kombinationen von Teilen der gesamten Information, wären aber möglicherweise – von der Zulässigkeitsfrage einmal abgesehen – hinsichtlich bestimmter Personen nutzbar, wenn sie aus irgend-einem Grund Gegenstand des Interesses wären.

Zu berücksichtigen ist bei diesen Überlegungen, daß eine, gewissermaßen auf Vorrat vorgenommene Zusammenführung von Daten aus verschiedensten Behördenbereichen die durch Art. 17 BayDSG, insbesondere Abs. 3 Satz 2 vorgeschriebene Zulässigkeitsprüfung vor Übermittlungen von Daten zwischen städtischen Behörden in ihrer Wirksamkeit gefährden könnte.

Ich habe die Stadt um vollständige und rechtzeitige Unterrichtung gebeten, damit meinen eventuellen Bedenken gegen das Projekt noch Rechnung getragen werden könnte (Art. 26 Abs. 2 und 4 BayDSG, siehe auch 3. Tätigkeitsbericht, Nr. 2.4, S. 8). Ich habe außerdem gebeten, die Notwendigkeit, personenbezogene Daten zur rechtmäßigen Erfüllung der durch Rechtsnorm zugewiesenen Aufgaben derart zusammenzuführen, eingehend zu erläutern. Ich gehe davon aus, daß die Gespräche über das Projekt nach eingehender Analyse des Volkszählungsurteils mit der Stadt fortgesetzt werden.

### 4.6.2. Kommunale Datenschutzbeauftragte

Aus Berichten und Schreiben kommunaler Datenschutzbeauftragter ist zu erkennen, daß bei Städten und Gemeinden Datenschutzfragen in großer Vielfalt auftreten. Ihre Lösung erfordert viel Überblick über Rechtslage und örtliche Gestaltungsmöglichkeiten, auch in organisatorischer Hinsicht. Die erfolgreiche Tätigkeit kommunaler Datenschutzbeauftragter zeigt meines Erachtens, daß sie die Tätigkeit des Landesbeauftragten für den Datenschutz sinnvoll ergänzen, zumal dessen beschränkte Personalkapazität eine zu intensive Befassung mit Datenschutzfragen der Kommunen verbietet.

Das Bayer. Datenschutzgesetz selbst enthält für den öffentlichen Bereich keine Verpflichtung für die Behörden, einen Datenschutzbeauftragten zu ernennen. Die Vollzugsbekanntmachung zum Bayer. Datenschutzgesetz verpflichtet jedoch die staatlichen Behörden zur Bestellung eines Beauftragten und empfiehlt dasselbe den Kommunen. Aufgrund § 79 Abs. 1 SGB X besteht im Sozialbereich eine entsprechende gesetzliche Verpflichtung. Das Bayer. Staatsministerium des Innern hat sich hierzu bereits erläuternd geäußert. Demnach hat bisher nur ein Teil der Städte einen „ausdrücklichen" Datenschutzbeauftragten als herausgehobene „Anlaufstelle" für den Bürger; in der Regel behelfen sich die Städte wohl mit der Zuweisung der Datenschutzaufgaben an eine meist zentrale städtische Dienststelle. Gleichwohl erweist sich die Benennung Datenschutzbeauftragter auch in den Kommunen nach meiner Erfahrung im allseitigen Interesse als nützlich.

Zur Frage, wie unabhängig ein kommunaler Datenschutzbeauftragter sein muß, vertrete ich die Ansicht, daß er innerhalb des Gefüges einer Stadt- bzw. Kommunalverwaltung eine möglichst weitgehende institutionelle Unabhängigkeit besitzen müßte, also möglichst nahe dem Stadt- oder Gemeinderat und dem Oberbürgermeister bzw. Bürgermeister angesiedelt sein sollte. Er muß Zugang zu den städtischen Ämtern haben, um sie kontrollieren und beraten zu können, ohne einen Dienstweg einhalten zu müssen. Er muß grundsätzlich berechtigt sein, alle Unterlagen, insbesondere alle personenbezogenen Daten, die die Bürger der Stadt anvertraut haben, einzusehen. Er muß deshalb in den Wirkungskreis des Stadtrats und des Oberbürgermeisters einbezogen und Angehöriger der Stadtverwaltung sein. Bei der Anwendung seiner Fachkunde auf dem Gebiete des Datenschutzes sollte er weisungsfrei sein und darf wegen der Erfüllung seiner Aufgaben nicht benachteiligt werden (ähnlich § 28 Abs. 3 BDSG, der allerdings nicht den staatlichen Bereich betrifft).

### 4.6.3. Auftragsdatenverarbeitung

Nach Art. 3 Abs. 1 Satz 2 BayDSG ist in Fällen von Auftragsdatenverarbeitung der Auftragnehmer unter besonde-

rer Berücksichtigung der Eignung der von ihm getroffenen technischen und organisatorischen Maßnahmen sorgfältig auszuwählen. Dies hatte eine Gemeinde bei den von ihr vergebenen Datenverarbeitungsaufträgen „außer Haus" unterlassen. In einem Fall fehlte sogar eine schriftliche Regelung (siehe VollzBekBayDSG Nr. 3.4), außerdem hatte die Gemeinde dem Auftragnehmer schon einige Zeit vor Vertragsabschluß personenbezogene Echtdaten zu Testzwecken zur Verfügung gestellt. In meinem 3. Tätigkeitsbericht habe ich hierzu unter Nr. 3.11.6 darauf hingewiesen, daß meiner Ansicht nach für Testzwecke nur solche Daten verwendet werden dürfen, die keinen Rückschluß auf bestimmte Personen zulassen.

4.6.4. Weitergabe von Anschriften kommunaler Mandatsträger an Dritte

In mehreren Eingaben wurde ich mit der Frage befaßt, ob Privatanschriften und Privattelefonnummern von Stadt-, Kreis- oder Gemeinderäten von Kreis oder Gemeinde an Dritte übermittelt bzw. veröffentlicht werden dürften. Mit Rücksicht auf Art. 2 Abs. 1 und Art. 1 Abs. 1 GG habe ich in entsprechender Anwendung des Gedankens aus Art. 18 BayDSG, der in der Regel nicht direkt anwendbar ist, da die Daten meist einer Liste und nicht einer Datei entnommen werden, dazu folgende Ansicht vertreten:

Eine Beeinträchtigung schutzwürdiger Belange der kommunalen Mandatsträger kann meines Erachtens nicht angenommen werden, soweit lediglich Daten aus den Wahlvorschlägen weitergegeben werden. Diese Daten sind aufgrund der Veröffentlichung der Wahlvorschläge allgemein bekannt und besitzen diese Eigenschaft jedenfalls für die Dauer der Wahlperiode. Die Bekanntgabe der Wohnanschrift ist außerdem vielfach nicht erforderlich, weil die Mandatsträger über die Anschriften des Landratsamtes bzw. der Stadt oder Gemeinde erreichbar sind. In einer kleineren kreisangehörigen Gemeinde könnte sich die Situation dagegen anders darstellen als für den Kreistag oder eine größere Stadt, da in einer solchen Gemeinde die Privatanschrift eines Gemeinderatsmitglieds wegen des kleineren überschaubareren Bereichs möglicherweise weitgehend bekannt ist.

Eine Beeinträchtigung schutzwürdiger Belange von Mandatsträgern ist aber ausgeschlossen, wenn diese ihr schriftliches Einverständnis zur Weitergabe der Privatadresse für bestimmte Zwecke erklärt haben. Durch eine Bestimmung der Geschäftsordnung kann dies meiner Ansicht nach nicht ersetzt werden. Ich habe deshalb angeregt, in einer Kreistags- bzw. Gemeinderatssitzung eine Liste umlaufen zu lassen, in der jeder Betroffene angeben kann, welche Anschriften (Landratsamt, ggf. Gemeindekanzlei etc., Privatanschrift) für welche Zwecke von der Verwaltung weitergegeben werden dürfen.

4.6.5. Weitergabe des Grundsteuermeßbetragsverzeichnisses

Wie mir bekannt wurde, haben verschiedene Gemeinden vollständige Grundsteuermeßbetragsverzeichnisse zum Zwecke der Festsetzung der Kirchengrundsteuer an die katholischen Kirchengemeinden weitergegeben. Soweit dieses Verzeichnis ausschließlich katholische Grundeigentümer von land- und forstwirtschaftlichen Flächen ausweist, bestehen im Hinblick auf § 31 Abs. 1 AO, Art. 16 Abs. 3 KirchStG, § 4 der Kath. Kirchengrundbuchordnung gegen eine derartige Datenübermittlung keine Bedenken. Sofern jedoch vollständige Grundsteuermeßbetragsverzeichnisse, ohne Beschränkung auf Bekenntnisangehörige weitergegeben wurden, haben die Gemeinden insoweit gegen den Grundsatz der Erforderlichkeit der Datenübermittlung verstoßen.

Da die in Frage kommenden Gemeinden im einzelnen nicht ermittelt werden konnten, habe ich das Kath. Kirchensteueramt gebeten, dafür zu sorgen, daß keine kompletten Meßbetragsverzeichnisse mehr angefordert werden. Die AKDB hat ihre Anwender ebenfalls auf unsere Bedenken hingewiesen (vergl. AKDB-Info v. 10.9.1983). Im übrigen sei an das Schreiben des Bayer. Staatsministeriums des Innern vom 22.8.1957 (MABl. S. 644) erinnert, in dem seinerzeit die korrekte Behandlung dieser Fälle im oben dargelegten Sinne erläutert wurde.

4.6.6. Angaben auf Überweisungsträgern und Lastschriftbelegen

Ein Bürger, der die gemeindliche Finanzverwaltung zum Einzug der Steuern und sonstigen Abgaben ermächtigt hatte, beschwerte sich in seiner Eingabe darüber, daß auf den Lastschriften der Verwendungszweck, nämlich „Gewerbesteuer", „Gewerbesteuervorauszahlung" und „Grundsteuer" einschließlich des Steuerbetrags ausgedruckt und damit dem Bankpersonal bekannt wird. Er hielt diese Verfahren für einen Verstoß gegen das Steuergeheimnis (§ 30 AO) und regte eine Verschlüsselung des Verwendungszweckes an. Die zur Stellungnahme aufgeforderte Gemeinde führte aus, daß die Angaben des Verwendungszweckes auf den Lastschriften aus Gründen der einfachen und sicheren Buchhaltung bei der Gemeinde erforderlich seien, da neben der Gewerbesteuer und Grundsteuer auch Wasser-, Abwasser-, Kanal- und Müllabfuhrgebühren einzuziehen wären.

Die Überprüfung ergab, daß gem. § 30 Abs. 4 Nr. 1 AO die Offenbarung der dem Steuergeheimnis unterliegenden Daten zulässig ist, soweit sie zu der Durchführung eines Steuerverfahrens dient. Dies ist hier anzunehmen, da die Angabe des Verwendungszwecks auf den Bankbelegen für die Begleichung der Steuerschuld zur eindeutigen Zuordnung bei der Gemeinde bzw. beim Steuerpflichtigen erforderlich ist, sofern der Steuerpflichtige bei der Bezahlung eine Bank einschaltet. Wer im Einzelfall mit dieser Verfahrensweise nicht einverstanden ist, kann einen Abbuchungsauftrag grundsätzlich widerrufen und die fälligen Steuern und Gebühren selbst bezahlen oder überweisen. Im Falle der Überweisung müssen allerdings auf dem Überweisungsträger wieder die entsprechenden Verwendungszwecke aufgeführt sein, damit die Zahlung bei der Stadt richtig verbucht werden kann. Eine numerische Verschlüsselung der jeweiligen Verwendungszwecke könnte zwar dazu beitragen, daß der Zahlungsgrund für das Bankpersonal zumindest nicht auf den ersten Blick ersichtlich wäre. Nach einiger Zeit würde jedoch die von der Gemeinde gewählte Verschlüsselungsart auch wieder bei der Bank bekannt sein, da es sich nur um wenige, sich stets wiederholende Verwendungszwecke handelt. Eine numerische Verschlüsselung konnte daher nicht gefordert werden.

Das Bayer. Staatsministerium des Innern hat in diesem Zusammenhang dem Arbeitskreis bayerischer Formularverlage vorgeschlagen, auf den Formularen, mit denen der Bür-

ger die Verwaltung von Einziehung von Beträgen ermächtigt, folgenden verdeutlichenden Hinweis anzubringen: „Die Überweisungsträger/Lastschriften enthalten die Angabe des Zahlungsgrundes und werden an die von ihnen bezeichnete Bank weitergegeben".

Hierdurch wird zumindest v o r Beginn des Lastschriftverfahrens den Betroffenen deutlich gemacht, daß die beteiligte Bank entsprechende Informationen zur Kenntnis nehmen kann.

4.6.7. Weitergabe von Standesamtsdaten

Mit der Begründung „Verwaltungsvereinfachung" hatte eine Gemeinde Durchschriften von Abstammungsurkunden an Banken weitergegeben, obwohl gem. § 104 Abs. 1 der Dienstanweisung für die Standesbeamten mit Einverständnis der Beteiligten lediglich eine beschränkte Zahl von Daten (Tag und Ort des Ereignisses, Vorname, Familienname, Wohnort, Wohnung) weitergegeben werden dürfen. Durch Weitergabe der Urkunde wurden mehr Daten übermittelt, als von der Einwilligung erfaßt waren. Das Verfahren wurde beanstandet.

Im konkreten Fall war außerdem das verwendete Einverständnis-Formular unzureichend, da die Betroffenen nicht erkennen konnten, welche ihrer Daten veröffentlicht bzw. an interessierte Firmen weitergegeben werden sollten.

In einem anderen Fall hatte eine Gemeinde bei Geburten und Eheschließungen Namen und Tag des Ereignisses veröffentlicht. Bei den meisten Geburten lagen jedoch aufgrund eines Mißverständnisses keine Einwilligungen vor. Die Gemeinde wurde gebeten § 104 DA künftig zu beachten.

Schließlich hat die Konferenz der Datenschutzbeauftragten des Bundes und der Länder zur Mitteilungspflicht des Standesbeamten über umherziehende Personen gem. § 103, 201 DA folgenden Beschluß gefaßt:

„Die Pflicht des Standesbeamten, bei Eintragungen über alle umherziehenden Personen ohne festen Wohnsitz die Kriminalpolizei zu unterrichten (§ 103 und 201 DA), muß gestrichen werden. Sie bedeutet eine pauschale Diskriminierung einer Personengruppe."

Die Datenschutzbeauftragten haben die zuständigen Geschäftsbereiche hiervon verständigt.

## 4.7. **Meldewesen**

4.7.1. Speicherung von Meldedaten in der Nebenwohnungsgemeinde

Unter dem Gesichtspunkt der Erforderlichkeit der Datenspeicherung im Melderegister benötigt eine Nebenwohnungs-Meldebehörde nicht in vollem Umfange dieselben Daten wie eine Hauptwohnungs-Meldebehörde. Ich habe das Bayer. Staatsministerium des Innern gebeten, dies in der Vollzugsbekanntmachung zum Meldegesetz klarzustellen (s. VollzBekMeldeG Nr. 3.2). Daß gleichwohl im amtlichen Meldeschein für die Nebenwohnung zunächst alle Daten wie für eine Hauptwohnung erhoben werden, hat seinen Grund in folgendem: Würde sich ein Zuziehender mit einer Nebenwohnung anmelden und entsprechend weniger Daten auf dem Meldeformular angeben, würde sich aber bei Prüfung der Hauptwohnung durch die Meldebehörde ergeben. daß die angemeldete Nebenwohnung tatsächlich die Hauptwohnung ist, hätte dies erneuten Verwaltungsaufwand und unter Umständen die Anordnung des persönlichen Erscheinens des Betroffenen bei der Meldebehörde zur Angabe der fehlenden Daten zur Folge. Um dem Bürger dies zu ersparen kann wohl hingenommen werden, daß auch im Falle einer Nebenwohnung zunächst alle in Art. 18 Abs. 1 MeldeG auch für Hauptwohnung vorgesehene Daten mit der Maßgabe erhoben werden, daß ihre Speicherung bei der Meldebehörde nach Prüfung anschließend auf das für die Nebenwohnung erforderliche Maß begrenzt wird.

4.7.2. Speicherung von Religionszugehörigkeiten im Melderegister

Gegenüber dem Bayer. Staatsministerium des Innern habe ich mehrfach die Ansicht vertreten, daß im Melderegister unter dem Gesichtspunkt der Erforderlichkeit zur Aufgabenerfüllung Daten über die Zugehörigkeit zu öffentlich-rechtlichen Religionsgesellschaften nur gespeichert werden dürften, soweit dies für steuerrechtliche und/oder Statistikzwecke erforderlich ist. Ich habe außerdem gefordert, daß eine Datenspeicherung über die Zugehörigkeit zu öffentlich-rechtlichen Religionsgesellschaften, die für den Ausdruck von Lohnsteuerkarten nicht erforderlich ist, sondern lediglich für statistische Zwecke erfolgt, nach der Datenübermittlung ans Statistische Landesamt zu löschen ist. Diese Ansicht zur Erforderlichkeit der Speicherung der Zugehörigkeit zu öffentlich-rechtlichen Religionsgesellschaften hat auch der wissenschaftliche Dienst des Landtags Rheinland-Pfalz in einer gutachtlichen Stellungnahme vom 9.6.1983 vertreten. Das Bayer. Staatsministerium des Innern teilt diese Ansicht nicht, da die Speicherung der rechtlichen Zugehörigkeit zu einer Religionsgesellschaft in Art. 3 Abs. 1 Nr. 11 vom Gesetz vorgesehen ist.

4.7.3. Speicherung eines Hinweises auf Vertriebene im Melderegister

Gegenüber dem Bayer. Staatsministerium des Innern habe ich die Ansicht vertreten, daß das Datum „Anschrift vom 1. September 1939 derjenigen Einwohner, die aus den in § 1 Abs. 2 Nr. 3 des Bundesvertriebenengesetzes bezeichneten Gebieten stammen" nach dem neuen Meldegesetz zur Datenübermittlung an den kirchlichen Suchdienst und nicht zur Datenspeicherung im Melderegister bestimmt ist. Danach müßten diese Anschriften gelöscht werden, weil sie für die Aufgabenerfüllung der Meldebehörde im übrigen nicht erforderlich sind. Sie werden nach dem neuen Melderecht nur für die Übermittlung an den Suchdienst zweckgebunden erhoben (s.a. Nr. 33 VollzBekMeldeG wonach keine Speicherung mehr vorgesehen ist).

4.7.4. Wegfall des Familienbezugs bei volljährigen Kindern im Melderegister

Die Neukonzeption des Meldewesens hat unter anderem auch bewirkt, daß künftig bei volljährigen Kindern kein Hinweis mehr auf die Eltern gespeichert sein darf (§ 2 Abs. 1 Nr. 16 MRRG, entsprechend Art. 3 Abs. 1 Nr. 16 MeldeG). Ich bin verschiedentlich darauf angesprochen worden, daß dies Nachforschungen nach Erben, in die auch Einwohnermeldeämter eingeschaltet waren, erschwere. Auch kann bei Volljährigen das Meldeamt deshalb beispielsweise nicht mehr den Geburtsnamen der Mutter feststellen, der bisher bei bestimmten Verfahren erforderlich war. Damit ist aber auch die Frage angeschnitten, ob die gegenwärtig für viele Gemeinden realisierte Konzeption, das automatisierte Einwohnerwesen nach dem sogenannten Familienverbund

auszurichten, aufrechterhalten werden kann. Ich habe das Bayer. Staatsministerium des Innern von diesen Anfragen unterrichtet.

4.7.5. Verordnung über regelmäßige Datenübermittlungen nach Art. 31 Abs. 5 MeldeG

Nach Art. 31 Abs. 4 und 5, Art. 45 S. 1 MeldeG werden im Laufe des Jahres 1984 in einer Rechtsverordnung die regelmäßigen Datenübermittlungen aus dem Melderegister festzulegen sein. In diesem Zusammenhang ist auf ein zentrales Problem hinzuweisen, das in dieser Verordnung angemessen gelöst werden müßte: Es ist zu klären, ob es mit der gebotenen Rücksicht auf den grundrechtlich garantierten Persönlichkeitsschutz vereinbar wäre, sämtliche Meldungen von Einwohnern über Zu- und Wegzüge ect. automatisiert mit Dateien von Sicherheitsbehörden abzugleichen.

Hierzu ist meines Erachtens folgendes zu bedenken: Würden sämtliche Wanderungsbewegungen der Bürger der Polizei in automatisierter Form zur Verfügung gestellt, um sie mit polizeilichen Datensammlungen abzugleichen, würde die Möglichkeit einer ständigen Rasterfahndung geschaffen. Im Gegensatz zu den für automatisierte Rasterfahndung bisher wohl allgemein anerkannten Voraussetzungen der Aufklärung einer schwerwiegenden Straftat und der konkreten Fragestellung, würden hier Daten zum Abgleich zur Verfügung gestellt, ohne daß diese strengen Anforderungen jeweils erfüllt wären. Selbst ein Abgleich mit solchen INPOL-Daten, die wegen Haftbefehls gesuchte Personen betreffen, wäre eine Erweiterung gegenüber der Rasterfahndung wegen schwerer Straftaten, weil Haftbefehle auch wegen geringfügiger Delikte ausgestellt sein können. INPOL-Dateien, mit denen Meldungen abgeglichen werden könnten, enthalten aber auch Personen, für die nur Suchvermerke (z.B. zur Aufenthaltsermittlung) vorliegen, jedoch kein Verdacht von Straftaten. Damit stellt sich wohl die Frage nach der Verhältnismäßigkeit eines so umfassenden Datenabgleichs. Unabhängig von diesen rechtlichen Zweifeln ist m.E. zu berücksichtigen, daß die bisherige tatsächliche Trefferquote bei Abgleich mit Daten aus der Wanderungsbewegung regional sehr unterschiedlich und auf das ganze Land bezogen gering war.

Soweit dem entgegengehalten wird, daß im automatisierten Verfahren nicht mehr Daten übermittelt würden, als bisher bei Übergabe der Meldescheine, ist darauf hinzuweisen, daß die Übermittlung, vor allem aber der Abgleich sämtlicher Meldescheine ebenfalls, aus denselben Gründen, zweifelhaft erscheint und im übrigen mit der Automation dieser Vorgänge durch Perfektion und Vollständigkeit des Abgleichs ein qualitativer Unterschied gegenüber dem bisherigen (schwerfälligeren) manuellen Verfahren eintreten würde. Unabhängig von den ebengenannten Bedenken wäre darauf zu achten, daß im Zuge dieses Abgleichs an die Polizei nicht mehr Daten übermittelt würden, als diese im Regelfall für ihre Aufgabenerfüllung benötigt. Die Tatsache, daß Fälle denkbar sind, in denen über den Regelfall hinaus weitere Daten zur eindeutigen Identifizierung einer Person notwendig sein können, dürfte meines Erachtens nicht dazu führen, daß in allen Fällen auch weitere Daten rein vorsorglich übermittelt würden. In den Ausnahmefällen, in denen die Polizei mehr identifizierende Daten benötigt, kann sie diese durch Anfrage bei der zuständigen Meldebehörde jederzeit ermitteln (Art. 31 Abs. 1 – 3 MeldeG).

Bedenklich wäre außerdem, wenn die Daten in automatisierter Form einer zentralen Behörde zum Abgleich übermittelt würden. Damit würde gegenüber der bisherigen Übermittlung der Meldescheine an die jeweils zuständigen örtlichen Polizeibehörden ein wesentlicher Unterschied eintreten. Während die örtliche Polizeibehörde entscheiden kann, ob sie wirklich alle Meldedaten mit dem Fahndungsbuch oder mit den das Fahndungsbuch ersetzenden ADV-Dateien abgleicht, weil sie aus der Kenntnis von örtlichen und persönlichen Umständen eine entsprechende Vorauswahl treffen kann, wäre bei zentraler Abwicklung im automatisierten Verfahren wohl nur ein 100%-iger Abgleich möglich. Die Entstehung eines zentralen Wanderungsregisters bei einer zentralen Stelle erscheint dagegen durch die Vorschrift der Nr. 31.2 Abs. 2 VollzBekMeldeG, die die Führung eigener Melderegister durch die Polizei verbietet, ausgeschlossen.

Eine weitere Problematik, die in dieser Verordnung zu lösen wäre, besteht darin, daß wohl ein Online-Anschluß „der Polizei" an die bei der Anstalt für Kommunale Datenverarbeitung in Bayern (AKDB) gespeicherten Daten von über 80% der Einwohner bayerischer Gemeinden zur Debatte stehen dürfte. Hier stellt sich meines Erachtens nicht nur die Frage, ob lediglich jeweils die örtliche Polizeibehörde die Daten aus ihrem Zuständigkeitsbereich abfragen darf, oder darüber hinaus auch Daten aus anderen Gemeinden. Das Vorhaben würde sich auch auf den Charakter der dortigen Datenspeicherung auswirken, da die AKDB Auftragnehmer der Gemeinden ist. Auf die damit verbundene generelle Problematik habe ich bereits in früheren Tätigkeitsberichten hingewiesen (3. TB Nr. 2.5 Seite 8/9, 5. TB Nr. 1.1.1 Seite 5).

4.7.6. Zum Ordnungsmerkmal des Melderegisters

Bei der Beratung des Entwurfs für das Landesmeldegesetz ist sowohl im Beirat beim Landesbeauftragten für den Datenschutz als auch im Ausschuß für Verfassungs-, Rechts- und Kommunalfragen des Bayerischen Landtags festgestellt worden, daß die Nutzung des Ordnungsmerkmals des Melderegisters durch andere Behörden als Meldebehörden, oder durch Dritte, durch den Landesbeauftragten beobachtet werden müsse, um zu prüfen, ob die Nutzungseinschränkungen des Art. 4 MeldeG ausreichen (siehe auch V. Tätigkeitsbericht Nr. 4.6.1, S. 35). Im folgenden seien Fragen dargestellt, die sich in diesem Zusammenhang ergaben:

4.7.7. Ordnungsmerkmale auf Lohnsteuerkarten

Aufgrund der früher nicht so eindeutigen Rechtslage enthielten die Lohnsteuerkarten in manchen bayerischen Gemeinden den Aufdruck des Ordnungsmerkmals im Sinne von Art. 4 des neuen Bayerischen Meldegesetzes. Hierdurch kann, entgegen Art. 4 Abs. 3 MeldeG, eine Übermittlung des Ordnungsmerkmals an den Arbeitgeber bewirkt werden. Das Bayerischen Staatsministerium der Finanzen hatte bereits mit Schreiben vom 29.12.1978 mir gegenüber erklärt, daß sich aus der „Sicht der Finanzverwaltung die Frage eines solchen Ordnungsmerkmals nicht stellt", der Ausdruck des OM mithin nicht für notwendig angesehen werde.

Ziel der verschiedenen in Art. 4 MeldeG enthaltenen Einschränkungen im Umgang mit dem Ordnungsmerkmal ist es, eine weitere Verbreitung des Ordnungsmerkmals zu verhindern, denn je weiter das Ordnungsmerkmal bei Stel-

len, die Daten verarbeiten, verbreitet wäre, desto wahrscheinlicher würde seine künftige Verwendung als einheitliches Verknüpfungsmerkmal von verschiedenen Datenbeständen. Da dies durch die Regelungen des Art. 4 MeldeG hinsichtlich des Ordnungsmerkmals der Melderegister verhindert werden soll, habe ich Gemeinden, soweit ich den Ausdruck des OM auf Lohnsteuerkarten feststellen konnte, auf die Unzulässigkeit dieser Verfahrensweise hingewiesen.

Das Bayer. Staatsministerium der Finanzen hat dies in seiner Bekanntmachung vom 25.7.1983 (FMBl S.369) klargestellt: „..., und daß der Ausdruck eines Ordnungsmerkmals auf den Lohnsteuerkarten durch die Gemeinden im Hinblick auf Art. 4 Abs. 3 MeldeG ab 1984 nicht mehr zulässig ist ...". Wenngleich ich der Ansicht bin, daß Art. 4 MeldeG gem. Art. 45 MeldeG bereits ab 1.4.1983 galt, begrüße ich doch diese Klarstellung.

4.7.8. Nutzung des Ordnungsmerkmals aus dem Melderegister bei anderen Dienststellen

In einer städtischen Bibliothek war bei Automatisierung des Leserbestandes – vor Inkrafttreten des MeldeG – dem Datensatz des Lesers als Benutzernummer sein zwölfstelliges Ordnungsmerkmal (OM) des Melderegisters zugeordnet worden. Leser, die später hinzukamen, erhielten zwar ebenfalls eine zwölfstellige Benutzernummer. Diese war jedoch nicht mehr mit dem OM des Melderegisters identisch, sondern enthielt eine von der Bibliothek vergebene, vom OM abweichende laufende Nummer und Prüfziffer. Bei der Nutzung des aus dem Melderegister übernommenen OM durch die Bibliothek war im vorliegenden Fall Art. 4 Abs. 2 Satz 3 MeldeG zu beachten. Danach darf die Bibliothek die mit dem OM identische Benutzernummer ausschließlich zum Datenaustausch mit der Meldebehörde verwenden. Im Verkehr mit anderen öffentlichen Stellen (z.B. mit anderen Bibliotheken) darf diese Benutzernummer dagegen nicht verwendet werden (andernfalls würde das OM des Melderegisters als allgemeine Identifikationsnummer weiter verbreitet). Die Verbreitung des OM alleine im Bibliotheksbereich würde zwar noch keine wesentliche Nutzungs-Ausweitung erzeugen. Der Sinn der Vorschrift des Art. 4 Abs. 2 Satz 3 MeldeG liegt hier aber darin, daß sich sonst aus mehreren Erweiterungen der Nutzung des OM, die jede für sich wenig bedeutsam erscheinen mögen, eine problematische Tendenz zum allgemeinen Verknüpfungsmerkmal ergeben könnte. Die genannte Stadtbibliothek ist nun dazu übergegangen, in den Fällen, in denen noch OM aus dem Melderegister die Benutzernummer bilden, neue Nummern und neue Bibliotheksausweise auszugeben.

4.7.9. Verwendung des Ordnungsmerkmals aus dem Meldereregister innerhalb der Gemeinde

Durch Art. 4 Abs. 2 Satz 3 MeldeG ist bestimmt, daß Ordnungsmerkmale vom Empfänger der Daten nur an die jeweilige Meldebehörde übermittelt werden dürfen. Der nachfolgende Satz 4 von Art. 4 Abs. 2 MeldeG legt die entsprechende Geltung von Art. 31 Abs. 7 Satz 1 und 2 MeldeG fest. Hieraus ergibt sich, daß innergemeindliche Empfänger von Daten mit Ordnungsmerkmalen aus dem Melderegister denselben Beschränkungen im Umgang mit dem Ordnungsmerkmal unterliegen, wie außergemeindliche Empfänger von Datenübermittlungen aus dem Melderegister. Gemeindliche Dienststellen, die Daten aus dem Meldeamt der gleichen Gemeinde erhalten, dürfen deshalb das Ordnungsmerkmal ihrerseits wiederum nur gegenüber diesem Meldeamt, nicht aber untereinander oder gegenüber anderen öffentlichen Stellen verwenden. Da das Ordnungsmerkmal nach Art. 4 Abs. 2 Satz 1 nur „im Rahmen von Datenübermittlungen" des Meldeamts, also zusammen mit Meldeamtsdaten übermittelt werden darf, wäre seine Übermittlung oder Weitergabe zusammen mit Daten einer anderen Stelle – z.B. mit Daten des Ausländeramts – unzulässig. Diese Auslegung wurde zusammen mit dem Bayer. Staatsministerium des Innern erarbeitet und inzwischen in Nr. 4.3 der VollzBekMeldeG übernommen.

4.7.10. Übermittlung von Meldedaten an Kreiswehrersatzämter

Wehrpflichtgesetz und Zivildienstgesetz des Bundes wurden im Berichtsjahr novelliert. § 24 Abs. 9 des Wehrpflichtgesetzes sieht nunmehr vor, daß Meldebehörden dem Kreiswehrersatzamt zur Wehrüberwachung Daten der 18-32 Jahre alten männlichen Deutschen sowie Änderungen dieser Daten mitteilen. Über ältere Personen werden Daten nur übermittelt, wenn der Meldebehörde durch Mitteilung der Wehrersatzbehörde bekannt ist, daß die Betroffenen der Wehrüberwachung unterliegen. Nach § 23 Abs. 3 des Zivildienstgesetzes übermittelt die Wehrersatzbehörde Daten der Personen, die nicht der Wehrüberwachung unterliegen, zum Zwecke der Zivildienstüberwachung dem Bundesamt für den Zivildienst. Das Bundesamt löscht die Daten, die zur Aufgabenerfüllung nicht benötigt werden.

Die Bundesregierung hatte sich zu einer entsprechenden Gesetzesinitiative u.a. wie folgt geäußert: „Die von der Bundesregierung vorgeschlagene Fassung des § 23 Abs. 3 ZDG hat den Vorteil, daß die Meldebehörden am Verfahren der Datenübermittlung gegenüber dem Bundesamt für den Zivildienst nicht mitwirken, demzufolge also auch nicht das Datum „Zivildienstüberwachung" zu erheben und zu speichern brauchen. Es ist bürgerfreundlich und verwaltungsökonomisch und trägt darüber hinaus den Belangen des Datenschutzes Rechnung."

Diese Auffassung wird aus der Sicht des Datenschutzes geteilt, weil danach im Melderegister bei den 18-32jährigen nicht mehr gespeichert wird, ob sie der Wehr- oder Zivildienstüberwachung unterliegen. Das Melderegister kann dann insoweit nach diesen Kriterien nicht mehr ausgewertet werden. Die Zahl der Behörden, die diese Angabe kennen, ist beschränkt. Auf den Meldevordrucken wird auf die Erhebung des Datums „unterliegt der Wehr/Zivildienstüberwachung" daher auch verzichtet.

4.7.11. Weitergabe von Listen über An- und Abmeldungen

Bei einer Stadt wurde festgestellt, daß bei An- und Abmeldungen sowie Umzügen innerhalb der Stadt listenmäßige Zusammenstellungen über Namen, Vornamen, Familienstand, Geburtsdatum, Religion, Staatsangehörigkeit, bisherige und neue Wohnung sowie Zuzugsdatum an 9 verschiedene Stellen, überwiegend innerhalb der Stadt, regelmäßig übermittelt wurden. Ich habe die Stadt aufgefordert, zu überprüfen, inwieweit sämtliche in den Listen enthaltene Meldedaten zur rechtmäßigen Aufgabenerfüllung der Datenempfänger erforderlich sind, da dies nach Art. 31 Abs. 1 (und 7) MeldeG Voraussetzung für die Zulässigkeit der Übermittlung sowohl nach außerhalb als auch innerhalb der Stadt ist. Dies bezog sich insbesondere auf die Weitergabe von Angaben über Religion, Staatsangehörigkeit und Familienstand an die Stadtwerke und andere Stellen. Außerdem

ist die Übermittlung der Angabe der Religionszugehörigkeit an die örtliche Polizeidienststelle durch die Verordnung zur Durchführung des Bayerischen Gesetzes über das Meldewesen nicht mehr vorgesehen (DVMeldeG vom 29.7.1983, GVBl Seite 647).

4.7.12. Datenübermittlung aus dem Melderegister an die Freiwillige Feuerwehr

In einer Eingabe wurde gefragt, ob es zulässig sei, einem (privatrechtlichen) Feuerwehrverein jährlich eine Liste über alle feuerwehrpflichtigen männlichen Einwohner zu übergeben, die dazu dient, bei den Betroffenen einen (freiwilligen) Beitrag einzuheben, der für Zwecke des Brandschutzes verwendet werden soll. Ich habe dazu die Ansicht vertreten, daß die Voraussetzungen des Art. 34 Abs. 3 MeldeG, der eine Gruppenauskunft zuläßt, soweit sie im öffentlichen Interesse liegt, erfüllt sind, wenn die Einnahmen ausschließlich für Zwecke des abwehrenden Brandschutzes und des technischen Hilfsdienstes – also zur Erfüllung von Aufgaben, die grundsätzlich nach Art. 1 Abs. 1 BayFwG den Gemeinden obliegen - verwendet werden (vergl. Nr. 5.2.1 letzter Satz VollzbekBayFwG vom 30.3.1983 – MABl Seite 273). Die Freiwilligen Feuerwehren müßten allerdings bei der Übergabe der Liste gemäß Art. 34 Abs. 4 MeldeG auf diese Zweckbindung hingewiesen werden. Die Vorschrift der Vollzugsbekanntmachung zum Meldegesetz über Gruppenauskünfte an nichtöffentliche Stellen ist dabei zu beachten (nach Nr. 34.6 – u.a. Zustimmung der Regierung).

4.7.13. Sammelauskünfte aus dem Melderegister

Wie mir bekannt wurde, hatte eine öffentliche Krankenkasse von einem Einwohnermeldeamt die Anschriften von Personen erbeten, die auf einer Liste namentlich aufgeführt wurden. Es handelte sich dabei durchwegs um 16-jährige, die die Schule zu diesem Zeitpunkt abschließen würden. Die Liste gab einen Hinweis darauf, daß Namenslisten von ganzen Schulklassen vorgelegt wurden. Es war anzunehmen, daß die Anschriften zu Werbezwecken erbeten wurden. Die Krankenkasse befand sich diesbezüglich in Wettbewerb zu anderen (öffentlichen) Krankenversicherungen.

Unbeschadet des für öffentliche Krankenversicherungen geltenden gesetzlichen Aufklärungsgebots habe ich die Auffassung vertreten, daß die Übermittlung der Anschriften in diesem Falle nicht zur rechtmäßigen Erfüllung der in der Zuständigkeit des Empfängers liegenden Aufgabe „erforderlich" und daher nicht zulässig ist (Art. 31 Abs. 1 MeldeG). Dabei ging ich davon aus, daß nicht angenommen werden kann, daß die Übermittlung von Anschriften jedesmal zur Aufgabenerfüllung „erforderlich" ist, wenn eine von mehreren konkurrierenden öffentlichen Krankenversicherungen Daten erbittet.

Zum selben Ergebnis würde in diesem Falle eine Gleichstellung der öffentlichen Stelle mit nicht-öffentlichen Stellen wegen des vorliegenden Wettbewerbs führen. Art. 22 Abs. 1 BayDSG legt diese Überlegung nahe. Würde eine nichtöffentliche Stelle eine entsprechende Sammelauskunft beantragen, deren Grundlage beispielsweise Jahresberichte von Schulen, Namenslisten von Behördenangehörigen, Jahrbücher o.ä. sind, würde m. E. ein Mißbrauch des in Art. 34 Abs. 1, insbesondere Satz 2 MeldeG, vorgesehenen Sammelauskunftsverfahrens vorliegen, so daß die Datenübermittlung nicht als erlaubt angesehen werden könnte. In der Vollzugsbekanntmachung zum Meldegesetz ist dieser Mißbrauch inzwischen untersagt worden (Nr. 34.1.2).

4.7.14. Weitergabe von Meldedaten durch Bürgermeister

Der 2. Bürgermeister einer Gemeinde hatte eine Kopie einer Melderegister-Karteikarte eines Gemeindeeinwohners einem Privatmann weitergegeben. Ein Fall der Vertretung des 1. Bürgermeisters lag damals nicht vor. Auch gehörte der Aufgabenbereich Einwohnerwesen bzw. Verwaltung des Melderegisters nicht zu den Aufgaben des 2. Bürgermeisters, der die Daten nach seiner Einlassung als Privatmann weitergab. Die Weitergabe sämtlicher Melderegisterdaten eines Einwohners durch den 2. Bürgermeister an einen Privatmann war nach Art. 4 Abs. 1, 18 Abs. 1 BayDSG und nach der damals geltenden Vollzugsbekanntmachung zum Meldegesetz unzulässig (der Vorfall ereignete sich noch vor Inkrafttreten des neuen Meldegesetzes, aus dem sich allerdings keine andere Beurteilung des Sachverhaltes ergeben würde). Die Weitergabe der Fotokopie der Melderegisterkarte durch den 2. Bürgermeister wurde daher gem. Art. 30 Abs. 1 BayDSG beanstandet. Der Fall hat auch gezeigt, daß es erforderlich ist, innerhalb der Gemeinde, also auch für weitere Bürgermeister, klarzustellen, wer zur Weitergabe von Meldedaten befugt ist und dies ggf. auch durch organisatorische Maßnahmen zu sichern.

Der Fall gibt aber auch zu der folgenden Überlegung Anlaß: Eine Beanstandung bezieht sich nach Art. 30 BayDSG auf eine festgestellte „Verletzung von Vorschriften über den Datenschutz". Nach Art. 2 BayDSG unterliegen dem Datenschutzgesetz und damit auch der Datenschutzkontrolle des Landesbeauftragten für den Datenschutz die öffentlichen Stellen. Sie sind ggf. Adressat einer Beanstandung. Da Verstöße gegen Datenschutzvorschriften jeweils menschliches Handeln voraussetzen, ist vor einer Beanstandung auch zu prüfen, ob ein bestimmtes nicht mit Datenschutzvorschriften übereinstimmendes Handeln der betreffenden öffentlichen Stelle zuzurechnen ist. Eine Beanstandung einer Datenübermittlung kann beispielsweise nicht in Frage kommen, wenn sie der Behörde ohne Zweifel nicht zuzurechnen wäre, wie im Falle einer Weitergabe von Daten durch einen Einbrecher (hier könnte allenfalls mangelnde Sicherung beanstandet werden). Anderes gilt, wenn Bedienstete und insbesondere Personen, die zur Vertretung der Gemeinde nach außen grundsätzlich berufen sind, gegen Datenschutzrechte verstoßen. Ist dieser Verstoß besonders schwerwiegend, ist der persönliche Anteil des Betreffenden an der Verantwortung für die rechtswidrige Handlung in der Beanstandung entsprechend hervorzuheben, so daß vor allem ihn die Mißbilligung, die die Beanstandung darstellt, trifft.

4.7.15. Übermittlung von Wähleranschriften an politische Parteien nur nach Art. 35 Abs. 1 MeldeG

Nach Art. 35 Abs. 1 MeldeG darf die Meldebehörde „Parteien und Wählergruppen im Zusammenhang mit allgemeinen Wahlen und mit Abstimmungen in den sechs der Stimmabgabe vorangehenden Monaten Auskunft aus dem Melderegister über die in Art. 34 Abs. 1 Satz 1 bezeichneten Daten von Gruppen von Wahlberechtigten erteilen ...." Unabhängig davon bestand nach § 19 Abs. 4 der Landeswahlordnung und § 5 Abs. 5 der Gemeindewahlordnung die Möglichkeit, während der Auslegungsfrist Abschriften oder Auszüge des Wählerverzeichnisses, das ebenfalls Namen und Anschriften der Wahlberechtigten enthält, zu erteilen. Da diese Möglichkeit nach dem Wahlrecht erst ab dem

24. bzw. 27. Tag vor der Abstimmung möglich war und dies für eine Direktadressierung von Wahlwerbung wohl zu kurzfristig ist, wurde im Landesmeldegesetz die neue Bestimmung des Art. 35 Abs. 1 MeldeG (entsprechend einer früheren Regelung in der Vollzbek. zum früheren MeldeG) geschaffen. Die Neuregelung wurde mit der Einführung einer Widerspruchsmöglichkeit in Art. 35 Abs. 1 Satz 3 MeldeG verbunden, so daß sich nun die Frage des Verhältnisses dieser Regelung zu den Bestimmungen über die Weitergabe von Abschriften der Wählerlisten stellte.

Ich habe gegenüber dem Bayerischen Staatsministerium des Innern die Auffassung vertreten, daß ich die Einfügung des Widerspruchsrechts für eine wichtige Konkretisierung des Verhältnismäßigkeitsgrundsatzes bzw. Übermaßverbotes halte. Da das Widerspruchsrecht im Verhältnis zum Landes- und Gemeindewahlrecht in einer späteren Rechtsnorm enthalten ist und als konkrete Regelung zur Weitergabe von Anschriften der Wahlberechtigten zum Zwecke der Wahlwerbung eine Spezialvorschrift gegenüber den allgemeinen Vorschriften der Wahlordnungen darstellt, geht die neuere Regelung vor. Auch ist Anliegen der Wahlordnung im wesentlichen die Transparenz des Wahlverfahrens, nicht aber die Nutzbarkeit der Anschriften für Direktadressierung. Auch als gesetzliche Regelung der Konfliktlage geht Art. 35 Abs. 1 MeldeG den Regelungen über die Wählerlisten in den Wahlordnungen vor. Es wäre unverständlich, dem Widerspruch eines Wahlberechtigten gegen die Weitergabe seiner Anschriften für Direktwerbung durch Parteien und Wählergruppen während des 6. bis einschließlich 2. Monats vor der Wahl zu entsprechen, nach Auslegung der Wählerlisten jedoch eine uneingeschränkte Nutzung der Wähleranschriften durch Parteien und Wählergruppen zuzulassen. Ich habe daher angeregt, in der anstehenden Änderung des Gemeindewahlrechts und durch Änderung des Landeswahlrechts klarzustellen, daß die Frage der Nutzung von Wähleranschriften durch Parteien oder Wählergruppen, abgesehen von der Nutzung zur Überprüfung der Wählerlisten auf inhaltliche Richtigkeit, ausschließlich nach Art. 35 Abs. 1 MeldeG zu beurteilen ist. Das Bayerische Staatsministerium des Innern hat dies in § 5 Abs. 5 der Gemeindewahlordnung durch Anfügung eines neuen Satzes 6 berücksichtigt, der lautet: „Für Parteien oder Wählergruppen bemißt sich die Anfertigung oder Erteilung von Abschriften und Auszügen nach Art. 35 Abs. 1 des MeldeG." Das Ministerium hat außerdem mitgeteilt, daß in Aussicht genommen sei, im Rahmen der im Jahre 1985 vorgesehenen Novellierung der Landeswahlordnung die gleiche Änderung vorzunehmen, wie bei der Gemeindewahlordnung.

### 4.7.16. Nutzung von Einwohnerdaten für eine Partei außerhalb der Sechsmonatsfrist des Art. 35 Abs. 1 MeldeG

Durch eine Eingabe wurde bekannt, daß ein Bürgermeister Adreßaufkleber aus dem Einwohnerdatenbestand seines gemeindlichen Melderegisters zur Adressierung eines Werbeschreibens der Partei, der er angehört, verwendet hatte. Der Sachverhalt war einmal nach Art. 31 MeldeG (Weitergabe von Meldedaten an den Bürgermeister), zum andern nach Art. 35 MeldeG (Übermittlung an Parteien) zu prüfen. Die Inanspruchnahme der Daten durch den Bürgermeister war durch Art. 31 MeldeG nicht gedeckt. Die Aufgaben der Meldebehörde, für deren Erfüllung Einwohnerdaten genutzt werden dürfen, sind in Art. 2 MeldeG festgelegt. Die Nutzung von Meldedaten zur Adressierung von Schreiben von Parteien gehört nicht zu diesen Aufgaben. Sie gehört aber auch nicht zu den übrigen Aufgaben der Gemeinde oder zu den Aufgaben des Bürgermeisters als Gemeindeorgan. Die Inanspruchnahme der Daten konnte daher nicht mit der Erfüllung einer Aufgabe des Datenempfängers begründet werden. Art. 6 MeldeG, wie auch Art. 14 Abs. 1 BayDSG verbieten darüber hinaus auch Gemeindebediensteten personenbezogene Daten zu einem anderen als den zur jeweiligen rechtmäßigen Aufgabenerfüllung gehörenden Zweck zu verarbeiten, bekannt zu geben, zugänglich zu machen oder sonst zu nutzen.

Nach Art. 35 Abs. 1 MeldeG wäre es dagegen zulässig, Anschriften der, wie im vorliegenden Fall 18 – 30jährigen Wahlberechtigten innerhalb von 6 Monaten vor einer allgemeinen Wahl an Parteien im Zusammenhang mit der Wahl zu übermitteln. Der Empfänger müßte die Daten spätestens einen Monat nach der Wahl löschen. Da die Inanspruchnahme der Daten jedoch lange vor Beginn der Sechsmonatsfrist vor der Wahl lag, kam die für Parteien geschaffene Sondervorschrift des Art. 35 Abs. 1 MeldeG nicht zur Anwendung.

Es war aber auch nicht möglich eine solche Datenübermittlung vor Beginn dieser Sechsmonatsfrist nach Art. 34 Abs. 3 MeldeG (Gruppenauskunft an nichtöffentliche Stellen) zu rechtfertigen. Art. 35 MeldeG stellt für die dort genannten Datenempfänger (Parteien, Presse, Adreßbuchverlage u.a.) eine Spezialvorschrift dar, die die Anwendung von Art. 34 Abs. 3 MeldeG ausschließt (so auch jetzt die VollzBekMeldeG in Nr. 35.1 Abs. 2).

Die Anwendbarkeit von Art. 34 Abs. 3 MeldeG (entsprechend § 22 Abs. 1 MRRG) setzt für jede Art von Gruppenauskünften die Bejahung eines „öffentlichen Interesses" voraus. Mit der Frage, inwieweit für Melderegisterauskünfte an Parteien, Presse, Adreßbuchverlage etc. ein solches „öffentliches Interesse" angenommen werden kann, hat sich nun aber bereits der Gesetzgeber in Art. 35 MeldeG auseinandergesetzt. Er hat die von ihm für sachgerecht gehaltenen Grenzen und Bedingungen, darunter die 6-Monats-Frist, in dieser Vorschrift festgelegt. Nach der früheren Rechtslage, die für solche Gruppenauskünfte ebenfalls ein öffentliches Interesse zur Voraussetzung machte, war stets angenommen worden, daß für Auskünfte über Anschriften von Wahlberechtigten an Parteien ein solches öffentliches Interesse dann angenommen werden konnte, wenn die Anschriften innerhalb von 6 Monaten vor der Wahl für Zwecke der Wahl erbeten wurden (siehe die frühere VollzbekMeldeG, Nr. 3.3.2). Diese bewährte Regelung ist nun vom Gesetzgeber unmittelbar in Art. 35 Abs. 1 MeldeG übernommen worden. Es liegen auch keine Anhaltspunkte dafür vor, daß der Gesetzgeber außerhalb der Sechsmonatsfrist den Meldebehörden freistellen wollte, ein öffentliches Interesse für derartige Gruppenauskünfte anzunehmen. Der Gesetzgeber hat damit einen Kompromiß geschlossen zwischen der von ihm anerkannten Notwendigkeit, den Parteien im zeitlichen Zusammenhang mit Wahlen ein direktes Anschreiben der Wahlberechtigten zu ermöglichen und den andererseits aus einer unbeschränkten Weitergabe von Anschriften an Parteien ansonsten zu erwartenden Beeinträchtigungen. Hierzu wurde im Berichtsjahr bekannt, daß von Privatpersonen eine Vereinigung gegründet worden war, die sich als Partei ausgab um von Meldeämtern Adressenmaterial zu erhalten. Die Adressen sollten in Wirklichkeit für Versicherungs- bzw. Mitgliederwerbung genutzt werden.

In diesem Zusammenhang sei im Vorgriff auf den Tätigkeitsbericht 1984 kurz darüber berichtet, daß vor der Kommunalwahl 1984 erneut eine größere Anzahl von Beschwerden wegen Nutzung von Meldedaten durch Parteien beim Landesbeauftragten für den Datenschutz eingingen. Diesen Fällen war gemeinsam, daß die Betroffenen von ihrem Recht, der Weitergabe ihrer Anschrift an Parteien zu widersprechen (Art. 35 Abs. 1 Satz 3 MeldeG) keine Kenntnis hatten. Ich weise deshalb auch in diesem Bericht, wie schon in früheren Stellungnahmen zur Entwicklung des Melderechts, darauf hin, daß für die sogenannten „Altfälle" (also für diejenigen Betroffenen, die sich vor Inkrafttreten des neuen MeldeG angemeldet hatten und daher keine Kenntnis von den Widerspruchsmöglichkeiten nach Art. 35 MeldeG erhielten) eine angemessene Möglichkeit zur Bekanntgabe der Widerspruchsrechte gefunden werden muß (Gleichbehandlung). Ich habe hierzu wiederholt vorgeschlagen, daß die Meldebehörden etwa zweimal jährlich hierüber einen Hinweis veröffentlichen oder eine entsprechende Bekanntmachung aushängen sollen. Dem ist bisher vom Staatsministerium des Innern stets mit dem Argument widersprochen worden, die Verwaltung könne unmöglich auf sämtliche Rechte, die ein Bürger hat, öffentlich hinweisen. Dem ist grundsätzlich zuzustimmen; hier aber handelt es sich um Rechte aller Bürger, bei denen sich die Voraussetzungen für ihre Inanspruchnahme in bestimmten Abständen wiederholen. Deshalb meine ich, daß auf die Widerspruchsmöglichkeit nach Art. 35 MeldeG durchaus immer wieder öffentlich hingewiesen werden könnte, ohne daß dadurch in nennenswertem Umfang Bezugsfälle entstünden. Für Adreßbuchverlage wurde dies inzwischen in Nr. 35.4 VollzBekMeldeG, in einer Soll-Vorschrift, vorgesehen.

4.7.17. Verwendung der im Melderegister gespeicherten Seriennummer von Paß oder Personalausweis (Art. 3 Abs. 2 Nr. 7 MeldeG)

Von anderen Landesbeauftragten für den Datenschutz und dem Bundesbeauftragten für den Datenschutz ist wiederholt die Speicherung der Seriennummer des Personalausweises und des Passes im Melderegister kritisiert worden. Die Nummern seien Daten, die der Identitätsfeststellung von Einwohnern dienen würden. Die Daten, die im Melderegister zur Identitätsfeststellung von Personen gespeichert werden dürfen, seien aber durch das Melderechtsrahmengesetz auch für den Landesmeldegesetzgeber bindend und abschließend festgelegt. Darunter befindet sich die Angabe über die Seriennummer von Paß oder Personalausweis nicht.

Art. 3 Abs. 2 Nr. 7 MeldeG gestattet der Meldebehörde, „für die Mitwirkung bei Maßnahmen der Gefahrenabwehr oder Strafverfolgung" die Seriennummer des Passes oder Personalausweises zu speichern. Diese Zweckbestimmung umfaßt eine Vielzahl möglicher Verwendungen bei der Polizei. Ich habe daher versucht zu klären, inwieweit die Polizei die genannten Daten für andere Zwecke als die Feststellung der Identität einer Person benötigt.

Das Bayer. Staatsministerium des Innern hatte bereits in den Beratungen über den Entwurf eines Landesmeldegesetzes im Beirat beim Landesbeauftragten für den Datenschutz erklärt, diese Angabe diene nicht der Feststellung der Identität des Einwohners, sondern zur Feststellung von gestohlenen und als verloren gemeldeten Personalausweisen und Pässen. Ich habe daraufhin das Bayer. Staatsministerium des Innern gebeten, den Arbeitsablauf zu schildern, der bei der Nutzung der Seriennummer von Paß oder Personalausweis bei der Polizei abläuft.

## 4.8. **Steuerverwaltung**

### 4.8.1. Steuerverwaltung, allgemein

Auch in diesem Berichtsjahr – wie in den Vorjahren – habe ich mich mit den Datenschutzbeauftragten der Länder und des Bundes um eine Klarstellung des Verhältnisses des Steuergeheimnisses zur Kontrollzuständigkeit der Datenschutzbeauftragten in der Abgabenordnung bemüht. Das Bayer. Staatsministerium der Finanzen hat sich die Forderung nach Ergänzung der Abgabenordnung (AO) im Zuge der geplanten AO-Novelle aus folgenden Erwägungen nicht zu eigen gemacht:

„Der ursprüngliche Referentenentwurf sieht eine Aufnahme des Kontrollrechts der Datenschutzbeauftragten in die Ausnahmevorschrift des § 30 Abs. 4 AO nicht vor, weil man der Auffassung war, daß eine solche Bestimmung nicht aus der Aufgabenstellung der Finanzverwaltung, sondern der Datenschutzbeauftragten herrühren und deshalb letztere ihren Einfluß auf den Gesetzgeber geltend machen sollten, wenn sie eine derartige Vorschrift als für ihre Arbeit erforderlich ansehen würden. Die Finanzverwaltung hat sich stets gegen eine weitgehende Durchlöcherung des Steuergeheimnisses durch Ausnahmevorschriften gewandt und deshalb auch davon abgesehen, einer hier gewiß mit guten Argumenten begründbaren Durchbrechung das Wort zu reden."

In meiner Stellungnahme zu einem überarbeiteten Referentenentwurf eines Gesetzes zur Änderung der Abgabenordnung, die auch über den Bundesbeauftragten für den Datenschutz dem Bundesminister für Finanzen zugeleitet wurde, habe ich die Aufnahme einer die Kontrollbefugnis der Datenschutzbeauftragten entsprechend klarstellenden Regelung in § 30 Abgabenordnung erneut gefordert. Gleichzeitig habe ich das Bayer. Staatsministerium der Finanzen gebeten, die entsprechenden Vorschläge zu unterstützen.

### 4.8.2. Kontrollmitteilungen

Mehrere Petenten hatten sich mit der Bitte um Überprüfung der Zulässigkeit der regelmäßigen Übersendung von Kontrollmitteilungen über Vergütungen an Finanzämter an mich gewandt. Die Datenschutzbeauftragten der Länder und des Bundes hatten auf die ihrer Ansicht nach bestehende Notwendigkeit, die Kontrollmitteilungen auf eine eindeutige Rechtsgrundlage zu stützen, bereits hingewiesen. Der Bundesminister der Finanzen hat das Problem in einem Entwurf zur Änderung der Abgabenordnung aufgegriffen. Gleichwohl war es aufgrund der Eingaben erforderlich, für die Zeit bis zum Inkrafttreten einer Ergänzung der Abgabenordnung eine aus der Sicht des Datenschutzes befriedigende Lösung zu finden.

Die Zulässigkeit der Kontrollmitteilungen beurteilt sich nach den Vorschriften der Abgabenordnung (AO), da das Bayer. Datenschutzgesetz zurücktritt, wenn besondere Vorschriften über den Datenschutz, über Verschwiegenheitspflichten oder über Verfahren der Rechtspflege gelten (Art. 2 Abs. 2 BayDSG). § 93 AO regelt die Auskunftspflicht der Beteiligten und anderer Personen, gegenüber der das BayDSG mit seinen Übermittlungsregelungen zurücktritt. § 93 AO begründet eine Auskunftspflicht der Beteiligten, sowie dritter Personen über die für die Besteuerung erheb-

liche Sachverhalte. Nichtbeteiligte dritte Personen dürfen nach § 93 Abs. 2 Satz 1 AO nur im Einzelfall aufgrund eines konkreten Auskunftsersuchens in Anspruch genommen werden. Dabei ist nach § 93 Abs. 1 Satz 1 AO sorgfältig zu prüfen, ob die Auskunft zu Feststellung des steuererheblichen Sachverhalts erforderlich ist. Zunächst ist daher der Steuerpflichtige selbst zu befragen. § 93 Abs. 1 Satz 3 AO regelt ausdrücklich, daß nichtbeteiligte Dritte nur in Anspruch genommen werden sollen, wenn die Sachverhaltsaufklärung durch die Beteiligten nicht zum Ziele führt oder keinen Erfolg verspricht.

Die Soll-Vorschrift des § 93 Abs. 1 Satz 3 AO ist m.E. so auszulegen, daß Dritte zur Ermittlung des Steuersachverhaltes nur herangezogen werden können, soweit sich dies ausnahmsweise und im Einzelfall als erforderlich erweist. Auch der Bundesfinanzhof hat in seinem Urteil vom 27.10.1981 (Bundessteuerblatt 82, S. 141) ausgeführt, daß die Finanzverwaltung in der Regel nach der Soll-Vorschrift des § 93 Abs. 1 Satz 3 AO verfahren muß und nur in atypischen Fällen von der dort festgelegten Verfahrensweise abweichen darf. Einen solchen atypischen Fall sieht der Bundesfinanzhof z.B. darin, daß der Steuerpflichtige unbekannt ist. In diesem Fall kann sich das Finanzamt also der Hilfe Dritter zur Sachverhaltsaufklärung bedienen. Es ist jedoch zu unterscheiden zwischen der Ermittlung des unbekannten Steuerpflichtigen und der Ermittlung der die Steuerpflicht begründenden weiteren Besteuerungsgrundlagen. Wenn die Ermittlung des unbekannten Steuerpflichtigen in manchen Fällen nur durch Zuhilfenahme dritter Personen zum Erfolg führt, so gilt dies nicht in jedem Fall gleichzeitig auch für die Übermittlung der Besteuerungsgrundlagen. Ist der Steuerpflichtige erst einmal bekannt, so muß sich die Finanzverwaltung zur Aufklärung des Steuersachverhaltes zunächst an ihn wenden. Nur wenn dies ohne Erfolg bleibt, oder im Einzelfall feststeht, daß die Ermittlung beim Steuerpflichtigen keinen Erfolg haben wird, darf von Dritten auch Auskunft über Besteuerungsgrundlagen gefordert werden. Kontrollmitteilungsverfahren, die gleichzeitig die Besteuerungsgrundlagen mitteilen, können daher gegen § 93 AO verstoßen.

Im Zusammenhang mit Kontrollmitteilungen, die vom Bayer. Rundfunk an Finanzämter übersandt wurden, ist nun ein Vorschlag für eine praktische Lösung entwickelt worden, der sich in dem vom Bundesfinanzhof für zulässig erachteten Rahmen hält. Danach sollen die Mitarbeiter Honorarabrechnungen erhalten, die inhaltlich den bisherigen Kontrollmitteilungen an die Finanzbehörden entsprechen. Die Finanzbehörden sollen gleichzeitig Mitteilungen über die Namen und Anschriften der Mitarbeiter erhalten und können dann im Einzelfall bei Bedarf die Ermittlungen bei den einzelnen Mitarbeitern aufnehmen und ggf. die Honorarabrechnungen anfordern. Bis zu einer endgültigen Regelung in der Abgabenordnung wird das Bayer. Staatsministerium der Finanzen gegen dieses Verfahren keinen Einwand erheben.

Ich habe hierüber die Petenten und auch den Bayer. Volkshochschulverband unterrichtet.

4.8.3. Einzelfälle

Im Zusammenwirken mit der Steuerverwaltung waren aufgrund von Bürgereingaben eine Zahl von Einzelfragen zur Datenoffenbarung im Steuerverfahren zu klären:

- Angabe der Steuernummer auf Zahlungsträgern, die auch dritte Stellen zu Gesicht bekommen:

  Zur eindeutigen Zuordnung des Schriftverkehrs und als notwendiges Unterscheidungsmerkmal in den Fällen, in denen einem Steuerpflichtigen mehrere Steuernummern zugeteilt werden müssen, ist nach Auffassung der Finanzverwaltung die Steuernummer zur eindeutigen Zuweisung zum betroffenen Steuerkonto erforderlich. Dies gilt auch für Steuerrückerstattungen, da sonst Erstattungsanweisungen, die zurücklaufen, weil sie von Banken nicht bearbeitet werden können, ebenfalls nicht zugeordnet werden könnten. Um eine Durchbrechung des Steuergeheimnisses durch Gebrauch der Steuernummer durch unbefugte Dritte zu verhindern, sind die Finanzämter angewiesen, sich bei telefonischen Anfragen unter Bezugnahme auf die Steuernummer über die Personenidentität des Anrufers durch weitere spezielle Fragen zu vergewissern, bzw. den Steuerpflichtigen mit der in der Steuererklärung angegebenen Telefonnummer selbst anzurufen. Die Angabe der Steuernummer auf Zahlungsträgern erscheint deshalb gem. § 30 Abs. 4 Ziff. 1 AO zur Durchführung des Steuerverfahrens gerechtfertigt.

- Bekanntgabe der auf einzelne Kommanditisten entfallenden Einkünfte auch an alle übrigen Kommanditisten durch das Finanzamt:

  Im Rahmen der durch die Abgabenordnung vorgeschriebenen gesonderten und einheitlichen Feststellung der Einkünfte der Gesellschaft zu einer Kommanditgesellschaft ist notwendiger Inhalt des Bescheides die Feststellung, wer an dem festgestellten Betrag beteiligt ist und wie dieser sich auf die einzelnen Beteiligten verteilt. Dieser gesamte Bescheid ist allen Gesellschaftern gegenüber bekanntzugeben (§ 179, 180 AO).

- Übermittlung der Steuernummer sowie des betreffenden Gewerbesteuermeßbetrags durch das Finanzamt an die Handwerkskammer:

  Sie ist nach § 31 AO zulässig, da der Handwerkskammerbeitrag an den Gewerbesteuermeßbetrag anknüpft.

- Bekanntgabe der für das Verfahren der Forderungspfändung benötigten Angaben über den Vollstreckungsschuldner durch das Finanzamt an einen unbeteiligten Dritten, der nicht, wie in einem mir mitgeteilten Fall irrtümlich angenommen, Schuldner des Vollstreckungsschuldners ist:

  Eine solche Bekanntgabe ist wegen Verstoßes gegen das Steuergeheimnis (§ 30 AO) unzulässig.

## 4.9. **Personalwesen**

### 4.9.1. Datenschutzfragen im Beihilfewesen

Staat, Gemeinden und Gemeindeverbände sowie viele andere öffentliche Stellen gewähren ihren Beamten im Rahmen der sogenannten Beihilfe-Richtlinien im Krankheitsfalle finanzielle Beihilfen, da sie nicht der Sozialversicherung unterliegen. Den durch Beihilfe nicht gedeckten Teil der Krankheitskosten (bis zu 50%) muß der Beamte durch eine private Krankenversicherung selbst abdecken, zu der der Arbeitgeber keinen Zuschuß leistet. Die öffentliche Hand erspart dadurch die Zahlung entsprechender Arbeitgeberanteile zur Krankenversicherung.

Folge der Beihilfegewährung ist, daß die Beihilfeberechtigten dem Dienstherrn mit den Beihilfeanträgen Rechnungen von Ärzten, Krankenhäusern und Apotheken als Belege

vorlegen müssen, um Beihilfe zu erhalten. Dies betrifft auch ihre Familienangehörigen. Bis vor einiger Zeit war in diesem Zusammenhang in verschiedenen Eingaben immer wieder beanstandet worden, daß Behörden nicht sichergestellt hätten, daß ärztliche Rechnungen mit Diagnosen und Behandlungsangaben in verschlossen Umschlägen direkt der jeweiligen Beihilfestelle übergeben werden könnten (siehe auch 5. Tätigkeitsbericht Nr. 4.10, Seite 40/41). Seit Ärzte nun durch die seit Anfang 1983 geltende neue Gebührenordnung gezwungen sind, wesentlich eingehendere Angaben über Krankheit und Behandlung des Patienten auf der Liquidation auszuweisen, ist die Sorge der Betroffenen, der Dienstherr könne hiervon Kenntnis nehmen und daraus problematische Schlüsse ziehen, gewachsen. Nicht zuletzt veranlaßt durch diese Eingaben habe ich mich im Berichtsjahr zunächst an das für Beihilfe federführende Bayerische Staatsministerium der Finanzen und dann an die übrigen Geschäftsbereiche gewandt und die tatsächliche und rechtliche Problematik vorgetragen.

Ich habe dabei auch darauf hingewiesen, daß die teilweise mangelnde Abschottung des Verfahrens der Beihilfebearbeitung von der übrigen Verwaltung, insbesondere der Personalverwaltung, dazu führen könnte, daß Beihilfeberechtigte in manchen Fällen vorsorglich davon absähen, Rechnungen zur Beihilfegewährung einzureichen, oder überhaupt den Arzt aufzusuchen, um nicht den Eindruck eingeschränkter gesundheitlicher Eignung für ihr weiteres berufliches Fortkommen zu erwecken. Auch von therapeutischen Behandlungseinrichtungen wurde diese Sorge vorgetragen, die über entsprechende Ängste von Patienten berichteten.

Unter rechtlichen Gesichtspunkten habe ich den in Frage stehenden Umgang mit personenbezogenen und deshalb besonders schutzwürdigen medizinischen Daten folgendermaßen beurteilt: Die in Art. 86 des Bayerischen Beamtengesetzes festgelegte Pflicht des Dienstherrn, im Rahmen des Dienst- und Treueverhältnisses für das Wohl des Beamten und seiner Familie zu sorgen, ist nicht nur Grundlage für den Beihilfeanspruch selbst. Sie enthält meines Erachtens auch die Verpflichtung, das Beihilfewesen so zu organisieren, daß Beihilfeberechtigte im Krankheitsfall die Beihilfe in Anspruch nehmen können, ohne Nachteile durch anderweitige Verwendung der Daten befürchten zu müssen. Es wäre unverständlich, wenn sich aus dem mit der besonderen beamtenrechtlichen Fürsorgepflicht des Dienstherrn begründeten Beihilfewesen in der Praxis eine Schlechterstellung der Beamten gegenüber anderen Beschäftigten des Öffentlichen Dienstes ergeben würde. Dies ist jedenfalls denkbar, weil nicht beihilfeberechtigte Bedienstete, sowie Beamte, die freiwillig Mitglieder von Ortskrankenkassen oder Ersatzkassen sind, dem Dienstherrn medizinische Angaben nicht zur Abrechnung von Krankheitskosten zu offenbaren brauchen.

Hieraus folgt meines Erachtens, daß die Verwaltung der Beihilfe von der übrigen Verwaltung, einschließlich der Personalverwaltung, hineichend getrennt sein muß.

Verfassungsrechtliche Erwägungen führen ebenfalls zu diesem Ergebnis. Das Urteil des Bundesverfassungsgerichts vom 15.12.1983 zum Volkszählungsgesetz 1983 hat die in Weiterführung der bisherigen Rechtssprechung (siehe auch 5. Tätigkeitsbericht Nr. 4.10 Seite 40/41 und 4.2., Seite 13/14) festgestellt, daß das durch Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 des Grundgesetzes gewährleistete allgemeine Persönlichkeitsrecht auch die aus dem Gedanken der Selbstbestimmung folgende Befugnis des Einzelnen umfaßt, grundsätzlich selbst zu entscheiden, wann und innerhalb welcher Grenzen er persönliche Lebenssachverhalte offenbaren will. Dieses Recht auf „informationelle Selbstbestimmung" ist jedoch nicht schrankenlos gewährleistet.

Beamte unterliegen im Rahmen ihres Dienstverhältnisses bestimmten gesetzlichen Beschränkungen. Eine entsprechende Beschränkung fehlt jedoch hinsichtlich der Beihilfedaten des Beamten und seiner Angehörigen. Dem kann meines Erachtens auch nicht entgegengehalten werden, daß der betroffene Beamte mit seinem Antrag auf Beihilfe in eine beliebige Nutzung seiner Beihilfedaten durch den Dienstherrn konkludent einwillige, denn er kennt den genauen Umfang eventueller, neben der Beihilfeberechnung denkbarer sonstiger Nutzungen der vorgelegten Abrechnungen nicht. Zudem ist festzustellen, daß Personalverwaltungen grundsätzlich erklären, derartige Informationen würden nicht für sonstige Zwecke, auch nicht der Personalverwaltung, genutzt. Da die Daten beim Arzt einer besonderen Schweigepflicht unterliegen, die gerade vor staatlichen Eingriffen schützen soll, kann nicht unterstellt werden, die Betroffenen würden einer sonstigen Nutzung zustimmen (vergl. § 203 Abs. 1 Nr. 1 und Abs. 3 StGB, §§ 53 Abs. 1 Nr. 3, 53 a, 97 Abs. 1 Nr. 2 und 3 und Abs. 4 StPO, § 76 SGB X). Schließlich steht dem Betroffenen in der Regel keine Alternative zum Beihilfeantrag zu Gebote. Er muß deshalb darauf vertrauen können, daß ihm aus seinem Antrag keine Beschwer erwächst, die nicht mit der Abrechnung unmittelbar zusammenhängt.

Ich halte daher die rechtliche Befugnis zur Kenntnisnahme und Nutzung der mit dem Beihilfeantrag vorgelegten medizinischen Daten durch den Zweck des Antrags, die Beihilfeabrechnung, für absolut beschränkt, denn diese Befugnis leitet sich ausschließlich aus der Vorlage durch den Betroffenen, und damit aus seiner entsprechenden Einwilligung, ab. Ob eine Beamter, der eine Arztrechnung nicht einreicht, möglicherweise verpflichtet wäre den Dienstherrn auf gesundheitliche Beschränkungen hinzuweisen, die seine Verwendbarkeit erheblich berühren, ist eine andere Frage. Eine rechtliche Befugnis des Dienstherrn, den physischen Besitz an der zur Beihilfe eingereichten Arztrechnung zur anderweitigen Nutzung der darin enthaltenen Informationen zu verwenden, vermag ich nicht zu erblicken.

Dem Staat ist es m. E. auch verwehrt, Beihilfe nur unter der Bedingung zu gewähren, daß die medizinischen Daten auch anderweitig von dem Dienstherrn genutzt werden dürfen. Dies würde den Betroffenen in eine rechtlich bedenkliche Zwangslage versetzen. Denn der öffentliche Arbeitgeber, der u.a. aus Kostengründen die Beihilfezahlung der Entrichtung von Arbeitgeberanteilen zur Krankenversicherung vorzieht, läßt dem Betroffenen wirtschaftlich gesehen keine Wahl, da er ihn finanzell nur im Falle der Einreichung des Beihilfeantrages unterstützt.

In seltenen Ausnahmefällen könnte denkbar sein, daß eine vorgelegte Beihilferechnung auf eine Krankheit des Beamten hinweist, die eine massive akute Gefahr für andere darstellt. Soweit in diesen Fällen die in § 34 des Strafgesetzbuches genannten Voraussetzungen des rechtfertigenden Notstands vorliegen, halte ich im Einzelfall eine auf das unerläßliche Maß beschränkte Nutzung der Information aus

dem Beihilfeantrag in entsprechender Anwendung des Rechtsgedankens aus dieser Vorschrift für gerechtfertigt. In allen übrigen Fällen muß der Dienstherr solche Daten meines Erachtens jedoch unberücksichtigt lassen, wie bei Angestellten, Arbeitern oder privat in der Sozialversicherung versicherten Beamten, von denen er keine Arztrechnungen vorgelegt erhält. Ergänzend sei darauf hingewiesen, daß in Fällen von ansteckender Krankheiten das besondere Verfahren nach dem Bundesseuchengesetz die angemessene Reaktion auf eine Gefahr vorsieht.

Aus den dargelegten Erwägungen halte ich eine strikte Trennung des Beihilfeantragsverfahrens vom sonstigen Posteinlauf und -auslauf sowie der Beihilfebearbeitung vom sonstigen Aufgabenvollzug – insbesondere der Personalverwaltung – und der Beihilfeakten von sonstigen Akten – insbesondere Personalakten – für erforderlich. Dies muß durch geeignete organisatorische Maßnahmen sichergestellt werden. Hierbei muß auch das Problem der Interessenkollision der mit der Bearbeitung von Beihilfeanträgen betrauten Personen, denen gleichzeitig der Vollzug anderer Verwaltungsaufgaben übertragen ist, in deren Rahmen Daten aus dem Beihilfeantrag Verwendung finden könnten, einwandfrei gelöst werden.

Inzwischen wurden mit den Geschäftsbereichen Gespräche über die Möglichkeiten zur Lösung der angeschnittenen Fragen geführt. Ich habe dabei grundsätzliches Verständnis für meine Überlegungen gefunden. Das Ergebnis wird wohl der nächste Tätigkeitsbericht enthalten.

Unabhängig von der vorstehend beschriebenen Tätigkeit des Landesbeauftragten für den Datenschutz hat sich auf Initiative des Vorsitzenden des Beirats, MdL Regensburger, der Bayer. Landtag sowie der Bayerische Senat der Frage angenommen. Beide Stellungnahmen sind im Anhang zu diesem Tätigkeitsbericht abgedruckt (Anhang Nr. 8 und Nr. 9).

### 4.9.2. Datenschutzgerechte Gestaltung von Beihilfeanträgen

Neben der grundsätzlichen Frage des Umgangs mit Beihilfedaten (siehe oben) bin ich an das Bayerische Staatsministerium der Finanzen mit der Bitte herangetreten, die gegenwärtig verwendeten Beihilfeformulare unter dem Gesichtspunkt des Datenschutzes zu überprüfen. Die Überprüfung unter dem Gesichtspunkt der Erforderlichkeit der Datenerhebung halte ich für geboten bei den detaillierten Angaben zum Familienstand, zur Art der Leistung in der Zusammenstellung der Aufwendungen (die entsprechenden Angaben können Belegen entnommen werden), sowie zum Ehegatten und den Kindern, wenn Beihilfe nur für den Antragsteller selbst beantragt wird.

Im Zusammenhang mit einer deshalb wünschenswerten Neukonzeption der Antragsformulare könnten im übrigen auch Einzelheiten für die formelle büromäßige Behandlung der Antragsformulare und der beigefügten Belege bis zur Beihilfestelle geregelt werden, so daß alle Angaben, die darin z.B. über Einkünfte des Ehegatten oder dessen Arbeitsverhältnis enthalten sind, jedenfalls nur der Beihilfeberechnungsstelle bekannt werden.

### 4.9.3. Personalbögen

Durch Datenschutzkontrollen und Eingaben bin ich auf die Problematik des Datenumfangs bei Personalbögen des öffentlichen Dienstes gestoßen. Einige von staatlichen Stellen verwendete Personalbögen sehen umfangreiche Fragen an den Bewerber vor, die im Falle der Anstellung im Personalakt verbleiben. Ich habe dem Bayerischen Staatsministerium der Finanzen das vorläufige Ergebnis meiner Überprüfung mitgeteilt – sowohl was die gegenwärtige rechtliche Basis der Datenerhebung und Speicherung betrifft, als auch Bedenken gegen einzelne Fragen, die ich in Personalbögen gefunden habe. Da eine Stellungnahme des Ministeriums noch nicht vorliegt, beschränke ich mich im folgenden auf eine kurze Wiedergabe meiner rechtlichen Beurteilung.

1. Der Personalbogen stellt einen Teil des Personalaktes dar. Soweit für die Personalbogenführung keine besondere Vorschriften bestehen, ist diese daher nach den Regelungen und Grundsätzen der Personalaktenführung zu beurteilen. Das Personalaktenrecht des öffentlichen Dienstes wiederum muß unter Berücksichtigung der Besonderheiten des öffentlichen Dienstes, vor dem Hintergrund des arbeitsrechtlichen Personaldatenrechts, gesehen werden.

   Das Personaldatenrecht des öffentlichen Dienstes ist nur lückenhaft positiv gesetzlich geregelt und wird weitgehend von hergebrachten und von der Rechtssprechung bestätigten Grundsätzen bestimmt. Hierzu gehören zum einem das Recht des Dienstherrn auf Führung von Personalakten, das allgemein auch dort anerkannt wird, wo es nicht positiv gesetzlich geregelt ist, sowie das von der Rechtsprechung wiederholt bestätigte Vollständigkeitsprinzip. Hinzu kommt der Grundsatz der Fürsorgepflicht des Dienstherrn, der zuweilen als mildes Korrektiv dem Vollständigkeitsprinzip entgegengesetzt wird. Zu den für das Personalrecht geltenden Grundsätzen zählen auch die Verfassungsgrundsätze des Vorbehalts des Gesetzes und des Übermaßverbotes, sowie das aus Art. 2 Abs. 1 und 1 Abs. 1 des Grundgesetzes abzuleitende allgemeine Persönlichkeitsrecht. Dies könnte gegebenenfalls dazu führen, die oben genannten Grundsätze des Personalaktenrechts zu überdenken.

   In Bayern besteht folgende Rechtslage:

   Dem Grundsatz des Vorbehalts des Gesetzes wird für Beamten im Bayerischen Beamtengesetz Rechnung getragen, das als eines der wenigen bundes- bzw. länderrechtlichen Beamtengesetze in Art. 100 ausdrücklich das Recht der Personalaktenführung regelt. Zumindest im Hinblick auf die zu erwartende Automatisierung der Personaldatenverarbeitung im staatlichen Bereich wäre eine Überarbeitung der hierzu bestehenden Verwaltungsvorschriften erforderlich.

   Für die Angestellten des öffentlichen Dienstes gilt der Bundesangestelltentarifvertrag (BAT). In § 13 BAT ist das Einsichtsrecht des Angestellten in die Personalakte geregelt. Das Recht des Dienstherrn auf Führung der Personalakte wird, wie in den meisten dienst- und beamtenrechtlichen Vorschriften, vorausgesetzt. Eventuelle Bedenken, die sich hier aufgrund des Vorbehaltes des Gesetzes ergeben, könnten grundsätzlich durch die Aufnahme einer Art. 100 BayBG entsprechenden Regelung im BAT ausgeräumt werden. Für das Personalaktenrecht der Angestellten des öffentlichen Dienstes gelten im übrigen dieselben Grundsätze wie für das der Beamten, soweit sich nicht unmittelbar aus Art. 33 Abs. 5 GG so-

wie dem Bayerischen Beamtengesetz Besonderheiten ergeben. Aus dem Urteil des Bundesverfassungsgerichts zum Volkszählungsgesetz 1983 könnten sich darüber hinaus auch gewisse Anforderungen an den Grad der Genauigkeit solcher Vorschriften ergeben.

2. Das Bayerische Datenschutzgesetz ist nach seinem Art. 1 Abs. 1 nur anzuwenden, wenn Personaldaten in Dateien gespeichert werden. Die Personalbögen fallen als Teil des Personalaktes somit nicht unter den Schutzbereich des BayDSG. Auch wo dieses Gesetz nicht unmittelbar eingreift, weil Daten nicht in Dateien verarbeitet werden, besteht jedoch grundsätzlich kein datenschutzfreier Raum. Es muß vielmehr auf die tragenden Bestimmungen der Verfassung zum Schutz der Persönlichkeit zurückgegriffen werden. Aufgrund der Rechtsprechung bestehen generell keine Bedenken, die entsprechenden Bestimmungen des Bayerischen Datenschutzgesetzes als Regelungsmaßstab mit heranzuziehen, wenn es gilt, die Zulässigkeit der Datenverarbeitung der personenbezogenen Daten durch Behörden zu beurteilen (vergl. OVG Rheinland-Pfalz vom 24.7.1980). Es muß deshalb auch im hier interessierenden Bereich grundsätzlich davon ausgegangen werden, daß die Erhebung und Speichung von Daten nur zulässig ist, wenn sie zur rechtmäßigen Erfüllung einer öffentlichen Aufgabe der öffentlichen Stelle erforderlich ist (Analog Art. 6 BayDSG).

   Für Beamte ist diese Aufgabenzuweisung bereits in Art. 100 BayBG konkretisiert. Der zulässige Umfang eines Personalbogens hat seine äußerste Grenze daher in den Grenzen des nach dem BayBG für Personalakten zulässigen Inhalts. Nach der Rechtsprechung sind Personalakten eine Sammlung von Urkunden und Aktenvorgängen, die die persönlichen dienstlichen Verhältnisse eines Beamten betreffen (vergl. BVerVG E 85, 153 ff). Maßgebend ist hiernach der Grundsatz, daß die Personalakten ein möglichst vollständiges Bild der Persönlichkeit des Beamten geben sollen (vergl. BVerwG E 1979 ff). In den Kommentaren zum Beamtenrecht finden sich Umschreibungen von vom Bundesverwaltungsgericht geprägten Formeln, die jedoch nur deutlich machen, wie schwierig es ist, brauchbare Abgrenzungskriterien zu finden. Im übrigen wird auch klar, daß Rechtsprechung und Literatur sich mit dem Personalaktenbegriff bisher wenig unter dem Gesichtspunkt des Übermaßverbotes – das durch das Vollständigkeitsprinzip geradzu außer Kraft gesetzt zu sein scheint – befaßt hat und zudem die Fragestellung meist vom Personalakteneinsichtsrecht ausging. Bei der Frage der Überprüfung einzelner in Personalbogen enthaltener Daten kann auf Rechtsprechung nur vereinzelt zurückgegriffen werden, da sich diese insbesondere meist nur mit dem Einsichtsrecht befaßt hat – anders die arbeitsrechtliche Rechtsprechung, die sich häufiger mit dem Fragerecht des privaten Arbeitgebers auseinandergesetzt und zu einzelnen Fragen Stellung genommen hat.

   Schließlich sind die einzelnen Daten der Personalbögen unter dem Gesichtspunkt der Erforderlichkeit, der die besondere datenschutzrechtliche Ausprägung des Verfassungsgebotes der Verhältnismäßigkeit und des Übermaßverbotes darstellt, zu überprüfen. Während der „Zusammenhang mit dem Beamtenverhältnis" erste Voraussetzung für die Bejahung der Erforderlichkeit ist, können sich hieraus im Einzelfall aber auch Einschränkungen ergeben. Jedenfalls kann die Zulässigkeit der Datenerfassung und Speicherung im Personalbogen nicht angenommen werden, wenn die Erforderlichkeit nicht bejaht werden kann. Bei der Prüfung der Erforderlichkeit können sich abweichende Beurteilungen zwischen Personalbögen der Beamten und der Angestellten ergeben. Es sei jedoch darauf hingewiesen, daß die bisherige Rechtsprechung des Bundesarbeitsgerichts zum Personalaktenbegriff sich stark an die des Bundesverwaltungsgerichts angelehnt hat und kaum Differenzierungen zwischen Beamten und Angestellten vornimmt.

   Über das Ergebnis der Erörterungen zu einzelnen Fragen der Personalbögen hoffe ich im nächsten Tätigkeitsbericht berichten zu können.

4.9.4. Bundeskindergeldgesetz, Datenerhebung und Übermittlung

In Eingaben wurde wiederholt geltend gemacht, daß die im Fragebogen zur Überprüfung der Kindergeldminderung nach § 10 Abs. 2 des Bundeskindergeldgesetzes (BKGG) geforderten Einzelangaben, aus denen sich die „Summe der positiven Einkünfte" errechnet, zu weitgehend seien. Es sei unzumutbar, diese Einzelheiten, insbesondere auch über Einkommensverhältnisse des Ehegatten, gegenüber dem Dienstherrn zu offenbaren, der beispielsweise für Beamte das Kindergeld berechnet (für Beschäftigte außerhalb des öffentlichen Bereichs wird dies von den Arbeitsämtern durchgeführt).

Diesen Bedenken habe ich mich gegenüber dem federführenden Bayer. Staatsministerium der Finanzen angeschlossen und die Ansicht vertreten, daß es ausreichen müßte, lediglich die Summe der positiven Einkünfte anzugeben und ihre Richtigkeit auf Dienstpflicht zu versichern, was auch in anderen Fällen, z.B. bei Nebeneinkünften, üblich ist.

Im Gegensatz zu früher verwendeten Fragebogen wird in einem neu entwickelten Vordruck die betragsmäßige Darlegung der Einkommensverhältnisse, sowie die Angabe der Steuernummer nicht mehr verlangt. Die entsprechenden Beträge entnimmt die Kindergeldstelle vielmehr selbst dem Einkommensteuerbescheid, dem Bescheid über den Lohnsteuerjahresausgleich bzw. der Jahreslohnbescheinigung, wobei auf der vorzulegenden Kopie die für Kindergeld nicht erforderlichen Angaben unkenntlich gemacht werden können.

Die Datenschutzbeauftragten der Länder und des Bundes hatten in ihrem gemeinsamen Beschluß vom 6./7. Juni 1983 gefordert, in den Erhebungsformularen künftig nur noch die nach dem Bundeskindergeldgesetz maßgebliche Summe der positiven Einkünfte zu erheben, nicht aber deren Aufschlüsselung in einzelne Einkunftsarten zu verlangen und die Überprüfung der angegebenen Einkommensverhältnisse durch Vorlage des Einkommensteuerbescheides oder durch Einholung von Auskünften bei Finanzämtern auf solche Einzelfälle oder Fallgruppen zu beschränken, bei denen konkrete Anhaltspunkte für Mißbrauch gegeben sind oder Unstimmigkeiten vorliegen, die mit dem Antragsteller nicht geklärt werden können. Die Datenschutzbeauftragten haben angeregt zu prüfen, ein Verwaltungsverfahren zu finden, das es den Finanzbehörden ermöglicht, das für die Kindergeldberechnung maßgebliche Einkommen in einer gesonderten Bescheinigung für den Betroffenen auszuweisen. Ich habe daher die Initiative des Bayer. Staatsministe-

rium der Finanzen, einen entsprechenden Vorschlag dem Normprüfungsausschuß zu übermitteln, begrüßt.

In ihrem Beschluß haben die Datenschutzbeauftragten darauf hingewiesen, daß die für die Kindergeldbearbeitung erhobenen Daten einer strengen Zweckbindung unterliegen, die es dem KindergeldSachbearbeiter verbietet, Kindergelddaten (ohne Einwilligung des Betroffenen) an die mit der Bearbeitung von Personalsachen Betrauten weiterzugeben, oder, wenn er selbst auch mit der Bearbeitung von Personalsachen betraut ist, hierfür Kindergelddaten zu verwenden. Nach überwiegender Meinung unterliegt die Verarbeitung der Kindergelddaten dem Sozialgeheimnis nach dem Sozialgesetzbuch. Daraus ergibt sich, daß eine Verwendung von Kindergelddaten grundsätzlich die Einwilligung der Betroffenen voraussetzt (§ 35 SGB I, § 67 SGB X).

Zu Ende des Berichtsjahres waren die Verhandlungen über die Neugestaltung des Verfahrens zum Einkommensnachweis sowie über das Verfahren in den Kindergeldberechnungsstellen noch nicht abgeschlossen.

4.9.5. Vereinheitlichung der von Behörden geforderten Verdienstbescheinigungen der Arbeitgeber

Die Arbeitsgemeinschaft der Bayer. Industrie- und Handelskammern hat vorgeschlagen, die von den Arbeitgebern für die Vorlage bei Behörden auszustellenden Verdienstbescheinigungen zu vereinheitlichen. Wie ich erfahren habe, soll die unabhängige Kommission für Rechts- und Verwaltungsvereinfachung beim Bundesminister des Innern diesen Vorschlag prüfen. Auch aus der Sicht des Datenschutzes sind, so meine ich, Maßnahmen, die der Vereinfachung von Verfahren dienen und damit ihre Übersichtlichkeit für die Betroffenen fördern, zu begrüßen. Sollte es tatsächlich zur Entwicklung eines einheitlichen Vordruckes kommen, so wäre von seiten der Datenschutzbeauftragten darauf zu achten, daß dieser den jeweiligen Datenempfängern nicht mehr Daten preisgibt, als dies bisher geschehen bzw. für den konkreten Verwaltungsvollzug erforderlich ist. Gegebenenfalls müßte ein Verfahren gefunden werden, das diejenige Datenmenge, die von allen anfordernden Behörden übereinstimmend benötigt wird, von den speziellen Daten, die nur für einzelne Behörden erforderlich sind, trennt.

4.9.6. Aufnahme des Schwerbehindertenbescheides in den Personalakt

In der Eingabe eines schwerbehinderten öffentlich Bediensteten wurde mitgeteilt, daß der Dienstherr die Vorlage des Bescheides über die Anerkennung der Schwerbehinderteneigenschaft nach Abschnitt IX der Bekanntmachung des Bayerischen Staatsministeriums der Finanzen vom 6.4.1978 verlange. Der Petent vertrat die Auffassung, daß nicht alle im Bescheid enthaltenen Angaben über seine Behinderung für die Entscheidung des Dienstherrn über seinen möglichen Arbeitseinsatz erforderlich seien. Es gäbe vielmehr Behinderungen, die zwar bei der Berechnung der Behinderung der Erwerbsfähigkeit Beachtung finden, jedoch keine Auswirkungen auf die konkrete Arbeitsfähigkeit hätten und deren Offenbarung im Personalakt für ihn peinlich seien. Ich habe das Bayerische Staatsministerium der Finanzen um Überprüfung der seinerzeitigen Bekanntmachung gebeten.

Mit Schreiben vom 22. August 1983 (Nr. 26-P 1132-2/8-49029) hat das Bayerische Staatsministerium der Finanzen nun allen Geschäftsbereichen mitgeteilt, daß es an der Regelung über die Vorlage des rechtskräftigen Bescheids über die Anerkennung der Schwerbehindertеneigenschaft zur Beinahme zu den Personalakten nicht mehr festhalte. Nach dem Schreiben wird es in der Regel vielmehr genügen, eine Ablichtung des Schwerbehindertenausweises zu den Akten zu nehmen. Ausnahmen davon seien dann möglich, wenn ein besonders herausgehobener Dienstposten oder ein Dienstposten mit bestimmten Anforderungen an die körperliche Gewandtheit zu besetzen sei. Die gelte insbesondere für den gesamten Schulbereich, die Polizei sowie den Justizvollzugsdienst. Das Ministerium weist darauf hin, daß es in manchen Fällen wünschenswert erscheinen mag, daß der Behinderte nicht nur den Schwerbehindertenausweis vorlege, sondern auch die festgestellten Behinderungen mitteile. Die Erfüllung der besonderen Fürsorgepflicht z. B. für eine behindertengerechte Beschäftigung einschließlich des beruflichen Fortkommens und für die Ausgestaltung des Arbeitsplatzes könne im Einzelfall vom Wissen um die Art der Behinderung abhängen. In diesem Fall sei jedoch bei der Weigerung der Behinderten zur Vorlage des Feststellungsbescheides der ihm gegenüber bestehenden besonderen Fürsorge dadurch genüge getan, daß auf die mit der Nichtvorlage möglicherweise verbundenen Nachteile hingewiesen werde. Abschnitt IX Nr. 1 Satz 1 des Fürsorgeerlasses werde im Rahmen der nächsten Änderung dieser Bekanntmachung entsprechend neu gefaßt werden.

4.9.7. Personaldatenerhebung bei Trägern der Wohlfahrtspflege durch Kostenträger

In der Neufassung der Pflegesatzvereinbarung ist vorgesehen, daß die Träger der Wohlfahrtspflege eine Übersicht über den Personalaufwand der einzelnen Heime erstellen und diese den Kostenträgerverbänden übermitteln. Diese Übersicht enthält, zugeordnet zu einer laufenden Nummer über jeden Arbeitnehmer, u.a. Angaben über die Funktion, Vergütungsgruppe, Dienstalterstufe, Familienstand und Zahl der Kinder, Bruttojahreskosten sowie Honorare etc. Auch wenn in der Übersicht die Arbeitnehmer nicht namentlich genannt werden, bleiben die Angaben dennoch personenbezogen, da über die Funktionsbezeichnung Rückschlüsse auf die Person des betroffenen Arbeitnehmers gezogen werden können. Die vorgesehenen Datenerhebungen bzw. -übermittlungen habe ich daher, auf eine Eingabe hin, überprüft. Die in § 24 Abs. 1 BDSG genannten Voraussetzung der Erforderlichkeit zur Wahrung berechtigter Interessen eines Dritten habe ich in diesem Falle angesichts der den Trägern nach dem Bundessozialhilfegesetz und der Haushaltsordnung zukommenden Aufgaben als gegeben angenommen. Bei der Prüfung unter dem Gesichtspunkt der schutzwürdigen Belange des Betroffenen ergaben sich jedoch Bedenken gegenüber den geforderten Angaben zum Familienstand und zur Zahl der Kinder, da in besonderen Fällen (Scheidung, uneheliche Kinder ect.) sensitive Bereiche betroffen werden können. Gegen die Angabe der Bruttojahreskosten (Einkommen bzw. Honorare) habe ich keine Bedenken erhoben, soweit hierunter lediglich die dem Leistungsträger in Rechnung gestellten Beträge verstanden werden. Eine Überprüfung der Rechtsituation für öffentlich rechtlich organisierte Träger der Freien Wohlfahrtspflege nach Art. 17 Abs. 1 BayDSG kommt zum gleichen Ergebnis.

4.9.8. Veröffentlichung von Personaldaten im Handbuch eines Beamtenverbandes

Ein Beamtenverband bat mich um Äußerung zu der Frage, ob er von Personalverwaltungen Name, Vorname, Dienststellung und Dienststelle zum Zwecke der Veröffentlichung in einem Handbuch übermittelt erhalten könne. Hierfür sollten auch Angaben über Beamte übermittelt werden, die nicht Mitglieder des Verbandes sind, darunter auch über Beamte einer Laufbahngruppe, die in der Regel nicht Mitglied des Verbandes ist. Das Handbuch würde eine Veröffentlichung darstellen, die grundsätzlich für jedermann beziehbar wäre. Die Nutzung der Daten im Handbuch durch Interessenten außerhalb des Kreises der betroffenen Beamten mußte daher in die Beurteilung mit einbezogen werden. Außerdem war davon auszugehen, daß die Daten aus einer Personaldatei oder -kartei entnommen würden, so daß das BayDSG auf ihre Übermittlung anzuwenden ist. Ich habe mich zu der Anfrage wie folgt geäußert:

a) Beurteilung nach BayDSG:

Die Zulässigkeit der Übermittlung von Personaldaten durch eine personalverwaltende Dienststelle an den Verband zum Zwecke der Veröffentlichung ist zunächst nach Art. 18 Abs. 1 BayDSG zu beurteilen. Voraussetzung ist danach, daß der Empfänger ein berechtigtes Interesse an der Kenntnis der zu übermittelnden Daten glaubhaft macht und dadurch schutzwürdige Belange des Betroffenen nicht beeinträchtigt werden. Da es sich gleichzeitig um eine Auskunft über mehrere, vom Empfänger nicht namentlich bezeichneten Personen (Gruppenauskunft) handelt, ist die Personalbehörde gehalten, das Vorliegen eines „öffentlichen Interesses" an der Datenübermittlung zu prüfen (Nr. 18.2.4 VollzBekBayDSG). Das berechtigte Interesse des Verbandes an der Übermittlung der Daten zum Zwecke der Veröffentlichung kann unterstellt werden, da zu seinen Aufgaben mit Sicherheit auch die Herstellung von Transparenz im Personalangelegenheiten gehört. Dies konnte jedoch nicht ausschlaggebend sein, da nach der genannten Regelung der Vollzugsbekanntmachung an der vorgesehenen Gruppenauskunft auch ein öffentliches Interesse bestehen müßte. Es wäre Aufgabe der zuständigen Personaldienststelle dies zu begründen.

Zur Frage der Beeinträchtigung schutzwürdiger Belange Betroffener wies ich auf meine Erfahrungen aus einer Reihe von Beschwerden hin, die bei mir im Zusammenhang mit der Herausgabe eines entsprechenden Handbuchs durch einen Lehrerverband eingingen. Danach mußte ich davon ausgehen, daß durch die Veröffentlichung von Personaldaten in einem solchen Handbuch schutzwürdige Belange der betroffenen Personen durchaus beeinträchtigt werden können. Dies gilt z.B. für Beamte, die nicht Mitglieder des Verbandes sind, und möglicherweise besonders, wenn mehrere Berufsverbände bestehen, da nicht jeder Beamte mit den Zielen eines jeden Verbandes übereinstimmt. Ich hielt es daher für erforderlich, darauf Rücksicht zu nehmen, wenn Beamte in solchen Handbüchern mit personenbezogenen Daten nicht erscheinen wollten.

In der Satzung des genannten Lehrerverbandes war die Herausgabe des Handbuches vorgesehen, das Einzelangaben u.a. über Alter, Geburtstag, Ernennungs- und Beförderungsdatum, Prüfungsjahrgang, Amtsbezeichnung, Titel, Dienststelle, Funktion, Fächerverbindung und sonstige Tätigkeiten enthält. In Anbetracht dieses Datenumfangs ist von mir nach Art. 18 Abs. 1, Art. 4 Abs. 1 Nr. BayDSG die Einwilligung der Betroffenen in die Datenübermittlung zur Veröffentlichung als deren notwendige Voraussetzung angesehen worden. Dabei bin ich davon ausgegangen, daß die genannte Satzungsbestimmung die Einwilligung für Mitglieder des Verbandes ersetzt. Von Nichtmitgliedern des Verbandes werden schriftliche Einwilligungserklärungen Einzelner eingeholt. Dieses Verfahren hat die Regierung von Oberbayern als zuständige Datenschutzaufsichtsbehörde für den nichtöffentlichen Bereich gegenüber dem Verband so bestätigt. Grundsätzlich ebenso zu beurteilen wären Mitgliederverzeichnisse anderer Verbände, in denen relativ detaillierte Angaben, wie Anschriften, Geburtsdaten oder Angaben über berufliche Fachrichtungen der Betroffenen veröffentlicht würden. Bei Verbänden mit Zwangsmitgliedschaft wäre allerdings eine andere Ausgangslage gegeben.

Das Bayer. Staatsministerium des Innern vertritt als oberste Datenschutz-Aufsichtsbehörde für den nicht-öffentlichen Bereich zur Weitergabe von Mitglieder-Daten durch Vereine darüber hinaus die Ansicht, daß Vereine den einzelnen Vereinsmitgliedern in Zweifelsfällen Gelegenheit zum Widerspruch einräumen sollten.

Der Beamtenverband, zu dessen Anfrage Stellung zu nehmen war, beabsichtigte nun im Gegensatz zu den vorgenannten Veröffentlichungen lediglich im Schulbereich, Namen, Vornamen, Dienststellung und Dienststelle zu veröffentlichen. Es ist anzunehmen, daß eine Beeinträchtigung schutzwürdiger Belange der Betroffenen gegenüber den vorgenannten Fällen, in denen wesentlich detailliertere Angaben veröffentlicht werden, geringer ist. Eine völliger Ausschluß von Beeinträchtigungen kann aber nicht mit Sicherheit angenommen werden, zumal in erheblichen Umfange Daten von Nichtmitgliedern des Verbandes betroffen sind.

Denkbar wäre auch, daß dienstältere Beamte, die in herausgehobener Stellung tätig sind und einen größeren Bekanntheitsgrad genießen, gegen solche Veröffentlichungen seltener Bedenken haben als junge Kollegen. Dem entspricht im übrigen, daß der Öffentlichkeit, der das Buch auch zur Verfügung stehen würde, ein berechtigtes Interesse an der Kenntnisnahme personenbezogener Daten eher bei Beamten mit hervorgehobenen Tätigkeiten zuerkannt werden kann, als bei Kollegen mit weniger herausgehobene Tätigkeiten. Ich habe im übrigen in Fällen von örtlichen Behördenwegweisern, zu deren Zulässigkeit ich Stellung zu nehmen hatte, stets die Ansicht vertreten, daß Dienststellenleiter oder Leiter wichtiger Abteilungen (wie z.B. Kfz-Zulassungsstelle oder Meldeamt einer Stadt) eine Veröffentlichung ihres Namens hinnehmen müssen, weil sie eine herausgehobene öffentliche Funktion wahrnehmen. Der Veröffentlichung von Angaben über Mitarbeiter und Hilfskräfte der Verwaltung, die in Behördenwegweisern ohnehin in der Regel nicht sinnvoll ist, könnten dagegen eher Bedenken wegen möglicher Beeinträchtigung schutzwürdiger Belange entgegenstehen.

Um nun festzustellen, ob und inwieweit schutzwürdige Belange durch das Vorhaben des Verbandes beeinträchtigt werden können, halte ich es für erforderlich, allen

betroffenen Beamten Gelegenheit zu geben, von dem Vorhaben Kenntnis zu nehmen und der Veröffentlichung der eigenen Daten gegebenenfalls zu widersprechen. Wäre sichergestellt, daß jeder Betroffenen durch innerdienstliche Mitteilungen über die vorgesehene Datenübermittlung zum Zwecke der Veröffentlichung und über die Möglichkeit, dieser Übermittlung zu widersprechen, Kenntnis erlangte, so könnte meines Ermessens davon ausgegangen werden, daß die Veröffentlichung der vorgesehenen Daten derjenigen Betroffenen, die innerhalb einer angemessenen Frist keinen Widerspruch gegen die Datenübermittlung einlegen, schutzwürdige Belange nicht beeinträchtigt. Voraussetzung für das Abgehen vom Einwilligungserfordernis wäre meines Erachtens, daß tatsächlich jeder Betroffene zuverlässig von seiner Möglichkeit, der Veröffentlichung zu widersprechen, erführe. Mitteilungen am Schwarzen Brett, oder in der Staatszeitung würde ich hierfür nicht für ausreichend halten.

Eine Beeinträchtigung schutzwürdiger Belange könnte aber auch durch Nutzung der Kenntnis über Widersprüche durch die personalverwaltende Behörde für andere Zwecke, als die Abwicklung der Datenübermittlung an den Verband, eintreten. Im Verfahren müßte daher die ausschließlich zweckgebundene Nutzung dieser Kenntnis der personalverwaltenden Behörde durch entsprechende organisatorische Maßnahmen sichergestellt werden. Personalakten, -dateien oder -karteien dürften keinerlei Vermerke oder Hinweise auf das Widerspruchsverhalten der Beamten enthalten. Die Unterlagen über die Widersprüche müßten gesondert geführt werden. Übersichten über die Widersprechenden in jeder Zeit greifbarer und damit theoretisch auch für andere Zwekke nutzbarer Form dürften nicht geführt werden bzw., sobald es möglich ist, gelöscht bzw. vernichtet werden. Bei einer Neuauflage des Handbuches wäre – auch weil sich bis dahin die Zusammensetzung der Beamtenschaft geändert haben wird – erneut die Möglichkeit zum Widerspruch einzuräumen.

b) Rechtsprechung des Bundesverwaltungsgerichts:

Im Zusammenhang mit dem Antrag des Verbandes waren auch Anforderungen zu prüfen, die sich aus einer Entscheidung des Bundesverwaltungsgerichts zur Geheimhaltung von Personalunterlagen ergeben:

Auch unter dem Gesichtspunkt der Geheimhaltung von Personaldaten ist von der Stelle, die Daten zur Veröffentlichung abgibt, eine Abwägung der schutzwürdigen Interessen der Beamten an der Geheimhaltung von Daten mit einem schutzwürdigen Interesse der Allgemeinheit an ihrer Kenntnis unter Beachtung des Gebotes der Verhältnismäßigkeit vorzunehmen (BVerwG, DVBl 1971/143 ff). Das Interesse der Betroffenen kann beispielsweise darin bestehen, daß in ihrem privaten Bereich Ruhe und Sicherheit nicht gefährdet werden. Dem ist bei den Vorhaben des Verbandes zwar bis zu einem gewissen Grade dadurch Rechnung getragen, daß Privatanschriften nicht mitveröffentlicht werden sollen. Unter Beiziehung örtlicher Adreßbücher und gegebenenfalls Telefonbücher wird aber die Festlegung der Privatanschriften bei einer erheblichen Zahl von Betroffenen, aufgrund der Angabe der Dienststelle ohne weiteres möglich sein. Es muß bei der Beurteilung auch davon ausgegangen werden, daß vom gewerblichen Adreßhandel die Mühe, Privatadressen der Beamten festzustellen, nicht gescheut wird, da dadurch brauchbares Adreßmaterial hergestellt werden kann. Hierdurch entsteht aber auch Adreßmaterial für Störaktionen im privaten Lebensbereich der Beamten. Durch Störaktionen könnten auch deren Familien und dadurch die Beamten selbst über das dienstlich unvermeidbare Maß hinaus belästigt oder gar bedroht und gefährdet werden.

Die personalverwaltende Stelle wird daher für jeden Betroffenen prüfen müssen, ob dieser durch die Herausgabe der Daten – wegen der in den meisten Fällen gegebenen Möglichkeiten, Privatanschriften leicht festzustellen – gefährdet wird. Dabei kann m.E. nicht davon ausgegangen werden, daß diese Gefährdung ohnehin bereits durch die Tätigkeit oder aufgrund der Veröffentlichung von Beförderungen im Staatsanzeiger besteht. Die wirksame Durchführung abträglicher Aktionen gegenüber Beamten wird eventuell hieran interessierten Stellen durch derartiges Datenmaterial erheblich erleichtert (BVerwG a.a.O.). Der umfassende Überblick des Handbuchs ist mit gelegentlichen Veröffentlichungen im Staatsanzeiger nicht vergleichbar.

Hinzuweisen ist schließlich noch auf das Argument des Bundesverwaltungsgerichts, daß die Herausgabe der Daten (unter Berücksichtigung der überwiegend leichten Feststellbarkeit von Privatanschriften) auch für Stellen außerhalb der Bundesrepublik ein leicht zu handhabendes und möglicherweise besonders wirksames Mittel sein könnte, Beamte in der Bundesrepublik zu überwachen, etwaige Angehörige in anderen Staaten zu ermitteln und womöglich unter Druck zu setzen (BVerwG a.a.O.).

## 4.10. **Gesundheitsbereich**

### 4.10.1. Zu gesetzlichen Regelungen über personenbezogene Krankheitsregister

In Ergänzung der ausführlicheren Darstellung im fünften Tätigkeitsbericht (Nr. 4.2) ist über die Entwicklung auf diesem Gebiet folgendes zu berichten: Das Bayer. Staatsministerium des Innern hat im Zusammenhang mit einem außerbayerischen Regelungsvorhaben zur Forschungsdatenverarbeitung eine Stellungnahme abgegeben, deren wesentliche Aussage lautet:

„Zusammenfassend halten danach die bayerischen obersten Landesgesundheitsbehörden unbeschadet des Arztgeheimnisses (§ 203 Abs. 1 Nr. 1 StGB) zwar ebenfalls die Schaffung spezieller Rechtsgrundlagen für die Erfassung und Auswertung personenbezogener Krankheitsdaten zum Zweck der Krebsforschung für erforderlich. Sie können aber einen prinzipiellen Vorrang des Forschungsinteresses vor dem Persönlichkeitsrecht, wie ihn der Wissenschaftsrat in seiner Stellungnahme vom 5. November 1982 tendenziell behauptet, nicht anerkennen, denn nach ständiger Rechtsprechung des Bundesverfassungsgerichts stehen die Persönlichkeit des Bürgers (Art. 1 Abs. 1, Art. 2 Abs. 1 GG) und die Grundrechte aus Art. 5 GG gleichrangig nebeneinander, so daß es für staatliche Eingriffe in das Persönlichkeitsrecht des Bürgers in jedem Fall einer sorgfältigen Abwägung aller Umstände des Einzelfalles unter strikter Wahrung des Verhältnismäßigkeitsgrundsatzes bedarf (vgl. BVerfGE 30, 173, 195 ff.; 32, 373/378 ff.; 35, 202/220 ff.). Die

Zulassung der personenbezogenen Erfassung nicht übertragbarer Krankheiten (wie etwa Krebs) ist ein Eingriff in das grundrechtlich geschützte Selbstbestimmungsrecht des Patienten.

Aus den genannten Gründen haben die bayerischen obersten Landesgesundheitsbehörden in den erwähnten Stellungnahmen alle Bestrebungen abgelehnt, die in der Praxis auf eine personenbezogene Sammlung von Daten nicht übertragbarer Krankheiten ohne Wissen und Wollen der Betroffenen hinauslaufen würden. Ausgeschlossen ist damit zwar nicht, daß ausnahmsweise auch ohne Einwilligung von Betroffenen die Erfassung persönlicher Krankheitsdaten in verfassungskonformer Weise zugelassen werden kann, und zwar dann, wenn dem Betroffenen die zur Wirksamkeit seiner Einwilligung erforderliche Aufklärung in seinem gesundheitlichen Interesse objektiv nicht zumutbar ist. Nur muß dann verhindert werden, daß eine solche Ausnahmeklausel in der Praxis als Alibi benutzt und die Weitergabe personenbezogener medizinischer Daten so zum praktischen Regelfall wird. Keinesfalls halten wir es als verfassungsrechtlich für vertretbar, sich hinsichtlich der Frage der Einwilligungsbedürftigkeit allein an den Belangen der Forschung zu orientieren...."

Die Konferenz der für das Gesundheitswesen zuständigen Minister und Senatoren der Länder hat am 17./18. November 1983 eine Entschließung zum Thema „Krebsregister" gefaßt, in der sie von Bund und Ländern gemeinsam aufgestellte Thesen zur Errichtung regionaler Krebsregister zur Kenntnis nahm und diese als eine geeignete Grundlage für die Errichtung von regionalen Krebsregistern nach einheitlichen Kriterien bezeichnete. Sie empfahl jenen Ländern, die ein regionales Krebsregister einrichten wollen, die in den Thesen festgelegten Grundsätze zu berücksichtigen.

Die Thesen enthalten aus der Sicht des Datenschutzes wichtige Aussagen: So wird zum Auf- und Ausbau regionaler Krebsregister und zur wissenschaftlichen Auswertung der dort erfaßten Daten die Schaffung rechtlicher Voraussetzungen als nötig erachtet; dies gelte auch für auszubauende Klinikregister; Grundsatz solle die namentliche Meldung nur mit Einwilligung des Patienten sein, die Voraussetzungen für Ausnahmen seien im Rahmen entsprechender gesetzlicher Regelungen genau zu definieren; dem Patienten sei eine vorsorgliche Einspruchsmöglichkeit einzuräumen, die bis zu ihrem Widerruf zu beachten sei; eine möglichst frühzeitige Anonymisierung der personenbezogenen Daten müsse sichergestellt werden; für etwaige Abgleiche zur Aktualisierung von Anschriften der Patienten müßten entsprechende rechtliche Voraussetzungen vorhanden sein bzw. geschaffen werden; die Voraussetzungen für die Abgabe anonymisierter Daten für wissenschaftliche Zwecke sei festzulegen. Die Abgabe personenbezogener Daten müsse auf Zwecke der Krebsforschung und unter besonderen Vorkehrungen beschränkt werden; die gesetzliche Regelung müsse auch eine etwaige Befragung des Patienten oder von Dritten regeln; schließlich sei die Auskunft aus dem Register zu regeln und die Erteilung von Negativattesten auszuschließen.

Eine Erörterung dieser Thesen durch die Datenschutzbeauftragten ist bisher nicht erfolgt. Zunächst bleibt die Erstellung eventueller Gesetzentwürfe abzuwarten. Die Datenschutzbeauftragten gehen davon aus, daß ihre bisherigen Äußerungen zu Krebsregistern bzw. zur Einrichtung klinischer Krebsdokumentationen hierbei Berücksichtigung finden (s.u. und Anlage Nr. 7 zu diesem Bericht).

4.10.2. Klinische Krebsdokumentation

Die Datenschutzbeauftragten der Länder und des Bundes hatten sich im Berichtsjahr mit Datenschutzfragen auseinandergesetzt, die durch – öffentliche geförderte – Projekte für klinische Krebsdokumentationen ausgelöst wurden. Wesentliche Punkte waren die Klarstellung der Verantwortlichkeit für die Einhaltung der Vorschriften des Datenschutzes, also der „speichernden Stelle", die Definition von Inhalt, Umfang, Übermittlungs- und Speicherungsdauer von Daten aus der Krebsbehandlung und -nachsorge, die Aufklärung des Patienten über die Speicherung seiner Daten, die Nutzung solcher Daten über den Behandlungszusammenhang hinaus aufgrund eines „informed consent", sowie die Erforderlichkeit strenger technischer und organisatorischer Datensicherungsmaßnahmen. Die Erörterung hat in einem gemeinsamen Beschluß der Datenschutzbeauftragten ihren Niederschlag gefunden. Dieser ist unter Nr. 7 im Anhang abgedruckt.

4.10.3. Weitergabe von Patientendaten: Anonymisierung/ Einwilligung

Bei einem Forschungsprojekt, das die Weitergabe von Patientendaten durch ein Krankenhaus an eine privatrechtlich organisierte Forschungsgesellschaft vorsah, war zu prüfen, ob die zur Weitergabe vorgesehenen Patientendaten hinreichend anonymisiert waren. Die Forschungsgesellschaft hatte dazu Fragebögen mit einem „anonymisierten medizinischen Teil" vorgelegt, der vom Krankenhaus an sie übermittelt werden sollte. Ich habe demgegenüber die Meinung vertreten, daß es in Einzelfällen beim Datenempfänger wohl möglich wäre, mit Hilfe der erhobenen Daten die betroffenen Patienten auch ohne Kenntnis des „personenbezogenen Teils", der unter anderem Namen und Anschrift der Patienten enthielt, und der nicht übermittelt werden sollte, zu identifizieren. Die nach Ansicht der Forschungsgesellschaft anonymisierten Erhebungsbögen enthielten unter anderem folgende Angaben: Geburtsdatum (Monat/Jahr), Geschlecht, Familienstand, Wohnsitz (Kreis), Berufsschlüssel, Schulbildung, Krankenhaus-Aufnahme-Datum, Krankenhaus-Entlassungs-Datum, ggf. Todesdatum. Die Kombination dieser Angaben könnte es meiner Ansicht nach in manchen Fällen, insbesondere bei Angehörigen seltener oder herausgehobener Berufsgruppen ermöglichen, den Betroffenen zu bestimmen ohne daß es dazu eines unverhältnismäßigen Aufwandes bedürfte. Der beim Krankenhaus verbleibende „personenbezogene Teil" und der weiterzugebende Teil sollten dabei dieselbe Dokumentationsnummer tragen, um Änderungsdaten dem Bestand beim Empfänger zuordnen zu können. Der Personenbezug dieser Dokumentationsnummer wäre nur dem abgebenden Krankenhaus bekannt. Nach Ziff. 5.1.5 der Vollzugsbekanntmachung zum Bayer. Datenschutzgesetz gelten aber unter einem Schlüssel geführte Daten zu einer Person (hier Fallnummer, Bogennummer) als noch personenbezogen, unabhängig davon, ob die speichernde Stelle den Schlüssel kennt, oder auf andere Weise seine Entschlüsselung durchführen kann. Zu berücksichtigen war schließlich im vorliegenden Fall, daß die erhobenen Daten hohen Vertraulichkeitsgrad besitzen: Herzinfarkt, frühere Krankheiten, Grund der Berentung, körperlicher Zustand nach der Entlassung, ggf. Todesursache. Es mußte daher eine zuverlässige, dabei praktikable Lösung gefunden werden.

Die Forschungsgesellschaft hatte vorgesehen, eine Einverständniserklärung der Patienten mit dem Hinweis einzuholen, daß die erhobenen Daten „nur in anonymisierter Form" an das Institut zur Auswertung weitergegeben würden. Da nach der Rechtsprechung eine Einwilligung nur dann rechtswirksam erteilt wird, wenn der Einwilligende Wesen, Bedeutung und Tragweite seiner Entscheidung voll zu erfassen imstande ist, war eine solche Einverständniserklärung als problematisch anzusehen, weil der Betroffene durch das Wort „anonymisiert" über die tatsächliche Situation im Unklaren gelassen worden wäre. Ich habe daher vorgeschlagen, auf die Bewertung „anonymisiert" in der Einwilligungserklärung zu verzichten und klar mitzuteilen, daß medizinische Daten lediglich ohne Namen und Anschriften, aber mit einer Dokumentationsnummer, deren Personenbezug nur dem abgebenden Krankenhaus bekannt ist, an das Institut zur Auswertung weitergegeben werden.

Die Forschungsgesellschaft hat daraufhin die Einwillungserklärung entsprechend abgefaßt.

4.10.4. Patientenstrukturanalyse bei Bezirkskrankenhäusern

Wie ich erfuhr, war vorgesehen, daß eine Gesellschaft (GmbH) eine Patientenstrukturanalyse in bayerischen Bezirkskrankenhäusern durchführt. Dabei sollten mit Hilfe von Fragebögen die näheren Umstände des Krankenhausaufenthalts der einzelnen Patienten erhoben werden.

Hierzu habe ich darauf hingewiesen, daß nach Art. 13 Abs. 5 BayKrG die Weitergabe von Patientendaten durch das Krankenhaus, sofern der Patient dadurch identifiziert werden kann, nur zulässig ist, wenn der Patient zustimmt. Das Zustimmungserfordernis entfällt also, wenn der Patient durch die Weitergabe nicht identifiziert werden kann. Der für die Erhebung vorgesehene Fragebogen enthielt zwar keine Angaben über Namen oder Anschrift der betroffenen Patienten. Die erhobenen Daten gelten aber auch dann noch als personenbezogen, wenn die Person durch Angaben unter Zuhilfenahme zusätzlicher Informationen identifiziert werden kann. Entscheidend ist dabei, ob der Datenempfänger die Person, auf die sich die Daten beziehen, mit einem verhältnismäßigen und im Rahmen seiner Möglichkeiten liegenden Aufwand bestimmen kann.

Der im Fragebogen erhobene Ortsname des Patientenwohnorts würde insbesondere bei Kleingemeinden die Identifizierung des Patienten erleichtern; er war nach meinem Kenntnisstand auch nicht unbedingt erforderlich, da die ebenfalls erhobene Postleitzahl eine wohl ausreichende regionale Zuordnung ermöglichte. Die Speicherung der chiffrierten laufenden Patientennummer bei der auswertenden Gesellschaft war auf den unbedingt erforderlichen Zeitraum zu beschränken. Spätestens nach der Plausibilitätsprüfung der erfaßten Fälle müßten die Patientennummern gelöscht und die Fragebogen an die beteiligten Bezirkskrankenhäuser zurückgesandt werden. Von einer Speicherung der Patientennummer in der bereinigten Datei war also abzusehen. Zu klären war außerdem die Frage nach dem Löschungszeitpunkt bzw. dem Verbleib der gespeicherten Daten nach Abschluß der Auswertung.

Die Forderung nach ausreichender Anonymisierung der Patientendaten muß selbstverständlich auch für die Veröffentlichung der Untersuchungsergebnisse gelten.

Ich habe den Verband der Bayerischen Bezirke von meiner Beurteilung unterrichtet. Der Auftrag an die Gesellschaft wurde daraufhin entsprechend gestaltet.

4.10.5. Abgabe von Krankengeschichten an das Städtische Archiv

Auf Anfrage einer Krankenhausstiftung habe ich mich zur Zulässigkeit der Abgabe von Krankengeschichten an ein städtisches Archiv folgendermaßen geäußert:

Die Abgabe von Krankenunterlagen durch ein Krankenhaus an ein Archiv stellt eine Offenbarung von Patientendaten im Sinne des Art. 13 Bayer. Krankenhausgesetz (BayKrG) dar. Eine solche Offenbarung ist nach Art. 13 Abs. 5 BayKrG nur zulässig, wenn der Patient zustimmt und kein überwiegendes öffentliches Interesse entgegensteht. Das Zustimmungserfordernis entfällt, wenn der Patient durch die Weitergabe nicht identifiziert werden kann. Nach Art. 13 Abs. 8 BayKRG bleiben die sich aus anderen Vorschriften ergebenden Schweige- und Auskunftspflichten unberührt. Eine solche Schweigepflicht ist in § 203 Abs. 1 und 3 StGB vorgesehen. Dies ist für ärztliche Unterlagen aus dem Krankenhausbereich ebenfalls zu berücksichtigen. Die Rechtsprechung zu § 203 StGB läßt erkennen, daß eine Befugnis zum Offenbaren von Daten, die der ärztlichen Schweigepflicht unterliegen, im vorliegenden Fall nur angenommen werden kann, wenn eine ausdrückliche Zustimmung des Betroffenen – etwa ausgesprochen noch vor seinem Tode – vorliegt. Dabei ist zu beachten, daß nach § 203 Abs. 4 StGB eine unbefugte Offenbarung fremder Geheimnisse auch nach dem Tode des Betroffenen strafbedroht ist.

Eine Befugnis kann sich auch aufgrund besonderer Gesetze ergeben. Eine ausdrückliche gesetzliche Befugnis liegt derzeit für die Abgabe von Krankenunterlagen an Archive jedoch nicht vor. Sie könnte evtl. durch ein künftiges Archivgesetz geschaffen werden. In Bayern ist mit Vorbereitungen für eine Archivgesetz begonnen worden (siehe Nr. 4.13 dieses Tätigkeitsberichts).

Die gegenwärtige Rechtslage hat zur Folge, daß Krankenunterlagen an Archive meines Erachtens nur dann abgegeben werden dürften, wenn entweder die Betroffenen in die Weitergabe eingewilligt haben, oder die Krankenunterlagen durch Löschung der identifizierenden Angaben so aufbereitet sind, daß der Betroffene nicht mehr bestimmbar ist. Dies wird jedoch aus Praktikabilitätsgründen kaum in Frage kommen.

Soweit aus Raumgründen eine Entscheidung unaufschiebbar wurde, habe ich keine datenschutzrechtlichen Bedenken erhoben, wenn vorhandene Krankenunterlagen in den Räumen von Archiven nur eingelagert würden. Dies bedeutet, daß das abgebende Krankenhaus in diesen Fällen allein verfügungsberechtigt bliebe und weder das Personal des Archivs noch andere Personen oder Stellen Zugang erhielten. Durch besondere Schutzvorkehrungen technischer und organisatorischer Art in den Räumen des Archivs wäre sicherzustellen, daß auf die Patientendaten nicht unberechtigt zugegriffen werden könnte.

4.10.6. Gesundheitsfragebogen

Im 5. Tätigkeitsbericht wurde über die Entwicklung eines neuen allgemeinen Gesundheitsfragebogens anläßlich von Schuluntersuchungen berichtet (Nr. 4.11.6, S. 44). Ich hatte seinerzeit darauf hingewiesen, daß das früher verwendete

Formular Fragen enthielt, die sehr stark in die Privatsphäre der Eltern eindrangen, wie mit Fragen nach Risikoschwangerschaft und Auffälligkeiten bei der Geburt. Das zuständige Staatsministerium für Arbeit und Sozialordnung hat dazu mitgeteilt, daß der Datenumfang in dem Elternfragebogen dem schulärztlichen Auftrag aus Art. 57 des bayerischen Gesetzes über das Erziehungs- und Unterrichtswesen, eine exakte Diagnose und eine gesundheitliche Schulprognose zu stellen, entspräche. Bei äußerlich meist gesund erscheinenden Kindern bestehe nicht selten eine körperliche Leistungsschwäche, ohne daß der objektive Befund Abweichungen von der Norm erkennen ließe. Für den Schularzt habe daher die Krankheitsvorgeschichte des Kindes eine ebenso große Bedeutung wie die Befunderhebung. Wichtige Punkte der Krankheitsvorgeschichte seien der Schwangerschaftsverlauf, die Geburt, das Geburtsgewicht und die ersten Stunden nach der Geburt. Sie seien bei Schuluntersuchungen – wie z.B. auch erlittene Infektionskrankheiten, die bisherige psychosomatische Entwicklung oder die Umwelt des Kindes – recht entscheidende Faktoren für die gesamte Beurteilung; sie könnten stichhaltige Hinweise darüber geben, was dem betreffenden Kind unter Berücksichtigung seiner konstitutions- und umweltgebundenen Gesundheit zugemutet werden könne. Deshalb werde die Auffassung vertreten, daß gezielte Krankheitsvorgeschichten auch zur schulärztlichen Untersuchung gehören, weil sie den Einzelfall besser erklären könnten.

Gegen diese Auffassung habe ich aus der Sicht des Datenschutzes keine Bedenken erhoben. Auf meine Bitte wurde jedoch in den endgültigen Formularen noch vorgesehen, daß eine Rückmeldung an den Schularzt durch den Arzt, der aufgrund eines Hinweises des Schularztes zur Behandlung oder Untersuchung aufgesucht wird, mit dem Einverständnis der Erziehungsberechtigten erfolgt.

Die Neuregelung der Schulgesundheitspflege durch Gem. Bek. v. 12.10.83 ist im MABl 1983, S. 825 veröffentlicht worden.

4.10.7. Umfang ärztlicher Gutachten bei der Aufnahme in Alters- und Pflegeheime

Im Zusammenhang mit der Kostenübernahme einer Heimunterbringung durch einen Sozialleistungsträger war aufgrund einer Eingabe dazu Stellung zu nehmen, welche Fragestellungen an den begutachtenden Arzt aus fachlicher Sicht für die Aufnahme in Alters- oder Pflegeheime erforderlich sind. Bei der Bewertung des Sachverhalts gehe ich davon aus, daß die Weitergabe des ärztlichen Gutachtens an ein Alters- oder Pflegeheim nach den Regeln der ärztlichen Schweigepflicht nur mit Einwilligung des Betroffenen erfolgen kann. Damit richtet sich auch der Umfang des Gutachtens nach der Einwilligung des Betroffenen. Die Heime fordern zur Ergänzung des Aufnahmeantrags ärztliche Gutachten unterschiedlichen Umfangs an. In vielen Fällen lassen aber die örtlichen, sachlichen und persönlichen Verhältnisse des Betroffenen eine freie Auswahl der Unterbringung zwischen Heimen nicht zu. Auf das in der Regel privatrechtliche Verhältnis zum Heim ist § 23 BDSG anzuwenden (bei Heimen bayerischer öffentlicher Träger im Rahmen von Art. 22 BayDSG). In § 23 BDSG findet auch der Grundsatz des Übermaßverbots im Rahmen des Persönlichkeitsschutzes Ausdruck. Die Zulässigkeit einer Datenspeicherung hängt danach davon ab, ob sie sich im Rahmen der Zweckbestimmung des Vertrags bzw. des Vertragsverhältnisses hält. Datenspeicherungen, die diesen Rahmen sprengen, wären unzulässig, die Erhebung solcher Daten unverhältnismäßig. Im Rahmen des Verhältnismäßigkeitsgrundsatzes sollten daher die Angaben aus ärztlicher Sicht über den Betroffenen auf den unbedingt erforderlichen Umfang begrenzt werden. In Ausnahmefällen können auch umfangreichere Gutachten im Hinblick auf besondere pflegerische Maßnahmen erforderlich sein.

Diese Überlegungen habe ich dem Bayer. Staatsministerium für Arbeit und Sozialordnung mitgeteilt. In seiner Stellungnahme geht das Ministerium davon aus, daß in jedem konkreten Einzelfall unter Beachtung der Grundsätze von Treu und Glauben und der Verhältnismäßigkeit über den Umfang der unbedingt notwendigen Auskünfte zu entscheiden sei. Aus fachlicher Sicht seien Art und Umfang der Fragestellungen an den begutachtenden Arzt von besonderer Bedeutung, da sie primär über die Aufnahme in die Alten-, oder aber in die Pflegeabteilung eines Alten- und Pflegeheimes entscheiden. Die Fragen müssen deshalb auf die Hilfs- oder Pflegebedürftigkeit abzielen und darüber hinaus auch ausreichende Informationen über bestimmte Leiden zulassen, um möglichen, plötzlichen Komplikationen ohne Verzögerungen und gezielt begegnen zu können.

4.10.8. Namensangaben auf Überweisungsträgern für die Gutachtenvergütung von Ärzten von Nervenkrankenhäusern

Aus dem ärztlichen Bereich erfuhr ich, daß im Zuge der Überweisung der Gutachtensvergütung für die Ärzte von Bezirkskrankenhäusern im Rahmen von Gutachten für Sozialgerichte die Gerichtskasse auf dem Überweisungsträger den Namen des Patienten vermerkt. Gleiches gilt für Erstattung von Rentengutachten für die Landesversicherungsanstalten. Bei dieser Verfahrensweise erfährt das angewiesene Geldinstitut, ob ein bestimmter, namentlich benannter Betroffener durch einen Nervenarzt untersucht wurde. Auch die Ärzte der Bezirkskrankenhäuser sahen in dieser Sachbehandlung eine aus ihrer Sicht nicht erforderliche Gefährdung des persönlichen Bereichs des Betroffenen. Ich habe die Bayerischen Staatsministerien der Justiz und für Arbeit und Sozialordnung hiervon unterrichtet und gebeten, mich in dem Bemühen zu unterstützen, hier eine unnötige Kenntnisnahme Dritter zu verhindern.

Das Staatsministerium für Arbeit und Sozialordnung hat sich bereit erklärt, die Bedenken auszuräumen und Sozialgerichte, Sozialversicherungsträger und Behörden der Versorgungsverwaltung entsprechend zu unterrichten. Es ist nunmehr vorgesehen, nicht nur im Falle von Gutachten von Nervenärzten, sondern auch bei Untersuchungen durch andere Ärzte den Namen des Betroffenen bei der Überweisung der Gutachtensvergütung auf dem Überweisungsträger einheitlich durch ein Aktenzeichen oder eine Aufnahmenummer zu ersetzen.

Auch das Staatsministerium der Justiz hat sich die Bedenken zueigen gemacht und die Gerichte und Staatsanwaltschaften gebeten, die Verwendung des Namens des Betroffenen zu vermeiden und stattdessen nur Rechnungsdatum und -nummer oder Geschäftsnummer bzw. nicht personenbezogene Bezugsdaten zu verwenden.

4.10.9. Weitergabe von Daten über Krankenhauspatienten an den Oberbürgermeister

Auf Anfrage einer Stadt war zu prüfen, ob der Oberbürgermeister für Genesungswünsche die Namen hervorgehobe-

ner Personen, die Patienten des Städtischen Krankenhauses waren, erfahren dürfte. Aufgrund Art. 13 Abs. 5 des Bayerischen Krankenhausgesetzes sowie unter Hinweis auf § 203 Abs. 1 Nr. 1 StGB habe ich darauf hingewiesen, daß, auch wenn es sich ausschließlich um Persönlichkeiten des öffentlichen Lebens handeln würde, die Weitergabe personenbezogener Daten über Patienten von deren Einwilligung abhängt.

## 4.11. **Sozialbereich**

### 4.11.1. Offenbarung von Angaben über Klienten einer Sozialbehörde an Studenten einer Fachhochschule – Fachrichtung Sozialwesen

Von einem Landratsamt bin ich um Stellungnahme zu der Frage gebeten worden, ob den Studenten einer Fachhochschule – Fachrichtung Sozialwesen – Angaben über Klienten von Sozialleistungsträgern offenbart werden dürfen. Ich habe dazu das Bayerische Staatsministerium für Arbeit und Sozialordnung um eine Äußerung gebeten und dabei folgende Ansicht zum Sachverhalt vertreten: Unter dem Gesichtspunkt des Datenschutzes ist meines Erachtens von wesentlicher Bedeutung, welche Stellung der Studierende im Ausbildungsamt einnimmt. Unterliegt er im Rahmen eines Ausbildungsvertrages den Weisungen der Ausbildungsstelle und wird er darüber hinaus fallweise in der Klientenbetreuung tätig, so stehen meiner Ansicht nach die Bestimmungen zum Schutz der Sozialdaten nach dem X. Buch zum Sozialgesetzbuch einer Kenntnisnahme der erforderlichen personenbezogenen Daten nicht im Wege. Die Pflicht zur Wahrung des Sozialgeheimnisses nach § 35 Abs. 1 SGB I verbietet es allerdings, dem Studierenden unbeschränkten Zugang zu allen vorhandenen Akten und Dateien zu gewähren. Er ist insoweit wohl einem Bediensteten der Ausbildungsstelle gleichgestellt, der den berechtigten Zugang zu Unterlagen nur im Rahmen seiner Aufgabenzuweisung erhält. Als Rechtsgrundlage für eine solche Einordnung des Studierenden kommt die Rahmenstudienordnung für den Fachhochschulstudiengang Sozialwesen vom 20.1.1981 (KMBl I Nr. 4/1981, S. 104) in Betracht. Anlage 2 dieser Bestimmungen enthält den Ausbildungsplan für die praktischen Studiensemester des Fachhochschulstudiengangs Sozialwesen. Nach dem dort beschriebenen Ausbildungsinhalt lernen und üben die Studenten berufliches Handeln durch Beteiligung am Arbeitsablauf der Ausbildungsstelle entsprechend deren Arbeitsfeld und Aufgaben. Als Ausbildungsziel ist u.a. die Fähigkeit und Bereitschaft genannt, Aufgaben und Verantwortung an der Ausbildungsstelle zu übernehmen. Dies erscheint ohne enge Einbindung des Studierenden in die Ausbildungsbehörde nicht möglich. Als Folge dieser Einbindung ist eine förmliche Verpflichtung der Studierenden nach dem Verpflichtungsgesetz, gegebenenfalls nach dem BDSG vorzunehmen.

Nach dem Ausbildungsplan soll der Ausbildungsbeauftragte der Ausbildungsstelle in der Regel Sozialarbeiter/Sozialpädagoge sein. Ist beabsichtigt, praktische Fälle aus dem Tätigkeitsbereich des Ausbilders dem Studierenden zu offenbaren, so ist in solchen Fällen neben den Bestimmungen zum Schutz der Sozialdaten nach dem X. Buch zum Sozialgesetzbuch auch § 203 StGB in die Überlegungen mit einzubeziehen. Die besondere persönliche berufliche Verschwiegenheitspflicht für staatlich anerkannte Sozialarbeiter oder staatlich anerkannte Sozialpädagogen, auf die § 203 Abs. 1 Nr. 5 StGB Bezug nimmt, gilt auch im innerbehördlichen Bereich. Der Studierende steht nach § 203 Abs. 3 StGB den Vorgenannten gleich. Dies rechtfertigt für sich allein aber noch nicht die Annahme, daß die betroffenen Klienten mutmaßlich oder konkludent in eine Offenbarung ihrer Daten an den Studierenden einwilligen. Daher werden Daten, die den Sozialarbeitern bzw. Sozialpädagogen im Rahmen ihrer Tätigkeit bekannt geworden sind, in aller Regeln nicht ohne Zustimmung der betroffenen Klienten an Studierende offenbart werden dürfen. Eine andere Beurteilung ist m.E. nur möglich, wenn der Studierende unmittelbar in dem betreffenden Fall als Bearbeiter tätig geworden ist.

Eine Weitergabe von personenbezogenen Unterlagen an Ausbildungskräfte der Studenten, die nicht im Ausbildungsamt beschäftigt sind (z.B. Supervisoren), begegnet in allen Fällen datenschutzrechtliche Bedenken. Das Bayerische Staatsministerium für Arbeit und Sozialordnung hat sich dieser Auffassung im wesentlichen angeschlossen.

Offen ist derzeit noch die Frage, ob die fachpraktische Ausbildung von Fachoberschülern der Ausbildungsrichtung Wirtschaft, Verwaltung und Rechtspflege datenschutzrechtlich vergleichbar eingeordnet werden kann. Nach meiner Kenntnis fehlt hier eine Ausbildungsordnung mit Rechtnormqualität. Darüberhinaus ist wohl auch die Tätigkeit und das Ausbildungsziel der Praktikanten anders zu bewerten als bei den Studenten der Fachhochschule. Eine Stellungnahme des Bayerischen Staatsministeriums für Unterricht und Kultus zu dieser Frage steht noch aus.

### 4.11.2. Vordrucke zur Prüfung des „mißglückten Arbeitsversuches"

Nach meinen Feststellungen verwenden die einzelnen gesetzlichen Krankenkassen verschiedenartige Vordrucke zur Prüfung des „mißglückten Arbeitsversuches" eines Arbeitnehmers. Diese Prüfung ist in bestimmten Fällen zur Feststellung erforderlich, ob ein versicherungspflichtiges Beschäftigungsverhältnis vorliegt.

Die dabei vorgesehenen Fragestellungen sind zum Teil mißverständlich. Ein befragter Arbeitgeber hat mich z.B. auf eine Formulierung hingewiesen („War in der Arbeitsleistung des Beschäftigten ein merkbarer Unterschied im Vergleich zu anderen, gleichartigen Beschäftigten festzustellen?"), die als Aufforderung zur qualitativen Bewertung des Arbeitnehmers im Sinne eines Arbeitszeugnisses mißverstanden werden könnte. An anderer Stelle wird der in solchen Fragen unzuständige Arbeitgeber um Angabe von Krankheiten und Krankheitserscheinungen des Arbeitnehmers befragt.

Aufgrund dieser und anderer Fragestellungen in den mir nur in wenigen Beispielen vorliegenden Fragebogen habe ich dem Landesverband der Ortskrankenkasse vorgeschlagen, den Gesamtkomplex „Fragebogen zur Prüfung des mißglückten Arbeitsversuches" unter Berücksichtigung der neueren Rechtsprechung des Bundessozialgerichts, der Mitwirkungspflichten nach § 60 SGB I und der einschlägigen Datenschutzbestimmungen zu überarbeiten und das Ergebnis den beteiligten Krankenkassen zur Verwendung zu empfehlen.

Der Landesverband der Ortskrankenkassen hat mitgeteilt, daß nach Beratung im zuständigen Fachausschuß nunmehr die Auffassung vertreten wird, daß nach der gefestigten Rechtssprechung des Bundessozialgerichts für die Prüfung

eines „mißglückten Arbeitsversuchs" in erster Linie die im Zeitpunkt der Arbeitsaufnahme bestehende Arbeitsunfähigkeit des Beschäftigten maßgebend ist und deshalb auf das Befragen des Arbeitgebers bzw. des Arbeitnehmers weitgehend verzichtet werden kann. Aus diesem Grunde sollte nach Meinung des Fachausschusses von dem bisherigen Verfahren abgegangen werden. Künftig sollten zunächst nur Maßnahmen zur Prüfung der Arbeitsunfähigkeit ergriffen werden. Da die genannten Fragebogen jedoch bundesweit Verwendung finden, ist noch eine Erörterung mit den Spitzenverbänden der Krankenkassen erforderlich. Ein Ergebnis steht noch aus.

4.11.3. Weitergabe von Kassenarztverzeichnissen

Die Kassenärztliche Vereinigung Bayerns hat mir gegenüber die Rechtsauffassung vertreten, daß sich eine Datenoffenbarung aus dem Arztverzeichnis der Kassenärztlichen Vereinigung nach § 35 SGB I, §§ 67 ff SGB X richte. Hiernach haben auch die Kassenärzte Anspruch darauf, daß Einzelangaben über ihre persönlichen und sachlichen Verhältnisse von der Kassenärztlichen Vereinigung als Sozialgeheimnis gewahrt und nicht unbefugt offenbart werden. Die Weitergabe von Arztverzeichnissen an die gesetzlichen Krankenkassen sei gemäß § 69 Abs 1 Nr. 1 SGB X zulässig. Die Weitergabe des Kassenarztverzeichnisses an Kassenärzte sei zur Erfüllung des Sicherstellungsauftrages der Kassenärztlichen Vereinigung aus den §§ 368, 368 n RVO erforderlich, damit die Kassenärzte mit den an der kassenärztlichen Versorgung beteiligten Kollegen und Einrichtungen bei der Durchführung der ambulanten Behandlung der Versicherten zusammenwirken können. Da die Offenbarung gemäß § 69 Abs. 1 Nr. 1 SGB X aber nur im Rahmen der Erforderlichkeit zur Aufgabenerfüllung zulässig sei, könnten die Kassenärzte das Kassenarztverzeichnis jeweils nur für den Bereich ihrer Bezirksstelle, nicht aber mit den Angaben über alle Kollegen bzw. Einrichtungen in Bayern erhalten. Außerdem vertrat die KV die Auffassung, daß die Weitergabe von Arztadressen an Privatpersonen (z.B. Firmen, ärztliche Verbände) nicht mit der Erfüllung gesetzlicher Aufgaben im Sinne des § 69 Abs. 1 Nr. 1 SGB X in Zusammenhang gebracht werden könne.

Das Bayerischen Staatsministerium für Arbeit und Sozialordnung hat mir in einem Schreiben mitgeteilt, daß die Rechtsansicht der Kassenärztlichen Vereinigung Bayerns nicht zu beanstanden sei. Auch ich habe diese Auffassung nicht beanstandet. Zu beanstanden war jedoch, daß die Kassenärztliche Vereinigung Bayerns die Praxis der Weitergabe von Kassenarztverzeichnissen erst mit Beschluß vom 26.3.1983 änderte. Sie hatte nach dem Inkrafttreten des SGB am 1.1.1981 zunächst noch bis April 1983 in den Bezirksstellen Kassenarztverzeichnisse an alle Interessenten (darunter ärztliche Verbände, Pharmaindustrie) abgegeben.

Ich gehe im übrigen davon aus, daß neben der Überlassung der Kassenarztverzeichnisse an Kassenärzte bzw. gesetzliche Krankenkassen weitere Möglichkeiten einer Offenbarung von Arztdaten in Form dieses Verzeichnisses im Rahmen der gesetzlichen Aufgabenerfüllung gemäß § 69 Abs. 1 Nr. 1 SGB X bestehen können. Bei einem Offenbarungsersuchen solcher Art wäre im Einzelfall zu prüfen, ob die erbetene Offenbarung von Arztanschriften zur Sicherstellung der ärztlichen Versorgung in dem in § 368 Abs. 2 RVO bezeichneten Umfang erforderlich ist, einschließlich der Prüfung, ob regionale Begrenzungen zum gewünschten Ergebnis führen. Die bisher von der Kassenärztlichen Vereinigung geltend gemachte Unzulässigkeit der Offenbarung von Arztanschriften an Krankenhäuser oder Universitäts-Polikliniken muß meines Erachtens überdacht werden. Ein Ergebnis dieser Überlegungen steht noch aus. Das Bayerische Staatsministerium für Arbeit und Sozialordnung wurde in diese Überlegungen eingeschaltet.

4.11.4. Umfang der Ausnahmeregelung nach § 76 Abs. 2 SGB X

Die Sozialleistungsträger, insbesondere die Träger der gesetzlichen Kranken-, Unfall- und Rentenversicherung benötigen für Entscheidungen über Leistungsanträge häufig Angaben über die gesundheitlichen Verhältnisse des Antragstellers aus der Vergangenheit. Sie ersuchen sich deshalb gegenseitig um Offenbarung der behandelnden Ärzte, der Krankheitszeiten und der Diagnosen für einen bestimmten Zeitraum. In diesem Zusammenhang hat eine Ortskrankenkasse bei mir angefragt, welche medizinischen Daten im Rahmen der erleichterten Offenbarungsbefugnis nach § 76 Abs. 2 SGB X an andere Sozialleistungsträger weitergegeben werden können.

In meiner Stellungnahme habe ich die Auffassung unterstützt, daß es nicht Sinn und Zweck der Regelung nach § 76 Abs. 2 SBG X sein kann, jede Datenbewegung mit medizinischen Daten zwischen den Sozialleistungsträgern und zu den Gerichten von einer Einwilligung des Betroffenen abhängig zu machen bzw. mehrere ärztliche Untersuchungen durchführen zu müssen. Dies entspräche auch nicht dem Grundgedanken des § 96 SGB X.

Ich habe daher keine Bedenken, Daten, die bei ärztlichen Untersuchungen im Sinne des § 96 SGB X gewonnen werden, innerhalb des Geltungsbereiches des § 76 Abs. 2 SGB X einzuordnen. Das gleiche gilt für medizinische Daten, die offenkundig mit der Zweckbestimmung erstellt und zugänglich gemacht worden sind, eine Sozialleistung zu erhalten oder die Bescheinigung eines Sozialleistungsträgers ausgestellt zu bekommen. Liegt dagegen eine andere Zweckbestimmung vor (z.B. Angabe einer Verdachtsdiagnose bei Krankenhauseinweisung oder bei der Quartalsabrechnung, Arztbriefe an mit- oder nachbehandelnde Ärzte, Entlassungsberichte aus Krankenhäusern) und wurden die Unterlagen nicht selbst vom Betroffenen als „Beweismittel" in das Verfahren eingebracht, so dürfte eine Datenoffenbarung im Rahmen des § 76 Abs. 2 SGB X nicht in Betracht kommen. Meine Auffassung stützt sich dabei im wesentlichen auf die Überlegung, daß medizinische Daten, die zunächst mit anderer Zielsetzung erstellt wurden, den nunmehr bedeutsamen Sachverhalt möglicherweise nur ungenau und mit verändertem Schwerpunkt darstellen. Da eine Offenbarung medizinischer Daten im Rahmen des § 76 Abs. 2 SGB X dem Betroffenen häufig nicht bekannt wird, ist das Widerspruchsrecht des Betroffenen nach dieser Bestimmung kein geeignetes Mittel für die Mitwirkung des Betroffenen beim Verfahrensablauf.

Von diesen Überlegungen werden Fälle nicht erfaßt, bei denen ärztliche Unterlagen nach Feststellung einer anderen sachlichen Zuständigkeit an einen anderen Leistungsträger abgegeben werden müssen (z.B. bei Rehabilitationsmaßnahmen). Eine Prüfung nach § 76 Abs. 2 SGB X kann in solchen Fällen unterbleiben, da eine Datenweitergabe bereits nach § 76 Abs. 1 SGB X zulässig sein dürfte.

Das Bayerische Staatsministerium für Arbeit und Sozialordnung hat sich meiner Rechtsauffassung angeschlossen und ergänzend ausgeführt: Die Ausnahmeregelung des § 76 Abs. 2 SGB X umfaßt nicht die üblichen Anamnese-, Befund- und Diagnosedaten des behandelnden Arztes, sondern nur solche personenbezogenen Daten, die im Zusammenhang mit einer Begutachtung erfaßt wurden. Entscheidend kommt es demnach darauf an, daß die Daten bei einer gezielten, auf die Prüfung der Voraussetzungen für eine bestimmte Sozialleistung ausgerichteten Begutachtung erfaßt wurden. Es reicht nicht aus, daß die Daten bei einer allgemeinen Untersuchung oder Behandlung festgehalten und dann zur Begründung eines Leistungsantrages herangezogen werden. Der Gesichtspunkt der ärztlichen Schweigepflicht spricht ebenfalls für diese Auslegung. Nur die Daten sollen weitergegeben werden können, bei deren Erhebung dem Betroffenen klar war, daß sie das Arzt-Patientenverhältnis verlassen werden, um für die Begutachtung wegen der Erbringung von Sozialleistungen oder der Ausstellung einer Bescheinigung geoffenbart zu werden.

Ich habe die gesetzlichen Krankenkassen in diesem Sinne unterrichtet.

4.11.5. Errichtung einer städtischen „Kommission für Sozialhilfe"

Im 5. Tätigkeitsbericht wird unter Nr. 4.3.1, 4. auf die noch nicht abgeschlossene Überprüfung der Datenübermittlung an eine städtische Kommission für Sozialhilfe zur Überwachung der laufenden Angelegenheiten der Sozialhilfe hingewiesen. Da in diesem Zusammenhang kommunalrechtliche Fragen im Vordergrund standen, u.a. die Frage, ob der Kommission auch Nichtgemeinderatsmitglieder angehören könnten, habe ich – wie in solchen Fällen stets – das Bayerische Staatsministerium des Innern eingeschaltet.

Nach der Stellungnahme des Ministeriums ergeben sich bereits aus der Sicht des Kommunalrechts gewisse Beschränkungen für Tätigkeit und Zusammensetzung solcher Kommissionen: Hierdurch wird die ursprüngliche datenschutzrechtliche Problematik weitgehend entschärft. Wesentliche Punkte waren aus kommunalrechtlicher Sicht, daß die Arbeit einer beratenden Kommission im Ergebnis nicht dazu führen darf, daß Entscheidungskompetenzen unterlaufen werden, die das Kommunalverfassungsrecht gemeindlichen Organen, insbesondere dem Gemeinderat übertragen hat, so daß nicht bestimmte Sachbereiche aus dieser Verantwortung ausgeklammert und den jeweiligen Interessengruppen zur Entscheidung überlassen werden können. Dies würde letztendlich zur Aufsplitterung der umfassenden Zuständigkeit der Gemeindeorgane und zur Bildung einer ganzen Reihe von Einzelgremien führen, die lediglich ihre Einzelinteressen verfolgen. Den Entscheidungen dieser Gremien könnte sicher keine Integrationskraft und Konsensfähigkeit für die Gemeinde im ganzen zukommen. Auch wäre eine Verlagerung von Kompetenzen auf eine Kommission, der auch Nichtgemeinderatsmitglieder angehören, mit Art. 28 Abs. 1 Satz 2 GG nur schwer vereinbar. Nach dieser Verfassungsbestimmung muß das Volk in den Gemeinden eine allgemein gewählte Vertretung haben. Beratende Kommissionen können daher nur zu dem Zweck gebildet werden, den Gemeindeorganen eine Anhörung oder Beratung zu ermöglichen. Dagegen wäre es kommunalrechtlich unzulässig, ihnen eigene Rechte auf Beratung oder sogar Entscheidung einzuräumen. Die Überwachungsbefugnis des Gemeinderats kann im Rahmen der Geschäftsordnung oder durch Beschluß im Einzelfall auf einzelne Gemeinderatsmitglieder übertragen werden. Die Bildung einer Überwachungskommission in Sozialhilfeangelegenheiten, die nur aus Mitgliedern des Stadtrats besteht, kann als zulässig angesehen werden; hier werden aufgrund Art. 56 Abs. 1 Satz 2 GO dem Gemeinderat zustehende Befugnisse auf einzelne Gemeinderatsmitglieder übertragen. Gegen die Bildung einer Überwachungskommission für Sozialhilfefragen bestehen auch unter dem Gesichtspunkt der Zuständigkeitsabgrenzung zwischen Gemeindrat und 1. Bürgermeister keine grundsätzlichen Bedenken. Die Überwachungsbefugnis des Gemeinderats bezieht sich auch auf Aufgabenbereiche, die der 1. Bürgermeister gemäß Art. 37 Abs. 1 Satz 1 GO in eigener Zuständigkeit erledigt. Im Gegensatz zur Entscheidungszuständigkeit ist die Überwachungszuständigkeit des Gemeinderats nämlich keinen Beschränkungen unterworfen. Dies rechtfertigt sich daraus, daß die Überwachung der gemeindlichen Verwaltungstätigkeit kein Recht beinhaltet, die Entscheidungen anderer Gemeindeorgane aufzunehmen oder zu ändern, was insbesondere auch für Entscheidungen des 1. Bürgermeisters gemäß Art. 37 Abs. 1 Satz 1 GO gilt. Im Einzelfall muß daher darauf geachtet werden, daß die Kommissionsarbeit keinesfalls die nach Art. 37 Abs. 1 Satz 1 GO gegebene Zuständigkeit des 1. Bürgermeisters unterlaufen darf. Soweit es zur Durchführung der danach zulässigen beratenden und überwachenden Tätigkeit dieser Kommission erforderlich ist, dient die Übermittlung von Sozialdaten an diese nach § 69 Abs. 1 Nr. SGB X nach Auffassung des Bayerischen Staatsministerium des Innern der Erfüllung einer gesetzlichen Aufgabe nach dem Sozialgesetzbuch.

Ich habe mich dieser Rechtsauffassung angeschlossen und auf die Geheimhaltungspflicht der Mitglieder der Kommission nach § 78 SGB X und die Zweckbindung der Daten auf „die Überwachung der laufenden Angelegenheiten der Sozialhilfe" hingewiesen.

## 4.12. **Schul- und Hochschulverwaltung**

### 4.12.1. Datenerhebung an Schulen

#### 4.12.1.1. Datenerhebung für Forschungszwecke

Mit der Datenerhebung an Schulen hatte ich mich bereits in meinem letzten Tätigkeitsbericht ausführlich befaßt. Rechtsgrundlage ist Art. 62 Bayer. Gesetz über das Erziehungs- und Unterrichtswesen (BayEUG). Art. 62 Abs. 1 BayEUG erlaubt die Erhebung der Daten, die die Schulen zu ihrer Aufgabenerfüllung benötigen. Zur Abgabe dieser Daten sind die Schüler verpflichtet. Obwohl Art. 62 BayEUG für die Datenerhebung eine eindeutige und klare Regelung gibt, hatte das Staatsinstitut für Bildungsforschung und -planung im nachfolgend geschilderten Fall diese Datenschutzvorschriften zunächst nicht beachtet.

Das Staatsinstitut führte im Berichtszeitraum eine Untersuchung über die Schullaufbahnen ausländischer Schüler an Haupt-, Real- und Wirtschaftsschulen sowie Gymnasien in Bayern durch. In diese Untersuchungen wurden Klassen der Jahrgangsstufen 5 – 10 einbezogen, in denen sich Schüler(innen) griechischer, italienischer, jugoslawischer, spanischer, portugiesischer und türkischer Staatsangehö-

rigkeit befanden. Neben einem sog. „Klassenfragebogen", der weitgehend anonymisierte Daten enthalten sollte, hatten die jeweiligen Klassenleiter für jeden einzelnen Schüler einen „Schüler-Bogen" auszufüllen. Dieser „Schüler-Bogen" enthielt auf 8 Seiten 28 Fragestellungen, die teilweise in mehr als 10 Unterfragen aufgegliedert waren. Die für das Ausfüllen des „Schüler-Bogens" notwendigen Angaben sollten die Klassenleiter den an der Schule befindlichen Schulunterlagen entnehmen oder von den Schülern erfragen.

Aus der Sicht des Datenschutzes waren folgende Probleme von Belang:

Notwendige Anonymisierung

Eine Reihe von Fragestellungen im Schüler-Bogen berührte sensible Lebensbereiche. Hierzu gehörten beispielsweise die Fragen:

- nach den Wünschen des Schülers und den Absichten der Eltern hinsichtlich des weiteren Aufenthalts in der Bundesrepublik Deutschland,
- nach der Stellung des Schülers in der Klassengemeinschaft (Grad der Ablehnung oder Zuneigung),
- nach den schulischen Leistungen und nach einigen Charaktereigenschaften des Schülers (Ängstlichkeit, Aggressivität),
- danach, ob die Eltern berufstätig oder arbeitslos sind, in welchem Umfang sie beschäftigt sind, ob Vater oder Mutter nicht bei Familie leben.

Die in den Schüler-Bogen einzutragenden Angaben (z.B. Schule, genaue Bezeichnung der Klasse, Geschlecht, Geburtsjahr und Staatsangehörigkeit) ließen in vielen Fällen den Rückschluß auf bestimmte Schüler zu. Diese Daten waren somit personenbezogen. Weil selbst nach Auffassung des Staatsinstituts für die beabsichtigte wissenschaftliche Untersuchung bezüglich dieser ausländischen Schüler der Bezug zu bestimmten Personen nicht erforderlich war, war der mit dem Schüler-Bogen aber tatsächlich erlangte Bezug zu einzelnen Schülern unzulässig. Im übrigen bin ich der Auffassung, daß unabhängig von diesen datenschutzrechtlichen Überlegungen die Anonymität von Schülern und Eltern bei dieser Befragungsaktion allein schon deshalb hätte von Anfang an gewahrt werden müssen, um wegen mancher in der ausländischen Bevölkerung vorhandenen Ängste jeden Anschein zu vermeiden, die erhobenen Daten könnten als Anhaltspunkte für Maßnahmen gegen einzelne Schüler oder deren Eltern verwendet werden.

Freiwilligkeit der Angaben

Art. 16 Abs. 2 Bayer. Datenschutzgesetz fordert bei der Erhebung von Daten den Hinweis an den Befragten auf die Freiwilligkeit seiner Angaben, wenn, wie dies bei dem Schüler-Bogen bei einigen Fragestellungen der Fall war, keine Rechtsgrundlage zur Beantwortung der Fragen verpflichtet hat. Dieser Hinweis auf die Freiwilligkeit war bei der Fragebogenaktion allerdings nicht gewährleistet, weil die Klassenleiter auf die vorgenannte Bestimmung nicht aufmerksam gemacht worden waren. Zudem hatten einige Fragen im Schüler-Bogen Auskünfte der Schüler über ihre Eltern verlangt. Auf die Fragen beispielsweise zum „Umfang der beruflichen Tätigkeit und besondere Merkmale" und „Stellung im Beruf" wurden Angaben verlangt zur eventuellen Arbeitslosigkeit der Eltern, zum Umfang deren Berufstätigkeit sowie Aussagen zu der Tatsache, ob ein Elterteil nicht bei der Familie lebt. Die Entscheidung, ob diese teilweise sensiblen Daten freiwillig abgegeben werden durften, konnte nicht den 14-jährigen Kindern überlassen bleiben; wenn überhaupt, hätten diese Fragen unter Hinweis auf die Freiwilligkeit den Eltern gestellt werden müssen.

Auswertung der an der Schule befindlichen Schülerunterlagen

Zur Beantwortung einiger Fragen im Schüler-Bogen mußte der Klassenleiter die für schulische Zwecke angelegten Schülerunterlagen auswerten (z.B. für die Angaben zur Schullaufbahn mit eventuellen Klassenwiederholungen und zur Bewertung der schulischen Leistungen, die auf einzelne Fächer aufgesplittet werden sollten). Die Weitergabe solcher Daten an Stellen außerhalb der jeweiligen Schule darf schutzwürdige Belange der Schüler selbstverständlich nicht beeinträchtigen. Dies erfordert zum einen eine Beschränkung der Daten auf das unbedingt erforderliche Maß, zum anderen eine weitgehende Anonymisierung der Daten mit dem ausdrücklichen Verbot der Datenweitergabe an sonstige Dritte.

Auf meine datenschutzrechtlichen Bedenken hin hatte das Bayer. Staatsministerium für Unterricht und Kultus die Befragungsaktion zunächst gestoppt. Sodann wurde mit dem Staatsministerium für Unterricht und Kultus und dem Staatsinstitut für Bildungsforschung und Bildungsplanung hinsichtlich dieser Befragungsaktion folgendes erreicht:

Die im Rahmen dieser Untersuchung verwendeten Fragebogen wurden durch Wegfall der Bezeichnung der Schule und der genauen Angabe der Klasse so anonymisiert, daß ein Bezug auf konkrete Schüler ausgeschlossen sein dürfte.

Angaben zu den Eltern der Schüler wurden nur noch den Schulunterlagen entnommen. Die Schüler wurden nach den Lebensverhältnissen der Eltern nicht mehr befragt. Auf die besonders sensiblen Fragen zu den Absichten der Eltern und deren Arbeitsverhältnissen wurde verzichtet. Soweit sich noch Fragen an die Schüler unmittelbar richteten, wurden diese auf die Freiwilligkeit hingewiesen. Bei solchen Freiwilligkeitshinweisen an Schüler ist selbstverständlich darauf zu achten, inwieweit die Schüler aufgrund ihres Alters bereits in der Lage sind, über ihre Daten zu bestimmen.

Für den Fall, daß Klassenleiter den Schüler-Bogen in der beanstandeten Fassung bereits ausgefüllt hatten, wurde ihnen die Möglichkeit eingeräumt, die Daten selbst zu löschen, die im Hinblick auf die Vereinbarung nicht mehr erforderlich waren. Des weiteren wurde sichergestellt, daß das Staatsinstitut die Daten nicht auswertet, die unter Verletzung des Freiwilligkeitshinweises erhoben worden waren.

Damit war den Datenschutzbelangen weitgehend Rechnung getragen.

Diese Fragebogenaktion hatte in der Öffentlichkeit große Aufmerksamkeit gefunden. Zwar ist es für jede Behörde sehr unangenehm, wenn sie wegen Nichtbeachtung von Datenschutzvorschriften öffentliche Kritik findet, doch hat diese meist eine erfreuliche Schärfung des Datenschutzbewußtseins zur Folge. Ich gehe davon aus, daß bei künftigen Fragebogenaktionen im schulischen Bereich, die von staatlichen Stellen durchgeführt werden, die Datenschutzbelange strikt beachtet werden.

4.12.1.2. Datenerhebung im Rahmen des Schulunterrichts

Der nachfolgende Fall zeigt, daß auch fünf Jahre nach Inkrafttreten das Bayerischen Datenschutzgesetzes manche Lehrer nicht das notwendige Gespür für die Belange des Datenschutzes aufbringen.

Im Anschluß an eine während des Unterrichts durchgeführte Diskussion mit Landtagsabgeordneten verteilte der Klasslehrer einen „Fragebogen zur politischen Diskussion"an seine Gymnasial-Schüler mit der Aufforderung, diesen innerhalb von 10 Tagen ausgefüllt zurückzugeben. Im Fragebogen war u.a. die Frage gestellt, ob die Schüler Mitglied in einer politischen Partei seien. Weder enthielt der Fragebogen einen Hinweis auf die Freiwilligkeit der Angabe, noch war eine ausreichende Anonymisierung der Schülerantworten gewährleistet. Nach Art. 62 Abs. 1 BayEUG ist die Erhebung und Verarbeitung von personenbezogenen Schülerdaten, grundsätzlich nur zur Erfüllung der den Schulen durch Rechtsnorm zugewiesenen Aufgaben zulässig. Der Fragebogen enthielt aber Fragestellungen, die vom Unterrichtsauftrag nicht gedeckt waren. Damit war die Datenerhebung auf dem Fragebogen unzulässig. Auf meine Bitte hin wurden die Fragebogen von der Schulleitung eingesammelt und vernichtet.

4.12.1.3. Datenerhebung durch außerschulische Organisationen

Durch Bürgereingaben bin ich auf folgenden Sachverhalt aufmerksam geworden:

Kurz vor dem jeweiligen Schulabschluß häuften sich bei den Schülern Besuche von Versicherungsvertretern, die Angebote für Lebens-, Kranken- und Aussteuerversicherungen vorlegten. Auch Kreditinstitute, mit denen weder die Eltern der Schüler, noch die Schüler selbst bis zu diesem Zeitpunkt Verbindung gehabt hatten, meldeten sich bei den Schülern. Offensichtlich war den Versicherungen und den Kreditinstituten Name, Anschrift und Alter der Schüler bekannt. Entsprechende Rückfragen bei den Schulen, die die Schüler jeweils besucht hatten, ergaben durchwegs die Auskunft, daß die fraglichen Schülerdaten von den Schulen nicht weitergegeben worden waren. Als mögliche Gelegenheiten, bei denen die Daten über Schüler und Schülerinnen Dritten bekannt werden könnten, nannten die Schulen mehrere im Rahmen des Unterrichts bzw. im sonstigen schulischen Bereich stattfindende Veranstaltungen:

- Betriebsbesichtigung durch Schulklassen bei Sparkassen und Kreditinstituten – hierbei wird manchmal ein Klassenfoto gemacht, das denjenigen Schülern zugesandt wird, die ihre Anschrift hinterlassen;
- Angebot eines „Bewerbungssets" mit Musterlebenslauf, Musterbewerbung und ähnlichem durch ein Kreditinstitut und nachfolgende Zusendung an die Schüler, welche ihre Anschriften mitteilen;
- Ausbildung in Sofortmaßnahmen bei Unfällen – es wurde eine Teilnehmerliste mit Namen, Geburtsdaten und Anschriften der Schüler gefertigt; ähnliches gilt für die Durchführung einer Mofa-Ausbildung samt Prüfung an der Schule;
- Vorträge eines Mitarbeiters einer Krankenversicherung im Rahmen des Sozialkundeunterrichts über die Sozialversicherung – hierbei werden Anschriften gesammelt, um Schülern Poster und Broschüren zuzusenden;
- Aufforderung des Arbeitsamtes an die Schüler, ihre Adressen zur Zustellung von Broschüren bekanntzugeben und
- Schülerpreisausschreiben anläßlich des Weltspartages durch die örtliche Kreissparkasse – auf entsprechenden Aushang am Schwarzen Brett sollten sich die interessierten Schüler unter Angabe ihrer Anschrift bei der Sparkasse melden.

Ich gehe davon aus, daß diese Aufzählung bei weitem nicht vollständig ist und ggf. weitere Aktivitäten im schulischen Bereich festgestellt werden können, bei denen über Informations- und andere Angebote indirekt auch Werbung und Adressenbeschaffung betrieben wird. Angesprochene Sparkassen haben mir versichert, daß derartiges Adressenmaterial nur für eigene Zwecke verwendet und nicht an dritte Stellen weitergegeben werde. Gleichwohl steht fest, daß immer wieder Adressenmaterial aus dem schulischen Bereich – auf welchen der genannten Wege auch immer – nach außen gelangt und zu einer nachhaltigen Umwerbung der Abschlußschüler führt.

Angesichts dieses Umstandes halte ich es für angezeigt zu überprüfen, ob Veranstaltungen von Sparkassen und anderen Unternehmungen, die auch der Werbung und der Beschaffung von Adressenmaterial dienen und im Rahmen der Schule stattfinden, mit Art. 61 des Gesetzes über das Erziehungs- und Unterrichtswesen (BayEUG) vereinbar sind oder eine Umgehung des aus datenschutzrechtlicher Sicht begrüßenswert strengen Art. 62 Abs. 1 BayEUG darstellen. Ich vertrete die Ansicht, daß Informations- und Unterrichtsangebote derartiger Stellen von den Schulen strenger darauf überprüft werden sollten, ob sie lediglich ein vordergründiges Unterrichtsangebot enthalten und sich daneben oder sogar in erster Linie als Werbungsmaßnahme der betreffenden Stelle darstellen. Die Schulen sollten ggf. die Veranstalter darauf hinweisen, daß sie keine personenbezogenen Daten von Schülern im Rahmen von Informationsveranstaltungen an Schulen oder bei Gelegenheit von außerschulischen Veranstaltungen, wie etwa von der Schule durchgeführten Betriebsbesichtigungen, erheben sollen, es sei denn, die ausdrückliche Einwilligung der Eltern liegt vor. Darüber hinaus sollten im Rahmen solcher Veranstaltungen im Einzelfall gleichwohl erhobene Daten, etwa der Anschriften für die Zusendung von Informationsmaterial, ausschließlich für diesen Zweck verwendet und nicht an weitere Stellen übermittelt werden. In dieser Angelegenheit bin ich mit dem Bayer. Staatsministerium für Unterricht und Kultus im Gespräch.

4.12.2. Schulchronik, Jahresberichte

Anläßlich einer Schulausstellung zum 10-jährigen Jubiläum einer Volksschule war die bei dieser Schule geführte Schulchronik ausgelegt und stand den Besuchern zur Einsicht offen. Die Schulchronik enthielt auch persönliche Daten der Lehrkräfte, wie Geburtsdaten und Fehlzeiten wegen Krankheit oder Mutterschaftsurlaub, sowie in Einzelfällen die Art der Erkrankung, die Todesursache einer Lehrkraft und die Tatsache der Wiederholung der 2. Lehramtsprüfung. Einige Lehrer haben sich wegen dieser Bekanntgabe ihrer persönlichen Daten an mich gewandt.

Ich habe keinen Zweifel, daß die durch die Auslegung der Schulchronik ermöglichte Kenntnisnahme von persönlichen Daten ohne ausdrückliche Einwilligung der betroffenen

Lehrkräfte unzulässig ist. Dabei kann ein etwa von der Lehrerkonferenz widerspruchslos akzeptierter Vorschlag zur Auslegung der Schulchronik jedenfalls dann keine wirksame Einwillung darstellen, wenn deren Inhalt, was die hier erörterten persönlichen Daten anbelangt, den Lehrkräften weitgehend unbekannt ist. Die zuständige Schulaufsichtsbehörde hatte im übrigen, schon bevor dieser Fall an mich herangetragen wurde, im Rahmen einer Dienstaufsichtsbeschwerde das Vorliegen eines objektiven Verstoßes gegen die beamtenrechtliche Verschwiegenheitspflicht festgestellt. Wenn auch der beamtenrechtliche Schuldvorwurf nach den Ermittlungen der Schulaufsichtsbehörde im konkreten Fall gering war, so sollte der Vorfall allen Beteiligten als Warnung dienen, der Pflicht zur Verschwiegenheit in Personalangelegenheiten besondere Beachtung zu schenken. Insoweit kann auch eine vertrauensvolle Zusammenarbeit zwischen Schulleitung und Lehrkräften dem Schutz der Privatsphäre dienlich sein.

Auch in Jahresberichten der Schulen finden sich gelegentlich personenbezogene Daten, deren Veröffentlichung nicht unproblematisch erscheint. So enthielt der Jahresbericht eines Gymnasiums z.B. Personendaten über das Schulverwaltungs- und Hausverwaltungspersonal, die Privatanschriften der Elternbeiräte und den jeweiligen Wohnort der Schüler. Art. 62 Abs. 3 des Bayerischen Gesetzes über das Erziehungs- und Unterrichtswesen stellt demgegenüber ausdrücklich klar, welche personenbezogenen Daten in Jahresberichten der Schulen ausschließlich enthalten sein dürfen. Die oben genannten Daten sind dort nicht aufgezählt; ihre Veröffentlichung ohne Einwilligung der Betroffenen halte ich daher für unzulässig.

### 4.12.3. Neugestaltung der Zeugnisformulare

Das Bayerische Staatsministerium für Unterricht und Kultus hat mich darauf aufmerksam gemacht, daß im Kopfteil der Zeugnisse bei einigen Schularten die Bekenntnisangehörigkeit des Schülers angegeben ist, bei anderen Schularten jedoch nicht. Werde nun im Zuge einer Vereinheitlichung beispielsweise auf die Angabe der Bekenntnisangehörigkeit im Kopfteil der Zeugnisse verzichtet, jedoch beim Fach Religion kenntlich gemacht, welchen Religionsunterricht der Schüler besucht habe, ergebe sich folgendes Problem:

Bei den Angehörigen kleiner Religionsgemeinschaften, bei denen die Religionsgemeinschaft erklärt habe, daß ihre Grundsätze mit denen des Lehrplans des katholischen oder evangelisch-lutherischen Religionsunterricht übereinstimmen und daher dieser Religionsunterricht von ihren Bekenntnisangehörigen besucht werden könne, ist die Angabe des Bekenntnisses des Schülers mit dem besuchten Religionsunterricht nicht identisch. Entsprechendes gilt bei einer etwaigen Teilnahme bekenntnisloser Schüler am Religionsunterricht. Bei der Frage, ob gegebenenfalls auf den Nachweis der Religionszugehörigkeit völlig verzichtet werden könnte, hatte ich folgendes festgestellt: Das Datenschutzrecht ist von dem Grundsatz beherrscht, daß nur die Daten gespeichert, übermittelt oder sonst genutzt werden dürfen, die für die Erfüllung der jeweiligen Aufgabe erforderlich sind. Angesichts der Tatsache, daß die Angabe der Bekenntnisangehörigkeit ein besonders sensibles Datum ist, weshalb dessen Bekanntgabe schutzwürdige Belange beeinträchtigen kann, und eines Fehlens einer entsprechenden gesetzlichen Aufgabenzuweisung an die Schule, die Religionszugehörigkeit im Zeugnis ausdrücklich kenntlich zu machen, dürfte die Angabe der Bekenntnisangehörigkeit im Kopfteil der Zeugnisse nicht zulässig sein. Dies dürfte auch im Hinblick auf 136 Abs. 3 Satz 1 Weimarer Reichsverfassung problematisch sein, weil bei jeder Vorlage des Zeugnisses zwangsläufig die Bekenntnisangehörigkeit offenbart wird. Ebenfalls nicht unproblematisch dürfte die Angabe der Bekenntnisangehörigkeit bei der Note für das Fach Religionslehre sein. Weil in einzelnen Fällen aus dieser Angabe falsche Schlüsse gezogen werden können, also das Datum nicht richtig interpretiert wird, sollte auch insoweit auf die Angabe der Bekenntnisangehörigkeit verzichtet werden.

Das Bayerische Staatsministerium für Unterricht und Kultus hat mir mitgeteilt, daß es meine datenschutzrechtlichen Bedenken gegen die Angabe der Bekenntnisangehörigkeit im Kopfteil der Zeugnisse voraussichtlich bei den neuen Zeugnisformularen berücksichtigen wird. Stattdessen soll jedoch durch einen Zusatz beim Unterrichtsfach Religionslehre deutlich gemacht werden, nach welchen Bekenntnis dieser Unterricht erteilt worden ist. Welchem Bekenntnis der Schüler tatsächlich angehört, wird nicht aufgenommen.

### 4.12.4. Universitätsinternes Personenkennzeichen

An einer bayerischen Universität wurde 1974 zur Identifikation der Studenten ein sog. „universitätsinternes Personenkennzeichen" in der Studentendatei entwickelt. Es enthält das Geburtsdatum, die Geschlechtskennziffer, die Ordnungsnummer, welche alle Studenten, die im selben Monat und Jahr geboren sind, hochzählt, und eine Prüfziffer. Die Universität hat dieses Personenkennzeichen (PK) in den Fällen auf Adreßaufkleber gedruckt, wo gleichlautende Namen Verwechslungen wahrscheinlich machten. Allerdings sind Adreßaufkleber mit Personenkennzeichen nur bei erstimmatrikulierten Studenten verwendet worden. Nach Angaben der Universität habe sich der Aufdruck dieses Personenkennzeichens deshalb als zweckmäßig erwiesen, weil Schreiben an erstimmatrikulierte Studenten häufig wegen Unzustellbarkeit zurückgekommen seien. Über das „PK" habe ohne erneute Öffnung des Schreibens mit Hilfe des Datensichtgeräts festgestellt werden können, ob der betreffende Student sich bereits wieder exmatrikuliert hat oder ob schon eine neue Adresse verfügbar ist.

Die Verwendung eines „Personenkennzeichens" halte ich bereits deshalb für nicht unbedenklich, weil die Einführung des bundesweiten Personenkennzeichens für das Meldeverfahren gerade auch an verfassungsrechtlichen Bedenken gescheitert war. Bereits aus diesem Grunde sollten öffentliche Stellen auch jeden Anschein vermeiden, sie würden ein verfassungsrechtlich bedenkliches Ordnungsmerkmal benützen. Die betroffene Universität hat mir nun zugesagt, daß die Bezeichnung „Personenkennzeichen" nach Verbrauch der derzeit vorhandenen EDV-Endlosformulare wieder durch den früher üblichen Ausdruck „Matrikelnummer" ersetzt würde. Des weiteren werde erwogen, das bisherige 12-stellige Kennzeichen durch ein Kennzeichen geringeren Umfangs zu ersetzen, welches das Geburtsdatum nicht mehr enthält. Im übrigen soll der offene Ausdruck des Kennzeichens in Zukunft wirklich auf die Fälle beschränkt werden, wo Unterscheidungen sonst nicht oder nur schwer durchzuführen wären. Letzteres scheint mir zumindest für eine Übergangszeit als hinnehmbar.

## 4.13. **Archivwesen**

Auf die Notwendigkeit einer eindeutigen gesetzlichen Regelung der mit der Archivierung personenbezogenen Materials zusammenhängenden Fragen habe ich bereits seit längerem hingewiesen. Derzeit wird in den Archivverwaltungen des Bundes, der Länder und der Kommunen die Rechtslage durch Akten- und Benutzungsordnungen, Bekanntmachungen einzelner Ressorts, Verwaltungsvorschriften und einige wenige gesetzliche Regelungen bestimmt. Angesichts der großen Mengen personenbezogener Daten, die die Archive mit dem ihnen überlassenen Archivmaterial verarbeiten, des teilweise sensiblen Inhalts der archivierten Daten und der durch die Abgabe der Daten an die Archive eingetretenen Zweckänderung ist gerade auch im Hinblick auf die vom Bundesverfassungsgericht im Volkszählungsurteil erarbeiteten Grundsätze eine eindeutige gesetzliche Regelung erforderlich.

Zum tatsächlichen Fortgang der Arbeiten an einem Bayerischen Archivgesetz kann ich über meine Ausführungen im 5. Tätigkeitsbericht hinaus nichts Neues berichten. Ein vom Bayerischen Staatsministerium für Unterricht und Kultus erarbeiteter erster Entwurf liegt nach wie vor dem Staatsministerium des Innern zur Stellungnahme und gegebenenfalls Ergänzung vor. Zu meinem Bedauern hat der Bayerische Städtetag sich gegen die Schaffung eines Archivgesetzes ausgesprochen. Er ist der Ansicht, die ins Feld geführten Probleme des Datenschutzes könnten ebensogut durch Änderung der bestehenden Datenschutzgesetze überwunden werden. Dieser Auffasssung muß widersprochen werden, weil mit der Schaffung einfacher Archivklausein die anstehenden Probleme nicht gelöst und umfangreiche archivarische Regelungen die Datenschutzgesetze jedoch sprengen würden. Bemerkenswert ist in diesem Zusammenhang, daß die Arbeitsgemeinschaft Bayerischer Stadtarchivare und damit eine Vertretung von Fachleuten die Bemühungen ausdrücklich begrüßt hat, das öffentliche Archivwesen in Bayern auf eine gesetzliche Grundlage zu stellen. Die Arbeitsgemeinschaft hat ausdrücklich erklärt, daß sie die grundsätzlich ablehnende Haltung des Bayerischen Städtetages zu einer gesetzlichen Regelung nicht teilen könne.

Bezüglich der einzelnen in einem Archivgesetz zu regelnden Probleme nehme ich auf meine Ausführungen im 4. und 5. Tätigkeitsbericht Bezug. Daneben haben die Datenschutzbeauftragten des Bundes und der Länder einen Musterentwurf eines Archivgesetzes erarbeitet, um die Schaffung von Archivgesetzen zu erleichern. Der Entwurf ist im Anhang (Nr. 10) abgedruckt.

## 4.14. **Straßenverkehrswesen**

### 4.14.1. Zentrales Verkehrs-Informationssystem (ZEVIS)

Die Zulassung von Kraftfahrzeugen führt zu Datenbeständen bei den örtlichen Kfz-Zulassungsstellen und beim Kraftfahrtbundesamt (KBA). Dabei handelt es sich um die Daten der Halter, technische Fahrzeugdaten sowie bestimmte tatsächliche und rechtliche Verhältnisse in Bezug auf das Kraftfahrzeug. Bei den örtlichen Kfz-Zulassungsstellen werden diese Daten derzeit noch überwiegend manuell geführt. In Bayern werden die Daten bei den Kraftfahrzeug-Zulassungsstellen in München und Nürnberg sowie in fünf Landkreisen automatisiert; auf die entsprechenden Probleme des Datenabrufs durch die Polizei habe ich im 5. Tätigkeitsbericht auf S. 24 Stellung genommen. Bundesweit sind ca. 30% der entsprechenden Daten automatisiert erfaßt.

Im folgenden befasse ich mich mit dem Zentralen Fahrzeugregister beim Kraftfahrtbundesamt. Zwar gehört das Kraftfahrtbundesamt in erster Linie zum Zuständigkeitsbereich des Bundesbeauftragten für den Datenschutz. Weil der maßgebliche Teil der dort gespeicherten Daten jedoch von den Ländern, also auch von Bayern, angeliefert wird und Landesbehörden vom KBA Daten erhalten, ist auch der Bayer. Landesbeauftragte für den Datenschutz berufen, sich mit der Datenverarbeitung beim KBA auseinanderzusetzen.

Das Zentrale Fahrzeugregister beim KBA hat einen Bestand von derzeit etwa 32 Millionen Fahrzeugen. Dieses Fahrzeugregister besteht aus Dateien der Fahrzeuge mit amtlichem Kennzeichen und der Fahrzeuge mit Versicherungskennzeichen, die nach Kennzeichen bzw. nach Hersteller- und Fahrzeugidentifizierungsnummern geordnet sind. Neben der Zahl von 32 Millionen erfaßten Kraftfahrzeugen macht der Umfang der täglich etwa 19000 Auskünfte deutlich, welchen datenschutzrechtlichen Belang dieses zentrale Fahrzeugregister besitzt. Das zentrale Kraftfahrzeugregister soll mit dem Vorhaben ZEVIS (Zentrales Verkehrs-Informations-System) modernisiert werden. Durch ZEVIS sollen Führung und Nutzung der Datenbestände verbessert werden. Außerdem soll neben den vorgenannten Fahrzeugdateien in bestimmtem Umfang auch das Verkehrszentralregister miterfaßt werden. Außerdem sind mit ZEVIS die technischen Möglichkeiten geschaffen worden, die Polizei online (Direkt-Abruf) an die Datenbestände anzuschließen und Auskünfte im einstelligen Sekundenbereich zu geben. Im Wege des Direkt-Abrufes können mit dem amtlichen Kennzeichen oder Teilen davon die zu diesen Kennzeichen gespeicherten Daten abgefragt werden. Für die Zukunft ist die sogenannte „P-Anfrage" vorgesehen, mit der unter Angabe eines Namens erfragt werden kann, ob und wenn ja welche Kraftfahrzeuge für eine bestimmte Person zugelassen und unter welcher Anschrift der Kraftfahrzeughalter die Fahrzeuge angemeldet hat. Zur Zeit sind neben den Fahrzeugbeständen einiger anderer Länder auch die Fahrzeugbestände Bayerns in ZEVIS enthalten und von der Bayer. Polizei im Online-Verfahren abrufbar.

Für Auskünfte über Kraftfahrzeughalter enthält § 26 Abs 5 StVZO, wonach „im Einzelfall auf Antrag Behörden" Auskunft über die Fahrzeuge, die Halter und die Versicherungen erteilt wird, eine Regelung, mit der ich mich im letzten Tätigkeitsbericht hinsichtlich der Automation der Kraftfahrzeugzulassungsstelle München auseinandergesetzt hatte. Für den Datenverkehr des Kraftfahrtbundesamtes und bayerischer Polizeibehörden gibt diese Vorschrift keine ausreichende Rechtsgrundlage. Für die Einführung von ZEVIS und den bundesweiten Anschluß von Polizeibehörden ist eine besondere Rechtsgrundlage erforderlich. Zwischenzeitlich liegt auch der Entwurf eines Gesetzes zur Änderung des Straßenverkehrsgesetzes vor, mit dem das Straßenverkehrsgesetz um einen Abschnitt über das „Fahrzeugregister" ergänzt werden soll. Der derzeit vorliegende Entwurf (Stand: 15.4.1984) wird zwar noch überarbeitet, dennoch ist meines Erachtens zu der grundsätzlichen Problematik dieser Gesetzgebung für das Fahrzeugregister folgendes festzuhalten:

Der Grundsatz der Zweckbindung der Datenverarbeitung, wie er auch vom Bundesverfassungsgericht im Volkszäh-

lungsurteil bestätigt worden ist, verlangt, daß die Daten im Fahrzeugregister grundsätzlich nur zu dem Zweck verwendet werden dürfen, zu dem sie erhoben worden sind. Dies bedeutet, daß die Daten der Identifizierung von Kraftfahrzeugen und Kraftfahrzeughaltern zu dienen haben. Eine Verwendung der Daten zu weitergehenden Zwecken, die nicht mehr mit dem Halten von Kraft fahrzeugen in Verbindung stehen, kann allenfalls in wenigen Ausnahmefällen zulässig sein. Insbesondere erscheint mir bedenklich, daß die sogenannte „P-Abfrage" über die Personalien der Halter von Kraftfahrzeugen durch Polizeidienststellen und andere Behörden ohne sachliche und regionale Beschränkung im Direkt-Abrufverfahren zugelassen werden soll. Mit der Gestattung des Online-Abrufs gelten die Daten nach der herkömmlichen Definition der Datenschutzgesetze als insgesamt übermittelt (vergleiche Art. 5 Abs. 2 Nr. 2 BayDSG). Gerade die Zulassung dieser Nutzungsform im Wege des direkten Abrufs führt zu einer bisher nicht vorhandenen qualitativen Änderung der Verwendungsmöglichkeiten der Kraftfahrzeugdaten durch die Polizei. Das Risiko ist nicht völlig von der Hand zu weisen, daß das zentrale Fahrzeugregister sich zu einer Art „Bundes-Adreß-Register" entwikkelt. Dies wäre jedoch mit den Zwecken eines zentralen Fahrzeugregisters nicht mehr vereinbar. Wegen der Signalwirkung, die die Gestattung einer solchen Nutzungsform haben könnte, bin ich mir mit den übrigen Datenschutzbeauftragten des Bundes und der Länder einig, daß diese Frage noch eingehend diskutiert werden muß. Um jede Fehlinterpretation dieser Ausführungen zu verhindern, stelle ich klar, daß die Polizei – gleiches gilt für andere Behörden, etwa die mit der Abwicklung von Bußgeldverfahren befaßten – selbstverständlich nicht von den Daten abgeschnitten werden darf, die sie zu ihrer gesetzlich zugewiesenen Aufgabenerfüllung benötigt. Auch in Einzelfällen kann sie sich kurzfristig die erforderlichen Informationen verschaffen, auch ohne Online-Anschluß! Strittig ist hier allein der Weg, auf dem diese Daten an die Behörden gelangen sollen. Auch bei der Frage der Nutzungsform einer Datenbank ist meines Erachtens jeweils zu prüfen, wie die Auswirkungen auf die Persönlichkeitssphäre der Bürger so gering wie möglich gehalten werden können.

Bezüglich dieser und weiterer Probleme dieses Gesetzesvorhabens, die beispielsweise die Einstellung von Suchvermerken und Steckbriefnachrichten in das Zentrale Fahrzeugregister und beabsichtigte Datenabgleiche betreffen, werde ich weiterhin mit dem Bayer. Staatsministerium für Wirtschaft und Verkehr in Kontakt bleiben.

4.14.2. Kartei über Fahrerlaubnisinhaber

Über die ausgehändigten Führerscheine hat die Kfz-Zulassungsstelle eine nach dem Namen der Führerscheininhaber geordnete Kartei zu führen (§ 10 Abs. 2 Satz 2 StVZO). Mit der Frage, welchen Umfang die auf den einzelnen Karteikarten vermerkten Angaben haben dürfen, hatte ich mich im Berichtszeitraum zu beschäftigen. Nach ersten Ermittlungen scheint festzustehen, daß die diesbezügliche Sachbearbeitung der einzelnen Kfz-Zulassungsstellen nicht einheitlich ist. Während manche Karteikarten nur die führerscheinbezogenen Angaben enthalten, also ob ein Führerschein erteilt, derzeit entzogen ist oder ein Fahrverbot besteht, enthält in anderen Fällen die Führerscheinkartei den zusammengefaßten Akteninhalt, also auch z.B. die Angabe darüber, wieviele Punkte für den jeweiligen Führerscheininhaber im Verkehrszentralregister eingetragen sind.

Eine abschließende rechtliche Beurteilung steht noch aus. Das Bayerische Staatsministerium des Innern, mit dem ich in dieser Frage noch in Verhandlungen stehe, führt derzeit eine Umfrage bei den Kreisverwaltungsbehörden durch, in welcher Form dort im einzelnen die Führerscheinkartei geführt wird und wie weit eine Verringerung des Inhalts deren Arbeit erschweren würde.

Ganz grundsätzlich ist zur rechtlichen Beurteilung der Zulässigkeit der Speicherung von Daten in der Führerscheinkartei, die zugleich im Verkehrszentralregister oder Bundeszentralregister eingetragen sind, folgendes festzustellen: Zunächst ist zwischen dem Zeitraum zu unterscheiden, in dem diese Daten noch in den vorgenannten Registern rechtmäßig festgehalten sind und dem Zeitpunkt, ab dem diese Daten getilgt oder zumindest tilgungsreif sind. Weiter ist bei der Beurteilung, ob die in den Zentralregistern niedergelegten Daten zugleich in der Kartei der Führerscheininhaber gespeichert werden dürfen, zu berücksichtigen, daß die im Verkehrszentralregister niedergelegten Daten nach § 30 Abs. 1 StVG einem beschränkten Verwertungszweck unterliegen. Diese Beschränkung darf meines Erachtens nicht durch eine parallele Führung in anderen Karteien oder Registern unterlaufen werden. Außerdem hat der Gesetzgeber nach Ansicht des Bundesverwaltungsgerichts durch die Einrichtung einer Verkehrszentralkartei deutlich erkennen lassen, „daß neben dieser zentralen Registrierung keine örtlichen Karteien weiter bestehen sollten". Schließlich ist bei der Frage der Erforderlichkeit eine Aufnahme dieser Daten in den dezentralen Führerscheinkarteien zu berücksichtigen, daß durch Rechtsvorschrift dem Kraftfahrtbundesamt ohnehin die Pflicht auferlegt ist, bei einem bestimmten Punktestand die zuständige Behörde von Amts wegen zu unterrichten. Somit ist eine parallele Führung der im Verkehrszentralregister enthaltenen Daten bei der zuständigen Verwaltungsbehörde grundsätzlich überflüssig.

Soweit allerdings die Verwaltungsbehörde einen Führerschein entzogen hat und sich diese Tatsache aus den entsprechenden Verwaltungsakten ergibt, dürfte die Tatsache des Entzugs der Fahrerlaubnis auch als wesentlicher Inhalt der Führerscheinkartei zur Aufgabenerfüllung der Kfz-Zulassungsstelle erforderlich sein.

Hinsichtlich getilgter oder tilgungsreifer Eintragungen gilt im Hinblick auf § 49 Abs. 1, § 50 Abs. 2 Bundeszentralregistergesetz folgendes: Soweit Eintragungen im Verkehrszentralregister getilgt sind, gilt das Verwertungsverbot des § 49 Abs. 1 BZRG jedenfalls für solche Eintragungen unbeschränkt, die nur im Verkehrszentralregister und nicht gleichzeitig im Bundeszentralregister enthalten waren. Die Ausnahme des § 50 Abs. 2 BZRG greift hier nicht ein. Somit können Eintragungen wegen Ordnungswidrigkeitenverfahren in einem Verfahren, das die Erteilung oder die Entziehung eines Führerscheins zum Gegenstand hat, nicht verwertet werden. Demnach ist auch ihre Speicherung zur Aufgabenerfüllung der Kfz-Zulassungsstelle nicht erforderlich und somit unzulässig. Hingegen dürften die übrigen im Bundeszentralregister enthaltenen Eintragungen über Verkehrsstraftaten nach § 50 Abs. 2 BZRG auch nach deren Tilgung oder Tilgungsreife für die Erteilung oder Entziehung von Führerscheinen verwertet werden. Allerdings gestattet es meines Erachtens dieser beschränkte Verwertungszweck keinesfalls, daß diese Verurteilungen auf der für den

„normalen" Geschäftsverkehr zur Verfügung stehenden Kartei der Führerscheine vermerkt bleiben. Denn für die Berücksichtigung dieser Tatsachen in einem Führerschein-Verfahren genügt es , wenn die Verwaltungsbehörde diese Daten von den übrigen Führerscheindaten getrennt, also im Sinne des Datenschutzrechts „gesperrt", verwahrt. Wenn weder ein Verfahren zur Erteilung noch zur Entziehung der Fahrerlaubnis anhängig ist, ist die Kenntnis dieser getilgten oder tilgungsreifen Eintragungen für die gewöhnliche Verwaltungstätigkeit der Kfz-Zulassungsstelle nicht erforderlich. Die Sperrung nach Art. 20 Abs. 1 Satz 2 BayDSG ist demnach geboten. In diesem Zusammenhang ist weiter zu berücksichtigen, daß die Führerscheinkarteien den zuständigen Polizeibehörden für deren Aufgabenerfüllung – teilweise auch nachts ohne Mitwirkung der KFZ-Zulassungsstelle – zugänglich sind. Auch hinsichtlich dieser Nutzung ist Sorge dafür zu tragen, daß die Führerscheinkarteien nur die erforderlichen Daten enthalten.

Über den weiteren Fortgang der Verhandlungen mit dem Bayerischen Staatsministerium des Innern werde ich berichten.

4.14.3. Verwertung von Verurteilungen im Führerscheinverfahren

Von einem Datenschutzbeauftragten eines anderen Bundeslandes wurde mir berichtet, daß dort einem Bürger im Rahmen des Verfahrens zur Neuerteilung seines Führerscheins Straftaten vorgehalten worden seien, die sowohl im Bundeszentralregister als auch im Verkehrszentralregister bereits getilgt waren. Die einschlägigen Vorgänge waren in den Jahren 1961 bis 1965 angefallen und lagen damit teilweise über 20 Jahre zurück. Diese Sachbehandlung war mit § 50 Abs. 2 Bundeszentralregistergesetz (BZRG) begründet worden, der bestimmt, daß für Verurteilungen, die auch in das Verkehrszentralregister einzutragen waren, das Verwertungsverbot des § 49 Abs. 1 BZRG dann nicht gilt, wenn es sich um ein Verfahren handelt, das die Erteilung oder Entziehung der Fahrerlaubnis zum Gegenstand hat. Zwar hat das Bundesverfassungsgericht bereits in einem Urteil aus dem Jahre 1976 festgestellt, daß die Tilgung einer Eintragung im Verkehrszentralregister ein Verwertungsverbot für den dem getilgten Eintrag zu Grunde liegenden Sachverhalt bewirkt. Danach dürfen Entscheidungen, die im Verkehrszentralregister eingetragen waren, nach deren Tilgung dem Betroffenen nicht mehr vorgehalten und nicht mehr zu seinem Nachteil verwertet werden.

Auf eine entsprechende Anfrage, wie diesbezüglich in Bayern verfahren werde, steht eine Antwort des Bayerischen Staatsministeriums des Innern noch aus. Sollten auch in Bayern dem Betroffenen längst getilgte Verurteilungen vorgehalten werden, werde ich eine Novellierung des § 50 Abs. 2 BZRG anregen.

4.14.4. Auskunftserteilung durch Kfz-Zulassungsstellen

Nach § 26 Abs. 5 StVZO erteilen die Kfz-Zulassungsstellen im Einzelfall auf Antrag bei Darlegung eines berechtigten Interesses Auskunft über die Fahrzeuge, die Halter und die Versicherungen. Zu einzelnen Fragen dieser Auskunftserteilung, insbesondere an Behörden, hatte ich bereits in meinem 5. Tätigkeitsbericht Stellung genommen. Anfragen an meine Geschäftsstelle zeigen, daß teilweise noch Anwendungszweifel über die Vorschrift des § 26 Abs. 5 StVZO bestehen. Daher ergänze ich meine früheren Ausführungen wie folgt:

An den Zentralruf der Autoversicherer sind auf fernmündliche Auskunftsverlangen Auskünfte über Kraftfahrzeughalter und deren Anschrift oder Fahrzeugdaten aus datenschutzrechtlichen Gründen nicht zu erteilen. Dagegen bestehen grundsätzlich keine Bedenken auf fernmündliche Anfrage des Zentralrufs der Autoversicherer Auskunft über die Versicherungsgesellschaft, die Versicherungsscheinnummer oder die Doppelkartennummer, falls nur diese bekannt ist, zu gewähren. Allerdings hat die Kraftfahrzeugzulassungsstelle, bevor sie eine fernmündliche Auskunft erteilt, regelmäßig neben der Nennung des Kraftfahrzeugkennzeichens auch den Namen des betroffenen Fahrzeughalters zu fordern. Damit besteht eine gewisse Gewähr dafür, daß der Zentralruf der Autoversicherer mit einer konkreten Schadensregulierung befaßt ist und die Daten hierfür benötigt. Dagegen sind Auskünfte über den Kraftfahrzeughalter und auch dessen Anschrift nur auf schriftlichen Antrag hin und erst nach Prüfung eines berechtigten Interesses zu erteilen. In dieser Auffassung bin ich mir mit dem Bayer. Staatsministerium für Wirtschaft und Verkehr einig.

Zwar sind diese vorgenannten Grundsätze auf fernmündliche Auskunftsverlangen von Rechtsanwälten und Privatpersonen grundsätzlich ebenfalls anzuwenden. Allerdings erscheinen telefonische Auskünfte hier nur zulässig, wenn der Anrufer auch begründet, weshalb eine unmittelbare fernmündliche Auskunft dringlich ist und eine schriftliche Beantwortung nicht mehr ausreicht. Das Vorbringen des Anrufers ist für Nachweiszwecke aktenkundig zu machen; insoweit verweise ich auf die Ausführung im 5. Tätigkeitsbericht, S. 54.

4.14.5. Erfassung total geschädigter Unfallfahrzeuge

Der Bundesminister für Verkehr plant eine Verlautbarung in seinem Amtsblatt aufzunehmen, wonach durch einen Unfall total geschädigte Personenkraftwagen vom Versicherer dem Kraftfahrtbundesamt gemeldet werden. Das Kraftfahrtbundesamt legt aufgrund dieser Meldung einen Suchvermerk an. Wird nun ein Fahrzeug mit denselben Fahrzeugdaten nach dem Unfalldatum wieder zugelassen, so unterrichtet das Kraftfahrtbundesamt das für den neuen Zulassungsbereich zuständige Landeskriminalamt. Aufgrund dieser Informationen veranlaßt das Landeskriminalamt unter Beteiligung der Zulassungsstelle eine Überprüfung des Falles. Zweck dieser Erfassung soll es sein, den Mißbrauch von Fahrzeugbriefen zu verhindern oder aufzuklären. Die zuständigen Behörden behaupten, Anhaltspunkte dafür zu haben, daß Fahrzeugbriefe von Unfallfahrzeugen unrechtmäßig verwendet werden. So wird zum Beispiel das unfallgeschädigte Fahrzeug nicht endgültig abgemeldet, sondern nur vorübergehend stillgelegt. Fahrzeugbrief und Schrottfahrzeug werden von Hehlern aufgekauft. Ein ähnliches wie das in dem Fahrzeugbrief beschriebene Fahrzeug wird gestohlen und mit den Daten des Fahrzeugbriefes in Übereinstimmung gebracht. Lassen sich die Kraftfahrzeugzulassungsstellen wie in Bayern wegen Einsparung von Verwaltungskosten die Fahrzeuge nicht vorführen, besteht das Risiko, daß solche Fahrzeuge dann unbeanstandet wieder zugelassen werden.

Für das Anliegen, den Mißbrauch total geschädigter Unfallfahrzeuge zu verhindern, habe ich volles Verständnis. Allerdings habe ich gegen die vollständige Erfassung aller Unfallfahrzeuge Bedenken angemeldet. Weil nach Ausssagen

des Bundesministers für Verkehr davon auszugehen ist, daß in den weitaus meisten Fällen eine rechtmäßige Wiederherstellung des Fahrzeugs und eine rechtmäßige Wiederzulassung vorliegt, ist die Übermittlung aller Neuzulassungen von Unfall-Kraftfahrzeugen an das zuständige Landeskriminalamt zu dessen Aufgabenerfüllung nicht erforderlich. Im übrigen werden dadurch die vielen Fahrzeughalter, die eine rechtmäßige Wiederzulassung vornehmen, zumindest vorübergehend als einer Straftat Verdächtige behandelt. Ich habe daher die Ansicht vertreten, daß zunächst die zuständige Kfz-Zulassungsstelle gemäß § 26 StVZO anhand der Papiere und der Kfz-Kartei festzustellen hat, ob das anzumeldende Kraftfahrzeug tatsächlich identisch mit dem Unfallfahrzeug ist. Erst wenn sich bei der Überprüfung der Verdacht einer mißbräuchlichen Verwendung der Fahrzeugpapiere ergeben sollte, darf die Kfz-Zulassungsstelle ausschließlich diese Fälle an die zuständige Strafverfolgungsbehörde übermitteln.

Das Bayer. Staatsministerium des Innern hat daraufhin vorgeschlagen, daß das Kraftfahrtbundesamt von der Übermittlung unfallgeschädigter Kraftfahrzeuge an das jeweils zuständige Landeskriminalamt nicht nur in den Fällen der Identität zwischen früherem und neuem Halter des als total geschädigt eingestuften Kraftfahrzeugs abgesehen wird, sondern auch dann, wenn aufgrund der aktenmäßigen Überprüfung durch die Zulassungsstelle die rechtswidrige Verwendung des Kraftfahrzeugbriefes ausgeschlossen werden kann. Hiermit ist einem wesentlichen Teil meines Anliegens Rechnung getragen.

## 4.15. **Einzelfragen**

### 4.15.1. Ergänzung der staatlichen Vordruckrichtlinien um Hinweise auf den Datenschutz

In den Jahren 1982 und 1983 hatte ich das für die staatlichen Vordruckrichtlinien zuständige Referat des Bayer. Staatsministeriums des Innern wiederholt gebeten, diese Richtlinien um eindeutige Hinweise zum Vollzug des Art. 16 Abs. 2 BayDSG zu ergänzen. Nach dieser Vorschrift des BayDSG muß der Betroffene bei der Datenerhebung auf die Vorschrift, die ihn zur Angabe der Daten verpflichtet, oder auf die Freiwilligkeit der Angabe ausdrücklich hingewiesen werden. Aufgrund der Ausführungen des Bundesverfassungsgerichts im Volkszählungsurteil zur notwendigen Transparenz der Datenerhebung für die Bürger und zur Klarstellung von Datenerhebungs- und Verwendungszwekken kommt dem Hinweis auf Datenerhebungsformularen nunmehr erhöhte Bedeutung zu. Eine Anpassung der Vordruckrichtlinien erscheint daher für Behörden, wie auch für Formularverlage, besonders dringlich.

### 4.15.2. Kaufpreissammlungen nach dem Bundesbaugesetz

Über die Änderung der Verordnung über die Gutachterausschüsse, die Kaufpreissammlungen und Bodenrichtwerte nach dem Bundesbaugesetz durch die am 1. Juli 1982 in Kraft getretene Änderungsverordnung (BayGVBl. 1982, S. 335) wurde im 5. Tätigkeitsbericht referiert (Ziff. 4.9.2, S. 39/40). Eine Stadt stellte hierzu die Frage, ob der Datenschutzbeauftragte die Nutzung von Daten aus der Kaufpreissammlung für sonstige kommunale Zwecke, z.B. die Nutzung der Angabe über die Grundstücksgröße für die Erstellung von Bescheiden über Erschließungs- und Kanalherstellungsbeiträge für zulässig halte. Ich habe hierzu die Ansicht vertreten, daß die Verordnung auch in der geänderten Fassung keine Befugnis zur Nutzung über die im neuen § 11 a genannten Zwecke (Wertermittlung) hinaus gibt.

Im 5. Tätigkeitsbericht war festgehalten, daß die Oberste Baubehörde im Bayer. Staatsministerium des Innern zu prüfen beabsichtigte, ob die Speicherung von Namen und Anschriften von Personen aus den Kaufverträgen in die eigentliche Kaufpreissammlung (Karteikarte) übernommen werden müsse. Eine Umfrage der Obersten Baubehörde führte zu dem Ergebnis, daß in Bayern etwa die Hälfte der Kaufpreissammlungen ohne Namensangabe von Käufern oder Verkäufern geführt wird. Ich habe deshalb unter dem Gesichtspunkt der Erforderlichkeit der Datenspeicherung in der der Einsichtnahme unterliegenden Kaufpreissammlung die Ansicht vertreten, daß nunmehr dem Erlaß einer entsprechenden Verwaltungsvorschrift, die den grundsätzlichen Verzicht auf die Nennung von Namen und Anschrift festlegt, nichts mehr im Wege stehen dürfte. Dabei habe ich auch an den erbetenen Erlaß einer Ausführungsvorschrift zu § 11 a der Verordnung erinnert (Einzelheiten hierzu hatte ich im 5. Tätigkeitsbericht dargestellt, siehe dort a.a.O.). Der Vorgang ist noch nicht abgeschlossen.

### 4.15.3. Mitteilung personenbezogener Daten im Zusammenhang mit Bußgeldentscheidungen durch die Kreisverwaltungsbehörde an die Handwerkskammer

Eine Handwerkskammer hatte ein Landratsamt gebeten, auch in den Fällen, in denen ein Bußgeldverfahren wegen unerlaubter Handwerks ausübung und Schwarzarbeit nicht aufgrund einer Anzeige durch die Handwerkskammer eingeleitet wurde, über die Personen, gegen die das Verfahren eingeleitet wurde, informiert zu werden. Ich habe gegenüber dem Landratsamt, das mich um Stellungnahme bat, die Ansicht vertreten, daß die gewünschte Datenübermittlung rechtlich keine Stütze findet. Weder die Handwerksordnung noch das Gesetz zur Bekämpfung der Schwarzarbeit, noch die gemeinsame Bekanntmachung der Bayer. Staatsministerien des Innern, der Finanzen, für Wirtschaft und Verkehr und für Arbeit und Sozialordnung vom 15. Juli 1982 (Nr. 4390 – ha – 23401), noch das Ordnungswidrigkeitengesetz und die entsprechend anzuwendenden Richtlinien rechtfertigen diese Begehren. Dabei war der mitgeteilte Sachverhalt nicht unmittelbar nach den Vorschriften des Bayer. Datenschutzgesetzes zu beurteilen, da es sich bei den erbetenen Mitteilungen nicht um eine Übermittlung aus einer Datei handeln würde, sondern um eine Übermittlung personenbezogener Daten aus Einzelakten. Zur Klärung der Frage, ob eine Weitergabe solcher Daten aus Akten mit dem Schutz der Persönlichkeit aus Art. 2 Abs. 1, Art. 1 Abs. 1 GG in Widerspruch steht, können aber die Grundgedanken der Datenschutzgesetze – im vorliegenden Fall aus Art. 17 BayDSG – entsprechend herangezogen werden. Es kommt danach aus der Sicht des Datenschutzes darauf an, inwieweit die Mitteilung personenbezogener Daten zur rechtmäßigen Erfüllung der durch Rechtsnorm der übermittelnden Stelle oder der Handwerkskammer zugewiesenen Aufgaben erforderlich ist (vgl. Art. 17 Abs. 1 BayDSG). Ergibt sich bereits aus der Prüfung des Erforderlichkeitsgrundsatzes, daß eine Datenübermittlung mangels Erforderlichkeit nicht verhältnismäßig und damit nicht zulässig sein kann, erübrigt sich die neuerdings, nach dem Volkszählungsurteil des Bundesverfassungsgerichtes wohl erforderliche Prüfung, ob mit der Datenübermittlung auch eine unverhältnismäßige Änderung des Nutzungszwecks der Daten eintreten könnte.

Im einzelnen habe ich zu der erbetenen Übermittlung folgendermaßen Stellung genommen:

1. Mitteilung personenbezogener Daten im laufenden Verfahren

   Nr. 185 Abs. 1 Satz 1 der Richtlinien für Straf- und Bußgeldverfahren (RiStBV) gewährt neben anderen Behörden auch öffentlich-rechtlichen Körperschaften auf Ersuchen Akteneinsicht während des laufenden Verfahrens, wenn diese ihr berechtigtes Interesse darlegen. Ein solches berechtigtes Interesse kann die Handwerkskammer aber nicht geltend machen. Zwar gehört es nach § 91 Abs. 1 Nr. 1 der Handwerksordnung (HandwO) zu den Aufgaben der Handwerkskammer, die Interessen des Handwerks, worunter auch die Bekämpfung der Schwarzarbeit fällt, zu fördern; diese allgemeine Aufgabenzuweisung umfaßt aber noch nicht ein derartiges Informationsrecht der Handwerkskammer gegenüber der Kreisverwaltungsbehörde. Vielmehr müßte die Kreisverwaltungsbehörde ihrerseits befugt sein, der Handwerkskammer die gewünschten personenbezogenen Daten zu übermitteln. Das heißt aber, daß die Mitteilung der personenbezogenen Daten nicht nur der Aufgabenerfüllung des Empfängers dienen, sondern hierfür auch erforderlich und verhältnismäßig sein muß. Dies muß in jedem Einzelfall geprüft werden. Kommt die Kreisverwaltungsbehörde im Rahmen dieser Überprüfung zu dem Ergebnis, daß eine Einschaltung der Handwerkskammer erforderlich ist, so bleibt es ihr unbenommen, die Handwerkskammer in das laufende Bußgeldverfahren einzuschalten und diese nach § 91 Abs. 3 HandwO zu hören bzw. als sachverständigen Gutachter (§ 91 Abs. 1 Nr. 2 HandwO) einzuschalten. Ein Rechtsanspruch der Handwerkskammer auf eine bestimmte Form der Interessenvertretung, wie eine automatische Mitteilung durch die Kreisverwaltung, ergibt sich nicht aus § 91 Abs. 1 Nr. 1 HandwO (vgl. Eyermann/Fröhler/Honig HandwO Nr. 3 zu § 91). Ein solcher ergibt sich auch nicht aus § 114 HandwO, der die Behörden innerhalb ihrer Zuständigkeit verpflichtet, den im Vollzug der HandwO an sie ergehende Ersuchen der Handwerkskammern zu entsprechen. Die Rechts- und Amtshilfepflicht findet ihre Grenze mit der Amtsverschwiegenheit der betreffenden Behörde (vgl. Eyermann/Fröhler/Honig a.a.O. Nr. 1 zu § 114). Auch § 91 Abs. 3 HandwO gibt kein derartiges Informationsrecht. Aus dieser Vorschrift läßt sich kein Rechtsanspruch auf Anhörung ableiten, sondern nur ein Recht auf fehlerfreie Ermessensentscheidung. Entscheidungsgegenstand ist aber, ob die Handwerkskammer gehört, nicht ob sie informiert wird. Ein Anspruch auf Auskunft im Sinne eines berechtigten Interesses ergibt sich auch nicht aus § 2 a des Gesetzes zur Bekämpfung der Schwarzarbeit oder aus Nr. 4 der oben zitierten gemeinsamen Bekanntmachung. Die Vorschrift regelt die Zusammenarbeit der Behörden bei der Bekämpfung von Schwarzarbeit und enthält in Abs. 2 eine Unterrichtungspflicht der zuständigen Behörden untereinander, die die Weitergabe personenbezogener Daten zuläßt. Zuständige Behörden sind, wie sich aus § 2 a Abs. 2 des Gesetzes zur Bekämpfung der Schwarzarbeit ergibt, die für die Verfolgung und Ahndung zuständigen Behörden. Dies sind nicht die Handwerkskammern, so daß eine Unterrichtungspflicht ihnen gegenüber entfällt. Auch Nr. 3.6 der gemeinsamen Bekanntmachung, auf die sich die Handwerkskammer stützte, begründet kein berechtigtes Interesse an den gewünschten Mitteilungen personenbezogener Daten. Diese Verwaltungsvorschrift enthält nur die Aufforderung an die Handwerkskammern, die Behörden bei der Bekämpfung der Schwarzarbeit zu unterstützen, regelt aber nicht den umgekehrten Fall.

2. Auskunft nach Rechtskraft über Ausgang des Verfahrens

   a) Ist das Verfahren eingestellt worden, so ist nach Nr. 185 Abs. 2 Satz RiStBV die Akteneinsicht zu versagen, wenn dem Interesse an der Einsichtnahme ein höheres Interesse des Betroffenen, namentlich an seiner Resozialisierung entgegensteht. Bei Einstellung des Bußgeldverfahrens wird dem Interesse an der Einsichtnahme und Auskunft regelmäßig ein höheres Interesse des Betroffenen gegenüberstehen, denn die Mitteilung personenbezogener Daten dieser Betroffenen könnte dazu führen, daß sie als potentielle „schwarze Schafe" geführt würden, obwohl das Verfahren eingestellt wurde.

   b) Abschluß durch Bußgeldbescheid

      Soweit die Kreisverwaltungsbehörde während des Verfahrens eine Beteiligung der Handwerkskammer im oben dargelegten Sinne nicht für erforderlich gehalten hat, kann nach Nr. 185 Abs. 2 Satz 1 RiStBV ebenfalls nicht zwingend auf ein berechtigtes Interesse der Handwerkskammer geschlossen werden, das die Mitteilung personenbezogener Daten rechtfertigen würde.

   Selbstverständlich ergibt sich eine andere Beurteilung, wenn das Verfahren aufgrund einer Anzeige der Handwerkskammer eingeleitet worden ist, bzw. die Handwerkskammer an dem Verfahren beteiligt war. Als Verfahrensbeteiligte kann die Handwerkskammer ein berechtigtes Interesse geltend machen, das Ergebnis des Verfahrens zu erfahren.

   Auch wenn dies nicht zutrifft, verkenne ich – trotz der datenschutzrechtlichen Beurteilung – nicht die Notwendigkeit einer freilich allgemeinen Unterrichtung der Handwerkskammer durch die Kreisverwaltungsbehörde. Ich habe daher vorgeschlagen, die Handwerkskammer in periodischen Abständen darüber zu unterrichten, wie viele Bußgeldverfahren in welchem Handwerkszweig und mit welchem Ergebnis durchgeführt worden sind. Die Weitergabe dieser Informationen ist durch die Aufgabenzuweisung des § 91 Abs. 1 Nr. 1 HandWO gerechtfertigt. Personenbezogene Daten werden dabei nicht mitgeteilt. Deshalb dürften Handwerkszweige mit sehr wenigen praktizierenden Handwerkern wegen der daher gegebenen Reidentifizierungsmöglichkeit hiervon nicht umfaßt sein. In meiner abschließenden Stellungnahme gegenüber dem Bayer. Staatsministerium für Wirtschaft und Verkehr habe ich angeregt, für die Zusammenarbeit zwischen Handwerkskammern und Kreisverwaltungsbehörden eine Verwaltungsvorschrift zusammen mit dem Bayer. Staatsministerium des Innern zu erarbeiten, denn bei der Bearbeitung des Falls ist bekanntgeworden, daß in Bayern keine einheitliche Praxis bei der Benachrichtigung durch die Kreisverwaltungsbehörde an die Handwerkskammern besteht. Zum Teil findet keine offizielle Benachrichtigung statt, zum Teil erhalten Handwerkskammern einen Abdruck der Bußgeldbescheide, dies

teilweise erst nach Rechtskraft; zum Teil erhalten die Handwerkskammern auf Ersuchen eine anonymisierte Zusammenstellung in periodischen Abständen, aus der hervorgeht, wie viele Bußgeldverfahren in welchem Handwerk eingeleitet und wie diese abgeschlossen wurden.

Das Bayer. Staatsministerium für Wirtschaft und Verkehr hat mich inzwischen über den Entwurf einer gemeinsamen Bekanntmachung unterrichtet, der vorsieht, daß die zuständige Behörde die jeweilige Handwerkskammer vom Erlaß eines Bußgeldbescheides durch Übersendung eines Abdrucks nur dann zu unterrichten hat, wenn die Handwerkskammer Anzeige erstattet hatte oder im Bußgeldverfahren beteiligt war.

## 5. Bericht zur Datenschutzkontrolle im technischen und organisatorischen Bereich

### 5.1. Technische und organisatorische Grundsatzfragen

#### 5.1.1. Grundsätze zur Revision der Datenverarbeitung

Die Revision steht manchmal vor großen Problemen, wenn es darum geht, die Ordnungsmäßigkeit der automatisierten Datenverarbeitung zu prüfen, nicht nur deshalb, weil es keine verbindlichen Vorschläge für Grundsätze zur ordnungsgemäßen Datenverarbeitung (GoDV) gibt. Die automatisierte Datenverarbeitung ist heute weit verzweigt. Sie umfaßt die Sachbearbeitung, beispielsweise die Dialogeingabe am Bildschirm, ebenso wie die Programmierung und Maschinenbedienung. Für die Revisionsfähigkeit der automatisierten Datenverarbeitung ist es aber unerläßlich, daß sich ein sachverständiger Dritter in einer angemessenen Zeit zurechtfindet. Für den Außenstehenden müssen deshalb die Datenflüsse und die Schnittstellen für manuelle Eingriffe erkennbar, die Dokumentation der Datenverarbeitung aussagefähig und Maßnahmen getroffen sein, die einem unkontrollierten Systemeingriff vorbeugen. Grundlage für die Revision der DV sind

- die Dokumentation,
- die Verfahrens- bzw. Programmfreigabe,
- der Terminplan und
- das Maschinenablaufprotokoll.

Dokumentation

Eine wesentliche Voraussetzung für eine nachträgliche Revision der Datenverarbeitung ist das Vorhandensein einer ausreichenden Dokumentation. Auf dem Softwaremarkt werden mittlerweile eine Vielzahl von Dokumentationshilfen angeboten. Aus der Sicht der Revision sollte die Dokumentation folgende Bestandteile umfassen:

- die Bibliotheksakte
- die Programmakte
- die Bedienungsakte
- die Dateiakte
- die Copyakte
- die Bildschirmformatakte.

Die Bibliotheksakte besteht aus dem Programmverzeichnis, dem Phasenverzeichnis einschließlich der Binderlisten, dem Dateiverzeichnis, dem Verzeichnis der Formatnamen, dem Verzeichnis der Transaktionscodes, der Querverweisliste und der Freigabemitteilungen, wobei es bei Änderungen unbedingt notwendig ist, daß Ursache und Art der Änderungen klar beschrieben sind. Das Programmverzeichnis enthält neben dem Programmnamen eine allgemein verständliche Programmbeschreibung, die Versionsnummer und das Datum der Freigabe. Das Verzeichnis der Transaktionscodes muß unbedingt Angaben über die Transaktionsberechtigungen enthalten. Die Querverweislisten, die möglichst aus dem SOURCE-CODE generiert werden, sollen u.a. Aufschluß darüber geben, welches Programm welche Programme aufruft, welche Dateien verarbeitet und welche Copy-Elemente benützt.

Zur Programmakte gehören neben dem Logbuch eine Programmbeschreibung mit Ablaufplan, eine Aufstellung aller Nachrichten und die Programmliste.

Die Bedienungsakte setzt sich neben dem Logbuch aus dem Datenflußplan, einem Anlagenbelegungsschema, einer Zusammenstellung der Ablaufsteuer- bzw. Parameterkarten und einer Aufstellung aller Nachrichten, die an der Konsole erscheinen, zusammen.

Die Dateiakte beteht aus der Datei- und der Datensatzbeschreibung.

Der Bildschirmformatakte gehören neben einem Logbuch ein Verzeichnis aller Bildschirmformate, die Formatbeschreibung inklusive eines Musters und deren Aufrufmodalitäten an.

Die früheren Versionen eines Programmes sollten zurückverfolgbar sein. Auch hier gibt es geeignete Software, die diese Forderungen – ohne manuellen Eingriff – automatisiert unterstützt. Man muß sich aber darüber im klaren sein, daß die Systemumgebung infolge der häufigen Wechsel der Betriebssystemsversionen und der Hardwarekonfiguration nicht reproduzierbar ist. Ein Ablauf eines Programms zu den Bedingungen, wie sie sich zu einem bestimmten Zeitpunkt in der Vergangenheit darstellten, also nicht überall möglich ist.

Freigabe

Die Art des Freigabeverfahrens ist grundsätzlich schriftlich festzulegen. Die Freigabe bedeutet die Schnittstelle von Programm- bzw. Verfahrenserstellung zum Verfahrenseinsatz. Erst nach Prüfung der Verarbeitungsergebnisse des Abschlußtests oder Piloteinsatzes durch die Fachabteilung kann die Freigabe eines Verfahrens erfolgen. Eine Funktionstrennung von Programmierung und Freigabe durch die Fachabteilung ist unabdingbar. Unter diesen Voraussetzungen werden Manipulationen am Programmcode erheblich erschwert.

Nach der Freigabe, also der Übernahme der Programme in die Produktionsbibliothek, muß die unkontrollierte Eingriffsmöglichkeit des Programmierers auf die ihm vertrauten Programme unterbunden werden. Dabei empfiehlt es sich, daß die Programme in gesonderten Produktionsbibliotheken abgespeichert werden, die zusätzlich durch Paßworte gegen den Zugriff Unbefugter geschützt sind und nur zur Programmausführung (FETCH) aufgerufen werden können.

Alle Programm-/Verfahrensänderungen sind von der Fachabteilung schriftlich zu beantragen, so daß ein Programmierer stets nur auf Veranlassung der Fachabteilung tätig wird. Durch den Einsatz von geeigneter Software lassen sich Umfang und Art von Änderungen im Programm-Code bzw. in einer Änderungsdatei nachweisen.

Trotzdem bietet auch ein ausgeklügeltes Freigabeverfahren keine Garantie gegen solche Manipulationen von Programmierern bei der Programmerstellung, die sich erst im Effek-

tivbetrieb auswirken. Durch eine regelmäßige Kontrolle der Produktionsläufe läßt sich aber die Wahrscheinlichkeit, solche Manipulationen aufzudecken, erhöhen.

Die Verwendung von Paßworten, die regelmäßig geändert werden, eine weitreichende Funktionstrennung sowie eine generelle Trennung von Programmentwicklung und Produktion bieten allerdings ein hohes Maß an Sicherheit gegen Übergriffe Unbefugter. Bei großen Anwendern wird das häufig hardwaremäßig erreicht, indem eine Maschine ausschließlich für die Programmerstellung und -pflege genutzt wird.

Terminplan

Die Ordnungsmäßigkeit der Datenverarbeitung verlangt auch eine rechtzeitige Vorbereitung und Planung aller Aufgaben, die maschinell abgewickelt werden und die Verarbeitung von Echtdaten betreffen. Dabei ist es unerheblich, in welchen Zeiträumen geplant wird. Der Terminplan für solche Produktionsaufgaben sollte auch dann, wenn ein automatisiertes Produktionssteuerungs- und -kontrollsystem eingesetzt wird, dem Rechenzentrum tage- oder wochenweise in gedruckter Form vorliegen. Die Maschinenbedienung notiert in dem Plan, wann die jeweilige Aufgabe mit welchem Ergebnis abgelaufen ist, oder ob Wiederholungsläufe notwendig wurden. In solchen Fällen ist die Angabe von Gründen zwingend erforderlich. Zur Kontrolle zeichnet die Arbeitsnachbereitung, sofern die Größe einer Institution eine solche rechtfertigt, gegen.

Die Steueranweisungen, die die DV-Anlage für den Ablauf der Aufgaben benötigt, werden – wiederum eine entsprechende Größe des Rechenzentrums vorausgesetzt – von einer unabhängigen Stelle, beispielsweise der Arbeitsvorbereitung, in Prozeduren bereitgestellt, die zweckmäßigerweise gegen Änderungen paßwortgeschützt sind, so daß diese vom Maschinenbediener zwar aufgerufen, jedoch nicht verändert werden können. Selbstverständlich sind solche Prozeduren Bestandteil der Dokumentation und jede Änderung muß in Bezug auf Art und Umfang über einen gewissen Zeitraum zurückverfolgbar sein.

Auch hier gewinnt das Prinzip der Funktionstrennung für die Sicherheit der Datenverarbeitung große Bedeutung.

Maschinenablaufprotokoll

Eine Kontrollierbarkeit der Arbeitsabwicklung ist eigentlich nur dann gegeben, wenn maschinelle Aufzeichnungen darüber vorliegen. Diese Aufzeichnungen sind vom Betriebssystem zu führen und sind als Maschinenablaufprotokoll bekannt. Die Brauchbarkeit solcher Aufzeichnungen steht und fällt jedoch mit der Zwangsläufigkeit der Protokollierung. Werden die Parameter für die Erzeugung des Maschinenablaufprotokolls geändert, so muß diese Operation im Protokoll ebenfalls erscheinen. Selbstverständlich ist diese Protokolldatei gegen Manipulationen zu schützen. Aus dem Maschinenablaufprotokoll muß erkennbar sein, welche Aufgaben zu welcher Zeit abliefen und auf welche Datenbestände zugegriffen haben und von wem veranlaßt wurden.

Bei der Auswertung des Maschinenablaufprotokolls geht es – wenn sie regelmäßig stattfindet – vor allem darum, Abweichungen und Singularitäten im Ablauf rechtzeitig zu finden, um diese dann im Nachhinein aufklären zu können.

In erster Linie ist an folgende maschinelle Standardauswertungen zu denken:

1. Umbenennung von Dateien, Produktionsphasen, Prozeduren und Dienstprogrammen,
2. Änderungen an Produktionsprogrammen und Prozeduren,
3. Änderungen der Paßworte, wobei die Paßworte selbst nicht protokolliert werden dürfen,
4. Benutzung von bestimmten Dateien, Programmen und Dienstprogrammen,
5. Kontrolle der Ausführung bestimmter Verfahren sowie der Anzahl der Druckvorgänge bei bestimmten Verfahren,
6. Kontrolle der Paßwort-Benutzung in bestimmten Zeiträumen, um eventuelle unberechtigte Paßwort-Benutzungen feststellen zu können.
7. Auflistung der Datenstationen, von denen bestimmte Verfahren gestartet wurden.
8. Kontrolle der Anschaltzeiten bestimmter Datenstationen, um die Einhaltung bestehender Signoff-Regelungen zu überprüfen.
9. Auflistung aller Verfahren, die vom System mit System-Codes abgebrochen wurden. In erster Linie sollen diese Auswertungen des Maschinenprotokolls die Ordnungsmäßigkeit der Arbeitsabwicklung belegen und die Richtigkeit des manuell geführten Logbuches bestätigen. Derartige Unterlagen können als Beweismittel für die Ordnungsmäßigkeit der Maschinenbedienung in Fällen von Sicherheitsverletzungen äußerst nützlich sein.

Zusammenfassung

Da es keine Garantie für die absolute Richtigkeit eines DV-Programmes gibt und die Abhängigkeit von der Datenverarbeitung ständig wächst, ist die Kontrollierbarkeit der DV-Systeme dringend erforderlich.

Die Revisionsfähigkeit der Datenverarbeitung setzt ein Zusammenwirken der oben beschriebenen Maßnahmen voraus. Um eine wirksame Prüfung ex post sicherzustellen, sind zusätzlich noch Regelungen über sinnvolle Aufbewahrungsfristen notwendig. Schließlich ist nicht außer acht zu lassen, daß besondere Risiken beim Einsatz von Fremdsystemen entstehen, da diese vom Benutzer oft nicht überblickbar sind und der Benutzer den vollen Funktionsumfang der Systeme häufig nicht kennt. Das trifft vor allem für Datenfernverarbeitungssysteme zu.

Die bisher bekanntgewordenen Fälle der Computerkriminalität wurden häufig dadurch begünstigt, daß die Arbeit eines einzelnen nicht mehr oder nur noch mit großem Aufwand überprüfbar ist. Infolge der Kostenexplosion im Personalbereich wurde durch den Einsatz von ADV-Systemen rationalisiert, so daß der Aufgabenbereich eines Sachbearbeiters anwachsen konnte. Zwar gab es auch in der konventionellen Datenverarbeitung Mißbrauchsmöglichkeiten, nur war das Risiko entdeckt zu werden damals höher. Ein Buchhalter „Computer" erkennt kriminelle Handlungen von Sachbearbeitern nicht.

Bei großen Institutionen bietet die konsequente Einhaltung einer Funktionstrennung und des 4-Augen-Prinzips immer noch ein wirksames Mittel zur gegenseitigen Kontrolle, weil sich hier ein altes Prinzip bewahrheitet, daß der Mißbrauch um so schwieriger wird, je mehr Personen er verheimlicht werden muß.

Die Hersteller von DV-Anlagen sind angehalten dem Anwender Möglichkeiten zu eröffnen Informationen über die Anlagenbenutzung systemseitig aufzuzeichnen. Darüberhinaus ist eine Software zur Verfügung zu stellen, die parametergesteuert das Maschinenlogging nach den oben beschriebenen Fragestellungen auswertet, so daß eine Eigenprogrammierung möglichst unterbleiben kann.

5.1.2. Mikroverfilmung

Bei der Mikroverfilmung unterscheidet man zwei Arten, den Computer-Output on Mikrofilm (COM) und die Schriftgutverfilmung. Im COM-Verfahren werden druckaufbereitete Daten vom Magnetband auf das Medium „Mikrofilm" – meist im Mikrofiche-Format – übertragen. COM-Verfahren arbeiten meist off-line, es sind jedoch auch On-line-Verfahren gebräuchlich. Um Papierkosten zu sparen, werden in manchen Rechenzentren die Ergebnisse von Testläufen auf Mikrofiche ausgegeben. Die On-line-Ausgabe auf Mikrofiche ist obendrein wesentlich schneller als die Papierausgabe über den Schnelldrucker. Bei der Schriftgutverfilmung werden Schriftstücke blattweise, häufig vor- und rückseitig in einem Arbeitsgang, verfilmt. Werden abgeschlossene, bereits archivierte Vorgänge verfilmt, spricht man von einer Passiv-Verfilmung, wird eine laufende Akte auf Mikrofilm übernommen, so wird das als Aktiv-Verfilmung bezeichnet. Als Aufnahmemedium dient bei der Schriftgutverfilmung in erster Linie der Rollfilm, der je nach der Art des Wiedergewinnungsverfahrens auch in ein „Fiche-Skelett" eingetascht werden kann. Das Duplikat, das für Sicherheitszwecke angefertigt wird, bleibt jedoch im Rollfilmform erhalten.

Befindet sich das Schriftgut auf Mikrofilm, ist zur Wiederauffindung der einzelnen Vorgänge eine Suchkartei notwendig. Zu diesem Zweck wird je Vorgang eine Karteikarte angelegt, auf der die Nummer der Filmrolle und die Position des Beginns des Vorgangs notiert sind. Viele Stellen verfilmen auch diese Suchkartei. Die Position des Vorgangs auf dem Film wird über das mechanische Zählwerk des Rollfilm-Lesegerätes bestimmt. Bei der Aktiv-Verfilmung werden meist alle Mikrofilmstücke eines Vorgangs in einem Jacket aneinandergereiht. Die Jackets haben DIN A 6-Format und können auf der Stirnseite beschriftet werden, so daß eine alphabetische oder sonstige Sortierung möglich ist. Darüber hinaus enthalten die Jackets Hinweise auf die Fundstellen in den Duplikaten des Sicherheitsfilmes. Wird bei der Aktiv-Verfilmung die Rollfilmorganisation beibehalten, so ist das nur sinnvoll, wenn ein automatisiertes System den Bestand verwaltet, da ein Vorgang auf mehrere Filmrollen verteilt sein kann und das manuelle Auffinden der Vorgangsteile den Rationalisierungseffekt zunichte machen würde (z.B. Verfahren „Oracle" - binärcodierte Mikrofilme ermöglichen die Verwaltung und Wiederauffindung von unsortiertem Schriftgut).

Wegen der hohen Anschaffungskosten für die erforderlichen Geräte wird die off-line COM-Verfilmung meistens Serviceunternehmen übertragen. Der Anschaffungspreis für Kameras zur Schriftgutverfilmung liegt jedoch wesentlich darunter, so daß im Einzelfall die Eigenverfilmung durchaus wirtschaftlich sein kann. So betreiben manche Behörden eigene Mikrofilmstellen, was aus der Sicht des Datenschutzes sowohl rechtlich als auch unter dem Gesichtspunkt der Datensicherung weniger problematisch ist als eine Mikroverfilmung außer Haus. Die Mikroverfilmung außer Haus wird in vielen Fällen zwar die wirtschaftlichere Art darstellen. Der Auftraggeber muß sich allerdings der Risiken, die mit der Auftragsvergabe an Privatunternehmen verbunden sein können, bewußt sein und gegebenenfalls Maßnahmen zur Risikominderung beim Auftragnehmer fordern.

Die Verfilmung von Schriftgut läßt sich in folgende Arbeitsschritte einteilen:

Aufbereitung und ggf. Durchnumerierung des Schriftgutes, Verfilmung in der Durchlaufkamera, Filmentwicklung mit anschließender Lesbarkeitskontrolle, Aufbereitung und Verwaltung des Filmgutes sowie die Vernichtung des verfilmten Schriftgutes.

Bei jedem Arbeitsschritt treten Risiken auf, insbesondere bei der Verfilmung außer Haus, wie unzulässige Offenbarung und unberechtigte Nutzung des Schriftgutes oder der Mikrofilme, unvollständige Verfilmung, unberechtigte Anfertigung von Kopien der Mikrofilme, Transportrisiken, unvollständige und schlechte Entsorgung des verfilmten Schriftgutes. Als Maßnahmen zur Risikoverminderung gelten die Aufbereitung des zu verfilmenden Schriftgutes durch eigenes Personal, die sorgfältige Auswahl der Firmen nach dem gebotenen Sicherheitsstandard, die Wahl eines örtlich entfernten Auftragnehmers, die Kontrolle des Dupliziervorganges bzw. die Führung von Protokollen über den Dupliziervorgang und der Transport des Schriftgutes durch eigenes Personal. Bei der Verfilmung von sensiblem Material ist grundsätzlich zu überlegen, ob einzelne Arbeitsschritte nicht von der Behörde selbst erledigt werden können, oder die Verfilmung vor Ort beim Auftraggeber mit mobilen Kameras erfolgen kann. Dies gilt insbesondere, wenn sonst unter Umständen eine unzulässige Offenbarung personenbezogener Daten anzunehmen wäre (z.B. bei Daten die der ärztlichen Schweigepflicht unterliegen).

Ein Risiko ganz besonderer Größe stellt die Duplizierung von verfilmten Unterlagen dar. Während die Duplizierung eines Rollfilms in der Praxis nur eine geringe Bedeutung hat, da bei der Aufnahme bereits ein Duplikatfilm erzeugt werden kann, ist die Duplizierung eines Mikrofiches sehr gebräuchlich, zumal die Duplizierung eines Fiches im Kontaktverfahren lediglich einige Sekunden dauert. Da die gängigsten im Handel angebotenen Geräte keine Zählkontrolleinrichtung besitzen, die anzeigt, wieviele Kopien angefertigt wurden, ist ein unbefugtes Kopieren nur durch organisatorische Maßnahmen festzustellen, etwa durch abgezählte Vorgabe des Filmmaterials, Rückgabe fehlerhafter Kopien. Es gibt Verfahren, die Kopien erzeugen, von denen keine weiteren lesbaren Kopien mehr angefertigt werden können. Im übrigen verschlechtert sich die Lesbarkeit, wenn Kopien von Kopien gezogen werden.

5.1.3. Neubaumaßnahmen

Auch in einer Zeit der knappen Haushaltsmittel ist die Zahl der Neubaumaßnahmen beachtlich. Aus der Sicht des Datenschutzes ist das erfreulich, denn in Neubauten lassen sich Datensicherungsmaßnahmen kostengünstiger realisieren, als durch den oft finanziell aufwendigen Umbau bestehender Gebäude.

So nahm im Berichtszeitraum die Zahl der Beratungen bei Neubaumaßnahmen weiter zu. In vielen Fällen konnten Verbesserungsvorschläge für Datensicherungsmaßnahmen gegeben werden. Einige der vorgelegten Baupläne enthielten bereits ausgereifte Lösungen bezüglich der räumlichen Sicherung solcher Bereiche, in denen personenbezogene Daten automatisiert gespeichert und verarbeitet werden.

Im Vergleich zu früheren Zeiten sind die heutigen Datenverarbeitungsanlagen meist so beschaffen, daß eine Bedienung von Zentraleinheit und Datenspeicher – soweit es sich um Festplatten handelt – nur noch in Ausnahmefällen notwendig ist. Dieser Teil der Hardware, das Herzstück der Datenverarbeitung, dessen Ausfall schlimme Folgen hätte, kann deshalb in solche Räume verlegt werden, die von außen nicht zugänglich sind und deren Zugang innerhalb des Gebäudes zusätzlich gesichert werden kann. Hingegen können der Bedienungsplatz (Konsole) und die peripheren Geräte, die u.a. der Datensicherung dienen (Magnetbandgeräte, Diskettenlaufwerke u.a.), in weniger geschützte Räumlichkeiten verlegt werden.

Als Orientierungshilfe bei der Planung von Neubauten können folgende Anregungen gelten: Bei der Standortplanung eines Rechenzentrums ist darauf zu achten, daß dieses in einem geschlossenen Brandabschnitt wenn möglich nicht im Erdgeschoß liegt, Türen und Fenster im bedienerlosen Betrieb über Alarmgeber gesichert sind, das Datenträgerarchiv in einem feuerfesten Bereich liegt und die Zahl der Türen zum Rechnerraum auf ein Mindestmaß beschränkt bleibt. Bei der Planung von Registraturen und Archiven, insbesondere von Zentralarchiven, sollte von dem Grundsatz ausgegangen werden, daß diese in nach außen geschützte Räume gelegt werden, soweit möglich fensterlos und vom Publikumsverkehr abgeschottet sind. Bei der Planung der Sachbearbeiterplätze in einem Großraumbüro ist darauf zu achten, daß Publikums- und Bearbeitungszone getrennt sind und Bildschirme nicht in Sichtnähe der Besucher stehen. Dem Problem des Mithörens durch Wartende ist besondere Bedeutung dort beizumessen, wo Gespräche sensibler Art mit dem Besucher geführt werden müssen. Bei Planung eines Großraumbüros empfiehlt es sich, einen Akustik-Experten zu Rate zu ziehen. Für Gespräche sensibler Art sollte auch hier ein abgeschlossener Besprechungsraum eingeplant werden. Großer Wert ist auch auf die Kontrollierbarkeit des Gebäudezugangs, den Schutz der Klimaanlage und eine klare Besucherführung zu legen. Auch Aufzüge müssen in die Sicherungskonzepte mit einbezogen werden.

Im kommunalen Bereich werden häufig nach Dienstschluß bestimmte Bereiche des Rathauses für besondere Veranstaltungen, wie Bürgerversammlungen oder Fraktionssitzungen, verwendet. Hier ist Sorge zu tragen, daß die anderen Amtsbereiche gegen unberechtigten Zutritt abgesichert werden können.

### 5.2. Kontrolle der technischen und organisatorischen Maßnahmen zum Datenschutz

Bei den Kontrollen der technischen und organisatorischen Maßnahmen zum Datenschutz zeigte sich, daß der Datenschutz von den geprüften Stellen durchwegs ernst genommen wird. Besonders beeindruckend war bei einer Stelle die Einrichtung einer Test-Fachabteilung, die ausschließlich für den Aufbau und die Pflege von Testfällen einer Testdatei zuständig ist. Diese Testfälle dienen der Programmierung als Testdatenbestand. Durch die Vielfältigkeit der Testdaten wird eine außergewöhnlich hohe Qualität und Stabilität der Programme erreicht, obwohl die Programme infolge häufiger Gesetzesänderungen ständigen Modifikationen unterworfen sind.

Eine andere Behörde, die Mitte der 70iger Jahre einen Neubau bezogen hatte, nahm im Bereich des Rechenzentrums Umbauten vor und verlegte den inneren Sicherheitsbereich in das Innere des Gebäudes, so daß das Problem der Außensicherung des Rechenzentrums dadurch gelöst wurde. Nahezu alle geprüften größeren Rechenzentren haben Zugangskontrollen eingerichtet und zwischen innerem und äußerem Sicherheitsbereich unterschieden.

Die Dokumentation der Datensicherungsmaßnahmen hat bei manchen Behörden ebenfalls einen hohen Stellenwert, wodurch bei den Kontrollbesuchen eine höhere Effektivität erzielt wird.

Schließlich wendeten viele Behörden einige Mühe dafür auf, Übersichten über manuell geführte Dateien zu erstellen. Bei der Durchsicht dieser Karteibeschreibungen stellte sich manchmal heraus, daß die Führung oder Aufbewahrung einiger Karteien überflüssig und manche aufwendige Datenübermittlungen daraus unzulässig waren. Die Einsparungen bei der Führung überflüssiger Karteien übertrafen den Aufwand für die Karteierfassung z.T. erheblich, so daß der Datenschutz letztlich zur Verwaltungsvereinfachung beitragen könnte.

Als Negativposten mußte bei fast allen Stellen, die einen Großrechner für die Unterstützung ihrer Verwaltungsaufgaben betreiben, die fehlende Transparenz des Maschinenablaufprotokolls, das keine Hilfe für eine nachträgliche Überprüfung bietet, bemängelt werden. Es hat sich gezeigt, daß das Maschinenablaufprotokoll in erster Linie als Nachweis einer ordnungsgemäßen Maschinenbedienung und für eine wirtschaftliche Systemauslastung gesehen wird. Diese Schwachstelle in der Betriebssystemsoftware ist jedoch nicht so sehr den Anwendern, als den Herstellern von DV-Systemen anzulasten. Bei Betrieb von Online-Verfahren konnten zwar anwendungsbezogene Ansätze festgestellt werden, für deren Realisierung jedoch der Anwender selbst verantwortlich zeichnete.

Die folgenden Ausführungen enthalten einen Überblick über die wesentlichsten festgestellten Mängel:

Bei Dienststellen mit Parteiverkehr erfordert der Schutz bestimmter Amtsbereiche größere Beachtung, da die Besucher nahezu ungehinderten Zugang zum Dienstgebäude haben und sich dort frei und unbeaufsichtigt bewegen können. Auch ein Pförtner bietet in diesen Fällen wenig Schutz, da er mehr für Auskünfte zuständig ist, als für die Bewachung des Gebäudes und die Verhinderung von unberechtigten Zutrittsversuchen. Amtsbereiche, die keinen oder nur sporadischen Parteiverkehr haben, dazu gehören insbesondere Rechenzentren, Rechnerräume (wenn es sich um Kleinrechner handelt), Archive, Postverteilungsstellen, sind gegenüber den übrigen Amtsbereichen durch geeignete Maßnahmen zu sichern. Gerade dort, wo die Datenverarbeitung für die Aufgabenerfüllung eine zentrale Bedeutung erlangt hat, sind besondere Sicherungsmaßnahmen erforderlich, da ein Ausfall der DV-Anlage eine ordnungsgemäße und termingerechte Aufgabenerfüllung in Frage stellen könnte.

Was den Betrieb im Rechenzentrum anbelangt, so war bezüglich des Zutritts im manchen Fällen trotz Installation eines Ausweislesesystems festzustellen, daß die Zahl der Zugangsberechtigten zum Maschinensaal zu groß war. Bei einer Gliederung des Rechenzentrums in einen inneren und

äußeren Sicherheitsbereich lassen sich Arbeiten, die mit der Maschinenbedienung und der Verwaltung des Datenträgerarchivs nichts zu tun haben, in den äußeren Sicherheitsbereich verlagern. In einem Mehrzweckrechenzentrum ist es unerläßlich, daß das Rechenzentrum alle Benutzer, deren Benutzeridentifikation und Aufgabengebiete kennt. Gegebenenfalls hat das Rechenzentrum Benutzer über notwendige und im Rechenzentrum mögliche Datensicherungsmaßnahmen zu beraten. Maschinell lesbare Datenträger haben den inneren Sicherheitsbereich nur im Rahmen des Datenträgeraustausches zu verlassen.

Überraschend häufig wurden Mängel bei der Dokumentation der DV-Verfahren festgestellt. Vor allem wurde kein schriftlicher Nachweis über Art, Umfang und Durchführung von Programmänderungen geführt. Nicht überall gehören Programmier- und Dokumentationsrichtlinien zum Standard, was eine Kontrolle durch sachverständige Dritte in einer angemessenen Zeit nicht zuläßt. Schließlich war wiederholt festzustellen, daß die Programmierer fast ausschließlich mit Echtdaten testen. In einem Fall arbeiten die Programmierer sogar mit einem täglich sich ändernden Datenbestand, was auch aus der Sicht der Programmierung ein Novum darstellen dürfte. Da sich dadurch auch die Testergebnisse täglich verändern können, ist das systematische Austesten eines Programmes erheblich erschwert. Den Programmierern kann zwar der Zugriff auf Echtdaten nicht ganz verwehrt werden. Der Zugriff auf Echtdaten sollte jedoch die Ausnahme darstellen und lediglich im Rahmen des Piloteinsatzes nach Absprache mit der Fachabteilung erfolgen sowie protokolliert werden, so daß die Notwendigkeit, so verfahren zu haben, im nachhinein überprüft werden kann.

Bei der Datenverarbeitung in herkömmlicher, nicht automatisierter Weise war immer wieder die ungenügende Entsorgung der Papierunterlagen und die Aufbewahrung sensibler Unterlagen zu bemängeln. Die zuständigen Stellen hatten zwar häufig Richtlinien für die Bearbeitung, Aufbewahrung und Vernichtung personenbezogener Unterlagen erlassen, die Einhaltung dieser Richtlinien wurde jedoch nicht überprüft. Ein allzu sorgloser Umgang mit sensiblem Datenmaterial kann im Konfliktfall, wie sich in der Praxis zeigte, zu unangenehmen Überraschungen führen.

### 5.3. **Technische Einzelfragen**

#### 5.3.1. Programmentwicklung

Die Qualität und Stabilität von neuentwickelten Anwendungsprogrammen hängt sehr davon ab, mit welcher Sorgfalt diese ausgetestet wurden. Da es kein mathematisches Verfahren gibt, die Fehlerfreiheit von Programmen nachzuweisen, muß man in der Praxis pragmatisch vorgehen und anhand aller denkbarer Fälle die Richtigkeit der Ergebnisse eines Programmlaufes prüfen. Je komplexer ein Aufgabengebiet ist, umso schwieriger ist es, eine Testdatenbasis zu konstruieren, die alle möglichen Fälle abdeckt. Der Aufbau einer Testdatenbasis erfordert stets ein Zusammenwirken von Programmierung und Fachabteilung. Bei den meisten Institutionen lastet der Aufbau und vor allem die Pflege eines komplexen Testdatenbestandes in etwa einen Mann aus. Aus Kostengründen wird deshalb häufig darauf verzichtet, für eine derartige, oft als unproduktiv angesehene Aufgabe die Arbeitskraft eines Mannes zu opfern. Es wird deshalb lediglich mit trivialen, ad-hoc-erstellten Testdaten gearbeitet und sobald das Programm ablauffähig erscheint, mit echten Daten getestet. Die Tests nehmen dann oft Wochen in Anspruch. Wie bereits erwähnt, ist auf solche Abschlußtests, häufig spricht man dabei auch von einem Piloteinsatz, nicht zu verzichten. Der Unterschied von Piloteinsatz und Funktionstest, der von der zuständigen Programmiergruppe veranlaßt wird, liegt aber darin, daß der Piloteinsatz unter der Federführung oder Begleitung der Fachabteilung ablaufen soll.

Die Gefahren und die Mißbrauchsmöglichkeiten, die bei einem unkontrollierten Zugriff der Programmierung auf die echten Daten entstehen können, sind jedoch beachtlich. Die Unmengen von Papierausdrucken, die für eine effektive Fehleranalyse die Voraussetzung sind, stellen ein nicht zu unterschätzendes Gefahrenpotential dar. Nicht selten verlassen Ausdrucke den Einflußbereich einer Institution, wenn Programmierer diese zur Fehlersuche und -analyse mit nach Hause nehmen. In den Räumen, in denen die Programmierer tätig sind, steht häufig kein ausreichender, absperrbarer Schrankraum zur Verfügung, so daß sich die Listen aus Testläufen auf den Schreibtischen und sonstigen Büromöbeln stapeln. Der Verlust einer Liste würde niemandem auffallen. Groß ist allerdings der Schaden, wenn eine solche Liste mit echten Daten an unrechter Stelle auftaucht.

Für Sicherheitszwecke und zur schnelleren Auskunftsbereitschaft im Online-Verfahren wird bei einigen speichernden Stellen der Datenbestand doppelt vorgehalten. Nach Dienstschluß, wenn die Online-Auskunftsverfahren nicht mehr aktiv sind, dient der zweite Bestand als Testdatenbestand für die Programmierung. Nicht selten ist der sogenannte „Testdatenbestand" noch aufzubereiten, so daß abends für die notwendigen Testläufe nur noch wenig Zeit übrig bleibt. Die Programmierung könnte aber effektiver arbeiten und hätte bessere Arbeitsbedingungen, wenn sie über längere Zeit – auch tagsüber – einen stationären Bestand zur Verfügung hätte, mit dem sie alle Funktionen austesten könnte. Abweichungen in den Testergebnissen können nämlich entweder durch neue Programmfehler oder durch die Aktualisierung der Datenbasis im täglichen Änderungsdienst entstanden sein. Der Aufbau einer signifikaten Testdatenbasis, die keinen Rückschluß auf irgendwelche Personen zuläßt, hätte also nicht nur aus der Sicht des Datenschutzes Vorteile, sondern könnte in vielen Fällen auch die Entwicklungszeit bestimmter Programme reduzieren.

#### 5.3.2. Zugriffskontrolle bei Online-Verfahren

Bereits im 5. Tätigkeitsbericht wurden unter der Textziffer 5.3.5 Hinweise zur Verbesserung des Zugriffsschutzes gegeben. Leider war in einigen Fällen festzustellen, daß der Stand der Technik gerade bei Online-Verfahren nicht immer ausreichend berücksichtigt wurde. Moderne Systeme bieten heute eine Reihe von Eigenschaften, die sowohl dem Benutzer eine einfache Bedienung als auch dem Revisor die Prüfung der Ordnungsmäßigkeit der Anwendung ermöglichen. Folgende Bedingungen sollten gegeben sein:

- Der Benutzer muß sich am Bildschirmgerät dem System gegenüber mit einer Benutzeridentifikation und einem individuellen Passwort ausweisen. Die Benutzeridentifikation wird ihm vom Systemverwalter o.ä. zugewiesen. Das Passwort vergibt der Benutzer selbst, so daß dieses in der Regel außer ihm selbst kein anderer mehr kennt. Für die regelmäßige Änderung des Passworts ist der Benutzer selbst verantwortlich. Vergißt er sein Passwort, muß systemseitig mit einer priviligierten Prozedur die Neuein-

richtung des Passwortes möglich sein, ohne daß dem Benutzer dabei Daten verloren gehen.

- Das System muß erfolglose Zugriffsversuche unter einem falschen Passwort protokollieren, bei wiederholten Fehlversuchen ist die Benutzeridentifikation zu sperren. Auf diese Weise kann man sich gegen ein systematisches Ausspionieren des Passwortes schützen. Diese Vorgehensweise ist vor allem in offenen Systemen (Aufbau der Verbindung über Wählleitung im Fernsprechnetz) von Bedeutung und findet beim Bildschirmtext Verwendung.
- Hat sich der Benutzer erfolgreich angemeldet, so sind ihm innerhalb des Menues nur solche Funktionen bzw. Transaktionscodes anzuzeigen, zu deren Ausführung er auch berechtigt ist.
- Befindet sich der Benutzer in einem Anwendungssystem, dürfen die Bildschirmmasken nur solche Felder enthalten, deren Inhalt der Benutzer zu bearbeiten befugt ist. Bereiche, die für die Aufgabenstellung irrelevant sind, sind aus den Bildschirmmasken zu entfernen. Bei einer nachträglichen Kontrolle würde sonst nicht eindeutig erkennbar sein, ob die Felder zufällig leer waren oder das Anwendungssystem diese Felder aufgrund besonderer Zugriffsvorschriften nicht versorgt hat.
- Vielfach gibt es verfahrensseitig maschinelle Protokollierungen, die beispielsweise die Revision wesentlich erleichtern können. In solchen Fällen ist jedoch darauf zu achten, daß durch die Protokollierung des Zugriffes auf einen bestimmten Datensatz keine Datei mit personenbezogenen Daten angelegt wird, die informationell eine neue Qualität entstehen läßt. Die Protokollierung soll vielmehr Recherchen darüber ermöglichen, wer wann auf welche Datei mit welchem Programm zugegriffen hat. Eine Aufzeichnung der Satzinhalte ist dazu im allgemeinen nicht erforderlich.

### 5.3.3. Schutz des Systempassworts im Betriebssystem BS2000

Anläßlich eines Kontrollbesuches in einem Rechenzentrum, das im Betriebssystem BS 2000 der Firma Siemens fährt, wurde festgestellt, daß für die Ausnützung des vollen Funktionsumfanges bestimmter Dienstprogramme (Start von der Konsole) dem Maschinenbediener das systemschützende Kennwort, das sog. TSOS-Passwort, bekanntgegeben werden muß. Da das TSOS-Passwort gewissermaßen den Schlüssel zur Umgehung der Schutzfunktionen im Betriebssystem BS 2000 darstellt, sollte es eigentlich nur den Systembetreuern bekannt sein. Bei den betreffenden Dienstprogrammen handelte es sich um das Initialisieren von Magnetbändern und Disketten (INIT), das Etikettieren und Formatieren von Plattenspeichern (VOLIN) und die Freispeicherplatzverwaltung (SPCCNTRL).

Bis zur Verfügbarkeit eines stufenweise wirkenden TSOS-Passwortes schlug mir die Firma Siemens folgende Übergangslösung vor: Der Systemverwalter hat die Möglichkeit, dem Operator die Verwendung von Dienstprogrammen über vordefinierte ENTER-Prozeduren zu ermöglichen, so daß diesem das TSOS-Passwort nicht bekannt zu machen ist. Bei der Katalogisierung erhalten diese Prozeduren ein Lesepasswort (READ-PASS) und ein Ausführungspasswort (EXEC-PASS). Der Maschinenbediener braucht zum Start der Funktionen nur das Ausführungpasswort zu kennen. Das Lesepasswort schützt die ENTER-Prozeduren vor unberechtigtem Lesen, so daß die systemeigenen Datenschutzkomponenten des BS 2000 zuverlässig gegen unberechtigte Inanspruchnahme geschützt werden. Diese Vorgehensweise ist ab Einsatz der Version 7.1 von BS 2000 möglich. Eine Beeinträchtigung des Arbeitsablaufes im Rechenzentrum tritt nach Aussage des Rechenzentrums, das dieses Verfahren geprüft hat und nunmehr einsetzt, nicht auf.

### 5.3.4. Organisatorische Maßnahmen

Im Bereich der Universitätskliniken ist die organisatorische Eingliederung des internen Datenschutzbeauftragten noch unterschiedlich gelöst. Ein Klinikum hat bespielsweise einen Datenschutzbeauftragten bestellt und ihm Beauftragte bei den Kliniken nachgeordnet. Der Beauftragte des Klinikums ist sozusagen als deren Sprecher anzusehen. Ein anderes Klinikum hat wiederum drei Beauftragte für den Datenschutz bestellt: für den medizinischen Bereich, für die Verwaltung und für das Rechenzentrum.

Die erstgenannte Regelung ist zwar grundsätzlich zu begrüßen, die Wirksamkeit einer solchen Regelung hängt jedoch sehr davon ab, welche Kompetenzen dem Sprecher der Datenschutzbeauftragten eingeräumt werden.

In der Geschäftsverteilung müßten die Aufgaben und Befugnisse des Sprechers definiert sein. Zu den Aufgaben des Sprechers der Datenschutzbeauftragten müßten insbesondere zählen

- die Einschaltung bei der Freigabe nach Art. 26 Abs. 2 Bayer. Datenschutzgesetz,
- die Führung von Übersichten über automatisiert und manuell geführte Dateien mit personenbezogenen Daten,
- die Meldung von automatisiert geführten Dateien zum Datenschutzregister im Benehmen mit dem zuständigen Klinik-Datenschutzbeauftragten,
- die Befugnis zu gelegentlichen Kontrollen der technischen und organisatorischen Maßnahmen zum Datenschutz bei den Kliniken.

Schließlich müßte der Sprecher der Datenschutzbeauftragten die Möglichkeit besitzen, sich ohne Einschaltung der Kommission für die Speicherung von Patientendaten direkt an den Landesbeauftragten für den Datenschutz wenden zu können.

### 5.3.5. Versand von personenbezogenen Unterlagen

Soweit keine gesetzlichen Vorschriften über die Versandart vorliegen, ist vom Versender im Einzelfall zu prüfen, ob bei Kenntnisnahme des Brief- oder Paketinhalts durch unbefugte Personen schutzwürdige Belange des Betroffenen verletzt werden können. Solange das Postgut sich in der Obhut der Bundespost befindet, muß man davon ausgehen, daß es durch die Garantien der Bundespost (z.B. Briefgeheimnis, Amtsgeheimnis, Verschwiegenheitspflicht der Postbediensteten als Amtsträger) vor dem Zugriff und damit vor der Kenntnisnahme durch Dritte sicher ist. Soweit die Verteilung des Postgutes über zentrale Einrichtungen (z.B. Poststelle eines Betriebes, Postfach) erfolgt, müßte sichergestellt sein, daß die mit der Verteilung oder Abholung betrauten Bediensteten sorgfältig ausgewählt worden sind. Bei der Zustellung an den Betroffenen selbst könnte theoretisch durch menschliches Fehlverhalten eine unrichtige Zustellung (z.B. falscher Briefkasten) oder die Leerung des Briefkastens durch eine andere fremde Person (z.B. Unter-

mieter) erfolgen. In solchen Fällen ließe sich bei Versand des Postgutes als Druck- oder Briefdrucksache eine unbefugte Kenntnisnahme durch Dritte nicht ausschließen oder eindeutig feststellen. Umfaßt der Inhalt sensiblere Informationen, wäre eine höherwertige Versandart geboten. Bei allen diesen Überlegungen ist aber auch der Grundsatz der Verhältnismäßigkeit zwischen angestrebtem Schutzzweck und nötigem Aufwand zu berücksichtigen (Art. 15 Abs. 1 BayDSG). Briefumschläge mit Adhäsions- oder Punktverschluß benötigen zwar zu ihrer Öffnung einen gewissen Aufwand, der jedoch geringer ist, als bei normalverschlossenen Briefumschlägen. Briefumschläge mit Adhäsions- oder Punktverschluß bieten ein deutlich geringeres Hindernis gegen unbefugte Kenntnisnahme ihres Inhalts. Ein Öffnen solcher Postsendungen hinterläßt oft keine äußerlichen Spuren, weil man diese nach dem Öffnen noch ein zweites Mal zukleben kann.

Unter Berücksichtigung dieser Grundsätze ist auch die Versendung von Formularen und Fragebogen zu sehen. Je nach der Sensibilität der zu erfragenden Daten, beispielsweise bei Vordrucken, die auf die Schwerbeschädigteneigenschaft abstellen, ist zwischen dem Versand als Briefdrucksache oder verschlossener Brief zu wählen. Der Versand von Unterlagen einer Vielzahl von Betroffenen ist anders zu beurteilen. Enthalten die Unterlagen sensible Daten, wie beispielsweise medizinische Daten, ist der Versand als Wertsendung notwendig.

Auch bei einer Wertangabe unter DM 3000.- ist nach Auskunft der Deutschen Bundespost eine erhöhte Sicherheit im internen Postbetrieb gewährleistet. Die postinternen, zusätzlichen Absicherungen können aus Sicherheitsgründen (Gefahr der Ausforschung) nicht dargelegt werden. Die Ablehnung einer höherwertige Versandart aus verfahrenstechnischen Gründen kann nicht hingenommen werden.

5.3.6. Fernwartung

Im Rahmen der Fern-Unterstützung und -Diagnose bieten auch Hersteller kleinerer Rechner, wie sie beispielsweise Landratsämter einsetzen, einen Hardware- und einen Software-Support an. Beim Hardware-Support werden gerätespezifische Statusinformationen, die in eigenen Fehlerdateien aufgezeichnet werden, analysiert. Im Software-Support wird die herstellereigene Systemsoftware ferndiagnostiziert.

Aus der Sicht des Datenschutzes bestehen gegen den Einsatz der Fernwartung dann keine Bedenken, wenn folgende Punkte erfüllt sind:

1. Die Fernwartung muß sich gegenüber dem Systemverwalter beim Kunden eindeutig identifizieren können. Der Aufbau der Dialogverbindung muß unter der Kontrolle des Systemverwalters erfolgen.

   2. Die Fernwartung darf nur auf solche Dateien zugreifen, die für die Fernwartung paßwortgeschützt eingerichtet sind.

3. Personenbezogene Dateien sind grundsätzlich durch Paßwort zu schützen; der Fernwartung muß der Zugriff auf solche Dateien verwehrt sein.
4. Alle Aktivitäten der Fernwartung sind aufzuzeichnen und müssen vom Systemverwalter an der Konsole verfolgbar sein.
5. Der Systemverwalter muß die Möglichkeit haben, den Dialog mit der Fernwartungszentrale trennen zu können.

Nach Rücksprache mit den Herstellern sind diese Forderungen grundsätzlich erfüllbar.

Manche Hardwarehersteller bieten auch komplette Anwendungssysteme an. Der Software-Support von Anwenderverfahren ist nur dann unbedenklich, wenn alle personenbezogenen Datenbestände von der Anlage genommen wurden und das System ausschließlich mit Testdaten gefahren wird.

## 6. Datenschutzregister

### 6.1. Stand

Nach wie vor erreichen meine Geschäftsstelle täglich Meldungen zum Datenschutzregister. Zum Zeitpunkt der Veröffentlichung des 2. Nachtrags zur Übersicht über das Datenschutzregister (StAnz. Nr. 45/1983 vom 11.11.1983) am 7. Oktober 1983 waren ca. 13.200 Einzeldateien von insgesamt 3.880 speichernden Stellen gemeldet. Die hohe Anzahl der Einzeldateien ist überwiegend auf die große Redundanz bestimmter Dateien, wie im Kommunalbereich das automatisierte Einwohnerwesen oder bei vielen Behörden im Personalwesen, z.B. für die Lohn- und Gehaltsabrechung, zurückzuführen. Der Anstieg der Zahl der Dateien gegenüber 1982 betrug immerhin 7%. Davon ist ein hoher Prozentsatz auf den vermehrten Einsatz von Computern im Schulverwaltungsbereich zurückzuführen. Im Kommunalbereich bedienen sich 313 der 346 Verwaltungsgemeinschaften der ADV (90,5%). Von den 2027 Gemeinden (Einheitsgemeinden und Mitgliedsgemeinden von Verwaltungsgemeinschaften ohne kreisfreie Städte) wickeln 1625 mindestens eine Verwaltungsaufgabe automatisiert ab (80,2%).

Wie jedes Jahr erschien über die Veröffentlichung des 2. Nachtrages zur Übersicht über das Datenschutzregister eine Pressenotiz, die dieses Mal jedoch eine große Zahl von Zuschriften auslöste, so daß in den letzten 6 Wochen des Berichtszeitraumes doppelt so viele Bürger Auskunft aus dem Datenschutzregister beantragten, wie in den gesamten 10 1/2 Monaten vorher. Ein Drittel der Zuschriften kam aus München, die Hälfte aus dem Regierungsbezirk Oberbayern.

Auch bei den Behörden mehren sich die Auskunftsersuchen über gespeicherte Daten. Dabei ist bemerkenswert, daß besonders kritische Bürger auch aus solchen Dateien Auskunft wünschen, zu denen sie von der Aufgabenbestimmung her keinerlei Bezug für ihre Person feststellen müßten. Das zeigt allerdings, daß vielen Bürgern nicht bewußt ist, daß Behörden nur dann Daten über Bürger in den jeweiligen Dateien speichern, wenn sie diese zur Aufgabenerfüllung benötigen.

### 6.2. Meldepflichtige Dateien

Nach § 2 der Verordnung über das Datenschutzregister (Datenschutzregisterverordnung, DSRegV) vom 23.11.1978 enthält das Datenschutzregister Angaben über die Verarbeitung personenbezogener Daten in automatisierten Verfahren. Im Berichtszeitraum wurde bei meiner Dienststelle wiederholt angefragt, wann eine personenbezogene Datensammlung zum Datenschutzregister zu melden sei. Grundsätzlich müssen dafür zwei Voraussetzungen gegeben sein. Die Datensammlung muß den Dateibegriff in Sachen der Datenschutzgesetze erfüllen und die Verarbeitung muß au-

tomatisiert erfolgen. Wird eine Datensammlung in logisch gleichartig aufgebauten Datensätzen in einer ADV-Anlage gespeichert und verarbeitet und besteht die Möglichkeit, die Datensammlung nach bestimmten Merkmalen auszuwerten und umzuordnen, ist sie zum Datenschutzregister zu melden. Die Größe der eingesetzten ADV-Anlage spielt dabei ebensowenig eine Rolle wie die Art der physischen Speicherung der Daten (sequentiell, gestreut, segmentiert, komprimiert, datenbankverwaltet). Genauso unerheblich ist, ob die Datei bei der speichernden Stelle oder außer Haus im Auftrag verarbeitet wird.

Die automatisierte Datenverarbeitung ist heute in Verwaltungsbereiche eingezogen, die vor Jahren noch als nicht automatisierbar galten. Dies gilt beispielsweise für folgende Bereiche:

- Gleitzeiterfassung: Werden die Daten über Dienstbeginn und -ende von Mitarbeitern zentral in einer Anlage gespeichert, ist diese Datei zum Datenschutzregister zu melden. Derartige Systeme gestatten es, gezielt Mitarbeiterkonten abzufragen und zu bearbeiten, sowie Gesamtlisten zu erstellen.
- Gesprächsdatenerfassung: Werden bei einer Fernsprechnebenstellenanlage Aufzeichnungen der Gesprächsdaten (nicht Inhalte) mitgeführt, so handelt es sich auch hier um eine meldepflichtige Datei.
- Textverarbeitung: Werden auf einem Textsystem Adressen gespeichert, die personenbezogene Daten enthalten sowie umsortierbar und selektierfähig sind, so ist diese Adreßdatei zum Datenschutzregister zu melden.
- Retrieval-Systeme: Bedient man sich bei der Verwaltung einer Behördenregistratur eines Kleincomputers, in dem zur Wiederauffindung von Vorgängen auch personenbezogene Daten gespeichert werden, ist das Verfahren zum Datenschutzregister zu melden.

  Nicht meldepflichtig sind dagegen z.B. maschinelle Verfahren, die Magnetkontenkarten verarbeiten, dazu aber keinen zentralen Speicher in der Anlage vorsehen, in dem eine Datei abgelegt werden kann, und Textverfahren, die lediglich zur Abwicklung der Korrespondenz und der Erfassung von unformatierten Texten dienen.

### 7. 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 5. Tätigkeitsberichts für den Zeitraum vom 1. Januar bis 31. Dezember 1983 nachgekommen.

Folgende Schwerpunkte lassen sich diesem Tätigkeitsbericht entnehmen:

Wie schon in vorangegangenen Tätigkeitsberichten geht der Datenschutzbeauftragte des Bayerischen Rundfunks erneut auf die datenschutzrechtlichen Aspekte bei der Einführung eines Personaldatensystems (PDS) ein. Im Berichtszeitraum sei das PDS im Bayerischen Rundfunk endgültig eingeführt worden. Als Mitglied einer neu gegründeten Arbeitsgruppe „Personaldatensystem" habe der Datenschutzbeauftragte des Bayerischen Rundfunks von Anfang an alle datenschutzrechtlichen Anforderungen einbringen können. So habe er beispielsweise

- sämtliche im PDS vorhandenen Datenfelder auf ihre Erforderlichkeit geprüft;
- die automatische Information der Mitarbeiter über die beim Bayerischen Rundfunk über sie gespeicherten Daten angeregt, um die Richtigkeit der Daten kontrollieren zu können und die Akzeptanz von PDS bei den Mitarbeitern zu erhöhen;
- auf eine klare Organisation im PDS hingewirkt, so daß Zuständigkeiten und Verantwortung der jeweiligen Aufgabenstellung entsprechen;
- an der Erstellung einer Datensicherungskonzeption mitgewirkt, bei der eindeutige und aufgabenorientierte Berechtigungen aufgestellt wurden, ohne daß hierbei die Handhabung des Systems für die daran arbeitenden Mitarbeiter unnötig erschwert wurde.

Bisher seien alle auftauchenden Datenschutzfragen im Einvernehmen mit der Personalabteilung gelöst worden. Der reguläre Start des Systems zum 5. Oktober 1983 sei dadurch möglich gewesen. Es stünden aber noch weitere Probleme und Aufgaben an, die auch in Zukunft für den Datenschutzbeauftragten des Bayerischen Rundfunks vorrangig sein würden.

Im Zusammenhang mit der Prüftätigkeit der Landesrechnungshöfe bei den Rundfunkanstalten, auf die der Datenschutzbeauftragte bereits in seinem 3. Tätigkeitsbericht eingegangen war, teilt der Datenschutzbeauftragte mit, daß sich die Rundfunkdatenschutzbeauftragten nunmehr eingehend mit der Frage der dabei gebotenen Beachtung datenschutzrechtlicher Vorschriften befaßt hätten. Die Rundfunkdatenschutzbeauftragten hätten hierzu Grundsätze erarbeitet und an die Intendanten die Empfehlung gegeben, vor Beginn der Prüftätigkeit die Einhaltung dieser Grundsätze mit dem jeweils zuständigen Rechnungshof zu vereinbaren. Diese Grundsätze sind im Anhang zum Tätigkeitsbericht des Datenschutzbeauftragten des Bayerischen Rundfunks abgedruckt.

Bezüglich der im letztjährigen Tätigkeitsbericht aufgegriffenen Rechtsprobleme bei den von der Finanzverwaltung geforderten jährlichen Kontrollmitteilungen über Honorarzahlungen an freie Mitarbeiter berichtet der Datenschutzbeauftragte, daß die für das Kalenderjahr 1983 vorgesehene Lösung, an die freien Mitarbeiter Jahresabrechnungen auszugeben, die sie den Finanzbehörden auf Verlangen vorlegen können, erstmals praktiziert worden sei. Hierbei habe es bisher keinerlei Probleme gegeben. Problematisch erscheint dem Datenschutzbeauftragten allerdings diesbezüglich der gegenwärtig in der Ausarbeitung befindliche Entwurf der Bundesregierung zur Änderung der Abgabenordnung, wonach die Praxis der Kontrollmitteilungen in einem weit größerem Rahmen als bisher gesetzlich sanktioniert würde. Der Datenschutzbeauftragte hat sich ferner befaßt mit datenschutzrechtlichen Fragen bei der Übermittlung von Honorardaten fest angestellter Mitarbeiter anderer Rundfunkanstalten an die Heimatanstalt, mit der absoluten Trennung von Beihilfestelle und Personalverwaltung, die

beim Bayerischen Rundfunk gewährleistet sei, sowie mit datenschutzrechtlichen Fragen bei der Feststellung der Höhe des Anspruchs auf Kindergeld.

Anknüpfend an seine Ausführungen im letztjährigen Tätigkeitsbericht betreffend die Überprüfung des Rechenzentrums des Bayerischen Rundfunks durch den Technischen Überwachungsverein Bayern e.V. teilt der Datenschutzbeauftragte mit, daß sämtliche in dem Bericht aufgezeigten Mängel und die gegebenen Empfehlungen mit allen betroffenen Fachabteilungen besprochen und die notwendigen Maßnahmen zur Verbesserung eingeleitet worden seien. Die insoweit vereinbarten Maßnahmen hätten insbesondere die Verbesserung der Zugangskontrolle zum Rechenzentrum betroffen, wo ein neuer Ausweisleser in Kombination mit Codezahlen installiert worden sei. Die Sicherheitsmaßnahmen im Zusammenhang mit der Reinigung des Rechenzentrums seien verstärkt worden. Im übrigen werde die Überarbeitung der Datenschutzrichtlinien und des Entsorgungskonzeptes für den Bayerischen Rundfunk in Kürze abgeschlossen sein.

Unter der Überschrift „Datenschutz und Rundfunkgebühren" berichtet der Datenschutzbeauftragte erneut über datenschutzrechtliche Probleme, die ihm in Zusammenhang mit dem Beauftragtendienst der Rundfunkanstalten beschäftigt hätten. Der Fragebogen des Beauftragtendienstes zur Erhebung nichtgemeldeter Rundfunkgeräte sei datenschutzrechtlich überprüft worden und solle nun im Jahre 1984 vom Beauftragtendienst eingesetzt werden. Gemeinsam mit der Gebührenstelle habe der Datenschutzbeauftragte Datenschutzrichtlinien für den Beauftragtendienst entwickelt; so solle u.a. von Minderjährigen unter 16 Jahren Auskunft nicht mehr gefordert werden.

Als weitere Themen, mit denen er sich beschäftigt habe, nennt der Datenschutzbeauftragte die Übermittlung von Daten über Inhaber von Kabelanschlüssen an den Bayerischen Rundfunk, die Übermittlung personenbezogener Daten im Befreiungsverfahren an die GEZ, sowie die Übermittlung der den Gemeinden bekannten Sozialdaten der Antragsteller an die Rundfunkanstalten im Rahmen der Bearbeitung der Befreiungsanträge. Zum letztgenannten Punkt hätten die Rundfunkdatenschutzbeauftragten im Hinblick auf den besonderen Sozialdatenschutz eine den Anforderungen der Landesdatenschutzgesetze entsprechende Einwilligungserklärung konzipiert, die künftig in die Befreiungsanträge aufzunehmen sein werde.

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 zu formellen Beanstandungen nicht habe festgestellt werden können. Seine entsprechenden Hinweise hätten bei den zuständigen Stellen Beachtung gefunden. Es habe sich auch im Berichtszeitraum wieder als ausreichend erwiesen, für die Zukunft Maßnahmen zur Verbesserung des Datenschutzes zu empfehlen. Themen dieser Tätigkeit seien insbesondere gewesen:

- Erfolgskontrolle im Zeitungsarchiv;
- Auskünfte an Kreditkarten-Organisationen;
- Nutzung der Hauspost und interner Adressen für externe Zwecke.

Im Abschnitt „Datenschutz bei der GEZ" teilt der Datenschutzbeauftragte mit, daß dieser Bereich nach wie vor ein Schwerpunkt der Tätigkeit der Rundfunkdatenschutzbeauftragten sei. Der Arbeitskreis Datenschutzbeauftragte der Rundfunkanstalten habe deshalb auch im Berichtsjahr dafür gesorgt, daß die GEZ weiterhin an der Vervollkommnung ihrer technischen und organisatorischen Vorkehrungen arbeitet, um so den Datenschutz ständig zu verbessern. Die von den Landesrundfunkanstalten und dem ZDF getragene GEZ hatte zum 31.12.1983 einen Bestand von 24.598.736 Hörfunkteilnehmern und 22.127.118 Fernsehteilnehmern zu verwalten. Dabei führte die GEZ 4.174.113 Hörfunkteilnehmer des Bayerischen Rundfunks, von denen 260.079 gebührenbefreit waren. Als Fernsehteilnehmer des Bayerischen Rundfunks waren 3.747.112 gemeldet, von denen 190.727 gebührenbefreit waren. Im Bereich des Bayerischen Rundfunks ergingen 158.199 Gebührenbescheide. Gegen säumige Rundfunkgebührenzahler wurden 16.029 Vollstreckungen eingeleitet und gegen Schwarzseher und -hörer wurden 1.729 Anträge auf Verfolgung als Ordnungswidrigkeit gestellt. Die Gesamtzahl dieser Maßnahmen sei im Vergleich zum Jahr 1982 erneut gestiegen, der Bayerische Rundfunk liege mit diesen Zahlen aber noch erheblich unter dem Durchschnitt innerhalb der ARD.

Die GEZ bearbeitet und beantwortet einfache Anfragen und sonstigen Routineschriftwechsel von Rundfunkteilnehmern in Datenschutzangelegenheiten selbständig. Geschäftsvorfälle mit grundsätzlichem Charakter und andere individuelle Anfragen schwieriger Art gibt sie an den Datenschutzbeauftragten der jeweils zuständigen Landesrundfunkanstalt ab. Auffallend sei, daß zunehmend Anfragen nach Daten Dritter die GEZ erreicht hätten, während Anfragen nach eigenen Daten deutlich zurückgegangen seien. Die GEZ werde im besonderen Maße darauf achten, daß personenbezogene Daten an Dritte grundsätzlich nicht weitergeben werden. Relativ zahlreiche Beschwerden seien nach einer vom Bayerischen Rundfunk zusammen mit dem SDR und SWF durchgeführten Direct-Mail-Aktion zur Werbung jugendlicher Rundfunkteilnehmer eingegangen. Datenschutzrechtlich sei diese Direct-Mail-Aktion, an deren Vorbereitung der Datenschutzbeauftragte von Anfang an beteiligt worden sei, unproblematisch gewesen, da es sich um eine reine Werbemaßnahme gehandelt habe. Bedenken gegen diese Art der Werbemaßnahme würde sich aber möglicherweise aus der hohen Zahl von Beschwerden ergeben. Die Planungen der GEZ für weitere Aktionen dieser Art im Jahr 1984 seien daher darauf gerichtet, durch vorherigen Datenabgleich von fremdem Adressenmaterial mit GEZ-Daten zu vermeiden, daß bereits gemeldete Teilnehmer die Werbeschreiben erhalten, um auf diese Weise die Erfolgsquote zu erhöhen und die Zahl der Beschwerden zu verringern.

In seiner Zusammenfassung weist der Datenschutzbeauftragte des Bayerischen Rundfunks darauf hin, daß die Zahl der Auskunftsersuchen und der sonstigen Reaktionen von Rundfunkteilnehmern und Dritten zu Fragen des Datenschutzes im Jahr 1983 im Vergleich zum Vorjahr erneut etwas zurückgegangen sei. Die Gründe hierfür sind nach seiner Auffassung wesentlich durch weitere Verbesserungen beim Rundfunkgebühreneinzugsverfahren bedingt. Darüber hinaus sei ein verstärktes Datenschutzbewußtsein in der Bevölkerung sowie eine weiter gewachsene Aufmerksamkeit für die Belange des Datenschutzes, auch bei den Mitarbeitern des Bayerischen Rundfunks und der GEZ festzustellen.

Anhang Nr. 1

**Urteil des Bundesverfassungsgerichts zum Volkszählungsgesetz 1983 vom 15.12.1983**

Leitsätze zum Urteil des Ersten Senats vom 15. Dezember 1983

– 1 BvR 209/83 u.a. –

1. Unter den Bedingungen der modernen Datenverarbeitung wird der Schutz des Einzelnen gegen unbegrenzte Erhebung, Speicherung, Verwendung und Weitergabe seiner persönlichen Daten von dem allgemeinen Persönlichkeitsrecht des Art. 2 Abs. 1 in Verbindung mit Art. 1 Abs. 1 GG umfaßt. Das Grundrecht gewährleistet insoweit die Befugnis des Einzelnen, grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen.

2. Einschränkungen dieses Rechts auf „informationelle Selbstbestimmung" sind nur im überwiegenden Allgemeininteresse zulässig. Sie bedürfen einer verfassungsgemäßen gesetzlichen Grundlage, die dem rechtsstaatlichen Gebot der Normenklarheit entsprechen muß. Bei seinen Regelungen hat der Gesetzgeber ferner den Grundsatz der Verhältnismäßigkeit zu beachten. Auch hat er organisatorische und verfahrensrechtliche Vorkehrungen zu treffen, welche der Gefahr einer Verletzung des Persönlichkeitsrechts entgegenwirken.

3. Bei den verfassungsrechtlichen Anforderungen an derartige Einschränkungen ist zu unterscheiden zwischen personenbezogenen Daten, die in individualisierter, nicht anonymer Form erhoben und verarbeitet werden, und solchen, die für statistische Zwecke bestimmt sind.

   Bei der Datenerhebung für statistische Zwecke kann eine enge und konkrete Zweckbindung der Daten nicht verlangt werden. Der Informationserhebung und -verarbeitung müssen aber innerhalb des Informationssystems zum Ausgleich entsprechende Schranken gegenüberstehen.

4. Das Erhebungsgrogramm des Volkszählungsgesetzes 1983 (§ 2 Nr. 1 bis 7, §§ 3 bis 5) führt nicht zu einer mit der Würde des Menschen unvereinbaren Registrierung und Katalogisierung der Persönlichkeit; es entspricht auch den Geboten der Normenklarheit und der Verhältnismäßigkeit. Indessen bedarf es zur Sicherung des Rechts auf informationelle Selbstbestimmung ergänzender verfahrensrechtlicher Vorkehrungen für Durchführung und Organisation der Datenerhebung.

5. Die in § 9 Abs. 1 bis 3 VZG 1983 vorgesehenen Übermittlungsregelungen (unter anderem Melderegisterabgleich) verstoßen gegen das allgemeine Persönlichkeitsrecht. Die Weitergabe zu wissenschaftlichen Zwecken (§ 9 Abs. 4 VZG 1983) ist mit dem Grundgesetz vereinbar.

Anhang Nr. 2

**Zum Hauptsacheverfahren über die Verfassungsmäßigkeit des Volkszählungsgesetzes 1983** hatte das Bundesverfassungsgericht folgende Fragen auch an den Bayerischen Datenschutzbeauftragten gerichtet:

1. Welchen konkreten Zwecken dient die einzelne Datenerhebung und Datenverarbeitung, die das Volkszählungsgesetz 1983 vorschreibt?

2. Sind die konkreten einzelnen Zwecke für den auskunftspflichtigen Bürger aus dem Volkszählungsgesetz 1983 hinreichend deutlich erkennbar?

3. Dient die einzelne Datenerhebung und Datenverarbeitung Zwecken, die vom Grundgesetz gebilligt sind?

4. Ist die Datenerhebung in der Form der Volkszählung als Totalerhebung noch ein geeignetes Mittel zur Erreichung der vom Volkszählungsgesetz 1983 konkret verfolgten Zwecke?

5. Ist eine Totalerhebung, wie es das Volkszählungsgesetz 1983 vorschreibt, erforderlich zur Erreichung der einzelnen vom Gesetz verfolgten Zwecke? Gibt es insbesondere keine für die Betroffenen milderen Mittel, welche die angestrebten konkreten Zwecke ebenso oder gar besser erreichen lassen (etwa auf der Grundlage moderner Sozial- und Statistikforschung aufbauende Stichprobenerhebungen für bestimmte einzelne Zwecke, Gruppen und Gebiete)?

6. Stehen die mit der einzelnen Datenerhebung und Datenverarbeitung verbundenen Nachteile für den betroffenen Bürger in einem offensichtlichen Mißverhältnis zu ihrem Nutzen?

7. Welche verfassungsrechtliche Bedeutung hat der Grundsatz der Zweckbindung der Daten? Kann der Staat ohne vorhergehende konkrete Bestimmung eines Verwendungszieles, also Angabe der einzelnen Zwekke, Daten erheben und/oder speichern? Kann er Daten, die für ein bestimmtes Verwendungsziel erhoben worden sind, als Informationsquelle für andere Zwecke nutzbar machen, vor allem Daten, die im Zusammenhang mit Zwecken für die Statistik des Bundes unter bußgeldbewehrter Auskunftsverpflichtung erhoben werden, aus diesem Zusammenhang lösen und sie für andere Verwendungszwecke, insbesondere für den Verwaltungsvollzug zur Verfügung stellen?

8. Auf welche verfassungsrechtliche Kompetenzvorschrift stützt der Bund seine Regelungsbefugnis für den Registerabgleich (§ 9 Abs. 1 VZG 1983) und die Datenübermittlungen nach § 9 Abs. 2 S.4 VZG 1983?

9. Ist im Interesse der für den verfassungsrechtlichen Persönlichkeitschutz notwendigen Geheimhaltung und des Grundsatzes der Anonymität die Weitergabe von Einzelangaben an Gemeinden und Gemeindeverbände nach § 9 Abs. 3 VZG 1983 dadurch zu vermeiden, daß die für die dort genannten Zwecke notwendigen Statistiken nach den Angaben der Gemeinden oder Gemeindeverbände durch das Statistische Landesamt erstellt werden, insbesondere bei kleinen Kommunen?

10. Muß der Vollzug des Volkszählungsgesetzes (Zählorganistion, Fragebogen), gegebenenfalls in welchem Umfang, durch den Gesetzgeber (Gesetz oder Rechtsverordnung aufgrund eines Gesetzes) im Hinblick auf den Vorbehalt des Gesetzes („Wesentlichkeitstheorie") geregelt werden?

11. Gibt es auch bei einer Totalerhebung für die Betroffenen mildere Vollzugsmittel, die insbesondere die Anonymität besser wahren (etwa durch Rücksendung der Fragebogen in verschlossenen Umschlägen, nach einem Verfahren, das dem der Briefwahl nachgebildet

ist, die Kontrolle der Abgabe ermöglicht, aber nach Öffnung der anonymen Umschläge und Herausnahme der Fragebogen ohne Namen, Kennnummer und Anschrift einen Rückschluß auf den Betroffenen nicht mehr zuläßt?

12. Welche Fehlerquote an nicht, unvollständig oder falsch ausgefüllten Bogen könnte in Kauf genommen werden, ohne daß die für die Bundesstatistik gesetzten Ziele gefährdet würden?

13. Ist es richtig, daß der Bund nach Durchführung der Volkszählung 1983 keine weiteren Totalerhebungen mehr für die Zukunft beabsichtigt, wie das in der Schweiz der Fall sein soll?

    a) Welche Formen der Erhebung plant der Bund alsdann für die Zukunft? b) Weshalb wird in diesem Fall noch auf der Durchführung der Volkszählung 1983 bestanden?

14. Hat die Durchführung der Volkszählung 1983 für die Öffentliche Hand alsdann noch einen Wert, wenn Datenübermittlungen im Sinne des § 9 Abs. 1-4 VZG 1983 aus verfassungsrechtlichen Gründen nicht erlaubt sein sollten?

Anhang Nr. 3

**Entschließung**

der Konferenz der Datenschutzbeauftragten des Bundes
und
der Länder sowie der Datenschutzkommission
Rheinland-Pfalz
vom 27./28.3.1984

über die Auswirkungen des Volkszählungsurteils

Auswirkungen des Volkszählungsurteils

– Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder und der Datenschutzkommission Rheinland-Pfalz –

**1. Allgemeine und grundsätzliche Konsequenzen**

1.1 Datenschutz hat Verfassungsrang

Das vom Bundesverfassungsgericht in seinem Urteil vom 15.12.1983 zum Volkszählungsgesetz 1983 festgestellte Recht auf informationelle Selbstbestimmung gewährleistet dem einzelnen die Befugnis, grundsätzlich selbst über die Preisgabe und Verwendung seiner Daten zu bestimmen. Es schützt ihn gegen unbegrenzte Erhebung, Speicherung, Verwendung und Weitergabe seiner persönlichen Daten. Einschränkungen dieses Rechts bedürfen einer verfassungsgemäßen gesetzlichen Grundlage.

Da das Bundesverfassungsgericht das Recht auf informationelle Selbstbestimmung unmittelbar aus Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG ableitet und als Konkretisierung des allgemeinen Persönlichkeitsrechts versteht, ist nunmehr klargestellt, daß der Datenschutz Verfassungsrang hat.

1.2 Datenschutz ist mehr als Schutz vor Mißbrauch

Durch die verfassungsrechtliche Verpflichtung des Gesetzgebers, für jede Einschränkung des Selbstbestimmungsrechts eine gesetzliche Grundlage zu schaffen, ist klargestellt, daß das Datenschutzrecht sich nicht allein auf den Schutz vor Mißbrauch der Daten beschränkt, sondern die Erhebung, Speicherung, Verwendung und Weitergabe personenbezogener Daten ohne Rücksicht darauf zu regeln hat, ob ein Mißbrauch zu befürchten ist. Damit bestätigt das Bundesverfassungsgericht das – bislang nicht unbestrittene – Datenschutzverständnis, daß Gegenstand des Datenschutzes der rechtmäßige Umgang mit personenbezogenen Daten ist und nicht nur die Verhinderung vorwerfbaren Fehlverhaltens.

1.3 Das Recht auf informationelle Selbstbestimmung ist umfassend

Das Recht auf informationelle Selbstbestimmung ist bei jeder Erhebung und jeder weiteren Verwendung personenbezogner Daten zu beachten. Es ist nicht auf bestimmte Datenarten begrenzt. Durch den Verwendungszusammenhang kann ein für sich gesehen belangloses Datum einen neuen Stellenwert erhalten, so daß die Sensitivität einer Angabe nicht Voraussetzung dafür ist, daß sie vom Recht auf informationelle Selbstbestimmung umfaßt wird. Entscheidend sind jeweils die Nutzbarkeit und die Verwendungsmöglichkeit der Daten. Das Bundesverfassungsgericht differenziert auch nicht nach den Verarbeitungsformen und bestimmten Verarbeitungsphasen.

Datenschutz besteht deshalb grundsätzlich unabhängig davon,
- welche personenbezogenen Daten berührt sind,
- ob die Verarbeitung manuell oder automatisiert erfolgt,
- ob die Daten in Dateiform oder auf andere Weise verarbeitet werden,
- ob eine der im geltenden BDSG definierten Phasen der Datenverarbeitung gegeben ist.

Gleichwohl sind die genannten Gesichtspunkte bei der Ausgestaltung des Datenschutzes zu berücksichtigen. So stellt das Gericht fest, daß es von Art, Umfang und denkbaren Verwendungen der personenbezogenen Daten sowie von der Gefahr ihres Mißbrauchs abhängt, inwieweit das Recht auf informationelle Selbstbestimmung und im Zusammenhang damit der Grundsatz der Verhältnismäßigkeit zu gesetzlichen Regelungen der Datenverarbeitung zwingen. Insbesondere die Regelungstiefe der gesetzgeberischen Maßnahmen muß sich also an den jeweiligen Umständen orientieren.

1.4 Daten dürfen nur für den festgelegten Zweck verwendet werden

Die Verwendung der Daten ist auf den gesetzlich bestimmten Zweck begrenzt. Schon angesichts der Gefahren der automatisierten Datenverarbeitung ist ein – amtshilfefester – Schutz gegen Zweckentfremdung durch Weitergabe- und Verwertungsverbote erforderlich. Die Zweckbindung ist nicht nur in den Fällen zu beachten, in denen eine Auskunftspflicht besteht. Sie gilt genauso für die Verarbeitung personenbezogener Daten, die der Betroffene freiwillig (für bestimmte, bei der Erhebung angegebene Zwecke) angibt.

Mit dem Gebot einer konkreten Zweckumschreibung korrespondiert das strikte Verbot, personenbezogene Daten auf Vorrat, d.h. zu unbestimmten oder noch nicht bestimmbaren Zwecken zu sammeln. Eine Ausnahme gilt für die Statistik.

1.5 Die Grundsätze der Normenklarheit und Verhältnismäßigkeit müssen beachtet werden

Einschränkungen des Rechts auf informationelle Selbstbestimmung sind nur im überwiegenden Allgemeininteresse zulässig. Sie bedürfen einer gesetzlichen Grundlage, die den Grundsätzen der Normenklarheit und der Verhältnismäßigkeit genügen muß.

Die Voraussetzung und der Umfang der Beschränkungen müssen für den Bürger erkennbar geregelt sein. Aufklärungs- und Auskunftspflichten müssen ergänzend für eine ausreichende Transparenz sorgen.

Die Angaben, deren Erhebung und Verwendung geregelt wird, müssen für den festgelegten Verwendungszweck geeignet und erforderlich sein. Zumindest im Falle der Datenerhebung unter Zwang und in vergleichbaren Fällen ist folgendes sicherzustellen:

- Beschränkung auf das zur Erreichung des festgelegten Zwecks notwendige Minimum,
- ein möglichst wenig belastendes Erhebungsverfahren,
- eine präzise Bestimmung des Verwendungszwecks,
- ein amtshilfefester Schutz gegen eine Zweckentfremdung der Daten,
- keine Erhebung von unzumutbaren Intimangaben und von Selbstbezichtigungen.

1.6 Es müssen bereichsspezifische Regelungen erlassen werden

Das Recht auf informationelle Selbstbestimmung darf grundsätzlich nur aufgrund bereichsspezifischer Regelungen eingeschränkt werden. Nur ausnahmsweise reichen Generalklauseln in den allgemeinen Datenschutzgesetzen als Auffangnormen aus.

Bereichsspezifische Regelungen sind nicht nur in allen Fällen des gesetzlichen Auskunftszwangs erforderlich, sondern auch dann, wenn es zu den Obliegenheiten des Betroffenen gehört, Auskünfte im Zusammenhang mit Leistungen zu erteilen, von denen er abhängig ist. Gleichzusetzen sind Fälle, bei denen die Datenerhebung bewußt ohne Wissen und Wollen des Betroffenen erfolgt, weil der Wille des Betroffenen in diesen Fällen ebenso wie in den Fällen des Auskunftszwangs von vornherein bewußt nicht berücksichtigt wird. Beispiele hierfür sind Datenerhebungen durch (geheime) Beobachtung des Betroffenen und durch Befragung Dritter, wenn die Zustimmung des Betroffenen nicht vorliegt.

Bereichsspezifischer Regelungen bedarf es auch dann,

- wenn sensitive personenbezogene Daten, z.B. Angaben über Gesundheit, politische oder religiöse Anschauungen, oder
- wenn unter Zwang erhobene personenbezogene Daten für andere als die bei der Erhebung angegebenen Zwecke verwendet und
- wenn personenbezogene Daten im Wege der Datenfernverarbeitung (on-line-Anschlüsse) übermittelt werden sollen.

Beim Erlaß bereichsspezifischer Regelungen ist folgendes zu beachten:

- Die Auskunftspflicht, die von ihr erfaßten Daten und deren Verwendung sind präzise zu bestimmen. Aufgabenzuweisungsnormen für die datenverarbeitenden Stellen und die allgemeinen Vorschriften des Datenschutzgesetzes, die auf die Erforderlichkeit für die Aufgabenerfüllung abstellen, begründen keinen Auskunftszwang.
- Die Bürger müssen aus den maßgeblichen Rechtsvorschriften – ggf. nach Aufklärung durch die Exekutive – erkennen können, „wer was wann und bei welcher Gelegenheit über sie weiß".
- Der Gesetzgeber ist verpflichtet, zur Wahrung des Rechts auf informationelle Selbstbestimmung mehr als bisher organisatorische und verfahrensrechtliche Vorkehrungen zu treffen.

1.7 Das Recht auf informationelle Selbstbestimmung gilt auch im privaten Bereich

Das Recht auf informationelle Selbsbestimmung knüpft an Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG an. Es gilt nicht nur für die Datenverarbeitung der öffentlichen Verwaltung, sondern auch für die Datenverarbeitung von Privaten (Wirtschaft, Medien, Verbände). Deshalb ist der Gesetzgeber verpflichtet, durch geeignete bereichsspezifische Regelungen und Kontrollvorkehrungen den einzelnen auch vor den Gefahren der Datenverarbeitung durch private Instanzen zu schützen.

Die gilt beispielsweise für folgende Bereiche, in denen das Recht auf informationelle Selbstbestimmung bislang durch pauschale Einwilligungserklärungen faktisch unterlaufen wird.

- Bei Banken ist die Verwendung aller bei Dienstleistungen anfallenden personenbezogenen Daten so zu regeln, daß die Entscheidungsfreiheit des Betroffenen gewahrt bleibt. Dies gilt insbesondere für Übermittlungen; bei der Weitergabe von personenbezogenen Daten an Auskunfteien muß sichergestellt werden, daß die Daten ausschließlich für die Beurteilung kreditorischer Risiken verwendet werden.
- Für die Datenverarbeitung in der Versicherungswirtschaft hat der Grundsatz der Zweckbindung besondere Bedeutung. Die Übermittlung personenbezogener Daten an andere Versicherer auch innerhalb einer Versicherungsgruppe darf nur unter engen Voraussetzungen und unter Wahrung strenger organisatorischer und verfahrensrechtlicher Vorkehrungen für die Datensicherung zugelassen werden.
- Die Erhebung und Verwendung von Patientendaten muß auf den Behandlungszusammenhang beschränkt sein; die Verwendung für andere Zwecke (z.B. Forschung) bedarf der Einwilligung des Betroffenen.

1.8 Wirksame Datenschutzkontrolle ist erforderlich

Nicht nur wegen der für den Bürger bestehenden Undurchsichtigkeit der Datenverarbeitung, sondern auch

im Interesse eines vorgezogenen Rechtsschutzes durch rechtzeitige Vorkehrungen mißt das Bundesverfassungsgericht der Beteiligung unabhängiger Datenschutzbeauftragter erhebliche Bedeutung für einen effektiven Schutz des Rechts auf informationelle Seibstbestimmung zu. Hieraus ergeben sich folgende praktische Konsequenzen:

- Die unabhängige Datenschutzkontrolle ist ein kraft der Verfassung notwendiges Element eines effektiven Grundrechts- schutzes. Dies hat der Gesetzgeber bei der Bestimmung der Aufgaben und Befugnisse der Datenschutzbeauftragten zu berücksichtigen.
- Die Aufgaben und Befugnisse der Datenschutzbeauftragten haben sich am Inhalt und Anwendungsbereich des Persönlichkeitsrechts auszurichten. Kontrollfreie Bereiche sind damit nicht zu vereinbaren.
- Bei der automatischen Datenverarbeitung kommt es in besonderem Maße darauf an, daß grundrechtssichernde Vorkehrungen rechtzeitig eingeplant werden. Eine Beteiligung von Datenschutzbeauftragten erst im Zeitpunkt der tatsächlichen Verarbeitung personenbezogener Angaben ist unzureichend. Die Informationspflichten der Verwaltung und die Befugnisse der Datenschutzbeauftragten müssen schon bei der Vorbereitung von Rechts- und Verwaltungsvorschriften und bei der Planung von (technischen) Vorhaben auf dem Gebiet der Informationsverarbeitung einsetzen.
- Niemand darf gemaßregelt oder benachteiligt werden, wenn er sich an den Datenschutzbeauftragten wendet.

Die Wirksamkeit der Datenschutzkontrolle im privaten Bereich darf dahinter nicht zurückbleiben.

## 2. Vordringliche Regelungen

Das Urteil des Bundesverfassungsgerichts hat weitreichende Auswirkungen auf die Erhebung und Verwendung personenbezogener Daten durch alle öffentlichen und nicht-öffentlichen Stellen. Die Datenschutzbeauftragten greifen im folgenden einige vordringlich zu regelnde Bereiche heraus:

### 2.1 Novellierung des Bundesdatenschutzgesetzes

Das Urteil unterstreicht die Notwendigkeit, das BDSG zu novellieren. Die Datenschutzbeauftragten sehen sich in ihren Forderungen bestätigt, die sie zuletzt in ihrer Entschließung vom 4.11.1983 zur Novelle des BDSG erhoben haben. Die Datenschutzbeauftragten erwarten, daß die Bundesregierung alsbald einen neuen Entwurf zur Novellierung des BDSG vorlegt, der den Anforderungen des Bundesverfassungsgerichts (vgl. Nr. 1) gerecht wird.

### 2.2 Informationsverarbeitung der Sicherheitsbehörden

Durch die Informationsverarbeitung der Behörden der Polizei, der Staatsanwaltschaft, des Verfassungsschutzes, des Bundesnachrichtendienstes und des Militärischen Abschirmdienstes wird der Bürger in der Regel empfindlich betroffen. Hinzu kommt, daß die Bürger die Speicherung und Verwendung von Daten in diesem Bereich meist nicht durchschauen können. Aus dem Urteil des Bundesverfassungsgerichts läßt sich ableiten, daß die gesamte Informationsverarbeitung im Bereich der Gefahrenabwehr und der Strafverfolgung sowie die Tätigkeit der Nachrichtendienste präzise geregelt werden müssen. Deshalb sind die Strafprozeßordnung sowie die Polizeigesetzes und die Verfassungsschutzgesetze des Bundes und der Länder zu novellieren. Für den Militärischen Abschirmdienst und den Bundesnachrichtendienst sind gesetzliche Grundlagen zu schaffen. Sämtliche Verknüpfungs- und Verwertungsmöglichkeiten und auch die Dauer der Aufbewahrung müssen konkret geregelt werden. Im einzelnen festzulegen sind beispielsweise die Voraussetzungen und Grenzen der polizeilichen Beobachtung, des Abgleichs mit anderen Datenbeständen und der Identitätsfeststellungen sowie die Kriterien und das Verfahren der erkennungsdienstlichen Behandlung. Über Personen, die nicht Verdächtige und nicht Störer sind, dürfen Daten nur unter sehr engen Voraussetzungen verarbeitet werden. Auch die Nutzung moderner Aufzeichnungstechniken ist gesetzlich festzulegen und einzugrenzen. Zu regeln ist auch die Amtshilfe: Die Tätigkeitsbereiche von Polizei und Nachrichtendiensten, die sich in der Praxis vielfach überlappen, müssen klar voneinander getrennt werden; es muß sichergestellt werden, daß Übermittlungen auf das für die Aufgabenerfüllung unerläßliche Maß beschränkt werden. Auf keinen Fall darf im Erlaßwege die Verpflichtung des Bundesgrenzschutzes zur Amtshilfe gegenüber Vefassungsschutz und Bundesnachrichtendienst erweitert werden, wie es z.Z. beabsichtigt ist.

Die Pflicht zur Erteilung von Auskünften an die Bürger ist auf die Sicherheitsbehörden auszudehnen. Soweit die Aufgabenerfüllung Ausnahmen von der Auskunftspflicht gebietet, sind diese gesetzlich festzulegen. Da die Verweigerung der Auskunft durch Gerichte und Datenschutzkontrollinstanzen nachprüfbar sein muß, dürfen Sicherheitsbehörden nicht von der Begründungspflicht freigestellt werden.

### 2.3 Personalausweisgesetz

Die Datenschutzbeauftragten des Bundes und der Länder begrüßen die Absicht, den Termin für das Inkrafttreten des Bundespersonalausweisgesetzes aufzuheben und die Einführung der neuen Personalausweise einstweilen zurückzustellen.

Verpflichtungen des Bürgers, für die Ausstellung eines Personalausweises und bei dessen Kontrolle personenbezogene Daten preiszugeben und anschließende Verwendungen zu dulden, sind als Einschränkungen seines Rechts auf informationelle Selbst bestimmung nur im überwiegenden Allgemeininteresse zulässig und bedürfen bereichsspezifischer gesetzlicher Grundlagen, die dem Gebot der Normenklarheit und Verhältnismäßigkeit entsprechen müssen.

Ob es im überwiegenden Allgemeininteresse geboten ist, den Personalausweis maschinenlesbar zu gestalten, wird inzwischen von vielen Experten bezweifelt. Insbesondere ist es fraglich, ob ein mit der Maschinenlesbarkeit möglicherweise erreichbarer Sicherheitsgewinn neue Risiken für das Persönlichkeitsrecht rechtfertigt. Die Datenschutzbeauftragten empfehlen daher nochmals zu prüfen, ob auf einen solchen Personalausweis nicht doch verzichtet werden kann.

Sollte der Gesetzgeber nach erneuter Prüfung die Einführung des neuen Personalausweises gleichwohl für unerläßlich halten, so ist nach dem Urteil nachdrücklich an die gebotenen flankierenden Maßnahmen zu erinnern: Wie der Deutsche Bundestag schon in seiner Entschließung vom 17.1.1980 und die Datenschutzbeauftragten des Bundes un der Länder nochmals in ihrem Konferenzbeschluß vom 13.9.1983 klargestellt haben, sind gesetzliche Regelungen für die Informationsverarbeitung der Polizei im Polizeirecht des Bundes und der Länder sowie im Strafverfahrensrecht von Verfassungs wegen unerläßlich. Insbesondere die Voraussetzungen für polizeiliche Beobachtungen und für Identitätsfeststellungen sowie die Verwendungszwecke erhobener Daten müssen präzise bestimmt werden. Das Gesetz über Personalausweise selbst genügt in einer Reihe von Vorschriften nicht den Geboten der Normenklarheit und Verhältnismäßigkeit. So sind die mit der Maschinenlesbarkeit verbundenen Fragen (Lesezone, Nutzungsmöglichkeiten) nicht klar genug geregelt. Auch fehlt es an Vorkehrungen, die die Erstellung von Bewegungsbildern verhindern, an einer Definition des Fahndungsbegriffs und an einer Vorschrift, die den Inhalt und die Verwendung der örtlichen Personalausweisregister regelt.

Die Datenschutzbeauftragten unterstreichen, daß eine Einführung neuer maschinenlesbarer Personalausweise jedenfalls so lange unterbleiben muß, bis die geforderten gesetzlichen Regelungen für den Sicherheitsbereich in Bund und Ländern in Kraft getreten sind.

2.4 Meldewesen

Das Meldewesen darf nicht die Funktion einer potentiell unbegrenzten Informationssammlung oder -bereitstellung für Aufgaben anderer Behörden übernehmen. In der Formulierung des § 1 Abs. 1 MRRG muß dies dadurch zum Ausdruck gebracht werden, daß die Registrierung der für Zwecke der Identitätsfeststellung und des Wohnungsnachweises nicht erforderlichen Daten nur zugelassen wird, soweit es sich um bestimmte traditionelle Mitwirkungstätigkeiten der Meldebehörde (Wahlen, Lohnsteuerkartenausstellung, Personalausweise, Wehrdienst, Familienbuch) handelt oder soweit eine eigene Datenerhebung und -speicherung durch die Behörde, die die Daten zur Erfüllung ihrer gesetzlich festgelegten Aufgaben benötigt, nur mit unverhältnismäßig hohem Aufwand möglich ist. Nach § 2 Abs. 3 MRRG kann durch Landesgesetz bestimmt werden, daß für die Erfüllung von Aufgaben der Länder weitere Daten gespeichert werden dürfen. Mit Rücksicht auf die verfassungsrechtlichen Schranken einer Erweiterung der Zwecke des Meldewesens sollte auch diese Ermächtigung enger gefaßt werden.

Die Übermittlungsvorschrift des § 18 Abs. 1 Satz 1 MRRG übernimmt derzeit fast wörtlich die Fassung der Generalklausel des § 10 Abs. 1 Satz 1 BDSG und entbehrt deshalb der bereichsspezifischen Präzisierung, die das BVerfG für die Verwendung zwangsweise erhobener Daten fordert. Da der im Einzelfall möglicherweise entstehende Übermittlungsbedarf nicht von vornherein ermittelt werden kann, erscheint eine Konkretisierung in der Weise, daß alle denkbaren Übermittlungsempfänger und deren Aufgaben enumerativ aufgeführt werden, nicht möglich. Um gleichwohl hinreichenden Schutz herzustellen, muß die Zulässigkeit der Datenübermittlung davon abhängig gemacht werden, daß wenigstens die Verwendung der Daten durch den Datenempfänger bereichsspezifisch präzisiert ist. Im MRRG ist dies dadurch zum Ausdruck zu bringen, daß Übermittlungen nach § 18 Abs. 1 Satz 1 nur zur Erfüllung gesetzlich festgelegter Aufgaben zulässig sind.

Der formale Gesetzes- bzw. Verordnungsvorbehalt in § 20 Abs. 1 in Verbindung mit § 18 Abs. 4 MRRG eröffnet die Einrichtung regelmäßiger Datenübermittlungen ohne inhaltliche Einschränkungen und grenzt weder den Kreis der Datenempfänger noch die zur Übermittlung vorgesehenen Datenarten, die Übermittlungszwekke und den Verwendungszusammenhang ein. § 20 Abs. 1 MRRG als Ermächtigungsgrundlage für Verordnungen genügt damit nicht dem verfassungsrechtlichen Gebot der Normenklarheit.

Der Grundsatz der Normenklarheit für gesetzliche Einschränkungen des Rechts auf informationelle Selbstbestimmung gebietet es, widersprüchliche Regelungen in verschiedenen Gesetzen zu beseitigen. Nach § 3 Abs. 4 des Personalausweisgesetzes darf die Seriennummer des Personalausweises nicht zur Errichtung und Erschließung von Dateien verwendet werden. Daher ist es nicht angängig, daß Landesmeldegesetze aufgrund landesrechtlicher Bedürfnisse (§ 2 Abs. 3 MRRG) die Speicherung dieses Merkmals im Melderegister vorschreiben. Denn die Speicherung der Seriennummer würde es unter geeigneten technisch-organisatorischen Bedingungen ermöglichen, das Melderegister mit ihrer Hilfe zu erschließen. Die Speicherung der Seriennummer im Melderegister muß auch deshalb unterbleiben, weil der Bundesgesetzgeber sie für die von ihm bestimmten Aufgaben des Meldewesens nicht für erforderlich erachtet hat und weil die Gefahr besteht, daß aufgrund der Übermittlungsregelungen des Landesmelderechts die Seriennummer an Stellen weitergegeben werden könnte, bei denen eine dem § 3 Abs. 4 Personalausweisgesetz zuwiderlaufende Verwendung nicht auszuschließen ist.

Auch die landesgesetzlichen Vorschriften bedürfen einer Überprüfung. Insbesondere muß sichergestellt werden, daß die Meldedaten auch innerhalb der Gemeindeverwaltung grundsätzlich nur zweckgebunden verwertet werden. Die Voraussetzungen für die Nutzung der besonderen Meldescheine für Beherbergungsstätten (vgl. z.B. § 24 MG BW) sowie der Beherbergungsverzeichnisse von Krankenhäusern und Heimen (vgl. z.B. §§ 25, 26 Abs. 2 MG BW) müssen eingeschränkt werden.

Gegen die ausschließliche Verantwortung des Datenempfängers für die Datenübermittlung (nur in § 29 Abs. 1 Satz 3 MG BW) bestehen Bedenken. Hinsichtlich der Gruppenauskunft an Parteien und Wählergruppen (vgl. z.B. § 34 Abs. 1 MG BW) sollte eine Widerspruchsmöglichkeiten für den Bürger festgelegt werden.

2.5 Statistik

Eine Volkszählung darf künftig nur noch als reine Statistik durchgeführt werden. Übermittlungen von Einzel-

angaben aus der Volkszählung zu anderen als statistischen Zwecken sind in Zukunft ausgeschlossen. Auch zu statistischen Zwecken dürfen sie nur dann übermittelt werden, wenn durch Rechtsvorschrift, Organisation und geeignete Verfahren sichergestellt ist, daß die statistische Zweckbindung der Daten strikt eingehalten wird und keine Vermischung administrativer und statistischer Aufgaben eintritt.

Besondere Bedeutung hat das Gericht dem Grundrechtsschutz durch Verfahren beigemessen, der von nun an bei der Ausgestaltung jeder amtlichen Statistik beachtet werden muß. Hierzu zählen u.a. Form und Verfahren der statistischen Erhebung, Auswahl der Zähler und Maßnahmen der Datensicherung, Belehrung und damit korrespondierende Auskunftsverpflichtung, verbunden mit einer deutlichen Empfehlung an den Gesetzgeber, diese „grundrechtssichernden Maßnahmen" durch Rechtsvorschrift zu garantieren.

Der Gesetzgeber muß darüber hinaus vor jeder Totalerhebung prüfen, ob diese nach dem jeweils aktuellen Stand der sozialwissenschaftlichen und statistischen Methoden noch verhältnismäßig ist. Seine „Methodenwahl" ist also jeweils wissenschaftlich zu legitimieren mit der Pflicht, bei geänderten Umständen ggf. von einer Befragung aller Bürger abzusehen.

Das Statistikgeheimnis selbst (§ 11 Bundesstatistikgesetz) muß neu formuliert werden; hierbei müssen Geheimhaltungs- und Übermittlungsnormen getrennt und eindeutige Kriterien für Anonymität, faktische Anonymisierung und Aggregation von Einzelangaben geschaffen werden.

Eng damit zusammen hängt auch das Verbot der Vermischung statistischer und administrativer Funktionen. Damit wird für alle Statistiken, die diese Funktionsvermischung kennen, eine Revision erforderlich, weil sonst eine verfassungskonforme Durchführung dieser Statistiken nicht mehr gewährleistet wäre. Hierzu gehören beispielsweise die Statistik der Bevölkerungsbewegung, die Hochschulstatistik, die Berufsbildungsstatistik und die Viehzählungsstatistik.

Grundrechtssichernde Verfahren sind bei der EG-Arbeitskräftestichprobe erforderlich. Die EG-Verordnung entspricht nicht den verfassungsrechtlichen Kriterien des Volkszählungsurteils, insbesondere das Erhebungsprogramm und das Verfahren der Statistik widersprechen dem verfassungsrechtlichen Bestimmtheitsgebot. Auch das Verfahren des Mikrozensus ist zu überprüfen. Die Datenschutzbeauftragten verweisen insoweit auf ihren Beschluß vom 27./28.3.1984.

Die Landesgesetzgeber werden nicht mehr umhin können, Landesstatistiken gesetzlich zu regeln. Die Kommunalstatistik bedarf gleichfalls einer gesetzlichen Grundlage und ebenso einer durch Rechtsvorschrift garantierten Abschottung zu der übrigen Gemeindeorganisation in den jeweiligen Gemeindeordnungen der Länder. Eine spezialgesetzliche Norm für Planungs- und Statistikdaten könnte die gleiche Funktion haben. Die rechtliche Notwendigkeit ergibt sich aus dem Gebot der „informationellen Gewaltenteilung" innerhalb der Gemeindeorganisation, das das Bundesverfassungsgericht formuliert hat.

2.6 Sozial- und Gesundheitsverwaltung

Das Zehnte Buch des Sozialgesetzbuches enthält zwar bereichsspezifische Datenschutzregelungen; doch sind auch hier weitere Verbesserungen geboten. Ergänzungsbedürftig sind insbesondere die Regelungen über den Umfang der Datenerhebungen durch die Sozialleistungsträger sowie über den Austausch personenbezogener Daten der Sozialleistungsträger untereinander.

Im Rahmen der Mitwirkungspflicht (§ 60 SGB I) dürfen vom Antragsteller pauschale Einwilligungserklärungen nicht verlangt werden, ohne daß die Erforderlichkeit der Erhebung und Weitergabe von Daten streng überprüft worden ist. Dem Gebot, sich auf das für die Erreichung des angestrebten Zwecks erforderliche Minimum zu beschränken, wird künftig mehr Beachtung geschenkt werden müssen.

§ 69 SGB X läßt unter der Voraussetzung der Erforderlichkeit für die Aufgabenerfüllung einen großzügigen Datenaustausch der Sozialleistungsträger untereinander, aber auch mit dritten Stellen zu, die in die Gewährung von Sozialleistungen eingebunden sind. In zunehmendem Maße erhalten die Sozialversicherungsnummer, aber auch andere Kennzeichnungen (wie z.B. Betriebs-Nr. und Institutions-Nr.) die Funktion von Surrogaten eines Personenkennzeichens. Deshalb müssen dem Datenaustausch auch innerhalb der Sozialverwaltung künftig klarere Grenzen gezogen werden.

Ein hoher Regelungsbedarf besteht auch für die Gesundheitsverwaltung. Zwar gewährleistet die ärztliche Schweigepflicht Schutz vor der Offenbarung medizinischer Daten an Dritte. In welchem Umfang aber etwa im Rahmen der öffentlichen Gesundheitsfürsorge oder der kassenärztlichen Abrechnung Daten offenbart werden dürfen, ist weitgehend unklar.

Die Erhebung und Verarbeitung medizinischer Daten, insbesondere in der öffentlichen Gesundheitsverwaltung, sind eindeutig gesetzlich zu regeln. Die Aufgaben und Befugnisse des Amtsarztes gegenüber den Bürgern und seine Zusammenarbeit mit anderen Stellen (Sozialämter, Jugendämter, öffentliches Personalwesen, niedergelassene Ärzte und Krankenhäuser) müssen festgelegt werden. Der Betroffene muß stets wissen, ob das Gesundheitsamt ihn lediglich berät, auf freiwilliger Basis ein Gutachten erstellt oder im überwiegenden Allgemeininteresse Maßnahmen auch zwangsweise gegen ihn durchsetzen kann.

Auch innerhalb der Gesundheitsverwaltung muß die Verschiedenartigkeit der Funktionen (z.B. Bekämpfung ansteckender Krankheiten oder Beratung von Sucht- und Abhängigkeitskranken) bei der Festlegung von Zugriffsberechtigungen und bei der Datensicherung berücksichtigt werden.

2.7 Arbeitnehmerdatenschutz

Angesichts der Gefährdung des Rechts auf informationelle Selbstbestimmung durch die umfassenden Kontrollmöglichkeiten moderner Personalinformationssysteme bedarf auch die Verarbeitung von Arbeitnehmerdaten einer speziellen gesetzlichen Schutzregelung; eine korrigierende Auslegung bestehender Vorschriften im Sinne der „Drittwirkung" reicht zur Gewährleistung des Grundrechts nicht aus.

Die Anforderungen des BVerfG gelten in jedem Fall dort, wo ein Zwang zur Angabe personenbezogener Daten besteht, wo etwa der Arbeitgeber entweder in die Datenerhebung zugunsten von Steuerbehörden und Sozialleitstungsträgern eingeschaltet ist oder aber selbst anstelle der Sozialverwaltung Leistungen gewährt. Datenbestände, die der Arbeitgeber zu Zwecken der Kindergeldgewährung, der Unterstützung im Krankheitsfall (Beihilfe) usw. erhebt und vorhält, müssen dementsprechend aufgrund spezieller Rechtsvorschrift strikt zweckgebunden genutzt und von den für die Personalverwaltung bestimmten Informationen abgeschottet werden.

Wegen der Abhängigkeit des Arbeitsnehmers von Arbeitsplatz und Einkommen zur Sicherung seiner Existenz stellt sich für ihn darüber hinaus generell die Pflicht zur Angabe seine Daten als zwangsweise Erhebung im Sinne der Urteilsgründe dar. Hieraus ergibt sich für das Beschäftigungsverhältnis die Notwendigkeit einer bereichsspezifischen und präzisen Bestimmung der Verwendungszwecke der erhobenen Daten, des Schutzes vor Zweckentfremdung durch Weitergabe- und Verwertungsverbot sowie der Beschränkung auf das zur Zweckerreichung erforderliche Datenminimum. Die Bestimmungen der §§ 23 ff. BDSG genügen – auch im Zusammenwirken mit Regelungen des sonstigen arbeitsrechtlichen Informationsschutzes – den Anforderungen an Zweckbindung und Normenklarheit nicht.

Vielmehr muß gesetzlich festgelegt werden,

- daß Speicherung, Auswertung, Veränderung und Übermittlung von Arbeitnehmerdaten auf die Fälle gesetzlicher Verarbeitungspflichten und der Duchführung der Arbeits- bzw. Dienstverhältnisse beschränkt wird, mithin die Verarbeitungsbefugnis aufgrund „berechtigter Interessen" des Arbeitgebers entfällt,
- daß Auswertungen und Verknüpfung, die zur Herstellung eines „Persönlichkeitsbildes" der Arbeitnehmer führen, sowie die Speicherung solcher „Profile" grundsätzlich unzulässig sind.

Als verfahrensrechtliche Schutzvorkehrungen fordert das Gericht die Statuierung von Aufklärungs-, Auskunfts- und Löschungspflichten, um Datentransparenz herzustellen bzw. die Zweckbindung zu verstärken.

- Der Auskunftsanspruch des Arbeitsnehmers ist daher über § 26 Abs. 2 BDSG hinaus auszudehnen auf alle, nicht nur die regelmäßigen Datenempfänger, sowie die Auswertungsprogramme bzw. Einzelauswertungen, in die seine Daten einbezogen werden.
- Die Auskunftseinschränkungen nach Nr. 4 und 5 von § 26 Abs. 4 BDSG (bei Daten aus allgemein zugänglichen Quellen und bei gesperrten Daten) müssen entfallen.
- Daten müssen – vergleichbar der Regelung in § 84 SGB X – dann gelöscht und nicht nur gesperrt werden, wenn sie zur Durchführung des Arbeitsverhältnisses nicht mehr erforderlich sind und durch die Löschung schutzwürdige Belange des Beschäftigten nicht beeinträchtigt werden.

Anhang Nr. 4 04.11.1983

**Erklärung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder und der Datenschutzkommission Rheinland-Pfalz zur Novellierung des Bundesdatenschutzgesetzes**

I. Die öffentliche Diskussion zu den Themen Volkszählung, maschinenlesbarer Personalausweis, Personalinformationssysteme wie auch Bildschirmtext und andere Neue Medien zeigt eine zunehmende Sensibilisierung zu Fragen des Datenschutzes. Vor diesem Hintergrund ist in der Öffentlichkeit die Erwartung entstanden, daß eine Novellierung des Bundesdatenschutzgesetzes

- die bisher gewonnenen Erfahrungen sowie die neu aufgetretenen Probleme aufgreift und regelt und
- den Datenschutzinstanzen wirksamere Kontrollinstrumente an die Hand gibt.

Die Datenschutzbeauftragten haben sich mehrfach für eine Novellierung ausgesprochen und sind nach wie vor der Meinung, daß das Bundesdatenschutzgesetz novellierungsbedürftig ist. Sie sehen jedoch im vorliegenden Referentenentwurf keinen geeigneten Beitrag zur Fortentwicklung des Datenschutzes, weil er

1. das geltende Datenschutzrecht teilweise verschlechtert,
2. hinter den bisherigen Entwürfen (CDU-Entwurf von 1980, SPD/FDP-Entwurf von 1980, Referentenentwurf von 1982) zurückbleibt,
3. wesentliche Forderungen der Datenschutzbeauftragten (Beschluß der Konferenz vom 21.6.1982) unberücksichtigt läßt und
4. den Anforderungen nicht gerecht wird, die sich aus der technischen Entwicklung ergeben.

II. Die Datenschutzbeauftragten fordern zu folgenden Punkten:

1. Aufgabe des Datenschutzes

   Die Umschreibung der Aufgabe des Datenschutzes im Bundesdatenschutzgesetz als Schutz vor Mißbrauch ist irreführend, widerspricht dem Regelungsgehalt des Gesetzes und verkürzt den Schutz des Betroffenen. Im Gesetz ist deshalb klarzustellen: Aufgabe des Datenschutzes ist die Regelung des rechtmäßigen Umgangs mit personenbezogenen Daten und nicht nur die Verhinderung vorwerfbaren Fehlverhaltens. Neben der Speicherung, Veränderung, Löschung und Übermittlung sind deshalb auch die Erhebung und sonstige Nutzung Gegenstand des Datenschutzes.

2. Dateibegriff

   Die Entscheidung des Gesetzgebers, bei der Anwendung des Bundesdatenschutzgesetzes von der Verarbeitung personenbezogener Daten in Dateien auszugehen, ist für den Bürger kaum verständlich, führt in der Praxis zu Unzuträglichkeiten und mindert die Wirksamkeit des Datenschutzes. Solange diese Anknüpfung besteht, muß der Dateibegriff wenigstens so definiert werden, daß ein Höchstmaß an Schutz für den Betroffenen erreicht wird. Dazu gehört, daß alle automatisierten Verfahren und alle Akten und Akten-

sammlungen einbezogen werden, die mit Hilfe automatisierter Verfahren erschlossen werden können.

3. Interne Dateien

   Ausnahmeregelungen für interne Dateien sind mit einem konsequenten Schutz der Betroffenen unvereinbar. Deshalb muß das Bundesdatenschutzgesetz grundsätzlich auch auf interne Dateien anwendbar sein.

4. Einwilligung

   Da das Gesetz jede Datenverarbeitung zuläßt, wenn die Einwilligung des Betroffenen vorliegt, muß der Gesetzgeber durch besondere Regelungen den Betroffenen davor schützen, daß er durch soziale, wirtschaftliche und psychische Zwänge (etwa als Mieter, Patient oder Arbeitssuchender) in seiner Entscheidungsfreiheit unangemessen eingeschränkt wird.

5. Unterrichtung des Betroffenen

   Transparenz der Datenverarbeitung ist eine notwendige Voraussetzung des Datenschutzes. Der Betroffene ist deshalb in jedem Fall über die Tragweite seiner Einwilligung in die Datenverarbeitung sowie über die Rechtsgrundlage der Datenerhebung zu unterrichten, und zwar auch dann, wenn er dies nicht ausdrücklich verlangt. Die Unterrichtung bei der Datenerhebung muß ohne Rücksicht darauf erfolgen, ob die Daten in einer Datei, in Akten oder sonstigen Unterlagen festgehalten werden.

6. Verschuldensunabhängiger Schadensersatzanspruch und Folgenbeseitigungsanspruch

   Bei unzulässiger oder unrichtiger Datenverarbeitung muß der Betroffene einen verschuldensunabhängigen Schadensersatzanspruch (auch für Nichtvermögensschäden) sowie einen Folgenbeseitigungsanspruch haben.

7. On-line-Anschlüsse

   Der direkte Zugriff auf automatisierte Dateien über on-lineAnschlüsse ist für den Bürger mit besonderen Risiken verbunden. Dies gilt vor allem dort, wo Daten aus dem Medizin-, Sozial- und Sicherheitsbereich oder über strafbare Handlungen, Ordnungswidrigkeiten, religiöse und politische Anschauungen zum Abruf bereitgehalten werden. Diesen Risiken trägt der Entwurf nicht hinreichend Rechnung. Die Anforderungen an die Zulässigkeit von on-line-Anschlüssen sind zu erhöhen und präziser zu fassen.

8. Zweckbindung

   Die Zweckbindung der Daten ist eine der wichtigsten Voraussetzungen für den Schutz des Bürgers. Sie muß insbesondere in folgenden Bereichen verstärkt werden:

   - Die Datenweitergabe innerhalb derselben Behörde muß grundsätzlich den gleichen Einschränkungen unterworfen werden wie die Datenübermittlung an andere öffentliche Stellen.
   - Bei der Datenübermittlung an andere öffentliche Stellen muß die Verantwortung der übermittelnden Stelle ungeschmälert bleiben.
   - Werden Daten an Stellen außerhalb des öffentlichen Bereichs übermittelt, so darf der Empfänger die Daten nur für den Zweck verwenden, zu dessen Erfüllung sie ihm übermittelt wurden.

9. Auskunftsanspruch

   Das Recht des Bürgers auf Auskunft über seine Daten ist ein grundlegendes Datenschutzrecht. Es darf nicht eingeschränkt, sondern muß verstärkt werden. Dieses Auskunftsrecht muß gegenüber allen Behörden bestehen, grundsätzlich auch gegenüber den Sicherheits- und Finanzbehörden. Eine generelle Befreiung von der Begründungspflicht ist abzulehnen. Sie stände weder mit der Verfassung noch mit der Rechtssprechung in Einklang. Die Verweigerung einer Auskunft in Ausnahmefällen muß nachprüfbar sein. Die Erteilung der Auskunft muß stets kostenfrei sein.

10. Kontrolle

    Im Interesse des Bürgers ist eine unabhängige und umfassende Datenschutzkontrolle unerläßlich. Die Datenschutzbeauftragten stellen dazu fest:

    - Ihre Kontrollbefugnis umfaßt die Einhaltung der Datenschutzgesetze und aller anderen Datenschutzvorschriften, unabhängig davon, ob Daten in Dateien, in Akten oder in sonstiger Form festgehalten werden.
    - Sie haben das Recht, uneingeschränkt alle Akten einzusehen, die mit der Verarbeitung personenbezogener Daten in Zusammenhang stehen.
    - Besondere Geheimhaltungsvorschriften können ihnen bei ihrer Tätigkeit nicht entgegengehalten werden.

III. Eine Novellierung des Bundesdatenschutzgesetzes kann notwendige bereichsspezifische Regelungen nicht ersetzen. Die Datenschutzbeauftragten erinnern an ihre frühere Forderung nach Sonderregelungen insbesondere für den Sicherheitsbereich und für den Arbeitnehmerdatenschutz.

IV. Unabhängig von den verschiedenen Vorstellungen zur Novellierung des Bundesdatenschutzgesetzes können und dürfen die sich aus der technologischen Entwicklung ergebenden Konsequenzen nicht übersehen werden. Das Vordringen mittlerer und kleinerer Datenverarbeitungssysteme, die automatisierte Textverarbeitung sowie die Einführung bundesweiter Kommunikationssysteme stellen die Eignung des jetzigen Datenschutzkonzeptes in Frage. Der Gesetzgeber wird daher nicht umhin können, in naher Zukunft erneut und umfassend zum Datenschutz Stellung zu beziehen.

Anhang Nr. 5 27./28.3.84

Konferenz der Datenschutzbeauftragten des Bundes und der Länder

**Erklärung zur Kabelkommunikation**

In mehreren Bundesländern werden in nächster Zeit Projekte zur Einführung von Kabelrundfunk und Kabelkommunikation auf Breitbandkabel geplant oder teilweise beginnen. Angesichts der Gefahren, die für den Persönlichkeitsschutz der Teilnehmer aus dem Betrieb dieser Systeme entstehen können, haben die Datenschutzbeauftragten des Bundes und der Länder Vorstellungen über eine gesetzliche Regelung des Datenschutzes bei der Kabelkommmunikation ent-

wickelt. Sie sind dabei von den Grundsätzen für den Datenschutz bei den Neuen Medien (insbesondere bei Bildschirmtext und Kabelfernsehen) ausgegangen, die auf der 7. Konferenz am 11. Dezember 1980 in Berlin beschlossen wurden.

Zur Sicherung des Datenschutzes halten sie eine gesetzliche Regelung für erforderlich, die vorbehaltlich der bei den einzelnen Projekten in den Ländern entstehenden Gestaltungsunterschiede nach dem gegenwärtigen Erkenntnisstand zumindest folgende Regelungen enthalten muß:

A
Datenschutz

Abs. 1:

Für die Erhebung, Verarbeitung und sonstige Nutzung personenbezogener Daten sind, soweit nichts anderes bestimmt ist, die jeweils geltenden Vorschriften über den Schutz personenbezogener Daten anzuwenden, unabhängig davon, ob die Daten in einer Datei verarbeitet werden.

Abs. 2:

Personenbezogene Daten über die Inanspruchnahme einzelner Angebote dürfen nur erhoben und gespeichert werden, soweit und solange diese erforderlich sind, um

1. den Abruf von Angeboten zu vermitteln (Verbindungsdaten),
2. die Abrechnung der für die Inanspruchnahme der technischen Einrichtungen und der Angebote seitens des Teilnehmers zu erbringenden Leistungen zu ermöglichen (Abrechnungsdaten).

Abs. 3:

Die Speicherung der Abrechnungsdaten (Abs. 2 Nr. 2) darf Zeitpunkt, Dauer, Art, Inhalt und Häufigkeit bestimmter vom einzelnen Teilnehmer in Anspruch genommener Angebote nicht erkennen lassen, es sei denn, der Teilnehmer beantragt eine andere Art und Weise der Speicherung. Die Übermittlung (Bekanntgabe) von Abrechnungs- und Verbindungsdaten an Anbieter und Dritte ist unzulässig. Abrechnungsdaten sind zu löschen, sobald sie für Zwecke der Abrechnung nicht mehr erforderlich sind. Verbindungsdaten nach Abs. 2 Nr. 1 im übrigen sind nach Ende der jeweiligen Verbindung zu löschen.

Abs. 4:

Die Abs. 2 und 3 gelten entsprechend für Einzelmitteilungen.

Abs. 5:

Für das Bereithalten personenbezogener Daten als Inhalt von Angeboten sind auf den Anbieter die für die Übermittlung geltenden Vorschriften über den Datenschutz anzuwenden und vom Anbieter zu beachten.

Abs. 6:

Der Anbieter darf vom Teilnehmer personenbezogene Daten nur erheben, wenn die Inanspruchnahme von Angeboten anderenfalls unmöglich wäre. Werden Daten des Teilnehmers vom Anbieter gespeichert oder übermittelt, ist der Teilnehmer hierauf vor der Erhebung besonders hinzuweisen. Diese Daten dürfen ohne Einwilligung des Betroffenen nur im Rahmen der Zweckbestimmung des Angebots verarbeitet werden. Der Teilnehmer ist in geeigneter Weise über die Bedeutung der Einwilligung aufzuklären. Die Leistung darf nicht davon abhängig gemacht werden, daß der Betroffene in die Verarbeitung seiner Daten außerhalb der Zweckbestimmung des Angebots einwilligt. Wird die Einwilligung über den Rückkanal gegeben, so wird sie nach Bestätigung durch den Betroffenen wirksam.

Abs. 7:

Zu Zwecken der wissenschaftlichen Begleitforschung sowie zur Feststellung der Akzeptanz der Kabelkommunikation und von anderen Diensten dürfen personenbezogene Daten nur erhoben und gespeichert werden, wenn der Betroffene eingewilligt hat; über die Bedeutung der Einwilligung ist er vorher in geeigneter Weise aufzuklären. Eine weitere Datenverarbeitung ist nur zulässig, wenn die Einzelangaben so anonymisiert werden, daß sie dem Betroffenen nicht mehr zuzuordnen sind.

Abs. 8:

Personenbezogene Daten, die über Abs. 2 bis 7 hinaus im Zusammenhang mit der Kabelkommunikation erhoben und gespeichert werden, dürfen an Dritte nur übermittelt werden, wenn der Betroffene eingewilligt hat. Abs. 7 Satz 1, 2. Halbsatz findet Anwendung.

Abs. 9:

Die Auskunfts-, Berichtigungs-, Löschungs- und Sperrungsansprüche der Teilnehmer nach Datenschutzrecht bleiben unberührt. Die Auskunftsansprüche gelten entsprechend für die gem. Abs. 5 gespeicherten Daten. Die Ansprüche nach Sätzen 1 und 2 richten sich gegen den Anbieter, soweit personenbezogene Daten den Inhalt von Angeboten betreffen oder vom Anbieter gespeichert werden, im übrigen gegen den Betreiber. Der Teilnehmer hat ferner einen Anspruch auf Löschung der Abrechnungs- oder Verbindungsdaten, soweit der Betreiber zur Löschung gem. Abs. 3 Satz 3 und 4 verpflichtet ist.

Abs. 10:

Die bei dem Betreiber tätigen Personen sind zur Geheimhaltung der bei ihrer Tätigkeit bekannt gewordenen Tatsachen verpflichtet, soweit sie nicht offenkundig sind oder ihrer Natur nach der Geheimhaltung nicht bedürfen.

B
Fernwirkdienste

Abs. 1:

Angebote, die ferngesteuert in der Wohnung von Teilnehmern Messungen vornehmen oder andere Wirkungen auslösen (Fernwirkdienste), dürfen nur mit schriftlicher Einwilligung des Betroffenen eingesetzt werden. Dieser ist zuvor über den Verwendungszweck sowie über Art, Umfang und den Zeitpunkt des Einsatzes der Dienste zu unterrichten. Verweigert ein Betroffener seine Einwilligung, dürfen ihm keine Nachteile entstehen, die über die unmittelbaren Kosten der Verweigerung hinausgehen. Der Betroffene kann seine Einwilligung jederzeit widerrufen.

Abs. 2:

Soweit im Rahmen von Fernwirkdiensten personenbezogene Daten erhoben werden, dürfen diese nur zu den vereinbarten Zwecken verarbeitet werden. Sie sind zu löschen, wenn sie zur Erfüllung dieser Zwecke nicht mehr erforderlich sind. Im übrigen gelten die Vorschriften über den Datenschutz und über technisch-organisatorische Maßnahmen entsprechend.

Abs. 3:

Die Einrichtung von Fernwirkdiensten ist nur zulässig, wenn beim Betroffenen ein Anzeigengerät installiert ist, das jederzeit erkennen läßt, wann ein Dienst in Anspruch genommen wird und welcher Art der Dienst ist und wenn der Betroffene jederzeit den Dienst abschalten kann. Im Zweifel gilt das Abschalten eines Dienstes durch den Betroffenen als Widerruf der Einwilligung.

C

Technische und organisatorische Maßnahmen

Abs. 1:

Betreiber und Anbieter haben die technischen und organisatorischen Maßnahmen zu treffen, die über die Vorschriften der Datenschutzgesetze hinaus erforderlich sind, um die Ausführung der datenschutzrechtlichen Bestimmungen zu gewährleisten. Das Kabelnetz und seine Zusatzeinrichtungen sind nach dem Stand der Technik und Organisation so auszugestalten und zu betreiben, daß personenbezogene Daten nicht verfälscht, gestört und nicht über den in A und B genannten Umfang hinaus oder durch eine andere als die dort genannte Stelle erhoben, gespeichert oder auf sonstige Weise verarbeitet werden können.

Abs. 2:

Betreiber haben sicherzustellen, daß

1. die Verbindungsdaten unmittelbar nach Ende der Verbindung gelöscht werden,
2. der Teilnehmer personenbezogene Daten nur durch eine eindeutige und bewußte Handlung übermitteln kann,
3. die zu Zwecken der Datensicherung vergebenen Codes einen dem Stand der Technik entsprechenden Schutz vor unbefugter Verwendung bieten,
4. der Teilnehmer seine Verbindung mit dem Veranstalter jederzeit abbrechen kann. In diesem Fall sind alle bereits übermittelten Daten beim Veranstalter sofort zu löschen.

D

Meinungsumfragen

Abs. 1:

Meinungsumfragen mittels Kabelkommunikation über Angelegenheiten, die in den gesetzgebenden Organen des Bundes, der Länder, in den entsprechenden Organen der Gemeinden, der sonstigen kommunalen Gebietskörperschaften, in den Bezirksverordnetenversammlungen oder Bezirksversammlungen behandelt werden, sind unzulässig. Die Ergebnisse von Meinungsumfragen mittels Rückkanal bei den einzelnen Teilnehmern über deren Wahl- oder Stimmverhalten, die sechs Wochen vor der Wahl oder Abstimmung nicht veröffentlicht sind, dürfen vor der Wahl oder Abstimmung nicht bekannt gemacht werden.

Abs. 2:

Bei Meinungsfragen mittels Rückkanal dürfen personenbezogene Daten nur in anonymisierter Form verarbeitet werden.

E

Kontrolle

Abs. 1:

Der Landesbeauftragte für den Datenschutz kontrolliert die Einhaltung der Vorschriften über den Datenschutz.

Abs. 2:

Betreiber und Anbieter sind verpflichtet, dem Datenschutzbeauftragten zur Erfüllung seiner Aufgaben

1. die erforderlichen Auskünfte unverzüglich zu erteilen. Der Auskunftspflichtige kann die Auskunft auf solche Fragen verweigern, deren Beantwortung ihn selbst oder einen der in § 383 Abs. 1 Nr. 1 bis 3 der ZPO bezeichneten Angehörigen der Gefahr strafrechtlicher Verfolgung oder eines Verfahrens nach dem Gesetz über Ordnungswidrigkeiten aussetzen würde;
2. jederzeit den kostenlosen Abruf von Angeboten zuzulassen, Zutritt zu Grundstücken und Geschäftsräumen zu gewähren, dort Prüfungen und Besichtigungen zu gestatten und Einsicht in die geschäftlichen Unterlagen, in die gespeicherten personenbezogenen Daten und die Datenverarbeitungsprogramme nehmen zu lassen. Der Auskunftspflichtige hat die Maßnahme zu dulden. Das Grundrecht der Unverletzlichkeit der Wohnung (Art. 13 GG, Art. 19 Abs. 2 der Verfassung von Berlin) wird insoweit eingeschränkt.

Anhang Nr. 5a

**Entschließung der Konferenz der Datenschutzbeauftragten zur Einführung des Telefon-Fernwirksystems „Temex" vom 6./7. Juni 1984**

Bei der Deutschen Bundespost wird zur Zeit ein sog. „Telefon-Fernwirksystem" mit der Bezeichnung „Temex" vorbereitet.

Weil Fernwirksysteme erlauben, von außen in einer Wohnung Wirkungen auszulösen, Messungen vorzunehmen und Beobachtungen anzustellen, berühren sie maßgeblich die durch Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG geschützte Privatsphäre und das Grundrecht der Unverletztlichkeit der Wohnung (Art. 13 GG). In diese Grundrechte darf nur in engen gesetzlichen Grenzen unter strikter Wahrung des Grundsatzes der Verhältnismäßigkeit bzw. mit ausdrücklicher Einwilligung des Betroffenen eingegriffen werden.

Um eine Verletzung dieser Grundrechte auszuschließen und ausreichenden Datenschutz zu gewährleisten, müssen vor Einführung von Fernwirkdiensten daher eindeutige gesetzliche Regelungen geschaffen werden, die auch die von der Verfassung vorgesehene Kompetenzverteilung zwischen Ländern und Bund berücksichtigt. Solange derartige bereichsspezifische Regelungen fehlen, dürfen Telefon-Fernwirkdienste nicht eingeführt werden.

Anhang Nr. 6

**Beschluß der Internationalen Konferenz der Datenschutzbeauftragten vom 18. Oktober 1983 zur Gewährleistung des Datenschutzes bei Neuen Medien**

1. Die Internationale Konferenz der Datenschutzbeauftragten geht übereinstimmend davon aus, daß der Einsatz Neuer Medien, die über Kabelnetze verbreitet werden, eine erhebliche Gefährdung für die Persönlichkeitsrechte mit sich bringen kann.

   Soweit bei den Neuen Medien die Kommunikation zwischen Informationsanbietern und Teilnehmern durch elektronische Datenverarbeitungsanlagen gesteuert wird, ist – im Gegensatz zu herkömmlichen Medien –

die Speicherung personenbezogener Daten in einem gewissen Umfang erforderlich.

So werden beim Medium „Bildschirmtext" (Videotext) Verbindungs- und Abrechnungsdaten gespeichert. Bei manchen Diensten werden die vom Teilnehmer abgerufenen Sendungen registriert. Das Recht der Unverletzlichkeit der Wohnung wird berührt, wenn mit neuen Diensten von außen in den Wohnungen Wirkungen ausgelöst und Messungen vorgenommen werden.

Über die auf diese Weise an zentralen Stellen automatisiert entstehenden Sammlungen personenbezogener Daten könnten Persönlichkeitsprofile aller Benutzer erstellt werden. Deren soziale Beziehungen und Verhaltensweisen können damit zum Gegenstand von Maßnahmen gemacht werden.

Darüber hinaus können mit Hilfe der Neuen Medien personenbezogene Daten jeglicher Art mit geringem Aufwand und in großem Umfang verbreitet werden. Erfahrungen mit Bildschirmtext haben gezeigt, daß Anbieter und Benutzer mißbräuchlich sensible Daten über die Neuen Medien veröffentlichen.

2. Um die Rechte der Bürger beim Einsatz Neuer Medien zu wahren, erachtet die Konferenz folgendes für erforderlich:

   Durch geeignete Maßnahmen, insbesondere der Gesetzgebung, sollten in jedem Land die Betriebsbedingungen so gestaltet werden, daß durch den Einsatz der Neuen Medien Persönlichkeitsrechte nicht beeinträchtigt werden.

   Hierzu müssen Erhebung, Speicherung und Übermittlung personenbezogener Daten bei der Nutzung auf das unumgängliche Maß eingeschränkt werden. Die Erstellung von Nutzungsprofilen muß untersagt werden.

   Der Inhalt der Informationsangebote darf Persönlichkeitsrechte nicht verletzen. Technische und organisatorische Maßnahmen, die dem jeweiligen Stand der Technik entsprechen, müssen die Durchsetzung dieser rechtlichen Forderungen unterstützen.

   Die Staaten sollten dabei die Auswirkungen bei der grenzüberschreitenden Nutzung beachten; insbesondere sollte verhindert werden, daß durch die Verarbeitung personenbezogener Daten in einem Land bestehende gesetzliche Bestimmungen in einem zweiten Land umgangen werden können. Der Mindeststandard der Richtlinien über den Datenschutz und den grenzüberschreitenden Verkehr mit personenbezogenen Daten der OECD vom 23. September 1980 sowie der Datenschutzkonvention des Europarates vom 28. Januar 1981 sollte auch bei der Nutzung Neuer Medien gewährleistet sein, und zwar auch dann, wenn das nationale Recht Ausnahmebestimmungen vom Datenschutz für Presse und Rundfunk vorsieht.

3. Die Konferenz hält eine internationale Zusammenarbeit der Kontrollinstitutionen für den Datenschutz bei der Überwachung Neuer Medien für geboten.

Anhang Nr. 7

**Beschluß der Konferenz der Datenschutzbeauftragten des Bundes und der Länder und der Datenschutzkommission Rheinland-Pfalz zum Aufbau und zur Einrichtung klinischer Krebsdokumentationen**

Der Aufbau und die Einrichtung klinischer Krebsdokumentationen in den Ländern muß nach Ansicht der Datenschutzbeauftragten der Länder und des Bundes sowie der Datenschutzkommission Rheinland-Pfalz durch Datenschutzkonzeptionen ergänzt werden, die der besonderen Sensitivität dieser Datensammlungen gerecht werden. Die Datenschutzbeauftragten erwarten von den Trägern, die den Aufbau dieser Krankheitsdokumentation fördern und betreiben, neben fachlichen Vorgaben für die Förderung dieser Projekte, im Interesse des betroffenen Patienten auch die Festlegung datenschutzrechtlicher Rahmenbedingungen, die unbedingt eingehalten werden müssen.

Dazu gehört vor allem, daß die Verantwortung für die Einhaltung aller Vorschriften des Datenschutzes eindeutig feststeht. Die unterschiedlichen Bezeichnungen wie „Tumorzentrum e.V.", „Onkologischer Schwerpunkt", haben die Konturen der datenschutzrechtlichen Verantwortlichkeit mehr verwischt als klar umrissen.

Für die Datenschutzbeauftragten kommt als speichernde Stelle in diesem Sinne nur die behandelnde Einrichtung oder Person in Betracht. Gegen diese richten sich auch die subjektiven Rechte der Patienten nach dem Datenschutzgesetz und anderen Vorschriften zur Sicherung ihrer persönlichen Integrität. Aufgaben und Befugnisse in Bezug auf die Verwendung der klinischen Krebsdokumentationen der behandelnden Einrichtungen werden durch den Behandlungsvertrag bestimmt und begrenzt. Dort, wo eine klinische Krebsdokumentation gesondert von der individuellen Patientendokumentation zur Optimierung der Krebsbehandlung und Nachsorge besteht, wird auch ihr Inhalt, Umfang sowie Übermittlung und Speicherungsdauer durch den Behandlungszusammenhang definiert. Über eine klinische Krebsdokumentation ist der Patient bei der Aufnahme einer Behandlung aufzuklären, die erste Speicherung seiner Daten ist ihm mitzuteilen. Werden die Daten für ein bestimmtes Forschungsprojekt über den Behandlungszusammenhang hinaus personenbezogen genutzt, ist in jedem Fall eine Einwilligung nach Aufklärung (informet consent) des betroffenen Patienten erforderlich, es sei denn, die Patientendaten sind anonymisiert bzw. aggregiert.

Die Datenschutzbeauftragten werden auf stenge Maßnahmen der technischen und organisatorischen Datensicherung achten und deren Einhaltung kontrollieren.

Sollte sich im Laufe der Entwicklung zeigen, daß der Behandlungsvertrag bzw. der Behandlungszusammenhang keine geeigneten Kriterien für ausdifferenzierte Dokumentation bietet, ist auch die Notwendigkeit gesetzlicher Regelung bei der Eingriffsintensität einer derartigen personenbezogenen Informationsverarbeitung nicht auszuschließen. Je mehr sich die klinische Dokumentation aus dem Behandlungszusammenhang löst, umso mehr müssen die Grundsätze und Kriterien auch für diese Krebsdokumentation Geltung erlangen, die die Datenschutzbeauftragten zum Modellentwurf für ein Krebsregistergesetz verabschiedet haben.

Anhang Nr. 8

Bayerischer Landtag
10. Wahlperiode

Drucksache 10/3996
07.06.84

Beschluß
des Bayerischen Landtags

Der Landtag hat in seiner heutigen öffentlichen Sitzung beraten und beschlossen:

Antrag der Abgeordneten Regensburger u.a. CSU Drs. 10/2973, 3553, 3812

**Beihilfeunterlagen**

Die Staatsregierung wird ersucht, durch geeignete Maßnahmen und Kontrollen sicherzustellen, daß Beihilfeunterlagen der Mitarbeiter des öffentlichen Dienstes grundsätzlich nur den unmittelbar mit der Bearbeitung der Anträge befaßten Mitarbeitern zur Kenntnis gelangen und nicht zum Nachteil der Betroffenen bei Personalentscheidungen verwertet werden.

Außerdem ist darauf hinzuwirken, daß auch bei den Kommunen entsprechend verfahren wird.

Der Präsident:
Dr. Heubl

Anhang Nr. 9

Bayerischer Senat
1984

Sen-Drucksache 33/84
(zu Sen-Drs 5/84, 20/84)
23.02.84

Beschluß
des Bayerischen Senats

Zum Antrag der Senatoren Gebhard, Burnhauser, Kattenbeck, Dr. Sewering, Spokojny, Dr. Stehle, Dr. Wrede, Dr. Zedelmaier Sen-Drs 5/84

**Persönlichkeitsschutz für Beihilfeberechtigte und Geheimhaltung von Beihilfeanträgen**

Der Senat hat den Antrag in seiner heutigen öffentlichen Sitzung beraten und beschlossen:

Die Staatsregierung wird ersucht, durch organisatorische oder personelle Maßnahmen – soweit bisher noch nicht geschehen – dafür Sorge zu tragen, daß die Krankheitsdaten Beihilfeberechtigter ausschließlich den Beihilfestellen zugänglich bleiben und, wenn dies wegen unvermeidbarer Personalunion der Beihilfesachbearbeitung und anderer dienstlicher Aufgaben nicht möglich ist, die anderweitige Verwertung der Beihilfedaten zu untersagen.

Die Staatsregierung wird außerdem ersucht, dafür Sorge zu tragen, daß in den Gemeinden, Landkreisen, Bezirken und sonstigen der Aufsicht des Staates unterliegenden Körperschaften, Anstalten und Stiftungen des öffentlichen Rechts entsprechend verfahren wird.

Das allgemeine Persönlichkeitsrecht und die Vorschriften über die Geheimhaltung von Beihilfeanträgen sind zu beachten.

Begründung:

In einer Magazin-Sendung des Fernsehens wurde jüngst darauf hingewiesen, daß die Krankheitsdaten Beihilfeberechtigter, die zwangsläufig über die ärztlichen Liquidationen nach der neuen GOÄ erkennbar werden, nicht nur den Beihilfestellen zugänglich sind. In der Folge ist es nicht auszuschließen, daß diese Krankheitsdaten für anderweitige dienstrechtliche Entscheidungen verwendet werden oder diese beeinflussen. Dies hat in der Praxis schon dazu geführt, daß Beihilfeberechtigte davon Abstand nehmen, den ihnen zustehenden Beihilfeanspruch geltend zu machen, weil sie befürchten müssen, daß die damit offengelegten gesundheitlichen Erkenntnisse zu dienstrechtlichen Maßnahmen führen können. In kleineren Verwaltungen ist wegen der Personalunion von Beihilfesachbearbeitung und Personalbewirtschaftung eine Zurückhaltung dieser Daten manchmal nicht möglich. Für diesen Fall muß sichergestellt sein, daß die auf diesem Weg gewonnenen Erkenntnisse nicht in dienstrechtliche Entscheidungen einfließen können.

Der vorstehende Antrag ist auch aus dem Gesichtspunkt des allgemeinen Persönlichkeitsrechts geboten.

Der Präsident:
Dr. Weiß

Anhang Nr. 10 4. November 1983

**Entwurf eines bundeseinheitlichen Gesetzes über die Sicherung und Nutzung von Archivgut**

§ 1
Aufgaben der staatlichen (öffentlichen) Archive

(1) Die staatlichen (öffentlichen) Archive haben die Aufgabe, das Archivgut der öffentlichen Stellen des Landes (der Gemeinden und Gemeindeverbände) und der sonstigen der Aufsicht des Landes unterstehenden juristischen Personen des öffentlichen Rechts und deren Vereinigungen sowie deren Rechtsvorgänger zu erfassen, zu übernehmen, auf Dauer zu verwahren, zu erhalten und insbesondere für wissenschaftliche Zwecke nutzbar zu machen und zu verwerten.

*Anm.:*
*Die Klammerzusätze beachten länderspezifische Unterschiede.*

(2) Die staatlichen (öffentlichen) Archive können auch Archivgut anderer, als der in Abs. 1 genannten öffentlichen Stellen archivieren.

*Anm.:*
*Nur aufzunehmen, wenn in § 1 Abs. 1 „staatliche" Archive steht. Wenn dort „öffentliche" Archive steht, ist dieser Absatz entbehrlich. Folgender Zusatz wäre denkbar: § 4 Abs. 6 bleibt unberührt.*

(3) Die staatlichen (öffentlichen) Archive sammeln sonstiges Dokumentationsmaterial, soweit es der Ergänzung des staatlichen Archivguts dient und für seine Verwahrung keine andere Stelle zuständig ist.

(4) Die staatlichen Archive beraten die in Abs. 1 genannten Stellen des Landes ..... bei der Verwaltung und Sicherung ihrer Registraturen.

*Anm.:*
*Abs. 4 erstreckt sich auf automatisierte Registraturen.*

(5) Die staatlichen (öffentlichen) Archive nehmen Aufgaben im Rahmen der archivarischen Fachausbildung wahr und wirken bei der Aus- und Fortbildung des Registraturpersonals mit.

*Anm.:*
*Hier sind länderspezfische Unterschiede vorhanden.*

§ 2
Archivgut

(1) Archivgut sind alle archivwürdigen Unterlagen wie Akten, Einzelschriftstücke, Bild- und Tonmaterial, Karten, Pläne, Dateien oder Teile davon, maschinenlesbare Datenträger, auf diesen gespeicherte Informationen und Programme zu ihrer Auswertung sowie sonstiges Informationsmaterial und Hilfsmittel zu ihrer Nutzung, die bei den in § ... (Verweis aus Geltungsbereich) genannten Stellen oder deren Rechts- oder Funktionsvorgängern oder bei natürlichen oder juristischen Personen erwachsen sind oder sich in deren Besitz befinden.

*Anm.:*
*Dieser Teilsatz soll sicherstellen, daß auch die Unterlagen der Rechtsvorgänger (z. B. alliierte Spruchkammern) Archivgut darstellen.*

(2) Archivwürdig sind Unterlagen, die für die Erforschung und das Verständnis der Geschichte von bleibendem Wert sind und Unterlagen, die aufgrund von Rechtsvorschriften dauernd aufzubewahren sind.

*Anm.:*
*Es ist darauf verzichtet worden, Unterlagen auch für Zwekke der Verwaltung als archivwürdig zu bezeichnen, weil eine Vermischung von Aufgaben und Nutzungsrechten vermieden werden soll.*

§ 3
Aussonderung und Anbietung von Archivgut

(1) Die in § 1 Abs. 1 bezeichneten Stellen sind verpflichtet, dem zuständigen Archiv die Unterlagen, die sie zur Erfüllung der Aufgaben nicht mehr dauernd benötigen (die zu der durch Rechtsnorm zugewiesenen Aufgabenerfüllung nicht mehr erforderlich sind), unverzüglich zur Übernahme anzubieten, es sei denn, die Unterlagen sind offensichtlich von geringer Bedeutung. Unterlagen sind spätestens 30 Jahre nach ihrer Entstehung auszusondern und anzubieten, soweit nicht Rechtsvorschriften andere Fristen vorsehen.

*Anm.:*
*Hier soll die Mitwirkung der Archive bei der Löschung von Daten entfallen. Die Archivklausel (z. B. § 16 Abs. 3 S. 1 BrDSG) ist zu streichen.*

*Anm.:*
*Diese Verpflichtung umfaßt auch personenbezogene Daten, die vom Landesdatenschutz geschützt sind, selbst wenn sie gesperrt sind (dieser deklatorische Satz kann auch in den Gesetzestext übernommen werden).*

(2) Soweit gleichförmige Unterlagen, die in großer Zahl anfallen, archivwürdig sind, sind Art und Umfang der vom zuständigen Archiv zu übernehmenden Unterlagen durch Vereinbarung der jeweils zuständigen obersten Landesbehörde mit dem zuständigen Archiv im Grundsatz festzulegen. Diese Unterlagen dürfen nicht vollständig, sondern nur in einer Auswahl übernommen werden.

*Anm.:*
*Diese Regelung schützt davor, daß das Datenschutzgesetz leerläuft.*

(3) Anzubietende Unterlagen können auch Abbildungen von automatisierten Dateien zu einem bestimmten Stichtag sein. Stichtag, Umfang und Auswahl sind durch Vereinbarung zwischen der jeweils zuständigen obersten Landesbehörde und dem zuständigen Archiv im Benehmen mit dem Landesbeauftragten für den Datenschutz festzulegen. Diese Unterlagen sind dem zuständigen Archiv unmittelbar nach Erstellung anzubieten. Einsichtnahme und Nutzung (Benützung) durch das Archiv sind nicht vor Ablauf der in § 6 Abs. 3 genannten Fristen zulässig.

(4) Die gesetzgebenden Körperschaften sowie die der Aufsicht des Landes unterstehenden juristischen Personen des öffentlichen Rechts und deren Vereinigungen bieten, vorbehaltlich anderer gesetzlicher Regelungen oder soweit sie kein eigenes Archiv unterhalten, Unterlagen entsprechend Abs. 1 dem zuständigen Archiv zur Übernahme an.

*Anm.:*
*Hier sollen auch die Verfassungsorgane eingezogen werden.*

(5) In Ausnahmefällen ist im Benehmen mit dem zuständigen Archiv die Abgabe an ein anderes Archiv zulässig, wenn die Einhaltung der in diesem Gesetz für die Aufbewahrung und Benutzung von Archivgut getroffenen Bestimmungen gewährleistet ist.

§ 4
Übernahme des Archivgutes

(1) Das zuständige Archiv übernimmt die von ihm im Benehmen mit der anbietenden Stelle als archivwürdig bestimmten Unterlagen. Übernimmt das Archiv nicht binnen 6 Monaten die angebotenen Unterlagen, sind diese zu vernichten.

(2) Archivwürdige Unterlagen können bereits vor dem Entstehen der in § 3 Abs. 1 genannten Anbietungspflicht endgültig in das zuständige Archiv übernommen werden.

(3) Das zuständige Archiv kann im Auftrage staatlicher (öffentlicher) Stellen Unterlagen aufbewahren. Speichernde (verantwortliche) Stelle für diese Unterlagen bleibt die abgebende Stelle. Die Regelungen zur Anbietungspflicht, zur Entscheidung über die Archivwürdigkeit und Übernahme der Unterlagen finden Anwendung.

(4) Den Vertretern der staatlichen (öffentlichen) Archive ist zur Erfüllung ihrer Aufgaben Zutritt zu den Registraturen der Behörden und sonstigen öffentlichen Stellen und Einsicht in die angebotenen Unterlagen und die Findmittel der Registraturen zu gewähren.

*Anm.:*
*Kann auch in § 3 geregelt werden.*

(5) Die oberste Archivbehörde wirkt bei der Archivgutaussonderung mit. Sie erläßt insbesondere Richtlinien zur Bestimmung der Archivwürdigkeit.

*Anm.:*
*Diese Regelung gilt nur für Flächenstaaten mit Mittelbehörden.*

(6) Die staatlichen (öffentlichen) Archive können von Behörden und sonstigen öffentlichen Stellen des Bundes, bundesunmittelbarer Körperschaften, Anstalten und Stiftungen des öffentlichen Rechts sowie von Vereinigungen

solcher Körperschaften, Anstalten und Stiftungen, soweit sie nicht der Aufsicht des Landes unterliegen, archivwürdige Unterlagen übernehmen, soweit dies im öffentlichen Interesse liegt. Dies gilt entsprechend für die Übernahme privaten Archivgutes.

§ 5
Sicherung des Archivgutes

(1) Die staatlichen (öffentlichen) Archive sind befugt, das Archivgut nach archivwissenschaftlichen Gesichtspunkten zu ordnen, durch Findmittel zu erschließen, zu nutzen sowie Unterlagen, deren Archivwürdigkeit nicht mehr gegeben ist, auszusondern und zu vernichten. Das Zusammenführen personenbezogener Informationen durch das Archiv ist nur zu lässig, wenn schutzwürdige Belange Betroffener oder Dritter nicht beeinträchtigt werden. Für Abbildungen nach § 3 Abs. 3 gilt Satz 1 erst nach Ablauf der Fristen des § 6 Abs. 3.

(2) Sie haben die technischen und organisatorischen Maßnahmen zu treffen, die erforderlich sind, um die ordnungs- und sachgemäße dauernde Aufbewahrung und Benutzbarkeit des Archivguts sowie seinen Schutz vor unbefugter Benutzung oder vor Vernichtung sicherzustellen. Gleiches gilt für die im Auftrag verwahrten Unterlagen.

*Anm.:*
*In der Begründung kann auf die Regelungen in den Datenschutzgesetzen hingewiesen werden.*

(3) Von einem staatlichen (öffentlichen) Archiv verwahrtes Archivgut des Landes kann mit Zustimmung der obersten Archivbehörde (gegen einen angemessenen Wertausgleich) an ein anderes Archiv abgegeben werden, wenn die Abgabe im öffentlichen Interesse liegt, archivwissenschaftlichen Grundsätzen entspricht und wenn schutzwürdige Belange Betroffener und Dritter dadurch nicht beeinträchtigt werden.

§ 6
Nutzung von Archivgut

(1) Jedermann hat das Recht, auf Antrag das in den öffentlichen Archiven verwahrte Archivgut nach Ablauf der festgelegten Sperrfristen zu wissenschaftlichen oder journalistisch-redaktionellen Zwecken sowie zur Wahrung berechtigter persönlicher Belange zu benutzen, soweit durch dieses Gesetz oder aufgrund dieses Gesetzes nichts anderes bestimmt ist. Bestehende Informationsrechte oder besondere Vereinbarungen mit Eigentümern privaten Archivguts bleiben unberührt. Die Nutzung von Archivgut ist einzuschränken oder zu versagen, wenn schutzwürdige Belange Betroffener, Dritter oder überwiegende Gründe des Gemeinwohls entgegenstehen oder der Erhaltungszustand des Archivguts gefährdet ist. Das Archiv kann die Nutzung von der Beachtung der Nebenbestimmungen abhängig machen.

*Anm.:*
*Hier könnte ein Hinweis auf Bußgeldbewehrung angebracht sein.*

(2) Belange von Amtsträgern sind in der Regel nicht vorrangig schutzwürdig, wenn die Amtsträger in Ausübung ihrer dienstlichen Obliegenheiten gehandelt haben.

(3) Soweit durch Rechtsvorschriften keine anderen Sperrfristen bestimmt sind, bleibt Archivgut mit Ausnahme bereits bei ihrer Entstehung zur Veröffentlichung bestimmter Unterlagen für 30 Jahre nach der Übernahme durch das Archiv von der Benutzung ausgeschlossen. Archivgut, das besonderen Geheimhaltungsbestimmungen unterliegt, bleibt darüber hinaus 60 Jahre nach der Übernahme durch das Archiv von der Benutzung ausgeschlossen. Archivgut, das sich nach seiner Zweckbestimmung auf natürliche Personen bezieht (personenbezogenes Archivgut), darf jedoch frühestens 30 Jahre nach dem Tode des Betroffenen durch Dritte benutzt werden. Ist der Todestag nicht festzustellen, endet die Sperrfrist 120 Jahre nach der Geburt des Betroffenen. Werden Unterlagen vor Ablauf der Aufbewahrungsfristen vom Archiv übernommen, verlängert sich die Sperrfrist um den noch nicht abgelaufenen Aufbewahrungszeitraum.

*Anm.:*
*zum Zeitpunkt der „Übernahme": Aus datenschutzrechtlicher Sicht ist diese klare Regelung erforderlich (abweichend von anderen Formulierungsvorschlägen), da dadurch eine eindeutige Fristberechnung möglich ist.*

(4) Mit Zustimmung der abgebenden Stelle können die Sperrfristen im Einzelfall oder für bestimmte Archivgutgruppen verkürzt oder um höchstens 20 Jahre verlängert werden, wenn dies im öffentlichen Interesse liegt und kein Grund zur Annahme besteht, daß schutzwürdige Belange der Betroffenen oder Dritter entgegenstehen. Bei personenbezogenem Archivgut ist eine Verkürzung nur zulässig, wenn dies zur Erreichung des wissenschaftlichen Zwecks, zur Behebung einer bestehenden Beweisnot oder aus sonstigen, im überwiegenden Interesse der abgebenden Stelle liegenden Gründen oder bei rechtlichem Interesse eines Dritten erfolgt und durch Anonymisierung oder auf andere Weise sichergestellt ist, daß schutzwürdige Belange des Betroffenen oder Dritter nicht beeinträchtigt werden oder wenn die Betroffenen in die Benutzung eingewilligt haben.

(5) Behörden ist die Benutzung solcher personenbezogener Daten zu versagen, die bei der abgegebenen Stelle aufgrund besonderer Vorschriften zum Schutz des Betroffenen hätten gelöscht oder gesperrt werden müssen; gleiches gilt für sonstige Unterlagen, die aufgrund von Rechtsvorschriften hätten vernichtet werden müssen. Dies gilt nicht, wenn die Daten aufgrund von Rechtsvorschriften für Zwecke der Sicherung von Rechten oder Beweisen aufzubewahren sind oder wenn ihre Benutzung durch die Behörde dem Vorteil des Betroffenen zu dienen bestimmt ist oder wenn der Betroffene eingewilligt hat.

(6) Das Nähere wird durch eine Benutzungsordnung geregelt.

§ 7
Recht auf Auskunft und Gegendarstellung

(1) Dem Betroffenen ist auf Antrag nach Maßgabe des § ... des Landesdatenschutzgesetzes Auskunft über die im Archivgut zu seiner Person enthaltenen Daten zu erteilen. Statt einer Auskunft kann das Archiv Akteneinsicht gewähren.

(2) Das Archiv ist verpflichtet, eine Gegendarstellung des Betroffenen und bei rechtlichem Interesse seiner Hinterbliebenen dem Archivgut hinzuzufügen, die sich auf die Person des Betroffenen bezieht, wenn der Betroffene durch fal-

sche Tatsachenbehauptungen beeinträchtigt ist und ein berechtigtes Interesse an der Gegendarstellung glaubhaft gemacht wird.

(3) Aufgrund besonderer Rechtsvorschriften zu berichtigende Unterlagen sind um eine Richtigstellung zu ergänzen. Ist dies nicht möglich, besteht eine Verpflichtung zu deren besonderen Kennzeichnung.

(4) Diese Bestimmungen gelten nicht für amtliche Niederschriften über Sitzungen der gesetzgebenden oder beschließenden Körperschaften des Bundes, der Länder, der Gemeinden (Gemeindeverbände) und der Gerichte.

§ 8
Offenbarung von Geheimnissen

(1) Landesrechtliche Regelungen über Berufs- oder besondere Amtsgeheimnisse stehen einer Anbietung und Übernahme von Unterlagen nicht entgegen.

*Anm.:*
*Baden-Württemberg wird einen Formulierungsvorschlag erarbeiten, der insbesondere die Probleme der besonderen Berufs- und Amtsgeheimnisse berücksichtigt (z.B. § 203 StGB).*

(2) Archivgut, das einem Berufs- oder besonderen Amtsgeheimnis unterliegt, darf erst 60 Jahre nach seiner Übernahme, jedoch frühestens 150 Jahre nach der Geburt des Betroffenen benutzt werden.

§ 9
Sonstige öffentliche Archive

Soweit die in § 3 Abs. 4 genannten Stellen eigene Archive unterhalten und für diese Stellen keine besonderen Rechtsvorschriften gelten, sind die Bestimmungen dieses Gesetzes sinngemäß anzuwenden.

§ 10

Die oberste Archivbehörde wird ermächtigt, durch Rechtsverordnung

1. die örtliche und sachliche Zuständigkeit der staatlichen (öffentlichen) Archive,
2. das Verfahren zur Zulassung und die Benutzung der staatlichen Archive,
3. ...
4. ...

zu regeln.

§ 11
Ordnungswidrigkeiten

Schlußbemerkung

Eine eigene Regelung für Kommunen ist insbesondere für Flächenstaaten angezeigt.

Anhang Nr. 11 4. November 1983

**Beschluß der Datenschutzbeauftragten der Länder zur MiStra**

I. Allgemeines

Die Landesbeauftragten und der Bundesbeauftragte sowie die Datenschutzkommission Rheinland-Pfalz haben bereits mit Beschluß vom 30. September 1980 zu der Anordnung über Mitteilungen in Strafsachen (MiStra) Stellung genommen. Schwerpunkte dieses Beschlusses waren die Forderungen, die MiStra so zu überarbeiten, daß nur noch die Vorschriften bestehen bleiben, für die eine gesetzliche Rechtsgrundlage besteht, oder andernfalls eine eindeutige gesetzliche Grundlage zu schaffen. Dabei sollte auch der Umfang der bisherigen Mitteilungspflichten reduziert werden.

Die Datenschutzbeauftragten begrüßen es, daß ein von den Justizverwaltungen eingerichteter Arbeitskreis die Anordnung über Mitteilungen in Strafsachen einer Überprüfung unterzogen hat.

Auf der Grundlage des vorgenannten Beschlusses ist zu dem vorliegenden Entwurf der Anordnung für Mitteilungen in Strafsachen (MiStra) folgendes zu bemerken:

1. Mit Bedauern wird festgestellt, daß die im Beschluß genannten Forderungen und Anregungen nur zu einem geringen Teil aufgegriffen werden.
2. Eine Klärung der Frage steht noch aus, inwieweit für die Mitteilungen in Strafsachen bereits eine Rechtsgrundlage besteht oder ob eine weitergehende gesetzliche Grundlage geschaffen werden muß. Der Entwurf hält offensichtlich an der bisherigen Rechtsqualität als Verwaltungsvorschrift fest, ohne eine Begründung zu nennen, obwohl der Unterausschuß der Justizministerkonferenz selbst sich auf der Sitzung am 18. und 19. Mai 1981 für die Schaffung einer Rechtsgrundlage ausgesprochen hat. Weil derartige Mitteilungen für die Betroffenen einen Eingriff darstellen, bedürfen sie einer Rechtsgrundlage.
3. Der Grundsatz der Zweckbindung der Verwendung von Daten im Datenschutzrecht soll sicherstellen, daß Daten nur von denjenigen Stellen verwendet werden, die sie zur gesetzlichen Aufgabenerfüllung benötigen. Eine strenge Zweckbindung soll damit verhindern, daß Daten an andere Stellen gelangen und dort für andere als die ursprünglich vorgesehenen Zwecke Verwendung finden. Wegen der Sensibilität der auf Grund der MiStra mitgeteilten Daten hat der Grundsatz der Zweckbindung besonderes Gewicht. Neben einer Regelung in Nr. 3 (vgl. die dortigen Anmerkungen) ist eine eindeutige Vorschrift in der MiStra notwendig, die die Beachtung der Zweckbindung in allen Mitteilungsfällen sicherstellt.
4. Der vorliegende Entwurf sieht ohnehin eine Vielzahl von einzelnen Mitteilungsvorgängen vor. Eine Erweiterung dieses Katalogs durch relativ weitgehende Bestimmungen (vgl. Nr. 2 Abs. 2 Nr. 3 und Nr. 29) birgt die Gefahr in sich, daß die auf den Einzelfall bezogenen Regelungen und deren bewußte Beschränkungen umgangen werden. Damit wäre aber der Sinn der Einzelregelungen gefährdet, nämlich die mögliche Beeinträchtigung der durch Art. 1 Abs. 1 und Art. 2 Abs. 1 GG geschützten Persönlichkeitssphäre des Betroffenen zu begrenzen. Daher sollte die Neufassung eine abschließende Regelung der Mitteilungsvorgänge enthalten.
5. Im Hinblick auf die Auswirkungen, die die Mitteilungen für den Betroffenen haben können, sollten diese im Regelfall vom Richter oder Staatsanwalt veranlaßt werden. Nur in Fällen, in denen nach den Einzelregelungen kein

Entscheidungsspielraum besteht, sollte die Geschäftsstelle zur Anordnung der Mitteilung befugt sein. Diese Umkehrung des im Entwurf und der geltenden Fassung der MiStra enthaltenen Regel- und Ausnahmeverhältnisses drängt sich auch nach den Begründungen des Arbeitskreises der Justizverwaltungen auf. Dieser Arbeitskreis lehnt bei einer Reihe von Bestimmungen eine Neuregelung deshalb ab, weil die Geschäftsstellen bei einem geänderten, dem Datenschutz aber eher Rechnung tragenden Vollzug überfordert wären.

6. Die Mitteilungen in Strafsachen sollen die zu benachrichtigenden Behörden in Kenntnis von den Vorgängen setzen, auf die sie im Rahmen des ihnen zugewiesenen Aufgabenbereichs zu reagieren haben. Ein strafrechtlich relevanter Sachverhalt läßt sich jedoch abschließend erst nach Abschluß des Strafverfahrens beurteilen. Damit den von den Mitteilungen Betroffenen nicht unnötige Nachteile entstehen, sollte der Grundsatz in der MiStra ausdrücklich festgelegt werden, daß Mitteilungen erst nach rechtskräftigem Abschluß des Strafverfahrens erfolgen dürfen. Auch der Inhalt der Mitteilungen ist auf das im Einzelfall wirklich notwendige Mindestmaß zu beschränken. Das bedeutet, daß im Regelfall die Mitteilung der Tatsache einer Verurteilung unter Angabe der Straftat genügen wird. Ausnahmen hinsichtlich einer vorzeitigen Mitteilung oder eines umfangreicheren Inhalts der Mitteilungen müssen auf die Fälle beschränkt werden, in denen wegen der Bedeutung des möglicherweise verletzten Rechtsguts die begründete Ausnahme besteht, daß vorzeitige Maßnahmen veranlaßt sind oder die zu benachrichtigende Behörde nur auf Grund umfassender Kenntnis des dem Strafverfahren zugrundeliegenden Sachverhalts geeignete Maßnahmen treffen kann.

   Im einzelnen ist hier folgendes zu beachten:

   Soweit unter Berücksichtigung des Verhältnismäßigkeitsgrundsat- zes Mitteilungen überhaupt erforderlich sind, sollten diese erst nach rechtskräftigem Urteil, das eine Verurteilung ausspricht, erfolgen. Diese Mitteilungen sollten sich entweder auf die Tatsache der Verurteilung oder auf den Abdruck des Urteilstenors beschränken.

   Sollten Mitteilungen vorher erforderlich sein, dann dürfen diese grundsätzlich erst zum Zeitpunkt der Erhebung der öffentlichen Klage gemacht werden. Erst zu diesem Zeitpunkt ist bereits eine gewisse Erfolgsaussicht der Klage nach der Beurteilung des Staatsanwaltes anzunehmen. Diese vorzeitige Mitteilung kann nur dann veranlaßt sein, wenn begründete Anhaltspunkte vorliegen, daß die zu benachrichtigende Behörde Maßnahmen treffen muß, bevor das Verfahren abgeschlossen ist. Hierzu ist nur der Anklagesatz zu übermitteln. Keinesfalls darf das wesentliche Ergebnis der Ermittlungen übersandt werden.

   Mitteilungen über die Einleitung des Verfahrens sollten auf die wenigen Ausnahmefälle beschränkt bleiben, in denen begründete Anhaltspunkte vorliegen, daß die zu benachrichtigende Behörde sofortige Maßnahmen einleiten muß. Der Inhalt der Mitteilung ist auf die Formel des Strafvorwurfs zu beschränken. Gleiches gilt für Mitteilungen über den Erlaß eines Haftbefehls.

7. Der Betroffene ist grundsätzlich davon zu benachrichtigen, welchen Stellen Mitteilungen nach der MiStra gemacht wurden. Von einer Benachrichtigung des Betroffenen kann ausnahmsweise nur dann abgesehen werden, wenn schwerwiegende Bedenken in der Person des Betroffenen entgegenstehen.

   Die Benachrichtigung könnte organisationstechnisch ohne großen Aufwand beispielweise mit einem zusätzlichen Formblatt im Durchschreibeverfahren erfolgen. Wesentliche Kostenfolgen dürften damit wohl kaum verbunden sein.

8. Die in der Mitteilung von Strafsachen liegenden Eingriffe sind auf das unbedingt erforderliche Maß zu begrenzen. Deshalb ist durch eindeutige Adressierung sicherzustellen, daß von diesen Mitteilungen nur die Personen in den zu benachrichtigenden Behörden Kenntnis erlangen, welche diese Kenntnis zu ihrer Aufgabenerfüllung benötigen. (Beispielsweise sind Mitteilungen an den Leiter der Behörde oder die personalsachbearbeitende Stelle zu richten, wenn Mitteilungen öffentlich Bedienstete betreffen.) Außerdem sind derartige Mitteilungen in jedem Fall verschlossen zu versenden.

9. Die fahrlässige Begehung einer Straftat weist grundsätzlich auf ein geringeres Maß an strafrechtlicher Vorwerfbarkeit hin. Mitteilungen, die Fahrlässigkeitstaten betreffen, sollten daher grundsätzlich nicht im Rahmen der MiStra mitgeteilt werden. Dies gilt insbesondere bei fahrlässigen Verkehrsstraftaten. Nur bei engem Bezug zur beruflichen Tätigkeit des von der Mitteilung Betroffenen und besonderem Gewicht des verletzten Rechtsguts sollten Ausnahmen gemacht werden. Die Prüfung, ob auch in diesen Fällen eine Mitteilung nicht erst nach rechtskräftigem Abschluß des Verfahrens erfolgen muß, sollte bei Fahrlässigkeitstaten besonders gründlich erfolgen.

10. Der Vollzug der Mitteilung scheint nicht gleichmäßig zu erfolgen. Wegen der belastenden Wirkung, die die einzelnen Mitteilungen für die davon Betroffenen haben, entsteht hier eine nicht hinzunehmende Ungleichbehandlung. Möglicherweise ist diese Ungleichbehandlung ein Indiz dafür, daß manche Mitteilungspflichten als nicht mehr zeitgerecht empfunden werden; dies wäre ein Anlaß zu noch strengerer Prüfung der Erforderlichkeit.

## Stichwortverzeichnis

zum 6. Tätigkeitsbericht des Bayerischen Landesbeauftragten für den Datenschutz